BCP/DRP
By
Larry Greenblatt

http://www.InternetWorkDefense.com

Edited by: Charlene Wu, CISSP-ISSMP

This document is an open source document, feel free to distribute. This is intended to be a living document, a work in progress. We welcome suggestions for continual process improvement.
Send your comments to: admin@internetworkdefense.com

This document was produce by my good friend Larry Greenblatt. Larry has spent countless hours and lots of money to acquire all of the ISO standards that he used as references to produce this document..

I have simply done a bit of beautifying and added a bit here and there to highlight some of things you MUST know for the exam. Larry produce what I consider the best BCP and DRP resources you can get for your exam preparation while maintaining contact with reality by using real life scenarios and up to date information.

Work very well done my friend!!

Clement Dupuis, CD
Owner and Maintainer
The CCCure Family of Portals

Contents

BC/DR By Larry Greenblatt

Business Continuity and Disaster Recovery (BC/DR)

Exam objectives in this chapter

- Understand how to responsibly manage residual risks.
- Estimate the impact of a loss of critical business processes, service or supplies
- Create plans to handle actualized loss events to protect human life, the organization, and the common wealth.
- Develop and maintain relationships with outside providers to procure critical services and supplies to provide contingencies during a disaster scenario.
- Test plans, Train people and Exercise procedures (TT&E) for continual process improvement.

Unique Terms and Definitions

Business Continuity management (BCM)

> Umbrella term used by many international standards bodies for various sub-processes to maintain an organization after some disruption or disaster (similar to COOP in many US government standards)

Business Impact Analysis (BIA)

> Analysis of the affects to an organization, if an organization's residual risk were to be actualized effecting, with primary goal to establish criticality metrics and requirements

Continuity Of Operations (COOP)

> (See BCM)

Crisis / Disaster / Emergency

> Actualized risks that can result in loss of life or business

Emergency management team

> The overall team that responds to reports of disasters. Their job is not done until normal operations has been restored or reconstituted.

Emergency Operations Center (EOC)

Command and control center during a crisis / emergency or disaster

Information Communication Technology (ICT)

This is an International term use to describe the technical infrastructure supporting an organization. In the USA, this is usually expressed as Information Technology (IT)

Minimum Operating Requirements (MOR)

Services and supplies required to maintain essential functions. Part of service level management and sometimes referred to as Service Deliverable Objectives (SDO) or Service Level Objectives (SLO)

Occupant Emergency Plan (OEP)

Plans to protect the people in a facility including evacuation

Recovery

The process of restoring services after a disaster to acceptable levels in the required times

Recovery Team

Those charged with performing the Disaster Recovery Plan

Reconstitution

Returning to normal operations

Reconstitution Team

Those charged with the task of safe fail back to normal operations.

Recovery Point Objectives (RPO)

The point in time which data should be restored

Recovery Time Objectives (RTO)

The time by which mission critical processes must be recovered

Preparedness

The state of being ready for disaster or catastrophe with plans, procedures, equipment, facilities and trained personnel.

INTRODUCTION

If you ask the wrong questions, the answers won't matter. Many times information security is associated with privacy. But what good is an asset, if you can't access it? The Business Continuity and Disaster Recovery domain is frequently described as the most challenging part of the CISSP exam. Part of this is perhaps due to the fact that it is overlooked, for the above reason.

Another reason the BC/DR domain is so often difficult on the test as well as in the real world, I suspect, is due to the lack of consistency of the terminology used throughout the US and international business world. It is no easy task to either create or undertake an exam that tests for "common knowledge" in any of domains, but, in my view, the BC/DR domain is the toughest in terms of interpreting the meaning of the questions.

EXAM WARNING

I suspect that whenever possible, defaulting to ISO terminologies is safest for both taking the CISSP exam, as well as truly protecting the common wealth. In the last few years, the ISC2 appears to have a more consistent terminology, adopted from the ISO. To this nerdy author, the ISO is much like the Federation in the television show, Star Trek, not perfect by any means, but the best thing in the universe I know of, to get everyone on the same page. Personally, I believe this is a great step forward.

STATE OF THE ISO STANDARD ISO/IEC-27031

The ISO has a standard (in draft form) ISO/IEC-27031 - ICT readiness for business continuity (as part of the SC-27 or 27XXX series). The ISO/IEC-27031 aims to provide internationally recognized processes and terminologies for information communication technology, Business Continuity Management, or BCM.

While this proposed standard is in draft mode, there are many internationally recognized standards in existence, but they do not seem to line up exactly, thus causing confusion among practitioners. Even in the US government sector, terminology is not always consistent. For example, FEMA standard documentation refers to the BCM field as COOP, but in NIST documentation SP800-34, COOP is seen as a subset of BCP (Business Continuity Planning). Unfortunately, in my opinion, there is very little "common knowledge" in the BC/DR field.

EXAM WARNING

When preparing for the CISSP exam, it is very important to understand, not only the key BC/DR processes. In addition, it is equally important and perhaps even more challenging to understand the various terminologies used by national and international standards bodies (for example, the ISO, NIST, BSI, FEMA, SPRING) and best practice organizations (for example, DRII, BCI, NFPA); and the complex scenarios and writings used in previous ISC2 exams.

The CISSP candidates may have many years of experience in this field and can perform their job with proficiency, but they fail to understand the questions on the exam because of a misunderstanding of the terminologies. This is especially true, I find when the candidates, are not proficient in English. Some of my students speak up to six languages, but the CISSP exam is primarily offered in English (as of this writing the CISSP exam is now offered in English, French, German, Spanish, Koean, and Japanese versions).

UNDERSTAND HOW TO MANAGE RESIDUAL RISKS

In this chapter, the CISSP candidate is expected to:

1) Recall the lessons learned from the Information Security and Risk Management module, in particular, the concepts of accepted, ***yet high impact***, residual risks.
2) Understand BC/DR life cycle phases.
3) Recognize various terminologies that may be used to describe the processes, procedures and metrics performed and managed at the different phases in the BCM life cycle.
4) Deal with “High Impact / Low Likelihood” Events.

SCENARIO

The following scenario can be used to illustrate some of the key concepts of BC and DR:

Imagine you are driving to an appointment. Your destination is 100 miles away and typically this drive takes 2 hours but you gave yourself 3 hours just in case there was a problem. Along the way you get a flat tire and a blow out in the left lane during a downpour. The first thing you need to do is make sure you can get to the side of the road safely. Then you need to change the tire and get back on the road all within an hour since this is all the wiggle room you have.

The above scenario illustrates a *low likelihood but high impact* event for me personally. Since I have been driving a car for a number of years now and have had only one tire blowout on the highway throughout my driving history. However, it was also a high impact event because it was pouring rain and I was traveling in the left lane of the Schuylkill expressway (or "sure kill" as we say in Philadelphia), when I got the flat tire.

Criticality metrics:

In our flat tire example, a BC manager, would call the one hour "wiggle room" something like the "Maximum Tolerable Downtime" or **MTD**. When the service interruption (the flat) occurred, the first priority is to protect life by pulling over to the side of the road safely. Since this emergency management step may take some time, then the next two steps of putting on the spare tire and getting back on the road must be accomplished in less than the one hour window (recovery time objective). Thus, the recovery time objective or **RTO** must be less than the maximum tolerable downtime or **MTD**. But our driver is not out of the woods yet. The spare tire will likely not provide the same service level as the primary tire and he now no longer has a spare tire in case of another emergency.

Does the reader know the service life (in miles) of their emergency spare tire? I recommend you find out ;-)

Recap

List of very *testable* processes preparing for and following a disaster using our flat tire example.

Preparation	The fact that there was a spare tire, a jack, procedures and personnel trained to change tires.
Maximum Tolerable Downtime (MTD)	One hour wiggle room

Recovery Time Objective (RTO)	The total time that it will take to get back on the road (mount the spare tire, store the jack and the damaged tire and etc.)
Detection / Notification	Realizing something was wrong using negative feedback indicators such as feeling the ride get bumpy or seeing a problem in the rear view mirrors and etc. Notification to other stakeholders such as telling others in the car about the problem or putting on the blinkers for other drivers and etc.
Crisis/Emergency Management	Pulling to the side of the road and perform initial damage assessment with the primary focus on life and safety.
Activation	Based on the feedback of the damage / impact assessment, the decision to switch to alternate operations. This step requires *confirmation* of the incident. For example, perhaps the bumpy drive wasn't actually due to the owner's vehicle but just a bumpy road.
Recovery	“Fail Over”. Short term restoration of essential services, critical data and processes. In our example, we '”fail over” by switching to the spare tire.
Reconstitution	“Fail back”. Returning to normal operations. In our example, we repair / replace the original tire.
Resumption	Getting back on the road and headed towards the destination.

Exam Exercise

Bob is asked to perform a business impact analysis for the customer service department. He is currently reviewing the service level agreements to determine the **most** cost effective plan. Which of the following metrics will **MOST** help Bob in his analysis?

a) Resource Dependency Analysis

b) Supply Chain Management

c) Impact Assessment

d) Minimum Operating Requirements

The answer to the exercise above is: **d**

The question asked for "**metrics**" (measurements). Answers a, b and c are processes, not metrics. It is true that each of the above processes is quite necessary to understand the Minimum Operation Requirements or MOR metrics.

For example, Bob will need the outputs from resource dependency analysis, supply chain management and impact assessment processes in order to determine the most cost effective way to meet the Customer Service Department's requirements of 10GB per second per external network service to the mirrored site for example.

CREATE PLANS TO HANDLE ACTUALIZED LOSS EVENTS TO PROTECT LIFE AND THE ORGANIZATION

CONTINGENCIES

In Information Security and Risk Management, a manager understands that after taking all the prudent steps to reduce risks, there will always be residual risk (as learned in Information Security module). For risks that are considered low likelihood but high impact such as man-made or natural disasters, a responsible organization will have plans to deal with these security events. Business Continuity Management (BCM) is often used as a high level term that collectively includes components such as plans for emergency evacuations, crisis management, incident response, alternate data processing facilities, alternate end user facilities and other contingency plans. However, as I have alluded earlier, in some governmental agencies, the umbrella term for the above processes is termed Continuity of Operations (COOP).

Business Continuity and Disaster Recovery : Standards and Guidelines

While the ISO has the BC/DR as part of the 27001 standard, it has not yet completed a dedicated standard for ICT as part of the BCM. As mentioned earlier, there is a draft of ICT BCM, as part of the SC27 – Security Techniques series, which will become ISO/IEC-27031 when adopted.

Note:

The ISO did release a related document, ISO/PAS-22399:2007- Societal security - Guideline for incident preparedness and operational continuity management. This document is the first released under the Technical Committee 223 for societal security.

Please note, this is not part of the SC-27 series nor is it very technical, which is why it is listed as ISO/PAS for Publicly Available Specification (PAS) as opposed to the ISO/IEC for International Electrotechnical Commission (IEC).

For the purposes of passing the CISSP, I wouldn't expect much help from any further coverage of ISO/PAS 22399 and ISC2 questions will likely await passage of ISO/IEC-27031. I suspect the ISC2 will not cover any of ISO/PAS 22399:2007 on the exam.

