भारतीय
RESERVE BANK OF INDIA

परिचालन जोखिम प्रबंधन और परिचालन आघात-सहनीयता पर मार्गदर्शी नोट

आरबीआई/2024-25/31

विवि.ओआरजी.आरईसी. 21/14.10.001/2024-25 अप्रैल 30, 2024

1. उद्देश्य

1.1 परिचालन जोखिम सभी बैंकिंग/वित्तीय उत्पादों, सेवाओं, गतिविधियों, प्रक्रियाओं और प्रणालियों में अंतर्निहित है। परिचालन जोखिम का प्रभावी प्रबंधन विनियमित संस्थाओं (आरई) के जोखिम प्रबंधन ढांचे का एक अभिन्न अंग है। परिचालन जोखिम का सुदृढ़ प्रबंधन आरई के उत्पादों, सेवाओं, गतिविधियों, प्रक्रियाओं और प्रणालियों के पोर्टफोलियो को प्रशासित करने में निदेशक मंडल और वरिष्ठ प्रबंधन की समग्र प्रभावशीलता को दर्शाता है।

1.2 परिचालन संबंधी व्यवधान आरई की व्यवहार्यता को खतरे में डाल सकता है, इसके ग्राहकों और अन्य बाजार सहभागियों को प्रभावित कर सकता है और अंततः वित्तीय स्थिरता को प्रभावित कर सकता है। यह मानव निर्मित कारणों, सूचना प्रौद्योगिकी (आईटी) खतरों (उदाहरण के लिए, साइबर हमले, प्रौद्योगिकी में परिवर्तन, प्रौद्योगिकी विफलताएं, आदि), भू-राजनीतिक संघर्ष, व्यापार व्यवधान, आंतरिक/बाहरी धोखाधड़ी, निष्पादन/वितरण त्रुटियों, तृतीय पक्ष पर निर्भरता, या प्राकृतिक कारण (जैसे, जलवायु परिवर्तन, महामारी, आदि) के परिणामस्वरूप हो सकता है।

1.3 एक आरई को जोखिमों के संपूर्ण आयाम (अपनी जोखिम मूल्यांकन नीतियों/प्रक्रियाओं में उपर्युक्त जोखिमों सहित) को ध्यान में रखना होगा, उचित उपकरणों का उपयोग करके उनकी पहचान करना और उनका आकलन करना होगा, इसके भौतिक परिचालन जोखिमों की निगरानी करनी होगी और परिचालन संबंधी व्यवधानों को कम करने और महत्वपूर्ण कार्यों को जारी रखने के लिए मजबूत आंतरिक नियंत्रणों का उपयोग करके उचित जोखिम शमन/प्रबंधन रणनीतियां तैयार करना होगा, जिससे कि परिचालन आघात-सहनीयता सुनिश्चित हो सके।

1.4 अब तक, आरई को जिन प्रमुख परिचालन जोखिमों का सामना करना पड़ता था, वे बढ़ती निर्भरता और वित्तीय सेवाओं और मध्यस्थता के प्रावधान के लिए प्रौद्योगिकी को तेजी से अपनाने से

विनियमन विभाग, केंद्रीय कार्यालय, केंद्रीय कार्यालय भवन, 12वीं/13वीं मंजिल, शहीद भगत सिंह मार्ग, फोर्ट, मुंबई – 400001
टेलीफोन/ Tel No: 22661602, 22601000 फैक्स/ Fax No: 022-2270 5691 Email: cgmicdor@rbi.org.in
Department of Regulation, Central Office, Central Office Building, 12th/ 13th Floor, Shahid Bhagat Singh Marg, Fort, Mumbai – 400001

संबंधित दोष पूर्णता के कारण उत्पन्न होते थे। तथापि, वित्तीय क्षेत्र की तृतीय-पक्ष प्रदाताओं (प्रौद्योगिकी सेवा प्रदाताओं सहित) पर बढ़ती निर्भरता, जो कि आभासी कामकाजी व्यवस्थाओं पर अधिक निर्भरता के साथ कोविड-19 महामारी के कारण बढ़ गई है, ने परिचालन जोखिम प्रबंधन और परिचालन आघात-सहनीयता के बढ़ते महत्व को उजागर किया है; जो न केवल एक व्यवहार्य चालू संस्था बने रहने की क्षमता को मजबूत करके आरई को लाभ पहुंचाता है, बल्कि किसी भी व्यवधान के दौरान महत्वपूर्ण कार्यों की निरंतर डिलीवरी सुनिश्चित करके वित्तीय प्रणाली का समर्थन करता हैं।

1.5 पूर्वोक्त को ध्यान में रखते हुए, रिज़र्व बैंक, परिचालन जोखिम प्रबंधन और परिचालन आघात-सहनीयता पर इस मार्गदर्शी नोट (इसके बाद 'मार्गदर्शी नोट') के माध्यम से यह अभिप्रेत करना चाहता है कि:

1.5.1 आरई के परिचालन जोखिम प्रबंधन की प्रभावशीलता को बढ़ावा देना और इसमें और सुधार करना, और

1.5.2 वित्तीय प्रणाली के भीतर अंतर्संबंधों और अन्योन्याश्रितताओं को देखते हुए, जो उस जटिल और गतिशील परिस्थिति से उत्पन्न होता है जिसमें आरई संचालित होते हैं, उनके परिचालन आघात-सहनीयता को बढ़ाना ।

1.6 यह मार्गदर्शी नोट 14 अक्टूबर 2005 के "परिचालन जोखिम के प्रबंधन पर मार्गदर्शी नोट" को अद्यतन करता है। इसे मार्च 2021 में जारी बैंकिंग पर्यवेक्षण पर बासल समिति (बीसीबीएस) सिद्धांतों, अर्थात, (ए) ' परिचालन जोखिम के सुदृढ़ प्रबंधन के लिए संशोधित सिद्धांतों' और (बी) 'परिचालन आघात-सहनीयता के सिद्धांतों' के साथ-साथ कुछ अंतरराष्ट्रीय सर्वोत्तम प्रथाओं के आधार पर तैयार किया गया है ।

1.7 मार्गदर्शी नोट एक सिद्धांत-आधारित और आनुपातिक दृष्टिकोण अपनाता है ताकि विभिन्न आकार, प्रकृति, जटिलता, भौगोलिक स्थिति और उनके व्यवसायों के जोखिम प्रोफाइल के आरई में सुचारु कार्यान्वयन सुनिश्चित किया जा सके। यद्यपि सटीक दृष्टिकोण एक आरई से दूसरी आरई में भिन्न हो सकता है, अपितु मार्गदर्शी नोट आरई को उनके परिचालन जोखिम प्रबंधन ढांचे (ओआरएमएफ) को बेहतर बनाने और मजबूत करने के लिए एक व्यापक मार्गदर्शन प्रदान करता है। यह आरई को परिचालन जोखिम प्रबंधन के लिए पर्याप्त लचीलापन देता है ताकि संभावित परिचालन व्यवधानों का सामना करने, अनुकूलन करने और उनसे उबरने की उनकी क्षमता बढ़ सके और उनका परिचालन आघात-सहनीयता सुनिश्चित हो सके। इस मार्गदर्शी नोट में निर्धारित प्रणालियाँ, प्रक्रियाएँ और साधन सांकेतिक प्रकृति के हैं और इन्हें रिज़र्व बैंक द्वारा समय-समय पर जारी किए गए प्रासंगिक विनिर्देशों

के साथ संयोजन में पढ़ा जाना चाहिए। यदि कोई असंगतता हो तो रिज़र्व बैंक द्वारा जारी प्रासंगिक विनिर्देश मान्य होंगे।

1.8 परिचालन जोखिम विनियामक पूंजी आवश्यकताएं लागू दिशानिर्देशों [1] द्वारा निर्देशित होती रहेंगी।

2. प्रयोज्यता

2.1 यह मार्गदर्शी नोट निम्नलिखित आरई पर लागू होगा:

2.1.1 सभी वाणिज्यिक बैंक[2];

2.1.2 सभी प्राथमिक (शहरी) सहकारी बैंक/राज्य सहकारी बैंक/केंद्रीय सहकारी बैंक;

2.1.3 सभी अखिल भारतीय वित्तीय संस्थान (जैसे, एक्ज़िम बैंक, नाबार्ड, एनएचबी, सिडबी और एनएबीएफआईडी); और

2.1.4 आवास वित्त कंपनियों सहित सभी गैर-बैंकिंग वित्तीय कंपनियां।

3. निरसन और संक्रमणकालीन व्यवस्था

इस मार्गदर्शी नोट के जारी होने के साथ ही 14 अक्टूबर 2005 का "परिचालन जोखिम प्रबंधन पर मार्गदर्शी नोट" निरस्त हो जाएगा।

4. मुख्य परिवर्तन

निरस्त मार्गदर्शी नोट की तुलना में इस मार्गदर्शी नोट में किए गए मुख्य परिवर्तन **अनुबंध** में दिए गए हैं।

भवदीय,

(सुनील टी.एस. नायर)
मुख्य महाप्रबंध

---

[1] बैंकों के लिए परिचालन जोखिम पूंजी गणना का दृष्टिकोण समय-समय पर संशोधित 1 अप्रैल, 2024 के "मास्टर परिपत्र - बासल III पूंजी विनियमन" में उल्लिखित है। हालाँकि, लघु वित्त बैंक, भुगतान बैंक, क्षेत्रीय ग्रामीण बैंक, स्थानीय क्षेत्र बैंक, एनबीएफसी और सहकारी बैंकों जैसे आरई को परिचालन जोखिम के लिए अलग विनियामक पूंजी बनाए रखने की आवश्यकता नहीं है।

[2] "वाणिज्यिक बैंकों" का अर्थ है बैंकिंग विनियमन अधिनियम, 1949 की धारा 5 की उपधारा (सी), (डीए), (जेए) और (एनसी) के तहत परिभाषित सभी बैंकिंग कंपनियां, संबंधित नए बैंक, क्षेत्रीय ग्रामीण बैंक और भारतीय स्टेट बैंक। इसमें भारत के बाहर निगमित और भारत में संचालन के लिए लाइसेंस प्राप्त बैंक ('विदेशी बैंक'), स्थानीय क्षेत्र बैंक, भुगतान बैंक और लघु वित्त बैंक भी शामिल हैं।

परिचालन जोखिम प्रबंधन और परिचालन आघात-सहनीयता पर मार्गदर्शी नोट

अनुसूची

1. प्रस्तावना

1.1 परिचय

1.1.1 वैश्विक वित्तीय संकट ने दुनिया भर में वित्तीय स्थिरता को बहुत प्रभावित किया। इस तथ्य को देखते हुए कि संकट का प्रभाव बैंकों द्वारा परिकल्पित सभी परिदृश्यों की तुलना में बहुत अधिक गंभीर थे, बैंकों/वित्तीय संस्थानों की वित्तीय आघात-सहनीयता को मजबूत करने के लिए कई संरचनात्मक परिवर्तन किए गए। यद्यपि पूंजी और तरलता आवश्यकताओं ने बैंकों की प्रघात सहने की क्षमता में सुधार किया है, बैंकिंग पर्यवेक्षण पर बासल समिति (बीसीबीएस) का विचार था कि वित्तीय प्रणाली को अतिरिक्त सुरक्षा उपाय प्रदान करने के लिए परिचालन जोखिम प्रबंधन के क्षेत्र में और अधिक काम करने की आवश्यकता है।

1.1.2 बीसीबीएस ने 2001 में ऋण और बाजार जोखिमों के बाहर, परिचालन जोखिम को जोखिम के एक विशिष्ट वर्ग के रूप में मान्यता दी और 2003 में परिचालन जोखिम के प्रबंधन और पर्यवेक्षण के लिए ठोस प्रथाओं को लाया गया। इसके बाद, इन सिद्धांतों को 2011 में संशोधित किया गया था, ताकि 2007-08 के महान वित्तीय संकट से सीखे गए पाठ को शामिल किया जा सके। 2014 में, इन सिद्धांतों के कार्यान्वयन की समीक्षा यह आकलन करने के लिए की गई थी कि बैंकों द्वारा इन सिद्धांतों को किस सीमा तक लागू किया है, उनके कार्यान्वयन में महत्वपूर्ण कमियां, यदि कोई हो, की पहचान करना, और बैंकों में उभरती और उल्लेखनीय परिचालन जोखिम प्रबंधन प्रथाएं जिन्हें इन सिद्धांतों में शामिल किया जा सकता है उन्हें उजागर करना था। यह भी पाया गया कि कई सिद्धांतों को अभी तक पर्याप्त रूप से लागू नहीं किया गया है, तथा जोखिम पहचान और मूल्यांकन साधन, प्रमुख जोखिम संकेतक, व्यवसाय प्रक्रिया मानचित्रण, कार्य योजनाओं की निगरानी, परिवर्तन प्रबंधन कार्यक्रम और प्रक्रियाएं, सुरक्षा का त्री-स्तरीय कार्यान्वयन, निदेशक मंडल और वरिष्ठ प्रबंधन द्वारा निरीक्षण, परिचालन जोखिम की उत्कटता और सहिष्णुता विवरणों का ग्रंथन, जोखिम प्रकटीकरण, आदि जैसे क्षेत्रों में उनके कार्यान्वयन की सुविधा के लिए अधिक मार्गदर्शन की आवश्यकता थी। बीसीबीएस ने यह भी माना कि 2011 के सिद्धांतों ने परिचालन जोखिम के कुछ महत्वपूर्ण स्रोतों जैसे कि सूचना और संचार प्रौद्योगिकी (आईसीटी) जोखिम से उत्पन्न होने वाले जोखिम को पर्याप्त रूप से शामिल नहीं किया है।

1.1.3 इसके बाद, कोविड-19 महामारी के कारण सूचना प्रणालियों, कार्मिकों, सुविधाओं, तृतीय-पक्ष सेवा प्रदाताओं और ग्राहकों के साथ संबंधों को प्रभावित करने वाले व्यवधान उत्पन्न हुए। इसने आभासी कार्य व्यवस्था पर अधिक निर्भरता के परिप्रेक्ष्य में प्रौद्योगिकी पर उनकी बढ़ती माँगों को देखते हुए बैंकों के संचालन के तरीके को बदल दिया। इसके अलावा, साइबर खतरों (रैनसमवेयर हमले, फ़िशिंग, आदि) की घटनाओं में वृद्धि हुई, और लोगों, विफल प्रक्रियाओं और प्रणालियों के कारण होने वाले

परिचालन जोखिम की घटनाओं के साकार होने की संभावना बढ़ गई, जिससे बैंकों के परिचालन आघात-सहनीयता का परीक्षण हुआ।

1.1.4 इस परिप्रेक्ष्य में, बीसीबीएस ने महसूस किया कि महामारी, साइबर घटनाओं, प्रौद्योगिकी विफलताओं और प्राकृतिक आपदाओं जैसी परिचालन जोखिम संबंधी घटनाओं का सामना करने के लिए बैंकों की क्षमता को मजबूत करने के लिए और काम करना आवश्यक है, जो महत्वपूर्ण परिचालन विफलताओं या वित्तीय बाज़ारों में व्यापक व्यवधान का कारण बन सकते हैं। यह इस पृष्ठभूमि में है, कि बीसीबीएस 2021 में अद्यतन 'परिचालन जोखिम के सुदृढ़ प्रबंधन के लिए सिद्धांत' लेकर आया। इसके अतिरिक्त, यह बैंकों की सहनशीलता, अनुकूलन करने की क्षमता बढ़ाने के लिए 'परिचालन आघात-सहनीयता पर सिद्धांत' भी लेकर आया ताकि संभावित खतरों से उबरा जा सके।

1.2 पृष्ठभूमि

1.2.1 जोखिम की पहचान, मात्रा निर्धारण और शमन के परिप्रेक्ष्य में परिचालन जोखिम एक जटिल जोखिम श्रेणी है। यह कई कारकों से प्रभावित होता है जैसे आंतरिक व्यावसायिक प्रक्रियाएं, नियामक परिदृश्य, व्यवसाय वृद्धि, ग्राहक प्राथमिकताएं और यहां तक कि संगठन के बाहरी कारक भी है। यह प्रकृति में अत्यधिक गतिशील है जहां नई और उभरती ताकतें जैसे कि सफल प्रौद्योगिकियां, डेटा उपलब्धता, नए व्यापार मॉडल, तृतीय पक्ष के साथ इंटरैक्शन आदि, के कारण लगातार परिचालन जोखिम प्रबंधन ढांचे (ओआरएमएफ) पर नई अपेक्षाएँ निर्माण होती रहती हैं।

1.2.2 जबकि परिचालन जोखिम प्रबंधन एक आरई को परिचालन जोखिमों को बेहतर ढंग से पहचानने, आकलन करने और उसे कम करने की अनुज्ञा देता है, परिचालन आघात-सहनीयता इसे किसी भी व्यवधान की स्थिति में महत्वपूर्ण कार्य प्रदान करने की क्षमता प्रदान करता है। हालाँकि परिचालन जोखिम प्रबंधन और परिचालन आघात-सहनीयता अलग-अलग लक्ष्यों का समाधान करते हैं, लेकिन वे आपस में घनिष्ठ रूप से जुड़े हुए हैं। एक प्रभावी परिचालन जोखिम प्रबंधन प्रणाली और परिचालन आघात-सहनीयता का एक मजबूत स्तर एक साथ काम करता है ताकि परिचालन जोखिम की घटनाओं की आवृत्ति और प्रभाव को कम किया जा सके। उपरोक्त को ध्यान में रखते हुए, रिज़र्व बैंक का इस मार्गदर्शी नोट के माध्यम से परिचालन जोखिम प्रबंधन को प्रोत्साहित करने और आरई के परिचालन आघात-सहनीयता को बढ़ाने का अभिप्राय है।

1.2.3 परिचालन जोखिम प्रबंधन और परिचालन आघात-सहनीयता पर यह मार्गदर्शन नोट तीन स्तंभों पर बनाया गया है। वे तीन स्तंभ हैं:

(i) तैयारी और सुरक्षा

(ii) आघात-सहनीयता निर्मिति

(iii) सीखना और अनुकूलन

इन स्तंभों के व्यापक क्षेत्र या विषय

परिचालन जोखिम प्रबंधन और परिचालन आघात-सहनीयता पर मार्गदर्शी नोट

स्तंभ 1: **तैयारी और सुरक्षा**	**स्तंभ 2:** **आघात-सहनीयता निर्मिति**	**स्तंभ 3:** **सीखना और अनुकूलन**
• **अभिशासन और जोखिम संस्कृति**	• व्यवसाय निरंतरता योजना और परीक्षण	• प्रकटीकरण और रिपोर्टिंग
• **निदेशक मंडल और वरिष्ठ प्रबंधन की जिम्मेदारियां**	• अंतर्संबंधों और अन्योन्याश्रितताओं का मानचित्रण	• पाठ से सीख अभ्यास और अनुकूलन
• **जोखिम प्रबंधन: पहचान और मूल्यांकन** • **परिवर्तन प्रबंधन**	• तृतीय पक्ष निर्भरता प्रबंधन	• प्रतिसूचना प्रणाली के माध्यम से निरंतर सुधार
• **निगरानी एवं रिपोर्टिंग**	• घटना प्रबंधन	
• **नियंत्रण एवं शमन**	• साइबर सुरक्षा सहित आईसीटी	

1.2.4 ये तीन स्तंभ परिचालन जोखिम और परिचालन आघात-सहनीयता के प्रबंधन के लिए एक समग्र दृष्टिकोण का समर्थन करते हैं और एक प्रतिसूचना प्रणाली बनाते हैं जो परिचालन संबंधी व्यवधानों के

लिए आरई की तैयारी और व्यवधानों की वास्तविक घटना के दौरान इसके प्रदर्शन से प्राप्त अनुभवों को सतत रूप से शामिल करने को बढ़ावा देता है।

इन तीन स्तंभों में, मार्गदर्शी नोट में 17 सिद्धांत शामिल हैं जिनका विवरण इसके बाद पैराग्राफ 4-18 में दिया गया है।

2. परिभाषाएँ

2.1 **"व्यावसायिक इकाई"** उन उत्पादों, सेवाओं, गतिविधियों, प्रक्रियाओं और प्रणालियों में निहित जोखिमों की पहचान और प्रबंधन के लिए उत्तरदायी है जिसके लिए वह जवाबदेह है और इसमें सभी संबद्ध सहायता, कॉर्पोरेट और/या साझा सेवा कार्य, जैसे, वित्त, मानव संसाधन, तथा परिचालन और प्रौद्योगिकी शामिल हैं। इसमें जोखिम प्रबंधन और आंतरिक लेखापरीक्षा कार्य शामिल नहीं हैं जब तक कि अन्यथा विशेष रूप से उल्लिखित न किया गया हो।

2.2 "**महत्वपूर्ण परिचालन"** महत्वपूर्ण कार्यों[3], गतिविधियों, प्रक्रियाओं, सेवाओं और उनकी प्रासंगिक सहायक आस्तियों[4] को संदर्भित करता है, इनमें व्यवधान होने से यह आरई के निरंतर संचालन या वित्तीय प्रणाली में इसकी भूमिका को प्रभावित करेगा। कोई परिचालन "महत्वपूर्ण" है या नहीं, यह आरई की प्रकृति और वित्तीय प्रणाली में इसकी भूमिका पर निर्भर करता है। आरई की व्यवधान सहनशीलता को महत्वपूर्ण परिचालन स्तर पर लागू किया जाना चाहिए।

2.3 **"आकस्मिकता प्रबंधन"** एक परिचालन जोखिम घटना की पहचान, विश्लेषण, एंड-टू-एंड प्रबंधन और रिपोर्टिंग की प्रक्रिया है जो प्रोटोकॉल के पूर्व-निर्धारित सेट का पालन करती है।

