**5 Technology related business continuity planning (BCP) & Disaster recovery planning (DRP)**

**5.A Incorporate business impact analysis (BIA) requirements (e.g. legal, financial, stakeholders)**

**The Business Impact Analysis (BIA)** identifies time-critical aspects of the critical business processes, and determines their maximum tolerable downtime. The BIA helps to Identify organization functions, the capabilities of each organization unit to handle outages, and the priority and sequence of functions and applications to be recovered, identify resources required for recovery of those areas and interdependencies

In performing the Business Impact Analysis (BIA) it is very important to consider what the **dependencies** are. You cannot bring a system up if it depends on another system to be operational. You need to look at not only **internal dependencies** but external as well. You might not be able to get the raw materials for your business so dependencies are very important aspect of a BIA.

The BIA committee will not truly understand all business processes, the steps that must take place, or the resources and supplies these processes require. So the committee must gather this information from the people who do know— department managers and specific employees throughout the organization. The committee starts by identifying the people who will be part of the BIA data-gathering sessions. The committee needs to identify how it will collect the data from the selected employees, be it through surveys, interviews, or workshops. Next, the team needs to collect the information by actually conducting surveys, interviews, and workshops. Data points obtained as part of the information gathering will be used later during analysis. It is important that the team members ask about how different tasks— whether processes, transactions, or services, along with any relevant dependencies— get accomplished within the organization.

BIA - provides enterprise management with:

* a prioritized list of time-critical business processes.
* estimates a recovery time objective for each of the time critical processes.
* the components of the enterprise that support those processes.

There have been much discussion about the steps of the BIA and I struggled with this before deciding to scrape the question about "the four steps," and re-write the question using the AIO for a reference. This question should be easy.... if you know all eight steps.

The eight detailed and granular steps of the BIA are:

**1. Select Individuals to interview for the data gathering.**

**2. Create data gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).**

**3. Identify the company's critical business functions.**

**4. Identify the resources that these functions depend upon.**

**5. Calculate how long these functions can survive without these resources.**

**6. Identify vulnerabilities and the threats to these functions.**

**7. Calculate risk for each of the different business functions.**

**8. Document findings and report them to management.**

**Goals of BIA**

Criticality prioritization, downtime estimation, and resource requirments are the three primary goals of a BIA. Data processing continuity planning, data recovery plan maintenance, and testing the disaster recovery plan are steps in the DRP process. Scope and plan initiation, business continuity plan development, and plan approval and implementation are the other 3 elements of BCP. Facility requirements planning, facility security management, and administrative personnel controls are elements of administrative controls in Physical Security.

**Vulnerability analysis outcomes:**

**Quantitative loss criteria may be defined as follows:**

- Incurring financial losses from loss of revenue, capital expenditure, or personal liability resolution

- The additional operational expenses incurred due to the disruptive event

- Incurring financial loss from resolution of violation of contract agreements

- Incurring financial loss from resolution of violation of regulatory or compliance requirements

**Qualitative loss criteria may consist of the following:**

- The loss of competitive advantage or market share

- The loss of public confidence or credibility, or incurring public mbarrassment

During the vulnerability assessment, critical support areas must be defined in order to assess the impact of a disruptive event. A critical support area is defined as a business unit or function that must be present to sustain continuity of the business processes, maintain life safety, or avoid public relations embarrassment.

**Critical support areas could include the following:**

- Telecommunications, data communications, or information technology areas

- Physical infrastructure or plant facilities, transportation services

- Accounting, payroll, transaction processing, customer service, purchasing

The granular elements of these critical support areas will also need to be identified. By granular elements we mean the personnel, resources, and services the critical support areas need to maintain business continuity

IT contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. IT contingency planning fits into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization’s IT systems, business processes, and the facility. Because there is an inherent relationship between an IT system and the business process it supports, there should be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

**Disaster Recovery Plan (DRP)**

As suggested by its name, the DRP applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The DRP scope may overlap that of an IT contingency plan (see below); however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation. Dependent on the organization’s needs, several DRPs may be appended to the BCP.

**Business Continuity Plan (BCP)**

The BCP focuses on sustaining an organization’s business functions during and after a disruption. An example of a business function may be an organization’s payroll process or consumer information process. A BCP may be written for a specific business process or may address all key business processes. IT systems are considered in the BCP in terms of their support to the business processes. In some cases, the BCP may not address long-term recovery of processes and return to normal operations, solely covering interim business continuity requirements. A disaster recovery plan, business resumption plan, and occupant emergency plan may be appended to the BCP. Responsibilities and priorities set in the BCP should be coordinated with those in the Continuity of Operations Plan (COOP) to eliminate possible conflicts.

STEPS:

1.Develop the contingency planning policy statement and initiation of the project.

A formal policy provides the authority and guidance necessary to develop an effective contingency plan.