Re-cap:

BCM related documents from the ISO, SC 27: Security Techniques series (ISO 27xxx series)

Document Name / (type)	Scope
ISO/IEC-27001 (standard)	Information technology -- Security techniques -- Specification for an Information Security Management System
ISO/IEC-27002 (guideline)	Information technology -- Security techniques -- Code of practice for information security management
ISO/IEC-27005 (guideline)	Information technology -- Security techniques -- Information security risk management
ISO/IEC-27031 (draft)	ICT readiness for business continuity

The future of ISO/IEC 27031, the Business Continuity Institute's Good Practice Guidelines and the British Standards Institute

First published in 2002, the Good Practice Guidelines (GPG) from the Business Continuity Institute (BCI) has become a well recognized document for English-speaking business continuity professionals throughout the world. This free document is very closely associated the British Standards Institutes's documents on BCM. As BS 7799 became the template for ISO/IEC 27001 and ISO/IEC 27002, many experts believe BS 25999 and BS 25777 will be used as the primary templates for the final version of ISO/IEC 270301.

Document Name / (type)	Scope
BS 25999-1 (guideline)	Business continuity management. Code of practice
BS 25999-2 (standard)	Business continuity management. Specification
BS 25777 (guideline)	Information and communications technology continuity management. Code of practice

It is very likely that the above standards and guidelines will be used to form the majority of the forthcoming ISO/IEC 27031.

NOTE:

I highly recommend the CISSP candidate download the FREE GPG document from BCI to learn more about BCM in general as well as getting a head start on ISO/IEC 27031. ISC2 updates their test regularly and often these updates come from the evolving ISO SC27 documentations. For this reason, I have done my best to align this chapter with the processes and terminologies used in the GPG as much as possible.

The lack of an ISO standard on BC/DR (BCM) can make it very difficult to understand exactly what terms will be used in any documentation, including the CISSP test. For the purposes of helping the readers both follow the BCM processes discussed in this section and interpret the sometimes very difficult English grammar used on the CISSP test, I will focus on the GPG and the above mentioned BSI documents. I will also use different terms to describe the same processes and relate them. The terms are primarily taken from BCM standards and best practices from around the world, including the National Institute of Standards and Technologies (NIST) SP800-34, the National Fire Protection Association (NFPA) 1600, the Federal Emergency Management Agency (FEMA) FPC-65, the Disaster Recovery Institute International (DRII) and a few other references.

EXAM WARNING

Beware of the Jargons:

For Example, in our flat tire example above, the term **Maximum Tolerable Downtime** or **MTD** might be expressed on the CISSP exam using various terminologies from different standards or guidelines:

BCI GPG	Maximum Tolerable Downtime (MTD)
NIST SP800-34	Maximum Allowable Downtime (MAD)
BS-25999	Maximum Tolerable Period of Disruption (MTPD)

The CISSP Candidate should recognize the concepts more than the exact words used. Terms one might use in their respective organization may not be the same terms used on the test. In fact, it is likely that the same basic question will be asked several times on the same CISSP exam using different terms. This is likely by design to entrap candidates who have memorized "brain dumps" but have no conceptual view of the actual processes.

The various standards bodies around the world have sometimes created different process steps and names. Once again, for the purpose of both passing the CISSP and to prepare for the forthcoming ISO/IEC 27031, I will focus on the processes defined by the BCI GPG.

PREPARING FOR DISASTER

First, let's define a disaster. According to the DRII, a disaster has the following characteristics:

1) sudden
2) results in the inability to conduct business, and
3) results in great financial loss

Most BC/DR standards bodies would likely agree that, when planning for disaster, as the old saying goes, expect the unexpected.

Disasters frequently strike without warning and can be caused by many natural and man made events.

The term disaster may mean many things to different people and organizations. In the context of "Disaster Recovery" however, and for the purposes of understanding the CISSP exam questions, it is probably safe to associate the word disaster with a "Denial of Access" to a primary facility. While it is imperative to provide some form of end user facilities when a disaster strikes, the disaster recovery plan will likely focus on contingency sites for relocation of ICT services instead of the end-user facilities.

The Difference Between Accepting and Rejecting (Neglecting) a Risk

As stated earlier, there is no way to completely eliminate all organizational risks. A basic plan is created to handle the high probability issues and incidents. Organizations may choose to accept the risk of a high impact but extremely low probability event due to resource and budgetary constraints.

If a disaster was to occur and there was no plan in place, the organization would be less likely to respond to the disaster properly, not to mention the potential for *negligence* liability (due to lack of due diligence and due process.) Without serious plans, the organization is putting the people and the business at a higher risk. The ability to "switch to Plan B" is a critical success factor for organizations of all sizes.

To use the tire example to illustrate this concept

I do not know of anyone who could know exactly when he/she will incur a flat while driving. Yet, if a person were to drive, ignorant of the fact that tires can go flat for a variety of reasons, he/she would be very exposed to loss without:

1) Having a spare tire and tools to change it (jack, wrench) in the trunk

2) Procedures to steer the vehicle to a safe place and exchange the flat tire for the spare tire

3) Knowledge of and proficiency with the above procedures

If a 'flat' event actually does occur and the person does not have a plan or is not aware/educated on such event (rejecting/neglecting the risk), that person would likely panic or continue to drive on a flat and very likely in the process, endanger themselves and other drivers as well as other private or public infrastructure.

If the same person has a plan (accepting the risk), he/she would instead hopefully follow the proper plan, to:

1) Identify the problem

2) As safely as possibly, drive to the side of the road

3) Change the tire

4) Get back on the road

5) Repair / replace the original tire and get back to normal operations as soon as possible

All of the above steps are required to minimize risks to them and to society at large.

Business Continuity and Disaster Recovery planning is what separates “accepting” a risk versus “neglecting/rejecting” a risk. Remember the ISC2 Code of Ethics, the CISSP is ethically bound (like any Jedi Knight), to protect the common wealth and infrastructure.

The BC/DR Life Cycle

Regardless of the terminologies used, the basic process flow for any type of development is basically the same. Often an exam question will be easier to answer if the candidate understands the context of the question and answer. Understanding what processes are performed at which stage in a system development life cycle or SDLC will make it easier to select the correct answer during the exam.

EXAM WARNING

Example of how context can be used to interpret the CISSP exam questions:

Consider the use of the often ambiguous terms, “restore” or “restoration”. If a question is asking about restoration procedures, try to identify the point in time. For example, If the scenario is right after the damage assessment of the disruptive event, then restoration will likely refer to recovery, getting things up using contingencies. If the scenario seems to suggest that critical and essential services are already recovered, then restoration will likely refer to reconstitution, the process of returning to normal operation.

Once again, the lack of an international BC/DR standard from the ISO leads to taxonomy confusion, which often leads to misunderstandings. Not only are different terms used to describe the same phases in the life cycle, but often the number of phases and the events between the phases can vary from standard to standard.

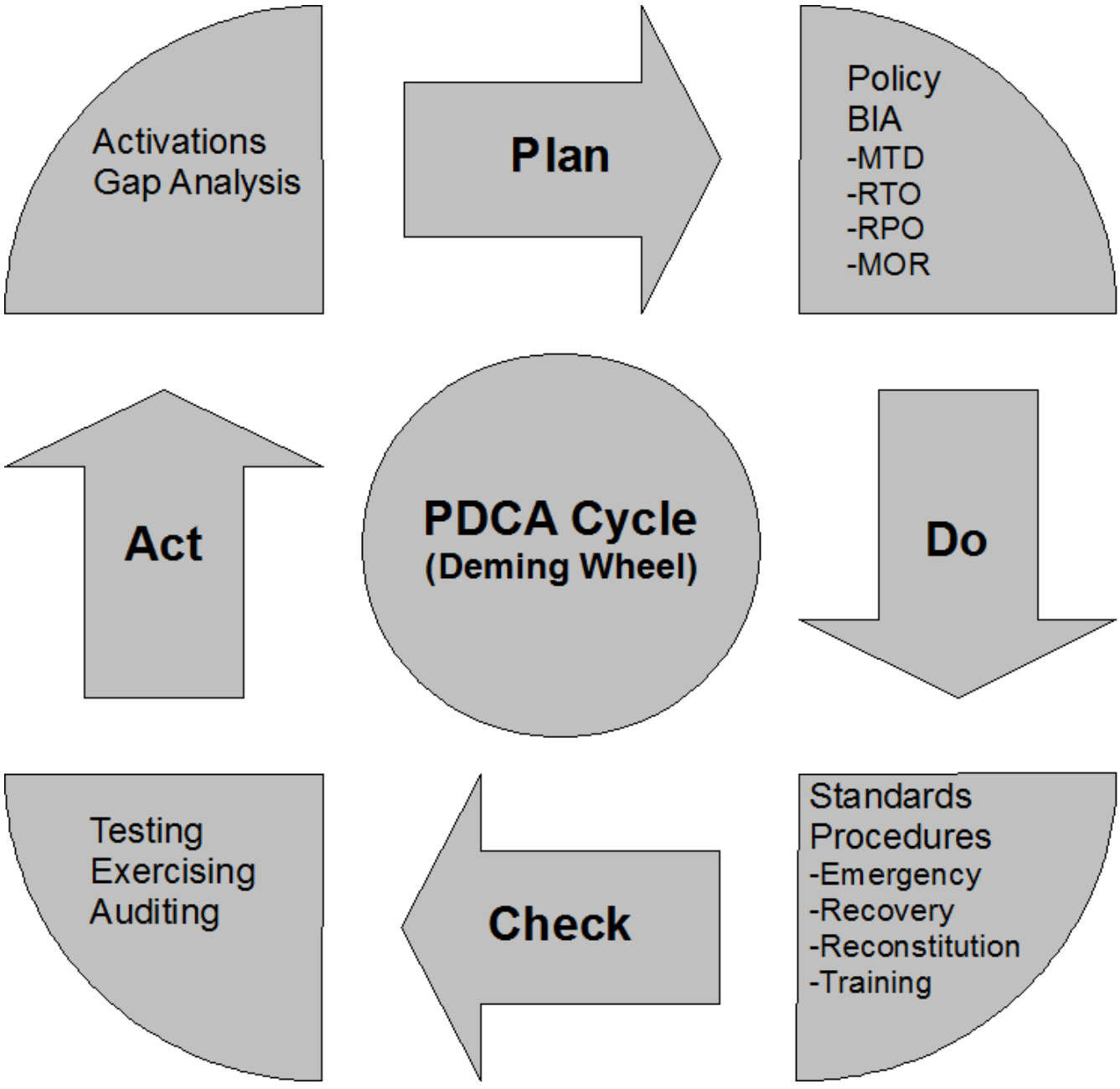
For example, the BSI and the BCI utilize a six step process to describe the BC/DR life cycle, whereas the DRII uses a seven step process. The lack of internationally recognized terms not only makes taking the CISSP exam challenging, it makes the entire BC/DR process very difficult.

Case in point:

Try to recall a few recent disasters and their corresponding response efforts? Are there any gap that comes to mind? In my opinion, if we can't agree or standardize on basic BC/DR terms, it is almost impossible to create a consistent and repeatable BC/DR process. It took the sinking of the Titanic to get the USA to standardize on Morse code (see The Radio Act of 1912).

For the purposes of making this as clear as possible, the CISSP candidate should start with the fundamental Plan-Do-Check-Act (PDCA) model illustrated below. PDCA model is well respected internationally and well-represented in many ISO standards including all the SC-27 series.