2.4 **"घटना"** वर्तमान या अतीत की विघटनकारी घटनाएँ हैं जिनके घटित होने से आरई के महत्वपूर्ण कार्यों पर प्रतिकूल प्रभाव पड़ेगा। घटना प्रबंधन किसी घटना (साइबर घटना सहित) की पहचान करने, विश्लेषण करने, सुधार करने और उससे सीखने और पुनरावृत्ति को रोकने या उसकी गंभीरता को कम करने की प्रक्रिया है। घटना प्रबंधन का लक्ष्य व्यवधान को सीमित करना और व्यवधान के लिए आरई की जोखिम सहनशीलता के अनुरूप महत्वपूर्ण परिचालन को बहाल करना है।

---

[3] वित्तीय स्थिरता बोर्ड (एफएसबी) के अनुसार, महत्वपूर्ण कार्यों को "तृतीय पक्ष के लिए की जाने वाली गतिविधियाँ के रूप में परिभाषित किया गया है, इनके असफल होने पर उन सेवाओं में व्यवधान उत्पन्न होगा जो वास्तविक अर्थव्यवस्था के कामकाज और आरई के समूह आकार या बाजार हिस्सेदारी, बाहरी और आंतरिक अंतर्संबंध, जटिलता और सीमा पार गतिविधियां के कारण वित्तीय स्थिरता के लिए महत्वपूर्ण हैं। उदाहरणों में वाणिज्यिक या खुदरा क्षेत्र में भुगतान, निगरानी, कुछ उधार और जमा लेने की गतिविधियां, समाशोधन और निपटान, थोक बाजारों के सीमित खंड, कुछ प्रतिभूतियों में बाजार बनाना और अत्यधिक केंद्रित विशेषज्ञ उधार क्षेत्र शामिल हैं।" (एफएसबी का मार्गदर्शन 'प्रणालीगत रूप से महत्वपूर्ण वित्तीय संस्थानों के लिए पुनर्प्राप्ति और समाधान योजना: महत्वपूर्ण कार्यों और महत्वपूर्ण साझा सेवाओं की पहचान पर मार्गदर्शन', दिनांक 16 जुलाई, 2013)।

[4] इस संदर्भ में, "सहायक आस्तियों" को महत्वपूर्ण कार्यों के वितरण के लिए आवश्यक व्यक्तियों, प्रौद्योगिकी, सूचना और सुविधाओं के रूप में परिभाषित किया गया है।

2.5 "सूचना और संचार प्रौद्योगिकी"[5] सूचना प्रौद्योगिकी और संचार प्रणालियों, व्यक्तिगत हार्डवेयर और सॉफ्टवेयर घटकों, डेटा और ऑपरेटिंग परिवेश के अंतर्निहित भौतिक और तार्किक डिजाइन को संदर्भित करता है।

2.6 "मैपिंग" महत्वपूर्ण परिचालन प्रदान करने में शामिल गतिविधियों की श्रृंखला की पहचान करने, दस्तावेजीकरण करने और समझने की प्रक्रिया है। इसमें व्यक्तियों, प्रक्रियाओं, प्रौद्योगिकी और तृतीय पक्षों सहित सभी अन्योन्याश्रितताओं और अंतर्संबंधों की पहचान शामिल है।

2.7 "परिचालन आघात-सहनीयता" का अर्थ व्यवधान की स्थिति में महत्वपूर्ण संचालन प्रदान करने की आरई की क्षमता है। यह क्षमता आरई को खतरों और संभावित विफलताओं से खुद को पहचानने और बचाने, प्रतिक्रिया देने और अनुकूलन करने के साथ-साथ विघटनकारी घटनाओं से उबरने और सीखने में सक्षम बनाती है ताकि व्यवधान की स्थिति में महत्वपूर्ण संचालन के वितरण पर उनके प्रभाव को कम किया जा सके। अपने परिचालन आघात-सहनीयता पर विचार करते समय, आरई को यह मान लेना चाहिए कि व्यवधान उत्पन्न होंगे, और व्यवधान या प्रभाव सहनशीलता के लिए अपनी समग्र जोखिम स्वीकार्यता और सहनशीलता को ध्यान में रखना चाहिए।

2.8 "परिचालन जोखिम" का अर्थ अपर्याप्त या असफल आंतरिक प्रक्रियाओं, लोगों और प्रणालियों या बाहरी घटनाओं के परिणामस्वरूप होने वाले नुकसान का जोखिम है। इसमें कानूनी जोखिम शामिल है लेकिन रणनीतिक और प्रतिष्ठा जोखिम शामिल नहीं है और यह सभी बैंकिंग/वित्तीय उत्पादों, गतिविधियों, प्रक्रियाओं और प्रणालियों में अंतर्निहित है।

2.9 "परिचालन जोखिम प्रबंधन" परिचालन जोखिम प्रबंधन जोखिम की पहचान, माप और मूल्यांकन, निगरानी और नियंत्रण, शमन, आरई के जोखिम एक्सपोजर पर वरिष्ठ प्रबंधन और निदेशक मंडल को रिपोर्ट करने, व्यवसाय निरंतरता प्रबंधन और सुधार के लिए फीडबैक के माध्यम से सीखने से लेकर गतिविधियों के संपूर्ण दायरे को संदर्भित करता है।

2.10 "परिचालन जोखिम प्रोफाइल" आरई की व्यावसायिक इकाइयों के परिचालन जोखिम एक्सपोजर और नियंत्रण पर्यावरण आकलन का वर्णन करता है और यह संभावित प्रभावों की श्रृंखला पर विचार करता है जो संभावित गंभीर नुकसान के अनुमान से उत्पन्न हो सकते हैं।

2.11 "विनियमित संस्थाएं" (आरई) नीचे उल्लिखित संस्थाओं को संदर्भित करती है:

2.11.1 सभी वाणिज्यिक बैंक[6];

[5] राष्ट्रीय मानक एवं प्रौद्योगिकी संस्थान (एनआईएसटी), यूएसए के अनुसार, सूचना एवं संचार प्रौद्योगिकी (आईसीटी) में डेटा और सूचना के संग्रहण, भंडारण, पुनर्प्राप्ति, प्रसंस्करण, प्रदर्शन, प्रतिनिधित्व, संगठन, प्रबंधन, सुरक्षा, स्थानांतरण और आदान-प्रदान के लिए सभी प्रौद्योगिकियां शामिल हैं।

2.11.2 सभी प्राथमिक (शहरी) सहकारी बैंक/राज्य सहकारी बैंक/केंद्रीय सहकारी बैंक;

2.11.3 सभी अखिल भारतीय वित्तीय संस्थान (एआईएफआई) (अर्थात, एक्ज़िम बैंक, नाबार्ड, एनएचबी, सिडबी और एनएबीएफआईडी); और

2.11.4 आवास वित्त कंपनियों सहित सभी गैर-बैंकिंग वित्तीय कंपनियां (एनबीएफसी)।

2.12 "**संबंधित कार्य"** आरई की त्री-स्तरीय कार्यप्रणाली में उपयुक्त कार्य को संदर्भित करता है, जो हैं (i) व्यावसायिक इकाई प्रबंधन; (ii) अनुपालन कार्य सहित एक स्वतंत्र परिचालन जोखिम प्रबंधन; और (iii) लेखापरीक्षा कार्य।

2.13 "**जोखिम स्वीकार्यता"** समग्र स्तर और जोखिम के प्रकार हैं जिन्हें एक आरई अपने रणनीतिक उद्देश्यों और व्यवसाय योजना को प्राप्त करने के लिए, पहले से और अपनी जोखिम क्षमता के भीतर स्वीकार करने के लिए तैयार है[7]।

2.14 "जोखिम सहनशीलता" निर्धारित जोखिम क्षमता की निकटवर्तीय भिन्नता है जिसे आरई वहन करने को तैयार है।

2.15 "**पर्यवेक्षी प्राधिकरण"** का अर्थ है,

2.15.1 वाणिज्यिक बैंकों (स्थानीय क्षेत्र बैंकों, भुगतान बैंकों, लघु वित्त बैंकों और प्राथमिक शहरी सहकारी बैंकों सहित), गैर-बैंकिंग वित्तीय कंपनियों और अखिल भारतीय वित्तीय संस्थानों के मामले में भारतीय रिज़र्व बैंक।

2.15.2 राज्य सहकारी बैंकों, केंद्रीय सहकारी बैंकों और क्षेत्रीय ग्रामीण बैंकों के मामले में राष्ट्रीय कृषि और ग्रामीण विकास बैंक (नाबार्ड)।

2.15.3 आवास वित्त कंपनियों के मामले में राष्ट्रीय आवास बैंक (एनएचबी)।

2.16 "**व्यवधान के प्रति सहनशीलता या प्रभाव सहनशीलता "** किसी भी प्रकार के परिचालन जोखिम से व्यवधान का स्तर है जिसे आरई कठिन लेकिन संभावित परिदृश्यों की एक श्रृंखला को स्वीकार करने के लिए तैयार है।

---

[6] "वाणिज्यिक बैंकों" का अर्थ है बैंकिंग विनियमन अधिनियम, 1949 की धारा 5 की उपधारा (सी), (डीए), (जेए) और (एनसी) के तहत परिभाषित सभी बैंकिंग कंपनियां, संबंधित नए बैंक, क्षेत्रीय ग्रामीण बैंक और भारतीय स्टेट बैंक। इसमें भारत में संचालन के लिए लाइसेंस प्राप्त भारत से बाहर निगमित बैंक ('विदेशी बैंक'), स्थानीय क्षेत्र बैंक, भुगतान बैंक और लघु वित्त बैंक भी शामिल हैं।

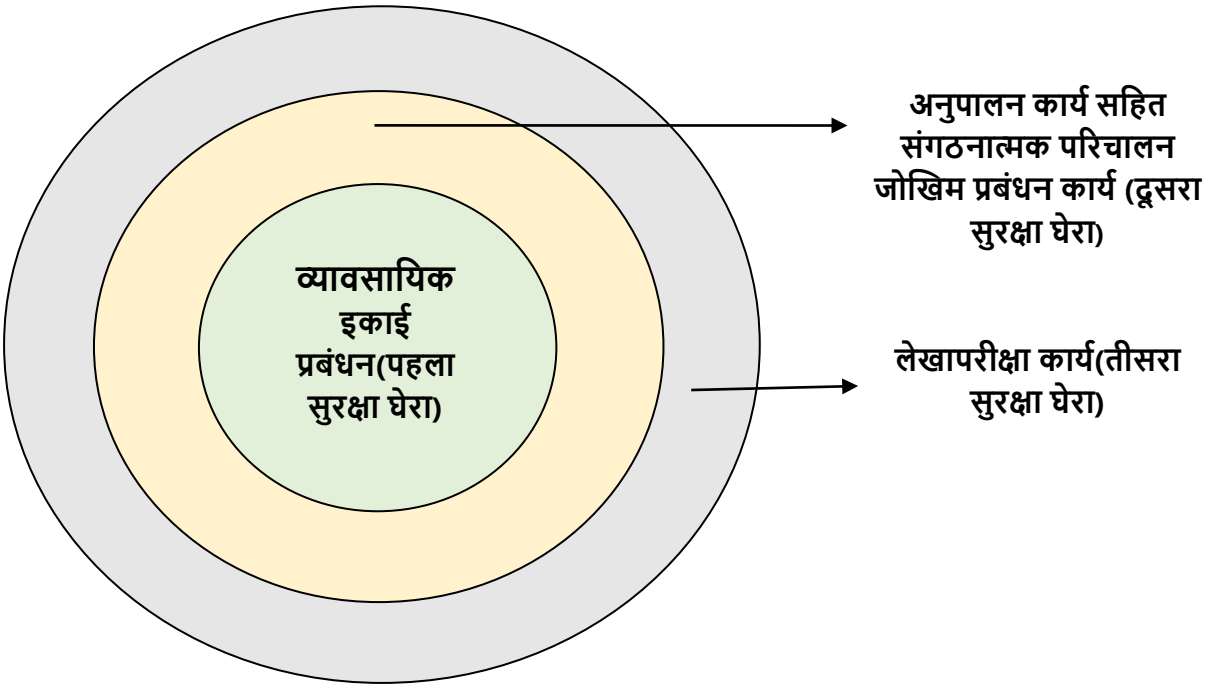
[7] "जोखिम क्षमता" को बीसीबीएस के 2015 कॉर्पोरेट प्रशासन दिशानिर्देशों में परिभाषित किया गया है, जो प्रभावी जोखिम क्षमता ढांचे के लिए एफएसबी के 2013 सिद्धांतों का उपयोग करते हैं।

स्तंभ I: तैयारी और सुरक्षा

3. परिचालन जोखिम के प्रबंधन के लिए की त्रिस्तरीय व्यवस्था

3.1 एक प्रभावी ओआरएमएफ की नींव सुदृढ़ आंतरिक अभिशासन बनाता है। आरई के परिचालन जोखिम अभिशासन कार्य को उनके समग्र जोखिम प्रबंधन अभिशासन ढांचे में पूरी तरह से एकीकृत किया जाना चाहिए। इस उद्देश्य के लिए आरई अपने मौजूदा जोखिम प्रबंधन कार्यों का लाभ उठा सकते हैं।

3.2 ओआरएमएफ के एक भाग के रूप में, आरई त्रिस्तरीय सुरक्षा घेरों पर निर्भर रहेंगे:



3.2.1 पहला सुरक्षा घेरा

3.2.1.1 व्यावसायिक इकाई प्रबंधन आमतौर पर सुरक्षा का पहला घेरा बनाता है। सुदृढ़ परिचालन जोखिम अभिशासन यह मानता है कि व्यावसायिक इकाई प्रबंधन उन उत्पादों, सेवाओं, गतिविधियों, प्रक्रियाओं और प्रणालियों में निहित जोखिमों की पहचान और उनका प्रबंधन करने के लिए जिम्मेदार है जिनके लिए वह उत्तरदायी है। आरई के पास ऐसी नीति होनी चाहिए जो संबंधित व्यावसायिक इकाइयों की स्पष्ट भूमिकाएं और जिम्मेदारियां परिभाषित करती हो। एक सुदृढ़ परिचालन जोखिम प्रबंधन संस्कृति को बढ़ावा देने में सुरक्षा के लिए प्रभावी पहले घेरे की जिम्मेदारियों में यह शामिल होना चाहिए:

(i) परिचालन जोखिम प्रबंधन साधन के उपयोग के माध्यम से अपने संबंधित व्यावसायिक इकाइयों में निहित परिचालन जोखिमों की भौतिकता की पहचान करना और उसका आकलन करना;

(ii) अंतर्निहित परिचालन जोखिमों को कम करने के लिए उचित नियंत्रण स्थापित करना और परिचालन जोखिम प्रबंधन उपकरणों के उपयोग के माध्यम से इन नियंत्रणों के डिजाइन और प्रभावशीलता का आकलन करना;

(iii) इसकी रिपोर्ट करना कि परिचालन जोखिमों की पहचान और आकलन सुनिश्चित करने के लिए व्यावसायिक इकाइयों के पास पर्याप्त संसाधन, उपकरण और प्रशिक्षण का अभाव है;

(iv) व्यावसायिक इकाइयों की परिचालन जोखिम प्रोफाइल की निगरानी और रिपोर्टिंग, तथा स्थापित परिचालन जोखिम स्वीकार्यता और सहनशीलता विवरण का पालन सुनिश्चित करना; और

(v) परिचालन हानि की घटनाओं, नियंत्रण की कमियों, प्रक्रिया की अपर्याप्तता और परिचालन जोखिम सहनशीलता के साथ गैर-अनुपालन सहित नियंत्रणों द्वारा कम नहीं किए गए अवशेष परिचालन जोखिमों की रिपोर्टिंग।

3.2.2 दूसरा सुरक्षा घेरा

3.2.2.1 कार्यात्मक रूप से स्वतंत्र संगठनात्मक परिचालन जोखिम प्रबंधन कार्य (ओओआरएफ) सुरक्षा का दूसरा घेरा बनाता है। एक सुदृढ़ परिचालन जोखिम प्रबंधन की संस्कृति को बढ़ावा देने में सुरक्षा की एक प्रभावी दूसरे के घेरे की जिम्मेदारियों में शामिल होना चाहिए:

(i) व्यावसायिक इकाइयों के संबंध में एक स्वतंत्र दृष्टिकोण विकसित करना (ए) पहचाने गए महत्त्वपूर्ण परिचालन जोखिम, (बी) प्रमुख नियंत्रणों का डिज़ाइन और प्रभावशीलता, और (सी) जोखिम सहनशीलता ;

(ii) परिचालन जोखिम प्रबंधन साधन, माप गतिविधियों और रिपोर्टिंग प्रणालियों के व्यावसायिक इकाई के कार्यान्वयन की प्रासंगिकता और स्थिरता को चुनौती देना और इस प्रभावी चुनौती का साक्ष्य प्रदान करना;

(iii) परिचालन जोखिम प्रबंधन और माप नीतियों, मानकों और दिशानिर्देशों का विकास और रखरखाव;

(iv) परिचालन जोखिम प्रोफ़ाइल की निगरानी और रिपोर्टिंग में समीक्षा और योगदान करना; और

(v) परिचालन जोखिम प्रशिक्षण डिजाइन और प्रदान करना तथा जोखिम जागरूकता स्थापित करना।

3.2.2.2 छोटे विनियमित संस्थाओं (अर्थात् इस मार्गदर्शी नोट के प्रयोजन के लिए एनबीएफसी-बेस लेयर और टियर 1 एवं 2 सहकारी बैंक) में, यदि सुरक्षा के पहले और दूसरे घेरे का कार्य एक ही इकाई द्वारा किए जाते हैं, तो कर्तव्यों के पृथक्करण (इस पर जोर देने वाली दस्तावेजी नीतियों और प्रक्रियाओं के साथ) तथा प्रक्रियाओं और कार्यों की स्वतंत्र समीक्षा के माध्यम से स्वतंत्रता प्राप्त की जा सकती है। बड़े आरई (अर्थात छोटे आरई के अतिरिक्त अन्य आरई) में, ओओआरएफ के पास जोखिम उत्पन्न करने वाली व्यावसायिक इकाइयों से स्वतंत्र रिपोर्टिंग संरचना होनी चाहिए और आरई के भीतर ओआरएमएफ के डिजाइन, रखरखाव और चल रहे विकास के लिए जिम्मेदार होना चाहिए। ओओआरएफ आमतौर पर परिचालन जोखिमों और नियंत्रणों के अपने आकलन का समर्थन करने के लिए प्रासंगिक कॉर्पोरेट नियंत्रण समूहों (जैसे, कानूनी, वित्त और आईटी) के साथ-साथ आरई के समग्र जोखिम प्रबंधन कार्य को शामिल करता है। आरई के पास एक नीति होनी चाहिए जो आरओओएफ की भूमिकाओं और जिम्मेदारियों को स्पष्ट रूप से परिभाषित करती हो, जो संगठन के आकार और जटिलता को प्रतिबिंबित करती हो।

3.2.2.3 स्वतंत्र ओआरएमएफ के अतिरिक्त**,** सुरक्षा के दूसरे घेरे में आमतौर पर अनुपालन कार्य भी शामिल होता है।

3.2.3 तीसरा सुरक्षा घेरा

सुरक्षा का तीसरा घेरा, अर्थात् लेखापरीक्षा का कार्य बोर्ड को आरई के ओआरएमएफ की उपयुक्तता के बारे में एक स्वतंत्र आश्वासन प्रदान करना है। इस कार्य के कर्मचारियों को परिचालन जोखिम प्रबंधन प्रक्रियाओं के विकास, कार्यान्वयन और संचालन में शामिल नहीं होना चाहिए जोकि सुरक्षा की अन्य दो घेरों द्वारा किया गया है। सुरक्षा समीक्षा का तीसरा घेरा आमतौर पर आरई के आंतरिक और/अथवा बाहरी लेखापरीक्षा द्वारा की जाती है, लेकिन इसमें उपयुक्त रूप से योग्य स्वतंत्र तृतीय पक्ष भी शामिल हो सकते हैं। समीक्षाओं का दायरा और आवृत्ति न केवल आरई की सभी गतिविधियों और कानूनी संस्थाओं को कवर करने के लिए पर्याप्त होनी चाहिए, बल्कि आरई के परिचालन जोखिम प्रोफ़ाइल के साथ संरेखित होनी चाहिए, और उन प्रमुख जोखिम क्षेत्रों की पहचान और प्राथमिकता देनी चाहिए जो गहन जांच की मांग करते हैं, बल्कि परिचालन जोखिम परिवेश की गतिशील प्रकृति के प्रति उत्तरदायी भी होनी चाहिए। एक प्रभावी स्वतंत्र समीक्षा में दो प्रक्रियाएँ शामिल हैं:

3.2.3.1 वैधीकरण

यह सुनिश्चित करना कि आरई द्वारा उपयोग की जाने वाली परिमाणीकरण प्रणालियाँ पर्याप्त रूप से मजबूत हों क्योंकि (i) वह इनपुट, धारणाओं, प्रक्रियाओं और कार्यप्रणालियों की अखंडता के बारे में

आश्वासन प्रदान करती हैं और (ii) परिचालन जोखिम का ऐसा आकलन करती हैं जो आरई के परिचालन जोखिम प्रोफाइल को विश्वसनीय रूप से दर्शाता है;

3.2.3.2 सत्यापन

(i) परिचालन जोखिम प्रबंधन प्रणालियों (बोर्ड की नीतियों के साथ अनुपालन और निरंतरता सहित) और सुरक्षा के पहले और दूसरे घेरे (सुरक्षा के दूसरे घेरे की स्वतंत्रता सहित) के माध्यम से संबंधित शासन प्रक्रियाओं के डिजाइन और कार्यान्वयन की समीक्षा;

(ii) सत्यापन प्रक्रियाओं की समीक्षा यह सुनिश्चित करने के लिए कि वह स्वतंत्र हैं और स्थापित आरई नीतियों के अनुरूप तरीके से कार्यान्वित की गई हैं;

