भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

भारिबैं/विवि/2025-26/337
विवि.ओआरजी.आरईसी.सं.256/21-04-158/2025-26 28 नवंबर 2025

भारतीय रिज़र्व बैंक (अखिल भारतीय वित्तीय संस्थान - आउटसोर्सिंग में जोखिमों का प्रबंधन) निदेश 2025

विषयसूची

अध्याय I – प्रारंभिक 3

ए. संक्षिप्त शीर्षक और प्रारंभ 3
बी. प्रयोज्यता और कार्यक्षेत्र 3
सी. परिभाषाएँ 6

अध्याय II - बोर्ड की भूमिका 8

ए. बोर्ड-अनुमोदित नीति 8
बी. प्रमुख जिम्मेदारियां 8

अध्याय III - सूचना प्रौद्योगिकी (आईटी) सेवाओं की आउटसोर्सिंग 9

ए. प्राधिकरण, जवाबदेही और निगरानी 9
बी. अभिशासन ढांचा 10

बी.1 आउटसोर्सिंग नीति 10
बी.2 वरिष्ठ प्रबंधन की भूमिका 11
बी.3 आईटी कार्य की भूमिका 12

सी. जोखिम प्रबंधन 13

सी.1 जोखिम प्रबंधन ढांचा 13

सी.2 जानकारी की गोपनीयता और सुरक्षा 13

डी. आउटसोर्सिंग प्रक्रिया 14

डी.1 सेवा प्रदाता मूल्यांकन 14

ई.2 आउटसोर्सिंग करार 16

डी.3 आउटसोर्स की गई सेवाओं की निगरानी और नियंत्रण 19

डी.4 आउटसोर्स की गई सेवाओं की सूची 20

डी.5 कारोबार निरंतरता और आपातकालीन बहाली योजना का प्रबंधन 20

डी.6 निकास रणनीति 21

डी.7 समापन 22

ई. विशिष्ट आउटसोर्सिंग व्यवस्थाएं 22

ई.1 समूह / संगुट के भीतर आउटसोर्सिंग 22

ई.2 अपतटीय या सीमापारीय आउटसोर्सिंग 23

ई.3 सुरक्षा परिचालन केंद्र (एसओसी) की आउटसोर्सिंग 23

ई.4 क्लाउड कंप्यूटिंग सेवाओं का उपयोग 24

एफ. आउटसोर्स की गई सेवाओं से संबंधित शिकायतों का निवारण 30

अध्याय IV – निरसन और अन्य प्रावधान 31

ए. निरसन और बचाव 31

बी. अन्य कानूनों के लागू होने पर रोक नहीं 31

सी. व्याख्याएं 32

भारतीय रिज़र्व बैंक अधिनियम 1934 की धारा 45एल और इस संबंध में भारतीय रिज़र्व बैंक (आरबीआई) को सक्षम बनाने वाले अन्य सभी प्रावधानों/कानूनों द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, आरबीआई संतुष्ट है कि ऐसा करना जनहित में आवश्यक और समीचीन है, इसलिए एतद्द्वारा निम्नलिखित निदेश जारी करता है।

अध्याय I – प्रारंभिक

ए. संक्षिप्त शीर्षक और प्रारंभ

1. इन निदेशों को भारतीय रिज़र्व बैंक (अखिल भारतीय वित्तीय संस्थान - आउटसोर्सिंग में जोखिमों का प्रबंधन) निदेश 2025 कहा जाएगा।

2. ये निदेश तत्काल प्रभाव से लागू होंगे।

   बशर्ते कि किसी अखिल भारतीय वित्तीय संस्थान के मौजूदा सूचना प्रौद्योगिकी (आईटी) आउटसोर्सिंग करार, चाहे वे इन निदेशों के प्रभावी होने की तिथि को या उसके बाद नवीनीकरण के लिए देय हों, नवीनीकरण के समय या **10 अप्रैल 2026** तक, जो भी पहले हो, इन निदेशों के प्रावधानों का अनुपालन करेंगे। तथापि, इन निदेशों की प्रभावी तारीख को या उसके बाद लागू होने वाले अखिल भारतीय वित्तीय संस्थान के नए आईटी आउटसोर्सिंग करार, करार की तारीख से ही इन निदेशों के प्रावधानों का पालन करेंगे।

   बशर्ते यह भी कि पिछले परंतुक में किसी भी बात का अर्थ यह नहीं लगाया जाएगा कि ऐसी व्यवस्थाओं पर लागू सांविधिक आवश्यकताओं अथवा किसी अन्य मौजूदा विनियामक अनुदेशों का अनुपालन नहीं करने की अनुमति दी गई है।

बी. प्रयोज्यता और कार्यक्षेत्र

3. ये निदेश अखिल भारतीय वित्तीय संस्थानों (एआईएफआई) पर लागू होंगे, जिनमें भारतीय निर्यात आयात बैंक ('एक्जिम बैंक'), राष्ट्रीय कृषि एवं ग्रामीण विकास बैंक ('नाबार्ड'), राष्ट्रीय अवसंरचना एवं विकास वित्तपोषण बैंक ('एनएबीएफआईडी'), राष्ट्रीय आवास बैंक ('एनएचबी') और भारतीय लघु उद्योग विकास बैंक ('एसआईडीबीआई') शामिल हैं, जिन्हें आगे सामूहिक रूप से 'एआईएफआई' और व्यक्तिगत रूप से 'एआईएफआई' कहा जाएगा।

4. ये निदेश एआईएफआई द्वारा आईटी सेवाओं के महत्वपूर्ण आउटसोर्सिंग पर लागू होंगे, जैसा कि इस निदेश के पैरा 6(3) में परिभाषित है। इस संदर्भ में, 'आईटी सेवाओं के आउटसोर्सिंग' में निम्नलिखित सेवाओं की आउटसोर्सिंग शामिल होगी:

(i) आईटी इंफ्रास्ट्रक्चर प्रबंधन, रखरखाव और समर्थन (हार्डवेयर, सॉफ्टवेयर या फर्मवेयर);

(ii) नेटवर्क और सुरक्षा समाधान, और रखरखाव (हार्डवेयर, सॉफ्टवेयर या फर्मवेयर);

(iii) एटीएम स्विच एएसपी सहित एप्लिकेशन सेवा प्रदाताओं (एएसपीएस) द्वारा एप्लिकेशन विकास, रखरखाव और परीक्षण;

(iv) डेटा केंद्रों से संबंधित सेवाएं और परिचालन;

(v) क्लाउड कंप्यूटिंग सेवाएं;

(vi) प्रबंधन की गई सुरक्षा सेवाएं; और

(vii) भुगतान प्रणाली पारिस्थितिकी तंत्र से जुड़ी आईटी मूलभूत सुविधाओं और प्रौद्योगिकी सेवाओं का प्रबंधन।

(2) ये निदेश निम्नलिखित सेवाओं पर लागू नहीं होंगे:

(i) एआईएफआई द्वारा किसी अन्य विनियमित संस्था (रेगुलेटेड एंटिटीज (आरई)) के कॉर्पोरेट ग्राहक या उप-सदस्य के रूप में प्राप्त की गई कॉर्पोरेट इंटरनेट बैंकिंग सेवाएं;

बशर्ते कि, इन निदेशों के प्रयोजन के लिए, निम्नलिखित सांकेतिक (परंतु संपूर्ण नहीं) संस्थाओं की सूची को आरई माना जाएगा – वाणिज्यिक बैंक; स्थानीय क्षेत्र बैंक; लघु वित्त बैंक; भुगतान बैंक; क्षेत्रीय ग्रामीण बैंक; आधार स्तर (एनबीएफसी - बीएल), मध्य स्तर (एनबीएफसी - एमएल) और ऊपरी स्तर (एनबीएफसी - यूएल) की गैर-बैंकिंग वित्तीय कंपनियाँ; अन्य एआईएफआई; साख सूचना कंपनियाँ; शहरी सहकारी बैंक; ग्रामीण सहकारी बैंक; और, भुगतान प्रणाली संचालक;

इन निदेशों के प्रयोजन से, 'वाणिज्यिक बैंक' का अर्थ बैंकिंग कंपनी (लघु वित्त बैंकों, स्थानीय क्षेत्र बैंकों, भुगतान बैंकों और क्षेत्रीय ग्रामीण बैंकों को छोड़कर), संबंधित नए बैंक और

भारतीय स्टेट बैंक, जैसा कि बैंककारी विनियमन अधिनियम, 1949 की धारा 5 के खंड (सी), (डीए), और (एनसी) के तहत परिभाषित किया गया है।

(ii) बाह्य लेखापरीक्षा सेवाएं जैसे भेद्यता मूल्यांकन (वल्नेरेबिलिटी असेसमेंट (वीए)) / प्रवेश परीक्षण (पेनिट्रेशन टेस्टिंग (पीटी)), सूचना प्रणाली लेखापरीक्षा और सुरक्षा समीक्षा;

(iii) एसएमएस गेटवे (बल्क एसएमएस सेवा प्रदाताओं सहित);

(iv) आईटी हार्डवेयर या उपकरणों की खरीद;

(v) लाइसेंस या सदस्यता के आधार पर आईटी सॉफ्टवेयर, उत्पाद या एप्लिकेशन (जैसे, कोर बैंकिंग सॉल्यूशन (सीबीएस), डेटाबेस और सुरक्षा सोल्युशन) का अधिग्रहण और वेंडर द्वारा ऐसे लाइसेंस प्राप्त तृतीय-पक्ष एप्लिकेशन में किए गए कोई भी सुधार (अपग्रेड के रूप में) या एआईएफआई द्वारा किए गए विशिष्ट परिवर्तन अनुरोध पर किए गए सुधार;

(vi) आईटी इंफ्रास्ट्रक्चर या लाइसेंस प्राप्त उत्पादों के लिए कोई भी रखरखाव सेवा (सुरक्षा पैच, बग फिक्स सहित), जो स्वयं मूल उपकरण निर्माता (ओईएम) द्वारा प्रदान की जाती है, ताकि एआईएफआई द्वारा उनका निरंतर उपयोग सुनिश्चित किया जा सके;

(vii) वित्तीय क्षेत्र के विनियामकों या संस्थानों जैसे क्लियरिंग कॉर्पोरेशन ऑफ इंडिया लिमिटेड (सीसीआईएल), नेशनल स्टॉक एक्सचेंज (एनएसई) और बॉम्बे स्टॉक एक्सचेंज (बीएसई) द्वारा प्रदान किए गए एप्लिकेशन;