The Plan-Do-Check-Act (PDCA) model



Unless otherwise specified, I will list utilize the steps in the six step process from the BCI as well as other SDLC steps, in the context of the PDCA model:

The BCI GPG (as well as BS-25999) defines a six step life cycle process required for business continuity management:

1) BCM Policy and Program Management

2) Understanding the Organization

3) Determining Business Continuity Strategies

4) Developing and Implementing a BCM Response

5) Exercise Maintenance and Review

6) Embedding BCM in the Organization's Culture

EXAM WARNING

Do not focus on memorizing the exact terms or even the number of steps. The key concept here is that any SDLC will contain a starting point where senior management sets policy and assigns responsibilities to the BC/DR manager and a steering committee. Next the BC/DR manager must understand the specific requirements that are important to the stakeholders and then create and maintain a solution to meet these requirements.

EXAM EXERCISE

After understanding the recovery time objectives for the human resources department, Alice reviewed various alternate data processing facilities to determine which would allow a recovery process in the required time frame. She found that while it would be less expensive to lease a site from a provider, there was no vendor with a site close enough to the primary site to meet the timing constraints. She therefore decided the organization should build its own facility. At what stage in the life cycle does Alice make such decisions?

a) During the Business Impact Analysis

b) Management review

c) System Development

d) Gap Analysis

The answer is: **c**

Regardless of the exact words used, the question suggested that the requirements (performed in the BIA) were already determined. Alice's job was specifically to develop a solution that meets the requirements.

System Development Life Cycle Phases

To assist the reader in comparing the different terms and taxonomies used in the various standards, I have created the following chart to map the BCM SDLC phases across three various process life cycle steps common to BCM.

BCM System Development Life Cycle			
PDCA (Demming Wheel)	The Disaster Recovery Institute (DRII)	The Business Continuity Institute (BCI) - GPG	NIST 800-34
Plan	Project Initiation	Program Management	Develop the contingency planning policy statement
	Functional Requirements	Understanding the Organization	Conduct Business Impact Analysis (BIA)
	Design and Development	Determining the BCP Options	Identify preventive controls
		Developing and Implementing a BCM Response	Develop Recovery Strategies
Do	Implementation		Develop an IT contingency plan
Check	Testing and Exercise	Exercising, Maintaining and Reviewing	Plan testing, training, exercise
Act	Maintenance and Updating	Embedding BCM in the Organization's Culture	Plan Maintenance
	Execution		

The reader can see that each standard or guideline, has different names and different numbers of

phases and they do not align horizontally across the standards. I will cover all of these steps in much greater detail later on this chapter.

For now, the basic description of each of these phases is as follows:

PLAN

BCM Policy and Program Management

This phase is where senior management sets the goals and scope of a project. Management will assign responsibilities and forecast budget and scheduling constraints. Within the context of BC/DR, this is where the BC/DR policy is created.

Functional Requirements - Understanding the Organization

This is perhaps the most difficult phase in any SDLC (Define). This phase is where a very detailed description of the requirements and outcomes of the project are defined and documented. The BC/DR manager will work closely with the various business unit mangers to understand their specific requirements in the Business Impact Analysis (BIA). Some examples of the tasks include, but are not limited to, RTO, RPO and MOR metrics creations and definitions.

DO

Develop and Implement a BCM Response

Design architectures and specifications to meet the identified requirements gathered in the previous phase. For example, if the RPO for a given process is less than 24 hours, the design may specify a live data mirroring solution to a remote location.

Development of response plans for activation, recovery and reconstitution, as well as procedures, technologies third party contracts, and teams are created to meet the specifications.

CHECK

Exercise Maintenance and Review

This phase is where on- going Tests, Training and Exercises (TT&E) as well as change management and regularly scheduled audits are done to identify improvement goals.

ACT

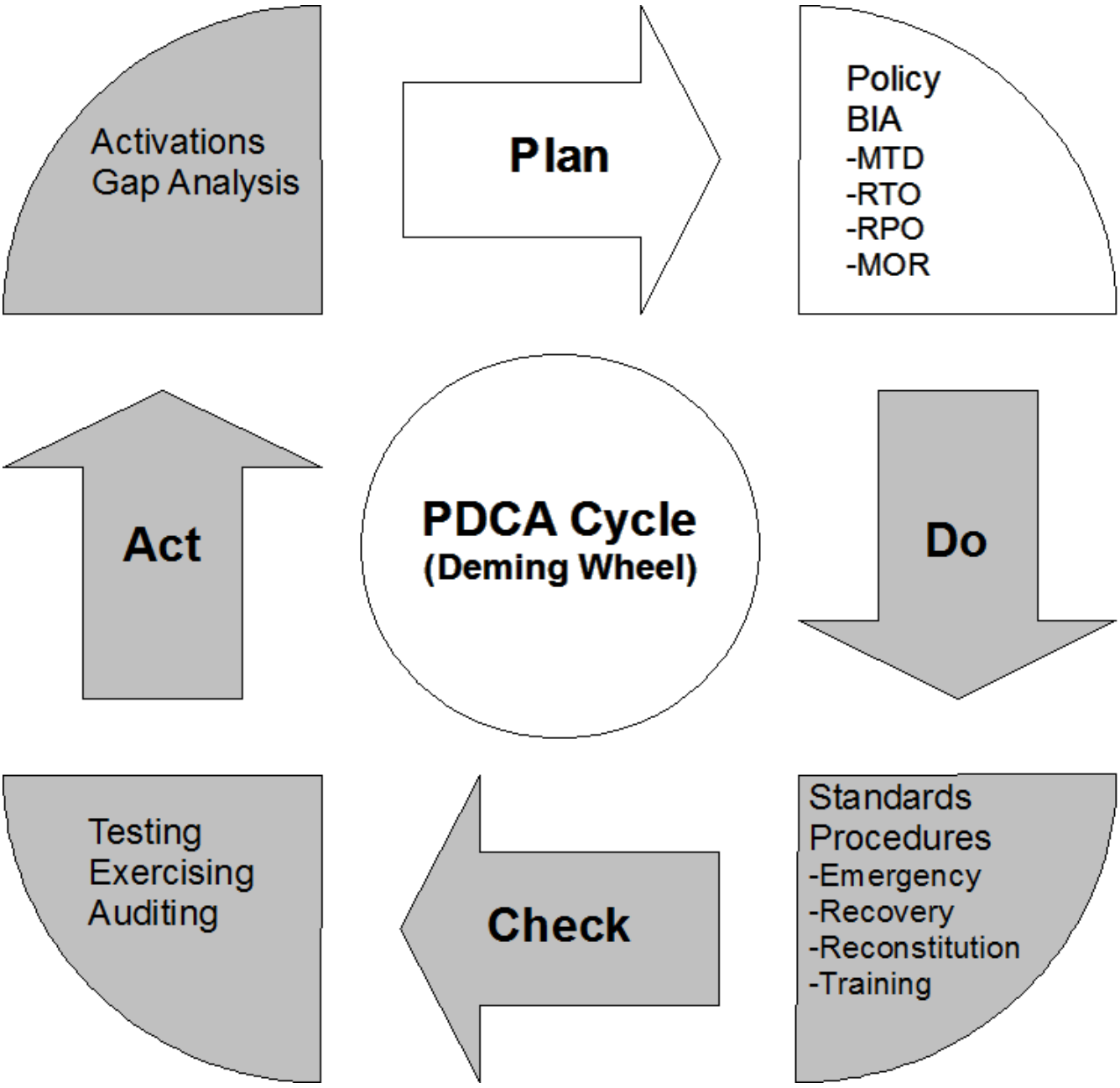
Embedding BCM in the Organization's Culture

Activation – This phase is unique to BC/DR and other incident / crisis / emergency management processes. In the event of an Emergency / Disaster, the plans will go live (activate). This is the step we really hope never happens in real life.

Another important action is **"Continuous Process Improvement"**: Continually REVIEW the outcome of tests, exercises and actual disasters, then perform a gap analysis to prioritize ways to improve the BC/DR plans.

Gap Analysis – This phase is where management addresses issues identified as needing improvements by using the outputs from tests, exercises and audits.

Plan – Do – Check – Act



Project Initiation - Understanding the Organization

The first step in creating effective BC/DR plans is to identify the residual risks and to develop a policy for dealing with these risks. These policies, as in all security policies, are based on business needs and legal requirements.

Here is an example:

For example, you might be willing to accept the risk of driving your car at 100 miles per hour, but the legal policy may require that you drive no faster than, some limit below that number.

In today's world, with ever changing laws, identifying legal risk is no easy task. It is critical that a security manager work with other line of business managers such as HR or Legal to understand their business and legal requirements

EXAM WARNING

> It is important to recognize that in the real world, a new BC/DR manager will likely inherit existing plans. This is also likely to be reflected in the CISSP exam. It is likely very ineffective and unrealistic to think one will start planning with a blank page. A review must be done by the a new BC/DR manager to understand what is already in place, check to see how much of the existing BCM program is appropriate and where improvements should be made. After the security manager understands major threats to the business, a presentation is made to senior management. After understanding the high level aspects of BC/DR and the organizational exposures, senior management then sets the policy.

NOTE ON LOSS CRITERIA

As a CISSP, or in any noble warrior certification program (Jedi Knight, etc), the number one priority is to protect life. After protecting people from loss of life, the next most valuable asset is the organization's image. It is not unusual to see an individual or an organization gone under as a result of loss of branding or reputation. Keep these two concepts in mind when taking the exam. While the loss of a certain system or asset can be very costly, the big picture is protecting the business as a whole.

Planning the BCM policy requires an understanding of the the organization's business needs. All organizations create products and or services. The BC/DR manager will need to understand what the products and/or services are created by the organization, how these products/services are made and delivered, and who is responsible for the various internal and external processes, Additionally, BC/DR manager will also need to understand the business requirements of their suppliers.

Functional Analysis

As stated earlier, perhaps the most difficult of all SDLC phases is the functional analysis. For the CISSP exam, the BIA task (part of the functional analysis phase) may account for the bulk of the BC/ DR questions. For this reason, I will cover this phase in the most depth. It is in the BIA that criticality metrics are determined.

The CISSP candidate should be MOST familiar with the following metrics:

Maximum Tolerable Downtime (**MTD**)

Recovery Time Objectives (**RTO**)

Recovery Point Objectives (**RPO**)

Minimum Operating Requirements (**MOR**)

Note:
As stated earlier, when reading an exam question, ***context*** is the key. Different words and taxonomies may be used to describe the requirements by the various business units, providers, partners, customers and other stakeholders.

Also it is important to consider ***perspective*** when reading an exam question.

For an example, consider the use of Minimum Operating Requirement (MOR) metrics in the following scenario:

For example, if the normal service levels for the sales department requires ten fully equipped desks (phone, computer, etc) but the results of a BIA determine that the organization could get by for up to 30 days with only four equally equipped desks (MOR = 4). Should a disaster strikes, the Sales Department can get by with just four desks and the other six desks may be used as alternate user sites for other department is the the same organization if so requested/required.

AN EXAMPLE OF FUNCTIONAL ANALYSIS:

When an organization in the US enters into a contract with a foreign organization there are functional requirements that are specific to that country.

For example, in Singapore, there are four languages commonly spoken in the country.

In this scenario, the US based company possibly have to create different texts in different languages, but metrics such as, inches, miles, pounds, etc may have to be converted to meters, liters, etc. Without verification of these specifications, the developer might create a very efficient system for US based companies, yet it will have fail to the meet the functional requirements of Singapore-based stakeholders.

EXAM WARNING

Anyone preparing for the CISSP exam will need to have a pretty good understanding of the objectives and terminologies used in the BIA. While in Risk Analysis, one identifies assets and assigns values for these assets, in the BIA one identifies essential processes and supplies and assigns criticality metrics to these processes/supplies.

