रा.आ.बैंक /नदि/डीआरएस/नीति परिपत्र सं.90/2017-18
15 जून, 2018

राष्ट्रीय आवास बैंक
NATIONAL HOUSING BANK

सभी पंजीकृत आवास वित्त कंपनियां,

महोदया/महोदय,

आ.वि.कं. हेतु सूचना प्रौद्योगिकी ढांचा

आवास वित्त कंपनी (आ.वि.कं.) क्षेत्र पिछले कुछ वर्षों में आकार और जटिलता में विकसित हुई है। चूंकि आवास वित्त उद्योग का क्षेत्र विकसित और व्यापक है, इसकी सूचना प्रौद्योगिकी / सूचना सुरक्षा (आईटी / आईएस) ढांचा, व्यापार निरंतरता योजना (बीसीपी), आपदा उद्धार (डीआर) प्रबंधन, आईटी लेखा परीक्षा आदि सर्वश्रेष्ठ प्रथाओं के लिए बेंचमार्क तैयार किया जाना चाहिए।

2. तदनुसार, आ.वि.कं. क्षेत्र के लिए आईटी ढांचे पर दिशानिर्देश, जिनसे आ.वि.कं. और उनके ग्राहकों के लिए लाभ की ओर अग्रसर प्रक्रियाओं में बचाव, सुरक्षा, दक्षता बढ़ाने की उम्मीद हैं, संलग्न किया गया है। आ.वि.कं. परिपत्र में इंगित कुछ आवश्यकताओं को लागू कर सकती है या पहले से लागू कर चुकी है। इसलिए आ.वि.कं. को परिपत्र में दी गई वर्तमान स्थिति और शर्तों के बीच एक औपचारिक अंतर का विश्लेषण और अंतर को संबोधित करने एवं दिशानिर्देशों का पालन करने के लिए समयबद्ध कार्रवाई योजना स्थापित करना अपेक्षित है।

3. प्रस्तावित आईटी ढांचे का केंद्र **आईटी अभिशासन, आईटी नीति, सूचना और साइबर सुरक्षा, आईटी परिचालन, आईएस लेखा परीक्षा, व्यापार निरंतरता योजना और आईटी सेवा आउटसोर्सिंग** पर है। दिशानिर्देशों को दो भागों में वर्गीकृत किया गया है, जो आ.वि.कं. सार्वजनिक जमा स्वीकार करने हेतु लागू हैं और जो पिछले लेखापरीक्षित तुलन-पत्र के अनुसार परिसंपत्ति आकार ₹ 100 करोड़ और उससे अधिक के साथ सार्वजनिक जमा स्वीकार नहीं करते हैं, अनुभाग-क में उपलब्ध कराए गए हैं। आ.वि.कं. के लिए दिशानिर्देश ₹ 100 करोड़ से कम संपत्ति आकार के साथ सार्वजनिक जमा को स्वीकार नहीं करते हैं, अनुभाग-ख में उपलब्ध कराए गए हैं।

4. आ.वि.कं. दिशानिर्देशों के विषय में अंतर-विश्लेषण और दिनांक 30 सितंबर, 2018 तक प्रस्तावित कार्रवाई के साथ-साथ इन दिशानिर्देशों को उनके बोर्ड के समक्ष रख सकता है।

5. अनुभाग-क में आने वाली आ.वि.कं. को दिनांक 30 जून, 2019 तक और अन्य आ.वि.कं. द्वारा दिनांक 30 सितंबर, 2019 तक दिशानिर्देशों का पालन करना होगा।

भवदीय,

(वी.वैदीश्वरण)
महाप्रबंधक
विनियमन और पर्यवेक्षण विभाग

संलग्नक: आ.वि.कं. हेतु सूचना प्रौद्योगिकी ढांचा – दिशा-निर्देश

अनुबंध

आ.वि.कं. हेतु सूचना प्रौद्योगिकी फ्रेमवर्क - दिशा-निर्देश

आवास वित्त कंपनी (आ.वि.कं.) क्षेत्र पिछले कुछ वर्षों में आकार और जटिलता में काफी विकसित हुई है। चूंकि आवास वित्त उद्योग का क्षेत्र परिपक्व और व्यापक है, इसकी सूचना प्रौद्योगिकी / सूचना सुरक्षा (आईटी / आईएस) ढांचा, व्यापार निरंतरता योजना (बीसीपी), आपदा उद्धार (डीआर) प्रबंधन, आईटी लेखा परीक्षा आदि सर्वश्रेष्ठ प्रथाओं के लिए बेंचमार्क तैयार किया जाना चाहिए।

2. तदनुसार, आ.वि.कं. क्षेत्र के लिए आईटी ढांचे पर दिशानिर्देश, जिनसे आ.वि.कं. और उनके ग्राहकों के लिए लाभ की ओर अग्रसर प्रक्रियाओं में बचाव, सुरक्षा, दक्षता बढ़ाने की उम्मीद हैं, संलग्न किया गया है। आ.वि.कं. परिपत्र में इंगित कुछ आवश्यकताओं को लागू कर सकती है या पहले से लागू कर चुकी है। इसलिए आ.वि.कं. को परिपत्र में दी गई वर्तमान स्थिति और शर्तों के बीच एक औपचारिक अंतर का विश्लेषण और अंतर को संबोधित करने एवं दिशानिर्देशों का पालन करने के लिए समयबद्ध कार्रवाई योजना स्थापित करना अपेक्षित है।

3. प्रस्तावित आईटी ढांचे का केंद्र **आईटी अभिशासन, आईटी नीति, सूचना और साइबर सुरक्षा, आईटी परिचालन, आईएस लेखा परीक्षा, व्यवसाय निरंतरता योजना और आईटी सेवा आउटसोर्सिंग** पर है। दिशानिर्देशों को दो भागों में वर्गीकृत किया गया है, जो आ.वि.कं. सार्वजनिक जमा स्वीकार करने हेतु लागू हैं और जो पिछले लेखापरीक्षित तुलन-पत्र के अनुसार परिसंपत्ति आकार ₹ 100 करोड़ और उससे अधिक के साथ सार्वजनिक जमा स्वीकार नहीं करते हैं, अनुभाग-क में प्रदान किया गया हैं। आ.वि.कं. के लिए दिशानिर्देश ₹ 100 करोड़ से कम संपत्ति आकार के साथ सार्वजनिक जमा को स्वीकार नहीं करते हैं, अनुभाग-ख में प्रदान किया गया हैं।

