

Introduction to Information Security

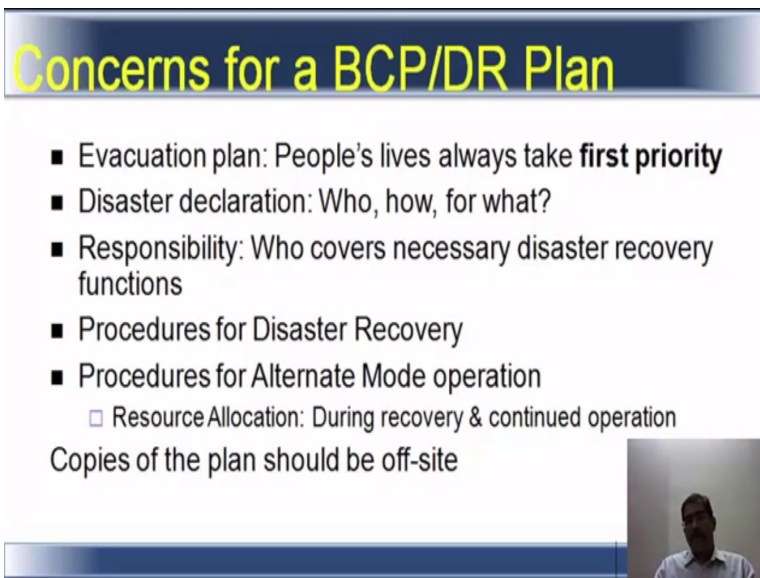
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

Lecture - 39


(Refer Slide Time: 00:11)



Concerns for a BCP/DR Plan

- Evacuation plan: People's lives always take **first priority**
- Disaster declaration: Who, how, for what?
- Responsibility: Who covers necessary disaster recovery functions
- Procedures for Disaster Recovery
- Procedures for Alternate Mode operation
 - Resource Allocation: During recovery & continued operation

Copies of the plan should be off-site



What are the concerns of BCP/DR plan your? Evacuation plan should be very clearly spelled out. Peoples live always take the first priority, even when you say people process technology we mention people first not technology process people or process people technology. So, peoples life is of the of most important value to any organization or work. Disaster declare declaration, who will declare a disaster? How will it be declared and for what purpose it will be declared?

Meaning there should be a definition of certain criteria under which a disaster can be declared. Then the responsibility, who covers necessary disaster recovery functions? Who has the responsibility to DO what? For example, who will contact law enforcement? Who will contact the media? Who will declare a disaster? What is the role of the IT during a disaster? Who takes care of the evacuating people or ensuring that people are safe?

Then what are the procedures of disaster recovery? Once it is declared, how do you bring back or how do you resume normal operation? How an alternate mode operation. So it has to be clearly laid down. in terms of resource and location. So, in the recovery site how many staff will you need? What are the systems that are required? How long will you continue? So, that needs to be clearly spelled out. And the copy of the BCP/DR should be available offsite also.

In the event that they are not able to access ((Refer Time: 02:00)). For example, of fire across everything is lost then, what you do with the BCP/DR which is good? So, you need to have a copy of that on the offsite also.

(Refer Slide Time: 02:12)