(iii) यह सुनिश्चित करना कि कारोबार इकाइयों का प्रबंधन उठाए गए मुद्दों पर तुरंत, सटीक तथा पर्याप्त रूप से प्रतिक्रिया दे, और लंबित और बंद मुद्दों पर नियमित रूप से निदेशक मंडल अथवा इसकी संबंधित समितियों को रिपोर्ट करें;

(iv) ओआरएमएफ में यदि कोई कमी हो तो उसकी पहचान करना तथा बोर्ड अथवा उसकी संबंधित समिति को रिपोर्ट करना**;** और

(v) ओआरएमएफ और संबंधित शासन प्रक्रियाओं की समग्र पर्याप्तता और उपयुक्तता पर राय प्रदान करना, यह आकलन करके कि क्या ओआरएमएफ संगठनात्मक आवश्यकताओं और अपेक्षाओं को पूरा करता है (जैसे जोखिम स्वीकार्यता और सहनशीलता के संबंध में और बदलती परिस्थितियों के अनुसार रूपरेखा का समायोजन) और क्या यह वैधानिक और विधायी प्रावधानों, संविदात्मक व्यवस्थाओं, आंतरिक नियमों और नैतिक आचरण का अनुपालन करता है।

3.3 आरई को यह सुनिश्चित करना चाहिए कि सुरक्षा का प्रत्येक घेरा:

3.3.1 भूमिकाएं और जिम्मेदारियां स्पष्ट रूप से परिभाषित करता हैं;

3.3.2 बजट, टूल्स और कर्मचारियों के मामले में पर्याप्त संसाधन उपलब्ध करता हैं;

3.3.3 सतत और पर्याप्त रूप से प्रशिक्षित किया जाता है;

3.3.4 पूरे संगठन में एक सुदृढ़ परिचालन जोखिम प्रबंधन संस्कृति को बढ़ावा देता है; और

3.3.5 ओआरएमएफ को मजबूत करने के लिए सुरक्षा के अन्य घेरे के साथ संचार करता है।

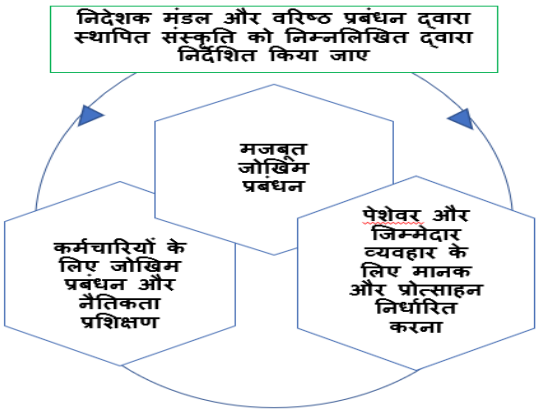
3.4 सुरक्षा की इन घेरों के बीच निर्बाध सहयोग एक मजबूत ढाल बन सकता है, जो न केवल व्यक्तिगत आरई को बल्कि संपूर्ण वित्तीय प्रणाली को संभावित खतरों और कमजोरियों से सुरक्षित रखेगा।

4. अभिशासन और जोखिम संस्कृति

सिद्धांत 1- निदेशक मंडल को एक मजबूत जोखिम प्रबंधन संस्कृति स्थापित करने में अग्रणी भूमिका निभानी चाहिए, जिसे वरिष्ठ प्रबंधन द्वारा कार्यान्वित किया जाना चाहिए। निदेशक मंडल और वरिष्ठ प्रबंधन को मजबूत जोखिम प्रबंधन द्वारा निर्देशित एक कॉर्पोरेट संस्कृति स्थापित करनी चाहिए, पेशेवर और जिम्मेदार व्यवहार के लिए मानक तथा प्रोत्साहन निर्धारित करना चाहिए, और यह सुनिश्चित करना चाहिए कि कर्मचारियों को उचित जोखिम प्रबंधन और नैतिकता प्रशिक्षण मिले।

4.1 जोखिम प्रबंधन और नैतिक व्यावसायिक प्रथाओं की मजबूत संस्कृति वाले आरई को नुकसानदायक परिचालन जोखिम घटनाओं का अनुभव होने की संभावना कम होती है और वह उन घटनाओं से प्रभावी ढंग से निपटने के लिए बेहतर स्थिति में होते हैं। निदेशक मंडल और वरिष्ठ प्रबंधन के कार्यों के साथ-साथ आरई की जोखिम प्रबंधन नीतियां, प्रक्रियाएं और प्रणालियां एक मजबूत जोखिम प्रबंधन संस्कृति के लिए आधार प्रदान करती हैं।

4.2 निदेशक मंडल को आचरण जोखिम के लिए आचार संहिता अथवा नैतिकता नीति स्थापित करनी चाहिए। यह संहिता अथवा नीति कर्मचारियों और बोर्ड के सदस्यों दोनों पर लागू होनी चाहिए। इसमें उच्चतम मानक की ईमानदारी और नैतिक मूल्यों के लिए स्पष्ट अपेक्षाएँ निर्धारित की जानी चाहिए, स्वीकार्य व्यावसायिक प्रथाओं की पहचान की जानी चाहिए, और हितों के टकराव अथवा वित्तीय सेवाओं के अनुचित प्रावधान (जानबूझकर अथवा लापरवाही से) को प्रतिबंधित किया जाना चाहिए। निदेशक मंडल द्वारा इसकी नियमित रूप से समीक्षा तथा अनुमोदन और कर्मचारियों द्वारा प्रमाणित किया जाना चाहिए। इसके कार्यान्वयन की देखरेख एक वरिष्ठ आचार समिति अथवा किसी अन्य बोर्ड-स्तरीय समिति द्वारा की जानी चाहिए, और इसे सार्वजनिक रूप से उपलब्ध होना चाहिए (उदाहरण के लिए आरई की वेबसाइट, शाखा परिसर पर)। आरई में विशिष्ट पदों (उदाहरण के लिए, ट्रेजरी डीलर आदि) के लिए एक अलग आचार संहिता स्थापित की जा सकती है।



4.3 वरिष्ठ प्रबंधन को स्पष्ट अपेक्षाएं निर्धारित करनी चाहिए और जवाबदेही को परिभाषित करना चाहिए ताकि यह सुनिश्चित हो सके कि आरई के कर्मचारी जोखिम प्रबंधन की अपनी भूमिकाओं और जिम्मेदारियों के साथ-साथ कार्य करने के अपने अधिकार को समझें।

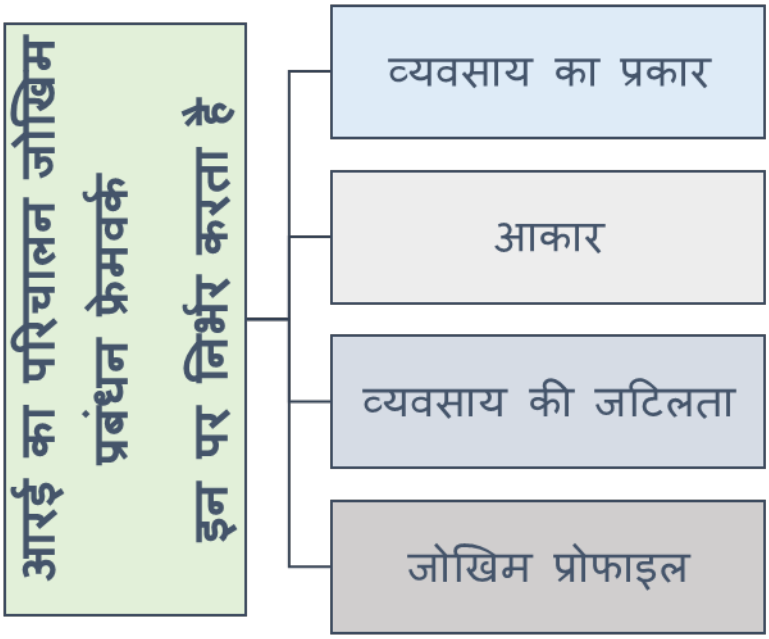
4.4 क्षतिपूर्ति नीतियों को जोखिम प्रबंधन ढांचे की समग्र सुदृढ़ता के साथ-साथ जोखिम और इनाम के उचित संतुलन के साथ आरई के जोखिम स्वीकार्यता और सहनशीलता के विवरण के अनुरूप होना चाहिए। अनुचित प्रोत्साहनों के परिणामस्वरूप मुकदमेबाजी, प्रतिष्ठा जोखिम अथवा आरई के लिए अन्य जोखिम बढ़ सकते हैं। अत: आरई को यह समीक्षा करनी चाहिए कि क्या प्रोत्साहन व्यवस्थाओं से उत्पन्न होने वाले जोखिमों के मद्देनजर उसका मौजूदा अभिशासन और नियंत्रण पर्याप्त है।

4.5 वरिष्ठ प्रबंधन को यह सुनिश्चित करना चाहिए कि संगठन में सभी स्तरों पर परिचालन जोखिम प्रशिक्षण का उचित स्तर उपलब्ध हो, जैसेकि व्यावसायिक इकाइयों के प्रमुख, आंतरिक नियंत्रण के प्रमुख और वरिष्ठ प्रबंधक। जिनके लिए यह अभिप्रेत है, प्रदान किया जाने वाला प्रशिक्षण उन व्यक्तियों की वरिष्ठता, भूमिका और जिम्मेदारियों को दर्शाना चाहिए। इसमें उचित रूप से नैतिकता प्रशिक्षण भी शामिल होना चाहिए।

4.6 परिचालन जोखिम प्रबंधन के लिए निदेशक मंडल और वरिष्ठ प्रबंधन का मजबूत और निरंतर समर्थन और नैतिक व्यवहार के साथ-साथ आचार संहिता और नैतिकता, क्षतिपूर्ति की रणनीतियों आदि को दृढ़तापूर्वक सुदृढ़ करता है।

सिद्धांत 2- आरई को ओआरएमएफ को विकसित, कार्यान्वित और बनाए रखना चाहिए जो आरई की समग्र जोखिम प्रबंधन प्रक्रियाओं में पूरी तरह से एकीकृत हो। किसी व्यक्तिगत आरई द्वारा अपनाया गया ओआरएमएफ इसकी प्रकृति, आकार, जटिलता और जोखिम प्रोफ़ाइल सहित कई कारकों पर निर्भर करेगा। इसके अतिरिक्त, आरई को अपने मौजूदा अभिशासन ढांचे का उपयोग एक प्रभावी परिचालन आघात-सहनीयता दृष्टिकोण स्थापित, उसकी देखरेख और उसे लागू करने के लिए करना चाहिए जो उन्हें व्यवधान कारी घटनाओं का जवाब देने और उनसे अनुकूलन, साथ ही उबरने और सीखने में सक्षम बनाता है ताकि व्यवधान से महत्वपूर्ण संचालन करने पर उनके प्रभाव को कम किया जा सके।

4.7 आरई के निदेशक मंडल और वरिष्ठ प्रबंधन को आरई के नए व्यावसायिक पहलों, उत्पादों, सेवाओं, गतिविधियों, प्रक्रियाओं और प्रणालियों के पोर्टफोलियो में निहित जोखिमों की प्रकृति और जटिलता को समझना चाहिए, जोकि अच्छे जोखिम प्रबंधन का एक बुनियादी आधार है। यह परिचालन जोखिम के लिए विशेष रूप से महत्वपूर्ण है, क्योंकि यह सभी व्यावसायिक उत्पादों, सेवाओं, गतिविधियों, प्रक्रियाओं और प्रणालियों में निहित है।



4.8 ओआरएमएफ के घटकों को आरई की समग्र जोखिम प्रबंधन प्रक्रियाओं में पहला सुरक्षा घेरा द्वारा पूरी तरह से एकीकृत किया जाना चाहिए, द्वितीय सुरक्षा घेरा द्वारा पर्याप्त रूप से चुनौती दी और समीक्षा की जानी चाहिए तथा तीसरे सुरक्षा घेरा द्वारा स्वतंत्र रूप से समीक्षा की जानी चाहिए। ओआरएमएफ को आरई के सभी स्तरों पर समूह और व्यावसायिक इकाइयों के साथ-साथ नई व्यावसायिक पहलों, उत्पादों, सेवाओं, गतिविधियों, प्रक्रियाओं और प्रणालियों में शामिल किया जाना चाहिए। इसके अतिरिक्त, आरई के परिचालन जोखिम मूल्यांकन के परिणामों को आरई की समग्र व्यावसायिक रणनीति विकास प्रक्रिया में शामिल किया जाना चाहिए। ओआरएमएफ के समग्र दृष्टिकोण में निम्नलिखित को प्रतिबिंबित किया जाना चाहिए:

4.8.1 परिचालन जोखिम का प्रबंधन आरई के बिजनेस लाइनों में अंतर्निहित है।

4.8.2 वरिष्ठ प्रबंधक आरई की एंड-टू-एंड प्रक्रियाओं में परिचालन जोखिम के प्रबंधन और स्वामित्व के लिए जिम्मेदार हैं।

4.8.3 अंततः बोर्ड परिचालन जोखिम प्रबंधन की निगरानी के लिए जिम्मेदार और जवाबदेह है।

4.9 ओआरएमएफ को निदेशक मंडल द्वारा अनुमोदित नीतियों में व्यापक और उचित रूप से प्रलेखित किया जाना चाहिए और इसमें परिचालन जोखिम और परिचालन हानि की परिभाषाएँ शामिल होनी चाहिए। यदि आरई परिचालन जोखिम और हानि जोखिम का पर्याप्त रूप से वर्णन और वर्गीकरण नहीं करते हैं, तो इसके परिणाम स्वरुप उनके ओआरएमएफ की प्रभावशीलता में काफी कमी होगी।

4.10 ओआरएमएफ दस्तावेज़ में स्पष्ट रूप से होना चाहिए:

4.10.1 परिचालन जोखिम को प्रबंधित करने के लिए उपयोग की जाने वाली अभिशासन संरचनाओं की पहचान करें, जिसमें रिपोर्टिंग लाइनें तथा उत्तरदायित्व और परिचालन जोखिम अभिशासन समितियों के अधिदेश और सदस्यता शामिल हैं;

4.10.2 सुसंगत परिचालन जोखिम प्रबंधन नीतियों और प्रक्रियाओं का संदर्भ दें;

4.10.3 जोखिम तथा नियंत्रण पहचान और मूल्यांकन के लिए साधन और उनका उपयोग करने में सुरक्षा के तीन घेरों की भूमिका और जिम्मेदारियों का विवरण दें;

4.10.4 आरई की स्वीकृत परिचालन जोखिम स्वीकार्यता और सहनशीलता का विवरण दें; अंतर्निहित और रिश्यूडअल जोखिम के लिए सीमाएँ, भौतिक गतिविधि ट्रिगर अथवा सीमाएँ; और अनुमोदित जोखिम न्यूनीकरण रणनीतियाँ और उपकरण;

4.10.5 नियंत्रणों के प्रभावी ढंग से डिज़ाइन, कार्यान्वित और संचालन सुनिश्चित करने के लिए आरई के दृष्टिकोण का विवरण दें;

4.10.6 अंतर्निहित और अवशिष्ट जोखिम, जोखिम के लिए थ्रेशोल्ड अथवा सीमाओं की स्थापना और निगरानी के लिए आरई के दृष्टिकोण का विवरण दें;

4.10.7 सभी व्यावसायिक इकाइयों (जैसे एक नियंत्रण पुस्तकालय में) द्वारा कार्यान्वित इनवेंटरी जोखिमों और नियंत्रणों का विवरण दें;

4.10.8 समय पर और सटीक डेटा के लिए जोखिम रिपोर्टिंग और प्रबंधन सूचना प्रणाली (एमआईएस) स्थापित करें;

4.10.9 सभी व्यावसायिक इकाइयों में जोखिम पहचान, रेटिंग और जोखिम प्रबंधन के उद्देश्यों की स्थिरता सुनिश्चित करने के लिए परिचालन जोखिम शर्तों का एक सामान्य वर्गीकरण दें। वर्गीकरण घटना के प्रकार, कारणों, भौतिकता और व्यावसायिक इकाइयों द्वारा परिचालन जोखिम जोखिमों को अलग कर सकता है जहां वह होते हैं; यह उन परिचालन जोखिम, जोखिमों को भी चिह्नित कर सकता है जो आंशिक रूप से अथवा पूरी तरह से कानूनी, आचरण, मॉडल और आईसीटी (साइबर सहित) जोखिमों के साथ-साथ क्रेडिट अथवा बाजार जोखिम सीमा में जोखिमों का प्रतिनिधित्व करते हैं;

4.10.10 जोखिम प्रबंधन प्रक्रिया के परिणामों की उचित स्वतंत्र समीक्षा और चुनौती के निहितार्थ दें; और

4.10.11 आंतरिक और बाह्य पर्यावरणीय परिवर्तनों को संबोधित करते हुए नियंत्रित परिवेश की गुणवत्ता के निरंतर आकलन के आधार पर अथवा जब भी आरई के परिचालन जोखिम प्रोफ़ाइल में कोई भौतिक परिवर्तन होता है, तो नीतियों की समीक्षा और संशोधन करने की आवश्यकता है।

5. निदेशक मंडल और वरिष्ठ प्रबंधन की जिम्मेदारियां

सिद्धांत 3 - निदेशक मंडल को ओआरएमएफ और परिचालन आघात-सहनीयता दृष्टिकोण को अनुमोदित तथा समय-समय पर इसकी समीक्षा करनी चाहिए और यह सुनिश्चित करना चाहिए कि वरिष्ठ प्रबंधन ओआरएमएफ और परिचालन आघात-सहनीयता दृष्टिकोण की नीतियों, प्रक्रियाओं और प्रणालियों को सभी निर्णय स्तरों पर प्रभावी ढंग से लागू करता है।

5.1 निदेशक मंडल को चाहिए कि:

5.1.1 जोखिम प्रबंधन संस्कृति स्थापित करें और यह सुनिश्चित करें कि आरई के पास अपनी वर्तमान और नियोजित रणनीतियों और गतिविधियों में निहित परिचालन जोखिम की प्रकृति और दायरे को समझने के लिए पर्याप्त प्रक्रियाएं हैं;

5.1.2 यह सुनिश्चित करना कि परिचालन जोखिम प्रबंधन प्रक्रियाएं व्यापक और गतिशील निरीक्षण के अधीन हैं और उद्यम में सभी जोखिमों के प्रबंधन के लिए समग्र ढांचे में पूरी तरह से एकीकृत अथवा समन्वित हैं;

5.1.3 ओआरएमएफ में अंतर्निहित सिद्धांतों के बारे में वरिष्ठ प्रबंधन को स्पष्ट मार्गदर्शन प्रदान करें और इन सिद्धांतों के साथ संरेखित करने के लिए वरिष्ठ प्रबंधन द्वारा विकसित संबंधित नीतियों को अनुमोदित करें;

5.1.4 नियमित रूप से ओआरएमएफ की प्रभावशीलता की समीक्षा और मूल्यांकन करें, और यह सुनिश्चित करने के लिए ओआरएमएफ को अनुमोदित करें कि आरई ने बाहरी बाजार परिवर्तनों और अन्य पर्यावरणीय कारकों से उत्पन्न होने वाले परिचालन जोखिम की पहचान की है और उसका प्रबंधन कर रहा है, साथ ही नए उत्पादों, सेवाओं, गतिविधियों, प्रक्रियाओं अथवा प्रणालियों से जुड़े परिचालन जोखिम, जिसमें जोखिम प्रोफाइल और प्राथमिकताओं में परिवर्तन (उदाहरण के लिए व्यावसायिक की मात्रा में परिवर्तन) शामिल हैं;

5.1.5 यह सुनिश्चित करना कि आरई का ओआरएमएफ सुरक्षा के तीसरे घेरे (लेखापरीक्षा अथवा बाहरी स्रोतों से अन्य उचित रूप से प्रशिक्षित स्वतंत्र तृतीय पक्ष) द्वारा प्रभावी स्वतंत्र समीक्षा के अधीन है; और

5.1.6 यह सुनिश्चित करें कि जैसे-जैसे सर्वोत्तम प्रथाएं विकसित होती हैं, प्रबंधन इन प्रगति का लाभ उठा रहा है।

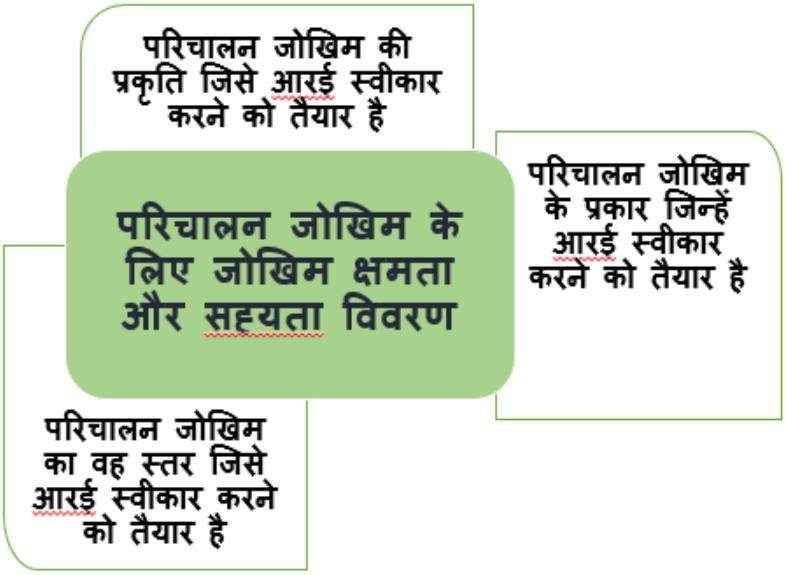
5.2 मजबूत आंतरिक नियंत्रण परिचालन जोखिम प्रबंधन का एक महत्वपूर्ण पहलू है। निदेशक मंडल को एक मजबूत नियंत्रण परिवेश को लागू करने के लिए प्रबंधन जिम्मेदारी और जवाबदेही स्पष्ट स्थापित करनी चाहिए। इसकी निरंतर प्रभावशीलता सुनिश्चित करने के लिए नियंत्रणों की नियमित रूप से समीक्षा, निगरानी और परीक्षण किया जाना चाहिए। नियंत्रण परिवेश को परिचालन जोखिम प्रबंधन कार्यों, व्यावसायिक इकाइयों और समर्थन कार्यों के बीच कर्तव्यों की उचित स्वतंत्रता/पृथक्करण प्रदान करना चाहिए।

