

IT Handbook Presentation Business Continuity Planning Booklet

Visual

Narrative

1. **IT Handbook Presentations**
**Business Continuity
Planning Overview**



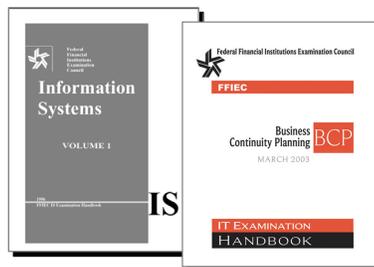
2. **Presentation Topics**

- Replacement of existing Chapter 10
- Evolution of BCP
- Booklet organization
- BCP workprogram

As an introduction to the Business Continuity Planning, or BCP, Booklet, this presentation will discuss four topics:

- How the new BCP Booklet replaces the existing Chapter 10 of the 1996 IS Examination Manual entitled *Corporate Contingency Planning*,
- How the BCP concept has changed in recent years,
- How the BCP booklet is organized, and
- The BCP workprogram.

3. **Business Continuity Planning**



This new BCP Booklet replaces the existing Chapter 10 of the 1996 IS Examination Manual. The Booklet will provide helpful guidance to examiners and financial institutions on a topic that has changed substantially in recent years.

4. **Business Continuity Planning**

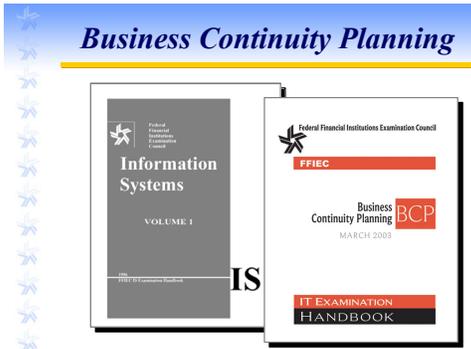


As in many of the other IT booklet topics, BCP has grown in both significance within the industry and in the volume of issues and technical information that is now considered associated with effective business continuity planning.

Visual

Narrative

5.



Consequently, you will find that the BCP Booklet has over three times the volume of information than the same topic provided in the 1996 handbook. The new version provides much more detail on many more topics.

6.



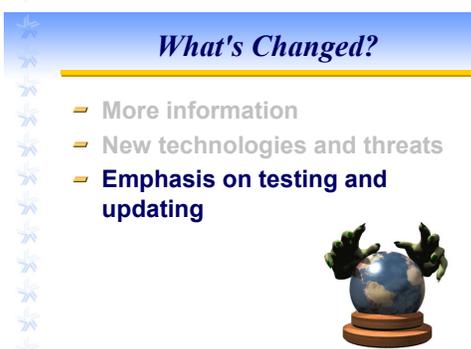
The years since the 1996 Handbook have shown a wide-range of increases in both the threats to business operations and in new technologies, which can help a financial institution keep operating in spite of an unplanned event.

7.



While the most obvious new threat is terrorism, an increase in institutional dependence on critical infrastructures such as telecommunications and third-party providers, has also dramatically increased the complexity of BCP.

8.



In addition, the new Booklet places more emphasis on testing and updating business continuity plans than was the case in 1996.

One important lesson learned over the past few years is that no one can predict everything that is going to happen. If a business continuity plan is to hold up in these "unpredictable" situations, it must be flexible, allowing for some measure of adaptability to adversities that actually occur.

Visual

Narrative

9.

What's Changed?

- More information
- New technologies and threats
- Emphasis on testing and updating
- **Focus on business resumption**

There's also a new focus on the business resumption aspect of BCP. The industry has come to realize that merely backing up data is not enough.

10.

Business Resumption



Recovered data does not necessarily guarantee that an institution can be ready to serve its customers again in a timely manner. For example, backup data may be of no use if the institution is without the electricity, facilities, or personnel it needs to operate.

11.

Contemporary BPC

- Maintaining
- Resuming
- Recovering



This point leads to perhaps the most pervasive difference between business continuity planning now and how it was treated in 1996 Handbook.

Business continuity planning is no longer about just recovering technology. It's about maintaining, resuming, and recovering the business.

12.

Business Resumption

- Possible new...
 - Location
 - Computers
 - Data connections

PLUS...

- Staff

In order to accomplish these goals, an institution may have to get its data to a new location, load it onto new computers, establish new communication links, and have the staff available to make it all work again.

If any one of those pieces is missing, the institution may fail to achieve its business resumption goals.

Visual

Narrative

13.

What's Changed?

- More information
- New technologies and threats
- Emphasis on testing and updating
- Focus on business resumption
- Requirement for enterprise-wide planning

If all of these pieces need to be in place for effective and timely business resumption, it follows that the business continuity plan must be developed on an enterprise-wide basis. The IT staff cannot accomplish effective BCP in isolation. Effective BCP requires involvement by all aspects of the business.

