बाह्य परिपत्र संख्या 89 /डॉस- 07 /2024 10 मई 2024

संदर्भ.सं.राबैं.प्रका.डॉस.पॉलिसी/ 657 /जे-1/2024-2025

अध्यक्ष, क्षेत्रीय ग्रामीण बैंक
प्रबंध निदेशक, सभी राज्य सहकारी बैंक
प्रबंध निदेशक/मुख्य कार्यकारी अधिकारी,
सभी जिला मध्यवर्ती सहकारी बैंक

महोदया/प्रिय महोदय,

**व्यवसाय निरंतरता योजना (बीसीपी) पर मार्गदर्शी नोट**

कृपया दिनांक 30 मार्च 2010 के हमारे पत्र संख्या राबैं.प्रका.डॉस.पॉलिसी/5390/ जे-1/2009-10 (परिपत्र संख्या 69/ डॉस.- 03/2009-10) का संदर्भ ग्रहण करें, जिसमें बैंकों को सलाह दी गई थी कि वे वित्तीय उत्पादों की बढ़ती जटिलता और इसके बढ़ते परिष्कार के साथ प्रौद्योगिकी के विस्तारित उपयोग के कारण परिचालन जोखिमों के प्रभाव को कम करने के लिए एक मजबूत व्यवसाय निरंतरता योजना (बीसीपी) लागू करें। इस सलाह का उद्देश्य बैंकों को अपने जोखिम प्रबंधन ढांचे को बढ़ाने में मार्गदर्शन करना है।

2. बढ़ती पर्यवेक्षी अपेक्षाओं और बैंकिंग पारिस्थितिकी तंत्र में बढ़ती जटिलता के कारण मजबूत व्यवसाय निरंतरता योजना को लागू करने का महत्व काफी बढ़ गया है। तदनुसार, यह महसूस किया गया है कि पर्यवेक्षित संस्थाओं (एसई) में व्यवधान की स्थिति में जोखिमों को कम करने के लिए व्यापार निरंतरता योजना पर दिशानिर्देशों पर फिर से विचार करने की आवश्यकता है। उन्हें महत्वपूर्ण व्यावसायिक कार्यों की पहचान करने और कमजोरियों और खतरों का मूल्यांकन करने के साथ-साथ यह निर्धारित करने की आवश्यकता के बारे में गहरी जागरूकता होनी चाहिए कि उनके पास बीसीपी के प्रभावी कार्यान्वयन के लिए एक मजबूत संगठनात्मक ढांचा और कॉर्पोरेट प्रशासन है। इसी तर्ज पर, बीसीपी पर मार्गदर्शन नोट को संशोधित किया गया है।

3. एसई को जोखिम शमन रणनीतियों को बढ़ाने के लिए एक मजबूत बीसीपी विकसित करने की सलाह दी जाती है ताकि वे विभिन्न खतरों और जोखिमों से निपटने के लिए बेहतर तैयारी कर सकें। उन्हें व्यापक जोखिम प्रबंधन योजनाएं विकसित करनी चाहिए जो वित्तीय जोखिम, तकनीकी जोखिम, पर्यावरणीय जोखिम, मानव संसाधन जोखिम आदि सहित उनके संचालन के सभी क्षेत्रों को कवर करती हैं। एसई को यह सुनिश्चित करना चाहिए कि बीसीपी पद्धति निम्नलिखित को कवर करती है:

(ए) एक बिजनेस इम्पैक्ट एनालिसिस (बीआईए) जो महत्वपूर्ण व्यावसायिक कार्यों की पहचान करता है और रिकवरी टाइम ऑब्जेक्टिव्स (आरटीओ) और रिकवरी प्वाइंट ऑब्जेक्टिव्स (आरपीओ) स्थापित करता है।

(बी) नियमित लेनदेन, भुगतान प्रणाली और ऑनलाइन बैंकिंग सहित सभी महत्वपूर्ण बैंक कार्यों पर विचार करते हुए व्यापक व्यावसायिक प्रभाव विश्लेषण के आधार पर संरचित जोखिम मूल्यांकन।

(सी) जोखिम निगरानी जिसमें नियमित अंतराल पर बीसीपी परीक्षण, स्वतंत्र ऑडिट और बीसीपी की समीक्षा और कर्मियों और आंतरिक/बाहरी वातावरण में परिवर्तन के आधार पर बीसीपी को अद्यतन करना शामिल है।

(डी) बीसीपी को व्यापक क्षेत्र की आपदाओं को प्रभावी ढंग से कम करने और परिचालन लचीलापन सुनिश्चित करने के लिए प्रक्रियात्मक, बुनियादी ढांचे, मानव संसाधन और प्रौद्योगिकी पहलुओं पर ध्यान देना चाहिए।

(ई) ऑडिट निष्कर्षों और विभागीय फीडबैक के आधार पर बीसीपी की नियमित समीक्षा और अद्यतनीकरण।

4. हम सलाह देते हैं कि सभी आरआरबी, सभी अनुसूचित एसटीसीबी और अन्य एसई जिनके पास 31 मार्च 2024 तक रु. 3000 करोड़ का व्यवसाय आकार हो, उनकी वित्तीय स्थिति के आधार पर उसी तारीख

से उन्हें ई-कैमलएससी आधारित पर्यवेक्षी दृष्टिकोण से गुजरना होगा. शेष बैंकों को चरणबद्ध तरीके से ई-कैमलएससी दृष्टिकोण के तहत लाया जाएगा. ई-कैमलएससी आधारित पर्यवेक्षी दृष्टिकोण के तहत आने वाले एसई को 30 सितंबर 2024 तक प्रभावी और मजबूत व्यवसाय निरंतरता योजना स्थापित करने की सलाह दी जाती है.

5. शेष बैंकों को 31 मार्च 2025 तक प्रभावी व्यवसाय निरंतरता योजना ढांचा तैयार करने की सलाह दी जाती है.

6. हम सलाह देते हैं कि इस परिपत्र की एक प्रति आपके बैंक के निदेशक मंडल की अगली बैठक में रखी जाए ताकि आपके बैंक में दिशानिर्देशों के कार्यान्वयन पर उचित निर्णय लिया जा सके।

7. कृपया अपने राज्य/केंद्र शासित प्रदेश में नाबार्ड क्षेत्रीय कार्यालय को इस परिपत्र की प्राप्ति की सूचना दें.

भवदीय

ह/-
(सुधीर कुमार रॉय)
मुख्य महाप्रबंधक

संलग्नक: मार्गदर्शी नोट

## मुख्य दस्तावेज़

| | |
|---|---|
| **दस्तावेज़ का शीर्षक** | व्यवसाय निरंतरता योजना पर मार्गदर्शी नोट |
| **ड्राफ्ट तैयार करने वाला विभाग** | पर्यवेक्षण विभाग |
| **अनुमोदन की तिथि** | 26 मार्च 2024 |
| **दस्तावेज़ का वर्गीकरण** | बाह्य |
| **दस्तावेज़ संख्या / संस्करण संख्या** | 2.0 |

## संस्करण का इतिहास

| संस्करण सं. | वित्तीय वर्ष | संशोधन/टिप्पणियाँ | संशोधनकर्ता |
|---|---|---|---|
| 1.0 | 2009-10 | नवीन | - |
| 2.0 | 2024-25 | संशोधित | पर्यवेक्षण विभाग |

## संस्करण का अनुमोदन

| संस्करण सं. | अनुमोदन की तिथि | संशोधन/टिप्पणियाँ | अनुमोदनकर्ता |
|---|---|---|---|
| 1.0 | 2009-10 | नवीन | पर्यवेक्षण निदेशक मंडल |
| 2.0 | 2024-25 | संशोधित | पर्यवेक्षण निदेशक मंडल |

## संदर्भ

| क्रम स. | संदर्भ | संदर्भ संख्या |
|---|---|---|
| 1 | परिचालन जोखिम प्रबंधन- व्यवसाय निरंतरता योजना | परिपत्र स. 69/ डॉस-09/2010, संदर्भ संख्या. राबैं.प्रका.डॉस.पॉलिसी/5390/ जे-1/2009-10 दिनांक 30 मार्च 2010 |

# व्यवसाय निरंतरता योजना

# पर मार्गदर्शी नोट

नाबार्ड

**विषयसूची**


**1. प्रस्तावना** ..... 1

**2. बीसीपी के उद्देश्य** ..... 2

**3. बीसीपी के लाभ** ..... 2

**5. बीसीपी की कार्य-पद्धति** ..... 7

**6. व्यवसाय प्रभाव विश्लेषण (बीआईए)** ..... 8

**6.1 रिकवरी टाइम के उद्देश्य** ..... 9

**6.2 रिकवरी पॉइंट के उद्देश्य** ..... 10

**7. जोखिम आकलन** ..... 10

**8. जोखिम अनुप्रवर्तन** ..... 13

**9. बीसीपी का परीक्षण** ..... 13

**9.1 परीक्षण तकनीक** ..... 14

**9.2 बीसीपी की समीक्षा / फ़ीडबैक** ..... 15

**10. बीसीपी के प्रक्रियात्मक पहलू** ..... 15

**11. बीसीपी के आधारभूत संरचनात्मक पहलू** ..... 15

**12. बीसीपी के मानव संसाधन पहलू** ..... 16

**13. बीसीपी के प्रौद्योगिकी पहलू** ..... 16

**13.1 आपदा रिकवरी** ..... 17

**अनुबंध 1** ..... 22

**अनुबंध 2** ..... 23

**अनुबंध 3** ..... 24

**अनुबंध 4** ..... 25

**अनुबंध 5** ..... 26

**अनुबंध 6** ..... 27

**अनुबंध 7** ..... 28

# व्यवसाय निरंतरता योजना (बीसीपी) पर मार्गदर्शी नोट

## 1. प्रस्तावना

वित्तीय उत्पादों की बढ़ती जटिलता और उन्नत प्रौद्योगिकी पर अधिक निर्भरता ने बैंकिंग उद्योग में परिचालन जोखिमों को और अधिक महत्वपूर्ण बना दिया है. जटिल वित्तीय उत्पादों में वृद्धि और प्रौद्योगिकी के विस्तारित उपयोग को देखते हुए, व्यापक व्यवसाय निरंतरता योजना (बीसीपी) दिशानिर्देश स्थापित करना आवश्यक है जो बैंकिंग वातावरण में लोगों, प्रक्रियाओं और प्रौद्योगिकी जैसे प्रमुख पहलुओं हेतु समाधान प्रदान करते हैं.

**परिचालन जोखिम** के महत्वपूर्ण क्षेत्रों में से एक - व्यवसाय व्यवधान और प्रणाली की विफलताओं के प्रतिकूल प्रभावों को कम करने हेतु व्यवसाय निरंतरता योजना (बीसीपी) एक महत्वपूर्ण पूर्व-आवश्यकता है. प्राकृतिक आपदाओं के घटित होने की स्थिति में बीसीपी का उद्देश्य निर्बाध ग्राहक सेवाएँ, बैकअप और पुनर्स्थापना प्रक्रियाएँ, बैकअपों की प्रभावशीलता, आपदा बचाव सुविधाएँ, उद्धार और पीछे हटने (फ़ॉलबैक) प्रक्रियाएँ हैं.

बीसीपी एक व्यापक, लिखित प्रलेख है जिसे बैंकिंग सेवा में किसी भी व्यवधान की स्थिति में ग्राहकों को सेवा प्रदान करने सहित व्यावसायिक परिचालनों को बनाए रखने और/ या फिर से शुरू करने हेतु विकसित किया गया है.