भाग-क

सूचना प्रौद्योगिकी (आईटी)अभिशासन

1. सूचना प्रौद्योगिकी (आईटी) अभिशासन

सूचना प्रौद्योगिकी (आईटी) अभिशासन कॉरपोरेट, अभिशासन का एक अभिन्न हिस्सा है। इसमें नेतृत्व समर्थन, संगठनात्मक संरचना और प्रक्रियाएं शामिल हैं ताकि यह सुनिश्चित किया जा सके कि आ.वि.कं. आईटी व्यापार कार्यनीतियों और उद्देश्यों को बनाए रखती है और विस्तार करती है। प्रभावी आईटी अभिशासन निदेशक मंडल और कार्यकारी प्रबंधन की ज़िम्मेदारी है।

आईटी अभिशासन को कार्यान्वित करते समय बोर्ड और वरिष्ठ प्रबंधन की स्पष्ट भूमिका और जिम्मेदारी महत्वपूर्ण हैं। स्पष्ट भूमिका प्रभावी परियोजना नियंत्रण सक्षम करती है। लोग, जब वे दूसरों की अपेक्षाओं से अवगत होते हैं, तो वह समय पर, बजट के भीतर और गुणवत्ता के अपेक्षित स्तर पर कार्य पूरा करने में सक्षम होते हैं। आईटी अभिशासन पणधारक में निम्नलिखित शामिल है: निदेशक मंडल, आईटी कार्यनीति समिति, मुख्य कार्यकारी अधिकारी, व्यवसाय कार्यपालक, मुख्य सूचना अधिकारी, मुख्य प्रौद्योगिकी अधिकारी, आईटी संचालन समिति (कार्यपालक स्तर पर परिचालन और प्राथमिकता स्वामित्व, संसाधन आवंटन और परियोजना ट्रैकिंग पर ध्यान केंद्रण), मुख्य जोखिम अधिकारी और जोखिम समिति।

मूल्य संवितरण, आईटी जोखिम प्रबंधन, आईटी संसाधन प्रबंधन और कार्य-निष्पादन प्रबंधन के बुनियादी सिद्धांतों को अभिशासन फ्रेमवर्क का आधार बनाना चाहिए। आईटी अभिशासन एक निरंतर चलने वाली प्रक्रिया है। यह एक ऐसी प्रक्रिया है जिसमें आईटी कार्यनीति उत्तरदायित्वों को निष्पादित करने हेतु आवश्यक संसाधनों का उपयोग करके प्रक्रियाओं को चलाती है। आईटी के महत्व को देखते हुए, आ.वि.कं. ऐसे विवेकपूर्ण अभिशासन मानकों के प्रासंगिक पहलुओं का पालन कर सकती है जिन्हें वित्त उद्योग में स्वीकार्यता मिली है।

1.1 आईटी कार्यनीति समिति: आ.वि.कं. को आईटी कार्यनीति समिति बनाने की आवश्यकता है। समिति का अध्यक्ष एक स्वतंत्र निदेशक होगा और मुख्य सूचना अधिकारी, मुख्य प्रौद्योगिकी अधिकारी को समिति का हिस्सा होना चाहिए। आईटी कार्यनीति समिति को उचित आवृत्ति पर मिलना चाहिए, लेकिन दो बैठकों के बीच छह महीने का अंतर नहीं होना चाहिए। समिति उन्हें इनपुट प्रदान करने के लिए अन्य बोर्ड समितियों और वरिष्ठ प्रबंधन के साथ साझेदारी में काम करेगी। यह समीक्षा भी करेगा और कॉरपोरेट कार्यनीतियों, बोर्ड नीति समीक्षा, साइबर सुरक्षा व्यवस्था और आईटी अभिशासन से संबंधित किसी भी अन्य मामले के अनुरूप आईटी कार्यनीतियों का संशोधन करेगा। इस पर विचार-विमर्श बोर्ड के समक्ष रखा जा सकता है।

1.2 आईटी कार्यनीति समिति की भूमिका और उत्तरदायित्व: भूमिकाओं और जिम्मेदारियों में निम्नलिखित शामिल हैं:

• आईटी कार्यनीति और नीति दस्तावेजों को अनुमोदित करना और यह सुनिश्चित करना कि प्रबंधन ने प्रभावी कार्यनीति योजना प्रक्रिया बना रखी है;
• यह सुनिश्चित करना कि प्रबंधन ने प्रक्रियाओं और प्रथाओं को लागू किया है जो सुनिश्चित करते हैं कि आईटी व्यवसाय को मूल्य सुपुर्दगी करती है;
• आईटी निवेश सुनिश्चित करना जो जोखिम और लाभ का संतुलन दर्शाती है और यह बजट स्वीकार्य है;
• कार्यनीतिक लक्ष्यों को प्राप्त करने के लिए आवश्यक आईटी संसाधनों को निर्धारित करने और आईटी संसाधनों के उपयोग और सोर्सिंग के लिए उच्च स्तरीय दिशा प्रदान करने हेतु प्रबंधन द्वारा उपयोग की जाने वाली विधि की निगरानी करना;
• आ.वि.कं. के विकास को बनाए रखने और आईटी जोखिमों और नियंत्रणों के एक्सपोजर के बारे में जागरूक होने के लिए आईटी निवेशों के उचित संतुलन को सुनिश्चित करना।

आईटी नीति

2. आ.वि.कं. अपने संगठन के उद्देश्यों के अनुरूप बोर्ड अनुमोदित आईटी नीति तैयार कर सकती है जिसमें निम्नलिखित शामिल है:

क) एक आईटी संगठनात्मक संरचना आ.वि.कं. द्वारा किए गए व्यावसायिक गतिविधियों के आकार, पैमाने और प्रकृति के अनुरूप है;

ख) आ.वि.कं. एक वरिष्ठ कार्यकारी अधिकारी को मुख्य सूचना अधिकारी (सीआईओ) या आईटी परिचालन के प्रभारी के रूप में नामित कर सकती है, जिसका उत्तरदायित्व **आईटी कार्यनीति, मूल्य संवितरण, जोखिम प्रबंधन और आईटी संसाधन को प्रबंधन में शामिल करके परिचालन स्तर हेतु आईटी नीति के कार्यान्वयन को सुनिश्चित करना है**;

ग) आ.वि.कं. के वरिष्ठ/मध्यम स्तर के प्रबंधन में तकनीकी क्षमता सुनिश्चित करने के लिए, आईटी प्रशिक्षण आवश्यकताओं का आवधिक मूल्यांकन तैयार किया जाना चाहिए ताकि यह सुनिश्चित हो कि पर्याप्त, सक्षम और कुशल मानव संसाधन उपलब्ध है;