2. Conduct the business impact analysis (BIA).

The BIA helps identify and prioritize information systems and components critical to supporting the organization’s mission/business functions. A template for developing the BIA is provided to assist the user.

3. Identify preventive controls.

Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.

4. Create contingency strategies.

Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.

5. Develop an information system contingency plan.

The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system’s security impact level and recovery requirements.

6. Ensure plan testing, training, and exercises.

Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.

7. Ensure plan maintenance.

The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

**Business Recovery Plan (BRP), also called the Business Resumption Plan**

The BRP addresses the restoration of business processes after an emergency, but unlike the BCP, lacks procedures to ensure continuity of critical processes throughout an emergency or disruption. Development of the BRP should be coordinated with the disaster recovery plan and BCP. The BRP may be appended to the BCP.

Continuity of Support Plan/IT Contingency Plan. OMB Circular A-130, Appendix III, requires the development and maintenance of continuity of support plans for general support systems and contingency plans for major applications. This planning guide considers continuity of support planning to be synonymous with IT contingency planning. Because an IT contingency plan should be developed for each major application and general support system, multiple contingency plans may be maintained within the organization’s BCP.

**The incident response plan** focuses on information security responses to incidents affecting systems and/or networks. It establishes procedures to address cyber attacks against an organization's IT systems. These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware or software. The continuity of support plan is the same as an IT contingency plan. It addresses IT system disruptions and establishes procedures for recovering a major application or general support system. It is not business process focused. The business continuity plan addresses business processes and provides procedures for sustaining essential business operations while recovering from a significant disruption. The continuity of operations plan addresses the subset of an organization's missions that are deemed most critical and procedures to sustain these functions at an alternate site for up to 30 days.

**The Criticality Survey is** implemented through a standard questionnaire to gather input from the most knowledgeable people. Not all personnel that is going to be part of recovery teams is necessarily able to help in identifying critical functions of the organization.

The intent of such a survey is to identify the services and systems that are critical to the organization.

Having a clearly stated purpose for the survey helps in avoiding misinterpretations.

Management's approval of the survey should be obtained before distributing it.

**DR and BCP -** The keyword is ' MOST CRITICAL ' and the correct answer is ' Management Support ' as the management must be convinced of its necessity and that's why a business case must be made. The decision of how a company should recover from any disaster is purely a business decision and should be treated as so.

**5.B Determine security strategies for availability and recovery**

**5.B.1 Identify solutions (e.g. cold, warm, hot, insource, outsource)**

**A Hot Site** contains everything needed to become operational in the shortest amount of time.

According to the OIG, a hot site is defined as a fully configured site with complete customer required hardware and software provided by the service provider. A hot site in the context of the CBK is always a RENTAL place. If you have your own site fully equipped that you make use of in case of disaster that would be called a redundant site or an alternate site.

Wikipedia: "A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data." A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software. Following a disruption to the original site, the hot site exists so that the organization can relocate with minimal losses to normal operations. Ideally, a hot site will be up and running within a matter of hours or even less. Personnel may still have to be moved to the hot site so it is possible that the hot site may be operational from a data processing perspective before staff has relocated. The capacity of the hot site may or may not match the capacity of the original site depending on the organizations requirements. This type of backup site is the most expensive to operate. Hot sites are popular with organizations that operate real time processes such as financial institutions, government agencies and ecommerce providers

**A warm site** has some basic equipment or in some case almost all of the equipment but it is not sufficient to be operational without bringing in the last backup and in some cases more computers and other equipment. A warm site is a location where the organisation can relocate to after the disruption that is already stocked with computer hardware similar to that of the original site, but does not contain backed up copies of data and information. It may or may not have the same capacity as the original site depending on the organisations requirements. Data will have to be restored onto the equipment at this site before activities can re-commence.

**A cold** **site** has basically power, HVAC, basic cabling, but no or little as far as processing equipment is concerned. All other equipment must be brought to this site. It might take a week or two to reconstruct. A cold site is the most inexpensive type of backup site for an organization to operate. It does not include backed up copies of data and information from the original location of the organisation, nor does it include hardware already set up. The lack of hardware contributes to the minimal startup costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

**A rolling hot-site** is fully configured with all the required hardware.

**Redundant -** Usually within most certification body of knowledge the terms Cold, Warm, and Hot sites refer to rental places.

A synonym for Redundant site would also be Alternate Side.

**A reciprocal agreement** between two companies with like equipments and processing needs provides an inexpensive alternative to other off-site facilities. Sometimes though this solution can prove to be inadequate since environments tend to be maxed out, or one site upgrades part of the equipment into something that is not necessarily compatible. As opposed to agreements with off-site facilities providers, reciprocal agreements cannot be enforced, so there is no guarantee that this facility will really be available to the company in a time of need.