5.3 निदेशक मंडल को आरई की जोखिम क्षमता और उसके महत्वपूर्ण परिचालनों में व्यवधान के प्रति सहनशीलता को ध्यान में रखते हुए आरई के परिचालन आघात-सहनीयता दृष्टिकोण की समीक्षा और उसे स्वीकृत करना चाहिए। व्यवधान के प्रति आरई की सहनशीलता को निरूपित करते समय, निदेशक मंडल को गंभीर लेकिन संभावित परिदृश्यों की एक विस्तृत श्रृंखला को देखते हुए इसकी परिचालन क्षमताओं पर विचार करना चाहिए जो इसके महत्वपूर्ण परिचालनों को प्रभावित करेंगे। निदेशक मंडल को यह सुनिश्चित करना चाहिए कि आरई की नीतियाँ उन मामलों को प्रभावी ढंग से करें जहाँ आरई की क्षमताएँ व्यवधान के प्रति अपनी घोषित सहनशीलता को पूरा करने के लिए अपर्याप्त हैं।

5.4 निदेशक मंडल को आरई के परिचालन आघात-सहनीयता दृष्टिकोण की व्यापक समझ स्थापित करने में, इसके उद्देश्यों के बारे में आरई के कार्मिक, तृतीय पक्षों और अंतर-समूह संस्थाओं सहित सभी संबंधित पक्षों को स्पष्ट संचार के माध्यम से सक्रिय भूमिका निभानी चाहिए।

5.5 निदेशक मंडल की देखरेख में, वरिष्ठ प्रबंधन को आरई के परिचालन आघात-सहनीयता दृष्टिकोण को लागू करना और यह सुनिश्चित करना चाहिए कि आरई के समग्र परिचालन आघात-सहनीयता दृष्टिकोण का समर्थन करने के लिए वित्तीय, तकनीकी और अन्य संसाधन उचित रूप से आवंटित किए गए हैं।

सिद्धांत 4- निदेशक मंडल को परिचालन जोखिम के लिए जोखिम स्वीकार्यता और सहनशीलता विवरण को स्वीकृत और समय-समय पर उसकी समीक्षा करनी चाहिए, जो परिचालन जोखिम की प्रकृति, प्रकार और स्तरों को स्पष्ट करता है जिसे आरई स्वीकार करने को तैयार है। निदेशक मंडल को प्रत्येक महत्वपूर्ण संचालन की पहचान और वर्गीकरण के साथ-साथ प्रभाव सहनशीलता के मानदंडों की भी समीक्षा और अनुमोदन करना चाहिए, ताकि आरई के परिचालन आघात-सहनीयता को बढ़ाया जा सके।



5.6 परिचालन जोखिम के लिए जोखिम स्वीकार्यता और सहनशीलता विवरण को निदेशक मंडल के अधिकार के तहत विकसित किया जाना चाहिए और इसे आरई की अल्पकालिक और दीर्घकालिक रणनीतिक और वित्तीय योजनाओं से जोड़ा जाना चाहिए। आरई के ग्राहकों और हितधारकों के हितों के साथ-साथ नियामक आवश्यकताओं को ध्यान में रखते हुए, एक प्रभावी जोखिम स्वीकार्यता और सहनशीलता विवरण तैयार किया जाना चाहिए।

5.6.1 सभी हितधारकों के लिए संवाद करना और समझना आसान हो;

5.6.2 इसमें प्रमुख पृष्ठभूमि जानकारी और धारणाएं शामिल हैं जो अनुमोदन के समय आरई की व्यावसायिक योजनाओं को सूचित करती हैं;

5.6.3 ऐसे विवरण शामिल किए जाए जो कुछ प्रकार के जोखिम लेने अथवा टालने के लिए प्रेरणा(ओं) को स्पष्ट रूप से व्यक्त करते हैं, और इन जोखिमों की निगरानी को सक्षम करने के लिए सीमाएँ या संकेतक (जो मात्रात्मक हो सकते हैं या नहीं) स्थापित करते हैं;

5.6.4 यह सुनिश्चित करना कि व्यावसायिक इकाइयों और कानूनी संस्थाओं की रणनीति और जोखिम सीमाएं, जहां तक प्रासंगिक हो, आरई-व्यापक जोखिम स्वीकार्यता विवरण के अनुरूप हों; तथा

5.6.5 भविष्योन्मुखी रहें और, जहां लागू हो, परिदृश्य और तनाव परीक्षण के अधीन रहें ताकि यह सुनिश्चित हो सके कि आरई यह समझता है कि कौन सी घटनाएं उसे जोखिम स्वीकार्यता और सहनशीलता के विवरण से बाहर कर सकती हैं।

5.7 किसी आरई के लिए अपनी परिचालनात्मक आघात-सहनीयता को विकसित करने हेतु प्रारंभिक बिंदु, अपने महत्वपूर्ण परिचालनों को परिभाषित करने के लिए मानदंड निर्धारित करना है। मानदंड को आरई को अपने महत्वपूर्ण संचालन की पहचान करने और व्यवधान की स्थिति में उन्हें प्राथमिकता देने में सक्षम बनाना चाहिए। इसे व्यवधान से उसके ग्राहकों को होने वाले जोखिम, आरई की व्यवहार्यता, सुरक्षा और सुदृढ़ता तथा समग्र वित्तीय स्थिरता पर विचार करके हासिल किया जाना चाहिए। महत्वपूर्ण परिचालनों की पहचान के लिए मानदंडों की समीक्षा की जानी चाहिए और बोर्ड द्वारा वार्षिक रूप से या व्यवसाय में भौतिक परिवर्तनों को लागू करने के समय अनुमोदित किया जाना चाहिए जिसमें अतिरिक्त महत्वपूर्ण परिचालन शामिल होंगे।

5.8 निदेशक मंडल को प्रत्येक महत्वपूर्ण परिचालन के लिए कम से कम वार्षिक रूप से अथवा जब भी व्यवधान उत्पन्न होता है, प्रभाव सहनशीलता की समीक्षा करनी चाहिए और उसे स्वीकृत करना चाहिए। प्रभाव सहनशीलता का उद्देश्य प्रत्येक महत्वपूर्ण ऑपरेशन के लिए व्यवधान के अधिकतम स्वीकार्य स्तर को निर्धारित करना है। इसकी उपयुक्तता निर्धारित करने के लिए गंभीर लेकिन संभावित परिदृश्यों के विरुद्ध इसका परीक्षण किया जाना चाहिए, अर्थात यह निर्धारित करने के लिए कि व्यवधान के दौरान आरई परिभाषित प्रभाव सहनशीलता के भीतर रहने में सक्षम है या नहीं।

5.9 एक आरई को अपने प्रत्येक महत्वपूर्ण परिचालन के लिए कम से कम एक प्रभाव सहिष्णुता मीट्रिक निर्धारित करना चाहिए। कम से कम, (ए) समय-आधारित मीट्रिक होनी चाहिए (उदाहरण के लिए, अधिकतम स्वीकार्य अवधि जो एक महत्वपूर्ण परिचालन किसी व्यवधान का सामना कर सकती है), (बी) मात्रा-आधारित मीट्रिक (उदाहरण के लिए, व्यवधान के परिणामस्वरूप डेटा हानि की अधिकतम सीमा जिसे एक आरई स्वीकार करेगा) और (सी) सेवा स्तर मीट्रिक (उदाहरण के लिए, वैकल्पिक व्यवस्था के तहत परिचालन करते समय आरई द्वारा सेवा का न्यूनतम स्तर बनाए रखा जाएगा।) अपनी परिचालनगत आघात-सहनीयता को और बढ़ाने के लिए, एक विनियमित संस्था को अतिरिक्त प्रभाव सहनीयता मेट्रिक्स पर विचार करना चाहिए, जैसे कि व्यवधान से प्रभावित ग्राहकों की अधिकतम सहनीय संख्या; व्यवधान से प्रभावित लेन-देन की अधिकतम संख्या; तथा प्रभावित लेन-देन का अधिकतम मूल्य।

सिद्धांत 5- वरिष्ठ प्रबंधन को निदेशक मंडल द्वारा अनुमोदन के लिए एक स्पष्ट, प्रभावी और मजबूत अभिशासन संरचना विकसित करनी चाहिए जिसमें जिम्मेदारी की सुपरिभाषित, पारदर्शी और सुसंगत लकीरे हों। वरिष्ठ प्रबंधन, पूरे संगठन में परिचालन जोखिम प्रबंधन के लिए नीतियों, प्रक्रियाओं और प्रणालियों को लगातार लागू करने और बनाए रखने के लिए जिम्मेदार है, जो कि आरई के सभी भौतिक उत्पादों, गतिविधियों, प्रक्रियाओं और प्रणालियों में जोखिम स्वीकार्यता और सहनशीलता के अनुरूप हो।

5.10 वरिष्ठ प्रबंधन को निदेशक मंडल द्वारा अनुमोदित ओआरएमएफ को विशिष्ट नीतियों और प्रक्रियाओं में परिवर्तित करना चाहिए जिन्हें विभिन्न व्यावसायिक इकाइयों के भीतर लागू और सत्यापित किया जा सकता है। इसे जवाबदेही को प्रोत्साहित करने और बनाए रखने के लिए प्राधिकरण, जिम्मेदारी और रिपोर्टिंग संबंधों को स्पष्ट रूप से निर्दिष्ट करना चाहिए, और यह सुनिश्चित करना चाहिए कि आरई की जोखिम स्वीकार्यता और सहनशीलता विवरण के अनुरूप परिचालन जोखिम को प्रबंधित करने के लिए आवश्यक संसाधन उपलब्ध हैं। इसके अलावा, इसे यह भी सुनिश्चित करना चाहिए कि प्रबंधन निरीक्षण प्रक्रिया किसी व्यावसायिक इकाई की गतिविधि में निहित जोखिमों के लिए उपयुक्त है।

5.11 वरिष्ठ प्रबंधन मजबूत चुनौती तंत्र और प्रभावी समस्या समाधान प्रक्रियाओं को स्थापित करने और बनाए रखने के लिए जिम्मेदार है। इनमें रिपोर्ट करने, ट्रैक करने और जब आवश्यक हो, समाधान सुनिश्चित करने के लिए मुद्दों को आगे बढ़ाने की प्रणाली शामिल होनी चाहिए। आरई को यह प्रदर्शित करने में सक्षम होना चाहिए कि त्रिस्तरीय सुरक्षा पद्धति संतोषजनक ढंग से कार्य कर रही है, तथा यह भी बताना चाहिए कि निदेशक मंडल, बोर्ड की स्वतंत्र लेखा परीक्षा समिति, तथा वरिष्ठ प्रबंधन किस प्रकार यह सुनिश्चित करते हैं कि इस पद्धति का क्रियान्वयन हो तथा यह उचित तरीके से कार्य कर रही है।

5.12 वरिष्ठ प्रबंधन द्वारा यह सुनिश्चित किया जाना चाहिए कि परिचालन जोखिम के प्रबंधन के लिए जिम्मेदार कर्मचारी ऋण, बाजार और अन्य जोखिमों के प्रबंधन के लिए जिम्मेदार कर्मचारियों के साथ-साथ उन लोगों के साथ प्रभावी ढंग से समन्वय और संवाद करें जो बीमा जोखिम हस्तांतरण और अन्य तृतीय-पक्ष व्यवस्थाओं जैसी बाह्य सेवाओं की प्राप्ति के लिए जिम्मेदार हैं। ऐसा न करने पर, किसी आरई के समग्र जोखिम प्रबंधन कार्यक्रम में महत्वपूर्ण अंतराल या अतिव्यापन (ओवरलैप) हो सकता है।

5.13 आरई के अंतर्गत ओओआरएफ के प्रबंधक पर्याप्त गुणवत्तापूर्ण होने चाहिए कि वे अपने कर्तव्यों का निर्वहन प्रभावी ढंग से कर सकें, आदर्श रूप से यह उपाधि अन्य जोखिम प्रबंधन कार्यों जैसे ऋण, बाजार और तरलता जोखिम के अनुरूप होनी चाहिए।

5.14 वरिष्ठ प्रबंधन को यह सुनिश्चित करना चाहिए कि आरई की गतिविधियां आवश्यक अनुभव, तकनीकी क्षमताओं और संसाधनों तक पहुंच वाले कर्मचारियों द्वारा संचालित की जाएं। विनियमित संस्था की जोखिम नीति के अनुपालन की निगरानी और प्रवर्तन के लिए जिम्मेदार कर्मचारियों के पास उन इकाइयों से स्वतंत्र प्राधिकार होना चाहिए जिनकी वे देखरेख करते हैं।

5.15 किसी आरई की शासन संरचना उसकी गतिविधियों की प्रकृति, आकार, जटिलता और जोखिम प्रोफाइल के अनुरूप होनी चाहिए। परिचालन जोखिम अभिशासन संरचना को डिजाइन करते समय, किसी भी आरई को निम्नलिखित बातों को ध्यान में रखना चाहिए:

5.15.1 समिति संरचना - बड़े और अधिक जटिल संगठनों के लिए एक ठोस उद्योग प्रक्रिया जिसमें एक केंद्रीय समूह कार्य और अलग-अलग व्यावसायिक इकाइयां होती हैं, जिसमें सभी जोखिमों की देखरेख के लिए बोर्ड द्वारा निर्मित उद्यम-स्तरीय जोखिम समिति का उपयोग किया जाता है, जिसके लिए प्रबंधन स्तर की परिचालन जोखिम समिति रिपोर्ट करती है। परिचालन जोखिम समिति की प्रकृति, आकार और जटिलता के आधार पर, उद्यम-स्तरीय जोखिम समिति परिचालन जोखिम समिति(यों), व्यवसाय या कार्यात्मक क्षेत्र से इनपुट प्राप्त कर सकती है। लधु और कम जटिल संगठन एक समतल संगठनात्मक संरचना का उपयोग कर सकते हैं जो बोर्ड की जोखिम प्रबंधन समिति के भीतर सीधे परिचालन जोखिम की देखरेख करता है।

5.15.2 समिति संयोजन - परिचालन जोखिम समितियों (या छोटे विनियमित संस्थाओं में जोखिम समिति) के लिए एक अच्छी उद्योग पद्धति यह है कि इसमें विभिन्न प्रकार की विशेषज्ञता वाले सदस्यों को शामिल किया जाए, जिसमें व्यावसायिक गतिविधियों, वित्तीय गतिविधियों, कानूनी, तकनीकी और नियामक मामलों तथा जोखिम प्रबंधन में विशेषज्ञता शामिल होनी चाहिए।

5.15.3 समिति संचालन - समिति की बैठकें उचित आवृत्तियों पर पर्याप्त समय और संसाधनों के साथ आयोजित की जानी चाहिए ताकि उत्पादक चर्चा और निर्णय लेने की अनुमति मिल सके। समिति के संचालन के रिकॉर्ड पर्याप्त और प्रलेखित (दस्तावेजित) होने चाहिए ताकि समिति की प्रभावशीलता की समीक्षा और मूल्यांकन की अनुमति मिल सके।

5.16 चूंकि परिचालन जोखिम प्रबंधन एक विकासशील क्षेत्र है, और कारोबारी माहौल लगातार बदल रहा है, इसलिए वरिष्ठ प्रबंधन को यह सुनिश्चित करना चाहिए कि ओआरएमएफ़ के तहत आरई की नीतियां, प्रक्रियाएं और प्रणालियां पर्याप्त रूप से मजबूत बनी रहें, ताकि परिचालन हानि का प्रबंधन और समय पर उनका समाधान सुनिश्चित किया जा सके। परिचालन जोखिम प्रबंधन में सुधार काफी हद तक वरिष्ठ प्रबंधन की सक्रियता और परिचालन जोखिम प्रबंधकों की चिंताओं को दूर करने के लिए शीघ्रता और उचित तरीके से कार्य करने की इच्छा पर निर्भर करता है।

6. जोखिम प्रबंधन पर्यावरण - पहचान और मूल्यांकन

सिद्धांत 6: वरिष्ठ प्रबंधन को सभी भौतिक उत्पादों, गतिविधियों, प्रक्रियाओं और प्रणालियों में निहित परिचालन जोखिम की व्यापक पहचान और मूल्यांकन सुनिश्चित करना चाहिए ताकि यह सुनिश्चित किया जा सके कि अंतर्निहित जोखिम और प्रोत्साहनों को अच्छी तरह से समझा गया है। लोगों, प्रक्रियाओं और प्रणालियों में आंतरिक और बाह्य खतरों तथा संभावित विफलताओं का शीघ्र और निरंतर आधार पर आकलन किया जाना चाहिए। महत्वपूर्ण परिचालनों में कमजोरियों का आकलन सक्रिय एवं त्वरित तरीके से किया जाना चाहिए। इसके परिणामस्वरूप उत्पन्न होने वाले सभी जोखिमों का प्रबंधन परिचालन आघात-सहनीयता दृष्टिकोण के अनुसार किया जाना चाहिए।

6.1 जोखिम की पहचान और मूल्यांकन एक प्रभावी परिचालन जोखिम प्रबंधन प्रणाली की मूलभूत विशेषताएं हैं, और परिचालन आघात-सहनीयता क्षमताओं में प्रत्यक्ष रूप से योगदान करते हैं। प्रभावी जोखिम पहचान आंतरिक और बाह्य दोनों कारकों पर विचार करती है। उचित जोखिम मूल्यांकन से आरई को अपने जोखिम प्रोफाइल को बेहतर ढंग से समझने और जोखिम प्रबंधन संसाधनों और रणनीतियों को अधिक प्रभावी ढंग से आवंटित करने में मदद मिलती है।

उदाहरण के लिए, नीचे दिया गया चित्र जोखिमों के व्यापक स्पेक्ट्रम (जोखिम जगत) को दर्शाता है जो तृतीय पक्ष के संबंधों में मौजूद हो सकते हैं।

6.2 परिचालन जोखिम की पहचान और आकलन के लिए उपयोग में लाए जाने वाले साधनो के उदाहरण (सांकेतिक हैं और विस्तृत नहीं) हैं:

6.2.1 स्व-मूल्यांकन – आरई अक्सर विभिन्न स्तरों पर अपने परिचालन जोखिमों और नियंत्रणों का स्व-मूल्यांकन करती हैं। मूल्यांकन में आमतौर पर अंतर्निहित जोखिम (नियंत्रणों पर विचार किए जाने से पहले का जोखिम), नियंत्रण पर्यावरण की प्रभावशीलता और अवशिष्ट जोखिम (नियंत्रणों पर विचार किए जाने के बाद जोखिम) का मूल्यांकन किया जाता है और इसमें मात्रात्मक (जैसे मेट्रिक्स, बेंचमार्किंग, आदि) और गुणात्मक (जैसे अंतर्निहित और अवशिष्ट जोखिम रेटिंग के निर्धारण में जोखिम घटना की संभावना और परिणाम) दोनों तत्व शामिल होते हैं। मूल्यांकन व्यावसायिक प्रक्रियाओं, गतिविधियों और संगठनात्मक कार्यों में प्रमुख चरणों के साथ-साथ संबंधित जोखिमों और नियंत्रण की कमजोरी के क्षेत्रों की पहचान करने के लिए व्यावसायिक प्रक्रिया मानचित्रण का उपयोग किया जा सकता है। मूल्यांकन में व्यावसायिक पर्यावरण, परिचालन जोखिम, अंतर्निहित कारणों, नियंत्रणों और नियंत्रण प्रभावशीलता के मूल्यांकन पर पर्याप्त विस्तृत जानकारी होनी चाहिए, ताकि एक स्वतंत्र समीक्षक यह निर्धारित कर सके कि आरई द्वारा अपनी रेटिंग किस प्रकार प्राप्त की गई। नियंत्रण की समग्र प्रभावशीलता के बारे में एक सार्थक दृष्टिकोण बनाने और वरिष्ठ प्रबंधन, जोखिम समितियों और निदेशक मंडल द्वारा निरीक्षण की सुविधा के लिए इस जानकारी को एकत्रित करने के लिए जोखिम रजिस्टर रखा जा सकता है।

6.2.2 परिचालन जोखिम घटना डेटा – आरई अक्सर एक व्यापक परिचालन जोखिम घटना डेटासेट बनाए रखते हैं जो आरई द्वारा अनुभव की गई सभी सामग्री घटनाओं को एकत्र करता है और परिचालन जोखिम आकलन के लिए आधार के रूप में कार्य करता है। इवेंट डेटासेट में आम तौर पर आंतरिक हानि डेटा, निकट चूक आदि शामिल होते हैं, और इसे ओआरएमएफ नीतियों में परिभाषित वर्गीकरण के अनुसार वर्गीकृत किया जाता है और लगातार आरई में लागू किया जाता है। इसमें घटना की तिथि (घटना तिथि, खोज तिथि और लेखांकन तिथि) और हानि की स्थिति में वित्तीय प्रभाव भी शामिल होता है। जब घटनाओं के लिए अन्य मूल कारण की जानकारी उपलब्ध हो, तो आदर्श रूप से उसे परिचालन जोखिम डेटासेट में भी शामिल किया जा सकता है। जब घटनाओं के लिए अन्य मूल कारण की जानकारी उपलब्ध हो, तो आदर्श रूप से उसे परिचालन जोखिम डेटासेट में भी शामिल किया जा सकता है।जहां संभव हो, आरई को बाहरी परिचालन जोखिम घटना डेटा इकट्ठा करने और इस डेटा का उपयोग अपने आंतरिक विश्लेषण में करने के लिए प्रोत्साहित किया जाता है, क्योंकि यह अक्सर उन जोखिमों की जानकारी देता है जो पूरे उद्योग में आम हैं।