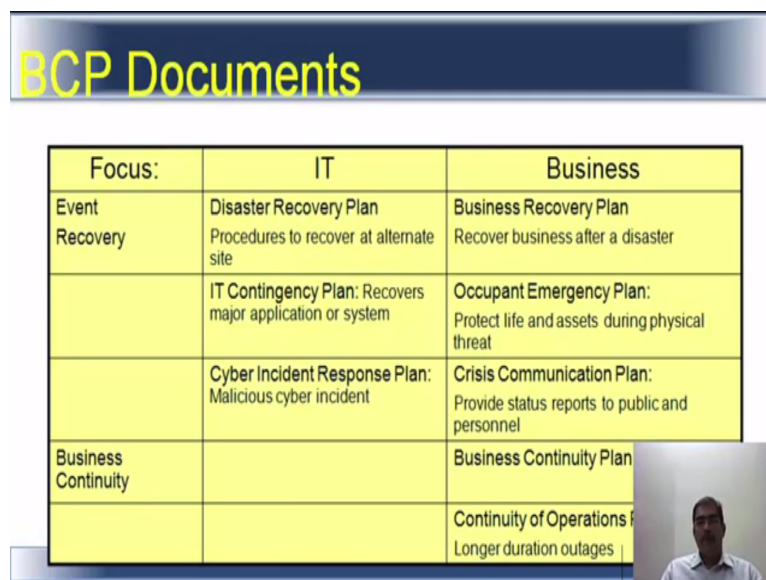


We spoke about responsibilities, disaster recovery responsibilities. Let us take a look at this general business. So, when you take the business in general, then the first responder is responsible for what evacuation, fire, and health of employee. Then there is damage assessment. Now, these need not be different people it would be responsibilities allocated to different people doing different functions.

Then there is emergency management, legal affairs, usually people involved with the law. However there is legal department within the organization they will do it. Then transportation and relocation, coordination. So, this is transportation of people, transportation of equipment, all those things happen. Then supplies emergency supplies not only organization supplies, even suit maybe a factor here. Then how do you salvage what all is lost?

Training who will train employees to act when a disaster occurs. So, mock DR test should be done. Who is in charge of the training? Who accesses the effectiveness of training? What frequency is the training conducted? So, all this is very important. Then in IT specific functions we have software, what softwares are required? What version? What build? How many packets are in group? The application what applications are required, then in emergency operations, what actually who will draw it as a service. Then the recovery of the network itself, the hardware, the data base or entries. Then the information the security, now in all these the contact information is very important. People should know whom to contact when and how in the event if some incident occur.

(Refer Slide Time: 04:00)



Focus:	IT	Business
Event Recovery	Disaster Recovery Plan Procedures to recover at alternate site	Business Recovery Plan Recover business after a disaster
	IT Contingency Plan: Recovers major application or system	Occupant Emergency Plan: Protect life and assets during physical threat
	Cyber Incident Response Plan: Malicious cyber incident	Crisis Communication Plan: Provide status reports to public and personnel
Business Continuity		Business Continuity Plan
		Continuity of Operations Plan Longer duration outages

What are the document for BCP? Now, if you look at the table it says it has three columns. One is the focus, focus is the IT and business. Let us take an example of event recovery. So, under IT there is a disaster recovery plan, what it specifies, procedures to recover at alternate site. Under business we have a business recovery plan or business resumption plan. That is how to recover a business after a disaster. These are spread out, then there is IT contingency plan. It recovers major application or system. So, contingency plan is a very important asset under your business continuity plan.

Then when it comes under the head of business, it is occupant emergency plan. That is protection of life and assets during physical threat. Then cyber incident response plan, if there is a malicious cyber attack or incident what is to be done. Under business it is crisis

communication plan. That is to provide a status report to public and the insiders or the personnel. Business continuity you will have a business continuity plan which would specify continuity of operations plan. And what happens during longer duration of outages. All this have to be mandatorily kept by an organization.

(Refer Slide Time: 05:48)

Business Continuity Overview

Criticality Class (Critical or Vital)	Business Process	Incident or Problematic Event(s)	Procedure for Handling
Vital	Registration	Computer Failure	DB Backup Procedure DB Recovery Procedure - Registration Mobile Site Plan
Critical	Teaching	Computer Failure	DB Backup Procedure DB Recovery Procedure - Teaching Section Mobile Site Plan

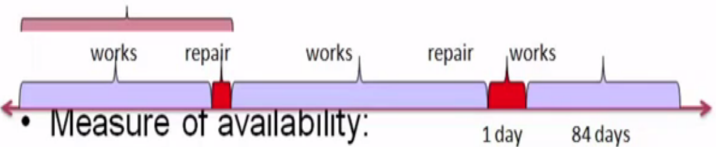
Looking back at the same example of the university, we can classify let us say the critically class critical or vital. What are the business process affected? What is the incident or problematic events and what is the procedure for handling? If the criticality is vital, the business process is registration. A computer failure can be classified as the incident or problematic event. The procedure for handling these things are data base backup procedure , proper database backup should be taken. Database recovery procedure should be there for registration, there could also be a mobile site plan. If it is critical in nature, it affects the teaching faculty.