Remember that criticality is associated with ***availability***. The BIA differs from the "Impact Assessment/Analysis" phase of traditional risk management in terms of how the loss value is expressed. A traditional risk assessment often assumes impact as a ***static*** metric, asset value x exposure factor will give you the Single Loss Expectancy (SLE), where exposures are measure in some percentage. In this traditional risk management model, the "Impact Assessment/Analysis" phase, the loss is expressed as a static loss value.

For example, if an asset is currently valued at $10,000.00 and 20% of the asset would likely be damaged in a given loss event, then the expected loss (SLE) would be $2,000.00.

In a "Business Impact Analysis" or BIA, the loss is expressed as a ***dynamic*** metric. For example, how much loss would occur if there was no electricity for a minute, and hour, a day?

Maximum Tolerable Downtime (MTD)

Dynamic metrics for BC/DR include the maximum tolerable downtime for each process. This is one of the metrics that you may see different organizations using different terms to express this same metric.

In most CISSP literature I have seen, this is referred to as Maximum Tolerable Downtime (MTD) as listed in the glossary of the BCI GPG. However, in my experience many organizations around the world refer to this as Maximum Tolerable Period of Disruption (MTPD) as in BS-25999. In NIST SP800-34, this is termed Maximum Allowable Downtime, which comes out a little funny as MAD. Other terms, I have seen used to describe this metric, are Maximum Acceptable Outage (MAO) and even Acceptable Interruption Window (AIW).

Note:

For consistency and brevity (three key strokes rather than four) I will refer to this as MTD but for purposes of taking the test, be prepared to see other terms, especially MTPD. Either way the concept is consistent, what is the maximum time an organization could withstand without a critical function, service, process or supplies including data.

Recovery Time Objective (RTO)

Time allowed for recovery processes to be completed in order to meet the MTD.

In our flat tire example, there was a MTD of one hour. So the plan to replace the spare tire must meet our next Metric, the RTO. Considering that we needed some time to get to the side of the road safely, the RTO is always less than the MTD. Also consider that when there is a report of a disaster, the first step is to confirm the incident and then do a damage assessment. Issuing a "disaster declaration" should only occur after the damage assessment.

NOTE:

Remember not to confuse "disaster recovery," which is associated with recovery of the ICT and infrastructure to a minimum level, with "emergency/crisis management," which is primarily associated with the initial response, with the priority goal to protect life and contain damages.

In the flat tire example, where the emergency is not really over until the normal tire is restored. Similarly, for an organization, the emergency is not over until all processes are fully reconstituted to the repaired / new primary site(s) and operating under normal service levels.

EXAM WARNING

In the ISC2 2007 edition of their official guide to the CISSP, the metric RTO appears to be used to describe what we just referred to as the MTD and I see no mention of the other terms that I have mentioned. Perhaps this is because of an oversight, or it may be because, from a DR perspective, this metric is the focal point since this is more in line with the recovery process planning. Where MTD includes the crisis management phase, DR is more associated with RTO.

Note from Clement:

Larry it seem ISC2 has heard you. The RTO, RPO, and MTD are better explained in the ISC2 official study guide, second edition, on page 278-282. However they still consider RTO and MTD to be the same. They define it as: "The amount of time the business can function without that application before significant business impact occurs". Here is an extract:

"The RTO or MTD for a business process or for an application is going to determine the recovery strategy for the process or application. The more time that can elapse before the recovery need to occur, the more recovery options are available. The more time sensitive an application or function is, the fewer options you will have in selecting a recovery strategy."

Minimum Operating Requirements (MOR)

The essential supplies and services required for a given business process.

Using our tire example, the spare tire we typically have in most automobiles does not provide the same service levels as our primary tires. This brings us to our third metric, Service Level Objectives (SLO). In other standards and best practices I have seen it referred to as Service Deliverable Objectives (SDO) and even Service Level Objectives (SLO) as part of service level management

Regardless of the differences in terminology, the key issue is that it is typically ***NOT*** cost effective to expect the same service levels during a disaster. As such, management needs to define minimum acceptable service levels. In our example of the spare tire, the spare or recovery tire should be able to operate minimally at 55 miles per hour and provide this service for about 100 miles.

Mutual Aid Agreements, Reciprocal Agreement, and MOR

A Mutual Aid Agreement is when two or more organizations agree to provide recovery assistance for each other (referred to as **"Reciprocal Agreements"** within the official study guide). While this can be very difficult to manage, this is often used by organizations, to save on the higher cost of commercial service providers. A useful outcome of determining MOR for BC/DR manager is in crafting mutual aid agreement. If the site in question is not affected by a disaster but is requested to provide assistance for another organization, the BC/DR manager will need MOR metric.

Mutual Aid Agreements are more likely to be acceptable for related organizations, such as public services or separate branch offices for the same organization. My uncle is more likely to lend me his car in an emergency, than he would to some friend of mine, that he has never met.

Supply chain management

Understanding the supplies for a given process is often overlooked, but it is key to effective MOR planning. I was blessed with the opportunity to teach over 3000 CISSP candidates over the past few years. What I often heard from them is that supply chain contingency planning is the most overlooked part of a BC/DR plan. I have heard many BC/DR war stories, where the entire ICT infrastructure worked flawlessly, yet the recovery effort was unsuccessful because the plan failed to include supply chain contingencies.

Consider one of the war stories that will illustrate this point:

A student went through recovery situations where the ICT infrastructure worked great as far as the underlying electronic equipment and communications was concerned, but the plan did not include a way to supply paper for the printers!

They had to rush to local office supply stores to acquire paper but still only had about 10% of what they needed. Ah paper that is what really makes the printer so important to the business. To reiterate the importance of functional requirements during BC/DR life cycle, the BC/DR manager needs to work with the line business managers to understand and document inter-dependencies, inputs and outputs of their business processes.

Maximum Time in Alternative Operations (MTA)

The amount of time an organization can survive in recovery mode.

In the flat tire example, if the spare tire met the above mentioned minimum service levels (MOR), the driver should also plan to get back to normal within these constraints.

Reconstitution is the term used by most organizations to describe returning to normal.

But the term to describe how long one can operate under reduced service levels is often overlooked or contained within the MTD. In the BCI GPG, this is referred to as both Maximum Time in Alternative Operations (MTA) and Maximum Acceptable Outage (MAO).

Recovery Point Objective (RPO)

The point in time recovered data must meet for critical processes.

In information security, criticality not only affects how long can one afford to be without a process or service (MTD), but also when restoring data onto a recovered system, how old can the data be?

For a high risk system such as banking system, the RPO can be very short with the goal of no data loss.

For example, if I electronically deposit my pay check into a bank Tuesday morning at 11:23 and the bank experiences a disaster that affects the data, I would be very upset if they only did nightly backups and were only able to make my account look like it did the night before I made my deposit.

While I might be able to afford the banks closure for a day or two (MTD = 24-48 hours), I would hope that the RPO (in this example no data loss) was respected.

NOTE:

RPO is a critical output in creating an effective data backup schedule. For any system that has an RPO of less than 24 hours, nightly backups are not timely enough. Many of today's organizations have departments and processes with very low or near-zero RPO values. For these systems, remote data replication services have become very popular.

In the new ISC2 Official Study Book, Second Edition, the subject of RPO is covered on page 280-281.

EXAM WARNING

Critical vs Important

In the BIA, the analyst will identify critical processes and identify the MTD, RTO, RPO, MOR and MTA for each process. Note the difference between critical and important. Criticality is associated with time. All the departments and processes are likely to be important to an organization, but each department will vary with its criticality. For example, the audit department is very important and so is customer service. In a disaster scenario however, an organization could likely survive days, weeks, or even months without audit but less likely to survive without customer service for as little as a few hours or may even have a MTD of less than an hour! In this example, the customer service department is critical but the audit department is important.

It is also important to understand the inter-dependencies between process and business units. For example, telecommunications is required to supply customer service with the much needed phone service to support customers. Depending on the recovery methods eventually selected, the BC/DR plan must address the inter-dependencies between these processes (telecommunication and customer services). In this same example, if the management agrees that the most appropriate recovery method that meets the RTO is outsourced phone infrastructure, then this interdependency between internal telecommunication group and customer service group can be greatly reduced as a risk.

NOTE:

I have observed that the terms ***essential*** and ***critical*** are often used interchangeably. Moreover some organizations (FEMA for one) use the term ***essential*** to refer to functions and the term ***critical*** to refer to resources used to support the functions. For example, customer service is an

essential function and the customer database is a critical resource for the customer service function.

Human Resources, Lines of Authorities and Succession Requirements

Succession Plans

A Succession Plan is written to provide directions for key personnel in your organization to follow, in the event of an upset or a disaster.

However, during a disaster, key personnel named in a succession plan may not be available to perform their duties for a variety of reasons, including direct effects of the disaster itself. Because of this, it is critical to identify in the Succession Plan, other competent individuals who can perform these duties.

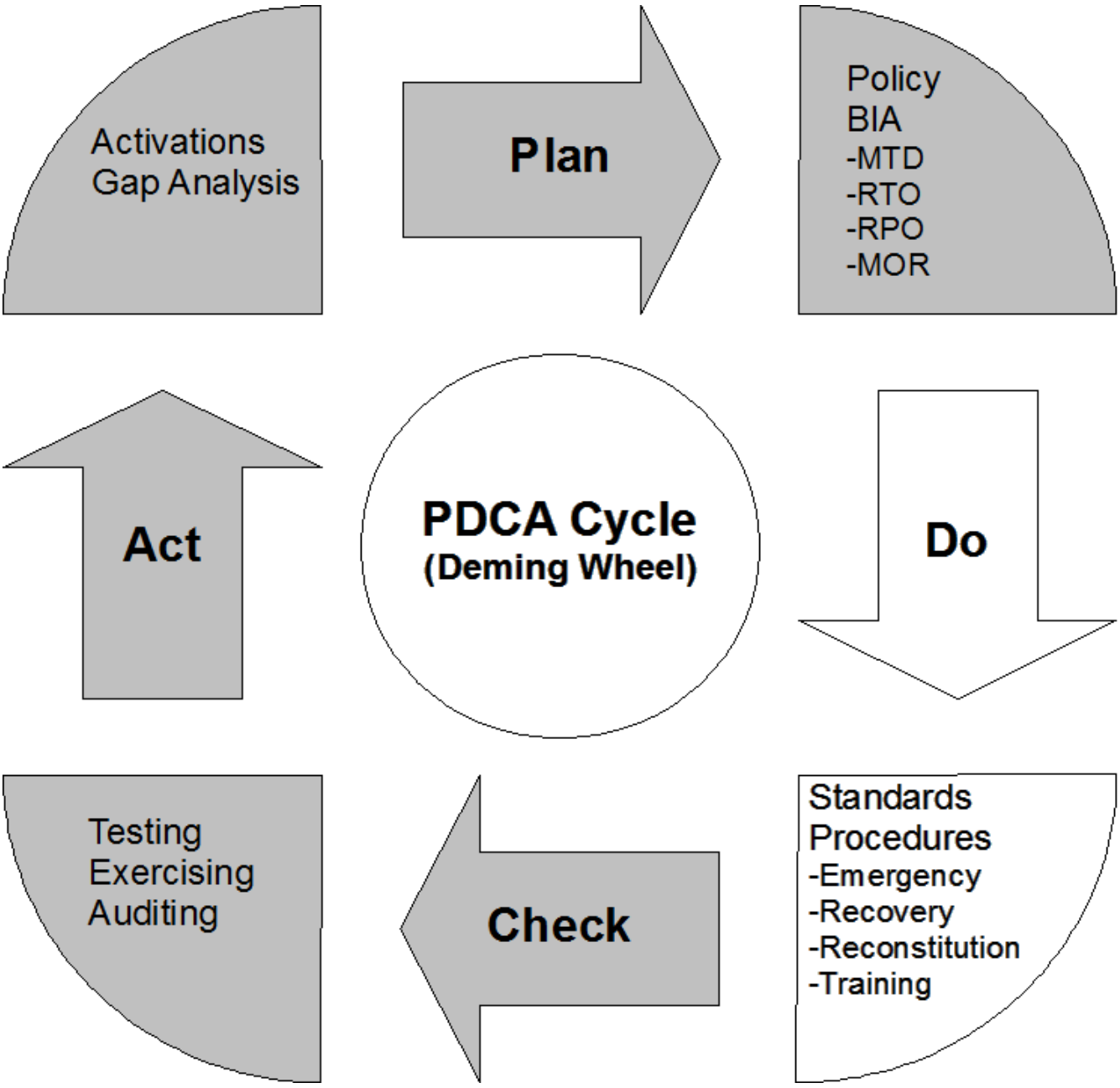
It is important to point out that a clear line of authority must be established in a disaster. Creating a succession plan is critical in minimizing the impact of the crisis on the organization in the event of key personal being unavailable.