6.2.3 घटना प्रबंधन – एक ठोस घटना प्रबंधन दृष्टिकोण में आम तौर पर नए परिचालन जोखिमों की पहचान करने के लिए घटनाओं का विश्लेषण, अंतर्निहित कारणों और नियंत्रण कमजोरियों को समझना, और समरूप घटनाओं की पुनरावृत्ति को रोकने के लिए उचित प्रतिक्रिया तैयार करना

शामिल होता है। यह जानकारी स्व-मूल्यांकन और विशेष रूप से नियंत्रण प्रभावशीलता के आकलन के लिए एक इनपुट है।

6.2.4 नियंत्रण निगरानी और आश्वासन ढाँचा – उपयुक्त नियंत्रण निगरानी और आश्वासन ढांचे को शामिल करने से प्रमुख नियंत्रणों के मूल्यांकन, समीक्षा और सतत निगरानी और परीक्षण के लिए एक संरचित दृष्टिकोण की सुविधा मिलती है। नियंत्रणों का विश्लेषण यह सुनिश्चित करता है कि ये पहचाने गए जोखिमों के लिए उपयुक्त रूप से डिजाइन किए गए हैं तथा प्रभावी रूप से कार्य कर रहे हैं। विश्लेषण में पर्याप्त रोकथाम, पता लगाने और प्रतिक्रिया रणनीतियों सहित नियंत्रण कवरेज की पर्याप्तता पर भी विचार किया जाना चाहिए। नियंत्रण निगरानी और परीक्षण विभिन्न परिचालन जोखिमों और व्यवसाय क्षेत्रों के लिए उपयुक्त होना चाहिए। नियंत्रण और शमन पर आगे का विवरण इस मार्गदर्शन नोट के पैराग्राफ 9 में दिया गया है।

6.2.5 मेट्रिक्स – परिचालन जोखिम घटना डेटा और जोखिम एवं नियंत्रण आकलन का उपयोग करते हुए, आरई अक्सर अपने परिचालन जोखिम, जोखिम का आकलन और निगरानी करने के लिए मेट्रिक्स विकसित करते हैं। ये मेट्रिक्स सरल संकेतक हो सकते हैं, जैसे कि घटनाओं की संख्या, या अधिक परिष्कृत एक्सपोजर मॉडल का परिणाम हो सकते हैं। मेट्रिक्स व्यवसाय के चालू निष्पादन और नियंत्रण पर्यावरण की निगरानी करने तथा परिचालन जोखिम प्रोफ़ाइल की रिपोर्ट करने के लिए प्रारंभिक चेतावनी जानकारी प्रदान करते हैं। प्रभावी मेट्रिक्स संबंधित परिचालन जोखिमों और नियंत्रणों को स्पष्ट रूप से जोड़ते हैं। निर्धारित सीमाओं या सहनीय स्तरों के विरुद्ध समय के साथ मेट्रिक्स और संबंधित प्रवृत्तियों की निगरानी करने से जोखिम प्रबंधन और रिपोर्टिंग उद्देश्यों के लिए बहुमूल्य जानकारी मिलती है।

6.2.6 परिदृश्य विश्लेषण – परिदृश्य विश्लेषण एक ऐसी विधि है जिसके द्वारा विभिन्न परिदृश्यों की पहचान, मापन और विश्लेषण किया जाता है, जिनमें कम संभावना और उच्च गंभीरता वाली घटनाएं शामिल हैं, जिनमें से कुछ के परिणामस्वरूप गंभीर परिचालन जोखिम हानि हो सकती है। इसमें आमतौर पर वरिष्ठ प्रबंधन, व्यवसाय प्रबंधन और वरिष्ठ परिचालन जोखिम कर्मचारियों और अन्य कार्यात्मक क्षेत्रों जैसे अनुपालन, मानव संसाधन और आईटी जोखिम प्रबंधन सहित विषय वस्तु विशेषज्ञों की कार्यशालाएं या बैठकें शामिल होती हैं, ताकि संभावित घटनाओं के चालकों और परिणामों की सीमा को विकसित और विश्लेषित किया जा सके। परिदृश्य विश्लेषण के इनपुट में आमतौर पर प्रासंगिक आंतरिक और बाह्य हानि डेटा, स्व-मूल्यांकन से जानकारी, नियंत्रण निगरानी और आश्वासन ढांचा, दूरदर्शी मेट्रिक्स, मूल कारण विश्लेषण और प्रक्रिया ढांचा शामिल होंगे। परिदृश्य विश्लेषण प्रक्रिया का उपयोग संभावित घटनाओं के परिणामों की एक श्रृंखला को विकसित करने के लिए किया

जा सकता है, जिसमें जोखिम प्रबंधन उद्देश्यों के लिए प्रभाव आकलन, ऐतिहासिक डेटा या वर्तमान जोखिम आकलन के आधार पर अन्य साधनो का पूरक शामिल है। आरई को अपनी प्रत्येक महत्वपूर्ण सेवा के लिए, अपने परिचालन में व्यवधान की स्थिति में प्रभाव सहनशीलता के भीतर रहने की अपनी क्षमता का परीक्षण करने के लिए, उपरोक्त मापदंडों का उपयोग करते हुए नियमित परिदृश्य विश्लेषण करना चाहिए। परिदृश्य विश्लेषण करने में, आरई को अपने व्यवसाय और जोखिम प्रोफाइल के लिए प्रासंगिक, अलग-अलग प्रकृति, गंभीरता और अवधि की प्रतिकूल परिस्थितियों की पहचान करनी चाहिए और उन परिस्थितियों में आरई की महत्वपूर्ण सेवाओं की डिलीवरी के लिए जोखिमों पर विचार करना चाहिए। परिचालन आघात-सहनीयता के आगे के परीक्षण के लिए इस तरह के अभ्यास को आपदा समुत्थान और व्यवसाय निरंतरता योजनाओं के साथ भी एकीकृत किया जा सकता है। परिदृश्य प्रक्रिया की व्यक्तिपरकता को देखते हुए, प्रक्रिया की अखंडता और स्थिरता सुनिश्चित करने के लिए एक मजबूत शासन ढांचा और स्वतंत्र समीक्षा महत्वपूर्ण है।

6.2.7 बेंचमार्किंग एवं तुलनात्मक विश्लेषण – बेंचमार्किंग और तुलनात्मक विश्लेषण आरई के भीतर तैनात विभिन्न जोखिम माप और प्रबंधन साधनो के परिणामों की तुलना है, साथ ही उद्योग में अन्य आरई के साथ आरई के मेट्रिक्स की तुलना भी है। ऐसी तुलनाएं आरई के परिचालन जोखिम प्रोफ़ाइल की समझ को बढ़ाने के लिए की जा सकती हैं। उदाहरण के लिए, आंतरिक नुकसान की आवृत्ति और गंभीरता की तुलना स्व-मूल्यांकन से करने से आरई को यह निर्धारित करने में मदद मिल सकती है कि उसकी स्व-मूल्यांकन प्रक्रियाएँ प्रभावी रूप से काम कर रही हैं या नहीं। परिदृश्य विश्लेषण डेटा की तुलना आंतरिक और बाह्य हानि डेटा के साथ की जा सकती है, जिससे संभावित जोखिम घटनाओं के प्रति आरई के जोखिम की गंभीरता को बेहतर ढंग से समझा जा सके।

6.3 परिचालन जोखिम मूल्यांकन साधनो के आउटपुट निम्नलिखित हों, इसके लिए यह सुनिश्चित करना चाहिए कि:

6.3.1 सटीक डेटा पर आधारित, जिसकी अखंडता मजबूत शासन और मजबूत सत्यापन और प्रमाणीकरण प्रक्रियाओं द्वारा सुनिश्चित की जाती है;

6.3.2 आंतरिक मूल्य निर्धारण और प्रदर्शन माप तंत्र के साथ-साथ व्यावसायिक अवसरों के आकलन को पर्याप्त रूप से ध्यान में रखना; तथा

6.3.3 आवश्यकता पड़ने पर ओओआरएफ़ द्वारा निगरानी की जाने वाली कार्य योजनाओं या सुधार योजनाओं के अधीन।

6.4 ये परिचालन जोखिम मूल्यांकन साधन सीधे तौर पर किसी आरई के परिचालन आघात-सहनीयता दृष्टिकोण में योगदान करते हैं, विशेष रूप से घटना प्रबंधन, स्व-मूल्यांकन और परिदृश्य विश्लेषण प्रक्रियाओं में, क्योंकि वे आरई को उनके महत्वपूर्ण परिचालनों के लिए आंतरिक और बाह्य दोनों प्रकार के खतरों और कमजोरियों की पहचान करने और उन पर निगरानी रखने की अनुमति देते हैं। आरई को अपने परिचालन आघात-सहनीयता नियंत्रणों और प्रक्रियाओं का प्रबंधन, समाधान और सुधार करने के लिए इन साधनो के आउटपुट का नियमित आधार पर और समयबद्ध तरीके से उपयोग करना चाहिए, ताकि उन्हें महत्वपूर्ण परिचालन वितरण को प्रभावित करने से रोका जा सके। ऐसा करने के लिए, परिचालन जोखिम प्रबंधन कार्य को अन्य प्रासंगिक कार्यों के साथ मिलकर काम करना चाहिए। ये आकलन महत्वपूर्ण परिचालनों के किसी भी अंतर्निहित घटक में परिवर्तन की स्थिति में, साथ ही घटनाओं के बाद भी किए जाने चाहिए, ताकि सीखे गए पाठ और घटना के कारण उत्पन्न नए खतरों और कमजोरियों (यदि कोई हो) को ध्यान में रखा जा सके।

7. परिवर्तन प्रबंधन

सिद्धांत 7: वरिष्ठ प्रबंधन को यह सुनिश्चित करना चाहिए कि आरई की परिवर्तन प्रबंधन प्रक्रिया व्यापक हो, उसके पास समुचित संसाधन हों तथा प्रासंगिक सुरक्षा घेरों के बीच पर्याप्त रूप से स्पष्टता हो।

7.1 सामान्यतः, किसी आरई का परिचालन जोखिम तब विकसित होता है जब वह परिवर्तन आरंभ करता है, जैसे कि नई गतिविधियों में संलग्न होना या नए उत्पाद या सेवाएं विकसित करना; अपरिचित बाजारों या अधिकार क्षेत्रों में प्रवेश करना; नई व्यावसायिक प्रक्रियाओं या प्रौद्योगिकी प्रणालियों को क्रियान्वित करना या संशोधित करना; और/या ऐसे व्यवसायों में संलग्न होना जो भौगोलिक दृष्टि से मुख्यालय से दूर हों। परिवर्तन प्रबंधन को प्रारंभ से लेकर समाप्ति तक (उदाहरण के लिए किसी उत्पाद के संपूर्ण जीवन चक्र के दौरान) समय के साथ संबद्ध जोखिमों के क्रम-विकास का आकलन करना चाहिए[8]).

7.2 आरई के पास सहमत वस्तुनिष्ठ मानदंडों के आधार पर परिवर्तन की पहचान करने, प्रबंधन करने, चुनौती देने, अनुमोदन करने और निगरानी करने के लिए प्रक्रिया को परिभाषित करने वाली नीतियां और प्रक्रियाएं होनी चाहिए। परिवर्तन कार्यान्वयन की निगरानी विशिष्ट निरीक्षण नियंत्रणों द्वारा की जानी चाहिए। परिवर्तन प्रबंधन नीतियों और प्रक्रियाओं की स्वतंत्र और नियमित समीक्षा और

[8] किसी उत्पाद या सेवा के जीवन चक्र में विकास, चल रहे परिवर्तन, ग्रैंडफादरिंग और समापन तक विभिन्न चरण शामिल होते हैं। वास्तव में, जोखिम का स्तर बढ़ सकता है, उदाहरण के लिए जब नए उत्पाद, सेवाएँ, गतिविधियाँ, प्रक्रियाएँ, या प्रणालियाँ परिचयात्मक स्तर से उस स्तर तक परिवर्तित हो जाती हैं जो राजस्व या व्यवसाय-महत्वपूर्ण संचालन के भौतिक स्रोतों का प्रतिनिधित्व करता है।

अद्यतन के अधीन होना चाहिए, और विशेष रूप से त्रिस्तरीय सुरक्षा मॉडल के अनुसार भूमिकाओं और जिम्मेदारियों को स्पष्ट रूप से आवंटित किया जाना चाहिए:

7.2.1 सुरक्षा के पहले घेरे को नए उत्पादों, सेवाओं, गतिविधियों, प्रक्रियाओं और प्रणालियों का परिचालन जोखिम और नियंत्रण मूल्यांकन करना चाहिए, जिसमें निर्णय लेने और योजना बनाने के चरणों से लेकर परिवर्तन के कार्यान्वयन और कार्यान्वयन के बाद की समीक्षा तक आवश्यक परिवर्तन की पहचान और मूल्यांकन शामिल है।

7.2.2 सुरक्षा के दूसरे घेरे (ओओआरएफ) को सुरक्षा की पहले घेरे के परिचालन जोखिम और नियंत्रण आकलन को चुनौती देनी चाहिए, साथ ही उचित नियंत्रण या उपचारात्मक कार्यों के कार्यान्वयन की निगरानी करनी चाहिए। ओओआरएफ में इस प्रक्रिया के सभी चरणों को शामिल किया जाना चाहिए। इसके अलावा, ओओआरएफ को यह सुनिश्चित करना चाहिए कि सभी प्रासंगिक नियंत्रण समूह (जैसे, वित्त, अनुपालन, कानूनी, व्यवसाय, आईसीटी, जोखिम प्रबंधन) उचित रूप से शामिल हों।

7.2.3 सुरक्षा के तीसरे घेरे अनुच्छेद 3.2.3 में परिभाषित अधिदेश के अनुसार उपरोक्त की समीक्षा कर सकती है।

7.3 परिवर्तन प्रबंधन अभ्यास के एक भाग के रूप में, एक संशोधित संस्था के पास नए उत्पादों, सेवाओं, गतिविधियों, प्रक्रियाओं और प्रणालियों की समीक्षा और अनुमोदन के लिए नीतियां और प्रक्रियाएं होनी चाहिए। समीक्षा एवं अनुमोदन प्रक्रिया में निम्नलिखित बातों पर विचार किया जाना चाहिए:

7.3.1 अंतर्निहित जोखिम – जिसमें कानूनी, आईसीटी और मॉडल जोखिम शामिल हैं – अपरिचित बाजारों में नए उत्पादों, सेवाओं, गतिविधियों और परिचालनों के शुभारंभ (लॉन्च) में, तथा नई प्रक्रियाओं, लोगों और प्रणालियों के कार्यान्वयन में (विशेषकर जब तृतीय पक्ष की सेवाओं का उपयोग किया जाता है)।

7.3.2 आरई के परिचालन जोखिम प्रोफाइल, स्वीकार्यता और सहनशीलता में परिवर्तन, जिसमें मौजूदा उत्पादों या गतिविधियों, विशेष रूप से महत्वपूर्ण परिचालनों के जोखिम में परिवर्तन शामिल हैं।

7.3.3 आवश्यक नियंत्रण, जोखिम प्रबंधन प्रक्रियाएँ और जोखिम शमन रणनीतियाँ।

7.3.4 अवशिष्ट जोखिम।

7.3.5 प्रासंगिक जोखिम थ्रेशोल्ड या सीमाओं में परिवर्तन।

7.3.6 नए उत्पादों, सेवाओं, गतिविधियों, बाजारों, क्षेत्राधिकारों, प्रक्रियाओं और प्रणालियों के जोखिम का आकलन, निगरानी और प्रबंधन करने के लिए प्रक्रियाएं और मैट्रिक्स।

7.4 समीक्षा और अनुमोदन प्रक्रिया में यह सुनिश्चित करना शामिल होना चाहिए कि परिवर्तन लागू करने से पहले मानव संसाधन और प्रौद्योगिकी अवसंरचना के लिए उचित निवेश किया गया है। परिवर्तनों की निगरानी, उनके कार्यान्वयन के दौरान और उसके बाद की जानी चाहिए, ताकि अपेक्षित परिचालन जोखिम प्रोफाइल में किसी भी भौतिक अंतर की पहचान की जा सके और किसी भी अप्रत्याशित जोखिम का प्रबंधन किया जा सके।

7.5 परिवर्तनों की निगरानी को सुविधाजनक बनाने के लिए आरई को अपने उत्पादों और सेवाओं का यथासंभव (तृतीय पक्ष की व्यवस्था सहित) एक केंद्रीय रिकॉर्ड बनाए रखना चाहिए।

7.6 आरई को परिचालन आघात-सहनीयता सुनिश्चित करने के लिए महत्वपूर्ण परिचालनों के वितरण और उनके अंतर्संबंधों और अन्योन्याश्रितताओं पर संभावित प्रभावों का आकलन करने के तरीके के रूप में परिवर्तन प्रबंधन प्रक्रियाओं के अनुसार परिवर्तन प्रबंधन क्षमताओं का लाभ उठाना चाहिए।

8. निगरानी एवं रिपोर्टिंग

सिद्धांत 8: वरिष्ठ प्रबंधन को परिचालन जोखिम प्रोफाइल और भौतिक परिचालन जोखिमों की नियमित निगरानी के लिए एक प्रक्रिया लागू करनी चाहिए। परिचालन जोखिम के सक्रिय प्रबंधन करने के लिए निदेशक मंडल, वरिष्ठ प्रबंधन और व्यावसायिक इकाई स्तरों पर उचित रिपोर्टिंग तंत्र मौजूद होना चाहिए।

8.1 एक विनियमित संस्था को यह सुनिश्चित करना चाहिए कि उसकी रिपोर्टें व्यापक, सटीक, सुसंगत और सभी व्यावसायिक इकाइयों और उत्पादों पर लागू होने योग्य हों। इस उद्देश्य के लिए, सुरक्षा के पहले घेरे को परिचालन जोखिम घटनाओं, नियंत्रण कमियों, प्रक्रिया अपर्याप्तताओं और परिचालन जोखिम सहनशीलता के गैर-अनुपालन सहित किसी भी अवशिष्ट परिचालन जोखिम पर रिपोर्टिंग सुनिश्चित करनी चाहिए। रिपोर्ट का दायरा और मात्रा प्रबंधनीय होनी चाहिए, जिसमें आरई के परिचालन जोखिम प्रोफाइल पर दृष्टिकोण और परिचालन जोखिम स्वीकार्यता तथा सहनशीलता विवरण का अनुपालन शामिल हो; प्रभावी निर्णय लेने में डेटा की अत्यधिक मात्रा और कमी दोनों के कारण बाधा आती है।

8.2 आरई द्वारा रिपोर्टिंग समय पर होनी चाहिए तथा सामान्य एवं तनावपूर्ण दोनों बाजार स्थितियों में रिपोर्ट तैयार करने में सक्षम होनी चाहिए[9]। रिपोर्टिंग की आवृत्ति में शामिल जोखिम तथा परिचालन पर्यावरण में परिवर्तन की गति और प्रकृति प्रतिबिंबित होनी चाहिए। निगरानी गतिविधियों के परिणामों को नियमित प्रबंधन और बोर्ड रिपोर्टों में शामिल किया जाना चाहिए, जैसे कि आंतरिक/बाह्य लेखापरीक्षा और/या जोखिम प्रबंधन कार्यों द्वारा किए गए ओआरएमएफ के आकलन को शामिल किया जाना चाहिए। पर्यवेक्षी प्राधिकारियों द्वारा या उनके लिए तैयार की गई रिपोर्टें आंतरिक रूप से वरिष्ठ प्रबंधन और निदेशक मंडल को भी भेजी जानी चाहिए।

8.3 परिचालन जोखिम रिपोर्ट में आंतरिक वित्तीय, परिचालन और अनुपालन संकेतक, के साथ ही निर्णय लेने के लिए प्रासंगिक घटनाओं तथा स्थितियों के बारे में विदेशी बाजार या पर्यावरणीय जानकारी देते हुए आरई के परिचालन जोखिम प्रोफ़ाइल का वर्णन किया जाना चाहिए।

परिचालन जोखिम रिपोर्ट में निम्नलिखित शामिल हो:	आरई की जोखिम स्वीकार्यता और सहनशीलता विवरण, साथ ही थ्रेशोल्ड, सीमाएं या गुणात्मक आवश्यकताओं का उल्लंघन।
	प्रमुख एवं उभरते जोखिमों पर चर्चा एवं मूल्यांकन।
	हाल की महत्वपूर्ण आंतरिक परिचालन जोखिम घटनाओं और हानियों का विवरण (मूल कारण विश्लेषण सहित)।
	निकट चूक की पहचान और नियंत्रण की प्रभावकारिता का आकलन।
	प्रासंगिक बाह्य घटनाएँ या विनियामक परिवर्तन और आरई पर कोई संभावित प्रभाव।

8.4 डेटा कैप्चर और जोखिम रिपोर्टिंग प्रक्रियाओं का समय-समय पर विश्लेषण किया जाना चाहिए जिनका लक्ष्य जोखिम प्रबंधन प्रदर्शन को सुधारने के साथ-साथ जोखिम प्रबंधन नीतियों, प्रक्रियाओं और प्रथाओं को आगे बढ़ाने का होना चाहिए।