(viii) रॉयटर्स, ब्लूमबर्ग और सोसाइटी फॉर वर्ल्डवाइड इंटरबैंक फाइनेंशियल टेलीकम्युनिकेशन (स्विफ्ट) जैसी संस्थाओं द्वारा उपलब्ध कराए गए प्लेटफॉर्म;

(ix) एआईएफआई द्वारा सब्सक्राइब किए गए कोई अन्य ऑफ-दि-शेल्फ उत्पाद (जैसे, एंटीवायरस सॉफ़्टवेयर और ईमेल सोल्युशन), जिसमें केवल लाइसेंस की खरीद बिना या न्यूनतम कस्टमाइज़ेशन के साथ की जाती है;

(x) किसी केंद्रीकृत भुगतान प्रणाली (सीपीएस) के उप-सदस्य के रूप में एआईएफआई द्वारा किसी अन्य आरई से प्राप्त सेवाएं;

(xi) कारोबार प्रतिनिधि (बीसी) सेवाएं, पेरोल प्रोसेसिंग और स्टेटमेंट प्रिंटिंग।

सी. परिभाषाएँ

6. इन निदेशों में, जब तक कि संदर्भ से अन्यथा अपेक्षित न हो, यहां प्रयुक्त शब्दों का अर्थ नीचे दिए गए अनुसार होगा:

(1) अंतर-समूह लेनदेन और एक्सपोजर के प्रयोजन के लिए, **'समूह'** को भारतीय रिज़र्व बैंक (वाणिज्यिक बैंक - संकेन्द्रण जोखिम प्रबंधन) निदेश 2025, समय-समय पर संशोधित, में यथापरिभाषित किया जाएगा;

(2) '**आईटी सेवाएं**' से तात्पर्य आईटी सेवाएं / आईटी सक्षम सेवाएं / आईटी गतिविधियां है।

(3) '**आईटी सेवाओं का महत्वपूर्ण आउटसोर्सिंग**' वे सेवाएं हैं जो:

(i) बाधित या छेड़छाड़ होने पर एआईएफआई के कारोबार संचालन पर महत्वपूर्ण प्रभाव डाल सकती हैं; या

(ii) ग्राहक जानकारी की अनधिकृत एक्सेस, हानि या चोरी की स्थिति में एआईएफआई के ग्राहकों पर महत्वपूर्ण प्रभाव डाल सकती हैं।

(4) '**आउटसोर्सिंग**' का अर्थ है किसी एआईएफआई द्वारा किसी तीसरे पक्ष (चाहे वह किसी कॉर्पोरेट समूह के भीतर संबद्ध संस्था हो या कॉर्पोरेट समूह से बाहर की संस्था) का उपयोग करके उन गतिविधियों को निरंतर आधार पर करवाना जो सामान्यतः एआईएफआई द्वारा वर्तमान या भविष्य में की जाती हैं। 'निरंतर आधार' में सीमित अवधि के लिए किए गए करार भी शामिल होंगे।

(5) **'सेवा प्रदाता'** से तात्पर्य आईटी सेवाओं के प्रदाताओं से है, जिनमें एआईएफआई से संबंधित संस्थाएं या वे संस्थाएं शामिल हैं जो उसी समूह या संगुट से संबंधित हैं जिससे एआईएफआई संबंधित है।

बशर्ते कि इन निदेशों के प्रयोजन के लिए, वेंडर और संस्थाओं की निम्नलिखित सांकेतिक (परंतु संपूर्ण नहीं) सूची को ऊपर परिभाषित 'सेवा प्रदाता' नहीं माना जाएगा:

(i) आईटी का उपयोग करके कारोबार सेवाएं प्रदान करने वाले वेंडर (उदाहरण के लिए, बीसी;);

(ii) भुगतान और निपटान प्रणाली अधिनियम 2007 के तहत भारतीय रिज़र्व बैंक द्वारा भारत में भुगतान प्रणाली स्थापित करने और संचालित करने के लिए अधिकृत भुगतान प्रणाली संचालक (पीएसओ);

(iii) साझेदारी आधारित फिनटेक फर्में, जैसे कि सह-ब्रांडेड एप्लिकेशन, उत्पाद और सेवाएं प्रदान करने वाली फर्में;

(iv) डेटा पुनर्प्राप्ति, डेटा सत्यापन और प्रमाणीकरण जैसी सेवाएं प्रदान करने वाली फिनटेक कंपनियां, जैसे बैंक स्टेटमेंट विश्लेषण, जीएसटी रिटर्न विश्लेषण, वाहन जानकारी प्राप्त करना, डिजिटल दस्तावेज़ निष्पादन, डेटा एंट्री और कॉल सेंटर सेवाएं;

(v) दूरसंचार सेवा प्रदाता जिनसे पट्टे पर ली गई लाइनें या इसी तरह की अन्य अवसंरचना का उपयोग डेटा के प्रसारण के लिए किया जाता है; और

(vi) स्वतंत्र तृतीय-पक्ष लेखापरीक्षक, सलाहकार, या प्रमुख कार्यान्वयनकर्ता के रूप में अपनी भूमिका में आईटी अवसंरचना, आईटी सेवाओं या सूचना सुरक्षा सेवाओं से संबंधित प्रमाणीकरण, लेखापरीक्षा या वीए/पीटी के लिए नियुक्त सुरक्षा या लेखापरीक्षा सलाहकार।

(6) *स्पष्टीकरण:* यदि आरई द्वारा एआईएफआई को आईटी सेवा प्रदान की जाती है (जैसा कि इन निदेशों के दायरे में लागू होता है), तो इन निदेशों के तहत आरई को भी एआईएफआई का सेवा प्रदाता माना जा सकता है। **'उप-संविदाकार'** से तात्पर्य सेवा प्रदाता को महत्वपूर्ण आईटी सेवाएं प्रदान करने वालों से है और यह महत्वपूर्ण आईटी सेवाओं की व्यवस्था के लिए विशिष्ट है जो एआईएफआई ने सेवा प्रदाता के साथ की है।

7. इन निदेशों में परिभाषित न किए गए अन्य सभी शब्दों का वही अर्थ होगा जो बैंककारी विनियमन अधिनियम 1949 या भारतीय रिज़र्व बैंक अधिनियम,1934 या सूचना प्रौद्योगिकी अधिनियम 2000 या कंपनी अधिनियम 2013 और उसके अंतर्गत बनाए गए नियमों, या उसके किसी सांविधिक आशोधन या पुनर्अधिनियमन या भारतीय रिज़र्व बैंक द्वारा प्रकाशित शब्दावली या वाणिज्यिक भाषा में प्रयुक्त शब्दों का है, जैसा भी मामला हो।

अध्याय II - बोर्ड की भूमिका

8. एआईएफआई द्वारा किसी आईटी सेवाओं की आउटसोर्सिंग करने से उसके और उसके बोर्ड और वरिष्ठ प्रबंधन का दायित्व कम नहीं होता हैं क्योंकि आउटसोर्स की गई गतिविधि के लिए परम जिम्मेदारी उन्हीं की होती है।

ए. बोर्ड-अनुमोदित नीति

9. एआईएफआई जो अपनी किसी आईटी सेवाओं को आउटसोर्स करने की मंशा रखता है, उसे बोर्ड द्वारा अनुमोदित व्यापक आईटी आउटसोर्सिंग नीति लागू करनी होगी, जिसका दायरा पैराग्राफ 15 में इंगित किया गया है।

बी. प्रमुख जिम्मेदारियां

10. बोर्ड अन्य बातों के साथ-साथ निम्नलिखित के लिए उत्तरदायी होगा:

(i) जोखिमों और महत्ता के आधार पर आउटसोर्सिंग गतिविधियों के अनुमोदन के लिए एक ढांचा तैयार करना;

(ii) सभी मौजूदा और संभावित आउटसोर्सिंग व्यवस्थाओं के जोखिमों और महत्ता का मूल्यांकन करने के लिए नीतियों को अनुमोदन देना;

(iii) वरिष्ठ प्रबंधन के लिए उपयुक्त प्रशासनिक ढांचा तैयार करना;

(iv) स्वयं या अपनी समिति के माध्यम से यह सुनिश्चित करना कि तृतीय-पक्ष के साथ व्यवस्थाओं (एन्गेजमेंट) से हितों का कोई टकराव उत्पन्न न हो, विशेषकर जब इस आवश्यकता में अपवाद की अनुमति दी जाती है कि आउटसोर्स सेवाओं का सेवा प्रदाता, यदि समूह कंपनी नहीं है, तो किसी निदेशक, प्रमुख प्रबंधकीय कर्मियों, आउटसोर्सिंग व्यवस्था के अनुमोदक या उनके रिश्तेदारों के स्वामित्व या नियंत्रण में नहीं होगा जैसा कि इन निदेशों के पैरा 12(vi) के परंतुक में दिया गया है; और

(v) निगरानी एवं नियंत्रण गतिविधियों पर वरिष्ठ प्रबंधन को प्रस्तुत रिपोर्टों में उल्लिखित किसी भी प्रतिकूल घटनाक्रम की समीक्षा करना।

अध्याय III - सूचना प्रौद्योगिकी (आईटी) सेवाओं की आउटसोर्सिंग

ए. प्राधिकरण, जवाबदेही और निगरानी

11. जैसा कि पैरा 8 में उल्लेख किया गया है, एआईएफआई द्वारा किसी भी आईटी सेवा की आउटसोर्सिंग उसके दायित्वों को कम नहीं करेगा और न ही उसके बोर्ड और वरिष्ठ प्रबंधन के दायित्वों को कम करेगा, जिनकी आउटसोर्स की गई सेवा के लिए अंतिम जिम्मेदारी है।

12. एआईएफआई यह सुनिश्चित करेगा कि:

(i) सेवा प्रदाता सेवाओं के निष्पादन में उसी उच्च स्तर की सावधानी बरतता है जैसा कि एआईएफआई द्वारा बरती जाती, यदि सेवाएं एआईएफआई के भीतर ही संचालित की जाती और आउटसोर्स नहीं की जाती;

(ii) यह किसी ऐसे सेवा प्रदाता को नियुक्त नहीं करेगा जिसके परिणामस्वरूप इसकी प्रतिष्ठा से समझौता हो या वह कमजोर हो जाए;

(iii) सेवा प्रदाता भारत में स्थित हो या विदेश में, आउटसोर्सिंग से एआईएफआई की अपनी सेवाओं की प्रभावी ढंग से निगरानी और प्रबंधन करने की क्षमता में कोई बाधा या हस्तक्षेप नहीं होगा;