## 2. बीसीपी के उद्देश्य

व्यवसाय निरंतरता योजना का मुख्य लक्ष्य व्यवधानों के दौरान घाटे को कम करना है. इसमें वित्तीय घाटे, परिचालन घाटे और सेवा या परिचालन में व्यवधान के कारण होने वाले किसी भी अन्य नुकसान को कम करना शामिल है. बीसीपी का एक अन्य प्रमुख उद्देश्य किसी भी प्रकार के व्यवधान की स्थिति में व्यापार की निरंतरता सुनिश्चित करना है. इसका मतलब यह है कि बैंकों को न्यूनतम व्यवधान के साथ परिचालन जारी रखने हेतु किसी भी संभावित व्यवधान के लिए तैयार रहना चाहिए. बीसीपी का तीसरा उद्देश्य जोखिम शमन रणनीतियों को बढ़ावा देना है ताकि बैंक विभिन्न खतरों और जोखिमों से निपटने के लिए बेहतर तैयारी कर सकें. संगठनों को व्यापक जोखिम प्रबंधन योजनाएं विकसित करनी चाहिए जो वित्तीय जोखिम, प्रौद्योगिकीय जोखिम, पर्यावरणीय जोखिम, मानव संसाधन जोखिम आदि सहित उनके परिचालनों के सभी क्षेत्रों को कवर करती हैं.

एक अच्छी तरह से तैयार की गई बीसीपी आपदा के प्रभाव को कम कर सकती है और **परिचालन, वित्तीय, कानूनी और प्रतिष्ठा जोखिमों** के साथ-साथ ऐसी आपदा से उत्पन्न होने वाली अन्य समस्याओं को भी कम कर सकती है. कठिन परिस्थिति से उबरने और आपदा के घटित होने पर गतिविधियों को फिर से शुरू करने की बैंक की क्षमता, ग्राहक के विश्वास, विकास और अस्तित्व हेतु महत्वपूर्ण है.

## 3. बीसीपी के लाभ

बीसीपी संभावित कमजोरी का मूल्यांकन करने और किसी भी आपदा की स्थिति में संभावित रूप से गलत होने वाली स्थिति से निपटने की योजना बनाने की प्रक्रिया है. यह प्रबंधन को अपने व्यवसाय की बेहतर समझ प्राप्त करने का मौका प्रदान करता है जिससे अंततः संगठन को किसी भी प्रकार की कमियों को मजबूत करने के तरीकों को चिह्नित करने में मदद मिलती है, यहां तक कि उन क्षेत्रों में भी जिन पर पहले ध्यान नहीं दिया गया था.

बीसीपी न केवल बड़े पैमाने की समस्याओं के समक्ष संगठन को मजबूती प्रदान कर सकती है, बल्कि विस्तृत योजना के माध्यम से छोटी समस्याओं को हल करने में भी मदद करती है जो निरंतरता में बाधा उत्पन्न कर सकती हैं. बीसीपी संगठन की छवि, ब्रांड और प्रतिष्ठा की रक्षा करने में मदद करती है. किसी आपदा के घटित होने की स्थिति में यह नुकसान को बड़ी सीमा तक कम कर सकती है.

## 4. बीसीपी संगठन संरचना और कॉरपोरेट अभिशासन

बीसीपी की अंतिम जिम्मेदारी निदेशक मंडल और शीर्ष प्रबंधन की है. बोर्ड को बीसीपी के संबंध में शीर्ष प्रबंधन को स्पष्ट मार्गदर्शन और दिशा प्रदान करनी चाहिए. वरिष्ठ प्रबंधन बीसीपी प्रक्रिया की देखरेख के लिए जिम्मेदार है जिसमें निम्नलिखित शामिल हैं:

क. यह निर्धारित करना कि संस्था चिह्नित जोखिमों का प्रबंधन और नियंत्रण किस प्रकार करेगी.
ख. बीसीपी के कार्यान्वयन हेतु सुविज्ञ कर्मियों और पर्याप्त वित्तीय संसाधनों को आवंटित करना.
ग. महत्वपूर्ण व्यावसायिक कार्यों की प्राथमिकता तय करना.
घ. एक बीसीपी समन्वय समिति को नामित करना जो व्यवसाय निरंतरता प्रबंधन के लिए जिम्मेदार होगी.
ङ. शीर्ष प्रबंधन को प्रतिवर्ष संस्थान की व्यवसायिक पुनर्प्राप्ति, आकस्मिक योजनाओं और परीक्षण परिणामों की पर्याप्तता की समीक्षा करनी चाहिए और उन्हें बोर्ड के समक्ष प्रस्तुत करना चाहिए.
च. जब भी महत्वपूर्ण कार्यों को आउटसोर्स किया जाए, तो शीर्ष प्रबंधन को आकस्मिक आयोजना की पर्याप्तता और सेवा प्रदाताओं द्वारा उनके आवधिक परीक्षण का मूल्यांकन करवाने करने पर विचार करना चाहिए.
छ. यह सुनिश्चित करना कि बीसीपी की स्वतंत्र रूप से समीक्षा और अनुमोदन न्यूनतम वार्षिक रूप से किया जाता है.
ज. यह सुनिश्चित करना कि कर्मचारी बीसीपी के कार्यान्वयन में अपनी भूमिकाओं के प्रति प्रशिक्षित और जागरूक हों.
झ. यह सुनिश्चित करना कि बीसीपी का उद्यम-व्यापी आधार पर नियमित रूप से परीक्षण किया जाता है.
ञ. बीसीपी परीक्षण कार्यक्रम और परीक्षण परिणामों की नियमित आधार पर समीक्षा करना.
ट. यह सुनिश्चित करना कि बीसीपी का लगातार अद्यतन वर्तमान परिचालन वातावरण को परिलक्षित करने हेतु किया जाता है.

### 4.1 बीसीपी प्रमुख अथवा व्यवसाय निरंतरता समन्वयक

एक वरिष्ठ अधिकारी को बीसीपी गतिविधि अथवा कार्य के प्रमुख के रूप में नामित करने की आवश्यकता है. उनकी जिम्मेदारियों में निम्नलिखित शामिल हैं:

क. एक उद्यम-व्यापी बीसीपी को विकसित करना और उन व्यावसायिक उद्देश्यों और महत्वपूर्ण कार्यों को प्राथमिकता देना जो पुनर्प्राप्ति हेतु आवश्यक हैं.
ख. व्यवसाय निरंतरता योजना में केवल प्रौद्योगिकी घटकों की ही पुनर्प्राप्ति नहीं, बल्कि व्यवसाय के सभी पहलुओं की पुनर्प्राप्ति, पुनः आरंभ और रखरखाव भी शामिल है.
ग. वित्तीय बाजारों में संस्था की भूमिका के एकीकरण पर विचार करना.
घ. व्यावसायिक प्रक्रियाओं में बदलाव, लेखा-परीक्षा अनुशंसाओं और परीक्षण से मिली सीख के आधार पर व्यवसाय निरंतरता योजनाओं को नियमित रूप से अपडेट करना.
ङ. एक चक्रीय, प्रक्रिया-उन्मुख दृष्टिकोण का पालन करना जिसमें व्यावसायिक प्रभाव विश्लेषण (बीआईए), जोखिम मूल्यांकन, जोखिम निगरानी और बीसीपी का परीक्षण शामिल है.
च. सभी कारकों पर विचार करते हुए और "संकट" घोषित करने का निर्णय लेना.

### 4.2 बीसीपी समिति

चूँकि इलेक्ट्रॉनिक बैंकिंग के कार्य एक से अधिक विभागों में फैले हुए हैं, इसलिए यह आवश्यक है कि प्रत्येक विभाग योजना में अपनी भूमिका को समझे. यह भी आवश्यक है कि इसे बनाए रखने में हर व्यक्ति अपना सहयोग

प्रदान करे. किसी आपदा के घटित होने की स्थिति में, प्रत्येक व्यक्ति को पुनर्प्राप्ति प्रक्रिया हेतु तैयार रहना चाहिए, जिसका उद्देश्य महत्वपूर्ण कार्यों की सुरक्षा करना है.

अतः मानव संसाधन, सूचना प्रौद्योगिकी (आईटी), विधि, व्यवसाय और सूचना सुरक्षा जैसे विभागों के प्रमुखों/वरिष्ठ अधिकारियों की एक समिति निम्नलिखित व्यापक अधिदेश के साथ गठित की जानी चाहिए:

क. आवश्यकतानुसार व्यवसाय निरंतरता योजना को आवश्यकतानुसार क्रियान्वित करना, बनाए रखना और लागू करना.
ख. संवाद करें, प्रशिक्षित करें और जागरूकता को बढ़ावा दें.
ग. यह सुनिश्चित करें कि बीसीपी अन्य योजनाओं और संबंधित प्राधिकारियों की आवश्यकता के अनुरूप है.
घ. बजट संबंधी मुद्दे.
ङ. संबंधित टीमों और कर्मचारियों का बीसीपी पर प्रशिक्षण और उस पर उनकी जागरूकता सुनिश्चित करें.
च. अन्य पुनर्प्राप्ति, निरंतरता, प्रतिक्रिया टीमों की गतिविधियों का समन्वय करना और महत्वपूर्ण निर्णय लेने की प्रक्रिया को संभालना.
छ. अन्य कार्यों में आपदा से उत्पन्न होने वाले विधिक मामलों को और जनसंपर्क तथा मीडिया पूछताछ को संभालना शामिल है.

### 4.3 बीसीपी की प्रबंधन टीमें

आवश्यकतानुसार केंद्रीय कार्यालय के साथ-साथ ही एकल नियंत्रण कार्यालयों या शाखा स्तर पर बीसीपी के विभिन्न पहलुओं हेतु पर्याप्त टीमें होंनी चाहिए. आवश्यकता के आधार पर जिन टीमों पर विचार किया जा सकता है उनमें घटना प्रतिक्रिया टीम, आपातकालीन कार्रवाई और परिचालन टीम, विशेष व्यावसायिक कार्यों की टीम, क्षति मूल्यांकन टीम, हार्डवेयर, सॉफ्टवेयर, नेटवर्क सहायता हेतु आईटी टीम, रसद के आयोजन हेतु आपूर्ति टीम, स्थानांतरण टीम, प्रशासनिक सहायता टीम, समन्वय टीम शामिल हैं.

बीसीपी की समितियों या टीमों हेतु नमूना दिशानिर्देश नीचे दिए गए हैं:

| **बीसीपी के व्यक्ति अथवा समूह** | **एचआर** |
|---|---|
| विषय | विचार |
| 1. भूमिकाएँ, जिम्मेदारियाँ और प्राधिकार | • स्टाफ और स्थल पर ठेकेदारों को संप्रेषण.<br>• घातक घटनाओं से निपटना या परामर्श देना.<br>• संसाधन<br>• स्टाफ और ठेकेदारों के डेटाबेस को बनाए रखना |
| 2. आवश्यक योग्यताएँ/ क्षमताएँ | • दस्तावेजीकरण आयोजना<br>• प्रबंधन में परिवर्तन<br>• एचआर सीआईपीडी (चार्टर्ड इंस्टीट्यूट ऑफ पर्सनेल एंड डेवलपमेंट) प्रमाणीकरण |

| | |
|---|---|
| | • स्वास्थ्य एवं सुरक्षा |
| 3. प्रशिक्षण आवश्यकताओं के विश्लेषण के प्रति दृष्टिकोण | • परामर्श<br>• प्रशिक्षण परिदृश्य<br>• डेस्कटॉप अभ्यास<br>• पता करें कि क्या प्रबंधक समुदाय में बीसीपी लागू करने हेतु जिम्मेदारियों से अवगत हैं. |
| 4. उपयुक्त प्रशिक्षण | • टेबल टॉप<br>• परिदृश्य के अनुभाग<br>• पूर्ण अभ्यास |
| 5. आवश्यक योग्यता/क्षमता को मापने के तरीके | • लेखापरीक्षाएँ<br>• प्रयोगात्मक अभ्यास<br>• प्रत्यक्ष उद्घोष |
| 6. शिक्षा, प्रशिक्षण, कौशल, अनुभव और योग्यताओं के उपयुक्त अभिलेख | • पिछले अभ्यासों की रिपोर्टें |