The incident or problematic event could be a computer failure. Again the procedure for handling here is the database backup procedure, database recovery procedure for the teaching asset then the mobile site plan. So, this is just an overview or an example of how the BCP overview looks like.


(Refer Slide Time: 07:10)

MTBF = MTTF + MTTR

- Mean Time to Repair (MTTR)
- Mean Time Between Failure (MTBF)



- Measure of availability:
- 5 9s = 99.999% of time working = 5 ½ minutes of failure per year.




Then you have something called MTBF, which is mean time between failure and MTTR is mean time to repair. So, basically it is a measure of availability. Now, 5 9s 99.999 percent of time, is five and a half hours of downtime minutes of failure per year. So, if you say you are going to provide an uptime of 99.999 or 5 9s that means you can afford only 5 and a half minutes of failure per year. So, that is a very high objective to attain. MTTF is mean time to failure.

(Refer Slide Time: 07:59)

Disaster Recovery Test Execution

Always tested in this order:

- Desk-Based Evaluation/Paper Test:** A group steps through a paper procedure and mentally performs each step.
- Preparedness Test:** Part of the full test is performed. Different parts are tested regularly.
- Full Operational Test:** Simulation of a full disaster



Now, a disaster recovery test execution is always tested in the order what is given in the slide. It is a test based evaluation or paper test, a group steps through a paper procedure and mentally performs each step. Then the second one is preparedness test. Now, it is a part of full test which is performed and different parts are tested regularly. And a full operational test which is simulation of full disaster. So, mock tests are conducted in a lot of your IT parks this mock disaster recovery is conducted on half yearly basis by the people who are manage the facilities, just to ensure preparedness of the different organizations who work out in that building and to ensure that people are aware what to do when a disaster occurs. What are the test types of business continuity tests?


(Refer Slide Time: 08:59)



Business Continuity Test Types

- Checklist Review:** Reviews coverage of plan – are all important concerns covered?
- Structured Walkthrough:** Reviews all aspects of plan, often walking through different scenarios
- Simulation Test:** Execute plan based upon a specific scenario, without alternate site
- Parallel Test:** Bring up alternate off-site facility, without bringing down regular site
- Full-Interruption:** Move processing from regular site to alternate site.

08:59

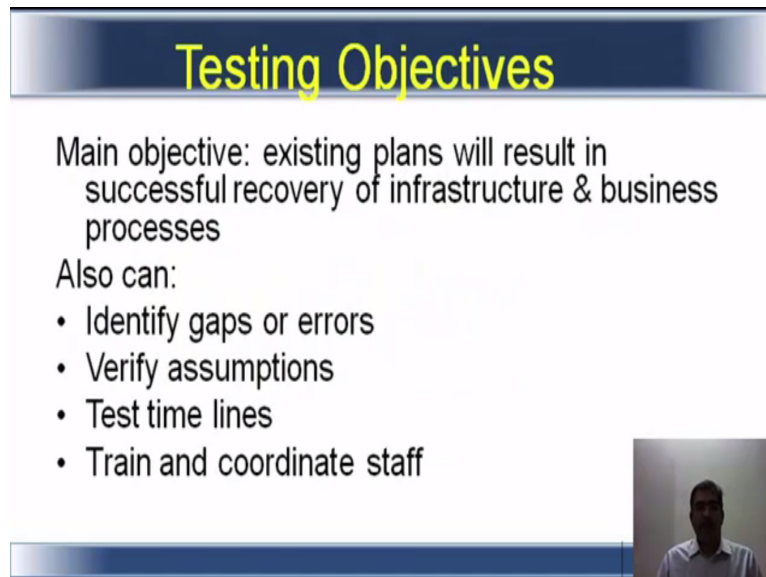


Always checklist review, it reviews the coverage of plan are all important concerns covered, that is what give the checklist cover. Structured walkthrough, review all aspects of the plan. Often walking through different scenarios. So, if a plan is made what happens if x incident happen, what happens if y happens. So, the structured walkthrough is conducted. The third is a stimulation test that is execute plan based on a specific scenario without alternate site. So, you actually stimulate the test and execute or invoke the plan and see what the results are.