(iv) आउटसोर्सिंग आरबीआई के पर्यवेक्षी कार्यों और उद्देश्यों के निष्पादन में बाधा नहीं डालती है;

(v) आउटसोर्सिंग के संबंध में समुचित जांच-पड़ताल करते समय सभी प्रासंगिक कानूनों, विनियमों, नियमों, दिशा-निर्देशों और अनुमोदन, लाइसेंसिंग या पंजीकरण की शर्तों पर विचार किया गया है; और

(vi) सेवा प्रदाता, यदि वह समूह कंपनी नहीं है, तो एआईएफआई के किसी निदेशक, प्रमुख प्रबंधकीय कार्मिक, आउटसोर्सिंग व्यवस्था के अनुमोदक या उनके रिश्तेदारों के स्वामित्व या नियंत्रण में न हो। 'नियंत्रण', 'निदेशक', 'प्रमुख प्रबंधकीय कार्मिक' और 'रिश्तेदार' शब्दों का वही अर्थ होगा जो कंपनी अधिनियम 2013 और उसके अंतर्गत समय-समय पर निर्मित नियमों में दिया गया है।

बशर्ते कि उपर्युक्त आवश्यकता में अपवाद बोर्ड या बोर्ड की किसी समिति के अनुमोदन से किया जा सकता है, जिसके बाद ऐसी व्यवस्थाओं का उचित प्रकटीकरण, निरीक्षण और निगरानी की जाएगी।

13. एआईएफआई को आईटी सेवाओं के आउटसोर्सिंग की आवश्यकता का मूल्यांकन, इससे जुड़े लाभों, जोखिमों और उन जोखिमों के प्रबंधन के लिए उपयुक्त प्रक्रियाओं की उपलब्धता के व्यापक आकलन के आधार पर करना चाहिए। इस उद्देश्य के लिए, एआईएफआई को *अन्य बातों के साथ-साथ*, निम्नलिखित बातों पर विचार करना चाहिए:

(i) आउटसोर्स की जाने वाली सेवा की महत्ता / अहमियत के आधार पर आउटसोर्सिंग की आवश्यकता;

(ii) आउटसोर्सिंग से अपेक्षाएँ और परिणाम;

(iii) सफलता के कारक और लागत-लाभ विश्लेषण; और

(iv) आउटसोर्सिंग का मॉडल।

14. एआईएफआई यह सुनिश्चित करेगा कि साइबर घटनाओं की सूचना सेवा प्रदाता द्वारा बिना किसी अनुचित देरी के उसे दी जाए, ताकि सेवा प्रदाता द्वारा घटना का पता चलने के छह घंटे के भीतर एआईएफआई द्वारा आरबीआई को घटना की सूचना दी जा सके।

बी. अभिशासन ढांचा

बी.1 आउटसोर्सिंग नीति

15. कोई भी एआईएफआई जो अपनी आईटी सेवाओं को आउटसोर्स करना चाहता है, उसे बोर्ड द्वारा अनुमोदित व्यापक आईटी आउटसोर्सिंग नीति बनानी होगी, जिसमें *अन्य बातों के साथ-साथ* निम्नलिखित शामिल हों:

(i) आईटी सेवाओं के आउटसोर्सिंग के संबंध में बोर्ड, बोर्ड की समितियों (यदि कोई हो) और वरिष्ठ प्रबंधन, आईटी कार्य, कारोबार कार्य और निगरानी एवं आश्वासन कार्यों की भूमिकाएँ और जिम्मेदारियाँ;

(ii) ऐसी सेवाओं और सेवा प्रदाताओं के चयन के लिए मानदंड;

(iii) इन निदेशों के पैरा 6(3) में परिभाषित व्यापक मानदंडों के आधार पर महत्वपूर्ण आउटसोर्सिंग को परिभाषित करने के लिए पैरामीटर;

(iv) जोखिम और महत्ता के आधार पर अधिकार का प्रत्यायोजन;

(v) आपातकालीन बहाली और कारोबार निरंतरता योजनाएँ;

(vi) इन सेवाओं के संचालन की निगरानी और समीक्षा करने के लिए प्रणालियाँ; और

(vii) समापन प्रक्रियाएं और निकास रणनीतियां, जिसमें सेवा प्रदाता द्वारा आउटसोर्सिंग व्यवस्था से बाहर निकलने की स्थिति में कारोबार निरंतरता शामिल है।

बी.2 वरिष्ठ प्रबंधन की भूमिका

16. एआईएफआई का वरिष्ठ प्रबंधन, *अन्य बातों के साथ-साथ*, निम्नलिखित के लिए उत्तरदायी होगा:

(i) आईटी आउटसोर्सिंग नीतियों और प्रक्रियाओं को तैयार करना, मौजूदा और संभावित सभी आईटी आउटसोर्सिंग व्यवस्थाओं के जोखिमों और महत्ता का मूल्यांकन करना, जो कि जटिलता, प्रकृति और दायरे के अनुरूप ढांचे पर आधारित हो और बोर्ड द्वारा अनुमोदित एआईएफआई के उद्यम-व्यापी जोखिम प्रबंधन के अनुरूप हो तथा उसका कार्यान्वयन करना;

(ii) बोर्ड द्वारा अनुमोदित नीति के आधार पर भावी आईटी आउटसोर्सिंग व्यवस्थाओं का पूर्व मूल्यांकन और मौजूदा आईटी आउटसोर्सिंग व्यवस्थाओं का आवधिक मूल्यांकन, जिसमें सभी व्यवस्थाओं की कार्य निष्पादन समीक्षा, महत्व और संबंधित जोखिम शामिल हैं;

(iii) आईटी आउटसोर्सिंग से जुड़े जोखिमों की पहचान करना, उनकी निगरानी करना, उन्हें कम करना, उनका प्रबंधन करना और समय पर बोर्ड या बोर्ड की किसी समिति को उनकी रिपोर्ट देना;

(iv) यह सुनिश्चित करना कि किसी भी सेवा प्रदाता के बाहर निकलने सहित, वास्तविक और संभावित व्यवधानकारी परिदृश्यों पर आधारित उपयुक्त कारोबार निरंतरता योजनाएँ मौजूद हों और उनका समय-समय पर परीक्षण किया जाता है;

(v) यह सुनिश्चित करना कि (क) सेवा प्रदाता (और उसके उप-संविदाकारों) पर डेटा गोपनीयता के लिए प्रभावी निगरानी रखी जाए और (ख) ग्राहकों की शिकायतों का समय पर उचित निवारण किया जाए;

(vi) विधानों, विनियमों, बोर्ड द्वारा अनुमोदित नीति और कार्य निष्पादन मानकों के अनुपालन के लिए आवधिक आधार पर स्वतंत्र समीक्षा तथा लेखापरीक्षा सुनिश्चित करना और इसकी रिपोर्ट बोर्ड या बोर्ड की किसी समिति को प्रस्तुत करना; और

(vii) आउटसोर्स सेवाओं की उचित निगरानी के लिए एआईएफआई के भीतर आवश्यक कौशल सेट के साथ आवश्यक क्षमता का सृजन करना।

बी.3 आईटी कार्य की भूमिका

17. एआईएफआई के आईटी कार्य की जिम्मेदारियों में *अन्य बातों के साथ-साथ* निम्नलिखित शामिल होंगे:

(i) एआईएफआई में आईटी आउटसोर्सिंग जोखिम के स्तर की पहचान करने, मापने, निगरानी करने, कम करने और प्रबंधन करने में वरिष्ठ प्रबंधन की सहायता करना;

(ii) यह सुनिश्चित करना कि सभी आईटी आउटसोर्सिंग व्यवस्थाओं का एक केंद्रीय डेटाबेस बनाए रखा जाए और बोर्ड, वरिष्ठ प्रबंधन, लेखा परीक्षकों और पर्यवेक्षकों द्वारा समीक्षा के लिए वह उपलब्ध हो;

(iii) आउटसोर्स की गई आईटी सेवा की प्रभावी ढंग से निगरानी और पर्यवेक्षण करना ताकि यह सुनिश्चित किया जा सके कि सेवा प्रदाता निर्धारित कार्य निष्पादन मानकों को पूरा करते हैं और निर्बाध सेवाएं प्रदान करते हैं, वरिष्ठ प्रबंधन को रिपोर्ट करना तथा आवधिक सम्यक जांच का समन्वय करना और यदि कोई चिंता हो तो उसे उजागर करना; और

(iv) सेवा स्तर प्रबंधन, विक्रेता परिचालन की निगरानी, प्रमुख जोखिम संकेतकों और निर्धारित जोखिम के अनुसार विक्रेताओं को वर्गीकृत करने सहित संविदात्मक करारों के लिए आवश्यक दस्तावेज तैयार करना।

सी. जोखिम प्रबंधन

सी.1 जोखिम प्रबंधन ढांचा

18. एआईएफआई को एक जोखिम प्रबंधन ढांचा स्थापित करना होगा जो इस प्रकार की आईटी आउटसोर्सिंग व्यवस्थाओं से जुड़े जोखिमों की पहचान, माप, न्यूनीकरण, प्रबंधन और रिपोर्टिंग के लिए प्रक्रियाओं और जिम्मेदारियों को व्यापक रूप से करता हो।

19. एआईएफआई को निदेशक मंडल, वरिष्ठ प्रबंधन और आईटी विभाग की भूमिकाओं और जिम्मेदारियों के अनुरूप आवश्यक अनुमोदनों के साथ जोखिम आकलन को उचित रूप से दस्तावेजीकृत करना होगा और इसे बोर्ड द्वारा अनुमोदित नीति के अनुसार आवधिक आधार पर आंतरिक और बाहरी गुणवत्ता आश्वासन के अधीन करना होगा।

20. एआईएफआई को एक ही सेवा प्रदाता के साथ कई आउटसोर्सिंग व्यवस्थाओं द्वारा उत्पन्न संकेंद्रण जोखिम के प्रभाव और सीमित संख्या में सेवा प्रदाताओं को महत्वपूर्ण या आवश्यक कार्यों की आउटसोर्सिंग द्वारा उत्पन्न संकेंद्रण जोखिम का प्रभावी ढंग से आकलन करना चाहिए।

सी.2 जानकारी की गोपनीयता और सुरक्षा

21. एआईएफआई अपने ग्राहकों से संबंधित डेटा और जानकारी की गोपनीयता और अखंडता के लिए जिम्मेदार होगा जो सेवा प्रदाता के पास उपलब्ध है।