**Mobile Sites** are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.

**Mirrored Sites** are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.

Disaster Recovery should never be considered a **discretionary expense.** It is far too important a task. In order to maintain the continuity of the business Disaster Recovery should be a commitment of and by the organization.

A discretionary fixed cost has a short future planning horizon—under a year. These types of costs arise from annual decisions of management to spend in specific fixed cost areas, such as marketing and research.

A committed fixed cost has a long future planning horizon— more than on year. These types of costs relate to a company’s investment in assets such as facilities and equipment. Once such costs have been incurred, the company is required to make future payments.

**5.B.2 Define processing agreement requirements (e.g. recipricol, mutual, cloud, outsourcing, virtualization)**

**5.B.3 Establish recovery time objectives and recovery point objectives**

**The recovery point objective (RPO)** is the maximum acceptable level of data loss following an unplanned “event”, like a disaster (natural or man-made), act of crime or terrorism, or any other business or technical disruption that could cause such data loss. The RPO represents the point in time, prior to such an event or incident, to which lost data can be recovered (given the most recent backup copy of the data).

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.

**The recovery time objective (RTO)** is a period of time within which business and / or technology capabilities must be restored following an unplanned event or disaster. The RTO is a function of the extent to which the interruption disrupts normal operations and the amount of revenue lost per unit of time as a result of the disaster.

These factors in turn depend on the affected equipment and application(s). Both of these numbers represent key targets that are set by key businesses during business continuity and disaster recovery planning; these targets in turn drive the technology and implementation choices for business resumption services, backup / recovery / archival services, and recovery facilities and procedures.

Many organizations put the cart before the horse in selecting and deploying technologies before understanding the business needs as expressed in RPO and RTO; IT departments later bear the brunt of user complaints that their service expectations are not being met. Defining the RPO and RTO can avoid that pitfall, and in doing so can also make for a compelling business case for recovery technology spending and staffing.

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 has been done.

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.

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

Here are some examples of MTD values suggested by Shon Harris:

NonEssential 30 Days

Normal 7 Days

Important 72 Hours

Urgent 24 Hours

Critical Minutes to hours

**5.C Design Continuity Recovery solution**

**5.C.1 High availability, failover, resiliency (e.g. communication path diversity, paired development, pass-through network interfaces, application)**

**5.C.2 Availability of service porvidor/ supplier support (e.g. cloud, SLAs)**

**5.C.3 BCP/DRP Architecture Validation (e.g. test scenarios, requirements traceability matrix, trade-off matirces)**

After a test has been performed the most useful test results for management would be **knowing what worked and what didn't** so that they could correct the mistakes where needed.

**DR TEST:**

The structured walk-through test occurs when the functional representatives meet to review the plan in detail. This involves a thorough look at each of the plan steps, and the procedures that are invoked at that point in the plan. This ensures that the actual planned activities are accurately described in the plan. The checklist test is a method of testing the plan by distributing copies to each of the functional areas. The simulation test plays out different scenarios. The parallel test is essentially an operational test that is performed without interrupting current processing.

**BCP TEST:**

It is important to have ways to measure the success of the plan and tests against the stated objectives. Therefore, results must be quantitatively gauged as opposed to an evaluation based only on observation. Quantitatively measuring the results of the test involves a generic statement measuring all the activities performed during BCP, which gives the best assurance of an effective plan. Although choices A and B are also quantitative, they relate to specific areas, or an analysis of results from one viewpoint, namely the accuracy of the results and the elapsed time.

**The five types of BCP testing are:**

**Checklist—Copies** of the plan are sent to different department managers and business unit managers for review. This is a simple test and should be used in conjunction with other tests.

**Structured Walk-through**—Team members and other individuals responsible for recovery meet and walk through the plan step-by-step to identify errors or assumptions.

**Simulation**—This is a simulation of an actual emergency. Members of the response team act in the same way as if there was a real emergency.

**Paralle**l—This is similar to simulation testing, but the primary site is uninterrupted and critical systems are run in parallel at the alternative and primary sites. The systems are then compared to ensure all systems are in sync.

**Full interruption**—This test involves all facets of the company in a response to an emergency. It mimics a real disaster where all steps are performed to test the plan. Systems are shut down at the primary site and all individuals who would be involved in a real emergency, including internal and external organizations, participate in the test. This test is the most detailed, time-consuming, and expensive all of these.

**OTHER:**

**The Disaster Recovery Manager** should also be a member of the team that assisted in the development of the Disaster Recovery Plan. Senior-level management need to support the process but would not be involved with the initial process.

The cited source mentions that three concepts are used to create a level of fault tolerance and redundancy in transaction processing. **Electronic vaulting, remote journaling and database shadowing** provide redundancy at the transaction level. Other techniques like on-site or off-site mirroring or disk duplexing provides redundancy at a lower level.

**RCV** is the maximum amount your insurance company will pay you for damage to covered property before deducting for depreciation. The RCV payment is based on the current cost to replace your property with new, identical or comparable property.