| **बीसीपी के व्यक्ति अथवा समूह** | **बीसीपी टीमें** |
|---|---|
| विषय | विचार |
| 1. भूमिकाएँ, जिम्मेदारियाँ और प्राधिकार | • योजना में निर्धारित<br>• पदानुसार समानुदेशित |
| 2. आवश्यक योग्यताएँ/ क्षमताएँ | • व्यवसाय का ज्ञान<br>• प्रभाव को समझना<br>• सूचना का विश्लेषण करने की योग्यता<br>• नेतृत्व |
| 3. प्रशिक्षण आवश्यकताओं के विश्लेषण के प्रति दृष्टिकोण | • साक्षात्कार<br>• पिछला अनुभव<br>• आवश्यक कौशल<br>• परिदृश्य – "आप क्या करेंगे, यदि" के प्रभाव का विश्लेषण |
| 4. उपयुक्त प्रशिक्षण | • ज्ञान का साझा करना:<br>o वरिष्ठ स्टाफ<br>o कनिष्ठ स्टाफ<br>o बाह्य<br>• अभ्यास |
| 5. आवश्यक योग्यता/ क्षमता को मापने के तरीके | • प्रयोग का मूल्यांकन<br>• घटना के पश्चात समीक्षा की क्षमता |

| | |
|---|---|
| 6. शिक्षा, प्रशिक्षण, कौशल, अनुभव और योग्यताओं के उपयुक्त अभिलेख | • पिछले अभ्यासों की रिपोर्टें |

| **बीसीपी के व्यक्ति अथवा समूह** | **बीसीपी समिति** |
|---|---|
| विषय | विचार |
| 1. भूमिकाएँ, जिम्मेदारियाँ और प्राधिकार | • प्राधिकारियों को योजना का प्रयोग करना है, बनाए रखना है और लागू करना है (यदि निर्दिष्ट किया गया हो)<br>• संप्रेषण, प्रशिक्षण, और जागरूकता को बढ़ावा देना<br>• अन्य योजनाओं/प्राधिकरणों के अनुरूप हों.<br>• बजट<br>• अन्यों का प्रशिक्षित होना सुनिश्चित करें. |
| 2. आवश्यक योग्यताएँ/ क्षमताएँ | • व्यवसाय और व्यवसाय निरंतरता ढाँचे को समझना<br>• अपने कार्य में प्रवीणता और दक्षता<br>• प्रशिक्षित<br>• संप्रेषण की योग्यता/ क्षमता |
| 3. प्रशिक्षण आवश्यकताओं के विश्लेषण के प्रति दृष्टिकोण | • बीसीपी हेतु कॉर्पोरेट दृष्टिकोण/रणनीति<br>• बीसीपी को कैसे कार्यान्वित किया जाता है<br>• प्रतिनिधियों को शामिल करें<br>• कौशलों को उपयोग करने की क्षमता |
| 4. उपयुक्त प्रशिक्षण | • प्रशिक्षण आवश्यकताओं के विश्लेषण के प्रति दृष्टिकोण विषय के समान |

## 5. बीसीपी की कार्य-पद्धति

यह प्रलेख बीसीपी हेतु महत्वपूर्ण आवश्यकताओं की रूपरेखा तय करता है जिनका पालन किया जाना चाहिए. प्रत्येक बैंक की विशिष्ट गतिविधियों, प्रणालियों और प्रक्रियाओं के अनुरूप विस्तृत बीसीपी घटकों को विकसित करने की ज़िम्मेदारी बोर्ड और वरिष्ठ प्रबंधन की है.

बीसीपी की कार्य-पद्धति में निम्नलिखित शामिल होने चाहिए:

### चरण 1: व्यवसाय प्रभाव विश्लेषण (बीआईए)

1. बीआईए के साथ आने वाले सहायक कार्यों सहित महत्वपूर्ण व्यवसायों, स्वाधिकृत और साझे संसाधनों की पहचान.
2. बीआईए पर आधारित आरटीओ का गठन. उद्योग की सर्वोत्तम प्रथाओं के समक्ष बेंचमार्किंग द्वारा इसे समय-समय पर सुधारा भी जा सकता है.
3. आपदा के संबंध में महत्वपूर्ण और कठिन अवधारणाएँ ताकि अधिकतम दबावग्रस्त परिस्थितियों का सामना करने के लिए ढाँचा पर्याप्त रूप से व्यापक हो.
4. महत्वपूर्ण प्रणालियों में से प्रत्येक की डेटा हानि हेतु आरपीओ की पहचान और इस प्रकार की डेटा हानि से निपटने हेतु रणनीति.
5. किसी भी आपदा के दौरान प्रभावित होने वाली प्रक्रियाओं हेतु संसाधनों की आवश्यकताओं का अनुमान.

### चरण 2: जोखिम मूल्याँकन

1. व्यापक व्यवसाय प्रभाव विश्लेषण के आधार पर संरचित जोखिम मूल्याँकन. यह मूल्याँकन व्यवसाय की सभी प्रक्रियाओं पर करता है और यह केवल सूचना प्रसंस्करण सुविधाओं तक ही सीमित नहीं है.
2. बैंक के सहमत आरटीओ और आरपीओ को हासिल करने हेतु उपयुक्त रणनीति/ढाँचे को कार्यान्वित करके जोखिम का प्रबंधन.
3. ग्राहकों का सामना करने वाली प्रणालियों और भुगतान और निपटान प्रणालियों जैसे नकद संवितरण, एटीएम, इंटरनेट बैंकिंग, मोबाइल बैंकिंग, आईएमपीएस, आरटीजीएस, एनईएफटी या कॉल सेंटर सहित महत्वपूर्ण व्यावसायिक कार्यों को पुनर्स्थापित करने पर प्रभाव.
4. बाहरी संसाधनों और सहायता को के उपयोग में निहित निर्भरता और जोखिम.

### चरण 3: व्यवसाय निरंतरता रणनीति और विकल्पों का निर्धारण

1. बीसीपी को सूचना प्रौद्योगिकी के क्षेत्र से इतर भी विकसित होना चाहिए और इसमें लोगों, प्रक्रियाओं, तथा आधारभूत संरचना को आवश्यक रूप से शामिल किया जाना चाहिए.
2. शाखा में अथवा बाहरी स्थानों पर लोगों की सुरक्षा और कल्याण हेतु कार्य-पद्धति को आपदा के समय प्रभावी होना चाहिए.

3. आपदा की चिह्नित की गई श्रेणियों के आधार पर प्रतिक्रिया कार्रवाइयों को परिभाषित करें.
4. चयनित प्रक्रिया पुनरारंभ योजना के लिए बैंक, उद्योग और लागू विनियमों हेतु जोखिम स्वीकार्यता पर आवश्यक रूप से विचार करें.

**चरण 4: बीसीपी का कार्यान्वयन और विकास**

1. कार्य योजनाएँ (बैंक की प्रक्रियाओं हेतु विशिष्ट परिभाषित प्रतिक्रिया कार्रवाईयाँ), व्यावहारिक मैनुअल (क्या करें और क्या न करें, एकल व्यावसायिक इकाइयों हेतु अनुकूलित विशिष्ट पैराग्राफ) और परीक्षण प्रक्रियाएँ.
2. प्रबंधन के उत्तराधिकार और आपातकालीन शक्तियों की स्थापना करना.
3. बैंक और उसके सेवा प्रदाताओं दोनों के स्तर पर आकस्मिक योजनाओं की अनुकूलता और समन्वय.
4. पुन:प्राप्ति प्रक्रिया को पुन:प्राप्ति स्थान पर नियंत्रण परिवेश से समझौता नहीं करना चाहिए.
5. बैंक के व्यवसाय हेतु आउटसोर्स की गई गतिविधि की सार्थकता की डिग्री के आधार पर प्रत्येक आउटसोर्सिंग व्यवस्था के लिए विशिष्ट आकस्मिक योजनाएँ बनाना.
6. संस्थान या उसके सेवा प्रदाताओं में परिवर्तनों को आत्मसात करने हेतु आवधिक आधार पर अद्यतनीकरण. ऐसी स्थितियों के उदाहरण जो योजनाओं के अद्यतनीकरण को आवश्यक बनाती हैं, उनमें नए उपकरणों का अधिग्रहण, परिचालन प्रणालियों का उन्नयन और निम्नलिखित में परिवर्तन शामिल हैं

    क. कार्मिक
    ख. पते और दूरभाष नंबर
    ग. व्यवसाय रणनीति
    घ. स्थान, सुविधाएं तथा संसाधन
    ङ. विधान/ कानून
    च. ठेकेदार, आपूर्तिकर्ता और प्रमुख ग्राहक
    छ. प्रक्रियाएँ - नई अथवा वापस ले ली गईं
    ज. जोखिम (परिचालन और वित्तीय)

## 6. व्यवसाय प्रभाव विश्लेषण (बीआईए)

इसमें विभिन्न महत्वपूर्ण व्यवसायों, स्वाधिकृत और साझा किए गए संसाधनों और संभावित कमजोरियों, खतरों की पहचान और विश्लेषण शामिल है जिन पर बीआईए हेतु विचार किया जाना चाहिए. जोखिम के परिमाण और घटना के घटित होने की संभावना को ध्यान में रखते हुए, बीसीपी का प्रावधान रोकथाम और नियंत्रण दोनों के लिए होना चाहिए. आंतरिक लेखापरीक्षा विभाग द्वारा आवधिक अद्यतन के अधीन भेद्यता मूल्यांकन और समीक्षा बैंक के आंतरिक नियंत्रण का हिस्सा होना चाहिए. इसमें आरटीओ और आरपीओ तैयार करना शामिल है. निम्नलिखित प्रभाव विश्लेषण पैमाने का उपयोग उनके कार्यों की प्रकृति और गंभीरता के आधार पर विभिन्न प्रक्रियाओं का मूल्यांकन करने के लिए किया जा सकता है.

| स्कोर | स्तर | परिणाम के प्रकार | प्रभाव |
|---|---|---|---|
| 1 | महत्वहीन | वित्तीय | वित्तीय स्थिति बहुत कम प्रभावित |
| | | परिचालनात्मक | परिचालन बहुत कम प्रभावित |
| | | प्रतिष्ठात्मक | जनता के ध्यान पर बहुत कम प्रभाव |
| | | कानूनी और विनियामक अनुपालन | बहुत मामूली कानूनी मुद्दा. कोई दंड नहीं |
| 2 | निम्न | वित्तीय | वित्तीय स्थिति अल्प रूप से प्रभावित |
| | | परिचालनात्मक | परिचालन अल्प रूप से प्रभावित |
| | | प्रतिष्ठात्मक | जनता के ध्यान पर अल्प प्रभाव |
| | | कानूनी और विनियामक अनुपालन | मामूली कानूनी मुद्दा. कोई दंड नहीं |
| 3 | मध्यम | वित्तीय | वित्तीय स्थिति मध्यम रूप से प्रभावित |
| | | परिचालनात्मक | परिचालन मध्यम रूप से प्रभावित |
| | | प्रतिष्ठात्मक | जनता के ध्यान पर मध्यम प्रभाव |
| | | कानूनी और विनियामक अनुपालन | कानून का मध्यम उल्लंघन. मध्यम दंड |
| 4 | उच्च | वित्तीय | वित्तीय स्थिति महत्वपूर्ण रूप से प्रभावित |
| | | परिचालनात्मक | परिचालन महत्वपूर्ण रूप से प्रभावित |
| | | प्रतिष्ठात्मक | जनता के ध्यान पर महत्वपूर्ण प्रभाव |
| | | कानूनी और विनियामक अनुपालन | कानून का बड़ा उल्लंघन. उच्च दंड |
| 5 | गंभीर | वित्तीय | वित्तीय स्थित गंभीर रूप से प्रभावित |
| | | परिचालनात्मक | परिचालन गंभीर रूप से प्रभावित |
| | | प्रतिष्ठात्मक | जनता के ध्यान पर गंभीर प्रभाव |
| | | कानूनी और विनियामक अनुपालन | कानून का गंभीर रूप से उल्लंघन. उच्चतर दंड |

## 6.1 रिकवरी टाइम के उद्देश्य

*रिकवरी टाइम के उद्देश्य (आरटीओ)* को सूचना प्रौद्योगिकी आधारभूत संरचना के बिना अधिकतम समय व्यवसाय के रूप में परिभाषित किया गया है. किसी घटना के प्रभाव के बाद कार्यों को फिर से शुरू करने के लिए न्यूनतम देरी. यह भिन्न- भिन्न घटनाओं में भिन्न होगा. व्यवसाय प्रभाव विश्लेषण के आधार पर बैंक की व्यावसायिक प्रक्रियाओं को प्रभावित करने वाली विभिन्न संभावित घटनाओं के मामले में आरटीओ के रूप में संदर्भित आदर्श न्यूनतम प्रत्युथान समय, **अनुबंध 1** में दिया गया है. इस समय के आधार पर, बीसीपी की योजना बनाई जानी चाहिए और प्रत्युथान प्रक्रिया शुरू होनी चाहिए.