22. सेवा प्रदाताओं द्वारा एआईएफआई या उसके डेटा सेंटर में मौजूद डेटा तक एक्सेस 'आवश्यकतानुसार' आधार पर होगी, जिसमें सुरक्षा उल्लंघनों या डेटा के दुरुपयोग को रोकने के लिए उचित नियंत्रण लागू होंगे।

23. एआईएफआई को सेवा प्रदाता की अभिरक्षा या कब्जे में मौजूद ग्राहक जानकारी की सुरक्षा, संरक्षण और बचाव सुनिश्चित करने का प्रयास करना चाहिए। सेवा प्रदाता या उसके स्टाफ द्वारा ग्राहक जानकारी तक एक्सेस 'आवश्यकतानुसार' आधार पर ही होगी।

24. एकाधिक सेवा प्रदाता संबंधों की स्थिति में, जहां दो या अधिक सेवा प्रदाता संपूर्ण समाधान प्रदान करने के लिए सहयोग करते हैं, एआईएफआई उन सभी सेवा प्रदाताओं के नियंत्रण वातावरण को समझने और उसकी निगरानी करने के लिए उत्तरदायी रहेगा, जिनकी पहुंचउसके डेटा, सिस्टम, रिकॉर्ड या संसाधनों तक है।

25. ऐसे मामलों में, जहां कोई सेवा प्रदाता कई आरई के लिए आउटसोर्सिंग एजेंट के रूप में कार्य करता है, एआईएफआई पर्याप्त सुरक्षा उपाय बनाने का ध्यान रखेगा ताकि जानकारी, दस्तावेज़, रिकॉर्ड और आस्तियों का संयोजन न हो।

स्पष्टीकरण: डेटा को संयोजित या मिश्रित न करने की आवश्यकता के संबंध में, यह पर्याप्त होगा यदि डेटा (एआईएफआई और उसके ग्राहक विशिष्ट डेटा तथा जानकारी) का स्पष्ट पृथक्करण और अलगाव हो ताकि यह सुनिश्चित किया जा सके कि केवल एआईएफआई द्वारा अधिकृत कर्मी ही बहु-उपयोगकर्ता स्थिति / संरचना में अपने डेटा का अभिगम प्राप्त कर सकें।

26. एआईएफआई अपने सेवा प्रदाताओं की सुरक्षा प्रथाओं और नियंत्रण प्रक्रियाओं की नियमित रूप से समीक्षा और निगरानी करेगा और सेवा प्रदाता से सुरक्षा उल्लंघनों का प्रकटीकरण करने की अपेक्षा करेगा।

27. एआईएफआई को सुरक्षा उल्लंघन और ग्राहक संबंधी गोपनीय जानकारी के लीक होने की स्थिति में तत्काल आरबीआई को सूचित करना होगा। ऐसी स्थिति में, एआईएफआई को आरबीआई द्वारा समय-समय पर जारी किए गए घटना प्रतिक्रिया और बहाली प्रबंधन संबंधी अनुदेशों का पालन करना होगा।

डी. आउटसोर्सिंग प्रक्रिया

डी.1 सेवा प्रदाता मूल्यांकन

28. किसी आउटसोर्सिंग व्यवस्था पर विचार करते समय या उसका नवीनीकरण करते समय, एआईएफआई को सम्यक जांच करनी चाहिए, ताकि आउटसोर्सिंग करार में उल्लिखित दायित्वों का निरंतर पालन करने के लिए सेवा प्रदाता की क्षमता का आकलन किया जा सके।

29. ऊपर उल्लिखित सम्यक जांच में सेवा प्रदाता के बारे में, जहां लागू हो, सभी उपलब्ध जानकारियों का मूल्यांकन शामिल होगा, जिसमें निम्नलिखित शामिल हैं, लेकिन यह इन्हीं तक सीमित नहीं हैं:

(i) गुणात्मक, मात्रात्मक, वित्तीय, परिचालनात्मक, विधिक और प्रतिष्ठा संबंधी कारक;

(ii) किसी एक सेवा प्रदाता या सीमित संख्या में सेवा प्रदाताओं को आउटसोर्सिंग करने से उत्पन्न होने वाले अनुचित संकेंद्रीकरण से जुड़े जोखिम;

(iii) पूर्व अनुभव और संविदा अवधि के दौरान प्रस्तावित गतिविधि को लागू करने और उसका समर्थन करने की सिद्ध सक्षमता;

(iv) वित्तीय सुदृढ़ता और प्रतिकूल परिस्थितियों में भी प्रतिबद्धताओं को पूरा करने की क्षमता;

(v) व्यावसायिक प्रतिष्ठा और संस्कृति, अनुपालन, शिकायतें और लंबित या संभावित मुकदमेबाजी;

(vi) हितों का टकराव, यदि कोई हो;

(vii) सेवा प्रदाता जिस क्षेत्राधिकार में काम करता है, उस क्षेत्राधिकार का राजनीतिक, आर्थिक, सामाजिक और कानूनी वातावरण जैसे बाहरी कारक और अन्य घटनाएँ जो डेटा सुरक्षा और सेवा कार्य-निष्पादन को प्रभावित कर सकती हैं;

(viii) प्रौद्योगिकी, अवसंरचनात्मक स्थिरता, सुरक्षा और आंतरिक नियंत्रण, लेखापरीक्षा कवरेज, रिपोर्टिंग और निगरानी प्रक्रियाएं, डेटा बैकअप व्यवस्था, कारोबार निरंतरता प्रबंधन और आपातकालीन बहाली योजना;

(ix) एआईएफआई के डेटा की पहचान और पृथक्करण करने की क्षमता;

(x) सेवा प्रदाता द्वारा अपने कर्मचारियों और उप-संविदाकारों के प्रति की गई सम्यक जांच की गुणवत्ता;

(xi) आउटसोर्सिंग व्यवस्था की विनियामक और कानूनी आवश्यकताओं का अनुपालन करने की क्षमता;

(xii) सूचना/साइबर सुरक्षा जोखिम मूल्यांकन;

(xiii) यह सुनिश्चित करना कि सेवा प्रदाता द्वारा संसाधित, प्रबंधित या संग्रहीत डेटा की सुरक्षा और एआईएफआई की उस डेटा तक एक्सेस सुनिश्चित करने के लिए उचित नियंत्रण, आश्वासन आवश्यकताएं और संभावित संविदात्मक व्यवस्थाएं मौजूद हैं;

(xiv) गोपनीयता बनाए रखते हुए सभी ग्राहकों को प्रभावी ढंग से सेवा प्रदान करने की क्षमता, विशेष रूप से जहां सेवा प्रदाता कई संस्थाओं के साथ जुड़ा हुआ है; और

(xv) करार को लागू करने की क्षमता और उनके तहत उपलब्ध अधिकार, जिनमें डेटा भंडारण, डेटा संरक्षण और गोपनीयता जैसे पहलुओं से संबंधित अधिकार शामिल हैं।

30. एआईएफआई को इस प्रकार की सम्यक जांच गतिविधियों को करने में जोखिम-आधारित दृष्टिकोण अपनाना चाहिए।

31. जहां संभव हो, एआईएफआई को अपनी सम्यक जांच के निष्कर्षों को पूरक करने के लिए सेवा प्रदाता पर स्वतंत्र समीक्षा और बाजार प्रतिक्रिया प्राप्त करनी चाहिए।

ई.2 आउटसोर्सिंग करार

32. एआईएफआई यह सुनिश्चित करेगा कि उसके अधिकार और दायित्व तथा प्रत्येक सेवा प्रदाता के अधिकार और दायित्व कानूनी रूप से बाध्यकारी लिखित करार में स्पष्ट रूप से परिभाषित और निर्धारित हों। सिद्धांत रूप में, समझौते के प्रावधानों में एआईएफआई के कारोबार के लिए आउटसोर्स किए गए कार्य की गंभीरता, उससे जुड़े जोखिम और उन्हें कम करने या प्रबंधित करने की रणनीतियों का उचित रूप से ध्यान रखा जाएगा।

33. आउटसोर्सिंग व्यवस्था को अभिशासित करने वाले नियम और शर्तें एआईएफआई के कानूनी सलाहकार द्वारा सावधानीपूर्वक परिभाषित और उनकी कानूनी वैधता और प्रवर्तनीयता की जांच की जाएगी। एआईएफआई यह सुनिश्चित करेगा कि ऐसा करार पर्याप्त रूप से लचीला हो ताकि एआईएफआई आउटसोर्स की गई सेवा पर पर्याप्त नियंत्रण बनाए रख सके और कानूनी एवं विनियामक दायित्वों को पूरा करने के लिए उचित उपाय करने का अधिकार प्राप्त कर सके। करार में पक्षों के बीच कानूनी संबंध की प्रकृति का भी स्पष्ट रूप से उल्लेख किया जाएगा।

34. करार में (इन निदेशों के दायरे के अनुसार) कम से कम निम्नलिखित पहलुओं को भी शामिल होना चाहिए:

(i) आउटसोर्स की जा रही सेवा का विवरण, जिसमें उप-संविदाकारों, यदि कोई हो, के लिए उपयुक्त सेवा और कार्य निष्पादन मानक शामिल हों;

(ii) सेवा प्रदाता के पास उपलब्ध आउटसोर्स की गई सेवा से संबंधित सभी डेटा, बही-खातों, अभिलेखों, जानकारी, लॉग, अलर्ट और कारोबार परिसरों तक एआईएफआई का प्रभावी अभिगम;

(iii) एआईएफआई द्वारा जोखिमों के समग्र रूप से निरंतर प्रबंधन के लिए सेवा प्रदाता की नियमित निगरानी और मूल्यांकन, ताकि कोई भी आवश्यक सुधारात्मक उपाय तुरंत किया जा सके;

(iv) आउटसोर्स की गई सेवाओं से संबंधित महत्वपूर्ण प्रतिकूल घटनाओं के प्रकार (जैसे, डेटा उल्लंघन, सेवा से इनकार और सेवा की अनुपलब्धता) और एआईएफआई को रिपोर्ट की जाने वाली घटनाएं, ताकि एआईएफआई त्वरित जोखिम निवारण उपाय कर सके और सांविधिक तथा विनियामक दिशानिर्देशों का अनुपालन सुनिश्चित कर सके;

(v) ग्राहक डेटा की सुरक्षा के लिए सूचना प्रौद्योगिकी अधिनियम 2000 और अन्य लागू कानूनी आवश्यकताओं और मानकों के प्रावधानों का अनुपालन;

