BCP Audit Areas

Item Topic

1. Underlying assumptions:
   a. Is knowledge assumed, or is it available in a disaster?
   b. Is it assumed that something will be simple when, in fact, it is complicated and difficult?
   c. Has a counterparty (participant in the contract) committed to delivering what you are expecting?
   d. Have you created an effective reporting and communications structure in place that will ensure that everybody concerned knows what is happening and when it is happening, and knows immediately that something that should happen, hasn't happened? It's all too easy to assume others know what you are doing – but they won't know unless they are told.
   e. Is the basis of planning sufficiently broad to cope with different types of disaster and different causes?
2. The sequence of restoration for critical functions, operations, applications systems and services and dependencies provided by and to them. Does the sequence reflect dependencies and priorities?
3. Defined function and application priorities and processing and resource requirements of the operational departments. Are all mission-critical activities covered?
4. Incident management, escalation processes, BCP invocation, BC organization and management of the recovery effort.
5. Any unique equipment or services (including arrangements for safety of valuable works of art or items of cultural heritage) which should be addressed separately in the plan.
6. Identification of vital records and materials, existing backup and retention requirements including archive material, and retention, rotation, or retrieval procedures.
7. BCP notification procedures. Does call-out work?
8. Adequacy and accessibility of items stored offsite for continuity purposes. Is everything that is necessary for recovery kept offsite? Can all items be retrieved to enable recovery within the RTO and RPO? Is the offsite store in the same risk area as the main site?
9. BC procedures for move to an alternate operating site and to conduct operations there, including security and access requirements.
10. Existing procedures, manuals, etc. for critical operations identified in the BCP.
11 Location of standby site(s). Are they in the same risk area as the main site? Are they accessible? Can they be commissioned and operational in time to meet RTO and RPO?
12. Alternate (internal) site support agreements, procedures, etc.
13. Alternate site (hot site/cold site) support agreements, procedures, contracts, etc.
14. Alternate services support agreements, procedures, specifications, and contracts.
15. Considerations for production equipment, hardware, software, and data to support the recovery effort.
16. Documentation of existing configuration and procedures.
17. Documentation of configurations and procedures for the alternate site.
18. Insurance policies or summaries, claim procedures, etc.
19. Relationship of BCPs to existing (normal) contracts with customers and suppliers, contracts, and service level agreements.

20. Consistency within and between plans and consideration of their impact on group, sister companies, brands, stakeholders, and interested parties.
21. Reflection in each BCP of the requirements upon it made in other BCPs.
22. Audit trail of actions and identification of costs of disaster and recovery.
23. Procedures for updating and reviewing the BCP.
24. BCP exercising and testing procedures.

10.2 Testing, Exercising – What's the Difference?

Testing implies pass or fail. Exercise implies getting fit, practicing, rehearsing, and improving. Both are necessary to prove a BCP is effective.

Testing

A test is usually a physical activity to prove something – that a generator, for instance, works. Testing is usually non-disruptive – although if you switch live operations to standby equipment to test that failover works, it could be disruptive – especially if it doesn't! The word "test" has overtones of passing or failing, of testing to destruction.

Avoid damaging confidence in the BC project by giving the impression that an exercise is a pass or fail test – the exercise is a learning and training experience in which you can expect to find things do not always go as smoothly as expected.

Exercising

A BCP exercise should:

- Stress the BCP under different scenarios.
- Determine the actual availability of underlying resources.
- Train BC team members and give them experience in working under emergency conditions.
- Identify areas of weakness in the BC organization, BC assumptions, strategies, plans, appropriateness of team members, and allocation of resources and logistics.
- Identify ways to improve the BCP.

In practice, the words "test" and "exercise" are used interchangeably, but you should be aware of the difference in the two activities and do both. However, a BC test should always result in identifying ways in which you can improve the plan. That is why we prefer to use the word "exercise," which implies getting fit or "rehearsal," which implies practicing until perfect.

To avoid confusion, we use the terminology of ISO 22301 in describing the different types of exercise (see Appendix B).

10.3 The Need to Exercise

If we have not tested something, how do we know it works? Obviously, the armed forces do not sit around waiting for a war – they train, exercise, simulate, and practice. Police departments, fire departments, and ambulance services all undergo rigorous, realistic training to hone their skills and to perfect contingency plans. They know that unless they continue to practice their skills and test their plans, they will fail when faced with a real crisis.

According to the UK Chartered Management Institute,[4] fewer than half of all organizations with a plan (48%) test them on an annual basis and, worryingly, where shortcomings are identified, 9% of organizations still fail to take action to remedy them. Of the tests undertaken, 73% were simple table-top exercises, while 44% just covered IT disaster recovery. Only 22% were full emergency scenarios. Thus, the majority of companies with BCPs have no coherent testing strategy.

A Kroll Ontrack survey showed that only 33% of these organizations using cloud and virtualization test data recovery plans regularly to ensure their data is properly protected.[5] InformationWeek's 2013 State of Storage survey reveals that, of the 80% or organizations with DRPs, only 40% test their DRP regularly.[6]

Lack of testing and exercising can result in an unrealistic degree of confidence in all of the components of a business continuity plan and in its overall effectiveness. Many simply test the same thing (often with the same people) over and over again, while omitting to test crucial logistics, supply chain, pandemic, or support elements. Yet, alarmingly, 45% of organizations with BCPs have invoked them in an actual event.[7]

However, the good news is that finding flaws means that your test or exercise has been successful. If you find the faults in test or exercise conditions, you can put them right so they do not occur when your plan is put into action for real. A test, then, is not an activity designed spitefully to catch out the planner, but a structured learning and training exercise to improve the plan and the capacity of its teams to respond effectively.

Failure to test and exercise can mean failure on real invocation. Philip Jan Rothstein, FBCI, President of Rothstein Associates Inc., emphasizes "an unexercised contingency plan could be more dangerous than no plan at all!"

Why do so few organizations exercise their plans? Could it be excessive faith in the software-planning tool used to create the plan? While good BC software provides a sound structure and effective documentation, it can never guarantee that the underlying assumptions are correct, that the personnel involved can perform their tasks, or that the information it contains is valid and up-to-date.

Could it be unquestioned faith in the consultant or staff members who helped produce the plan? A good consultant will apply relevant experience to speed plan development; however, unless the plan is tested, how do you know the consultant did a good job? And what happens after the consultant leaves? Six months later, perhaps staff changes, organization structures change, accommodation moves take place, equipment changes, technology improves, or business priorities change.

> **While exercising is important, it is not worthwhile putting the business at risk from the test.**

10.4 When Should You Test or Exercise?

You should run tests or exercises on completion of:

- Each draft plan.
- Complementary plan(s).
- A suite of plans.
- Major revisions to the plan.

You should run tests or exercises regularly (at least once a year, preferably more often):

- To train BCP teams.
- To ensure plans reflect lessons from previous audits, reviews, tests, and exercises.