Parallel test, bring up alternate off site facility without bringing down regular site. See how the transition happens, whether it is moved at the same time you are not disturbing the normal operations. Full interruption, move processing from regular to alternate site. So, a lot banks have this full interruption test. They identify a particular day in a year or in once in half year.

They shut down the server, they bring up the disaster survey site. They test what happens how much time it takes to recover, what services are disturbed during that time, whether it is a partial failure or full failure. So, many things are tested in the full interruption test.

(Refer Slide Time: 10:41)



Testing Objectives

Main objective: existing plans will result in successful recovery of infrastructure & business processes

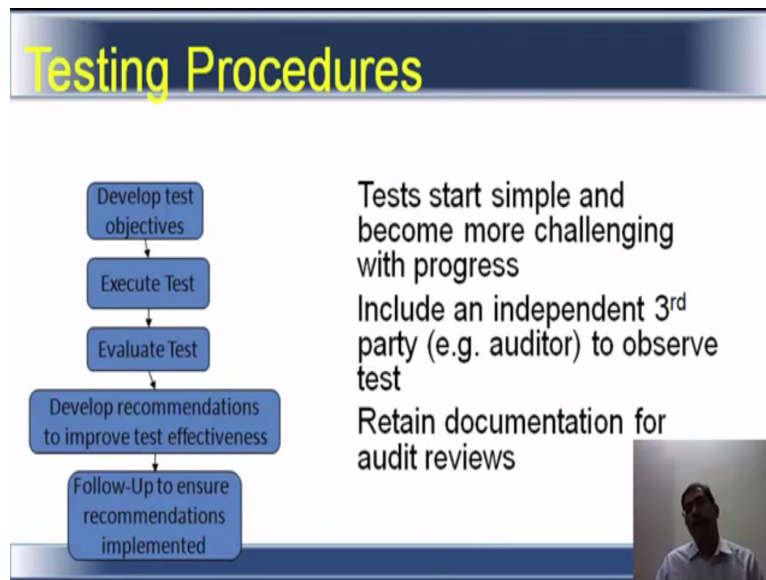
Also can:

- Identify gaps or errors
- Verify assumptions
- Test time lines
- Train and coordinate staff

What are the objectives of testing? The main objective is existing plans will result in successful recovery of infrastructure and business processes. For the objective of testing will help you determine whether the recovery is successful of infrastructure and business processes. It can also identify gaps or errors. So, if there are errors in the process or of there are gaps in the recovery times or in the process itself. You will come to know, then you verify assumptions.