बीसीपी तैयार करने में शाखाओं की मदद करने के लिए आधारभूत संरचना संबंधी कुछ घटनाएँ और सांकेतिक सुझाव **अनुबंध 2, 3, 4 और 5** में दिए गए हैं.

## 6.2 रिकवरी पॉइंट के उद्देश्य

*रिकवरी पॉइंट के उद्देश्य (आरपीओ)* को उस समय के बिंदु के रूप में परिभाषित किया गया है जिस पर डेटा बहाल किया जा सकता है. सरल शब्दों में, हम कितना डेटा खोने का जोखिम उठा सकते हैं. चूंकि हम ग्राहकों के डेटा से निपटते हैं और लेनदेन को खोने का जोखिम नहीं उठा सकते हैं, इससे हमारी विश्वसनीयता प्रभावित होगी और प्रतिष्ठात्मक जोखिम उत्पन्न होगा, आरपीओ भी आदर्श रूप से कम से कम सीबीएस परिदृश्यों में शून्य होना चाहिए. यह बैंक की तकनीकी प्रगति के आधार पर भिन्न हो सकता है.

# 7. जोखिम आकलन

जोखिम का मूल्यांकन व्यावसायिक प्रभाव के व्यापक विश्लेषण के आधार पर किया जाना है. इस मूल्यांकन में बैंक के सभी कार्यों को ध्यान में रखा जाना चाहिए और केवल सूचना प्रौद्योगिकी तक ही सीमित नहीं होना चाहिए. इसमें नियमित व्यवसाय लेनदेन, भुगतान और निपटान प्रणाली, नकद संवितरण, एटीएम, इंटरनेट बैंकिंग आदि जैसे सभी महत्वपूर्ण कार्यों को बहाल करना शामिल है.

## 7.1 खतरा/ भेद्यता/ जोखिम विश्लेषण

- **एक जोखिम** वह संभाव्यता है कि किसी दिए गए खतरे से संपत्ति को नुकसान/क्षति होने के लिए भेद्यताओं का दोहन किया जाएगा. यह अवांछनीय घटना के प्रभाव और घटना के घटित होने की संभावना का एक कार्य है.
- **भेद्यताएँ** संपत्ति से जुड़ी कमजोरियाँ हैं, जो ज्यादातर मामलों में आंतरिक नियंत्रण की कमी हैं. भेद्यता से नुकसान नहीं होता जब तक कि इनका दोहन न किया जाए.

## 7.2 भेद्यताओं के प्रकार

- पर्यावरण सुरक्षा का अभाव
- शारीरिक सुरक्षा का अभाव
- नेटवर्क अभिगम नियंत्रण का अभाव
- घुसपैठ का पता लगाने के लिए नेटवर्क की निगरानी का अभाव
- प्रणाली के रखरखाव की कमी - अगर ठीक से रखरखाव नहीं किया जाता है तो मशीनों और उपकरणों के टूटने का खतरा होता है. कोर बैंकिंग सॉल्यूशन (सीबीएस) के प्रादुर्भाव के साथ, बैंक के सभी डेटा को एक केंद्रीकृत स्थान पर संग्रहीत किया जाता है जिसे डेटा सेंटर (डीसी) कहा जाता है. इसमें कई नेटवर्क मशीनें (हार्डवेयर और सॉफ्टवेयर शामिल) हैं. परिसंपत्तियों की अच्छी देखभाल और रखरखाव के बावजूद, व्यवधान से इंकार नहीं किया जा सकता है.
- बैक-अप, भंडारण और बहाली प्रक्रियाओं में नियंत्रण का अभाव
- एंटी-वायरस उपायों की कमी

- डेटा सेंटर का अनुचित स्थान

## 7.3 खतरा

*खतरे* आंतरिक या बाहरी कारक हैं जो संपत्ति के क्षति / नुकसान / हानि का कारण बन सकते हैं और व्यवसाय में व्यवधान पैदा कर सकते हैं. खतरे आकस्मिक या इरादतन हो सकते हैं.

**खतरों के प्रकार**

कुछ प्रमुख प्रकार के खतरे इस प्रकार हैं:

### 7.3.1 प्राकृतिक आपदाएं

- *आकस्मिक बाढ़* - महत्वपूर्ण दस्तावेजों को टेबल के ऊपर रखने/दस्तावेजों को तिजोरी से सुरक्षित स्थान पर निकालने जैसी गतिविधियां शुरू की जानी चाहिए. पानी घटने तथा परिसर की सफाई हो जाने के बाद महत्वपूर्ण सेवाओं को प्राथमिकता देते हुए कार्य शीघ्र शुरू किया जाना चाहिए.
- *भूकंप* - विशेष रूप से भूकंप की आशंका वाले क्षेत्रों में आवश्यक सावधानी बरती जानी चाहिए. यदि भूकंप के तुरंत बाद परिसर का उपयोग नहीं किया जा सकता है, तो आसपास के क्षेत्र में एक अस्थायी व्यवस्था की जानी चाहिए और शाखा का कामकाज वैकल्पिक सेट-अप के साथ शुरू किया जाना चाहिए. शॉर्ट सर्किट/विफलताओं से बचने के लिए विद्युत कनेक्शन शुरू करने से पहले इसे एक योग्य तकनीशियन द्वारा बहाल किया जाना चाहिए. शाखा को ऐसे उपयुक्त स्थान की पहचान करनी चाहिए और जनता को उचित जानकारी/प्रदर्शन उपलब्ध कराया जाना चाहिए. भूकंप के बाद आवश्यकता पड़ने पर इंजीनियर द्वारा भवन की सुरक्षा का आवश्यक निरीक्षण किया जाना चाहिए.
- *आग का प्रकोप* - स्मोक डिटेक्टर और फायर अलार्म स्थापित किए जाने चाहिए और उनका नियमित आधार पर अनुरक्षण किया जाना चाहिए. स्थापना में दहनशील वस्तुओं का उपयोग या भंडारण नहीं किया जाना चाहिए. उचित कार्य के लिए समय-समय पर उनका परीक्षण किया जाना चाहिए. अग्नि निकास को स्पष्ट रूप से चिह्नित किया जाना चाहिए और उन्हें अबाधित रखना चाहिए. अग्नि बीमा पॉलिसियों को चालू रखा जाना चाहिए. कर्मचारियों को आग लगने की स्थिति में उनके द्वारा की जाने वाली कार्रवाइयों के बारे में पता होना चाहिए. आवधिक अंतराल पर फायर ड्रिल आयोजित की जानी चाहिए.

### 7.3.2 मानवीय हस्तक्षेप

- *चोरी या तोड़फोड़*
- *प्रसंस्करण में मानवीय त्रुटि*
- *बम या विस्फोटक की धमकी* - घटना के बाद परिसर की सफाई के उपरांत सेवाएं शुरू की जानी चाहिए. संग्रहीत और कहीं और रखे गए डेटा को एक नए हार्डवेयर में एकत्र और स्थापित किया जाना

चाहिए तथा शुरुआत में महत्वपूर्ण कार्य शुरू किए जाने चाहिए. इस तरह के कार्य से होने वाले नुकसान का आकलन काम-काज शुरू करने से पहले किया जाना चाहिए.

- *बहिःस्राव/ गैस रिसाव* - व्यक्तियों को तुरंत जगह खाली करने के लिए कहा जाना चाहिए. दरवाजे और खिड़कियां खुली रखी जानी चाहिए. जिस क्षण क्षेत्र मानव व्यवसाय के लिए उपयुक्त पाया जाता है, उसी क्षण सामान्य स्थिति बहाल की जानी चाहिए.
- *भौतिक अभिगम नियंत्रण* - डीसी/ सर्वर कमरों तक पहुंचने वाले कर्मियों के नाम दर्ज करते हुए विशेष एक्सेस कंट्रोल रजिस्टर का ठीक से रख-रखाव किया जाना चाहिए. डीसी/शाखा से संवेदनशील डेटा या उपकरण/घटक को हटाने की जांच/रोकथाम के लिए निकास नियंत्रण के उचित उपाय होने चाहिए. योजना में कुछ वस्तुओं जैसे सिस्टम रूम के दरवाजों पर इलेक्ट्रॉनिक/ मैनुअल लॉक, प्रमाणीकरण नियंत्रण (पासवर्ड नियंत्रण या कोड नंबर या बायोमैट्रिक्स के माध्यम से) आदि उपकरणों को शामिल किया जाना चाहिए जिससे केवल अधिकृत कर्मियों को सिस्टम रूम या डीसी के भीतर या अन्य संवेदनशील क्षेत्रों में प्रवेश करने की अनुमति दी जा सके. प्रमुख कोड या चाबियों की डुप्लिकेट प्रतियां जिनका उपयोग आपात स्थिति में भौतिक अभिगम नियंत्रण को पार करने के लिए किया जा सकता है, उन्हें प्राप्त किया जाना चाहिए और सीलबंद लिफाफे में सुरक्षित रूप से रखा जाना चाहिए, और यह लिफाफा केवल आपातकालीन स्थिति में ही खोला जाना चाहिए. इन सीलबंद लिफाफों को स्थापना के प्रमुख के पास रखा जाना चाहिए, जो इस चाबियों की प्रत्युत्थान के अनुदेशों के साथ प्रमुख स्थानों पर सुरक्षित रूप से संग्रहित करने की व्यवस्था करेगा.

### 7.3.3 प्रौद्योगिकी विफलताएं

- *ब्रेकडाउन से संबंधित आधारभूत संरचना*
- *हार्डवेयर विफलताएं*
- *सॉफ्टवेयर विफलताएं*
- *नेटवर्क घटक विफलता*
- *नेटवर्क अंतर्वेधन*
- *वायरस अटैक*
- *सिस्टम विफलता*
- *संचार कड़ी की विफलता*
- *पावर आउटेज* - बिजली और प्रोत्कर्ष सुरक्षा आवश्यकताओं की पहचान की जानी चाहिए, और पर्याप्त प्रोत्कर्ष सुरक्षा उपकरण स्थापित किए जाने चाहिए. पर्याप्त भार क्षमता का यूपीएस सिस्टम स्थापित किया जाना चाहिए. यूपीएस सिस्टम और बैटरियों का नियमित रूप से अनुरक्षण किया जाना चाहिए. लंबे समय तक बिजली बाधित होने से होने वाली आपदा से बचने के लिए आपातकालीन जनित्र लगाए जाने चाहीए. सभी संबंधितों की जानकारी और जागरूकता के लिए डीसी में एक प्रमुख स्थान पर इलेक्ट्रिकल/ लैन केबलिंग का आरेख प्रदर्शित किया जाना चाहिए. लैन केबलिंग को बिजली के तारों से अलग रखा जाना चाहिए.