(vi) सेवा स्तरीय करारों (एसएलए) सहित वे प्रदेय जो सेवा स्तरों की गुणवत्ता और मात्रा को मापने के लिए कार्य निष्पादन मानदंडों को औपचारिक रूप देते हैं;

(vii) मौजूदा विनियामक आवश्यकताओं के अनुसार केवल भारत में ही डेटा का भंडारण (जैसा लागू हो);

(viii) सेवा प्रदाता को कैप्चर, संसाधित और संग्रहीत किए गए डेटा (एआईएफआई और उसके ग्राहकों से संबंधित) का विवरण प्रदान करने की आवश्यकता वाले खंड;

(ix) एआईएफआई और उसके ग्राहकों के डेटा की गोपनीयता बनाए रखने के लिए नियंत्रण और सुरक्षा उल्लंघन तथा ऐसी जानकारी के लीक होने की स्थिति में एआईएफआई के प्रति सेवा प्रदाता की देयता को शामिल करना;

(x) सेवा प्रदाता को एआईएफआई के ग्राहक या किसी अन्य पक्ष के साथ साझा करने की अनुमति प्राप्त डेटा/जानकारी के प्रकार;

(xi) समाधान प्रक्रिया, चूक की घटनाएं, क्षतिपूर्ति, उपाय और संबंधित पक्षों के लिए उपलब्ध उपाय;

(xii) कारोबार निरंतरता और परीक्षण आवश्यकताओं को सुनिश्चित करने के लिए आकस्मिक योजना(एं);

(xiii) एआईएफआई द्वारा सेवा प्रदाता (जिसमें उसके उपसंविदाकार भी शामिल हैं) पर लेखापरीक्षा करने का अधिकार, चाहे वह उसके आंतरिक या बाह्य लेखापरीक्षकों द्वारा हो या उसकी ओर से कार्य करने के लिए नियुक्त एजेंटों द्वारा हो और एआईएफआई के लिए की गई सेवाओं के संबंध में सेवा प्रदाता पर की गई किसी भी लेखापरीक्षा या समीक्षा रिपोर्ट और निष्कर्षों की प्रतियां प्राप्त करने का अधिकार;

(xiv) सेवा प्रदाता से आपूर्ति श्रृंखला में शामिल तृतीय पक्षों के बारे में जानकारी प्राप्त करने का अधिकार;

(xv) सेवा प्रदाता और उसके किसी भी उप-संविदाकार का निरीक्षण करने के लिए आरबीआई या उसके द्वारा अधिकृत व्यक्ति (व्यक्तियों) के अधिकार को मान्यता देना।

(xvi) आउटसोर्सिंग व्यवस्था के दायरे के संबंध में और यथा लागू आरबीआई या उसके द्वारा अधिकृत व्यक्ति(यों) को सेवा प्रदाता और उसके किसी भी उप-संविदाकार का निरीक्षण करने और एआईएफआई के आईटी अवसंरचना, एप्लिकेशन, डेटा, दस्तावेजों और सेवा प्रदाता/या उसके उप-संविदाकारों को दी गई, द्वारा संग्रहीत या संसाधित की गई अन्य आवश्यक जानकारी को एक्सेस करने की अनुमति देने वाले खंड;

(xvii) वे खंड जो सेवा प्रदाता को उसके संविदाकारों के कार्य निष्पादन और जोखिम प्रबंधन प्रथाओं के लिए संविदात्मक रूप से उत्तरदायी बनाते हैं;

(xviii) एआईएफआई द्वारा निर्दिष्ट विशिष्ट संविदात्मक नियमों और शर्तों के माध्यम से सेवा प्रदाता को आउटसोर्स की गई सेवाओं के संबंध में आरबीआई द्वारा जारी निदेशों का पालन करने का सेवा प्रदाता का दायित्व;

(xix) आउटसोर्स की गई सेवा के सभी या कुछ हिस्सों के लिए सेवा प्रदाता द्वारा उपसंविदाकारों के उपयोग के लिए एआईएफआई के पूर्व अनुमोदन या सहमति की आवश्यकता वाले खंड;

(xx) एआईएफआई का समापन अधिकार, जिसमें आवश्यकता पड़ने पर या वांछनीय होने पर प्रस्तावित आउटसोर्सिंग व्यवस्था को किसी अन्य सेवा प्रदाता को व्यवस्थित रूप से हस्तांतरित करने की क्षमता शामिल है;

(xxi) एआईएफआई के दिवालियापन / समाधान की स्थिति में संबंधित अधिकारियों के साथ सहयोग करने का सेवा प्रदाता की बाध्यतादायित्व;

(xxii) मुख्य सेवाएं प्रदान करने वाले सेवा प्रदाताओं के कुशल संसाधनों को 'आवश्यक कर्मियों' के रूप में मानने का प्रावधान ताकि महत्वपूर्ण कार्यों को संचालित करने के लिए आवश्यक बैकअप व्यवस्था के साथ सीमित संख्या में कर्मचारी आपात स्थितियों (महामारी की स्थितियों सहित) के दौरान साइट पर काम कर सकें;

(xxiii) सेवा प्रदाताओं और ओईएम के बीच उपयुक्त बैक-टू-बैक व्यवस्था की आवश्यकता वाला खंड; और

(xxiv) सेवा प्रदाता द्वारा रखी गई जानकारी के संबंध में गैर-प्रकटीकरण करार की आवश्यकता वाला खंड।

डी.3 आउटसोर्स की गई सेवाओं की निगरानी और नियंत्रण

35. एआईएफआई के पास अपनी आउटसोर्स सेवाओं की निगरानी और नियंत्रण के लिए एक प्रबंधन संरचना होनी चाहिए। इसमें (इन निदेशों के दायरे के अनुसार), कार्य निष्पादन की निगरानी, प्रणालियों और संसाधनों का अपटाइम, सेवा उपलब्धता, एसएलए आवश्यकताओं का अनुपालन और घटना प्रतिक्रिया तंत्र शामिल होगी, लेकिन यह इन्हीं तक सीमित नहीं होगी।

36. एआईएफआई द्वारा आउटसोर्स की गई सेवाओं के संबंध में सेवा प्रदाताओं (उप-संविदाकारों सहित) की नियमित लेखापरीक्षा (इन निदेशों के दायरे में लागू) कराई जाएगी। ऐसी लेखापरीक्षा एआईएफआई की ओर से नियुक्त एआईएफआई के आंतरिक या बाह्य लेखापरीक्षकों द्वारा कराई जा सकती है।

37. विभिन्न आईटी सेवाओं को आउटसोर्स करते समय, एक से अधिक आरई एक ही सेवा प्रदाता से सेवाएं ले सकती हैं। ऐसे परिदृश्यों में, एक ही सेवा प्रदाता के लिए अलग-अलग आरई द्वारा अलग-अलग ऑडिट करने के बजाय, वे संयुक्त (साझा) ऑडिट का विकल्प चुन सकती हैं। इससे संबंधित आरई को अपने ऑडिट संसाधनों को साझा करने या किसी स्वतंत्र तृतीय-पक्ष ऑडिटर को संयुक्त रूप से एक ही सेवा प्रदाता का ऑडिट करने की सुविधा मिलती है। हालांकि, ऐसा करते समय, आरई की यह जिम्मेदारी होगी कि वे सेवा प्रदाता के साथ अपनी-अपनी संविदा से संबंधित ऑडिट आवश्यकताओं को प्रभावी ढंग से पूरा करें।

38. लेखापरीक्षाओं में अन्य बातों के साथ-साथ सेवा प्रदाता के कार्य निष्पादन, सेवा प्रदाता द्वारा अपनाई गई जोखिम प्रबंधन पद्धतियों की पर्याप्तता और कानूनों एवं विनियमों के अनुपालन का आकलन किया जाएगा। लेखापरीक्षा की आवृत्ति जोखिम की प्रकृति और सीमा तथा आउटसोर्सिंग व्यवस्थाओं से एआईएफआई पर पड़ने वाले प्रभाव के आधार पर निर्धारित की जाएगी। निगरानी एवं नियंत्रण

गतिविधियों पर रिपोर्टों की वरिष्ठ प्रबंधन द्वारा समय-समय पर समीक्षा की जाएगी और किसी भी प्रतिकूल घटनाक्रम की स्थिति में, इसकी जानकारी बोर्ड को दी जाएगी।

39. जोखिम मूल्यांकन के आधार पर, एआईएफआई स्वतंत्र ऑडिट कराने के बजाय सेवा प्रदाता द्वारा उपलब्ध कराए गए विश्व स्तर पर मान्यता प्राप्त तृतीय-पक्ष प्रमाणण पर भी भरोसा कर सकता है। हालांकि, इससे एआईएफआई सेवा प्रदाता के यहां डेटा सुरक्षा (सिस्टम की उपलब्धता सहित) सुनिश्चित करने के लिए आवश्यक नियंत्रणों और प्रक्रियाओं की पुष्टि करने की अपनी जिम्मेदारी से मुक्त नहीं होगा।

40. एआईएफआई को समय-समय पर सेवा प्रदाता की वित्तीय और परिचालन स्थिति की समीक्षा करनी चाहिए ताकि उसकी दायित्वों को पूरा करने की क्षमता का आकलन किया जा सके। एआईएफआई को समीक्षा की अवधि निर्धारित करते समय जोखिम-आधारित दृष्टिकोण अपनाना चाहिए। ऐसी गहन जांच में कार्य निष्पादन मानकों, गोपनीयता तथा सुरक्षा और परिचालन लचीलेपन की तैयारी में किसी भी प्रकार की गिरावट या उल्लंघन को उजागर किया जाना चाहिए।

41. एआईएफआई यह सुनिश्चित करेगा कि उचित सुरक्षा प्रोटोकॉल के अधीन, एआईएफआई, उसके लेखा परीक्षकों, आरबीआई और अन्य संबंधित सक्षम अधिकारियों द्वारा कानून के तहत अधिकृत प्रभावी निरीक्षण के उद्देश्य से सेवा प्रदाता (क) आउटसोर्स की गई सेवाओं से संबंधित डेटा; (ख) सेवा प्रदाता के संबंधित व्यावसायिक परिसर तक अप्रतिबंधित और प्रभावी एक्सेस प्रदान करे।