8.5 इसके अलावा, वरिष्ठ प्रबंधन तंत्र द्वारा आरई की व्यावसायिक इकाइयों में चल रही परिचालन के आघात-सहनीयता पर बोर्ड को समय पर रिपोर्ट देनी चाहिए ताकि बोर्ड को निगरानी करने में सुविधा रहें, विशेषकर जब बड़ी कमियाँ आरई के महत्वपूर्ण कार्यों की डिलीवरी को प्रभावित कर सकती हैं।

[9] रिपोर्टिंग प्रभावी जोखिम डेटा एकत्रीकरण और जोखिम रिपोर्टिंग के लिए बीसीबीएस के सिद्धांतों के अनुरूप होनी चाहिए (https://www.bis.org/publ/bcbs239.pdf)।

9. नियंत्रण एवं शमन

सिद्धांत 9: आरई के पास एक मजबूत नियंत्रण परिवेश होना चाहिए जो नीतियों, प्रक्रियाओं तथा प्रणालियों; उपयुक्त आंतरिक नियंत्रण; और उचित जोखिम शमन और/या स्थानांतरण रणनीतियों का उपयोग करता हो।

9.1 आंतरिक नियंत्रण को इस प्रकार डिज़ाइन किया जाना चाहिए जिससे उचित आश्वासन मिले कि आरई में कुशल और प्रभावी कार्य होगा; इसकी आस्तियों की सुरक्षा होगी; विश्वसनीय वित्तीय रिपोर्ट तैयार होगी; और लागू कानूनों और विनियमों का अनुपालन होगा। एक सुदृढ़ आंतरिक नियंत्रण कार्यक्रम में चार घटक होते हैं जो जोखिम प्रबंधन प्रक्रिया के अभिन्न अंग हैं: जोखिम मूल्यांकन, नियंत्रण गतिविधियाँ, सूचना और संचार, और निगरानी गतिविधियाँ[10]।

9.2 नियंत्रण क्रियाओं और प्रक्रियाओं में ऐसी प्रणाली शामिल होनी चाहिए जिससे नीतियों, विनियमों और कानूनों का अनुपालन सुनिश्चित किया जा सकें। नीति अनुपालन मूल्यांकन के प्रमुख तत्वों के निम्नलिखित उदाहरण हैं:

नीति अनुपालन मूल्यांकन के प्रमुख तत्वों के उदाहरण हैं:

- उल्लिखित उद्देश्यों की दिशा में प्रगति की शीर्ष-स्तरीय समीक्षा
- प्रबंधन नियंत्रण के अनुपालन का सत्यापन
- गैर-अनुपालन के मामलों के आचरण और समाधान की समीक्षा
- अपेक्षित अनुमोदन और प्राधिकरणों का मूल्यांकन ताकि प्रबंधन के उचित स्तर पर जवाबदेही सुनिश्चित की जा सकें
- निर्धारित या सीमा, प्रबंधन ओवरराइड और नीति, विनियमों और कानूनों से अन्य विचलन के लिए अनुमोदित अपवादों हेतु रिपोर्ट की ट्रैकिंग

9.3 नियंत्रण क्रियाओं और प्रक्रियाओं में इस बात पर ध्यान देना चाहिए कि आरई किस प्रकार सामान्य परिस्थितियों में और व्यवधान की स्थिति में संबंधित कार्यों में सम्यक जांच को दर्शाते हुए कार्य

[10] "बैंकिंग संगठनों में आंतरिक नियंत्रण प्रणालियों के लिए रूपरेखा, सितंबर 1998" विषय पर बीसीबीएस पेपर में आंतरिक नियंत्रणों पर अधिक विस्तार से चर्चा की गई है।

संचालन की निरंतरता सुनिश्चित करती है, जो कि आरई के परिचालन आघात-सहनीयता दृष्टिकोण के अनुरूप है।

9.4 किसी प्रभावी नियंत्रण परिवेश के लिए कर्तव्यों के उचित पृथक्करण की भी आवश्यकता होती है। ऐसे असाइनमेंट जिनमें अन्य प्रत्युपाय या दोहरे नियंत्रण के बिना {उदाहरण के लिए, एक ऐसी प्रक्रिया जिसमें संवेदनशील कार्यों या सूचना की सुरक्षा के लिए दो या दो से अधिक अलग-अलग संस्थाओं (आमतौर पर व्यक्तियों) का उपयोग होता है} व्यक्तियों या किसी टीम को परस्पर विरोधी ड्यूटी करना होता हैं, उनमें हानियों, त्रुटियों या अन्य अनुचित कार्यों को छिपाया जा सकता है। इसलिए, जिन क्षेत्रों में हितों का टकराव उत्पन्न हो सकता है, उनकी पहचान करके, उन्हें कम किया जाना चाहिए और उनकी सावधानीपूर्वक निगरानी तथा समीक्षा की जानी चाहिए।

9.5 कर्तव्यों के पृथक्करण और दोहरे नियंत्रणों के अलावा, आरई को यह सुनिश्चित करना चाहिए कि परिचालन जोखिम से निपटने के लिए अन्य पारंपरिक आंतरिक नियंत्रण, जैसा उपयुक्त हो, मौजूद हैं। इन नियंत्रणों के कुछ उदाहरण नीचे तालिका में दिए गए हैं:

इन नियंत्रणों के उदाहरण हैं:
• अनुमोदन के लिए स्पष्ट रूप से स्थापित प्राधिकारी और/या प्रक्रियाएं
• निर्धारित जोखिम थ्रेशोल्ड या सीमाओं के अनुपालन की बारीकी से निगरानी
• आरई के आस्तियां और अभिलेखों तक पहुंच और उनके उपयोग के लिए सुरक्षा उपाय
• तकनीकी विशेषज्ञता बनाए रखने के लिए स्टाफिंग स्तर और प्रशिक्षण की उपयुक्तता
• उन व्यावसायिक इकाइयों या उत्पादों की पहचान करने के लिए सतत प्रक्रिया, जहां रिटर्न उचित अपेक्षाओं के अनुरूप प्रतीत नहीं होते है।
• लेन-देन और खातों का नियमित सत्यापन और समाधान
• अनिवार्य अवकाश नीति, जो संवेदनशील पदों या परिचालन क्षेत्रों में तैनात कर्मचारियों को प्रति वर्ष में एक बार निर्धारित अवधि के लिए अनिवार्य रूप से अवकाश पर भेजने की अनुमति देती है, जो कर्मचारी के लिए आश्चर्यकारक होती है।

9.6 प्रौद्योगिकी का प्रभावी उपयोग और सुदृढ़ कार्यान्वयन नियंत्रण परिवेश में योगदान दे सकता है। उदाहरण के लिए, मैन्युअल प्रक्रियाओं की तुलना में स्वचालित प्रक्रियाओं में त्रुटि की संभावना कम होती है। हालाँकि, स्वचालित प्रक्रियाओं में जोखिम होता हैं जिन पर सुदृढ़ प्रौद्योगिकी अभिशासन और आधारभूत संरचना जोखिम प्रबंधन कार्यक्रमों के माध्यम से निपटा जाना चाहिए।

9.7 आरई द्वारा प्रौद्योगिकी से संबंधित उत्पादों, सेवाओं, गतिविधियों, प्रक्रियाओं और वितरण चैनलों का उपयोग उनमें परिचालन जोखिम और भौतिक वित्तीय नुकसान की संभावना को उजागर करता है।

परिणामस्वरूप, आरई के पास परिचालन जोखिम प्रबंधन के समान सिद्धांतों के साथ प्रौद्योगिकी जोखिमों की पहचान, माप, निगरानी और प्रबंधन के लिए एक एकीकृत दृष्टिकोण होना चाहिए। (इस मार्गदर्शी नोट का पैराग्राफ 15 भी देखें)

9.8 जबकि तृतीय-पक्ष सेवा प्रदाताओं जैसी संस्थाओं की सहायता लेने से लागत प्रबंधन, विशेषज्ञता प्रदान करने, उत्पाद की पेशकश का विस्तार करने और सेवाओं में सुधार करने में मदद मिल सकती है, यह उन जोखिमों को भी पेश करता है जिनसे आरई को निपटना चाहिए। आरई द्वारा अपने ओआरएमएफ के लिए अपनाए गए एकीकृत दृष्टिकोण में ऐसी तृतीय-पक्ष निर्भरताएं आवश्यक रूप से शामिल होनी चाहिए। अन्य बातों के अलावा, तृतीय-पक्ष के सेवा प्रदाताओं के संबंध में संकेंद्रण जोखिम, जटिलता और डाउनस्ट्रीम निर्भरता को ध्यान में रखा जाना चाहिए। तथापि, ये जोखिम अपरिहार्य हो सकते हैं, ऐसे जोखिमों की पहचान और निगरानी से आरई ऐसी कार्रवाई शुरू कर सकते हैं जो जोखिमों को उचित रूप से कम या प्रबंधित कर सकती है। इन जोखिम नीतियों और जोखिम प्रबंधन गतिविधियों में महत्वपूर्ण संचालन प्रबंधन और निर्भरता प्रबंधन शामिल होना चाहिए। (इस मार्गदर्शी नोट के पैराग्राफ 12 को भी देखें)

9.9 उन परिस्थितियों में जहां आंतरिक नियंत्रण जोखिम से पर्याप्त रूप से निपटते नहीं हैं और जोखिम से बाहर निकलना एक उचित विकल्प नहीं है, वहाँ प्रबंधन जोखिम को किसी अन्य पक्ष, जैसे बीमा के माध्यम से, को अंतरित करके नियंत्रण को पूरक कर सकता है। निदेशक मंडल को यह निर्धारित करना चाहिए कि आरई कितनी अधिकतम हानि जोखिम उठा सकती है तथा उसके पास कितनी वित्तीय क्षमता है और निदेशक मंडल को आरई के जोखिम और बीमा प्रबंधन कार्यक्रम, जिसमें आरई की विशिष्ट बीमा या जोखिम अंतरण आवश्यकताएं शामिल हैं, की वार्षिक समीक्षा करनी चाहिए।

9.10 चूंकि जोखिम अंतरण सुदृढ़ नियंत्रण और जोखिम प्रबंधन कार्यक्रमों के लिए एक अपूर्ण विकल्प है, इसलिए आरई को जोखिम अंतरण उपकरणों को आंतरिक परिचालन जोखिम नियंत्रणों के प्रतिस्थापन के बजाय पूरक के रूप में देखना चाहिए। विशिष्ट परिचालन जोखिम त्रुटियों को तुरंत पहचानने और सुधारने के लिए क्रियाविधि के होने से जोखिम को काफी कम किया जा सकता है। इस बात पर भी सावधानीपूर्वक विचार करने की आवश्यकता है कि जोखिम शमन उपकरण जैसे बीमा वास्तव में किस हद तक जोखिम को कम करते हैं, जोखिम को किसी अन्य व्यावसायिक सेक्टर या क्षेत्र में अंतरित करते हैं, या एक नया जोखिम पैदा करते हैं (उदाहरण के लिए, प्रतिपक्ष जोखिम, कानूनी जोखिम)।

स्तंभ 2: आघात-सहनीयता निर्मिति

10 परिचालन आघात-सहनीयता के आवश्यक तत्व

10.1 परिचालन आघात-सहनीयता एक ऐसा परिणाम है जो परिचालन जोखिम के प्रभावी प्रबंधन से लाभान्वित होता है। जोखिम की पहचान तथा मूल्यांकन, जोखिम शमन (नियंत्रण के कार्यान्वयन सहित) और जोखिमों की निगरानी तथा नियंत्रण प्रभावशीलता जैसी गतिविधियां परिचालन संबंधी व्यवधानों और उनके प्रभावों को कम करने के लिए मिलकर काम करती हैं। परिचालन आघात-सहनीयता का व्यापक सिद्धांत यह स्वीकार करना है कि व्यवधान उत्पन्न होंगे और आरई को तदनुसार प्रतिक्रिया देने के लिए तैयार रहना होगा और प्रभाव को सीमित करने के लिए उपाय करने होंगे। आरई को यह सुनिश्चित करना होगा कि उन्होंने प्रभावी ढंग से तैयारी की है और उनमें अपने महत्वपूर्ण कार्यों पर न्यूनतम प्रभाव के साथ व्यवधानों का सामना करने, अवशोषित करने, प्रतिक्रिया देने, अनुकूलन तथा उबरने और सीखने का लचीलापन है। इसके अलावा, व्यवधानों का जवाब देने और उनसे उबरने की आरई की क्षमता पर प्रबंधन का ध्यान, यह मानते हुए कि विफलताएं होंगी, परिचालन आघात-सहनीयता का समर्थन करेगा। संचालनात्मक रूप से लचीली आरई के कार्यों में असामयिक चूक और व्यवधानों से होने वाले नुकसान की संभावना कम होती है, जिससे महत्वपूर्ण कार्यों और संबंधित सेवाओं, कार्य-विधि और प्रणालियों पर प्रभाव कम होता है। हालांकि कुछ परिचालन जोखिमों जैसे महामारी से बचना संभव नहीं हो सकता है, लेकिन ऐसी घटनाओं के प्रति आरई के कार्यों के आघात-सहनीयता में सुधार करना संभव है।

10.2 कारोबार की निरंतरता, तृतीय-पक्ष पर निर्भरता और वह जिस तकनीक पर आरई भरोसा करती हैं, आरई के लिए अपने परिचालन आघात-सहनीयता को सुदृढ़ करते समय विचार करने के लिए महत्वपूर्ण कारक हैं।

10.3 आरई के लिए यह सुनिश्चित करना आवश्यक है कि मौजूदा जोखिम प्रबंधन ढांचे, व्यवसाय निरंतरता योजनाएं और तृतीय-पक्ष की निर्भरता प्रबंधन को संगठन के भीतर सुसंगतलागू किया जाए। चूंकि परिचालन आघात-सहनीयता व्यवसाय निरंतरता, तृतीय-पक्ष जोखिम प्रबंधन, आईसीटी और साइबर जोखिम प्रबंधन, घटना प्रबंधन और परिचालन जोखिम प्रबंधन के व्यापक पहलुओं जैसे तत्वों से आता है, यदि किसी आरई को अपने महत्वपूर्ण कार्यों के आघात-सहनीयता को बढ़ाना है, तो व्यवधान के प्रकार की परवाह किए बिना एक समग्र दृष्टिकोण आवश्यक है। किसी महत्वपूर्ण संचालन लेंस के माध्यम से परिचालन आघात-सहनीयता को स्वीकार करना, आरई और वित्तीय प्रणाली के लिए जो अत्यावश्यक या महत्वपूर्ण है उसे प्राथमिकता देने के लिए आरई को प्रोत्साहित करता है और उन कार्यों को करने में शामिल अंतर्संबंधों और अन्योन्याश्रितताओं को समझता है। इसलिए आरई को यह

सत्यापित करना चाहिए कि उनका परिचालन आघात-सहनीयता दृष्टिकोण उनकी समुत्थान और समाधान योजनाओं में निहित उल्लिखित कार्रवाइयों, संगठनात्मक मानचित्रण, महत्वपूर्ण कार्यों और महत्वपूर्ण साझा सेवाओं (उद्योग के लिए आवश्यक सेवाओं सहित), जो अंततः वित्तीय प्रणाली की स्थिरता के लिए महत्वपूर्ण हैं, के साथ उचित रूप से संगत है।

11. अंतर्संबंधों और अन्योन्याश्रितताओं का मानचित्रण

सिद्धांत 10: एक बार जब आरई ने अपने महत्वपूर्ण परिचालनों की पहचान कर ली है,तो उसे आंतरिक और बाहरी अंतर्संबंधों और अन्योन्याश्रितताओं को मैप करना चाहिए जो परिचालन आघात-सहनीयता के दृष्टिकोण के अनुरूप महत्वपूर्ण परिचालनों को करने के लिए आवश्यक हैं।

11.1 आरई के महत्वपूर्ण कार्यों को करने के लिए संबंधित कार्यों में जन, प्रौद्योगिकी, प्रक्रियाओं, सूचना, सुविधाओं और उनके बीच के अंतर्संबंधों और अन्योन्याश्रितताओं (अर्थात, पहचानना और दस्तावेजीकरण) को मानचित्रित करना चाहिए, जिसमें इसमें वे लोग भी शामिल हैं जो तृतीय-पक्ष या इंट्राग्रुप व्यवस्था पर निर्भर हैं, लेकिन इन्हीं तक सीमित नहीं हैं।

11.2 आरई महत्वपूर्ण परिचालनों की परिभाषाओं के लिए अपनी समुत्थान और समाधान योजनाओं, जैसा उचित हो, का लाभ उठा सकते हैं और उन्हें इस बात पर विचार करना चाहिए कि क्या उनके परिचालन आघात-सहनीयता के दृष्टिकोण उनके संबंधित समुत्थान और समाधान योजनाओं में निहित महत्वपूर्ण परिचालनों और महत्वपूर्ण तृतीय-पक्ष सेवा प्रदाताओं की संगठनात्मक मानचित्रण के साथ उचित रूप से संगत हैं।

11.3 आरई की जोखिम स्वीकार्यता और व्यवधान के प्रति सहनशीलता को ध्यान में रखते हुए, आरई के लिए मानचित्रण का दृष्टिकोण तथा कणिकी (ग्रैन्युलैरिटी) का पर्याप्त स्तर होना चाहिए ताकि सुभेद्यताओं की पहचान की जा सकें और व्यवधान की स्थिति में महत्वपूर्ण परिचालनों को करने की उनकी क्षमता के परीक्षण का समर्थन किया जा सकें। इस तरह की मानचित्रण आरई को सुभेद्यताओं को चिह्नित करने में सक्षम बनाएगी कि किस प्रकार महत्वपूर्ण परिचालन किए जा रहे हैं और यह पता लगाया जाए कि समुत्थान तथा समाधान योजनाओं का लाभ कहां उठाया जा सकता है। ऐसी सुभेद्यताओं के उदाहरणों में संकेंद्रण जोखिम, विफलता के एकल बिंदु और सेवा प्रदाताओं तथा संसाधनों की अपर्याप्त प्रतिस्थापनशीलता शामिल हो सकती है।

11.4 जहां कोई आरई किसी समूह का सदस्य है, उसे यह सुनिश्चित करना होगा कि समूह में कहीं और उत्पन्न होने वाले किसी भी अतिरिक्त जोखिम का हिसाब रखा जाए जो उसके कार्यों में गंभीर लेकिन संभावित व्यवधान से निपटने की उसकी क्षमता को प्रभावित कर सकता है।

12. तृतीय-पक्ष निर्भरता प्रबंधन

सिद्धांत 11: आरई को महत्वपूर्ण कार्यों को करने के लिए संबंधों पर अपनी निर्भरता का प्रबंधन करना चाहिए, जिसमें तृतीय-पक्ष (इंट्राग्रुप इकाइयां) शामिल हैं, लेकिन यह इन्हीं तक सीमित नहीं है।

12.1 आरई को अपने ओआरएमएफ,[11] तृतीय-पक्ष जोखिम प्रबंधन नीति और परिचालन आघात-सहनीयता दृष्टिकोण के अनुरूप तृतीय-पक्ष (जिसमें इंट्राग्रुप इकाइयां शामिल हैं) सहित, लेकिन जो इन्हीं तक सीमित नहीं है, व्यवस्था को करने से पहले जोखिम मूल्यांकन और सम्यक जांच करनी चाहिए। ऐसी व्यवस्था को करने से पहले, आरई को यह सत्यापित करना चाहिए कि क्या इन व्यवस्थाओं में शामिल तृतीय-पक्ष इंट्राग्रुप इकाई सहित के पास सामान्य परिस्थितियों और व्यवधान की स्थिति दोनों में आरई के महत्वपूर्ण परिचालनों की सुरक्षा उपाय हेतु उनके पास कम से कम समतुल्य स्तर का परिचालन आघात-सहनीयता है।

तृतीय-पक्ष सेवा प्रदाताओं के कुछ उदाहरण नीचे दी गई तालिका में दिए गए हैं (यह सूची विस्तृत न होकर सांकेतिक है)

तृतीय-पक्ष सेवा प्रदाताओं के उदाहरण		
प्रत्यक्ष बिक्री एजेंट	नकद/एटीएम प्रबंधन	आईटी/ संचालन वेंडर
उपभोक्ता सुविधा सेवाएं	बाहरी परामर्शदाता	विज्ञापन पार्टनर
वसूली एजेंसियां	वैश्लेषिकी सेवाएँ	स्टोरेज/बैकअप प्रदाता
भुगतान प्रसंस्करण फर्म	क्लाउड सेवा प्रदाता	लॉजिस्टिक्स प्रबंधन
मार्केटिंग एजेंट	विधिक सेवाएं	डेटा प्रबंधन

12.2 निदेशक मंडल और वरिष्ठ प्रबंधन तृतीय-पक्ष की व्यवस्था से जुड़े परिचालन जोखिमों को समझने और यह सुनिश्चित करने के लिए जिम्मेदार हैं कि ऐसी गतिविधियों में जोखिम का प्रबंधन करने के लिए प्रभावी जोखिम प्रबंधन नीतियां और प्रथाएं मौजूद हैं। सेवा प्रदाताओं के प्रबंधन पर बोर्ड द्वारा अनुमोदित नीति तृतीय-पक्ष पर निर्भरता से जुड़े जोखिमों के प्रबंधन के लिए महत्वपूर्ण है, चाहे वह आरई से संबंधित हो या नहीं। तृतीय-पक्ष जोखिम नीतियों (ओआरएमएफ की नीतियों के एक भाग के रूप में) और जोखिम प्रबंधन गतिविधियों में निम्नलिखित शामिल होना चाहिए:

[11] इस सिद्धांत में व्यक्त निर्भरता का प्रबंधन इस मार्गदर्शी नोट के नियंत्रण और जोखिम शमन नीतियों (सिद्धांत 9) के अनुरूप और संचालित किया जाना चाहिए।