*(कृपया बैंक शाखाओं में सुरक्षा सावधानी की चेकलिस्ट के लिए **अनुबंध 6** और बैंक के लिए आपातकालीन सेवा सूची के लिए **अनुबंध** 7 देखें)*

***टिप्पणी:*** *बैंक के सुचारू कार्यपद्धति में व्यवधान डालने वाली सभी आपदाओं/घटनाओं का उल्लेख करना संभव नहीं सकता क्योंकि यह शाखा/बैंक की भौगोलिक स्थिति और अपेक्षित विकृतियों/भेद्यताओं पर निर्भर करता है. कुछ वस्तुओं का उल्लेख मार्गदर्शन के रूप में किया गया है. बीसीपी तैयार करते समय, स्थान की अवस्थिति और विभिन्न घटनाएं जो हो सकती हैं, उन्हें शुरू की जाने वाली कार्रवाई के साथ स्पष्ट रूप से उल्लेख किया जाना चाहिए. (**कृपया सांकेतिक उदाहरणों के लिए अनुलग्नक देखें.**)*

## 8. जोखिम अनुप्रवर्तन

जोखिम निगरानी बीसीपी का एक अनिवार्य हिस्सा है. बैंक में सभी कार्यात्मक विभाग यह सुनिश्चित करेंगे कि उसका बीसीपी निम्नलिखित के माध्यम से व्यवहार्य है:

- कम से कम आवधिक आधार पर यथा अर्ध-वार्षिक/वार्षिक- बीसीपी का परीक्षण.
- जब भी आवश्यकता हो, बीसीपी की स्वतंत्र लेखा परीक्षा और समीक्षा.
- कर्मियों और आंतरिक / बाहरी वातावरण (तकनीकी प्रगति सहित और आवधिक प्रतिक्रिया के आधार पर) में परिवर्तन के आधार पर बीसीपी का अद्यतन.
- प्रधान कार्यालय में बीसीपी समिति चल रही निगरानी सुनिश्चित करने के लिए जिम्मेदार होगी..

## 9. बीसीपी का परीक्षण

बीसीपी के परीक्षण में बैंक के सभी पहलुओं और घटकों को शामिल किया जाना चाहिए अर्थात व्यक्ति, प्रक्रियाएं और संसाधन (प्रौद्योगिकी सहित). गलत अवधारणाओं, निरीक्षण या उपकरण या कर्मियों में परिवर्तन के मामले में, बीसीपी काम नहीं कर सकता है. बीसीपी परीक्षणों को यह सुनिश्चित करना चाहिए कि प्रत्युथान दल के सभी सदस्य और अन्य संबंधित कर्मचारी योजनाओं से अवगत हैं. बीसीपी के लिए परीक्षण अनुसूची को यह इंगित करना चाहिए कि योजना के प्रत्येक घटक का परीक्षण कैसे और कब किया जाना है. कुछ उपाय जो किए जा सकते हैं वे इस प्रकार हैं:

1. बैंकों को बीसीपी की प्रभावशीलता की जांच करने के लिए अपने आंतरिक लेखा परीक्षकों/आईएस लेखा परीक्षकों को शामिल करना चाहिए.
2. बैंक को महत्वपूर्ण तृतीय पक्षों के साथ बीसीपी ड्रिल की योजना बनाने पर विचार करना चाहिए, ताकि पूर्व-पहचान की गई न्यूनतम आवश्यक प्रक्रियाओं को जारी रखने के लिए सेवाएं और सहायता प्रदान किया जा सके.
3. बैंकों को समय-समय पर अपने परिचालनों - व्यक्तियों, प्रक्रियाओं और संसाधनों (सूचना प्रौद्योगिकी और गैर- सूचना प्रौद्योगिकी) सहित - को नियोजित डीआर साइट पर ले जाना चाहिए ताकि बीसीपी प्रभावशीलता का परीक्षण किया जा सके और सामान्य कार्यपद्धति में परिचालन लाने के लिए आवश्यक प्रत्युथान समय का भी पता लगाया जा सके.
4. बैंकों को डीआर साइट पर बैंक कर्मियों के आवागमन के बिना उपरोक्त परीक्षण करने पर विचार करना चाहिए. इससे डीआर साइट पर वैकल्पिक कर्मचारियों की तत्परता का परीक्षण करने में मदद मिलेगी.

यह आश्वासन देने के लिए विभिन्न तकनीकों का उपयोग किया जाना चाहिए कि योजना वास्तविकता में काम करेगी.

## 9.1 परीक्षण तकनीक

बीसीपी के परीक्षण के लिए आमतौर पर निम्नलिखित तकनीकों को अपनाया जाता है

- *सिमुलेशन परीक्षण* - यह परीक्षण तब किया जाता है जब प्रतिभागी एक विशिष्ट परिदृश्य चुनते हैं और ऑन-लोकेशन बीसीपी स्थिति सिमुलेट करते हैं. इसमें सभी संसाधनों का परीक्षण शामिल है जैसे व्यक्ति, सूचना प्रौद्योगिकी और अन्य. जिन्हें एक चुने हुए परिदृश्य के लिए व्यवसाय निरंतरता को सक्षम करने की आवश्यकता होती है. परीक्षण में ज्ञान, टीम इंटरैक्शन और निर्णय लेने की क्षमताओं सहित क्षमता के प्रदर्शन पर ध्यान केंद्रित किया गया है.
- *घटक परीक्षण*: यह परीक्षण बीसीपी की स्थापना की स्थिति में प्रक्रिया के एक वैयक्तिक भाग या एक उपप्रक्रिया के की कार्यपद्धति को सत्यापित करता है. यह किसी भी जोखिम जो इसके सुचारू रूप से चलने में बाधा उत्पन्न कर सकता है उसकी पहचान करने और उसके लिए तैयार रहने के लिए भाग या उप-प्रक्रिया के गहन परीक्षण पर ध्यान केंद्रित करता है. उदाहरण के लिए, एटीएम स्विच का परीक्षण.
- *टेबल-टॉप परीक्षण* - आपदाओं का उदाहरण व्यवसाय प्रत्युत्थान व्यवस्था पर चर्चा करना.
- *तकनीकी प्रत्युत्थान परीक्षण* - यह सुनिश्चित करना कि सूचना प्रणाली को प्रभावी ढंग से बहाल किया जा सकता है.
- *वैकल्पिक साइट पर पुत्युत्थान का परीक्षण करना* - मुख्य साइट से दूर प्रत्युत्थान कार्रवाइयों के समानांतर व्यावसायिक प्रक्रियाएँ चलाना.
- *आपूर्तिकर्ता सुविधाओं और सेवाओं के परीक्षण* - यह सुनिश्चित करने के लिए कि बाहरी रूप से प्रदान की गई सेवाएं और उत्पाद अनुबंधित प्रतिबद्धता को पूरा करेंगे.
- *पूर्ण पूर्वाभ्यास* - इसका परीक्षण कि संगठन, कर्मियों, उपकरणों, सुविधाओं और प्रक्रियाओं को रुकावटों का सामना करना कर सकें.

प्रत्येक संगठन को पूरी तरह से जोखिम और व्यावसायिक प्रभाव विश्लेषण किए जाने के बाद, परीक्षण के लिए चुने गए व्यावसायिक क्षेत्रों की आवृत्ति, अनुसूची और समूहों को परिभाषित करना चाहिए.

बैंक द्वारा एक प्रक्रिया की महत्वपूर्णता के आधार पर परीक्षण आवृत्ति निर्धारित करने के लिए नीचे दिए गए व्यापक दिशानिर्देशों पर विचार कर सकता है:

| **प्रक्रियाएँ** | **प्रक्रियाओं पर प्रभाव** | **टेबल-टॉप परीक्षण** | **सिमुलेशन परीक्षण** | **घटक परीक्षण** | **पूर्ण पूर्वाभ्यास** |
|---|---|---|---|---|---|
| प्रक्रिया 1 | उच्च | त्रैमासिक | त्रैमासिक | त्रौमासिक | वार्षिक |
| प्रक्रिया 2 | मध्यम | त्रैमासिक | अर्धवार्षिक | वार्षिक | वार्षिक |
| प्रक्रिया 3 | निम्न | अर्धवार्षिक | लागू नहीं | लागू नहीं | लागू नहीं |

## 9.2 बीसीपी की समीक्षा / फ़ीडबैक

ऑडिट टिप्पणियों और विभिन्न विभागों से प्राप्त फीडबैक के आधार बीसीपी की समीक्षा और अद्यतन किया जाना चाहिए ताकि ऐसे परिवर्तनों को शामिल किया जा सके और सुधार सुनिश्चित किया जा सके. बीसीपी प्रक्रियाओं को संगठन के प्रबंधन कार्यक्रम के भीतर शामिल किया जाना चाहिए ताकि यह सुनिश्चित हो सके कि व्यवसाय निरंतरता मामलों को उचित रूप से संबोधित किया गया है. आवधिकता का निर्णय बैंक द्वारा ही किया जाए.

परिवर्तनों को बैंक की औपचारिक प्रबंधन प्रक्रिया जो ऐसे परिवर्तनों की नीति या प्रक्रिया दस्तावेजों के लिए स्थापित हैं उनका पालन करना चाहिए. इस औपचारिक परिवर्तन नियंत्रण प्रक्रिया को यह सुनिश्चित करना चाहिए कि अद्यतन योजनाओं को पूरी योजना की नियमित समीक्षाओं द्वारा वितरित और प्रबलित किया जाए.

## 10. बीसीपी के प्रक्रियात्मक पहलू

क. बीसीपी को व्यापक क्षेत्र आपदाओं जो पूरे क्षेत्र को प्रभावित करती हैं और परिणामस्वरूप कर्मचारियों की होने वाली हानि या दुर्गमता की संभाव्यता को ध्यान में रखना चाहिए. इसे विभिन्न सेवा प्रदाताओं के बीच अन्योन्याश्रितताओं पर भी विचार करना चाहिए और उनका समाधान करना चाहिए.

ख. यदि बैंक ने सीबीएस को लागू किया है, तो उन्हें द्वितीयक साइटों या डीआर साइटों से कुछ महत्वपूर्ण प्रक्रियाएं और परिचालनों का संचालन करने पर विचार करना चाहिए, जिसमें प्रत्येक एक-दूसरे का बैक-अप प्रदान करेंगे. जहां कर्मचारी निर्दिष्ट कार्यालय परिसर तक पहुंचने में सक्षम नहीं हैं ऐसे परिदृश्यों के लिए कर्मियों पर निर्भरता को कम करने के लिए सभी महत्वपूर्ण प्रक्रियाओं का प्रलेखीकरण किया जाना चाहिए.

ग. सभी महत्वपूर्ण भूमिकाओं के लिए बैकअप/स्टैंडबाय कर्मियों की पहचान की जानी चाहिए. व्यक्तिगत वित्तीय प्राधिकरणों, वित्तीय क्षेत्र के व्यवसाय संघों और अन्य बैंकों तथा हितधारकों को शामिल करते हुए भविष्य में आने वाली आपातकालीन स्थितियों को बेहतर ढंग से समन्वयित करने के लिए एक कॉल मैट्रिक्स विकसित किया जाना चाहिए.

घ. बैंकों को प्राकृतिक आपदा/आपदा की स्थिति का सामना करने के लिए विस्तृत बीसीपी रखने पर विचार करना चाहिए. एक औपचारिक अपवाद नीति का प्रलेखीकरण किया जाना चाहिए जो प्रभावित क्षेत्रों के कर्मियों का स्वतंत्र रूप से कार्य करने के लिए मार्गदर्शन करेगी जब तक कि बाहरी दुनिया से संपर्क दोबारा शुरू नहीं हो जाता है.

## 11. बीसीपी के आधारभूत संरचनात्मक पहलू

क. बैंकों को सभी कार्यालयों में बिजली, पानी और प्राथमिक चिकित्सा बॉक्स जैसी आधारभूत सुविधाओं की उपलब्धता पर विशेष ध्यान देने पर विचार करना चाहिए.

ख. इमारतों पर इन-हाउस दूरसंचार प्रणालियों और वायरलेस ट्रांसमीटरों हेतु बैकअप पावर की व्यवस्था होनी चाहिए. अतिरिक्त प्रणाली, जैसे एनालॉग लाइन फोन और सैटेलाइट फोन (जहां उपयुक्त हो), और अन्य सरल उपाय, जैसे कि मोबाइल फोन के लिए अतिरिक्त बैटरी की उपलब्धता सुनिश्चित करना जो आधारभूत संरचना की व्यापक पैमाने पर विफलता के मामले में संचार को बनाए रखने के लिए आवश्यक साबित हो सकता है.