डी.4 आउटसोर्स की गई सेवाओं की सूची

42. एआईएफआई को सेवा प्रदाताओं को आउटसोर्स की गई आईटी सेवाओं की सूची बनानी होगी (जिसमें उनकी आपूर्ति श्रृंखला में शामिल प्रमुख संस्थाएं भी शामिल हों)। इसके अलावा, एआईएफआई को तृतीय पक्षों पर अपनी निर्भरता का आकलन करना होगा और सेवा प्रदाताओं से प्राप्त जानकारी का समय-समय पर मूल्यांकन करना होगा।

डी.5 कारोबार निरंतरता और आपातकालीन बहाली योजना का प्रबंधन

43. एआईएफआई को अपने सेवा प्रदाताओं से यह अपेक्षित है कि वे कारोबार निरंतरता योजना (बीसीपी) और आपातकालीन बहाली योजना (डीआरपी) के दस्तावेजीकरण, रखरखाव और परीक्षण के लिए एक मजबूत ढांचा विकसित और स्थापित करें, जो आउटसोर्स की गई सेवा की प्रकृति और

दायरे के अनुरूप हो, जैसा कि आरबीआई द्वारा समय-समय पर बीसीपी/डीआरपी आवश्यकताओं पर जारी किए गए मौजूदा अनुदेशों में उल्लेख किया गया है।

44. एआईएफआई को एक व्यवहार्य आकस्मिक योजना स्थापित करने में, आपात स्थिति में वैकल्पिक सेवा प्रदाताओं की उपलब्धता या आउटसोर्स की गई सेवा को वापस इन-हाउस करने की संभावना और इसमें शामिल लागत, समय और संसाधनों पर विचार करना चाहिए।

45. आउटसोर्सिंग करार की अप्रत्याशित समापन या सेवा प्रदाता के दिवालियापन या परिसमापन के जोखिम को कम करने के लिए, एआईएफआई को अपने आउटसोर्सिंग व्यवस्था पर उचित स्तर का नियंत्रण बनाए रखना चाहिए और साथ ही अपने कारोबार संचालन को जारी रखने के लिए उचित उपायों के साथ हस्तक्षेप करने का अधिकार भी रखना चाहिए।

46. एआईएफआई यह सुनिश्चित करेगा कि उसके सेवा प्रदाता एआईएफआई की जानकारी, दस्तावेज़, अभिलेख और अन्य परिसंपत्तियों को अलग रखने में सक्षम हों, ताकि प्रतिकूल परिस्थितियों या करार के समापन की स्थिति में, सेवा प्रदाता को दिए गए सभी दस्तावेज़, लेनदेन के अभिलेख और जानकारी तथा एआईएफआई की परिसंपत्तियों को सेवा प्रदाता के कब्जे से हटाया या उन्हें मिटाया, नष्ट किया जा सके या अनुपयोगी बनाया जा सके।

डी.6 निकास रणनीति

47. आईटी आउटसोर्सिंग नीति में आउटसोर्स की गई आईटी सेवाओं के संबंध में एक स्पष्ट निकास रणनीति होनी चाहिए, ताकि निकास के दौरान और उसके बाद कारोबार निरंतरता सुनिश्चित हो सके।

48. रणनीति में सेवाओं से निकास या समापन करने के विभिन्न परिदृश्यों के लिए योजनाएं शामिल होंगी, जिनमें आवश्यकतानुसार ऐसी योजनाओं को निष्पादित करने के लिए न्यूनतम अवधि का प्रावधान होगा।

49. अपनी निकास रणनीति का दस्तावेजीकरण करते समय, एआईएफआई को अन्य बातों के साथ-साथ, वैकल्पिक व्यवस्थाओं की पहचान करनी होगी, जिसमें किसी भिन्न सेवा प्रदाता द्वारा या स्वयं एआईएफआई द्वारा सेवा प्रदान करना शामिल हो सकता है।

50. सेवा प्रदाता सुचारू संक्रमण सुनिश्चित करने के लिए एआईएफआई और उसके नए सेवा प्रदाता (प्रदाताओं) दोनों के साथ पूर्ण सहयोग करने के लिए कानूनी रूप से बाध्य होगा।

51. एआईएफआई यह सुनिश्चित करेगा कि आउटसोर्सिंग करार में डेटा, हार्डवेयर और सभी अभिलेखों (डिजिटल और भौतिक) को सुरक्षित रूप से हटाने या नष्ट करने संबंधी आवश्यक खंड शामिल हों।

52. आउटसोर्सिंग करार में यह सुनिश्चित किया जाएगा कि सेवा प्रदाता को संक्रमणकालीन अवधि के दौरान किसी भी डेटा को मिटाने, हटाने, रद्द करने, वापस लेने या परिवर्तित करने से प्रतिबंधित किया जाए, जब तक कि आरबीआई या संबंधित एआईएफआई द्वारा विशेष रूप से ऐसा करने के लिए सूचित न किया जाए।

डी.7 समापन

53. यदि किसी कारणवश आउटसोर्सिंग करार समाप्त हो जाता है और सेवा प्रदाता एआईएफआई के ग्राहकों से व्यवहार करता है, तो एआईएफआई द्वारा इसकी उचित सूचना सार्वजनिक की जाएगी ताकि यह सुनिश्चित हो सके कि ग्राहक संबंधित सेवा प्रदाता से व्यवहार करना बंद कर दें।

ई. विशिष्ट आउटसोर्सिंग व्यवस्थाएं

ई.1 समूह / संगुट के भीतर आउटसोर्सिंग

54. एआईएफआई अपने व्यावसायिक समूह/ संगुट के भीतर किसी भी आईटी सेवा को आउटसोर्स कर सकता है, बशर्ते कि ऐसी व्यवस्था बोर्ड द्वारा अनुमोदित नीति द्वारा समर्थित हो और उसके समूह संस्थाओं के साथ उचित एसएलए/करार मौजूद हों।

55. समूह संस्था का चयन वस्तुनिष्ठ कारणों पर आधारित होगा जो किसी तीसरे पक्ष के चयन के समान हों और एआईएफआई को ऐसे आउटसोर्सिंग व्यवस्था से उत्पन्न होने वाले हितों के किसी भी टकराव से उचित रूप से निपटना होगा।

56. एआईएफआई को अपने समूह की संस्थाओं के साथ लेन-देन में हमेशा अहस्तक्षेपी संबंध बनाए रखना चाहिए। समूह की किसी संस्था को आउटसोर्सिंग करते समय एआईएफआई द्वारा अपनाई जाने वाली जोखिम प्रबंधन पद्धतियाँ, किसी गैर-संबंधित पक्ष के लिए निर्दिष्ट पद्धतियों के समान होनी चाहिए।

ई.2 अपतटीय या सीमापारीय आउटसोर्सिंग

57. सिद्धांत रूप में, आउटसोर्सिंग व्यवस्था केवल उन पक्षों के साथ की जाएगी जो ऐसे अधिकारक्षेत्रों में काम करते हैं जो सामान्यतः गोपनीयता शर्तों और करार का पालन करते हैं।

58. विदेश में सेवा प्रदाता(ओं) के साथ कार्य करते समय, एआईएफआई को निम्नलिखित कार्य करने होंगे:

(i) सेवा प्रदाता जिस क्षेत्राधिकार में स्थित है, वहां की सरकारी नीतियों और राजनीतिक, सामाजिक, आर्थिक और कानूनी स्थितियों की निरंतर निगरानी करना और देश के जोखिम को कम करने के लिए ठोस प्रक्रियाएं स्थापित करना। इसमें अन्य बातों के साथ-साथ, उचित आकस्मिकता और निकास रणनीतियां शामिल हैं;

(ii) आउटसोर्सिंग व्यवस्था के अभिशासी कानून को स्पष्ट रूप से निर्दिष्ट करना;

(iii) यह सुनिश्चित करना कि सेवा प्रदाता के परिसमापन की स्थिति में भी एआईएफआई और आरबीआई को अभिलेखों की उपलब्धता प्रभावित न हो;

(iv) विदेशी क्षेत्राधिकार में स्थित सेवा प्रदाता की लेखापरीक्षा या निरीक्षण निर्देशित करने और संचालित करने के एआईएफआई और आरबीआई के अधिकार को सुनिश्चित करना; और

(v) यह सुनिश्चित करना कि व्यवस्था सभी सांविधिक आवश्यकताओं के साथ-साथ आरबीआई द्वारा समय-समय पर जारी किए गए विनियमों का अनुपालन करती है।

ई.3 सुरक्षा परिचालन केंद्र (एसओसी) की आउटसोर्सिंग

59. एआईएफआई द्वारा सुरक्षा परिचालन केंद्र (एसओसी) के संचालन को आउटसोर्स करने से जुड़े जोखिमों को ध्यान में रखते हुए, जैसे कि डेटा का बाहरी स्थान पर संग्रहीत और संसाधित होना और सेवा प्रदाता (या उसके उप-संविदाकारों) द्वारा प्रबंधित किया जाना, जिस पर एआईएफआई की कम पहुंच होती है, इन जोखिमों को कम करने के लिए, एआईएफआई को इन निदेशों में निर्धारित नियंत्रणों के अतिरिक्त, एसओसी संचालन को आउटसोर्स करने के मामले में निम्नलिखित आवश्यकताओं को अपनाना होगा:

(i) सेवाओं के प्रावधान में उपयोग की जाने वाली आस्तियों (जैसे, सिस्टम, सॉफ्टवेयर, सोर्स कोड, प्रक्रियाएं और अवधारणाएं) के स्वामी की स्पष्ट रूप से पहचान करना;

(ii) यह सुनिश्चित करना कि एआईएफआई के पास नियम परिभाषा, अनुकूलन और संबंधित डेटा/लॉग, मेटा-डेटा और विश्लेषण (एआईएफआई के लिए विशिष्ट) पर पर्याप्त निगरानी और स्वामित्व हो;

(iii) सेवा वितरण में शामिल सभी भौतिक सुविधाओं, जैसे कि एसओसी और उन क्षेत्रों जहां ग्राहक डेटा संग्रहीत या संसाधित किया जाता है, सहित एसओसी के कामकाज का समय-समय पर मूल्यांकन करना;

(iv) आउटसोर्स किए गए एसओसी रिपोर्टिंग और एस्केलेशन प्रक्रिया को एआईएफआई की घटना प्रतिक्रिया प्रक्रिया के साथ एकीकृत करना; और

(v) अलर्ट या घटनाओं से निपटने की प्रक्रिया की समीक्षा करना।

ई.4 क्लाउड कंप्यूटिंग सेवाओं का उपयोग

60. समय के साथ कई क्लाउड परिनियोज और सेवा मॉडल उभर कर सामने आए हैं। ये आम तौर पर उपभोक्ता संस्था द्वारा अपनाई जाने वाली प्रौद्योगिकी स्टैक की सीमा पर आधारित होते हैं।