12.2.1 यह निर्धारित करने की प्रक्रियाएँ कि क्या किसी सेवा के लिए तृतीय-पक्ष की व्यवस्था को करने की आवश्यकता है और ऐसी व्यवस्था को कैसे किया जाए।

12.2.2 संभावित सेवा प्रदाताओं के चयन में सम्यक जांच को करने की प्रक्रियाएँ।

12.2.3 तृतीय-पक्ष की व्यवस्था की सुदृढ़ संरचना, जिसमें डेटा के स्वामित्व और गोपनीयता के साथ समाप्ति अधिकार भी शामिल हैं।

12.2.4 सेवा प्रदाता की वित्तीय स्थिति सहित तृतीय-पक्ष की व्यवस्था से जुड़े जोखिमों के प्रबंधन और निगरानी के लिए कार्यक्रम।

12.2.5 आरई और सेवा प्रदाता पर एक प्रभावी नियंत्रण परिवेश तैयार करना जिसमें तृतीय-पक्ष के संबंधों का एक रजिस्टर (जो विभिन्न सेवाओं की अहमियत की पहचान करता हो) और सेवा प्रदाता की निगरानी को सुविधाजनक बनाने के लिए मेट्रिक्स और रिपोर्टिंग शामिल होनी चाहिए।

12.2.6 व्यवहार्य आकस्मिक योजनाओं का विकास।

12.2.7 व्यापक संविदा और/या सेवा स्तर करार (जो लागू करने योग्य हैं) का निष्पादन जिसमें तृतीय-पक्ष सेवा प्रदाता और आरई के बीच जिम्मेदारियों का स्पष्ट आवंटन हो, बशर्ते कि अंतिम जिम्मेदारी आरई की हो।

12.2.8 आरई के पर्यवेक्षी और समाधान प्राधिकारियों की तृतीय-पक्षों तक पहुंच।

12.3 महत्वपूर्ण परिचालनों के प्रावधान को प्रभावित करने वाले तृतीय-पक्ष के स्तर पर विफलता या व्यवधान की स्थिति में आरई को अपने परिचालन आघात-सहनीयता को बनाए रखने के लिए आकस्मिक योजना प्रक्रियाओं और निकास रणनीतियों तथा उचित कारोबार निरंतरता को विकसित करना चाहिए। आरई की व्यवसाय निरंतरता योजनाओं के तहत परिदृश्यों में आरई के महत्वपूर्ण परिचालनों के लिए सेवाएं प्रदान करने वाले तृतीय-पक्षों की प्रतिस्थापन क्षमता और ऐसे अन्य व्यवहार्य विकल्पों का आकलन करना चाहिए जो तृतीय-पक्ष में आउटेज होने पर परिचालन आघात-सहनीयता की सुविधा प्रदान करें, जैसे कि आरई की सेवाओं को आन्तरिक करना।

12.4 सेवा प्रदाताओं पर बढ़ती निर्भरता के साथ-साथ आपूर्ति श्रृंखलाओं में जटिलता भी बढ़ी है। बड़ी संख्या में सेवा प्रदाता सेवाओं को उप-संविदा पर दे रहे हैं जो स्वयं किसी सेवा के प्रावधान के लिए किसी अन्य सेवा प्रदाता (चौथे पक्ष) पर निर्भर हैं। कुछ मामलों में, ये चौथे पक्ष के सेवा प्रदाता, बदले में, किसी अन्य सेवा प्रदाता पर और आगे चलकर nवें सेवा प्रदाता तक निर्भर हो सकते हैं, इस प्रकार श्रृंखला को लंबा कर सकते हैं। इस तरह की व्यवस्था के परिणामस्वरूप आरई बिना किसी प्रत्यक्ष करार के डाउनस्ट्रीम सेवा प्रदाताओं पर निर्भर हो जाती है। ऐसी आपूर्ति श्रृंखला की असुरक्षितता और

पारदर्शिता की कमी आरई के लिए परिचालन जोखिम को बढ़ा सकती है। इससे आरई की आपूर्ति श्रृंखला में जोखिमों को प्रबंधित करने की क्षमता भी बाधित हो सकती है और साथ ही उस पर विनियामक की अपेक्षाओं पर भी असर पड़ सकता है। इसलिए, आरई से अपेक्षा की जाती है कि वे किसी भी अन्य डाउनस्ट्रीम सेवा प्रदाताओं से जुड़े जोखिमों के बारे में जागरूक रहें और उनका प्रबंधन करें, ताकि आपूर्ति श्रृंखला और संभावित मुद्दों की गहन समझ बनी रहें जो इकाई के अपने महत्वपूर्ण परिचालनोंको करने की क्षमता को प्रभावित कर सकती हैं। इसलिए, आरई को, सेवा प्रदाताओं के साथ अपने करार में, सेवा प्रदाता को अपने उप-संविदाकारों (आपूर्ति श्रृंखला में nवें पक्ष सहित) के कार्य-निष्पादन और जोखिम प्रबंधन प्रथाओं के लिए संविदात्मक रूप से उत्तरदायी बनाने वाले खंड शामिल करने चाहिए।

13. व्यवसाय निरंतरता योजना और परीक्षण

सिद्धांत 12: आरई के पास व्यवसाय निरंतरता योजनाएं होनी चाहिए ताकि निरंतर आधार पर काम करने की उनकी क्षमता और गंभीर व्यवसाय व्यवधान होने पर घाटे को सीमित करना सुनिश्चित किया जा सकें। व्यवसाय निरंतरता योजनाओं को आरई के ओआरएमएफ से जोड़ा जाना चाहिए। आरई को कई गंभीर लेकिन संभावित परिदृश्यों के तहत कारोबार निरंतरता अभ्यास करना चाहिए ताकि व्यवधान की स्थिति में महत्वपूर्ण परिचालनों को करने की उनकी क्षमता का परीक्षण किया जा सकें।

13.1 आरई की कारोबार निरंतरता योजना के सुदृढ़ और प्रभावी प्रशासन के लिए निम्नलिखित आवश्यक है:

13.1.1 निदेशक मंडल द्वारा अनुमोदन और नियमित समीक्षा।

13.1.2 इसके कार्यान्वयन में वरिष्ठ प्रबंधन और व्यावसायिक इकाइयों के लीडर की मजबूत भागीदारी।

13.1.3 इसके डिज़ाइन के प्रति सुरक्षा के पहले और दूसरे घेरो की प्रतिबद्धता।

13.1.4 सुरक्षा के तीसरे घेरे द्वारा नियमित समीक्षा।

13.2 आरई को प्रासंगिक प्रभाव आकलन और समुत्थान प्रक्रियाओं से जुड़े परिदृश्य विश्लेषण के साथ भविष्योन्मुखी व्यवसाय निरंतरता योजना (बीसीपी) तैयार करनी चाहिए:

13.2.1 आरई की अपनी व्यवसाय निरंतरता योजना संभावित व्यवधानों के परिदृश्य विश्लेषण पर आधारित होनी चाहिए। व्यवसाय निरंतरता योजना में महत्वपूर्ण व्यावसायिक कार्यों और प्रमुख आंतरिक या बाहरी निर्भरताओं की पहचान करना और वर्गीकरण करना शामिल होना चाहिए। ऐसा

करने में, आरई को अपनी सभी व्यावसायिक इकाइयों के साथ-साथ महत्वपूर्ण प्रदाताओं और प्रमुख तृतीय पक्षों को भी कवर करना चाहिए।

13.2.2 प्रत्येक परिदृश्य को अपने वित्तीय, परिचालन, कानूनी और प्रतिष्ठित परिणामों के संबंध में मात्रात्मक और गुणात्मक प्रभाव मूल्यांकन या व्यावसायिक प्रभाव विश्लेषण (बीआईए) के अधीन होना चाहिए।

13.2.3 व्यवसाय निरंतरता प्रक्रिया के सक्रियण के लिए व्यवधान परिदृश्यों को न्यूनतम थ्रेशोल्ड या सीमा (जैसे अधिकतम सहनीय आउटेज) के अधीन होना चाहिए। व्यवसाय निरंतरता प्रक्रिया को निर्धारित समुत्थान समयावधि उद्देश्यों (आरटीओ) और समुत्थान बिंदु उद्देश्यों (आरपीओ) को पूरा करना चाहिए। इस प्रक्रिया में समुत्थान रणनीतियों और कार्यप्रणाली, बहाली पहलुओं के साथ-साथ प्रबंधन, कर्मचारियों, विनियामक प्राधिकारियों, ग्राहकों, आपूर्तिकर्ताओं और जहां उपयुक्त हो वहां अन्य अधिकारियों को सूचित करने के लिए संचार दिशानिर्देशों को भी होना चाहिए।

13.2.4 इन योजनाओं में परीक्षण कार्यक्रम, प्रशिक्षण तथा जागरूकता कार्यक्रम, और संचार तथा संकट प्रबंधन कार्यक्रम भी शामिल होने चाहिए।

13.3 व्यवसाय निरंतरता योजनाओं को तृतीय-पक्ष और इंट्राग्रुप इकाइयों के साथ संबंधों के माध्यम से, लेकिन यह इन्हीं तक सीमित नहीं है, नियमित व्यवसाय निरंतरता प्रक्रिया विकसित, कार्यान्वित और बनाए रखनी चाहिए जिसमें महत्वपूर्ण परिचालन और उनके अंतर्संबंध और अन्योन्याश्रितताओंशामिल हैं। व्यवसाय निरंतरता प्रक्रिया को गंभीर लेकिन संभावित परिदृश्यों की एक श्रृंखला के लिए संचालित और मान्य किया जाना चाहिए जिसमें विघटनकारी आकस्मिताएं और घटनाएं शामिल हों। अन्य व्यवसाय निरंतरता लक्ष्यों में, कारोबार निरंतरता प्रक्रिया को स्टाफ के प्रशिक्षण और स्टाफ की परिचालन आघात-सहनीयता जागरूकता का समर्थन करना चाहिए, जिसे विशिष्ट मामलों के आधार पर अनुकूलित किया जाना चाहिए ताकि वे घटनाओं पर प्रभावी ढंग से अनुकूलन कर सकें और प्रतिक्रिया दे सकें।

13.4 आरई के आपदा समुत्थान ढांचे को लागू करने के लिए व्यवसाय निरंतरता योजनाओं में विस्तृत मार्गदर्शन होना चाहिए। इन योजनाओं में परिचालन संबंधी व्यवधानों के प्रबंधन के लिए भूमिकाएं और जिम्मेदारियां होनी चाहिए और ऐसे व्यवधान, जो मुख्य कर्मचारीगण को प्रभावित करते हों, होने पर प्राधिकारी के उत्तराधिकार के संबंध में स्पष्ट मार्गदर्शन होना चाहिए। इसके अतिरिक्त, इन योजनाओं में आंतरिक निर्णय लेने की प्रक्रिया को स्पष्ट रूप से निर्धारित किया जाना चाहिए और आरई की व्यवसाय निरंतरता योजना को लागू करने के लिए ट्रिगर्स को परिभाषित किया जाना चाहिए।

13.5 आरई की समुत्थान और समाधान योजनाओं में निहित महत्वपूर्ण परिचालनों और महत्वपूर्ण तृतीय-पक्ष सेवाओं को करने के लिए उनकी व्यवसाय निरंतरता योजनाएं उनके परिचालन आघात-सहनीयता दृष्टिकोण के अनुरूप होनी चाहिए।

13.6 आरई को समय-समय पर अपनी व्यवसाय निरंतरता योजनाओं और नीतियों की समीक्षा करनी चाहिए ताकि यह सुनिश्चित हो सके कि रणनीतियाँ वर्तमान परिचालनों, जोखिमों और खतरों के अनुरूप बनी रहें। व्यवसाय निरंतरता प्रक्रियाओं का समय-समय पर परीक्षण किया जाना चाहिए ताकि यह सुनिश्चित किया जा सके कि समुत्थान तथा बहाली के उद्देश्यों और समय-सीमाओं को पूरा किया जा सके। जहां संभव हो, आरई को सेवा प्रदाताओं के साथ कारोबार निरंतरता परीक्षण में भाग लेना चाहिए। औपचारिक परीक्षण और समीक्षा गतिविधियों के परिणाम वरिष्ठ प्रबंधन और निदेशक मंडल को सूचित किए जाने चाहिए।

13.7 कोविड-19 को देखते हुए, विभिन्न प्रकार की भविष्य की महामारियों के लिए तैयारी, आरई की सर्वोच्च प्राथमिकताओं में से एक होनी चाहिए। ऐसी महामारी में आरई के सामने एक प्रमुख चुनौती कम स्टाफ की उपलब्धता की संभावना है जो व्यवसाय संचालन को संभावित रूप से लंबे समय तक बाधित कर सकती है। इसलिए आरई की व्यवसाय निरंतरता योजना में ऐसी भविष्य की महामारियों के प्रभाव को कम करने के उपाय शामिल होने चाहिए। आरई को भविष्य के प्रकोप के विभिन्न चरणों या ऐसी किसी भी अप्रत्याशित परिस्थितियों से निपटने के लिए एक व्यापक संगठन-व्यापी तैयारी और प्रतिक्रिया योजना बनानी चाहिए। योजना को अधिमानतः आरई के व्यापक ओआरएमएफ के साथ संरेखित होना चाहिए।

14. घटना प्रबंधन

सिद्धांत 13: आरई को उन घटनाओं को प्रबंधित करने के लिए प्रतिक्रिया और पुनर्प्राप्ति योजनाओं को विकसित और कार्यान्वित करना चाहिए जो आरई की जोखिम स्वीकार्यता और व्यवधान के प्रति सहनशीलता के अनुरूप महत्वपूर्ण परिचालनोंके वितरण को बाधित कर सकते हैं। आरई को पिछली घटनाओं से सीखे गए पाठ को शामिल करके अपनी घटना प्रतिक्रिया और पुनर्प्राप्ति योजनाओं में लगातार सुधार करना चाहिए।

14.1 आरई को अपनी प्रतिक्रिया और पुनर्प्राप्ति क्षमताओं का समर्थन करने के लिए घटना प्रतिक्रिया और पुनर्प्राप्ति, आंतरिक और तृतीय पक्ष के संसाधनों की एक सूची बनाए रखनी चाहिए।

14.2 घटना प्रबंधन के दायरे में किसी घटना के जीवन चक्र को शामिल किया जाना चाहिए,[12] जिसमें आम तौर पर निम्नलिखित शामिल हैं, लेकिन इन्हीं तक सीमित नहीं हैं:

14.2.1 पूर्वनिर्धारित मानदंडों के आधार पर किसी घटना की गंभीरता का वर्गीकरण (उदाहरण के लिए, सामान्य रूप से व्यवसाय को हमेशा की तरह बहाल करने का अपेक्षित समय), किसी घटना पर प्रतिक्रिया देने के लिए संसाधनों की उचित प्राथमिकता और असाइनमेंट को सक्षम करना।

14.2.2 घटना की प्रतिक्रिया और पुनर्प्राप्ति प्रक्रियाएं, जिसमें आरई की व्यवसाय निरंतरता, आपदा समुत्थान और अन्य संबंधित प्रबंधन योजनाओं और प्रक्रियाओं से उनका संबंध शामिल है।

14.2.3 आंतरिक और बाहरी दोनों हितधारकों (उदाहरण के लिए, नियामक अधिकारियों) को घटनाओं की रिपोर्ट करने के लिए संचार योजनाओं का कार्यान्वयन, जिसमें किसी घटना के दौरान प्रदर्शन मेट्रिक्स और सीखे गए पाठ का विश्लेषण शामिल है। यदि आवश्यक हो, तो आंतरिक संचार योजना में प्रमुख निर्णयकर्ता ओं, परिचालन कर्मचारियों और तृतीय पक्षों के साथ संवाद करने के तरीके पर एस्केलेशन रूट शामिल होने चाहिए। बाह्य संचार योजना में यह रेखांकित किया जाना चाहिए कि व्यवधान के दौरान इकाई अपने ग्राहकों, हितधारकों और विनियामकों के साथ कैसे संवाद करेगी।

14.3 आरई द्वारा घटना प्रतिक्रिया और पुनर्प्राप्ति प्रक्रियाओं की समय-समय पर समीक्षा, परीक्षण और अद्यतन किया जाना चाहिए। उन्हें सिलसिलेवार पुनरावृत्ति को रोकने या कम करने के लिए घटनाओं के मूल कारणों की भी पहचान करनी चाहिए और उनका समाधान करना चाहिए।

14.4 घटना प्रबंधन कार्यक्रम को अद्यतन करते समय दूसरों द्वारा अनुभव की गई घटनाओं के साथ-साथ निकट चूक सहित पिछली घटनाओं से सीखे गए पाठ को विधिवत प्रतिबिंबित किया जाना चाहिए। आरई के घटना प्रबंधन कार्यक्रम को आरई को प्रभावित करने वाली सभी घटनाओं का प्रबंधन करना चाहिए, जिसमें निर्भरता के कारण होने वाली घटनाएं भी शामिल हैं, लेकिन यह तृतीय पक्ष और इंट्राग्रुप संस्थाओं तक सीमित नहीं है।

[12] यह स्वीकार करते हुए कि किसी घटना का जीवन चक्र समय के कई मापों तक फैल सकता है जो घंटों से लेकर हफ्तों और महीनों तक हो सकता है।

15. साइबर सुरक्षा सहित सूचना और संचार प्रौद्योगिकी (आईसीटी)

सिद्धांत 14: आरई को अपने ओआरएमएफ के अनुरूप एक मजबूत सूचना और संचार प्रौद्योगिकी (आईसीटी) जोखिम प्रबंधन कार्यक्रम लागू करना चाहिए और एक आघात-सहनीय आईसीटी सुनिश्चित करना चाहिए इसमें साइबर सुरक्षा भी शामिल है जो सुरक्षा, पता लगाने, प्रतिक्रिया और पुनर्प्राप्ति कार्यक्रमों के अधीन है जिनका नियमित रूप से परीक्षण किया जाता है, उचित स्थितिजन्य जागरूकता को शामिल किया जाता है और आरई के महत्वपूर्ण संचालन के वितरण को पूरी तरह से समर्थन और सुविधा प्रदान करने के लिए जोखिम प्रबंधन और निर्णय लेने की प्रक्रियाओं के लिए प्रासंगिक समय पर जानकारी दी जाती है।

15.1 किसी आरई के लिए अपना व्यवसाय ठीक से संचालित करने के लिए प्रभावी आईसीटी प्रदर्शन और सुरक्षा सर्वोपरि है। सुदृढ़ आईसीटी जोखिम प्रबंधन का उचित उपयोग और कार्यान्वयन नियंत्रण परिवेश की प्रभावशीलता में योगदान देता है और आरई के रणनीतिक उद्देश्यों की प्राप्ति के लिए मौलिक है। आरई के आईसीटी जोखिम मूल्यांकन को यह सुनिश्चित करना चाहिए कि उसका आईसीटी उसके संचालन को पूरी तरह से समर्थन और सुविधा प्रदान करता है। आईसीटी जोखिम प्रबंधन को आरई के प्रत्यक्ष नुकसान, कानूनी दावों, प्रतिष्ठित क्षति, आईसीटी व्यवधान और प्रौद्योगिकी के दुरुपयोग को उसकी जोखिम स्वीकार्यता और सहनशीलता विवरण के अनुरूप परिचालन जोखिम को कम करना चाहिए।

15.2 आईसीटी जोखिम प्रबंधन में शामिल हैं:

15.2.1 महत्वपूर्ण जानकारी, आस्ति और बुनियादी ढांचे सहित आईसीटी जोखिम की पहचान और मूल्यांकन।

15.2.2 आईसीटी जोखिम शमन उपाय मूल्यांकन किए गए जोखिम स्तर के अनुरूप हैं (उदाहरण के लिए साइबर सुरक्षा, प्रतिक्रिया और पुनर्प्राप्ति कार्यक्रम, आईसीटी परिवर्तन प्रबंधन प्रक्रियाएं, आईसीटी घटना प्रबंधन प्रक्रियाएं, समय पर उपयोगकर्ताओं को प्रासंगिक सूचना प्रसारण सहित)।

15.2.3 इन उपायों की निगरानी (नियमित परीक्षण सहित)।

15.3 आरई के पास साइबर सुरक्षा सहित एक दस्तावेजित आईसीटी नीति होनी चाहिए, जो अभिशासन और निरीक्षण आवश्यकताओं, जोखिम स्वामित्व और जवाबदेही, आईसीटी सुरक्षा उपाय (उदाहरण के लिए, पहुंच नियंत्रण, महत्वपूर्ण सूचना आस्ति संरक्षण, पहचान प्रबंधन), साइबर सुरक्षा नियंत्रण और घटना प्रतिक्रिया के आवधिक मूल्यांकन और निगरानी, साथ ही व्यवसाय निरंतरता और आपदा समुत्थान योजनाओं को निर्धारित करती है।

15.4 डेटा और सिस्टम की गोपनीयता, अखंडता और उपलब्धता सुनिश्चित करने के लिए, निदेशक मंडल/उसकी समिति को नियमित रूप से आरई के आईसीटी जोखिम प्रबंधन की प्रभावशीलता की निगरानी करनी चाहिए और वरिष्ठ प्रबंधन को नियमित रूप से आरई के आईसीटी जोखिम प्रबंधन के डिजाइन, कार्यान्वयन और प्रभावशीलता का मूल्यांकन करना चाहिए। इसके लिए व्यवसाय, जोखिम प्रबंधन और आईसीटी रणनीतियों के नियमित संरेखण की आवश्यकता होती है जो आरई की जोखिम स्वीकार्यता और सहनशीलता विवरण के साथ-साथ गोपनीयता और अन्य लागू कानूनों के अनुरूप हों। आरई को अपनी आईसीटी की लगातार निगरानी करनी चाहिए और नियमित रूप से आईसीटी जोखिमों, नियंत्रणों और घटनाओं पर वरिष्ठ प्रबंधन को रिपोर्ट करनी चाहिए।