**critical support -** Business units or functions that must be present to sustain continuity of business, maintain life safety and avoid public embarrassment

**Electronic Vaulting** is the process of transferring backup data to off-site location through communication lines.

**Remote Journaling** is a higher level of transaction redundancy than Electronic Vaulting. Remote Journaling is a technology to facilitate sending copies of the journal of transaction entries from a production system to a secondary system in realtime. The remote nature of such a connection is predicated upon having local journaling already established. Local journaling on the production side allows each change that ensues for a journal-eligible object e.g., database physical file, SQL table, data area, data queue, byte stream file residing within the IFS) to be recorded and logged. It’s these local images that flow to the remote system. Once there, the journal entries serve a variety of purposes, from feeding a high availability software replay program or data warehouse to offering an offline, realtime vault of the most recent database changes.

**The least critical functions should be moved back first**

It's interesting to note that the steps to resume normal processing operations will be different than the steps of the recovery plan; that is, the least critical work should be brought back first to the primary site.

The most important point above in the steps would be to move the least critical items or resources back to the primary site first. This way you can ensure that the site was really well prepared and that all is working fine.

Before that first step would be done, you would get the green light from the salvage team that it is fine to move back to the primary site. The first step after getting the green light would be to move the least critical elements first.

**RAID Level 2 :-** The parity information is created using a hamming code that detects errors and establishes which part of which drive is in error.

The correct answer is ' **Critical recovery priority levels are not defined '** as the lack of definition of critical recovery priority levels would damage the recovery timeframe window, since this would cause applications to be recovered that might not be needed for the critical process.

**Mean-time-between failure (MTBF)** is the average length of time the hardware is functional without failure.

**Mean-time-to-repair** is the amount of time it takes to repair and resume normal operation after a failure has occurred.

Having a higher MTBF and a lower MTTR will increase the reliability of a piece of equipment, thus the system's overall reliability.

**ROLES:**

Many elements of a BCP will address senior management, such as the statement of importance and priorities, the statement of organizational responsibility, and the statement of urgency and timing. Executive management staff initiates the project, gives final approval and gives ongoing support. The BCP committee directs the planning, implementation, and tests processes whereas functional business units participate in implementation and testing.

The BCP committee should be made up of at least the following:

* Business Units
* Senior Management
* IT Department
* Security Department
* Communications Department
* Legal Department

The HR department is not included in this list and does not necessarily have to be a part of the BCP committee.

**Electronic vaulting** refers to the transfer of backup data to an off-site location. This is primarily a batch process of dumping backup data through communications lines to a server at an alternate location. Remote journaling refers to the parallel processing of transactions to an alternate site (as opposed to a batch dump process). Database shadowing uses the live processing of remote journaling, but creates even more redundancy by duplicating the database sets to multiple servers. Data clustering refers to the classification of data into groups (clusters).

**6 Physical security considerations**

**6.A Assess requirements**

**6.A.1 Policies and standards (e.g. export controls, escort policy, liase with law enforcement and external media)**

**6.A.2 Intergrate physical security with identity (e.g. wiring closet access, badge and enterprise identity management)**

**6.A.3 Map physical security needs against business drivers (e.g. outsourcing, relocations, mergers, acquisitions, divestitures, plant closings)**

**6.B Integrate Physical Products and Systems**

**6.B.1 Review common techniques, technologies and architectural principles**

A Class C fire extinguisher is preferable when a fire involves electrical equipment including wiriing. Common Class C suppression includes: gas (i.e. Halon, FM-200, Carbon Dioxide, etc) or soda acid.

To aid in memorization of Fire Class write on a paper the classes A through D, simply think of my firstname which is CLEMENT then put the word CLEM vertically as shown below:

Class A -> C = Combustible

Class B -> L = Liquid

Class C -> E = Electrical

Class D -> M = Metals

Below you will find a more detailed model.

Class A = Combustible

Type of Fire: Common Combustibles

Elements of Fire: wood products, paper, and laminates

Suppression Method: water, foam

Class B = Liquid

Type of Fire: Liquid

Elements of Fire: Petroleum products and coolants

Suppression Method: Gas, CO2, foam, dry powders.

Class C = Electrical

Type of Fire: Electrical

Elements of Fire: Electrical equipment and wires

Suppression Method: Gas, CO2, dry powders.

Class D = Metals

Type of Fire: Combustible Metals

Elements of Fire: Magnesium, sodium, potassium

Suppression Method: Dry powder.

**Halon -** It must be noted that Halon is now banned from being produce or manufacture in most country or cities.

Multiple countries have agreed to and signed The Montreal Protocol which disallow production of Halon.

Data Centers that still have Halon loaded within their cylinders will replace it with a safe replacement such as FM200 or Innergen if they ever make use of it.