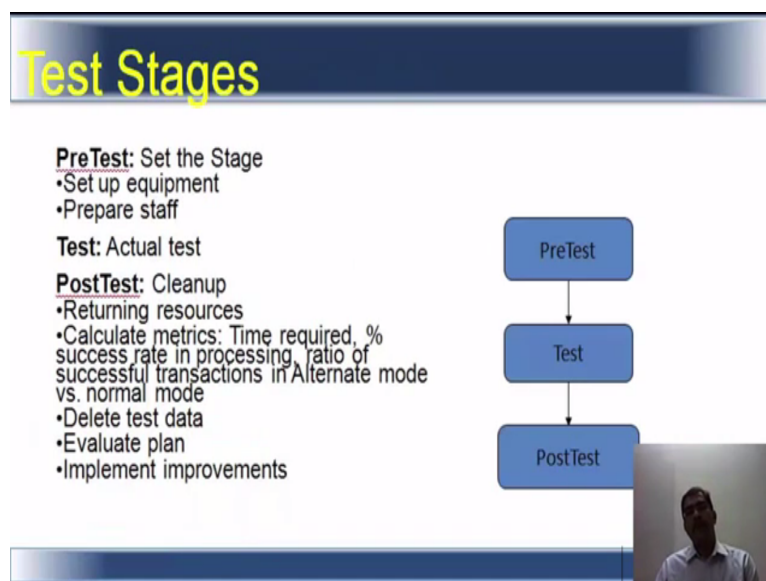
So, the person after detailed discussion assumption is made and the plan is written in such a way. So, you will come to know if the assumptions were made right or wrong. Then test time lines now you have mentioned a rpo of 4 minutes, rto of another 2 hours. For example, so you actually get to test the time lines whether it falls within that range, then you also get to train and co-ordinate staff.

(Refer Slide Time: 11:50)



So, during testing procedures your test starts in a simple way and becomes more challenging with progress. It is always better to include the independent third party to observe the test. It could be an auditor your information security auditor and retain the document for documentation review, for audit reviews. Now, the testing procedure first to develop the test objective. You execute the test, you evaluate the results of the test. You develop recommendations to improve the test effectiveness and then you follow up to ensure that the recommendations are implemented.

(Refer Slide Time: 12:34)



What are the stages of the test? There is a pre test a test and a post test. So, pre test is set the stage. In that you set up the equipment you prepare the staff for the test. Then the test phase is the actual test that you perform and the post test is you clean up return resources calculate metrics, time required then successful percentage rate in processing. Ratio of successful transactions in alternate mode versus normal mode. Then you delete the test plan or test data, evaluate the plan again implement improvements to the plan.

(Refer Slide Time: 13:17)

Gap Analysis

- Comparing Current Level with Desired Level
- Which processes need to be improved?
- Where is staff or equipment lacking?
- Where does additional coordination need to occur?




If there are variations you will have a gap analysis also done. So, you compare the current level with the desired level, which processes need to be improved, where is the staff or equipment lacking, what or where does additional coordination need to occur. All this will help to determine the improvements in the test process itself.

(Refer Slide Time: 13:42)

Insurance

IPF & Equipment	Data & Media	Employee Damage
Business Interruption: Loss of profit due to IS interruption	Valuable Papers & Records: Covers cash value of lost/damaged paper & records	Fidelity Coverage: Loss from dishonest employees
Extra Expense: Extra cost of operation following IPF damage	Media Reconstruction Cost of reproduction of media	Errors & Omissions: Liability for error resulting in loss to client
IS Equipment & Facilities: Loss of IPF & equipment due to damage	Media Transportation Loss of data during xport	

IPF = Information Processing Facility



Insurance is transfer of risks to a insurance company. Now, info IPF is information processing facility and equipment. Then there is data and media, then employee damage. There maybe insurance for data and media in other countries I am not so sure whether it is implemented in India itself because you need to arrive at the value of data before you can quantify that this is my value of the data.

So, if you look at this IPF and equipment business interruption, loss of profit due to information systems interruption, extra expense. Extra cost of operation following information processing facility damage. IS equipment and facilities loss of information processing facility and equipment due to damage. Then under data and media valuable papers and records are lost it covers the cash value of lost or damaged paper and record, but you need to actually assign a value and the insurance company has to accept the value.


Then the media reconstruction, cost of reproduction of media. Then loss of data during media transport, there will be an insurance for that. Fidelity coverage that is caused by employee damage loss from dishonest employees, errors and omissions, liability for error resulting in loss to a client. So, there had have been several incidents of errors and omissions. Few years back to be sure, HSBC had an incident, there have been similar incidents being reported in the newspapers often.