15.5 आरई द्वारा निर्धारित पूरक प्रक्रियाओं के साथ आईसीटी जोखिम प्रबंधन होना चाहिए:

15.5.1 प्रासंगिक उद्योग मानकों और सर्वोत्तम प्रथाओं के साथ-साथ उभरते खतरों (उदाहरण के लिए, साइबर) और विकसित या नई प्रौद्योगिकियों के विरुद्ध पूर्णता के लिए नियमित आधार पर समीक्षा की जानी चाहिए। आईसीटी से संबंधित जोखिमों के प्रति आघात-सहनीयता सुनिश्चित करने के लिए महत्वपूर्ण सूचना आस्तियों के लिए खतरा प्रोफ़ाइल की अधिक लगातार आधार पर समीक्षा और कमजोरियों के लिए परीक्षण किया जाना चाहिए;

15.5.2 घोषित जोखिम सहनशीलता उद्देश्यों के विरुद्ध अंतराल की पहचान करने और आईसीटी जोखिम पहचान/पता लगाने और घटना प्रबंधन में सुधार की सुविधा के लिए एक कार्यक्रम के हिस्से के रूप में नियमित रूप से परीक्षण किया जाना चाहिए; और

15.5.3 आईसीटी सिस्टम, नेटवर्क और अनुप्रयोगों की कमजोरियों के बारे में उनकी स्थितिजन्य जागरूकता को लगातार बढ़ाने और जोखिम या परिवर्तन प्रबंधन में प्रभावी निर्णय लेने की सुविधा के लिए कार्रवाई योग्य खुफिया जानकारी का उपयोग करें।

15.6 आरई को विघटनकारी बाहरी घटनाओं से दबावग्रस्त परिदृश्यों के लिए आईसीटी तत्परता के लिए दृष्टिकोण विकसित करना चाहिए, जैसे कि व्यापक पैमाने पर रिमोट-एक्सेस के कार्यान्वयन की सुविधा, भौतिक आस्तियों की तेजी से तैनाती और / या दूरस्थ उपयोगकर्ता कनेक्शन और ग्राहक डेटा सुरक्षा का समर्थन करने के लिए बैंडविड्थ का महत्वपूर्ण विस्तार। आरई को यह सुनिश्चित करना चाहिए कि:

15.6.1 आईसीटी प्रणालियों, नेटवर्क और अनुप्रयोगों में व्यवधान या करार से जुड़े संभावित जोखिमों के लिए उचित जोखिम शमन रणनीतियाँ विकसित की जाती हैं। उन्हें मूल्यांकन करना चाहिए कि क्या

इन रणनीतियों के साथ लिए गए जोखिम, इसकी जोखिम स्वीकार्यता और जोखिम सहनशीलता के अंतर्गत आते हैं;

15.6.2 विशेषाधिकार प्राप्त उपयोगकर्ताओं के प्रबंधन और एप्लिकेशन विकास के लिए अच्छी तरह से परिभाषित प्रक्रियाएं मौजूद हैं; और

15.6.3 उचित सुरक्षा स्थिति बनाए रखने के लिए साइबर सुरक्षा सहित आईसीटी में नियमित अपडेट किए जाते हैं।

15.7 आरई के कामकाज के लिए प्राथमिकताओं में हालिया बदलाव और प्रौद्योगिकी पर निर्भरता के आलोक में, उन्हें डेटा सुरक्षा और गोपनीयता से संबंधित सभी प्रासंगिक कानूनी और नियामक आवश्यकताओं का पालन करते हुए आईसीटी जोखिम मूल्यांकन और इसके महत्वपूर्ण परिचालनों के लिए महत्वपूर्ण सूचना आस्तियों के महत्व के आधार पर अपने साइबर सुरक्षा प्रयासों को प्राथमिकता देनी चाहिए। आरई को साइबर-घटना की स्थिति में महत्वपूर्ण जानकारी की अखंडता बनाए रखने के लिए योजनाएं विकसित करनी चाहिए और नियंत्रण लागू करना चाहिए, जैसे महत्वपूर्ण परिचालनों का समर्थन करने वाले डेटा के अपरिवर्तनीय मीडिया पर सुरक्षित भंडारण और ऑफ़लाइन बैकअप।

स्तंभ 3: सीखना और अनुकूलन

16. प्रकटीकरण और रिपोर्टिंग

सिद्धांत 15: आरई के सार्वजनिक प्रकटीकरण से हितधारकों को परिचालन जोखिम प्रबंधन और इसके परिचालन जोखिम जोखिम के प्रति इसके दृष्टिकोण का आकलन करने की अनुमति मिलनी चाहिए।

16.1 प्रासंगिक परिचालन जोखिम प्रबंधन जानकारी के आरई के सार्वजनिक प्रकटीकरण से पारदर्शिता और बाजार अनुशासन के माध्यम से बेहतर उद्योग प्रथाओं का विकास हो सकता है। प्रकटीकरण से आरई को अपनी प्रक्रियाओं और नियंत्रणों में सुधार के लिए सहकर्मी से सहकर्मी तुलनात्मक विश्लेषण करने की भी अनुमति मिलती है। प्रकटीकरण की सीमा और प्रकार आरई के परिचालन के आकार, जोखिम प्रोफ़ाइल और जटिलता और विकसित उद्योग अभ्यास के अनुरूप होना चाहिए।

16.2 आरई को अपने हितधारकों (महत्वपूर्ण परिचालन हानि की घटनाओं सहित) के लिए प्रासंगिक परिचालन जोखिम जोखिम जानकारी का प्रकटन करना चाहिए, जबकि इस प्रकटीकरण के माध्यम से परिचालन जोखिम निर्माण नहीं करना चाहिए (उदाहरण के लिए, असंबोधित नियंत्रण कमजोरियों का विवरण)। एक आरई को अपने ओआरएमएफ का प्रकटीकरण इस तरीके से करना चाहिए जिससे

हितधारकों को यह निर्धारित करने की अनुमति मिल सके कि आरई प्रभावी ढंग से परिचालन जोखिम की पहचान, मूल्यांकन, निगरानी और नियंत्रण/कम करता है या नहीं।

16.3 आरई के पास एक औपचारिक प्रकटीकरण नीति होनी चाहिए जो क्रमशः वरिष्ठ प्रबंधन और निदेशक मंडल द्वारा नियमित और स्वतंत्र समीक्षा और अनुमोदन के अधीन हो। नीति को यह निर्धारित करने के लिए आरई के दृष्टिकोण को संबोधित करना चाहिए कि यह कौन से परिचालन जोखिम प्रकटीकरण करेगा और कौनसे प्रकटीकरण प्रक्रिया पर आंतरिक नियंत्रण होगा। इसके अलावा, आरई को अपने प्रकटीकरण और प्रकटीकरण नीति की उपयुक्तता का आकलन करने के लिए एक प्रक्रिया लागू करनी चाहिए।

16.4 जहां संभव हो, ओआरएमएफ की निरंतर समीक्षा सुनिश्चित करने के लिए पर्यवेक्षकों और लेखा परीक्षकों के साथ प्रत्यक्ष रिपोर्टिंग तंत्र स्थापित किया जा सकता है**,** साथ ही पर्यवेक्षकों को आरई के हाल ही के सुधारों और संभावित विकास की योजनाओं की निगरानी**,** तुलना और मूल्यांकन करके आरई के चल रहे आंतरिक विकास प्रयासों को प्रोत्साहित करने में सक्षम बनाया जा सकता है।

17. पाठ से सीख अभ्यास और अनुकूलन

सिद्धांत 16: भविष्य की परिचालन घटनाओं को अनुकूलित करने और प्रतिक्रिया देने के लिए आरई की क्षमताओं को बढ़ाने के लिए एक महत्वपूर्ण या महत्वपूर्ण व्यावसायिक सेवा में व्यवधान के बाद एक पाठ सीख अभ्यास आयोजित किया जाना चाहिए।

17.1 एक आरई को महत्वपूर्ण सेवा पर जोर देने के साथ व्यावसायिक सेवा में किसी भी व्यवधान के बाद मूल कारण विश्लेषण सहित 'सीखे गए पाठ' का संचालन करना चाहिए। इसमें किसी तृतीय-पक्ष प्रदाता (समूह इकाई सहित, लेकिन केवल इन्हीं तक सीमित नहीं) के लिए कोई भी संभावित भौतिक व्यवधान शामिल है जो एक महत्वपूर्ण व्यावसायिक सेवा की डिलीवरी में योगदान देते हैं।

17.2 अभ्यास में सीखे गए पाठों को घटना प्रबंधन और आपदा पुनर्प्राप्ति प्रक्रिया के हिस्से के रूप में एकत्रित जानकारी का उपयोग करना चाहिए। घटना प्रबंधन प्रक्रिया के दौरान उचित होने के लिए निर्धारित निर्णय और पुनर्प्राप्ति प्रक्रियाओं को सीखे गए अभ्यास का आधार बनाना चाहिए।

17.3 एक आरई में घटनाओं से सीखे गए पाठ के आधार पर पूर्व निर्धारित मानदंड या प्रश्न होने चाहिए। इन प्रश्नों में उन कमियों की पहचान होनी चाहिए, जिनके कारण सेवा की निरंतरता में विफलता हुई और इन कमियों को प्राथमिकता के तौर पर समाधान किया जाना चाहिए। विशेष रूप से, कम से कम, निम्नलिखित पर विचार किया जाना चाहिए:

17.4 पाठ सीख अभ्यास में सेवा की निरंतरता में कमियों और विफलताओं को दूर करने के लिए प्रभावी उपचार उपायों को परिभाषित किया जाना चाहिए। महत्वपूर्ण संचालन और किसी भी प्रभाव सहनशीलता के समायोजन के लिए संसाधनों का अधिक कुशल उपयोग यह निर्धारित करता है कि विफलता का वित्तीय स्थिरता पर व्यापक प्रभाव पड़ सकता है या नहीं। घटना के बाद उक्त से युक्त एक रिपोर्ट/स्व-मूल्यांकन विश्लेषण दस्तावेज़ बोर्ड को प्रस्तुत किया जाना चाहिए।

17.5 पाठ से प्राप्त सीख अभ्यास एक आरई को परिचालन आघात-सहनीयता के लिए तीन-स्तंभ दृष्टिकोण पर प्रतिबिंबित करने की अनुमति देता है और पहले दो स्तंभों में प्रतिसूचना लूप की अनुमति देता है जो आरई की तैयारी और व्यवधानों से उबरने के तरीके में सुधार को प्रोत्साहित करता है। ऐसा करने से आरई को उपचारात्मक कार्रवाइयों पर सहमत होने और निर्धारित होने पर किसी भी प्रभाव सहनशीलता को समायोजित करने की भी अनुमति मिल जाएगी।

18. प्रतिसूचना प्रणाली के माध्यम से निरंतर सुधार

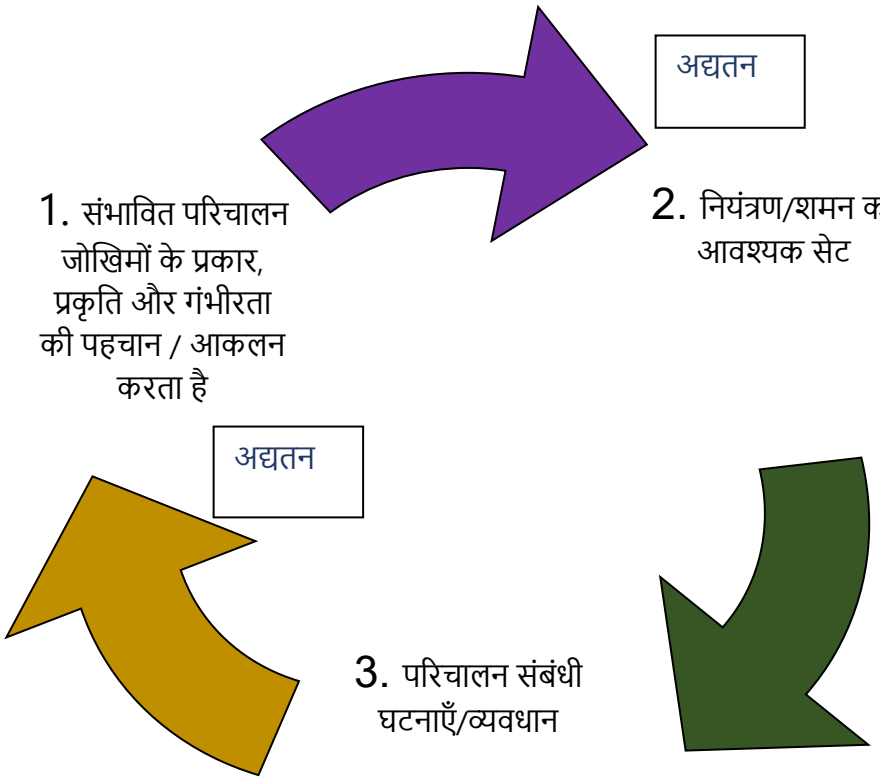
सिद्धान्त 17: एक आरई को सीखने की प्रभावी संस्कृति और निरंतर सुधार को बढ़ावा देना चाहिए क्योंकि प्रभावी प्रतिसूचना सिस्टम के माध्यम से परिचालन आघात-सहनीयता विकसित होता है।

18.1 परिचालन आघात-सहनीयता में निरंतर सुधार के लिए आरई को अपने अनुभवों से सीखने की आवश्यकता होती है क्योंकि समय के साथ इसके परिचालन दृष्टिकोण या प्रौद्योगिकी बुनियादी ढांचे में बदलाव परिपक्व होते हैं। यह न केवल किसी व्यवधान या घटना के घटित होने के बाद घटित होना चाहिए, बल्कि चालू परिचालन आघात-सहनीयतता विचार-विमर्श का हिस्सा होना चाहिए।

18.2 आरई को सीखने की प्रभावी संस्कृति को बढ़ावा देना चाहिए और परिचालन आघात-सहनीयता विकसित होने पर निरंतर सुधार करना चाहिए। आरई द्वारा लिए गए किसी भी रणनीतिक निर्णय में परिचालन आघात-सहनीयता मूलभूत तत्व होना चाहिए।

18.3 आरई को एक प्रभावी अधिगम वातावरण को बढ़ावा देने के लिए निरंतर सकारात्मक प्रतिसूचना लूप सुनिश्चित करने के लिए मजबूत प्रतिसूचना सिस्टम विकसित करना चाहिए, जो बदले में उन्हें बेहतर ओआरएमएफ तैयार करने और पर्याप्त परिचालन आघात-सहनीयता बनाने में मदद करता है।

18.4 उक्त सन्दर्भ में, एक प्रभावी प्रतिसूचना प्रणाली संभावित परिचालन जोखिमों के प्रकार, प्रकृति और गंभीरता की उचित रूप से पहचान और आकलन करती है, जिनका सामना आरई द्वारा किया जा सकता है और साथ ही जहां कमजोरियां हैं और उनका समाधान करने की आवश्यकता है। उसी पर आधारित, इन जोखिमों से निपटने के लिए नियंत्रण और शमन उपायों का एक आवश्यक सेट विकसित किया जा सकता है। इसके अलावा, वास्तविक समय परिचालन संबंधी घटनाओं या शमन उपायों के बावजूद होने वाले व्यवधानों के आधार पर, प्रतिसूचना प्रणाली संभावित परिचालन जोखिमों के प्रकार, प्रकृति और गंभीरता को अद्यतन करती है और इसलिए इन जोखिमों से निपटने के लिए नियंत्रण और शमन उपायों के आवश्यक समूह को अद्यतन करती है। सुधार और आवश्यक अद्यतनीकरण सुनिश्चित करने के लिए मौजूदा नियंत्रणों और प्रक्रियाओं में त्रुटियों/गलतियों को भी प्रतिसूचना में शामिल किया जाना चाहिए। इस प्रकार, प्रतिसूचना के माध्यम से, एक आरई इष्टतम परिचालन आघात-सहनीयता बनाए रखता है जैसा कि नीचे दिए गए चित्र में दिखाया गया है।



अनुबंध

निरस्त मार्गदर्शी नोट की तुलना में मार्गदर्शी नोट में किए गए मुख्य परिवर्तन

विवरण	निरसित मार्गदर्शी नोट दिनांक 14 अक्तूबर 2005	मार्गदर्शी नोट
केंद्र	परिचालन जोखिम प्रबंधन	परिचालन जोखिम प्रबंधन के परिणाम के रूप में परिचालन आघात-सहनीयता।
प्रयोज्यता	यह अनुसूचित वाणिज्यिक बैंकों पर लागू है।	यह सभी वाणिज्यिक बैंकों, सभी गैर-बैंकिंग वित्तीय कंपनियों (एनबीएफसी), सभी सहकारी बैंकों और सभी अखिल भारतीय वित्तीय संस्थानों (एआईएफआई) पर लागू है।
रक्षा मॉडल की तीन पंक्तियाँ	इसमें त्रिस्तरीय सुरक्षा मॉडल पर मार्गदर्शन शामिल नहीं है।	यह त्रिस्तरीय सुरक्षा मॉडल की व्याख्या करता है ▪ व्यावसायिक इकाई सुरक्षा का पहला घेरा है, ▪ संगठनात्मक परिचालन जोखिम प्रबंधन कार्य (अनुपालन कार्य सहित) सुरक्षा का दूसरा घेरा है, और ▪ लेखापरीक्षा कार्य सुरक्षा का तीसरा घेरा है।
प्ररूपी संगठनात्मक व्यवस्था	यह परिचालन जोखिम प्रबंधन के लिए एक प्ररूपी संगठनात्मक व्यवस्था प्रदान करता है।	चूँकि अब विभिन्न प्रकार की विनियमित इकाइयाँ (आरई) शामिल हैं, जिनके लिए संगठनात्मक व्यवस्था गतिविधियों के आकार और प्रकृति के

विवरण	निरसित मार्गदर्शी नोट दिनांक 14 अक्तूबर 2005	मार्गदर्शी नोट
		आधार पर भिन्न होगा, प्ररूपी संगठनात्मक व्यवस्था विनिर्दिष्ट नहीं किया गया है।
परिवर्तन प्रबंधन	इसमें परिवर्तन प्रबंधन को स्पष्ट रूप से विनिर्दिष्ट नहीं किया गया है।	इसमें विशेष रूप से विस्तृत सिद्धांत के साथ परिवर्तन प्रबंधन पर एक अद्यतन मार्गदर्शन है।
आंतरिक और बाह्य अंतर्संबंधों और अन्योन्याश्रितताओं का मानचित्रण, घटना प्रबंधन, सूचना और संचार प्रौद्योगिकी (आईसीटी), और प्रकटीकरण	यह आंतरिक और बाह्य अंतर्संबंधों और अन्योन्याश्रितताओं के मानचित्रण, घटना प्रबंधन, आईसीटी और प्रकटीकरण पर मूक है।	इसमें आंतरिक और बाह्य अंतर्संबंधों और अन्योन्याश्रितताओं के मानचित्रण, घटना प्रबंधन, आईसीटी और प्रकटीकरण के लिए अलग-अलग सिद्धांत हैं।
तृतीय पक्ष के संबंध	इसमें आउटसोर्सिंग पर बिखरे हुए मार्गदर्शन हैं।	इसमें तृतीय पक्ष के संबंधों पर एक केंद्रित सिद्धांत है, जो आउटसोर्सिंग की तुलना में एक व्यापक अवधारणा है।
सीखे गए पाठ और प्रतिक्रिया	इसमें पाठ सीख अभ्यास और निरंतर प्रतिक्रिया तंत्र पर बहुत सीमित/कोई मार्गदर्शन नहीं है।	इसने पाठ सीख अभ्यास और निरंतर प्रतिक्रिया तंत्र पर अलग-अलग सिद्धांत पेश किए हैं।
परिचालन जोखिम पूंजी गणना के लिए	इसमें परिचालन जोखिम पूंजी गणना के लिए विस्तृत दृष्टिकोण	इसने परिचालन जोखिम पूंजी गणना के दृष्टिकोण को हटा दिया है क्योंकि

विवरण	निरसित मार्गदर्शी नोट दिनांक 14 अक्तूबर 2005	मार्गदर्शी नोट
दृष्टिकोण	हैं।	स्थानीय क्षेत्र बैंकों, भुगतान बैंक, क्षेत्रीय ग्रामीण बैंक, एनबीएफसी और सहकारी बैंक, (मार्गदर्शी नोट के अंतर्गत शामिल) जैसे आरई को वर्तमान में परिचालन जोखिम के लिए एक अलग विनियामक पूंजी बनाए रखने की आवश्यकता नहीं है। इसके अलावा, बैंकों (सार्वजनिक क्षेत्र के बैंकों, निजी बैंकों और विदेशी बैंकों) के लिए परिचालन जोखिम पूंजी गणना का दृष्टिकोण दिनांक 1 अप्रैल 2024 के "मास्टर परिपत्र - बेसल III पूंजी विनियमन" के पैरा 9 में विस्तृत है (समय-समय पर संशोधित), जिसे 26 जून 2023 के "परिचालन जोखिम के लिए न्यूनतम पूंजी आवश्यकताओं पर मास्टर निदेश" के प्रभाव में आने के बाद प्रतिस्थापित किया जाएगा।
परिचालन जोखिम - विस्तृत हानि घटना प्रकार वर्गीकरण	यह एक विस्तृत परिचालन जोखिम हानि घटना प्रकार वर्गीकरण प्रदान करता है।	जैसा कि विस्तृत परिचालन जोखिम हानि घटना प्रकार वर्गीकरण 26 जून 2023 के "परिचालन जोखिम के लिए न्यूनतम पूंजी आवश्यकताओं पर मास्टर निदेश" में विनिर्दिष्ट किया गया है (जिसका आरई उपयोग कर सकते हैं) इसे मार्गदर्शन नोट में शामिल नहीं किया गया है।