घ) आ.वि.कं. जो वर्तमान में आईपीवी 6 प्लैटफार्म का उपयोग नहीं कर रही है, उन्हें समय-समय पर संशोधित 2012 में भारत सरकार द्वारा जारी राष्ट्रीय दूर-संचार नीति के अनुसार उक्त हेतु विस्थापित होना चाहिए।

सूचना एवं साइबर सुरक्षा

3. सूचना सुरक्षा

सूचना सभी आ.वि.कं. के लिए एक परिसंपत्ति है और संगठनात्मक लक्ष्यों को प्राप्त करने के लिए सूचना सुरक्षा (आईएस) इन परिसंपत्तियों की सुरक्षा को संदर्भित करता है। सूचना सुरक्षा का उद्देश्य केवल विधिसम्मत उपयोगकर्ताओं द्वारा उपयोग सुनिश्चित करके संवेदनशील जानकारी तक पहुंच नियंत्रित करना है ताकि डेटा को उचित प्राधिकार के बिना पढ़ा न जा सके। निम्नलिखित बुनियादी सिद्धांतों के साथ आ.वि.कं. के पास बोर्ड अनुमोदित सूचना सुरक्षा नीति होनी चाहिए:

क) गोपनीयता– केवल प्राधिकृत उपयोगकर्ताओं को संवेदनशील डेटा तक पहुंच सुनिश्चित करना;
ख) संपूर्णता– यह सुनिश्चित करके सूचना की यथार्थता और स्थिरता सुनिश्चित करना कि प्राधिकार देने के बिना कोई संशोधन नहीं है;
ग) उपलब्धता– यह सुनिश्चित करना कि आवश्यकता होने पर उपयोगकर्ताओं को निर्बाध डेटा उपलब्ध है;
घ) प्रामाणिकता – सूचना सुरक्षा के लिए यह सुनिश्चित करना आवश्यक है कि डेटा, लेनदेन, संचार या दस्तावेज (इलेक्ट्रॉनिक या भौतिक) प्रामाणिक है।

3.1 सूचना नीति को निम्नलिखित बुनियादी सिद्धांतों के साथ एक सूचना नीति ढांचे के लिए प्रदान करना होगा:

क) **सूचना परिसंपत्ति की पहचान और वर्गीकरण:** आ.वि.कं. परिसंपत्ति की विशिष्ट और स्पष्ट पहचान के साथ सूचना परिसंपत्ति की विस्तृत सूची अनुरक्षित रखेगी।

ख) **कार्यों का अलगाव :** सुरक्षा अधिकारी/समूह (भौतिक सुरक्षा के साथ-साथ साइबर सुरक्षा दोनों) के कर्तव्यों के कार्य को निष्पादित करता है, विशेष रूप से सूचना प्रणाली सुरक्षा और सूचना प्रौद्योगिकी विभाग के साथ जो वास्तव में कंप्यूटर सिस्टम से भिन्न होना चाहिये। सूचना सुरक्षा कार्य को कर्मचारियों की संख्या, कौशल और उपकरण के स्तर या जोखिम मूल्यांकन, सुरक्षा आर्किटेक्चर, असुरक्षितता मूल्यांकन, फोरेंसिक मूल्यांकन आदि जैसी तकनीकों के अनुसार पर्याप्त रूप से संसाधित होना चाहिए। इसके अतिरिक्त, सिस्टम प्रशासन, डेटाबेस प्रशासन और लेनदेन प्रोसेसिंग से संबंधित जिम्मेदारियों का एक स्पष्ट अलगाव होना चाहिए।

ग) **भूमिका आधारित अभिगम नियंत्रण**– जानकारी तक पहुंच स्पष्ट रूप से उपयोगकर्ता की भूमिका (सिस्टम प्रशासक, उपयोगकर्ता प्रबंधक, आवेदन मालिक आदि) पर आधारित होनी चाहिए, आ.वि.कं. किसी विशेष कार्य के लिए एक या कुछ व्यक्तियों पर निर्भरता से बचेगी। उपयोगकर्ता प्रोफाइल और अनुमतियों को अपग्रेड/बदलने के अधिकार और साथ ही प्रमुख व्यावसायिक पैरामीटर (जैसे ब्याज दरें) जिन्हें दस्तावेज किया जाना चाहिए के लिए प्राधिकरण का स्पष्ट प्रतिनिधिमंडल होना चाहिए।

घ) **वैयक्तिक सुरक्षा** - कुछ प्राधिकृत आवेदन मालिकों/उपयोगकर्ताओं को वित्तीय संस्थान की प्रक्रियाओं का परिचित ज्ञान हो सकता है और वे सिस्टम और डेटा के लिए संभावित खतरा पैदा करते हैं।

आ.वि.कं. के पास इस संबंध में उचित जांच और संतुलन की प्रक्रिया होनी चाहिए। सिस्टम प्रशासक, साइबर सुरक्षा कर्मियों, आदि जैसे को विशेषाधिकृत पहुंच के साथ कठोर पृष्ठभूमि जांच और स्क्रीनिंग के अधीन होना चाहिए।

ड.) **भौतिक सुरक्षा** – भौतिक संघटक हेतु भौतिक पहुंच और क्षति या विनाश के माध्यम से जानकारी की गोपनीयता, संपूर्णता और उपलब्धता को नुकसान पंहुचाया जा सकता है। आ.वि.कं. को सूचना सुरक्षा परिसंपत्ति की भौतिक सुरक्षा के लिए एक सुरक्षित वातावरण बनाने की आवश्यकता है जैसे महत्वपूर्ण डेटा के सुरक्षित स्थान, संवेदनशील क्षेत्रों जैसे डेटा केंद्र आदि तक सीमित पहुंच आदि।

च) मेकर- चेकर वित्तीय संस्थाओं की सूचना प्रणाली में प्राधिकार के प्रमुख सिद्धांतों में से एक है। प्रत्येक लेन-देन के लिए इसके पूरा होने हेतु कम से कम दो व्यक्तियों को जरूर होना चाहिए क्योंकि इससे त्रुटि का खतरा कम हो जाएगा और सूचना की स्थिरता सुनिश्चित होगी।

छ) आकस्मिक प्रबंधन - सूचना सुरक्षा नीति को परिभाषित करना चाहिए कि किसी घटना का गठन क्या होता है। आ.वि.कं. सूचना सुरक्षा घटनाओं को रोकने, पता लगाने, विश्लेषण करने और जवाब देने के लिए प्रक्रियाओं को विकसित और कार्यान्वित करेगी।