Halon is a compound consisting of bromine, fluorine, and carbon. Halons are used as fire extinguishing agents, both in built-in systems and in handheld portable fire extinguishers. Halon production in the U.S. ended on December 31, 1993, because they contribute to ozone depletion. Bromine being part of Halon is not a safe replacement for Halon.

**Halon replacement:**

**Innergen,**

**FM200**

**FE13**

The correc answer is: Order a **non-Hydrochlorofluorocarbon compound** from the manufacturer

The best choice is to find or replace the systems with a Non-Hydrochlorofluorocarbon compound. A safe replacement such as Innergen, FM-200, or other non ozone depleting agent would be used.

Four elements must be presentin order for fire to exist. These elements are HEAT, FUEL, OXYGEN and CHAIN REACTION.

While not everything is known about the combustion process, it is generally accepted that fire is a chemical reaction. This reaction is dependent upon a material rapidly oxidizing, or uniting with oxygen so rapidly that it produces heat and flame.

Until the advent of newer fire extinguishing agents, fire was thought of as a triangle with the three sides represented by heat, fuel, and oxygen. If any one of the three sides were to be taken away, the fire would cease to exist.

Studies of modern fire extinguishing agents have revealed a fourth element - a self propagating chain reaction in the combustion process. As a result, the basic elements of fire are represented by the fire tetrahedron - HEAT, FUEL, OXYGEN and CHAIN REACTION.

The theory of fire extinguishment is based on removing any one or more of the four elements in the fire tetrahedron to suppress the fire.

**REMOVING THE HEAT**

In order to remove the heat, something must be applied to the fire to absorb the heat or act as a heat exchanger. Water is not the only agent used to accomplish this, but it is the most common.

**REMOVING THE FUEL**

Under many circumstances, it is not practical to attempt to remove the fuel from the fire. When dealing with flammable liquid fires, valves can be shut off and storage vessels pumped to safe areas to help eliminate the supply of fuel to the fire. Flammable gas fires are completely extinguished by shutting off the fuel supply.

**REMOVE THE OXYGEN**

Oxygen as it exists in our atmosphere (21%) is sufficient to support combustion in most fire situations. Removal of the air or oxygen can be accomplished by separating it from the fuel source or by displacing it with an inert gas. Examples of separation would be foam on a flammable liquid fire, a wet blanket on a trash fire, or a tight fitting lid on a skillet fire. Agents such as CO2, nitrogen, and steam are used to displace the oxygen.

**INTERRUPT THE CHAIN REACTION**

Modern extinguishing agents, such as dry chemical and halons, have proven to be effective on various fires even though these agents do not remove heat, fuel, or oxygen. Dry chemical and halogenated agents are thought to suspend or bond with “free radicals” that are created in the combustion process and thus prevent them from continuing the chain reaction.

UPSs use battery packs that range in size and capacity. A UPS can be online or standby.

**Online UPS** systems use AC line voltage to charge a bank of batteries. When in use, the UPS has an inverter that changes the DC output from the batteries into the required AC form and that regulates the voltage as it powers computer devices.

Online UPS systems have the normal primary power passing through them day in and day out. They constantly provide power from their own inverters, even when the electric power is in proper use. Since the environment's electricity passes through this type of UPS all the time, the UPS device is able to quickly detect when a power failure takes place. An online UPS can provide the necessary electricity and picks up the load after a power failure much more quickly than a standby UPS.

**Standby UPS** devices stay inactive until a power line fails. The system has sensors that detect a power failure, and the load is switched to the battery pack. The switch to the battery pack is what causes the small delay in electricity being provided.

So an online UPS picks up the load much more quickly than a standby UPS, but costs more of course.

**A dry pipe system** is used in areas where the water in the pipes is subject to freezing, and to minimize the chances of accidental discharge of water if the pipes would freeze in the winter time, and It minimizes chances of accidental discharge of water as well by not releasing the water until the pressure in the pipe would drop due to one of the sprinkler head being opened.

**A Dry Pipe system** has the water being held back from charging the sprinkler pipe system by a special kind of check valve called a "dry pipe valve" or "clapper valve". A dry pipe system is also a system which the pipes are filled with pressurized air or nitrogen rather than water. The air uses a mechanical advantage which holds back a device known as a dry pipe valve or clapper valve that prevent the water from getting into the pipe when it is pressurized. A small amount of water, called priming water, is also inside the dry pipe system, which is filled with either air or nitrogen under pressure.

**The sprinkler pipe system** is filled with pressurized air or nitrogen, which keeps the dry pipe valve closed using mechanical advantage. When any of the sprinkler valves open, the pressurized air or nitrogen is released, and the dropping pressure permits the dry pipe valve to open. It's primary use is to protect the sprinkler pipes from freezing.