ग. बैंकों को इस पर विचार करना चाहिए कि महत्वपूर्ण दस्तावेज़, फाइलों, सर्वरों को भूतल जहां बाढ़ या जल जमाव की संभावना है वहाँ पर संग्रहीत किया जाए. हालांकि, बैंकों को इस पर भी विचार करना चाहिए कि ऊंची इमारतों के शीर्ष मंजिलों पर भी ऐसे संग्रहण न किए जाएँ ताकि संभावित आग के कारण होने वाले दुष्प्रभाव को कम किया जा सके.

घ. महत्वपूर्ण दस्तावेजों के लिए फायर-प्रूफ और वाटर-प्रूफ भण्डारण क्षेत्रों पर विचार किया जाना चाहिए.

ङ. बैंकों को अधिक समय के लिए होने वाली बिजली कटौतियों हेतु बिजली स्रोत के वैकल्पिक साधनों (जैसे अधिक डीजल/आपातकालीन बैटरी बैकअप अधिप्राप्ति आदि) पर विचार करना चाहिए.

च. बैंकों को ग्राहकों के प्रश्नों समाधान करने के लिए एक आपातकालीन हेल्पलाइन नंबर या राष्ट्रीयकृत आईवीआर संदेश रखने पर विचार करना चाहिए और यह सुनिश्चित करना चाहिए कि तनाव की स्थिति से बचा जा सके.

## 12. बीसीपी के मानव संसाधन पहलू

क. बैंक को मानव संसाधन से संबंधित मुद्दों को ध्यान में रखना चाहिए जो बीसीपी का मसौदा तैयार करते समय उत्पन्न हो सकते हैं. इसलिए, बीसीपी को तैयार करने में मानव संसाधन एक अभिन्न अंग होना चाहिए क्योंकि आम तौर पर, योजनाएं अक्सर तकनीकी मुद्दों पर बहुत अधिक केंद्रित होती हैं. व्यक्तियों से संबंधित एक अलग खंड को शामिल किया जाना चाहिए, जिसमें कर्मचारी कल्याण, परामर्श, स्थानांतरण विचार आदि शामिल हों.

ख. बीसीपी जागरूकता कार्यक्रमों को परिचयात्मक कार्यक्रम न्यूज़ लेटर, स्टाफ प्रशिक्षण अभ्यासों आदि के माध्यम से भी लागू किया जाना चाहिए, जो बीसीपी में कर्मचारियों की भागीदारी को दृढ़ता प्रदान करने के लिए काम करते हैं.

ग. बैंकों को विशिष्ट महत्वपूर्ण कार्यों के लिए एक से अधिक वैयक्तिक कर्मचारियों को प्रशिक्षित करने पर विचार करना चाहिए (अर्थात् एक कर्मचारी की अनुपस्थिति में कार्य में स्थगन या देरी नहीं की जानी चाहिए). उन्हें महत्वपूर्ण कार्यों और दस्तावेज़-परिचालन प्रक्रियाओं के लिए कर्मचारियों की क्रॉस-ट्रेनिंग पर विचार करना चाहिए.

## 13. बीसीपी के प्रौद्योगिकी पहलू

बैंकिंग प्रणाली में कई अनुप्रयोग और सेवाएं हैं जिनकी प्रकृति अत्यधिक महत्वपूर्ण किस्म की है और इसलिए समाधान को तैयार और कार्यान्वित करते समय उच्च उपलब्धता और दोष सह्यता पर विचार करने की आवश्यकता

होती है. इस पहलू को विशेष रूप से डेटा सेंटर सॉल्यूशन्स और कॉर्पोरेट नेटवर्क सॉल्यूशन्स तैयार करते समय ध्यान में रखा जाना चाहिए. प्रौद्योगिकी से संबंधित बीसीपी के पहलुओं में से एक आपदा प्रत्युत्थान योजना है.

## 13.1 आपदा रिकवरी

डेटा रिकवरी (डीआर) रणनीति का चयन करने से पहले, एक डीआर प्लानर को अपने संगठन के बीसीपी का उल्लेख करना चाहिए, जिसे व्यावसायिक प्रक्रियाओं के लिए आरपीओ और आरटीओ के प्रमुख मैट्रिक्स को इंगित करना चाहिए.

जैसे ही आरटीओ और आरपीओ मैट्रिक्स को सूचना प्रौद्योगिकी आधारभूत संरचना में मैप किया जाता है, डीआर प्लानर प्रत्येक प्रणाली के लिए सबसे उपयुक्त प्रत्युत्थान रणनीति निर्धारित कर सकता है. आरटीओ और आरपीओ मैट्रिक्स का उपलब्ध बजट और व्यावसायिक प्रक्रिया/कार्य की महत्वपूर्णता के साथ फिट होना आवश्यक है.

एक आपदा प्रत्युत्थान योजना बीसीपी का एक हिस्सा है. यह एक गतिशील दस्तावेज होना चाहिए; डेटा सेंटर के कार्यों में कोई भी बदलाव होने पर उन परिवर्तनों को प्रतिबिंबित करने के लिए योजना को अद्यतन किया जाना चाहिए. यह प्रत्युत्थान प्रक्रिया के हर पहलू को निर्धारित करता है, जिसमें शामिल हैं:

क. कौन सी घटनाएँ संभावित आपदाओं को दर्शाती हैं.
ख. संगठन के किन व्यक्तियों के पास आपदा घोषित करने और इस तरह योजना को लागू करने का अधिकार है.
ग. आपदा घोषित होने के बाद बैकअप साइट तैयार करने के लिए आवश्यक घटनाओं का अनुक्रम.
घ. योजना को पूरा करने के संबंध में सभी प्रमुख कर्मियों की भूमिकाएं और जिम्मेदारियां.
ङ. उत्पादन बहाल करने के लिए आवश्यक हार्डवेयर और सॉफ्टवेयर की एक सूची.
च. उन कर्मियों को सूचीबद्ध करने वाली एक अनुसूची जिसके अनुसार बैकअप साइट पर स्टाफ करेंगे को प्रतिनियुक्त किया जाएगा. जिसमें आपदा दल के सदस्यों को हटाए बिना चल रहे परिचालन का सहयोग करने के लिए एक रोटेशन शेड्यूल शामिल हो.

सामान्यतः बैंक डाटा रिकवरी के लिए कोर बैंकिंग सॉल्यूशन (सीबीएस) का अनुसरण करते हैं. सीबीएस के तहत, शाखाओं को डीसी में एक केंद्रीकृत डेटाबेस से जोड़ा जाता है और सभी कार्यों को एक केंद्रीय सर्वर से संभाला जाता है. कई मामलों में, एक संगठन अपने स्वयं के दूरस्थ सुविधाओं का उपयोग करने के बजाय एक स्टैंड-बाय साइट और सिस्टम प्रदान करने के लिए एक आउटसोर्स आपदा प्रत्युत्थान सेवा प्रदाता का उपयोग करने का चुनाव कर सकता है. प्रणाली की बहाली करने की आवश्यकता की तैयारी के साथ-साथ संगठनों को पहली जगह में आपदा को रोकने के उद्देश्य से एहतियाती उपायों को भी लागू करना चाहिए. इनमें निम्नलिखित में से कुछ शामिल हो सकते हैं:

i. बिजली आपूर्ति की विफलता की स्थिति में प्रणाली को चालू रखने के लिए निर्बाध बिजली आपूर्ति (यूपीएस) या बैकअप जनरेटर
ii. आग की रोकथाम-अलार्म, आग बुझाने वाले यंत्र
iii. एंटी-वायरस सॉफ्टवेयर और सुरक्षा उपाय

### 13.1.1 बैकअप साइट और आपदा उद्धार (डीआर) समाधान लागू करना*:*

**बैकअप साइट**: बैकअप साइट एक ऐसी जगह है जहाँ कोई संगठन किसी आपदा जैसे आग, बाढ़, आतंकवादी खतरा या अन्य विध्वंसक घटनाओं के बाद आसानी से स्थानांतरित हो सकता है. यह किसी संगठन की आपदा उद्धार योजना और व्यापक बीसीपी का एक अभिन्न अंग है.

**बैकअप साइटों के प्रकार**

- हॉट साइट
- कोल्ड साइट
- वार्म साइट

*हॉट साइट*: हॉट साइट किसी संगठन के मूल साइट की डुप्लिकेट होती है, जिसमें समग्र कम्प्यूटर प्रणाली के साथ-साथ यूजर डाटा का लगभग पूरा बैकअप होता है. व्यापक क्षेत्र नेटवर्क लिंक और विशेष सॉफ़्टवेयर का उपयोग करके, मूल साइट के डेटा की प्रकृति को प्रतिबिंबित करने के लिए दो साइटों के बीच रियल-टाइम सिंक्रनाइज़ेशन का उपयोग किया जाएगा. मूल साइट में व्यवधान के बाद, हॉट साइट मौजूद है ताकि संगठन न्यूनतम नुकसान के साथ सामान्य परिचालन के लिए स्थानांतरित हो सके.

*कोल्ड साइट*: किसी संगठन के परिचालन के लिए कोल्ड साइट सबसे सस्ती प्रकार की बैकअप साइट है. इसमें संगठन के मूल स्थान से डेटा और जानकारी की बैकअप प्रतियां शामिल नहीं हैं, न ही इसमें पहले से स्थापित हार्डवेयर शामिल है. हार्डवेयर की कमी कोल्ड साइट की न्यूनतम स्टार्ट-अप लागत में योगदान करती है, लेकिन आपदा के बाद अतिरिक्त समय की आवश्यकता होती है ताकि आपदा से पहले की क्षमता के करीब परिचालन चल सके.

वार्म साइट: वार्म साइट वार्म और कोल्ड के बीच एक समझौता है. इन साइटों में हार्डवेयर और कनेक्टिविटी पहले से ही स्थापित है, हालांकि मूल उत्पादन साइट या यहां तक कि हॉट साइट की तुलना में यह छोटे पैमाने पर स्थापित है. वार्म साइटों पर बैकअप उपलब्ध हैं, लेकिन वे पूरे नहीं हो सकते हैं और कुछ दिन से लेकर एक सप्ताह तक पुराने हो सकते हैं. उदाहरण के लिए कूरियर द्वारा वार्म साइट पर भेजे गए बैकअप टेप होंगे.

*नोट: उनके बीच मुख्य अंतर विक्रेताओं के समाधान के प्रत्येक के कार्यान्वयन में आवश्यक लागत एवं प्रयास और रूपरेखा से निर्धारित किए जाते है.*

### 13.1.2 सीबीएस में डीसी/ डीआर समाधान लागू करने में आने वाली समस्याएं

क. डीसी और डीआर के समाधान आर्किटेक्चर विक्रेताओं द्वारा प्रदान किए गए सभी एप्लिकेशन और सेवाओं के लिए समान नहीं हैं. बैंकों को समय-समय पर आवधिक समीक्षा और डीआर समाधानों को अपग्रेड करना होगा और यह सुनिश्चित करना होगा कि सभी महत्वपूर्ण एप्लिकेशन और सेवाएं निष्पादन और उपलब्धता के मामले में आदर्श प्रतीत हों.

ख. डीसी और डीआर पर सर्वर, नेटवर्क डिवाइस और अन्य उत्पादों का कॉन्फ़िगरेशन हर समय समान होना चाहिए. इसमें वे पैच शामिल हैं जो डीसी पर आवधिक रूप से लागू किए जाते हैं और नियामक आवश्यकताओं, प्रणाली परिवर्तन इत्यादि हेतु कस्टमाइजेशन और पैरामीटराइजेशन द्वारा समय-समय पर सॉफ़्टवेयर में किए गए बदलाव शामिल हैं.

ग. डीसी और डीआर के बीच डेटा और लेनदेन की शुद्धता सुनिश्चित करने के संदर्भ में आवधिक जांच अनिवार्य है. समाधान में परिभाषित आरटीओ और आरपीओ मापदंड होना चाहिए. इन मापदंडों के प्रौद्योगिकी पहलुओं के साथ-साथ डीआर में कटौती के लिए परिभाषित प्रक्रिया और निर्दिष्ट समय सीमा में आगे बढ़ने के लिए आवश्यक योग्यता स्तरों पर बहुत स्पष्ट प्रभाव पड़ता है.