ज) चिह्न - आ.वि.कं. यह सुनिश्चित करेगी कि लेखा परीक्षा सत्यापन परिसंपत्तियों के लिए विनियामक और विधिक आवश्यकताओं, लेखा परीक्षा को सुविधाजनक बनाने, आवश्यक होने पर फोरेंसिक साक्ष्य के रूप में कार्य करने और विवाद समाधान में सहायता करने सहित अपनी व्यावसायिक आवश्यकताओं को संतुष्ट करने के लिए मौजूद है। उदाहरण के लिए, यदि एक कर्मचारी, एक अनधिकृत अनुभाग तक पहुंचने का प्रयास करता है, तो यह अनुचित गतिविधि लेखा परीक्षा सत्यापन में दर्ज की जानी चाहिए।

झ) पब्लिक की इंफ्रास्ट्रक्चर (पीकेआई) – आ.वि.कं. डेटा, नियंत्रण पंहुच, डेटा स्थिरता, अधिप्रमाणन और अपरित्याग की गोपनीयता सुनिश्चित करने के लिए पीकेआई के उपयोग में वृद्धि कर सकती है।

3.2 साइबर सुरक्षा

बोर्ड द्वारा अनुमोदित साइबर सुरक्षा नीति की आवश्यकता

आ.वि.कं. को अपने बोर्ड द्वारा विधिवत अनुमोदित स्वीकृत स्तरों और व्यवसाय की जटिलता का स्तर देखकर साइबर हमलों का सामना करने हेतु उचित संपर्क सहित कार्यनीति को सपष्ट करके साइबर सुरक्षा नीति स्थापित करनी होगा। आ.वि.कं. को संगठनात्मक व्यवस्था की समीक्षा करनी होगी ताकि सुरक्षा संस्था को सराहा जाए, पर्याप्त सावधानी बरती जाए और जल्द कार्रवाई करने हेतु पर-क्रम में उचित स्तर के लिए बढ़ावा मिले।

3.3 असुरक्षितता प्रबंधन

असुरक्षितता को संगठन के सूचना प्रौद्योगिकी बेस के मूलभूत विन्यास में कमी के रूप में परिभाषित किया जा सकता है, यद्यपि वह हार्डवेयर अथवा सॉफ्टवेयर स्तर की हो जो कि किसी तृतीय पक्ष द्वारा संगठन की संवेदनशील सूचनाओं को हासिल करने हेतु प्रेरित की जा सकती है। असुरक्षितता प्रबंधन असुरक्षितता को कम या खत्म करने की प्रक्रिया को निर्धारित करने की एक निरंतर प्रक्रिया है जो असुरक्षितता के साथ जुड़ी लागत और जोखिम पर आधारित है। आ.वि.कं. असुरक्षितता का प्रबंध और खत्म करने हेतु कार्यनीति तैयार कर सकती है और ऐसी कार्यनीति साइबर सुरक्षा नीति में स्पष्ट रूप से देखी जा सकती है।

3.4 साइबर सुरक्षा तत्परता संकेतक

साइबर आघात-सहनीयता फ्रेमवर्क की पर्याप्तता और अनुपालन का मूल्यांकन किया जाना चाहिए और जोखिम/ तत्परता के स्तर का आकलन करने के लिए संकेतकों के विकास के माध्यम से मापा जाना चाहिए। इन संकेतकों का उपयोग स्वतंत्र अनुपालन जांच और योग्य और सक्षम पेशेवरों द्वारा किए गए लेखापरीक्षा के माध्यम से व्यापक टेस्टिंग के लिए किया जाना चाहिए। कर्मचारियों सहित पणधारकों के बीच जागरूकता भी इस मूल्यांकन का एक हिस्सा बन सकती है।

3.5 साइबर संकट प्रबंधन योजना

साइबर हमला प्रबंधन योजना (सीसीएमपी) तुरंत विकसित किया जाना चाहिए और समग्र बोर्ड अनुमोदित कार्यनीति का हिस्सा होना चाहिए। सीसीएमपी को निम्नलिखित चार पहलुओं को संबोधित करना चाहिए: (i) पता लगाना (ii) प्रतिक्रिया (iii) उद्धार और (iv) नियंत्रण। आ.वि.कं. को साइबर हमले रोकने और तत्काल किसी भी साइबर-घुसपैठ का पता लगाने के लिए प्रभावी उपाय करने की आवश्यकता है ताकि प्रतिक्रिया/उद्धार/ गिरावट शामिल हो सके। आ.वि.कं. से 'ज़ीरो-डे' हमलों, दूरस्थ खतरों और लक्षित हमलों जैसे उभरते साइबर-खतरों का सामना करने के लिए तैयार होने की अपेक्षा है। अन्य चीजों के अलावा, आ.वि.कं. को विभिन्न प्रकार के साइबर खतरों को संबोधित करने में आवश्यक निवारक और सुधारात्मक उपायों को अपनाना चाहिए, लेकिन सिमित नहीं बल्कि सेवा की मनाही, सेवाओं के संवितरण से मनाही (डीडीओएस), रेंसम-वेयर/क्रिप्टो वेयर, घातक मॉलवेयर, व्यवसाय ईमेल धोखाधड़ी में स्पैम, ईमेल फ़िशिंग, स्पेअर फ़िशिंग, व्हेलिंग, विशिंग धोखाधड़ी, ड्राइव बाय डाउनलोड, ब्राउज़र गेटवे, घोस्ट एडमिनिस्ट्रेटर उल्लंघन, पहचान धोखाधड़ी, मेमोरी अपडेट धोखाधड़ी, पासवर्ड से संबंधित धोखाधड़ी आदि शामिल हैं।

3.6 साइबर सुरक्षा पर जानकारी की रिपोर्टिंग

आ.वि.कं. अपनी आईटी संचालन समिति और जोखिम प्रबंधन समिति को सभी प्रकार की असामान्य सुरक्षा घटनाओं की रिपोर्ट करने हेतु एक उचित प्रक्रिया स्थापित करेगा।

आ.वि.कं. की आईटी प्रणाली जैसे आकड़े उल्लंघन, आकड़े विनाश इत्यादि से समझौता करने वाली घटनाएं, कंपनी के परिचालन को गंभीर रूप से प्रभावित करती हैं, कंपनी दो कार्य दिनों के भीतर आ.वि.कं. द्वारा की गई कार्रवाई रा.आ.बैंक को रिपोर्ट करेगी।