**A Wet Pipe system** has the pipes always charged with water, and the thermal-fusible link in each sprinkler head is holding back the water. If any sprinkler head is exposed to enough heat, for long enough, the link will break/melt and water will be discharged. A wet pipe system is generally used when there is no danger of the water in the pipes freezing or when there are no special conditions that require a special purpose sprinkler system.

**A Preaction Pipe system** is used where accidental activation is undesired. It is similar to a Dry Pipe system, except one or more other interlocks, such as fire/heat sensors, are used in addition to sprinkler head opening and relieving the air pressure, which then permits the water to charge the sprinkler pipe system and flow through the open sprinkler head. This system has the added value of requiring a series of events before the water is actually permitted to flow, which can enable personnel to handle a small fire or incident without the flow of water. Preaction systems are similar to dry pipe systems in that the water is not held in the pipes, but is released when the pressurized air within the pipes is reduced. Once this happens, the pipes are filled with water, but it is not released right away. A thermal-fusible link on the sprinkler head has to melt before the water is released. The purpose of combining these two techniques is to give people more time to respond to false alarms or to small fires that can be handled by other means. Putting out a small fire with a handheld extinguisher is better than losing a lot of electrical equipment to water damage. These systems are usually used only in data processing environments rather than the whole building, because of the higher cost of these types of systems.

**Deluge** A deluge system has its sprinkler heads wide open to allow a larger volume of water to be released in a shorter period. Because the water being released is in such large volumes, these systems are usually not used in data processing environments.

**6.B.2 Perimeter protection and internal zoning**

Power Excess

Spike --> Too much voltage for a short period of time.

Surge --> Too much voltage for a long period of time.

Power Loss

Fault --> A momentary power outage.

Blackout --> A long power interruption.

Power Degradation

Sag or Dip --> A momentary low voltage.

Brownout --> A prolonged power supply that is below normal voltage.

**6.C Evaluate Solutions**

**6.C.1 Define test scenarios**

**6.C.2 Evaluate test deficiencies**

**OTHER:**

**Electrical distribution systems**

When you consider top priority tickets for the data center, security, data protection, and power consumption rise to the top. But the one thing that every data center should have, that we often throw on the back burner, is fire protection. Right now, if you heard that your data center was engulfed in flames, you would likely sit in shock, especially if you were not equipped with the proper protection. Fortunately, you can avoid this reality by taking the proper steps to protect your data center.

Dave Admirand, chief data center engineer at PTS Data Center Solutions (www.ptsdcs.com), says in his own experience, electrical fires are the most common types of fires in data centers. He says, "These are typically caused by electronic equipment failures or failures of the branch circuits powering the data center equipment, including UPS and air-conditioning equipment—if located in the data center.”

So what does the industry offer when it comes to fire detectors and extinguishing systems designed for the data center? According to Ziemba, there is a myriad of different smoke and heat detectors available, and some, he says, are so sophisticated that they can detect—and help extinguish—a fire even before it reaches the incipient, or flame, stage. He says, “Detectors that provide early warning capabilities are very effective in this type of situation. Addressable control panels serve as the brains for the overall fire suppression system in that they receive the signals from the detectors, provide some type of warning to the occupants, and then discharge the system.”

**SENSORS:**

These types of sensors are designed for indoor use. Outdoor use would not be advised due to false alarm vulnerability and weather durability.

Passive infrared detectors

**The passive infrared detector (PIR) is** one of the most common detectors found in household and small business environments because it offers affordable and reliable functionality. The term passive means the detector is able to function without the need to generate and radiate its own energy (unlike ultrasonic and microwave volumetric intrusion detectors that are “active” in operation). PIRs are able to distinguish if an infrared emitting object is present by first learning the ambient temperature of the monitored space and then detecting a change in the temperature caused by the presence of an object. Using the principle of differentiation, which is a check of presence or nonpresence, PIRs verify if an intruder or object is actually there. Creating individual zones of detection where each zone comprises one or more layers can achieve differentiation. Between the zones there are areas of no sensitivity (dead zones) that are used by the sensor for comparison.

**Ultrasonic detectors**

Using frequencies between 15 kHz and 75 kHz, these active detectors transmit ultrasonic sound waves that are inaudible to humans. The Doppler shift principle is the underlying method of operation, in which a change in frequency is detected due to object motion. This is caused when a moving object changes the frequency of sound waves around it. Two conditions must occur to successfully detect a Doppler shift event:

There must be motion of an object either towards or away from the receiver.The motion of the object must cause a change in the ultrasonic frequency to the receiver relative to the transmitting frequency.The ultrasonic detector operates by the transmitter emitting an ultrasonic signal into the area to be protected. The sound waves are reflected by solid objects (such as the surrounding floor, walls and ceiling) and then detected by the receiver. Because ultrasonic waves are transmitted through air, then hard-surfaced objects tend to reflect most of the ultrasonic energy, while soft surfaces tend to absorb most energy.