14.

All of Operations

Technical

Business Units

Human Resources

Facilities

Customer Service



Those perspectives include not only technical personnel but also those of business units, human resources, facilities, and customer service—literally every aspect of the institution's operations. An automatic red flag should go up in examinations that reveal BCP to be the sole responsibility of a systems administrator.

15.

Comprehensive BCP Thinking



- System development
- Employee training
- Security
- Media relations

The wide range of departments involved in BCP also demonstrates the pervasive nature of BCP issues. Consequently, institutions should also consider BCP implications when developing other types of business process plans, such as:

- System development,
- Employee training,
- Security, and
- Media relations.

16.

Recovery Time Objectives



The same complexity that requires enterprise-wide BCP has also changed what are now considered to be acceptable recovery-time objectives, or the period of time that a process can be inoperable. At one time, an institution could be down for 24 or 48 hours without sustaining significant loss, but that length of time has grown shorter and shorter.

Visual

Narrative

17.

Shorter Recovery Times



Recovery time is now measured in hours, and, in certain time-sensitive situations, even in minutes. As the recovery-time objectives become shorter, the difficulty of effective BCP and the associated costs increase.

18.

Organizations Vary



Of course, as with most aspects of BCP, the appropriate recovery-time objectives for a given organization will vary, depending on the complexity and volume of its business activities.

19.

Interdependency



Another emerging issue in business continuity planning is interdependency; a term used frequently throughout the BCP booklet.

20.

Technology Dependent



As financial institutions have become more and more dependent on technology, they've also become increasingly dependent on organizations outside of the financial world.

Visual

Narrative

21.

Interdependency



Telecommunications, for example, is now critical to the successful completion of financial transactions of all types.

22.

Increasing Specialization



With this increasing dependency, it becomes imperative for an institution to consider all of the outside resources upon which it is dependent, as it develops its business continuity plan.

23.

Potential Loss of Access



Also a sign of the times is the possibility that an institution may lose access to one or more facilities, as a result of a disaster affecting a wide geographical area.

24.

Importance of HR



Even with backup tapes and access to a satisfactory backup facility with all of the necessary equipment, what about the people?

Visual

Narrative

25.

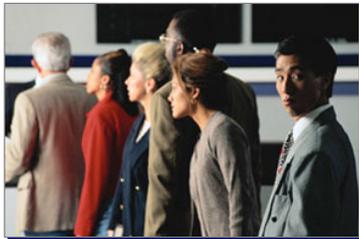
Importance of HR



- How are they going to get to the backup site?
- How long will they have to stay?
- Who is going?
- Where will they stay?
- Where will they eat?
- What about the customer service and the call center staff?
- How do the business units and customer service representatives get access to the information they need to keep functioning?

26.

New Perspectives



With the increasing realization of HR's importance to BCP, as with all of the changes we've discussed, there's one underlying theme. Some of the old assumptions made in the course of BCP are no longer reliable.

27.

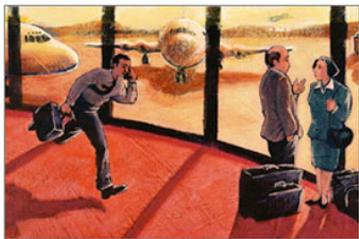
Old Assumptions



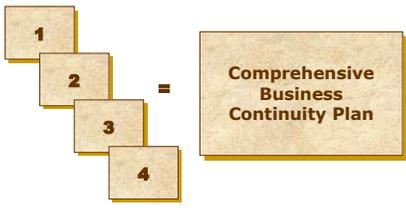
For example, in the past a business could safely assume that, if the main office was in New York and the backup was in Chicago, the staff would just fly to the backup location in the event of an unplanned disruption.

28.

New Perspectives



No one ever planned for all airlines being grounded—but it happened.

	Visual	Narrative
29.	<div style="border: 1px solid blue; background-color: #e6f2ff; padding: 5px; margin-bottom: 5px;"> <p style="text-align: center;"><i>Presentation Topics</i></p> <hr style="border: 1px solid yellow;"/> <ul style="list-style-type: none"> - Evolution of BCP - Booklet organization </div>	<p>Now that you have a general perspective on how BCP has evolved since 1996, let's take a look at how the booklet is organized.</p>
30.	<div style="border: 1px solid blue; background-color: #e6f2ff; padding: 5px; margin-bottom: 5px;"> <p style="text-align: center;"><i>Booklet Organization</i></p> <hr style="border: 1px solid yellow;"/> <ul style="list-style-type: none"> - Body - Appendices </div>	<p>There are two main parts to the BCP Booklet—the main body and the appendices.</p>
31.	<div style="border: 1px solid blue; background-color: #e6f2ff; padding: 5px; margin-bottom: 5px;"> <p style="text-align: center;"><i>Booklet Organization</i></p> <hr style="border: 1px solid yellow;"/> <ul style="list-style-type: none"> - Body <ul style="list-style-type: none"> - Business impact analysis - Risk assessment - Risk management - Risk monitoring - Appendices </div>	<p>The main body is organized to correspond with the four industry-recognized steps required for sound business continuity planning:</p> <ul style="list-style-type: none"> ▪ Business Impact Analysis, ▪ Risk Assessment, ▪ Risk Management, and ▪ Risk Monitoring.
32.	<div style="border: 1px solid blue; background-color: #e6f2ff; padding: 5px; margin-bottom: 5px;"> <p style="text-align: center;"><i>Process</i></p> <hr style="border: 1px solid yellow;"/>  </div>	<p>These four steps are sequential in nature, building on one another to form a comprehensive business continuity plan that meets the needs of the individual institution.</p>