3.7 पणधारकों / शीर्ष प्रबंधन / बोर्ड के बीच साइबर सुरक्षा जागरूकता

यह विचार किया जाना चाहिए कि साइबर जोखिम प्रबंधन हेतु संपूर्ण संगठन प्रतिबद्धता की आवश्यकता है ताकि साइबर-सुरक्षित वातावरण बनाया जा सके। इसके लिए सभी स्तरों के कर्मचारियों के बीच उच्च स्तर की जागरूकता अपेक्षित होगी। शीर्ष प्रबंधन और बोर्ड को भी खतरों की महीन बारीकियों के बारे में जागरूकता की उचित स्तर की जागरुकता होनी चाहिए और उपयुक्त परिचितता का आयोजन किया जा सकता है। आ.वि.कं. को अपने ग्राहकों, विक्रेताओं, सेवा प्रदाताओं और अन्य प्रासंगिक हितधारकों के बीच अपने साइबर आघात-सहनीयता उद्देश्यों की समझ को सक्रिय रूप से बढ़ावा देना चाहिए, और उनके एक समय पर होने वाले कई कार्यो के कार्यान्वयन और परीक्षण का समर्थन करने के लिए उचित कार्रवाई और सुनिश्चित करना आवश्यकता है।

3.8 डिजीटल हस्ताक्षर

डिजिटल हस्ताक्षर प्रमाणपत्र इलेक्ट्रॉनिक रूप से संस्था की पहचान प्रमाणित करता है। डिजिटल हस्ताक्षर प्रमाणपत्र का उपयोग करके आदान-प्रदान की गई जानकारी की पूर्ण गोपनीयता सुनिश्चित करके यह ऑनलाइन लेनदेन के लिए उच्च स्तर की सुरक्षा भी प्रदान करता है। आ.वि.कं. महत्वपूर्ण इलेक्ट्रॉनिक दस्तावेजों की प्रामाणिकता और अखंडता की रक्षा के लिए और उच्च मूल्य निधि हस्तांतरण के लिए भी डिजिटल हस्ताक्षरों का उपयोग करने का विचार कर सकता हैं।

3.9 आईटी जोखिम मूल्याकंन

आ.वि.कं. को कम से कम एक साल के आधार पर अपने आईटी प्रणाली का व्यापक जोखिम मूल्यांकन करना चाहिए। आ.वि.कं. को सूचना प्रौद्योगिकी आस्तियों हेतु खतरों और असुरक्षितता और आ.वि.कं. के मौजूदा सुरक्षा नियंत्रण और प्रक्रियाओं के मूल्यांकन पर विश्लेषण करना चाहिए। प्रयोग का नतीजा जोखिमों के उचित न्यूनीकरण हेतु जरूरी जोखिमों का पता लगाने और उचित स्तर के नियंत्रण निर्धारित करने हेतु होना चाहिए। जोखिम मूल्यांकन मुख्य जोखिम अधिकारी (सीआरओ), सीआईओ और आ.वि.कं. बोर्ड के नोटिस में लाया जाना चाहिए और सूचना सुरक्षा लेखापरीक्षकों हेतु एक इनपुट के रूप में प्रदान करना चाहिए।

3.10 मोबाइल वित्तीय सेवाएं

आ.वि.कं. जो पहले से ही मोबाइल वित्तीय सेवाओं का उपयोग कर रही हैं, उन्हें सूचना संपत्तियों की सुरक्षा के लिए एक तंत्र विकसित करना चाहिए जो मोबाइल सेवाओं के उपयोग द्वारा ग्राहकों को सेवाएं प्रदान करें। मोबाइल सेवाओं के लिए उपयोग की जाने वाली तकनीक की गोपनीयता, अखंडता, प्रामाणिकता सुनिश्चित करनी चाहिए और एंड टू एंड एन्क्रिप्शन प्रदान करना चाहिए।

3.11 सोशल मीडिया जोखिम

आ.वि.कं. को सोशल मीडिया का उपयोग करके अपने उत्पादों को बेचने के लिए सोशल मीडिया के जोखिम और खतरों को संभालने में अच्छी तरह से सुसज्जित होना चाहिए। चूंकि सोशल मीडिया खाता अधिग्रहण और मॉलवेयर वितरण, उचित नियंत्रण, जैसे एन्क्रिप्शन और सुरक्षित संबंध के लिए कमजोर है, इसलिए ऐसे जोखिमों को कम करने हेतु प्रचलित होना चाहिए।

3.12 प्रशिक्षण

सूचना सुरक्षा श्रृंखला में मानव लिंक सबसे कमजोर लिंक है। इसलिए, प्रारंभिक और चल रहे प्रशिक्षण और सूचना सुरक्षा जागरूकता कार्यक्रम हेतु अतिआवश्यक है। सूचना प्रौद्योगिकी प्रणाली, खतरों / भेद्यता और/या सूचना सुरक्षा ढांचे में परिवर्तनों को ध्यान में रखते हुए कार्यक्रम को समय-समय पर अपडेट किया जा सकता है। आकलन / परीक्षण प्रक्रिया के माध्यम से प्रशिक्षण कार्यक्रमों की प्रभावशीलता की स्थिति का पता करने हेतु एक प्रणाली का होना आवश्यक है। किसी भी समय, आ.वि.कं. को सूचना सुरक्षा से संबंधित उपयोगकर्ता प्रशिक्षण और जागरूकता पर अद्यतन स्थिति बनाए रखने की आवश्यकता होती है।

आईटी परिचालन

4. आईटी परिचालन को सूचना की प्रोसेसिंग और संचयन का समर्थन करना चाहिए, ताकि अपेक्षित सूचना समय पर, विश्वसनीय, सुरक्षित और आसानी से उपलब्ध हो। बोर्ड या वरिष्ठ प्रबंधन को मौजूदा और

योजनाबद्ध आईटी परिचालनों और जोखिम सहनशीलता से जुड़े जोखिम को ध्यान में रखना चाहिए और फिर जोखिम प्रबंधन हेतु नीतियों की स्थापना और निगरानी करनी चाहिए।

4.1 सूचना प्रणाली का अधिग्रहण और विकास (नया आवेदन सॉफ्टवेयर) और परिवर्तन प्रबंधन

आईटी परियोजनाओं को लागू करते समय यह अनुभव रहा है कि खराब प्रणाली डिज़ाइन और कार्यान्वयन, के साथ-साथ अपर्याप्त परीक्षण के कारण कई प्रणाली विफल हो जाती हैं। आ.वि.कं. को प्रणाली डिज़ाइन, विकास और परीक्षण चरणों में प्रणाली कमियों और दोषों की पहचान करनी चाहिए।

आ.वि.कं. को परियोजना के प्रत्येक चरण में प्राप्त होने वाले डिलिवरेबल्स सहित और परियोजना सारणी के अनुसार उपलब्धियों तक पहुंचने के लिए परियोजना की प्रगति को अन्वेक्षण और निगरानी प्रदान करने हेतु व्यापार स्वामी, विकास दल और अन्य पणधारकों से मिलकर एक संचालन समिति स्थापित करनी चाहिए।