When the surfaces are stationary, the frequency of the waves detected by the receiver will be equal to the transmitted frequency. However, a change in frequency will occur as a result of the Doppler principle, when a person or object is moving towards or away from the detector. Such an event initiates an alarm signal. This technology is considered obsolete by many alarm professionals, and is not actively installed.

**Microwave detectors**

This device emits microwaves from a transmitter and detects any reflected microwaves or reduction in beam intensity using a receiver. The transmitter and receiver are usually combined inside a single housing (monostatic) for indoor applications, and separate housings (bistatic) for outdoor applications. To reduce false alarms this type of detector is usually combined with a passive infrared detector or "Dualtec" alarm.

Microwave detectors respond to a Doppler shift in the frequency of the reflected energy, by a phase shift, or by a sudden reduction of the level of received energy. Any of these effects may indicate motion of an intruder.

**Photo-electric beams**

Photoelectric beam systems detect the presence of an intruder by transmitting visible or infrared light beams across an area, where these beams may be obstructed. To improve the detection surface area, the beams are often employed in stacks of two or more. However, if an intruder is aware of the technology's presence, it can be avoided. The technology can be an effective long-range detection system, if installed in stacks of three or more where the transmitters and receivers are staggered to create a fence-like barrier. Systems are available for both internal and external applications. To prevent a clandestine attack using a secondary light source being used to hold the detector in a 'sealed' condition whilst an intruder passes through, most systems use and detect a modulated light source.

**Glass break detectors**

The glass break detector may be used for internal perimeter building protection. When glass breaks it generates sound in a wide band of frequencies. These can range from infrasonic, which is below 20 hertz (Hz) and can not be heard by the human ear, through the audio band from 20 Hz to 20 kHz which humans can hear, right up to ultrasonic, which is above 20 kHz and again cannot be heard. Glass break acoustic detectors are mounted in close proximity to the glass panes and listen for sound frequencies associated with glass breaking. Seismic glass break detectors are different in that they are installed on the glass pane. When glass breaks it produces specific shock frequencies which travel through the glass and often through the window frame and the surrounding walls and ceiling. Typically, the most intense frequencies generated are between 3 and 5 kHz, depending on the type of glass and the presence of a plastic interlayer. Seismic glass break detectors “feel” these shock frequencies and in turn generate an alarm condition.

The more primitive detection method involves gluing a thin strip of conducting foil on the inside of the glass and putting low-power electrical current through it. Breaking the glass is practically guaranteed to tear the foil and break the circuit.

**Smoke, heat, and carbon monoxide detectors**

Most systems may also be equipped with smoke, heat, and/or carbon monoxide detectors. These are also known as 24 hour zones (which are on at all times). Smoke detectors and heat detectors protect from the risk of fire and carbon monoxide detectors protect from the risk of carbon monoxide. Although an intruder alarm panel may also have these detectors connected, it may not meet all the local fire code requirements of a fire alarm system.

Other types of volumetric sensors could be:

**Active Infrared**

**Passive Infrared/Microware combined**

**Radar**

**Accoustical Sensor/Audio**

**Vibration Sensor (seismic)**

**Air Turbulence**

**EMI**

Common-mode noise is electrical noise between the hot and ground wire and between the neutral and ground wire.

Common mode noise will disrupt the memory logic of the processor. Noise between neutral and ground creates problems since the theoretical zero voltage between neutral and ground is utilized by microprocessors and digital logic control systems as zero voltage reference. A voltage on the ground wire will disrupt the stored memory variables of today's fast microprocessors. Common mode noise can be incorrectly interpreted as data.

This noise can cause what appears to be "software glitches", erratic performance of the equipment and partial or complete memory loss. Poor grounding also contributes significantly to common mode noise and this dynamic situation can change with building age, material corrosion, soil conditions and construction.

**Crime Prevention Through Environmental Design (CPTED)** is a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior. It provides guidance about lost and crime prevention through proper facility contruction and environmental components and procedures.

Crime prevention through Environmental Design (CPTED) is a concept that encourages individuals to feel ownership and respect for the territory they consider occupy. By encouraging the use of physical attributes that express ownership, the individual is more apt to protect and be aware in that environment

The three main components of CPTED are:

1) natural access control - the guidance of people entering and leaving a space by the placement of doors, fences, lighting, and even landscaping

2) natural surveillance - the goal is make criminals feel uncomfortable by providing many ways observers could potentially see them

3) natural territorial reinforcement - creates physical designs that emphasize or extend the company's physical sphere of influence so users feel a sense of ownership of that space.

**Positive pressurization** means that when an employee opens a door, the air goes out and outside air does not come in.

In building construction, **a plenum (pronounced PLEH-nuhm, from Latin meaning full) is** a separate space provided for air circulation for heating, ventilation, and air-conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a drop-down ceiling. A plenum may also be under a raised floor. In buildings with computer installations, the plenum space is often used to house connecting communication cables. Because ordinary cable introduces a toxic hazard in the event of fire, special plenum cabling is required in plenum areas.