It is equally important that the order of succession is also addressed in a succession plan. Ask this question: who will assume the role for plan execution in the event that the highest level of authority documented in the plan is unavailable? In a crisis, people need to know who is in charge.

In summary, the output of the BIA phase should include the MTDs for each business process, the RPO, MOR and other requirements mentioned in the Plan phase of the SDLC.

The output of BIA for the organization should include specific recommendations for continuity of operations such as using alternative facilities, technologies, processes and people.

Plan – ***Do*** – Check – Act



System Design and development

In this phase, the BIA has already been performed (Plan-Functional Analysis phase of PDCA life cycle). A prerequisite for the system design phase is that the result of the BIA must be accepted by the proper accrediting officials, process owners or "keeper at the gate". Upon acceptance of the

BIA document (business requirements) the next step is to design a solution to meet these requirements captured in the BIA document.

The System Design phase generally addresses the "how-to" part of meeting the requirements whereas the functional requirements (the "what") are addressed in the BIA document. In this phase, the reader should consider questions such as: How will the required time lines outlined in the RTO, RPO and MOR be met? What people, process, technologies, sites and supplies will be used to recover lost operations?

In summary, system design is where the architect will create specifications and identify specific people, process and technologies. Readers should remember to include appropriate people skills and knowledge components (people-focused) when designing solutions, not just the process and technologies. I will outline the critical components in the following sections.

Alternate Facilities

Planning for a loss of access to a facility requires alternate locations for both the ICT infrastructure as well as end users. It is very unlikely that the alternate locations for these two constituents will be at the same facility simply because the requirements for people and technology tend to be very different.

When designing a solution for alternate facilities, the reader should be aware of the common solutions that are available from disaster recovery service providers. Generally, the choices for alternate facilities vary from Cold Sites to Mirrored Sites. We will cover some of these services in more detail below.

One of the key considerations for selecting the alternate facility is the physical location of the site. The alternate facility should be far enough away from the primary facility so as not to be affected by the same disaster, but close enough to meet the required MTD and RTO requirements defined in the BIA. There is not a fixed distance for a properly designed alternate location, since every organization is likely to have different recovery goals. However, I will point out some questions that the reader should ask when designing an alternate facility solution.

One should first consider the nature of the disaster, and then ask the following questions:

- How far away would an alternate site need to be to so as not be affected by the same earthquake, hurricane, downed power grid or pandemic virus?
- How will one transport essential personnel or data? High speed data mirroring solutions are much more feasible if the alternate site is closer to the primary.
- Should the alternate site be owned by the organization or leased from service provider? Leasing an alternate site from a provider is typically much more cost effective, but the provider may not have a location in the desired geographic location. Also most leased sites

are shared spaces and overbooking by a ratio of 25 even 40 to one is not uncommon. In such a situation the site most likely will be allocated to the first customer to make an official disaster declaration as defined in the service level agreements.

Commonly used terms for alternate facility options

Cold Site

A cold site is defined as a backup facility with environmental conditions only, that it, HVAC, electricity and very likely a communications line.

Warm Site

This site is partially equipped with information communication technology (ICT). This site is usually owned by the organization. As such, the systems stored in this facility tend to match better with the actual production systems such as proprietary equipment or applications.

Hot Site

A site that is fully equipped with hardware and software requiring only that the data be restored. In a leasing model, a hot-site service provider typically offers a choice of a dedicated site or a shared site. Generally speaking, a shared hot site option is more popular than a dedicated hot site option because it is far less expensive. However, note that in the shared hot site environment, it is very unlikely that the equipment at this facility will be identical to the customer's primary site. If an organization has a significant portfolio of proprietary critical systems and applications, a shared hot site may not be a good solution. Another very important caveat to the shared hot site option is that the provider tends to oversubscribe the same sites, as noted above in the alternate facilities discussion.

Mirrored Site

A mirrored site is similar to a Hot Site with an additional data replication service. The data is replicated at this site, thus saving the recovery team much of the effort in restoring their data. This option, while the most expensive, is best suited for customers with the shortest MTD, RTO and RPO. Organizations may choose from options that allow for partial to fully mirrored sites.

One potential downside of a hot site is that the data replication at the site may not be timely if the replication service is done via nightly tape backup. However, typically, if an organization specifies a mirrored site, it already has established a data backup solution with near-zero data loss. This requires technologies to include live data written to the alternate site in parallel with the primary site. It has been my experience that many banks in the US have specified at least three mirrored

hot sites. Each hot site would provide partial mirrors of their production data. Thus, any outage in any given hot site will not impact the availability of the data in real time.

Dual Data Center

The official study guide from ISC2 refers to the term Dual Data Center. This strategy would be used for applications which cannot accept any downtime without impacting the business. The applications are split between two geographically dispersed data centers and either load balanced between the two centers or hot swapped between the two centers. The surviving data center must have enough head room to carry the full production load in either case.

Mobile Site

A mobile site is defined as a transportable site equipped with all the important equipment required for recovery of ICT operations within the minimum operating requirements (MOR). In the industry, sometimes mobile site is referred as the "Rolling Hot Site." However, this can be misleading as these sites are rarely fully equipped and are more like "Rolling Warm" sites. Also note that the mobile site is for ICT and not very likely to be equipped with end-user environmental conditions.

EXAM WARNING

Note from Clement: Official Study Guide from ISC2, Second Edition, See page 282-283

You must be aware that ISC2 considers a Warm and a HOT site as a rented or leased facility. They consider a cold site as a shell or empty data centre space. In fact to ensure there is no confusion in the jargon about the usage of the term Hot Site they have:

Internal Hot Site

Standby site with all the necessary technology and equipment to run applications that needs to be recovered. Data is kept in sync between primary and alternate site. This site requires a minimal amount of time for recovery. The challenge is of course to keep the two environments as exact copy of each others. This is not a rental place, it is your own.

External Hot Site

Equipment is in place and ready to be use. The environment must be rebuilt for recovery. It is a rental or leased facility. Providers use generic hardware that meets most client requirements. You may need to bring your own specialize hardware or software.

EXAM EXERCISE:

Bob is charged with reviewing the recovery solution for the customer service department. In the last year, the application services for all of the critical customer processes have been outsourced to a third part service provider that uses cloud computing. The SLA from the provider guarantees the availability of the back end services by replicating all application and data access across multiple mirrored sites. Why might Bob design solution for only end user access to the ASP network?

a) Because of distance, Bob should perform user acceptance testing.

b) Because of the results of a cost benefit analysis

c) Hot sites never include alternate user facilities

d) Because of legal requirements

The answer is: **b**

Sometimes the hardest part of taking the CISSP exam is to understand what the heck the answers have to do with the question. The basic question is, why might Bob select a certain recovery option, and the best answer to that question is based on a cost benefit analysis.

After understanding recovery options, the develop and acquisition phase is where procedures, teams, contingency sites, equipment, and services are either developed in house or acquired from external providers.

This is where one will typically see plans for handling the actualized risks signed-off by the senior management. Depending on which recovery options that the senior management actually signs off i.e. customer service hotline mirrored hot site option, the BC manager must now create, with input from the various process owners, the actual plans that will be followed when the identified disaster does happen.

TERMS FROM THE OFFICIAL STUDY GUIDE YOU SHOULD KNOW

Surviving site
A surviving site strategy is implemented so that while services level may drop, a function never ceases to be performed because it operates in at least two geographically dispersed buildings that are fully equipped and staffed.

Self-Service
A business can transfer work to another of its own locations, which has available facilities and/or staff to manage the time sensitive workload until the interruption is over.

Internal Arrangements
Some of your internal rooms may be equipped to support business functions while staff from the impacted site travels to another site and resumes business.

Dedicated Alternate site
Built by the company to accommodate business functions or technology recovery.

Work from home
Simply employees that will work from home to support business functions.

External Suppliers
Business recovery needs are supplied by an external provider. Could be a wide range of services from mobile platforms, alternate site space and facilities, staff, etc…

No arrangements
For low priority business functions or applications that cannot be cost justified.

Some Key ICT BC/DR Plans and Teams (not exhaustive by any means, but in the context of the CISSP and ICT readiness the candidate should be especially familiar with the following):

Emergency / Crisis / Incident	Plans	Sample components
Emergency management team	Notification	Call trees, off site emergency operation facilities, confirmation of the incident, notification of emergency services (police, fire, medical), notification team members and other stakeholders.
Rescue team	Occupant Emergency	Safe evacuation of a facility, accounting for all affected personnel
Emergency management team	Succession	Address loss of key team members and decision makers
Emergency management team	Damage assessment	Impact assessment, decision to relocate
Recovery	Plans	Sample components
Recovery Team	Relocation of ICT data center	Restoring the back end infrastructure using alternate

		processing facilities, data recovery and restoration to alternate facilities.
Recovery Team and end users	Relocation of end user facilities	Provide users with access to alternate processing facilities and data
Reconstitution	Plans	Sample components
Reconstitution team also referred to as “Salvage” or “Restoration team	Relocation to original or new primary facilities	Fail back plan to ensure logical order, and necessary steps, to reduce the risk of migrating to the repaired or replaced site.

Emergency /Crisis Management Plans

The primary concern in an emergency is preserving life. However, the term emergency is also broadly applies to the entire disruption, not just life-threatening issues. In reality, the emergency begins when there is a confirmed incident and only ends when everything is running normally (people, process and technology). Disaster recovery is associated more with recovering processes after the first responders have achieved their objectives, or “stopped the bleeding.” Note that this does not mean that ICT systems are NOT part of the first response, it just means that first responders' objectives may or may not include ICT systems.

A very important and *testable* process for emergency management that would involve ICT may be to provide secure shutdown of critical systems, in Emergency Power Off or EPO plans.

The emergency or crisis management plan can go into effect in any denial of access to a facility (fire, gas leak, bomb threat, etc) but this does not necessarily trigger the activation of the disaster recovery (DR) plan. The DR plan is only activated in events requiring relocation.

Learn by Example to clarify difference between EM plan and DR plan

If the initial damage assessment determines that the primary site is usable, say in a false alarm, than it would be a waste of time and money to relocate.