4.2 आ.वि.कं. को अपने ग्राहकों और व्यापार की बदलती जरूरतों के अनुरूप नियमित रूप से अपनी आईटी प्रणाली को बदलने की आवश्यकता होती है। परिवर्तनों को इस तरह करने की आवश्यकता है कि ग्राहकों के लिए मूल्य को अधिकतम करते समय प्रतिकूल घटनाओं और सेवाओं में व्यवधान को कम किया जा सके। इस उद्देश्य हेतु, आ.वि.कं. को अपने बोर्ड की संस्वीकृति के साथ विकसित होना चाहिए, एक परिवर्तन प्रबंधन नीति जिसमें निम्न शामिल हैं:

क. व्यवसाय से प्रस्तावों को बदलने हेतु प्राथमिकता और जवाब देना,
ख. प्रस्तावित परिवर्तनों का लागत लाभ विश्लेषण,
ग. प्रस्तावित परिवर्तनों से जुड़े जोखिमों का आकलन,
घ. कार्यान्वयन, निगरानी और रिपोर्टिंग बदलें।

परिवर्तन प्रबंधन नीति का निरंतर आधार पर पालन किया जा रहा है, यह सुनिश्चित करने हेतु वरिष्ठ प्रबंधन की जिम्मेदारी होनी चाहिए।

4.3 आईटी समर्थित प्रबंधन सूचना प्रणाली

आ.वि.कं. के आईटी कार्य को व्यवसाय की ज़रूरतों के अनुसार विभिन्न व्यावसायिक कार्यों के संबंध में एक सुदृढ़ और व्यापक प्रबंधन सूचना प्रणाली (एमआईएस) का समर्थन करना चाहिए। एक अच्छी प्रबंधन सूचना प्रणाली (एमआईएस) को शीर्ष प्रबंधन सहित व्यापार के सभी स्तरों पर सूचना आवश्यकताओं का ख्याल रखना चाहिए।

4.4 आ.वि.कं. प्रबंधन सूचना प्रणाली का स्थान ले सकता है जो निर्णय लेने में शीर्ष प्रबंधन के साथ-साथ व्यापार प्रमुखों की सहायता करता है और विभिन्न व्यावसायिक विषमस्तरीय के संचालन पर भी निगरानी बनाए रखता है। सुदृढ़ आईटी सिस्टम के साथ, आ.वि.कं. के पास एमआईएस (संकेत सूची) बनाने हेतु एक प्रभावी प्रणाली के रूप में निम्नलिखित हो सकते है:

क. शीर्ष प्रबंधन हेतु लक्ष्य के सामने वित्तीय स्थिति संक्षिप्त में प्रस्तुत करने हेतु एक डैशबोर्ड की स्थापना की गई है। इसमें सभी श्रेणियों में परिसंपत्ति, प्रमुख विकास व्यापार क्षेत्र, निवल मालियत की गतिविधि इत्यादि पर विवरणी पर प्रवृत्ति पर सूचना शामिल हो सकती है।
ख. एनपीए की प्रणाली सक्षम पहचान और वर्गीकरण के साथ-साथ इस संबंध में एमआईएस रिपोर्टों का निर्माण।

ग. एमआईएस को उत्पादों की कीमत, विशेषत: बड़े जमा ऋण की सुविधा प्रदान करना चाहिए।
घ. एमआईएस को विनियामक आवश्यकताओं और उनके अनुपालन को ग्रहण करना चाहिए।
ङ. परिचालन और गैर-परिचालन राजस्व और व्यय, क्षेत्र/ विषमस्तरीय के लागत लाभ विश्लेषण, निधियों की लागत इत्यादि (लेनदेन स्तर पर विनियामक अनुपालन) सहित वित्तीय रिपोर्ट
च. ट्रेजरी परिचालन से संबंधित रिपोर्ट।
छ. धोखाधड़ी विश्लेषण- संदिग्ध लेनदेन विश्लेषण, गबन, चोरी या संदिग्ध धन-शोधन, परिसंपत्तियों का दुरुपयोग, वित्तीय रिकोर्ड में हेरफेर इत्यादि। रिपोर्टिंग धोखाधड़ी, यदि कोई हो, की विनियामक आवश्यकता प्रणाली चालित होनी चाहिए।
ज. आईटी सुरक्षा प्रणालियों की क्षमता और प्रदर्शन विश्लेषण
झ. घटना रिपोर्टिंग, भविष्य में ऐसी घटनाओं के गैर-समर्पण हेतु उनके प्रभाव और कदम उठाए गए।

4.5 पर्यवेक्षी आवश्यकताओं हेतु एमआईएस - एमआईएस जो कार्यनीतिक निर्णय लेने में प्रबंधन की मदद करेगा और पर्यवेक्षी हेतु अपेक्षित सूचना/ रिपोर्टिंग बनाने में भी सहायता करेगा। एमआईएस डिजाइन करते समय रिपोर्टिंग प्रणाली (पर्यवेक्षी हेतु) की वर्तमान संरचना को ध्यान में रखा जाना चाहिए। सभी विनियामक/ पर्यवेक्षी विवरणी ओआरएमआईएस/ विनियामक रिपोर्टिंग के तहत रिपोर्टिंग के प्रतिकूल प्रणाली चालित होनी चाहिए। इसके अतिरिक्त, यह आवश्यक है कि रा.आ.बैंक निरीक्षक या इसके द्वारा प्राधिकृत व्यक्तियों को "केवल पढ़ने" की पहुंच प्रदान की जाए।

आईएस लेखापरीक्षा

5. सूचना प्रणाली लेखापरीक्षा (आईएस लेखापरीक्षा) हेतु नीति

आईएस लेखापरीक्षा का उद्देश्य संगठन के आईटी बुनियादी संरचना की गोपनीयता, अखंडता और उपलब्धता सुनिश्चित करने हेतु नियंत्रण की प्रभावशीलता पर अंतर्दृष्टि प्रदान करना है। आईएस लेखा परीक्षा आईटी बुनियादी संरचना जैसे सर्वर संरचना, स्थानीय और विस्तृत क्षेत्र नेटवर्क, भौतिक और सूचना सुरक्षा, दूरसंचार इत्यादि से उत्पन्न होने वाले जोखिम को कम करने हेतु जोखिम और विधियों की पहचान करेगी।