Visual

Narrative

33.

Process

- Business impact analysis
- Risk assessment
- Risk management
- Risk monitoring

Throughout the booklet, it is this process that is emphasized, and it is the process that will be critical in your examination. Let's take a look at the four steps the booklet covers, one step at a time.

34.

Business Impact Analysis



- Threats
- Impacts

Step one is to determine possible threats to the institution's business continuity. Although there are lists of possible threats and threat tips available from many competent sources, the critical issue is that each institution identifies possible threats and possible impacts for its unique situation.

35.

Risk Assessment



Once identified, the potential threats and possible impact on the institution's business should be prioritized through a comprehensive risk assessment.

36.

Risk Assessment Matrix

	Severity			
Likelihood				

This is done effectively by developing a matrix of the threats that were identified in step one. One side of the matrix assigning the likelihood that a particular threat might occur and the other side indicating the severity of the results to the institution's business if, in fact, the threat does occur.

Visual

Narrative

37.

Risk Assessment Priorities

- ? Sabotage
- ? Theft
- ? Equipment Failure
- ? Flood
- ? Power Failure
- ? Terrorism
- ? Fire

Established priorities will vary by institution, depending on its geography, facilities, size, business interests, and so forth.

38.

Risk Assessment Priorities



Once again, it is the responsibility of the examiner to assess the appropriateness of the priorities established for the institution being examined.

39.

Risk Management



After prioritizing potential threats and possible impacts, the institution is ready to start developing its BCP. The plan should not only be written, but also disseminated to all key personnel.

40.

Risk Management

- **Business continuity plan:**
 - Specific
 - Flexible
 - Focused
 - Effective

The plan should be:

- Specific in when and how it is to be implemented;
- Flexible, to allow for unanticipated threat scenarios and changes in the business;
- Focused on getting the business back up and running, rather than on the precise nature of the disruption; and
- Effective in minimizing service disruptions and financial loss.

Visual

Narrative

41.

Risk Monitoring

- Business impact analysis (BIA)
- Risk assessment
- Risk management
- **Risk monitoring**



The final step in the process is risk monitoring. Because of constant changes in technology, society, personnel, and even the nature of the business itself, BCP must be a dynamic process to remain effective.

42.

Tested and Revised



The plan should be tested at least once a year, and revised based on changes to the internal and external environment in which the institution is operating.

43.

Tested and Revised



As with other areas critical to financial institutions, BCP testing should include independent audits and reviews.

44.

Booklet Organization

- **Body**
- **Appendices**
 - A: BCP Workprogram
 - B: Glossary
 - C: Internal & External Threats
 - D: Interdependencies
 - E: BCP Components

Consistent with other IT booklets, the BCP Booklet also has workprogram and glossary appendices. In addition the BCP Booklet provides three other appendices, which are designed to provide specific information of a more technical and detailed nature than is covered in the main body of the booklet. These three appendices can serve as important tools for those individuals actually responsible for various aspects of their institution's BCP.

Visual

Narrative

45.

Auxiliary Appendixes

These tools include:

- Appendix C: Internal and External Threats,



- Internal and external threats

46.

Auxiliary Appendixes

- Appendix D: Interdependencies, and



- Internal and external threats
- Interdependencies

47.

Auxiliary Appendixes

- Appendix E: BCP Components.



- Internal and external threats
- Interdependencies
- BCP components

48.

Internal and External Threats

Internal and External Threats provides users with an in-depth look at potential disasters and can be extremely helpful to those individuals actually working on business impact analyses or risk assessments.



Visual

Narrative

49.

Internal and External Threats

- Malicious activities
- Natural disasters
- Technical disasters

The appendix discusses potential disasters such as:

- Malicious activities, from blackmail to terrorism,
- Natural disasters, from fire to floods, and
- Technical disasters, such as power or equipment failure.

50.