I have had to evacuate sites due to false alarms quite a few times, including three bomb threats, and a greater number of false fire alarms in my career. In these examples, the DR plan was NOT activated but the Emergency plan was in effect.

False alarms alone can be costly to the organization but not as expensive if the disaster was declared.

Case in point:

Many organizations have an off-site agreement with a service provider as part of their DR plan. A typical agreement will likely include an off-site location that is shared with other organizations. This shared agreement is a common practice as it is generally less expensive than a dedicated site. However, once a disaster declaration is made, the bill will go up as there will be a charge for the declaration. This is why it is important to perform an initial damage assessment and determine if a DR plan needs to be activated.

It is also very important to prioritize response actions during damage assessment phase of the emergency or crisis management plan. For example, when a fire alarm sounds and the alert is confirmed, then the number one priority is to protect life. ***If there is a choice on your test to save Bob or the email server, for the test, save Bob***.

Occupant Emergency Planning

As stated before, saving life in a disaster scenario may include emergency evacuation of all occupants. This type of plan is frequently called the Occupant Emergency Plan (OEP). Most of the terms used in OEP are consistent with those in US NIST and FEMA.

NOTE:

In the context of many CISSP preparation documents, we may see other international terms that refer to OEP, such as Crisis or Incident management plans. However, the OEP concept should be recognizable as the "initial response to the emergency event."

Succession Planning

It is often said that the biggest threat to any business is the human risk. Having a plan is very different than executing a plan. It is very obvious that people DO NOT always respond according to the plan, especially during a disaster. In fact, in a disaster situation, the likelihood that a plan would not be executed greatly increases. When a person is traumatized and stressed, it is very difficult for them to respond according to a written plan. If an event causes a loss of life, there will be a natural grieving period, where the organization's requirements will be superseded by personal needs. This is why that is very important to develop a personnel succession plan.

A good succession plan will clearly identify a chain of authority and will include an alternate replacement authority in the event the primary person is unable to perform his/her identified duties. The identity of all proper authorities must be known by all team members as well as outside providers.

For example if the primary person with the authority to request media from an off-site provider was unavailable, there must be a plan with specific names to be allowed to make such requests.

BC/DR Teams

Clear lines of authority must be established for the three basic response teams:

1. Emergency Management Team

2. Recovery Team

3. Reconstitution / Salvage / Restoration Team

NOTE:

A common theme across all CISSP domain objectives is that senior management is accountable or "ultimately responsible" for security. ***On exam questions related to security decisions, the right answer is often to defer to senior management.***

So, what happens when the CEO and other senior members are unable to perform their duties during a disaster? Who is next in line to succeed in the chain of command? What if Bob, the organization's chief technical guru, the guy who designed everything, is unavailable? What about Alice, the primary operator who does most of the data entries for the Contact lists? She is the one who knows all the phone numbers, beepers, Twitter accounts, etc. All of these issues should be addressed in the succession plan.

Point Of Contact (POC) Lists

Typically an addendum to the overall BCP, the POC list is dynamic in nature and will require close communications between HR and ICT groups to ensure its usability and currency.

Examples of POC lists are Call Trees and Emergency Contact Lists. A workable contact list should identify primary, alternate and a third contact for each event. For each of these contacts, at least three phone numbers should be identified. Again, maximum timeouts should be defined before going to the next phone number and identified backup team member.

In summary, the primary concern during an emergency or crisis or disaster, once again, is the welfare of the people. Business Continuity Plans should identify sources for contact emergency services and grief counseling.

NOTE FROM CLEMENT:

The good old recall list is a great tool but can it be use the day you have a disaster?

Do you have people who have been identified as standby over long week end for example?

Do you restrict those people to be within a specific zone such as within 50 miles from work?

You cannot take for granted that the Plain Old Telephone System (POTS) will be available in case of a major disaster, in fact you cannot rely on the cellular phone either. You probable remember a shooting that took place at one of Virginia's university not that long ago. The authorities had difficulties communicating instruction because everyone today is on a cellular phone, in many case employees do not even have a copper line anymore. Is this the best solution? Not at all.

As you probably recall the campus police could not make use of the cellular network because it was completely clogged and congested. You had thousands of students attempting to call mom and dad to let them know they are alive. On the other side you had thousand of mom and dad and relatives attempting to call in. It was chaos.

You might want to think about alternate communication plans as well. It could include driving to someone's house, using the local radio station, using the local TV station. School Boards do it all the time as they do not wish to call hundreds of parents and they do not want them to call either.

Disaster Recovery (DR) Plans

The DR plan is where an organization addresses all of the critical to quality (CTQ) metrics gathered in the BIA, in particular, the MTPD (or MTD), RTO, RPO and MOR. **In the context of the CISSP test, this section is the major focus of BCM.**

To re-iterate the difference between emergency (or crisis) plan and disaster recovery plan made previously. The DR plan should only be activated if, while executing the emergency plan, the primary facility or any required service will be unavailable for a time that exceeds the maximum tolerable downtime (MTD).

Again, the triggers for a DR plan should be decided ahead of time. The Business Continuity Coordinator should have a clear understanding of the of metrics used to make the disaster declaration and relocate to an alternate facility, for example, if there is a loss of telecommunication services and the estimated downtime of the service exceeded the RTO.

Example:

Loss of any required service for an extended period could also become the trigger to activate DR plan. For example, if there is no HVAC, electricity or water, the DR plan could be activated. **During DR mode, the most critical processes will be recovered first.**

NOTE:

Each department should maintain their own sub-DR plan with pointers to the primary overall DR plan. For example, Bob, who supports accounting, does not need to know what Alice, who supports telecommunications, will do in her DR plan. This compartmentalization is very important for many reasons: privacy issues, version control issues and data sensitivity issues, just to name a few.

Additionally, for training purposes, the key is to keep it simple. Why burden anyone with additional steps that are NOT applicable to them?

Exam Warning

Reconstitution Plans

Reconstitution plans provide the steps to securely transition back from DR site. A first step in the reconstitution plan is a verification process to ensure the readiness of the primary site. Generally, **the least critical processes are failed back to the primary site first to ensure that the primary site is indeed ready for normal business services**.

While most of the work for ICT to relocate back to the primary site is closely related to the recovery processes, there are a few key differences. The main difference is the order of recovery: in the reconstitution plan, the order is from the least to the most critical, whereas in the recovery plan, the order is most to the least critical. Additionally, in the reconstitution plan, a key step is to securely clean out the alternate site to assure that no sensitive data is left residing at it.

EXAM WARNING

For the purposes of passing the CISSP exam, the candidate should understand three basic sets of plans:

1. Emergency/Crisis Management Plans
2. Disaster Recovery Plans
3. Reconstitution Plans

Notification of the actual crisis event could come from many sources: fire detectors, calls from neighbors or news organizations. Reports of disasters (either impending or unanticipated) can trigger the activation of the emergency or crisis management plan but not before some confirmation process. After the emergency situation has been confirmed, emergency response plans are used to contain the damages and to provide the contingency coordinator with status information i.e. outage estimates.

When taking the CISSP exam, it is important not to confuse the emergency with the disaster declaration. I have seen students frequently missed the practice test questions based on the different uses of the words emergency and disaster.

Exam Exercise

Question One

Who has the authority to make an emergency declaration?

a) Process Owners or backup personnel identified in the succession plan

b) Business Continuity Coordinator or backup personnel identified in the succession plan

c) Recovery team leader or backup personnel identified in the succession plan

d) Anyone

The correct answer is: **d**

This question is about ***emergency*** declaration. Anyone can pull a fire alarm which could require an emergency evacuation of the facility and denial of access to the facility, until public services assess the situation and declare the site safe.

Question Two

Who is has the authority to make a disaster declaration?

a) Process Owners or backup personnel identified in the succession plan

b) Business Continuity Coordinator or backup personnel identified in the succession plan

c) Recovery team leader or backup personnel identified in the succession plan

d) Anyone

The correct answer is: **b**

This question asked about the ***disaster*** declaration which refers to the decision to fail-over to recovery operations. This decision should only be made by the personnel with proper authority, typically this is the business continuity coordinator or backup personnel named in the succession plans.

IMPLEMENTATION

Plans are implemented in people, process and technologies. Implementation, infers that, above all, that people can perform their required work using the alternatives defined in the plan. This requires:

1) The plan is strategically appropriate and technically accurate

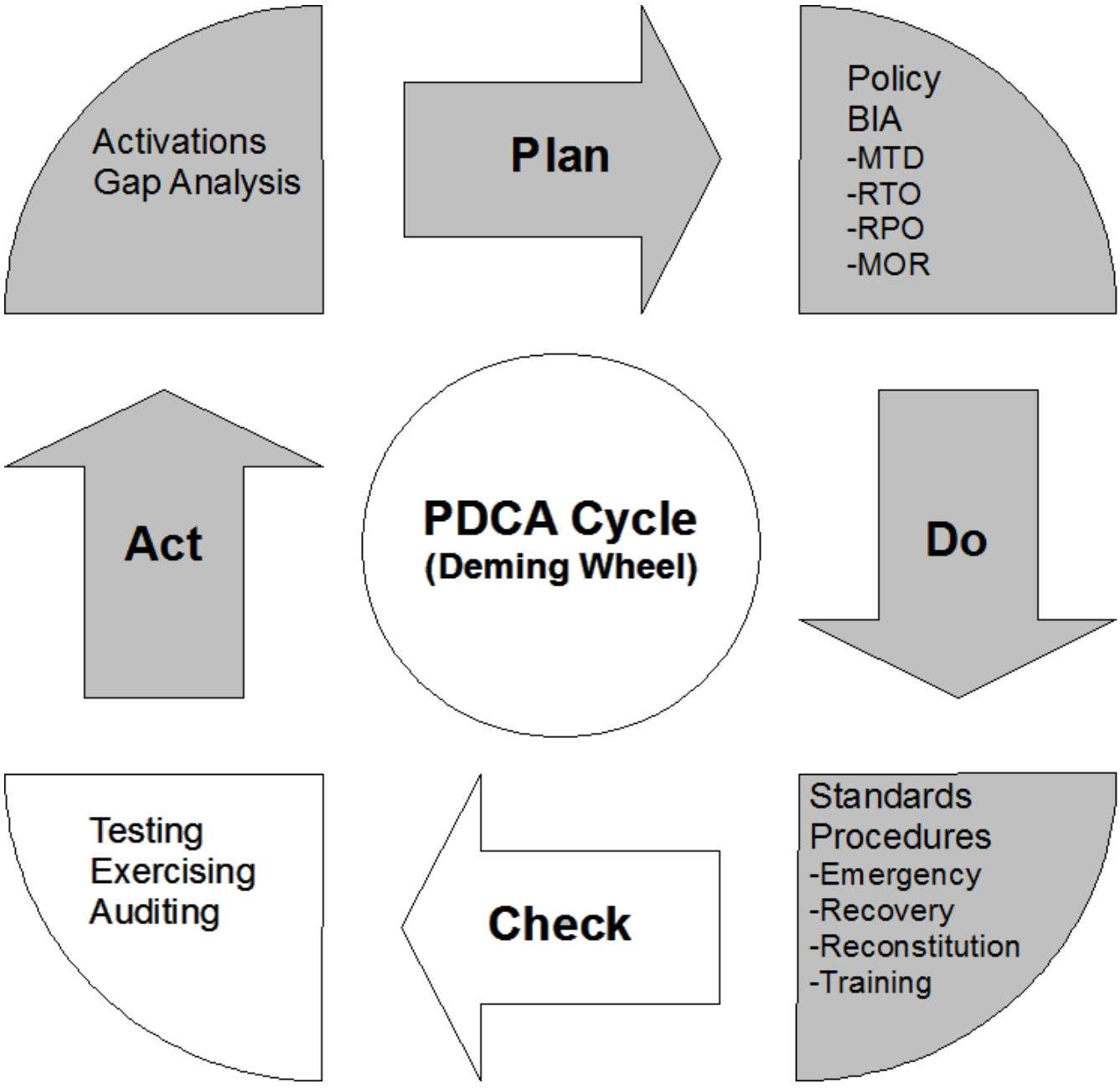
2) The people understand their roles and are adequately equipped

An example of additional plans implemented in this phase are:

Contracts, including appropriate Service Level Agreements (SLA), for recovery services and supplies must be negotiated with providers and suppliers.