(1) *उदाहरण - 1:* (i) कुछ क्लाउड सेवाएं निम्नलिखित हैं:

(ए) **इन्फ्रास्ट्रक्चर एज़ ए सर्विस (आईएएएस):** यह सेवा कंप्यूटिंग, स्टोरेज, नेटवर्क और अन्य बुनियादी संसाधन प्रदान करती है ताकि क्लाइंट अपने एप्लिकेशन विकसित और तैनात कर सकें।

(बी) **प्लेटफ़ॉर्म एज़ ए सर्विस (पीएएएस):** यह सेवा क्लाइंट को एप्लिकेशन, मिडलवेयर, डेटाबेस, डेवलपमेंट एनवायरनमेंट और अन्य टूल्स के निर्माण के लिए सॉफ्टवेयर के साथ-साथ बुनियादी ढांचा भी प्रदान करती है।

(सी) **सॉफ्टवेयर एज़ ए सर्विस (एसएएएस):** क्लाइंट सेवा प्रदाता द्वारा क्लाउड इन्फ्रास्ट्रक्चर पर उपलब्ध कराए गए एप्लिकेशन का उपयोग करता है।

(ii) तीन सामान्य एप्लिकेशन सेवाओं के अलावा, क्लाउड सेवा प्रदाता (सीएसपी) विभिन्न जोखिम स्तरों के साथ कई प्रकार की सेवाएं भी प्रदान करते हैं, जैसे कि डेटाबेस एज़ ए सर्विस, सिक्योरिटी एज़ ए सर्विस, स्टोरेज एज़ ए सर्विस और अन्य।

(2) *उदाहरण - 2:* क्लाउड सेवाओं की डिलीवरी के लिए कुछ लोकप्रिय डिप्लॉइमेंट मॉडल प्राइवेट क्लाउड, पब्लिक क्लाउड, हाइब्रिड क्लाउड और कम्युनिटी क्लाउड हैं।

61. क्लाउड डिप्लॉइमेंट और सर्विस मॉडल से जुड़ी विभिन्न सेवाओं, लाभों और जोखिम प्रोफाइल को ध्यान में रखते हुए, क्लाउड वातावरण में डेटा के स्टोरेज, कंप्यूटिंग और मूवमेंट के लिए क्लाउड सेवाओं का उपयोग करने वाला एआईएफआई, इन निदेशों में अन्य लागू प्रावधानों के अतिरिक्त, निम्नलिखित कार्य करेगा:

(i) मौजूदा आईटी एप्लिकेशन के उपयोग और उनसे संबंधित लागतों के संदर्भ में अपनी कारोबार रणनीति और लक्ष्यों का व्यापक मूल्यांकन करना। इस मूल्यांकन में क्लाउड से संबंधित विभिन्न व्यय मदों का विश्लेषण शामिल होगा, जैसे कि एप्लिकेशन रीफैक्टरिंग, एकीकरण, परामर्श, माइग्रेशन और कार्यभार की प्रकृति के आधार पर अनुमानित आवर्ती व्यय। क्लाउड को अपनाने का दायरा भिन्न हो सकता है, जिसमें गैर- कारोबारिक रूप से महत्वपूर्ण कार्यभारों को क्लाउड पर माइग्रेट करना, एसएएएस जैसे महत्वपूर्ण कारोबार एप्लिकेशन का डिप्लॉइमेंट या इनके बीच के अन्य संयोजन शामिल हो सकते हैं और यह विधिवत किए गए कारोबार प्रौद्योगिकी जोखिम मूल्यांकन के आधार पर निर्धारित किया जाएगा;

(ii) यह सुनिश्चित करना कि इन निदेशों के पैरा 15 में उल्लिखित 'आईटी आउटसोर्सिंग नीति' डेटा के संपूर्ण जीवनचक्र को कवर करती है, अर्थात् डेटा के सृजन से लेकर क्लाउड में उसके प्रवेश और उसके स्थायी रूप से मिटाए जाने या हटाए जाने तक की पूरी अवधि को शामिल करती है। यह भी सुनिश्चित करना कि निर्दिष्ट प्रक्रियाएं कारोबारिक आवश्यकताओं और कानूनी एवं विनियामक आवश्यकताओं के अनुरूप हों;

(iii) उचित जोखिम प्रबंधन ढांचा स्थापित करते समय क्लाउड सेवा विशिष्ट कारकों, जैसे कि बहु-किरायेदारी और डेटा के बहु-स्थान भंडारण या प्रसंस्करण तथा उनसे जुड़े जोखिमों को ध्यान में रखना;

(iv) एआईएफआई और क्लाउड सेवा प्रदाता (सीएसपी) के बीच साझा उत्तरदायित्व मॉडल की प्रयोज्यता के अनुसार, क्लाउड सुरक्षा सर्वोत्तम प्रथाओं का संदर्भ लेते हुए आवश्यक नियंत्रण लागू करना;

क्लाउड सुरक्षा के सर्वोत्तम तरीकों के लिए, एआईएफआई अन्य बातों के साथ-साथ, NIST SP 800-210 जनरल एक्सेस कंट्रोल गाइडेंस फॉर क्लाउड सिस्टम्स (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf) का संदर्भ ले सकता है

(v) एक सुस्थापित और दस्तावेजीकृत क्लाउड अडाप्शन पॉलिसी को अपनाकर और प्रदर्शित करके मजबूत क्लाउड गवर्नेंस स्थापित करना। ऐसी नीति में अन्य बातों के साथ-साथ निम्नलिखित शामिल होंगे:

(ए) उन सेवाओं की पहचान करना जिन्हें क्लाउड पर अंतरित किया जा सकता है;

(बी) विभिन्न हितधारकों के हितों की सुरक्षा को सक्षम और समर्थन प्रदान करना;

(सी) गोपनीयता, सुरक्षा, डेटा संप्रभुता, प्रतिलब्धता और डेटा वर्गीकरण के अनुरूप डेटा भंडारण आवश्यकताओं सहित विनियामक आवश्यकताओं का अनुपालन सुनिश्चित करना; और

(डी) सीएसपी से जुड़े जोखिमों के प्रबंधन और निरंतर निगरानी के लिए समुचित सावधानी बरतना;

(vi) यह सुनिश्चित करना कि सीएसपी का चयन सीएसपी के व्यापक जोखिम मूल्यांकन पर आधारित हो। एआईएफआई केवल उन्हीं सीएसपी के साथ संविदा करेगा जो ऐसे क्षेत्राधिकारों के अधीन हों जो करार की प्रवर्तनीयता और एआईएफआई को उपलब्ध अधिकारों का समर्थन करते हों, जिनमें डेटा संग्रहण, डेटा सुरक्षा और गोपनीयता जैसे पहलू शामिल हैं;

(vii) यह सुनिश्चित करना कि क्लाउड-आधारित एप्लिकेशन को समर्थन देने वाली सेवा और प्रौद्योगिकी संरचना विश्व स्तर पर मान्यता प्राप्त संरचना सिद्धांतों और मानकों के अनुपालन में निर्मित की गई है। प्रौद्योगिकी संरचना में निम्नलिखित विशेषताएं होनी चाहिए:

(ए) कंटेनर, इमेज और रिलीज़ के प्रबंधन के लिए मानक टूल और प्रक्रियाओं का एक सेट प्रदान करना;

(बी) सुरक्षित कंटेनर-आधारित डेटा प्रबंधन प्रदान करना, जहां एन्क्रिप्शन की और हार्डवेयर सुरक्षा मॉड्यूल एआईएफआई के नियंत्रण में हों;

(सी) बहु-किरायेदारी वाले वातावरण में डेटा अखंडता और गोपनीयता जोखिमों तथा डेटा के मिश्रण से सुरक्षा प्रदान करना; और

(डी) लचीला होना और क्लाउड आर्किटेक्चर में किसी एक या एक से अधिक घटकों की विफलता की स्थिति में डेटा/सूचना सुरक्षा पर न्यूनतम प्रभाव के साथ सुचारू रूप से रिकवरी करना;

(viii) सीएसपी के साथ पहचान और पहुंच प्रबंधन (आईएएम) पर सहमति बनाना और सुनिश्चित करना कि क्लाउड पर होस्ट किए गए एप्लिकेशन तक उपयोगकर्ता एक्सेस और विशेषाधिकार प्राप्त एक्सेस दोनों के संबंध में भूमिका-आधारित एक्सेस प्रदान की जाए। एआईएफआई को निम्नलिखित करना होगा:

(ए) क्लाउड-आधारित एप्लिकेशन हेतु आईएएम के लिए, ऑन-प्रिमाइसेस एप्लिकेशन के लिए लागू होने वाले सख्त एक्सेस नियंत्रण स्थापित करना;

(बी) क्लाउड-होस्टेड एप्लिकेशन में क्लाउड सर्विस मॉडल की परवाह किए बिना, सभी प्रकार के उपयोगकर्ता-एक्सेस और विशेषाधिकार-एक्सेस भूमिकाओं के लिए कर्तव्यों का पृथक्करण और भूमिका संघर्ष मैट्रिक्स लागू करना;

(सी) यह सुनिश्चित करना कि एक्सेस प्रदान करने का कार्य 'आवश्यकतानुसार' और 'न्यूनतम विशेषाधिकार' के सिद्धांतों द्वारा नियंत्रित हो; और

(डी) क्लाउड एप्लिकेशन तक एक्सेस के लिए बहु-कारक प्रमाणीकरण लागू करना;

(ix) यह सुनिश्चित करना कि क्लाउड-आधारित एप्लिकेशन में सुरक्षा नियंत्रणों का कार्यान्वयन ऑन-प्रिमाइसेस एप्लिकेशन में या उसके द्वारा प्राप्त किए गए नियंत्रण उद्देश्यों के समान या उससे उच्च स्तर के नियंत्रण उद्देश्यों को प्राप्त करता है। इसमें नेटवर्क सुरक्षा संसाधनों और उनके कॉन्फ़िगरेशन की उचित तैनाती के माध्यम से सुरक्षित कनेक्शन सुनिश्चित करना;

एआईएफआई द्वारा उपयोग की जाने वाली क्लाउड आस्तियों का उचित और सुरक्षित कॉन्फ़िगरेशन, निगरानी और क्लाउड एप्लिकेशन और संबंधित संसाधनों में परिवर्तन को अधिकृत करने के लिए आवश्यक प्रक्रियाएं शामिल हैं;