(Refer Slide Time: 15.31)

Auditing BCP

Includes:

- Is BIA complete with RPO/RTO defined for all services?
- Is the BCP in-line with business goals, effective, and current?
- Is it clear who does what in the BCP and DRP?
- Is everyone trained, competent, and happy with their jobs?
- Is the DRP detailed, maintained, and tested?
- Is the BCP and DRP consistent in their recovery coverage?
- Are people listed in the BCP/phone tree current and do they have a copy of BC manual?
- Are the backup/recovery procedures being followed?
- Does the hot site have correct copies of all software?
- Is the backup site maintained to expectations, and are the expectations effective?
- Was the DRP test documented well, and was the DRP updated?



Just like any other audit we need to audit BCP also. What is included in the BCP audit. Now, some of the broad categories are given here. A comprehensive checklist can be made after determining what exactly the organization is doing with disaster recovery and disaster recovery and business continuity plan? What kind of documentation they have? It can be interview observation, review of documentation. Observing a mock drill that happens and pointing out the common or pointing out the mistakes or areas of improvement.

Now, auditing BCP improves, is the business impact analysis complete with the recovery point objective and recovery time objective defined for all services or it is just for one or two services. So, for all services which are critical or non critical there should be a BIA. It should be complete; is the BCP in line with business goals is it effective and is it current. So, the BCP should be made in line with the business goals, it should not be a simple cut and paste from some another organization where you may not be having the same kind of infrastructure..

Then is it clear who does what in the BCP and DRP? For roles and responsibilities of people during a BCP not during an incident, whether it is clear, so you can interview them you can actually review the document. Whether the document is updated the document may have Mr. X but, when you actually interview it will be Mr. Y who is coming in place of Mr. X. So, you need to be clear who does what in a BCP/ DRP. Then is everyone trained competent and happy with their jobs, which is very important.

Otherwise in the event of any incident mera kya hua, I am going. So, that could be the attitude. Is the DRP detailed, is it maintained, is it tested on regular basis that should be audited. Is the BCP and DRP consistent in their recovery coverage? Now, BCP is a bigger document larger document DRP is a portion of that, both have to be consistent and complementary to each other.

Are people listed in the BCP or phone tree current and do they have a copy of business continuity manual? So, we have specified in some responsibility for different people in the organization, like I said a couple of minutes ago Mr. X was there now it is Mr. Y. So, does Mr. Y, has the copy of BCP and does he knows he or she knows what to do. Are the backup and recovery procedures being followed. So, that has to be audited, whether a grandfather, father or son started ((Refer Slide Time: 18:36)) or what is the frequency of backups, how it is made ((Refer Slide Time: 18:41)).

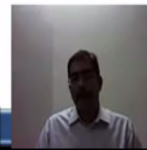
Does the hot site have current topics of all software. So, here it should be software and documentation. So, whether the hot site has the correct copies of all softwares and the documentation. Is the backup site maintained to expectations and are the expectations effective? Now we should not be a dumb. So, the backup facilities also should have simpler infrastructure as the main processing facility. And are the expectations effective that means can they really recover in case a disaster occurs. .

Was the DRP test documented well and was the DRP updated. Again the DRP was made two years back since then the organization has replaced their servers, they have replaced or upgraded their software. Whether that reflects in the updated DRP document. All those things have to be done during the audit of BCP, these are generic things. So, you need to go in detail formulate your own checklist or try to understand the business processes and what the IT is doing. And then conduct the audit of the BCP process itself in the organization.

(Refer Slide Time: 20:05)

Summary of BC Security Controls

- RAID
- Backups: Incremental backup, differential backup
- Networks: Diverse routing, alternative routing
- Alternative Site: Hot site, warm site, cold site, reciprocal agreement, mobile site
- Testing: checklist, structured walkthrough, simulation, parallel, full interruption
- Insurance



We have looked at RAID, we have looked at backups which is incremental backup differential backup. We have looked at networks, diverse routing and alternate routing. Then, alternative site for processing like the hot site, warm site, cold site, reciprocal agreement, mobile site. Testing of BCP/ DRP using checklist, structured walkthrough, simulation and parallel full interruption test. Finally, the insurance aspect.