Policies, procedures, training, testing and exercise plans for personnel (TT&E plans).

Plan-Do-***Check***-Act



In the context of BCM, testing generally refers to the plan. A test is conducted to determine the effectiveness and efficiency of the procedures. Exercising, in general refers to the people. Once there is confidence in the plan, regular exercising of the plan by the people provides the best assurance the plan will work as expected.

Organizational requirements change constantly, so BC/DR plans should also be periodically reviewed for effectiveness and efficiency. The reviews should involve self assessment as well as independent auditors, which will help insure that the plan is appropriate and that the names of people responsible for emergency, recovery and reconstitution duties are up to date.

Remember actions speak louder than words, so while everything can look good on paper, hands-on exercising practice is essential for successful execution.

While a realistic Types of Test and Exercises (TT&E) program is highly recommended, this step can be very costly and potentially dangerous to implement, without understanding and defining the appropriate testing and exercising policy. It is important to couple TT&E policy with documented procedures and to ensure that all personnel understand the scope of the TT&E plans.

There is a big difference between a "test" and a "drill or exercise." Understanding the difference will help the candidate on the exam.

The word "test" tends to be associated with a periodic or even a one-time event. A "drill" or "exercise" tends to refer to ongoing activity and provides quality assurance that the plans are effective, efficient and current. They also help insure that people understand their respective roles and responsibilities. It is my experience that a plan is tested for accuracy but drilled or exercised to provide people with regular reinforcement and continuous process improvement.

EXAM WARNING

One of the exam question refers to HOW OFTEN should the plan be tested?

There are two answers that could be possible:

1. *At least once a year*
2. *Whenever there are major changes in the plan*

Types of Tests and Exercises

When testing, it is imperative to define the testing policy, just as one would define the rules of engagement in a penetration test. While one would want to test as much as possible to provide optimum assurance, it is often too costly or even too dangerous to test for an actual event. For example, aside from fire departments, how many organizations set fires in a fire drill?

At first glance, when one reads the various standards and guidelines for BC/DR, there sometimes appears to be a big difference in the taxonomies and terminologies in BC/DR testing, which can lead to substantial challenges when interpreting the questions on the CISSP exam. After reviewing and comparing terms, I offer the following chart for clarification:

Test types	BCI GPG	Common US terms
Paper based for a single process	Desk Check	Checklist
Paper based for inter-processes	Walk through	1) Structured Walk through 2) Table Top
Equipment and test services	Simulation Exercises	Simulation Tests
Some live service fail-over to alternate facilities and operations	Activity Testing	Parallel Tests
Complete fail-over to alternate facilities and operations	Full Test	Full Interruption

An exercise can be broken into three basic methodologies and these are frequently represented in five more granular and testable types.

Basically the tests can be paper based only, simulated on test equipment and live where actual organizational services are delivered through the defined alternate operating facilities and processes.

TYPE OF TESTS AND EXERCISES

Paper Based Methods

Checklist
A copy of a functional plan is examined and approved individually by a process owner or a functional manager

Structured Walk through (Table Top)
A Process owner or a functional manager review plans together in a meeting. The output of this exercise tends to be more reliable since the group collectively is likely to spot inter-dependencies between functions.

Test Hardware and Services Methods

Simulation
In this exercise type, the paper plan is tried out in an isolated test environment. Ideally this plan should be created in the actual off site relocation facility. However, it is my experience that this is not always practical, especially in the federal space where mutual aid agreements are used. I do see this trend changing as some of the recent disasters have illustrated practicality of a more realistic test.

NOTE:

I have observed that description of the simulation exercise on many current CISSP practice tests can be confusing for candidates. Some of these questions imply that conducting a simulation exercises at the primary site is a common practice. I would not expect this statement to be true on the CISSP exam. ISC2 seems to be updating their tests faster than normal, based on some international standards. From what I've seen and read on these standards, a simulation test is more commonly conducted at the alternate facility rather than the primary site, which would be my answer, if it was asked on the exam.

Live Process Exercise Methods

Activity Testing
This generally refers to the live cut-over of some production services to the alternate operations center as part of the exercise. This exercise type can be very dangerous as this implies a test failure can result in loss of production services.

In some environments the risk of a true fail over test is too great to accept. For example, in some cases the activity testing may only go to the point of verifying that data mirrored to the alternate site is identical to the primary. This can be verified by having a user perform a test operation in parallel with a live process and comparing the results.

Example:

Let's assume that the email server is the productive service in this parallel testing exercise. Even when the email server cut-over occurs without a hitch during the simulation exercise, the entire production email service could still fail due to an unforeseen, dependent service such as DNS replication or routing issues. A company without mail for an extended period could go out of business, so this is a risky exercise and it's not commonly practiced in the industry.

Full Test

This exercise type is the most realistic but also the most dangerous. In this scenario, the organization will actually conduct all operations using contingency sites and services. It is my experience that this type of exercise is rarely attempted by organizations other than the military and some financial sectors.

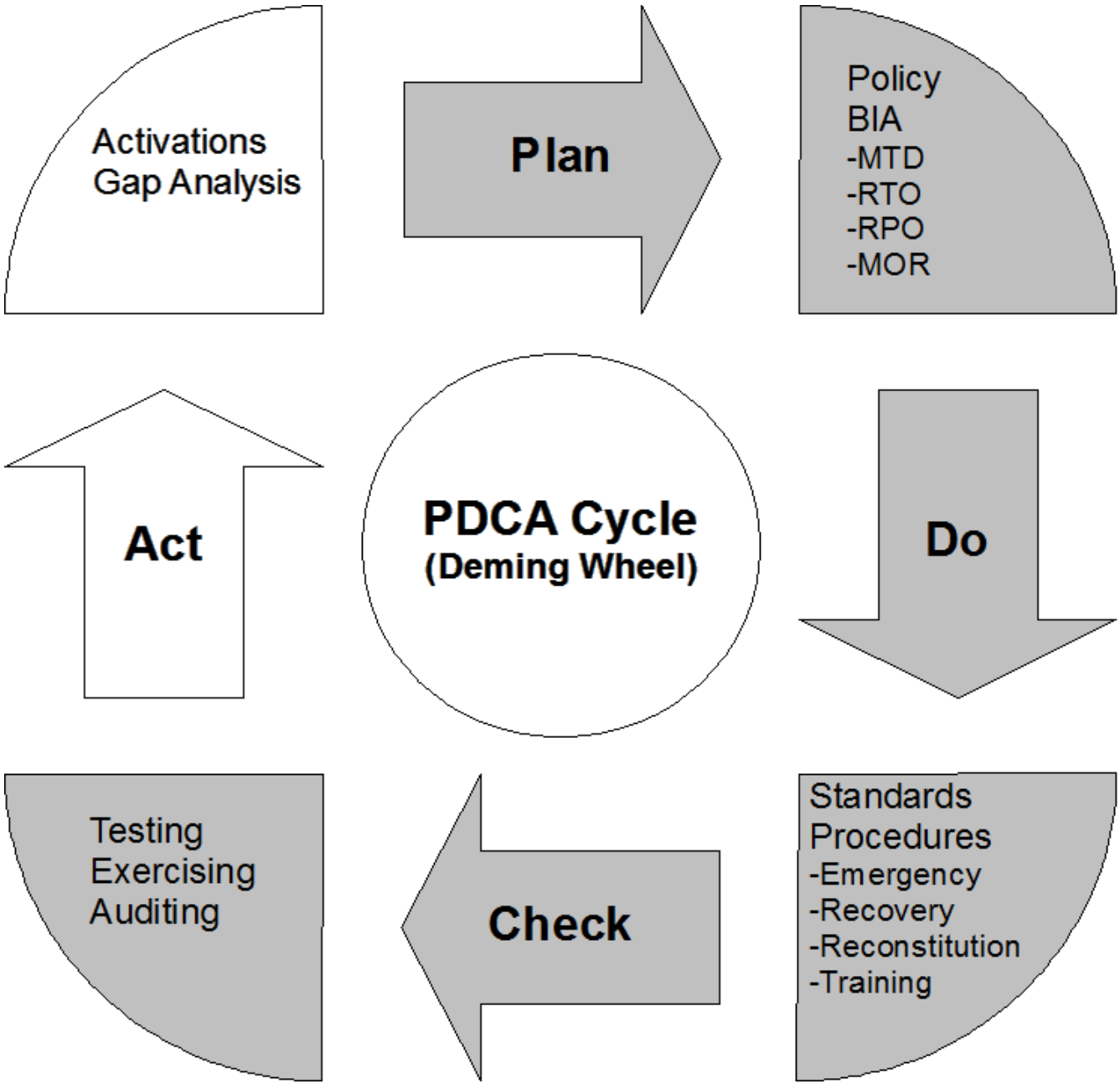
In summary, the ultimate goal of TT&E is to continuously improve the BC/DR plan, so when a disaster does strike, the documented business recovery objectives are achieved according to plan, as much as possible. At the same time, conducting a test introduces risk, so Test and Exercise plans should be limited only to a level appropriate for the organization.

AUDITS

There are two basic ways to check the effectiveness of the BC/DR program: Audits and Exercises. In an audit, whether internal or external, plans are checked for accuracy against a set of requirements. During plan exercises, a plan is stepped through one-by-one by the participants. This process simultaneously tests the plan and also trains the personnel.

In the Check phase of the life cycle, a critical means for achieving consistent process improvement is to employ an independent observer. During exercises and actual events, these independent observers are tasked with documenting and assessing the preparedness and the performance of the teams and the individual players. These independent observers should issue a gap analysis document outlining the deficiencies of the plan. The analysis is crucial in providing input to the Act phase (of PDCA), where the deficiencies should be addressed.

Plan-Do-Check-***Act***



Activation of the plan is ultimately the primary goal of BC/DR planning and is designed to be prepared to act appropriately during a disaster.

If all goes well, however, most of the actions we take in the "Act" phase of the PDCA process are Gap Analysis and process improvement. There may be gaps identified during a test, audit or an

actual disaster, as things rarely go exactly as planned. The output of the independent observer, as well as other stakeholder feedback, mentioned in the Check phase, should be presented to senior management and to the business continuity steering committee for correction. This will also identify problems with the plan, the performance of service providers or mistakes made by the recovery team members involved in the test.

One major cause for a failed exercise is due to undocumented changes - change in people, technology, corporate acquisitions and mergers, laws and regulations or other threat levels, for example, pandemic outbreaks.

Change management is easily one of the most important issues in security. BC/ DR plans must be constantly updated whenever there is a change in people, business processes and technology and other environmental issues.