घ. यह देखने के लिए कि डीआर काम कर रहा है या नहीं, डीआर ड्रिल समय-समय पर आयोजित की जानी चाहिए. डीसी और डीआर में सहायक आधारभूत संरचना, अर्थात, विद्युत प्रणाली, एयर कंडीशनिंग वातावरण और अन्य समर्थन प्रणालियों में फेलियर का एक भी बिंदु नहीं है और संसाधनों की नियमित और लगातार निगरानी करने के लिए प्रबंधन और निगरानी प्रणाली को बनाया गया है.

ङ. डीसी और डीआर के बीच अपनाया जाने वाला डेटा प्रतिकृति तंत्र एक अतुल्यकालिक प्रतिकृति तंत्र है जो या तो डेटाबेस प्रतिकृति तकनीकों या भंडारण-आधारित प्रतिकृति तकनीकों का उपयोग करके इसे पूरे उद्योग में लागू किया जाता है. आरपीओ सीधे तौर पर डीआर पर डेटाबेस को अपडेट करने के लिए डीसी से लेनदेन डेटा के लिए अनुमति विलंबता से संबंधित है. इसलिए, डेटा प्रतिकृति आवश्यकता के लिए कार्यान्वित प्रक्रिया उपरोक्त के अनुरूप होनी चाहिए और डेटा और लेनदेन शुद्धता से कोई समझौता नहीं होना चाहिए.

### 13.1.3 बैंकों द्वारा डीसी/ डीआर कार्यान्वयन में मुद्दे/ चुनौतियाँ/ समाधान

क. उपकरण और दूरसंचार डिजाइन और पुनर्प्राप्ति सेवाओं में काफी प्रगति के बावजूद, आईटी आपदा पुनर्प्राप्ति चुनौतीपूर्ण होती जा रही है. निरंतरता और पुनर्प्राप्ति पहलू आईटी रणनीति को प्रभावित कर रहे हैं और लागत निहितार्थ आईटी बजट को चुनौती दे रहे हैं.

ख. 24/ 365 परिचालनों की मांग के सामने पुनर्प्राप्ति के लिए समय सीमा कम हो रही है. इसका मतलब यह है कि पारंपरिक ऑफ-साइट बैकअप और पुनर्स्थापना विधियां अब पर्याप्त नहीं हैं. विभिन्न अंतर-संबंधित एप्लिकेशन (अलग-अलग समय पर बैकअप) के वृद्धिशील और फूल इमेज बैकअप को पुनर्प्राप्त करने, उन्हें सिंक्रनाइज़ करने और आपदा बिंदु के निकटतम स्थिति को फिर से बनाने में बहुत लंबा समय लगता है. निरंतर परिचालन - ऑफसाइट स्थानों पर डेटा मिररिंग और स्टैंडबाय कंप्यूटिंग और दूरसंचार - एकमात्र समाधान हो सकता है.

ग. जोखिम मूल्यांकन और व्यावसायिक प्रभाव विश्लेषण को विशिष्ट आईटी और दूरसंचार सेवाओं और एप्लिकेशनों के लिए निरंतरता का औचित्य स्थापित करना चाहिए.

घ. मजबूत सुरक्षा (सुरक्षा आश्वासन) प्राप्त करना केवल एक बार की गतिविधि नहीं है. यह एक निरंतर प्रक्रिया है जिसे संगठन की सुरक्षा स्थिति के नियमित मूल्यांकन और किसी भी भेद्यता का पता लगाने और उसे ठीक करने के लिए सक्रिय कदम उठाने की आवश्यकता होती है. प्रत्येक बैंक के पास संदिग्ध व्यवहार पर नज़र रखने, उपयोगकर्ताओं की निगरानी करने और फोरेंसिक कार्य-निष्पादन करने हेतु विशेषज्ञों तक त्वरित और विश्वसनीय पहुंच होनी चाहिए. जब भी ऐसी घटनाएं होती हैं तो संबंधित अधिकारियों - जैसे आरबीआई/ नाबार्ड /आईडीआरबीटी/ सीईआरटी-आईएन और अन्य संस्थानों को पर्याप्त रिपोर्टिंग एक स्वचालित उप प्रक्रिया होनी चाहिए.

ङ. बैंकों में दूरसंचार की समस्याएं भी उत्पन्न हो सकती हैं. यह सुनिश्चित करना महत्वपूर्ण है कि प्रासंगिक लिंक मौजूद हैं और संचार क्षमता उनके अनुरूप है. वॉयस और डेटा क्षमता की पर्याप्तता की जांच की जानी चाहिए. टेलीफोनी को आपदा स्थल से स्टैंडबाय साइट पर स्विच करने की आवश्यकता है. एक वित्तीय संस्थान के बीसीपी को अपनी दूरसंचार क्षमताओं के लिए विविधता दिशानिर्देशों को संबोधित करने पर विचार करना चाहिए. सभी वित्तीय संस्थानों द्वारा विविधता दिशानिर्देशों पर विचार किया जाना चाहिए और यह संस्थान के आकार, जटिलता और समग्र जोखिम प्रोफ़ाइल के अनुरूप होना चाहिए. विविधता दिशानिर्देशों में कई दूरसंचार प्रदाताओं के साथ व्यवस्थाएं शामिल हो सकती हैं. वित्तीय संस्थानों के लिए अपने प्राथमिक दूरसंचार वाहक और विभिन्न उप-वाहकों के बीच संबंधों को और जटिल नेटवर्क उनकी प्राथमिक और बैक-अप सुविधाओं से कैसे जुड़ता है उसे समझना महत्वपूर्ण है.

च. बीसीपी को बढ़ाने के लिए बैंक निम्नलिखित दूरसंचार विविधता घटकों पर विचार कर सकते हैं:

i. वैकल्पिक मीडिया, जैसे सुरक्षित वायरलेस प्रणाली
ii. इंटरनेट प्रोटोकॉल नेटवर्किंग उपकरण जो आसानी से कॉन्फ़िगर करने योग्य रीरूटिंग और ट्रैफ़िक लोड संतुलन क्षमताएं प्रदान करता है.
iii. एक से अधिक दूरसंचार वाहक के केंद्रीय कार्यालय के लिए स्थानीय सेवाएं, या स्वतंत्र केंद्रीय कार्यालयों के लिए विविध भौतिक पथ.
iv. बैकअप लोकेशन हेतु अलग बिजली स्रोत और अलग कनेक्शन
v. एकाधिक सुविधाओं का नियमित उपयोग जिसमें ट्रैफ़िक को लगातार कनेक्शनों के बीच विभाजित किया जाता है.
vi. हार्डवेयर और सॉफ्टवेयर आधारभूत संरचना की जरूरतों के लिए अलग-अलग आपूर्तिकर्ता.

छ. अंतर्निहित जोखिमों को अधिक प्रभावी ढंग से प्रबंधित करने के लिए बैंकों को दूरसंचार प्रदाताओं के साथ अपने सेवा संबंधों की निगरानी करने की आवश्यकता है. विक्रेताओं के साथ समन्वय में, प्रबंधन को यह सुनिश्चित करना चाहिए कि जोखिम प्रबंधन रणनीतियों में कम से कम निम्नलिखित शामिल हों:

i. सेवा स्तर के समझौते स्थापित करें जो आकस्मिक उपायों को संबोधित करते हैं और प्रदान की गई सेवाओं के लिए प्रबंधन में परिवर्तन करते हैं**.**
ii. सुनिश्चित करें कि प्राथमिक और बैक-अप दूरसंचार पाथ फेलियर का एक भी बिंदु साझा न करें.
iii. व्यापक परीक्षण के माध्यम से दूरसंचार सर्किट और रूटिंग पाथ को समय-समय पर सूचीबद्ध करने और मान्य करने के लिए प्रक्रियाएं स्थापित करें.

ज. *आउटसोर्सिंग के जोखिम*- विभिन्न कारणों से प्रत्येक बैंक अपना स्वयं का डीसी/ डीआर प्रदान करने में सक्षम नहीं होगा. सभी प्रौद्योगिकी गतिविधियों को किसी तृतीय-पक्ष सेवा प्रदाता को आउटसोर्स करना

महत्वपूर्ण है. प्रणाली इंटीग्रेटर उस गतिविधि को करता है जो बदले में कुछ गतिविधियों को कुछ अन्य विक्रेताओं को आउटसोर्स करता है लेकिन गतिविधियों का समन्वय बैंक से संबंधित होनी चाहिए. यह सुनिश्चित करना बैंक की जिम्मेदारी है कि गतिविधियां उन विक्रेताओं को आउटसोर्स की जाएं, जो उच्चतम मानकों को लागू करते हैं, जिनके पास एक सख्त अनुबंध है, जो सेवा विनिर्देशों और तकनीकी आवश्यकताओं और सेवा-स्तरीय समझौतों को स्पष्ट रूप से परिभाषित करते हैं.

## अनुबंध 1

## व्यवसाय प्रभाव विश्लेषण और प्रत्युत्थान समय सीमा (आरटीओ)

विभिन्न घटनाओं का सांकेतिक परिदृश्य. बैंक के लिए बीसीपी तैयार करते समय ऐसी सभी घटनाओं को योजना में रखा जाना चाहिए और उद्धार के समय, जिम्मेदारी आदि का उल्लेख किया जाना चाहिए.

| क्र. सं. | घटनाएं | विघटन का विस्तार | प्रत्युत्थान समय सीमा (आरटीओ) | संबंधित विभाग | आधिकारिक संपर्क |
|---|---|---|---|---|---|
| 1 | **मानव संबंधित अवरोध** | | | | |
| 1क | कर्मचारियों द्वारा हड़ताल | • पूर्ण बैंक | | | |
| 1ख | प्रौद्दोगिकी- जो सुरक्षा प्रक्रियाओं का अनुसरण नहीं करता है. | • शाखाओं, प्रशासनिक कार्यालयों, डाटा केंद्रों आदि में | | | |
| 2 | **उपकरण की खराबी** | • शाखाएं<br>• प्रशासनिक कार्यालयों<br>• डाटा केंद्र<br>• नेटवर्क आधारभूत संरचना<br>• अन्य | | | |
| 3 | **पर्यावरण संबंधी अवरोध** | | | | |
| 3क | भूकंप | • शाखाओं का समूह<br>• प्रशासनिक कार्यालय<br>• डाटा केंद्र<br>• नेटवर्किंग आदि | | ` | |
| 3ख | बाढ़ | • शाखाओं का समूह<br>• प्रशासनिक कार्यालय<br>• डाटा केंद्र आदि | | | |
| 3ग | भीषण आग/ बॉम्बिंग | • शाखाओं में<br>• प्रशासनिक कार्यालयों में<br>• डाटा केंद्र में आदि | | | |
| 3घ | फ़ैक्टरि बहिर्वाह प्रवाह/ गैस लीकेज | • शाखाओं का समूह<br>• प्रशासनिक कार्यालयों<br>• डाटा केंद्रों<br>• नेटवर्किंग आदि | | | |