5.1 आईएस लेखापरीक्षा आ.वि.कं. की आंतरिक लेखापरीक्षा प्रणाली का एक अभिन्न हिस्सा होनी चाहिए। आईएस ढांचे को डिजाइन करते समय, आ.वि.कं. इस संबंध में आईएसएसीए, आईआईए, आईसीएआई जैसे व्यवासायिक निकायों द्वारा जारी दिशा निर्देश का उल्लेख करेंगी। आईसीएआई ने विषय पर " आंतरिक लेखापरीक्षा (एसआईए) 14 पर मानक: सूचना प्रौद्योगिकी पर्यावरण में आंतरिक लेखापरीक्षा" प्रकाशित किया है। आ.वि.कं. अपने बोर्ड द्वारा अनुमोदित एक आईएस लेखापरीक्षा ढांचे को अपनाएगी। इसके अतिरिक्त, आ.वि.कं. के लेखापरीक्षा समिति में पर्याप्त कुशल कार्मिक होगें जो आईएस लेखापरीक्षा के परिणामों को समझ सकते हैं।

5.2 कवरेज: आईएस लेखापरीक्षा को आईटी प्रणाली की नीति और अन्वेक्षण की प्रभावशीलता, प्रक्रियाओं और आंतरिक नियंत्रणों की पर्याप्तता का मूल्यांकन, संबोधित विसंगतियों और अनुवर्ती हेतु सुधारात्मक कार्रवाई की सिफारिश को कवर करना चाहिए। आईएस लेखापरीक्षा को व्यापार निरंतरता योजना, आपदा वसूली रखने की प्रभावशीलता का मूल्यांकन करना चाहिए और यह सुनिश्चित करना चाहिए कि संगठन में बीसीपी प्रभावी रूप से लागू हो। आईएस लेखापरीक्षा की प्रक्रिया के दौरान, सभी लागू कानून और सांविधिक आवश्यकताओं के अनुपालन हेतु यथोचित महत्व दिया जाएगा।

5.3 कार्मिक – आईएस लेखापरीक्षा आ.वि.कं. की एक आंतरिक टीम द्वारा आयोजित किया जा सकता है। अपर्याप्त आंतरिक कौशल के मामले में, आ.वि.कं. एक बाहरी एजेंसी नियुक्त कर सकता हैं बशर्ते बाहरी

लेखापरीक्षक/ एजेंसी को सीईआरटी-इन के साथ पैनल में हो। इन मानकों के मुकाबले ढांचे की प्रभावकारिता का आकलन करने हेतु कानूनी और विनियामक आवश्यकताओं के कौशल और समझ का सही मिश्रण होना चाहिए। आईएस लेखापरीक्षकों को आ.वि.कं. प्रबंधन के व्यवहार और उपस्थिति दोनों में स्वतंत्र रूप से कार्य करना चाहिए। बाह्य व्यवसायिक सेवा प्रदाताओं की भागीदारी के मामले में, आजादी और जवाबदेही के मुद्दों को ठीक से संबोधित किया जा सकता है।

5.4 आवधिकता - आईएस लेखापरीक्षा की आवधिकता आदर्श रूप से आ.वि.कं. के आकार और परिचालन पर आधारित होनी चाहिए लेकिन दो वर्षों में कम से कम एक बार आयोजित की जा सकती है। सांविधिक लेखा परीक्षा से पहले प्राथमिकता से सूचना सुरक्षा लेखापरीक्षा की जानी चाहिए ताकि सांविधिक लेखापरीक्षकों को जांच एवं यदि कोई टिप्पणियां हो तो उन्हें लेखा परीक्षा रिपोर्ट में शामिल करने के लिए सूचना सुरक्षा लेखापरीक्षा रिपोर्ट समय पर उपलब्ध हो सके।

5.5 सूचना सुरक्षा लेखापरीक्षकों का रोटेशन- सूचना सुरक्षा लेखापरीक्षकों का रोटेशन इस तरीके से किया जाना चाहिए कि यदि दो वर्षों में एक बार लेखा परीक्षा की जाती है तो दो से ज्यादा लगातार अवधि के लिए या यदि वर्ष में एक बार लेखा परीक्षा की जाती है तो तीन लगातार अवधि के लिए लेखा परीक्षक लेखापरीक्षा न करें।

5.6 रिपोर्टिंग –बोर्ड या बोर्ड की समिति यानी बोर्ड की लेखा परीक्षा समिति के समक्ष फ्रेमवर्क में स्पष्ट रूप से रिपोर्टिंग फ्रेमवर्क निर्धारित किया जाना चाहिए।

5.7 अनुपालन–आ.वि.कं. प्रबंधन सूचना सुरक्षा लेखा परीक्षा के दौरान रिपोर्ट की गई टिप्पणियों एवं संस्तुतियों के प्रत्युत्तर में की जाने वाली उपयुक्त कार्रवाई पर निर्णय लेने के लिए जिम्मेदार है। फ्रेमवर्क में स्पष्ट से रूप अनुपालन/अनुपालन की पुष्टि, रिपोर्टिंग लाइन, अनुपालन प्रस्तुतीकरण की समयसीमा, अनुपालन स्वीकार करने के लिए प्राधिकरण वर्णित होने चाहिए। फ्रेमवर्क लेखा परीक्षकों/ निरीक्षण/ विनियामक प्राधिकरणों के लिए लेखा परीक्षा-प्रणाली की पहुंच प्रदान करें।

5.8 कंप्यूटरीकृत लेखा-परीक्षा तकनीक (सीएएटी): आ.वि.कं. सूचना सुरक्षा लेखापरीक्षा के लिए मैनुअल तकनीकों एवं कंप्यूटरीकृत लेखा-परीक्षा तकनीकों का एक उचित मिश्रण अपनाएंगे। कंप्यूटरीकृत लेखा-परीक्षा तकनीकों का उपयोग महत्वपूर्ण क्षेत्रों (जैसे राजस्व क्षरण का पता लगाना, ट्रेज़री कार्य, नियंत्रण कमजोरियों के प्रभाव का मूल्यांकन, एएमएल अपेक्षाओं के तहत ग्राहक लेनदेन की निगरानी तथा सामान्यत: उन क्षेत्रों में जहां बड़े पैमाने पर लेनदेन किए जाए) विशेषकर महत्वपूर्ण कार्यों या वित्तीय/विनियामक/विधिक परिणाम की प्रक्रियाओं के लिए किया जा सकता है।

व्यवसाय निरंतरता योजना

6. व्यवसाय निरंतरता योजना (बीसीपी) तथा आपदा उद्धार (डीआर)