(x) क्लाउड वातावरण में न्यूनतम निगरानी आवश्यकताओं को परिभाषित करना और सीएसपी की सूचना/साइबर सुरक्षा क्षमता का आकलन करना, यह सुनिश्चित करने के लिए कि यह:

(ए) कमजोरियों और खतरों के प्रति अपने जोखिमों के अनुरूप सूचना सुरक्षा नीति ढांचा बनाए रखता है;

(बी) सूचना आस्तियों या अपने कारोबारिक वातावरण में परिवर्तन के परिणामस्वरूप उत्पन्न होने वाली कमजोरियों और खतरों सहित, उनमें होने वाले परिवर्तनों के संबंध में अपनी सूचना/साइबर सुरक्षा क्षमता को बनाए रखने में सक्षम है;

(सी) एआईएफआई द्वारा आउटसोर्स की जा रही सेवाओं की महत्ता और खतरे के वातावरण के अनुरूप आउटसोर्स की गई सेवाओं के संबंध में नियंत्रणों के परीक्षण की प्रकृति और आवृत्ति निर्धारित की गई है; और

(डी) जहां लागू हो, उपसंविदाकारों के साथ साझा किए जा रहे डेटा की गोपनीयता, अखंडता और उपलब्धता के संबंध में उनका आकलन करने के लिए तंत्र मौजूद हैं;

(xi) जहां भी लागू हो, सीएसपी से प्राप्त लॉग और घटनाओं का एआईएफआई के एसओसी में उचित एकीकरण सुनिश्चित करना और क्लाउड पर तैनात सेवाओं से संबंधित घटनाओं की रिपोर्टिंग और प्रबंधन के लिए प्रासंगिक लॉग को क्लाउड में सुरक्षित रखना;

(xii) यह सुनिश्चित करना कि सीएसपी के साइबर रेज़िलिएंस नियंत्रण एआईएफआई के अपने एप्लिकेशन सुरक्षा उपायों के पूरक हों और एआईएफआई तथा सीएसपी दोनों ही सुरक्षा संबंधी सॉफ़्टवेयर के निरंतर और नियमित अपडेट बनाए रखें, जिनमें अपग्रेड, फिक्स, पैच और सर्विस पैक शामिल हैं, ताकि उन्नत खतरों और मैलवेयर से एप्लिकेशन को सुरक्षित रखा जा सके;

(xiii) यह सुनिश्चित करना कि सीएसपी के पास खतरों और कमजोरियों के प्रबंधन के लिए एक सुव्यवस्थित और संरचित दृष्टिकोण हो, जो आवश्यक उद्योग-विशिष्ट खतरे की खुफिया क्षमताओं द्वारा समर्थित हो;

(xiv) यह सुनिश्चित करना कि कारोबार निरंतरता ढांचा एआईएफआई की क्लाउड सेवाओं को प्रभावित करने वाली आपदा या सीएसपी की विफलता की स्थिति में महत्वपूर्ण कार्यों के निरंतर संचालन को न्यूनतम व्यवधान के साथ और डेटा अखंडता तथा सुरक्षा से समझौता किए बिना सुनिश्चित करे;

(xv) यह सुनिश्चित करना कि सीएसपी ने अपने द्वारा उपयोग की जा रही क्लाउड सेवाओं के संबंध में साइबर लचीलेपन के लिए तैयारी और तत्परता हेतु प्रदर्शनकारी क्षमताएं स्थापित की हैं, जिसमें अन्य बातों के साथ-साथ, मजबूत घटना प्रतिक्रिया और पुनर्प्राप्ति प्रक्रिया शामिल हैं, साथ ही क्लाउड सेवाओं के विभिन्न स्तरों पर आवश्यक हितधारकों सहित डीआर अभ्यास का संचालन करना भी शामिल है;

(xvi) निकास रणनीति विकसित करें जो

(ए) इसमें अन्य बातों के साथ-साथ, एआईएफआई की सेवा संबंधी संपार्श्विक और सीएसपी द्वारा धारित डेटा को वापस करने के लिए सहमत प्रक्रियाएं और समय-सीमा; डेटा की पूर्णता और सुवाह्यता; सीएसपी के वातावरण से एआईएफआई की जानकारी का सुरक्षित निष्कासन; सेवाओं का सुचारू संक्रमण; और देनदारियों, क्षति, दंड और क्षतिपूर्ति की स्पष्ट परिभाषा शामिल होनी चाहिए, जो एसएलए में सेवा स्तर की शर्तों का भी हिस्सा होनी चाहिए;

(बी) निकास योजनाओं को शामिल करें जो एप्लिकेशन और सेवा वितरण प्रौद्योगिकी स्टैक के चल रहे डिजाइन के अनुरूप हों;

(सी) इसमें संविदात्मक रूप से सहमत निकास/समापन योजनाएँ शामिल करें, जो यह निर्दिष्ट करती हों कि एआईएफआई के कारोबार निरंतरता पर न्यूनतम प्रभाव डालते हुए, अखंडता और सुरक्षा बनाए रखते हुए, क्लाउड-होस्टेड सेवा(ओं) और डेटा को क्लाउड से कैसे अंतरित किया जाएगा; और

(डी) सीएसपी से सभी लेन-देन संबंधी अभिलेखों, ग्राहक एवं परिचालन संबंधी जानकारी और कॉन्फ़िगरेशन डेटा को व्यवस्थित रूप से शीघ्रता से प्राप्त करने और सीएसपी स्तर पर उन्हें हटाने तथा सीएसपी से हस्ताक्षर करने से पहले स्वतंत्र आश्वासन सुनिश्चित करने के लिए खंड शामिल करें;

(xvii) यह सुनिश्चित करना कि ऑडिट / आवधिक समीक्षा / तृतीय-पक्ष प्रमाणन, प्रयोज्यता और क्लाउड उपयोग के अनुसार, अन्य बातों के साथ -साथ क्लाउड गवर्नेंस, एक्सेस और नेटवर्क नियंत्रण, कॉन्फ़िगरेशन, निगरानी तंत्र, डेटा एन्क्रिप्शन, लॉग समीक्षा, परिवर्तन प्रबंधन, घटना प्रतिक्रिया और लचीलापन तैयारी और परीक्षण में एआईएफआई और सीएसपी दोनों की भूमिकाओं और जिम्मेदारियों जैसे पहलुओं को कवर करते हैं।

एफ. आउटसोर्स की गई सेवाओं से संबंधित शिकायतों का निवारण

62. एआईएफआई के पास एक सुदृढ़ शिकायत निवारण तंत्र होना चाहिए, जिससे आउटसोर्सिंग के कारण किसी भी तरह से समझौता नहीं किया जाएगा, अर्थात आउटसोर्स की गई सेवाओं से संबंधित ग्राहकों की शिकायतों के निवारण की जिम्मेदारी एआईएफआई की होगी।

63. एआईएफआई द्वारा किए गए आउटसोर्सिंग व्यवस्था से एआईएफआई के विरुद्ध उसके ग्राहकों के अधिकारों पर कोई प्रभाव नहीं पड़ेगा, जिसमें ग्राहकों की प्रासंगिक कानूनों के तहत लागू निवारण प्राप्त करने की क्षमता भी शामिल है।

अध्याय IV – निरसन और अन्य प्रावधान

ए. निरसन और बचाव

64. इन निदेशों के जारी होने के साथ ही, एआईएफआई पर लागू आईटी सेवाओं के आउटसोर्सिंग से संबंधित मौजूदा निदेश, अनुदेश और दिशानिर्देश निरस्त हो गए हैं, जैसा कि दिनांक 28 नवंबर 2025 के परिपत्र विवि.आरआरसी.आरईसी.302/33-01-010/2025-26 के माध्यम से सूचित किया गया है। इन निदेशों के जारी होने से पहले निरस्त किए गए निदेश, अनुदेश और दिशानिर्देश निरस्त बने रहेंगे।

65. ऐसे निरसन के बावजूद, निरस्त निदेशों, अनुदेशों या दिशानिर्देशों के अंतर्गत की गई या की जाने वाली या आरंभ की गई कोई भी कार्रवाई, उनके प्रावधानों द्वारा शासित होती रहेगी। इन निरस्त सूचियों के अंतर्गत दिए गए सभी अनुमोदन या अभिस्वीकृतियाँ इन निदेशों द्वारा शासित मानी जाएँगी। इसके अलावा, इन निदेशों, अनुदेशों या दिशानिर्देशों को निरस्त करने से निम्न पर किसी भी प्रकार से प्रतिकूल प्रभाव नहीं पड़ेगा:

(1) इसके अंतर्गत अर्जित, उपार्जित या उपगत कोई भी अधिकार, दायित्व या देयता;

(2) इसके अंतर्गत किए गए किसी भी उल्लंघन के संबंध में कोई जुर्माना, जब्ती या दंड;

(3) किसी भी ऐसे अधिकार, विशेषाधिकार, दायित्व, देयता, जुर्माना, जब्ती या पूर्वोक्त दंड के संबंध में कोई जांच, विधिक कार्यवाही या उपचार; और ऐसी कोई भी जांच, विधिक कार्यवाही या उपचार शुरू किया जा सकता है, जारी रखा जा सकता है या लागू किया जा सकता है और ऐसा कोई भी जुर्माना, जब्ती या दंड लगाया जा सकता है जैसे कि इन निदेशों, अनुदेशों या दिशानिर्देशों को निरस्त नहीं किया गया हो।

बी. अन्य कानूनों के लागू होने पर रोक नहीं

66. इन निदेशों के प्रावधान वर्तमान में लागू किसी अन्य कानून, नियम, विनियम या निदेश के प्रावधानों के अतिरिक्त होंगे, न कि उनके प्रतिकूल।

सी. व्याख्याएं

67. इन निदेशों के प्रावधानों को प्रभावी बनाने के उद्देश्य से या इन निदेशों के प्रावधानों के अनुप्रयोग या व्याख्या में किसी भी कठिनाई को दूर करने के लिए, भारतीय रिज़र्व बैंक, यदि आवश्यक समझे तो, इसमें शामिल किसी भी मामले के संबंध में आवश्यक स्पष्टीकरण जारी कर सकता है और भारतीय रिज़र्व बैंक द्वारा इन निदेशों के किसी भी प्रावधान की दी गई व्याख्या अंतिम और बाध्यकारी होगी।

(सुनिल टी एस नायर)

मुख्य महाप्रबंधक