**अनुबंध 2**

## बीसीपी तैयार करते समय सेंपल घटनाएं और सुझाव दिए गए कार्रवाइयाँ

| घटना | विघटन का विस्तार | कार्रवाई की जाने का सुझाव |
|---|---|---|
| पावर फेलियर | प्रभावित स्थान | यूपीएस चालू करें. जनरेटर सेट चालू करें. |
| इलेक्ट्रिसिटी सप्लाई फेलियर | प्रभावित स्थान | यूपीएस पहले बैटरी से और पांच मिनट के बाद जनरेटर से स्वचालित रूप से बिजली प्राप्त करेगा. बिजली की बहाली के लिए अनुवर्ती कार्रवाई शुरू की जाएगी. इसके साथ ही, गैर-महत्वपूर्ण और अनावश्यक प्रणालियों को बंद कर दिया जाना चाहिए ताकि महत्वपूर्ण प्रणालियों को अधिक समय तक बिजली उपलब्ध करायी जा सके. |
| एक यूपीएस प्रणाली की फेलियर | प्रभावित स्थान | यह सलाह दी जाती है कि यूपीएस की दो इकाइयाँ रखें और एक सर्वर को एक यूपीएस से और दूसरे सर्वर को दूसरे यूपीएस से जोड़कर, खंडित दृष्टिकोण के माध्यम से कंप्यूटरों को बिजली की आपूर्ति को विभाजित करें ताकि प्रणाली में अतिरेक पैदा हो सके. |
| रॉ बिजली की फेलियर के साथ-साथ बैटरियों का ख़त्म होना | प्रभावित स्थान | चूंकि रॉ बिजली और बैटरी से बिजली दोनों उपलब्ध नहीं होगी, इसलिए प्रणाली प्रशासक को जनरेटर शुरू करना होगा. नियमित आवधिक अंतराल पर बैटरियों की क्रियाशीलता प्राप्त कर सक्रिय कार्यवाही भी की जायेगी. इसके साथ ही, प्रणाली प्रशासक को बैटरियों के प्रतिस्थापन के लिए विक्रेता का समर्थन प्राप्त करना चाहिए. |
| एयर कंडीशनर का काम नहीं करना | कोई प्रभाव नहीं | प्रशासन अनुभाग के माध्यम से प्रणाली प्रशासक को एसी इकाइयों की फेलियर पर ध्यान देना चाहिए, समस्या को ठीक करने के लिए विक्रेता का समर्थन प्राप्त करना चाहिए. |

## अनुबंध 3
## हार्डवेयर फेलियरओं की सेंपल घटनाएं और सुझाई गई कार्रवाई

| घटना | प्रभाव | कार्रवाई |
|---|---|---|
| इंटरनेट बैंकिंग सर्वर काम नहीं कर रहा है | इंटरनेट बैंकिंग तक पहुंच नहीं | समस्या को ठीक करने के लिए प्रणाली प्रशासक को विक्रेता का समर्थन प्राप्त करना चाहिए. |
| ईथरनेट कार्ड फेल होने की स्थिति में | प्रणाली रुक जाती है | प्रणाली प्रशासक को कनेक्टिविटी को दूसरे ईथरनेट कार्ड में भौतिक रूप से स्थानांतरित करने के लिए विक्रेता का समर्थन लेना चाहिए ताकि प्रणाली को ऊपर और कार्यशील स्थिति में लाया जा सके. |
| राउटर काम नहीं कर रहे हैं | नेटवर्क कनेक्टिविटी | समस्या को ठीक करने के लिए प्रणाली प्रशासक को विक्रेता का समर्थन प्राप्त करना चाहिए. |
| सुरक्षा प्रणालियाँ काम नहीं कर रही हैं | प्रणाली रुक जाती है | समस्या को ठीक करने के लिए प्रणाली प्रशासक को विक्रेता का समर्थन प्राप्त करना चाहिए. |

**अनुबंध 4**

## सॉफ़्टवेयर फेलियरओं की सेंपल घटनाएं और सुझाई गई कार्रवाई

| घटना | प्रभाव | प्रतिक्रियात्मक कार्रवाई |
|---|---|---|
| ऑपरेटिंग सिस्टम की समस्याएँ | सिस्टम रुक जाता है | समस्या को ठीक करने के लिए प्रणाली प्रशासक को विक्रेता का समर्थन प्राप्त करना चाहिए. |
| डेटाबेस संबंधी समस्याएँ | सिस्टम रुक जाता है | समस्या को ठीक करने के लिए प्रणाली प्रशासक को विक्रेता का समर्थन प्राप्त करना चाहिए |
| कोर बैंकिंग सॉल्यूशंस से संबंधित समस्याएं | सिस्टम रुक जाता है | समस्या को ठीक करने के लिए सिस्टम प्रशासक को विक्रेता का समर्थन प्राप्त करना चाहिए. |
| एप्लीकेशन सॉफ्टवेयर (इंटरनेट बैंकिंग) संबंधी समस्याएँ | सिस्टम रुक जाता है | समस्या को ठीक करने के लिए सिस्टम प्रशासक को विक्रेता का समर्थन प्राप्त करना चाहिए. |
| डाटा करप्शन | सिस्टम रुक जाता है | सिस्टम प्रशासक को नवीनतम बैकअप से डेटा को पुनर्स्थापित करना चाहिए. |
| बैकअप पुनर्प्राप्ति योग्य नहीं है | सिस्टम एक घंटे के लिए रुक जाता है | सिस्टम एडमिनिस्ट्रेटर को लॉग्स की मदद से पुराने बैकअप को फिर से बनाना चाहिए. |

## अनुबंध 5

## नेटवर्क फेलियर की सेंपल घटनाएं और सुझाई गई कार्रवाई

| घटना | प्रभाव | प्रतिक्रियात्मक कार्रवाई |
|---|---|---|
| इंटरनेट बैंकिंग फेल होने की स्थिति में लीज्ड लाइन लिंक | कोई प्रभाव नहीं | प्रणाली स्वचालित रूप से आईएसडीएन लिंक को ट्रिगर करता है.<br><br>हालाँकि, प्रणाली प्रशासक को लीज्ड लाइन लिंक को जल्द से जल्द चालू करने के लिए विक्रेता का समर्थन प्राप्त करना होगा. |
| लीज्ड लाइन और आईएसडीएन लिंक दोनों की फेल होने की स्थिति में | सिस्टम रुक जाता है | प्रणाली प्रशासक को लिंक लाने और काम करने के लिए विक्रेता का समर्थन प्राप्त करना होगा. |
| राउटर के फेल होने की स्थिति में | सिस्टम रुक जाता है | यदि आवश्यक हो, तो प्रणाली प्रशासक को स्टैंडबाय राउटर का आयोजन करके समस्या को ठीक करने के लिए विक्रेता का समर्थन प्राप्त करना होगा. |
| आईएसपी एंड पर पोर्ट फेलियर | सिस्टम कुछ समय के लिए रुक जाता है | पोर्ट सेटिंग्स को बदलने के लिए प्रणाली प्रशासक को विक्रेता का समर्थन प्राप्त करना होगा. |
| मोडम के फेल होने की स्थिति में | सिस्टम कुछ समय के लिए रुक जाता है | प्रणाली प्रशासक को स्टैंडबाय मॉडेम पर स्थानांतरित करने के लिए विक्रेता का समर्थन प्राप्त करना होगा. |

## अन्य फेलियर

| घटना | प्रभाव | प्रतिक्रियात्मक कार्रवाई |
|---|---|---|
| वायरस अटैक | सिस्टम धीमा/ रुक जाता है | समस्या को ठीक करने के लिए प्रणाली प्रशासक को विक्रेता का समर्थन प्राप्त करना होगा |
| सरविस अटैक का खंडन | सिस्टम धीमा/ रुक जाता है | समस्या को ठीक करने के लिए प्रणाली प्रशासक को विक्रेता का समर्थन प्राप्त करना होगा. |

## अनुबंध 6

### शाखाओं में सुरक्षा एहतियात की सांकेतिक जाँच सूची

1. क्या शाखा खोलते समय न्यूनतम दो स्टाफ सदस्य मौजूद रहते हैं?
2. यदि सशस्त्र गार्ड तैनात है, तो क्या वह सामान्यतः शाखा खोलते समय उपस्थित रहता है?
3. जब भी व्यक्तिगत स्टाफ सदस्य शाखा में प्रवेश करते हैं तो क्या गेट बंद कर दिए जाते हैं और फिर से ताला लगा दिया जाता है?
4. क्या व्यावसायिक घंटों के दौरान चैनल गेट आधे खुले और जंजीर से बंधे रहते हैं?
5. बैंकिंग समय समाप्त होने पर, क्या कोलैप्सिबल/ ग्रिल गेट को बंद रखा जाता है और वास्तविक ग्राहकों/ आगंतुकों को केवल पहचान के बाद और शाखा प्रबंधक से मंजूरी लेने के बाद ही प्रवेश की अनुमति दी जाती है?
6. क्या सशस्त्र गार्ड, जहां भी तैनात किया गया है, उपयुक्त स्थान पर तैनात किया गया है ताकि वह बैंकिंग हॉल का पूरा दृश्य देख सके और अपराधियों के खिलाफ अपने हथियार का प्रभावी ढंग से उपयोग कर सके?
7. क्या सशस्त्र गार्ड का उपयोग केवल सुरक्षा कर्तव्यों पर ही किया जाता है?
8. क्या कर्मचारियों के कार्य क्षेत्र के अंदर ग्राहकों/ आगंतुकों के प्रवेश की निगरानी और नियंत्रण किया जाता है?
9. क्या अग्निशामक यंत्र को समय पर भराया गया/ जांचा गया है?
10. क्या अलार्म सिस्टम छेड़छाड़रोधी है, चाहे वह कहीं भी उपलब्ध कराया गया हो?
11. क्या अलार्म सिस्टम चालू हालत में है और हमेशा 'ऑन' स्थिति में रहता है?
12. क्या कर्मचारी अलार्म सिस्टम के संचालन और उसके स्विचों के स्थान से परिचित हैं?
13. क्या नकदी रखने की सीमा का पालन किया जाता है?
14. क्या महत्वपूर्ण टेलीफोन नंबर प्रमुखता से प्रदर्शित किए गए हैं?
15. क्या महत्वपूर्ण टेलीफोन नंबर शाखा प्रबंधक/ लेखाकार की व्यक्तिगत डायरी में रखे जाते हैं?
16. क्या खिड़कियों/ वेंटीलेटरों में मजबूत ग्रिल हैं?
17. क्या कामकाजी घंटों के दौरान कैश केबिन को अंदर से बंद रखा जाता है?
18. क्या नकद प्रेषण के लिए वाहनों का चयन करने से पहले मालिकों और ड्राइवरों के पूर्ववृत्त की जाँच की जाती है?
19. क्या ट्रांसफार्मर, स्विचबोर्ड, एयर कंडीशनर और कंप्यूटर जैसे सभी विद्युत उपकरणों की समय-समय पर जाँच/ रखरखाव होता है?
20. क्या विद्युत परिपथ में सर्किट ब्रेकर का उपयोग किया जाता है?
21. क्या बैकअप दस्तावेज़ सुरक्षित परिसर, ऑफ-साइट पर रखे गए हैं?
22. क्या अग्निशामक यंत्रों की समय-समय पर सेवा ली जाती है?
23. क्या कर्मचारी अग्निशामक यंत्रों के उपयोग में प्रशिक्षित हैं?
24. क्या परिसर साफ-सुथरा रखा गया है?
25. क्या स्टेशनरी का सामान रैक में ठीक से रखा गया है?
26. क्या शाखाएँ/ कार्यालय 'धूम्रपान निषेध' क्षेत्र हैं?
27. क्या बेकार कागज़ों को पात्र में रखा जाता है और क्या उनका उचित और नियमित रूप से निपटान किया जाता है?

## अनुबंध 7

**आपातकालीन सेवा सूची**

| शाखा | सेवा | संपर्क |
|---|---|---|
| पुलिस स्टेशन | नगर नियंत्रण कक्ष | **100** |
| | **पुलिस मुख्यालय** | |
| | **ट्रेफिक पुलिस** | |
| | पुलिस स्टेशन 1 | |
| | पुलिस स्टेशन 2 | |
| अग्निशामक विभाग | नगर नियंत्रण कक्ष | |
| | अग्निशामक स्टेशन 1 | |
| | अग्निशामक स्टेशन 2 | |
| जिला प्रशासन | आयुक्त | |
| | कलेक्टर | |
| | पुलिस अधीक्षक | |
| अस्पताल/ एम्बुलेंस सेवा | अस्पताल 1 | |
| | अस्पताल 2 | |
| | अस्पताल | |
| | अस्पताल 4 | |
| सेवा प्रदाताओं के महत्वपूर्ण संपर्क | वकील | |
| | वैल्यूअर | |
| | इलेक्ट्रिशन | |
| | प्लंबर | |
| | कारपेंटर | |