**DATA CENTRE LOCATION**

You data center should be located in the middle of the facility or the core of a building to provide protection from natural disasters or bombs and provide easier access to emergency crewmembers if necessary. By being at the core of the facility the external wall would act as a secondary layer of protection as well.

Information processing facilities should not be located on the top floors of buildings in case of a fire or flooding coming from the roof. Many crimes and theft have also been conducted by simply cutting a large hole on the roof.

They should not be in the basement because of flooding where water has a natural tendancy to flow down :-) Even a little amount of water would affect your operation considering the quantity of electrical cabling sitting directly on the cement floor under under your raise floor.

The data center should not be located on the first floor due to the presence of the main entrance where people are coming in and out. You have a lot of high traffic areas such as the elevators, the loading docks, cafeteria, coffee shopt, etc.. Really a bad location for a data center.

So it was easy to come up with the answer by using the process of elimination where the top, the bottom, and the basement are all bad choices. That left you with only one possible answer which is the third floor.

**Capacitance detectors monitor** an electrical field surrounding the object being monitored. They are used for spot protection within a few inches of the object, rather than for overall room security monitoring used by wave detectors. Penetration of this field changes the electrical capacitance of the field enough to generate and alarm. Wave pattern motion detectors generate a frequency wave pattern and send an alarm if the pattern is disturbed as it is reflected back to its receiver. Field-powered devices are a type of personnel access control devices. Audio detectors simply monitor a room for any abnormal sound wave generation and trigger an alarm.

**Integrity Controls Mechanisms** are not part of physical security. All of the other detractors were correct this one was the wrong one that does not belong to Physical Security. Below you have more details extracted from the SearchSecurity web site:

Information security depends on the security and management of the physical space in which computer systems operate. Domain 9 of the CISSP exam's Common Body of Knowledge addresses the challenges of securing the physical space, its systems and the people who work within it by use of administrative, technical and physical controls. The following topics are covered:

* Facilities management: The administrative processes that govern the maintenance and protection of the physical operations space, from site selection through emergency response.
* Risks, issues and protection strategies: Risk identification and the selection of security protection components.
* Perimeter security: Typical physical protection controls.

The effectiveness of security controls is measured by the probability of detection at the point where there is enough time for a response team to interrupt an adversary. **The critical path** is the adversary path with the lowest probability of interruption.

**An adversary path** is an ordered sequence of actions against an asset that could result in it being compromised. Adversaries could normally be expected to take the easiest and most direct route. Early detection of unauthorised access enables a quicker response. Ideally interception should occur before access to the asset, but this depends on the asset and the security objectives. Interruption may not be required if tamper evidence is the objective for protecting the asset.

The ideal operating humidity range is defined as 40 percent to 60 percent. High humidity:

**(greater than 60 percent) can produce - Corrosion.**

**(less than 40 percent) can produce – Static Electricity**

Lighting should be used to discourage intruders and provide safety for personnel, entrances, parking areas and critical sections. **Critical areas should be illuminated 8 feet high and 2 feet out.**

**Magnetic media are affected from 100 degrees Fahrenheit.** Disks are damaged at 150 degrees Fahrenheit, computer equipment at 175 degrees Fahrenheit, and paper products at 350 degrees Fahrenheit.

**A static charge of 1500 volts** is able to cause disk drive data loss.

A charge of 1000 volts is likely to scramble monitor display and a charge of 2000 volts can cause a system shutdown.

It should be noted that charges of up to 20,000 volts or more are possible under conditions of very low humidity with non-static-free carpeting.

FAIL?

**Fail soft**

A system that experience a security issue would disable only the portion of the system being affected by the issue. The rest of the system would continue to function as expected. The component or service that failed would be isolated or protected from being abused.

**Fail Safe**

A fail-safe lock in the PHYSICAL security context will default to being unlocked in case of a power interruption.

A fail-safe mechanisms in the LOGICAL security context will default to being locked in case of problem or issues. For example if you have firewall and it cannot apply the policy properly, it will default to NO access and all will be locked not allowing any packet to flow through without being inspected.

**Fail open**

A Fail Open mean that the mechanism will default to being unlocked in case of a failure or problem. This is very insecure. If you have a door access control mechanism that fail open then it means that the door would be unlocked and anyone could get through. A logical security mechanism would grant access and do no access control.

**Fail closed**

A Fail closed mean that the mechanism will default to being locked in case of a failure or problem. That would be a lot more secure than Fail Open for a logical access control mechanism.

**Fail secure**

A fail-secure in the logical or physical security context will default to being locked in case of a power interruption or a service that is not functioning properly. Nobody could exit the building and nobody would be able to come in either. In case of the logical context there is no access granted and everything is locked.