Internal and External Threats



One value of using this appendix is that it helps those responsible for identifying potential threats to keep in mind both internal and external sources. Important because it is frequently the case that people concentrate on external threats such as mother nature, while underestimating the critical nature of potential internal threats such as sabotage by disgruntled employees.

51.

Interdependencies

- Telecommunications infrastructure
- Third party providers
- Key suppliers
- Business partners

Appendix D looks at crucial interdependencies between financial institutions and:

- Telecommunications infrastructure,
- Third party service providers,
- Key suppliers, and
- Business partners.

52.

Importance of Interdependence



After the events of September 11, 2001, it became apparent just how dependent financial institutions are on telecommunications links. Again, old assumptions did not hold up.

Visual

Narrative

53.

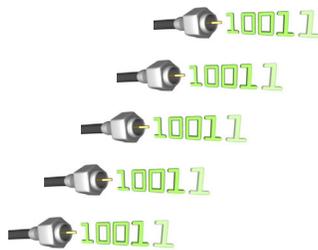
Importance of Interdependence



Institutions had planned for telecommunications failures by contracting with backup service providers.

54.

Multiple Providers



However, many businesses soon learned that their backup providers were ineffective because they used the same cables and/or junction boxes to transmit voice or data as the primary providers.

55.

Telecommunications Failures



Because many telecommunication providers lease lines from the same source, or in some cases from each other, simply having a backup provider may not be sufficient.

56.

Telecommunications Failures



The lesson? Institutions need to look for alternate communication paths when developing a BCP, not simply for alternate service providers.

Visual**Narrative**

57.

Finding Alternatives

Unfortunately, the only way to accomplish this is to sit down with various providers and actually map out the communication paths that the various providers use.

However, in some institutions, this very labor-intensive and expensive process may prove to be a wise investment.

58.

BCP Components

- Data center recovery alternatives
- Backup recovery facilities
- Geographic diversity
- Backup and storage strategies
- Data file backup
- Software backup
- Offsite storage
- Site relocation
- Post disaster communication

The BCP components appendix provides information on current technologies that banks can use in business continuity planning. Resources and issues covered here include:

- Data center recovery alternatives (such as data mirroring),
- Backup recovery facilities,
- Geographic diversity,
- Backup and storage strategies,
- Data file backup,
- Software backup,
- Offsite storage,
- Site relocation,
- Post disaster communication (with emergency personnel, employees, directors, regulators, vendors, suppliers, customers, and the media), and
- Other considerations

59.

Presentation Topics

- Evolution of BCP
- Booklet organization
- **BCP workprogram**

Now, let's take a look at the BCP workprogram.

	Visual	Narrative
60.	<p><i>Workprogram - Organization</i></p> <ul style="list-style-type: none"> - Scope the exam - Review plan and management involvement - Review BCP process 	<p>The workprogram follows the process outlined for effective BCP. First, scoping the exam – for this institution, what should the focus of the exam be?</p> <p>The next step is to review the institution’s business continuity plan and determine the adequacy of management involvement.</p> <p>Finally, examiners review the institution's BCP process.</p>
61.	<p><i>BCP Process</i></p> <ul style="list-style-type: none"> - Business impact analysis - Risk assessment - Risk management - Risk monitoring 	<p>Just as it is outlined in the booklet, examiners should look at the:</p> <ul style="list-style-type: none"> ▪ Business impact analysis, ▪ Risk assessment, ▪ Risk management, and the ▪ Risk monitoring <p>to see if the institution went through the appropriate process. Did they ask the right questions to develop a plan that has a reasonable chance to assist the institution in becoming functional again, should a disaster strike? Are the BCP plan and the recovery time objectives appropriate for the given situation?</p>
62.	<p><i>Exam Organization</i></p> <ul style="list-style-type: none"> - Scope the exam - Review plan and management involvement - Review BCP process - Conclusions 	<p>The concluding section then provides for examiners to outline corrective actions, which may be required for improvement in the institution's BCP.</p>
63.	<p><i>Presentation Topics</i></p> <ul style="list-style-type: none"> - Evolution of BCP - Booklet organization - BCP workprogram 	<p>So, we've looked at the evolution of BCP and the organization of the booklet and workprogram. The BCP Booklet will be a valuable resource for examiners and others looking for guidance on how to effectively plan for business continuity in their respective organizations.</p>

Visual**Narrative**

64.

Booklet Goals

- **Sound guidance in planning for business continuity within individual organizations**
- **Effective business continuity plan to meet the specific needs of any given financial institution**

As you review the booklet itself, keep in mind that it was designed to provide sound guidance in planning for business continuity within individual organizations. Its purpose is not to dictate the details of a plan, such as the ideal distance between primary and backup processing sites. Rather, its purpose is to support the development of effective processes for establishing an effective business continuity plan to meet the specific needs of any given financial institution.

65.

Credits