Embedding BCM in the Organization's Culture

Constantly evolving awareness campaigns must be developed and presented to all stakeholders. Awareness should be measured through some testing, training and exercising programs to assess the current level of awareness and skills and identifying measurable improvement goals.

The BCI GPG suggests that an effective business continuity program include measures to:

1. Assess the level of BCM awareness and training
2. Develop BCM within the organization's culture
3. Monitor cultural change

Summary

If an event occurs that disrupts a critical service that results in great loss, a responsible organization will have resources to protect life and the best interests of the organization's stakeholders.

Plans must be in-place to prepare for emergency services and recovery of all critical processes, in the proper time frames to minimize the impact of a loss event, as well as to restore normal operations in the most logical order.

Emergency management teams must be created to handle the overall event including the initial response.

Recovery teams are created to recover operations using contingencies.

Reconstitution teams are created to restore normal operations.

Alternative sites, equipment and suppliers must be established.

Tests, exercises and audits are used to validations the plans, technologies and readiness of the BC/DR teams

BC/DR must be part of organizational culture.

Self Test

Question 1

Which of the following is most likely to affect a change in an organization's BC/DR policy?

a) Failure of critical infrastructure technology

b) Change in staff

c) Identity theft incident

d) Legal requirement

Question 2

During a BIA, Alice notices that data for an online customer order tracking system is backed up nightly to a remote system. However if there were a disk crash, there could be a loss of up to a full day's transactions. When Alice informs the process owner, the owner performs a needs analysis do determine an acceptable backup schedule. What metric would Alice use to design a more appropriate solution?

a) Maximum Tolerable Period of Disruption (MTPD)

b) Recovery Time Objective (RTO)

c) Recovery Point Objective (RPO)

d) Maximum Allowable Downtime (MAD)

Question 3

Which of the following sites would require the most effort to recover a critical process?

a) Hot

b) Mirrored

c) Mobile

d) Cold

Question 4

During a BC/DR exercise, a critical system was not recovered in the required time frame. An assessment by an independent observer identified a gap in the point of contact list accuracy. After further analysis, it was determined that the human resource records were not consistent with the contact lists in the call trees. Which of the following is most likely to improve the process?

a) Better training for the team members to understand such problems are common

b) Change in BC/DR policy to require more efficient technologies

c) Synchronizing the Human Resource systems to auto update the point of contact lists

d) Threat analysis

Question 5

A company that makes corrugated boxes gets a call from their paper supplier informing them they have just had a fire and that the supplier will not be able to provide paper for at least a month. Without the paper, they company can no longer make corrugated boxes. What process would MOST specifically allow an organization to be prepared for such emergencies?

a) Minimum Operating Requirements

b) Supply chain management

c) The Clark Wilson model

d) Plan-Do-Check-Act

Question 6

Which test type provides the most assurance that the alternate technologies specified in the DR plan are appropriate in a most cost-effective manner?

a) Simulation

b) Desk Check

c) Parallel

d) Bell Lapadula

Question 7

In what situations would senior management more likely to make the decision to accept a risk and require a BC/DR plan?

a) Low likelihood low impact events

b) High likelihood low impact events

c) Low likelihood high impact events

d) High likelihood high impact events

Question 8

At what stage in the BC/DR life cycle are the specific criticality metrics determined?

a) Project initiation

b) Functional requirements

c) System Design

d) Testing and Exercising

Question 9

The primary concern addressed by BC/DR plans is to achieve what security goal?

a) Confidentiality

b) Integrity

c) Availability

d) Compliance

Question 10

Of the following issues, which is least likely to negatively effect the results of a BC/DR test?

a) Succession plans

b) Technology failures

c) Poorly trained administrators

d) Hot site data restoration

Question 11

The primary purpose of exercising recovery plans is to:

a) Test the plan for accuracy

b) Meet industry specific regulations

c) Identify gaps in technical infrastructures and their ability to meet the recovery time objectives

d) Train personnel

Question 12

Who would be in the most appropriate position to confirm the appropriateness of the contingency plans after an test and exercise?

a) Security management

b) Operations management

c) User management

d) Senior management

Question 13

What alternate site would provide the best solution for processes with the shortest recovery time objectives:

a) Mirrored

b) Hot

c) Mobile

d) Alternate data streams

Question 14

What is the relationship between Maximum Tolerable Downtime or MTD and Recovery Time Objectives or RTO?

a) They are different terms for the same concept

b) RTO must be less than MTD to allow for the initial emergency response including damage assessment

c) RTO is greater than the MTD to provide safe evacuation of the facility

d) RTO is for people and MTD is for processes

Question 15

Which of the following is more likely to result in making improvements to the BC/DR plans?

a) Efficient business impact analysis

b) Effective service level agreements

c) Gap analysis

d) Third party audits

Self Test with answers

Question 1

Which of the following is most likely to affect a change in an organization's BC/DR policy?

a) Failure of critical infrastructure technology

b) Change in staff

c) Identity theft incident

d) Legal requirement

Answer – d

An organization's BC/DR policy is most affected by the business goals and relevant laws and regulations.

Question 2

During a BIA, Alice notices that data for an online customer order tracking system is backed up nightly to a remote system. However if there were a disk crash, there could be a loss of up to a full day's transactions. When Alice informs the process owner, the owner performs a needs analysis do determine an acceptable backup schedule. What metric would Alice use to design a more appropriate solution?

a) Maximum Tolerable Period of Disruption (MTPD)

b) Recovery Time Objective (RTO)

c) Recovery Point Objective (RPO)

d) Maximum Allowable Downtime (MAD)

Answer – c

To determine the point in time data must be reconstructed, the BC/DR planner must know the recovery point objectives of the affected business units. For some files, that rarely change, such as application or operating system files and other static records, RPOs can be satisfied with nightly backup or even less frequency. But most organizations have some processes with near real time data protection requirements.

Question 3

Which of the following sites would require the most effort to recover a critical process?

a) Hot

b) Mirrored

c) Mobile

d) Cold

Answer – d

Cold sites, which supply only environmental conditions, would require that the recovery team bring equipment, build and configure infrastructure, and restore data. This process could take weeks to complete and should not be used for any process classified as high criticality.

Question 4

During a BC/DR exercise, a critical system was not recovered in the required time frame. An assessment by an independent observer identified a gap in the point of contact list accuracy. After further analysis, it was determined that the human resource records were not consistent with the contact lists in the call trees. Which of the following is most likely to improve the process?

a) Better training for the team members to understand such problems are common

b) Change in BC/DR policy to require more efficient technologies

c) Synchronizing the Human Resource systems to auto update the point of contact lists

d) Threat analysis

Answer – c

Maintaining point of contact (POC) lists is critical to effective execution of a plan. Many security problems can occur, such as: deliberate sabotage by a recently fired and disgruntled employee; or ineffective recovery plans due to failure to reach proper personnel. Problems are especially prevalent when HR systems are not effectively interfaced with other assurance functions.

Question 5

A company that makes corrugated boxes gets a call from their paper supplier informing them they have just had a fire and that the supplier will not be able to provide paper for at least a month. Without the paper, they company can no longer make corrugated boxes. What process would MOST specifically allow an organization to be prepared for such emergencies?

a) Minimum Operating Requirements

b) Supply chain management

c) The Clark Wilson model

d) Plan-Do-Check-Act

Answer – b

The question asked for a process. While the need for paper could be measured by determining the MOR metrics, supply chain management is a process.

Question 6

Which test type provides the most assurance that the alternate technologies specified in the DR plan are appropriate in a most cost-effective manner?

a) Simulation

b) Desk Check

c) Parallel

d) Bell Lapadula

Answer -a

While both the parallel (called “Activity Testing”) and simulation tests will include testing of the contingency ICT infrastructures, the simulation is less costly. Recall that in a Parallel or Activity test, there are data checking personnel involved and in some cases includes the increasingly risky step of actually migrating some production activities o the alternate site. In simulation tests, recovery teams only confirm that the technical infrastructure is adequate.

Question 7

In what situations would senior management more likely to make the decision to accept a risk and require a BC/DR plan?

a) Low likelihood low impact events

b) High likelihood low impact events

c) Low likelihood high impact events

d) High likelihood high impact events

Answer – c

For low impact events, it is possible that a manager can choose to accept a risk, understanding that even if the event were to occur, there would be minimal loss. High impact events with a high likelihood of occurrence should either be avoided, eliminated, reduced or transferred. However, if a risk is perceived as high impact but with a very low likelihood of occurrence, it may be accepted and dealt with only in the event the risk is actualized.

Question 8

At what stage in the BC/DR life cycle are the specific criticality metrics determined?

a) Project initiation

b) Functional requirements

c) System Design

d) Testing and Exercising

Answer – b

The criticality metrics of MTD, RTO, RPO and MOR are determined in the business impact analysis (BIA) to determine the functional requirements of the BC/DR plans

Question 9

The primary concern addressed by BC/DR plans is to achieve what security goal?

a) Confidentiality

b) Integrity

c) Availability

d) Compliance

Answer – c

While all of the above answers are important security goals for any BC/DR manager, the primary goal is to keep the business continuing, which requires availability of essential processes, supplies and personnel.

Question 10

Of the following issues, which is least likely to negatively effect the results of a BC/DR test?

a) Succession plans

b) Technology failures

c) Poorly trained administrators

d) Hot site data restoration

Answer – a

The question asked “which is least likely to negatively effect” the plan execution. Answers b,c and d are all potential problems. Having a succession plans are required resources for effective BC/DR planning.

Question 11

The primary purpose of exercising recovery plans is to:

a) Test the plan for accuracy

b) Meet industry specific regulations

c) Identify gaps in technical infrastructures and their ability to meet the recovery time objectives

d) Train personnel

Answer – d

Recall the the plan itself is tested and audited for accuracy and appropriateness. The primary goal of exercising is to train people on how to follow the plan.

Question 12

Who would be in the most appropriate position to confirm the appropriateness of the contingency plans after an test and exercise?

a) Security management

b) Operations management

c) User management

d) Senior management

Answer - c

The users in a given department or process are more likely to understand if the exercise was able to recover the required services in the proper time frames and with the required resources.

Question 13

What alternate site would provide the best solution for processes with the shortest recovery time objectives:

a) Mirrored

b) Hot

c) Mobile

d) Alternate data streams

Answer – a

Both hot and mirrored sites are presumed to have all the required hardware and even application servers available but the mirrored site also has production data replicated and ready for use, where a hot site will require some restoration of data. Mobile sites aren't typically as technically redundant as the hot site and Alternate data streams are a complete distraction, as this referrers to a feature of the NTFS file system

Question 14

What is the relationship between Maximum Tolerable Downtime or MTD and Recovery Time Objectives or RTO?

a) They are different terms for the same concept

b) RTO must be less than MTD to allow for the initial emergency response including damage assessment

c) RTO is greater than the MTD to provide safe evacuation of the facility

d) RTO is for people and MTD is for processes

Answer -b

The maximum tolerable downtime refers to the maximum time and organization can survive without a critical process. Recovery time objectives set the anticipated times required to recover a process

under contingency operations. Since there will likely be a time lag from the initial failure of a critical system to the time of disaster declaration, the RTO must be shorter than MTD

Question 15

Which of the following is more likely to result in making improvements to the BC/DR plans?

a) Efficient business impact analysis

b) Effective service level agreements

c) Gap analysis

d) Third party audits

Answer – c

After a test, exercise, audit or actual event, management must compare the actual outcomes to the desired goals of the plans. Gap analysis is used to prioritize the resources needed to make improvements to the plans.