व्यवसाय निरंतरता योजना एक संगठन के संपूर्ण व्यवसाय निरंतरता प्रबंधन योजना का एक महत्वपूर्ण भाग है, जिसमें महत्वपूर्ण व्यवसाय प्रक्रियाओं की रिकवरी, पुनरारंभ तथा निरंतरता को सुनिश्चित करने के लिए नीतियां, मानक एवं प्रक्रियाएं शामिल हैं। आपदा से उत्पन्न परिचालन, वित्तीय, विधिक, प्रतिष्ठा संबंधी एवं अन्य सामग्री परिणामों को कम करने के लिए व्यवसाय निरंतरता योजना को बनाया जाएगा। आ.वि.कं. को बोर्ड अनुमोदित व्यवसाय निरंतरता योजना नीति अपनानी चाहिए। बोर्ड द्वारा आवधिक रिपोर्ट के जरिए व्यवसाय निरंतरता योजना के कार्यों की निगरानी की जाएगी। मुख्य सूचना अधिकारी निरंतर प्रभावशीलता

को सुनिश्चित करने के लिए व्यवसाय निरंतरता योजना को बनाने, समीक्षा एवं निगरानी के लिए जिम्मेदार होगा। व्यवसाय निरंतरता योजना में निम्नलिखित मुख्य विशेषताएं हैं:

6.1 व्यवसाय प्रभाव विश्लेषण- आ.वि.कं. विस्तृत व्यवसाय प्रभाव विश्लेषण के साथ आगे बढ़ने के लिए पहले महत्वपूर्ण व्यवसाय उपांग, स्थान एवं साझा संसाधनों का पता लगाएंगे। प्रक्रिया में आ.वि.कं. के व्यवसाय पर किसी आकस्मिक प्राकृतिक या मानव-निर्मित आपदाओं के प्रभाव पर विचार किया जाएगा। संस्था प्राथमिकता से व्यवसाय प्रभाव क्षेत्रों की सूची बनाएगी।

6.2 रिकवरी कार्यनीति / आकस्मिक योजना- आ.वि.कं. विभिन्न प्रणालियों, विभागों एवं व्यवसाय प्रक्रियाओं के बीच परस्पर संबंधों से जुड़ी असुरक्षिततता को समझने की पूरी कोशिश करेंगी। व्यवसाय निरंतरता योजना विभिन्न असफल परिदृश्यों की संभावनाओं के साथ आगे बढ़नी चाहिए। आपदा की स्थिति में नुकसान कम करने के लिए सबसे किफायती, व्यावहारिक कार्यनीति का चयन किया जाना चाहिए और रिकवरी के लिए विभिन्न विकल्पों का मूल्यांकन किया जाना चाहिए।

6.3 आ.वि.कं. अपने महत्वपूर्ण व्यवसाय प्रणालियों एवं डेटा सेंटर के लिए आवश्यक बैकअप साइट रखने की आवश्यकता पर विचार करेंगी।

6.4 आ.वि.कं. यह निर्धारित करने के लिए कि यदि संस्था आकस्मिक योजना में निर्दिष्ट समयसीमा के भीतर व्यवसाय के स्वीकार्य स्तर से रिकवर हो सकती है, प्रतिवर्ष अथवा महत्वपूर्ण आईटी या व्यवसाय बदलाव होने पर व्यवसाय निरंतरता योजना की जांच करेंगी यह जांच 'सबसे खराब मामले के परिदृश्य' पर आधारित होनी चाहिए। परिणाम के साथ अंतर विश्लेषण को मुख्य सूचना अधिकारी एवं बोर्ड के समक्ष प्रस्तुत किया जा सकता है। अंतर विश्लेषण के साथ बोर्ड के विचार अद्यतीत व्यवसाय निरंतरता योजना के निर्माण का आधार होने चाहिए।

आईटी सेवाओं की आउटसोर्सिंग

7. आईटी सेवाओं की आउटसोर्सिंग हेतु नीति

आईटी संबंधित व्यवसाय प्रक्रिया की आउटसोर्सिंग एक आ.वि.कं. को मूल्यवान कार्यनीतिक एवं आर्थिक लाभ प्राप्त करने का अवसर प्रदान कर सकती है। हालांकि, कोई आउटसोर्सिंग प्रक्रिया शुरू करने से पहले, जोखिम पर सावधानीपूर्वक विचार, संविदात्मक व्यवस्था के खतरे तथा विनियामक अनुपालन दायित्व होना आवश्यक है। उच्च दक्षता, अपर्याप्त संसाधन और विशेष ज्ञान की कमी के कारण आमतौर पर कंपनियां तृतीय पक्ष वेंडर से अपनी आईटी संबंधित व्यवसाय प्रक्रिया को आउटसोर्स करती हैं। आ.वि.कं. का आईटी सेवाओं को आउटसोर्स का निर्णय संस्थान की संपूर्ण कार्यनीतिक योजना एवं कॉरपोरेट उद्देश्यों के लिए उपयुक्त होना चाहिए।

7.1 आ.वि.कं. और आउटसोर्सिंग सेवा प्रदाता के बीच संविदा का संचालन करने वाले नियम एवं शर्तों को सावधानीपूर्वक लिखित करार में परिभाषित किया जाना चाहिए और उसे आ.वि.कं. के कानूनी सलाहकार द्वारा अपने विधिक प्रभाव एवं प्रवर्तनीयता पर उसका निरीक्षण किया जाना चाहिए। संविदात्मक करार में निम्नलिखित प्रावधान हो सकते हैं:

क) **निगरानी एवं निरीक्षण:** आ.वि.कं. द्वारा सेवा प्रदाता की निरंतर निगरानी एवं मूल्यांकन करना ताकि यथाशीघ्र कोई भी आवश्यक सुधारात्मक उपाय किया जा सके। आउटसोर्सिंग सेवा प्रदाता के पास आउटसोर्स किए गए डेटा/एप्लिकेशन की सुरक्षा सुनिश्चित करने के लिए पर्याप्त प्रणाली एवं प्रक्रिया होनी चाहिए।

ख) **बुक एवं रिकॉर्ड तक पहुंच/ लेखा परीक्षण एवं निरीक्षण** : इसमें निम्नलिखित शामिल होंगे:

i. सुनिश्चित करे कि आ.वि.कं. के पास सेवा प्रदाता के पास उपलब्ध आउटसोर्स गतिविधियों से संबंधित सभी बुक, रिकॉर्ड एवं जानकारी तक पहुंच का अधिकार हो। तकनीकी आउटसोर्सिंग के लिए, अपेक्षित लेखा परीक्षा ट्रेल तथा प्रशासनिक गतिविधियों हेतु लॉग हो तथा अनुमोदित अनुरोध के आधार पर आ.वि.कं. की पहुंच में हो।

ii. आ.वि.कं को सेवा प्रदाता पर आंतरिक अथवा बाहरी लेखा परीक्षकों द्वारा या उसके पक्ष में कार्य करने के लिए नियुक्त बाहरी विशेषज्ञों द्वारा लेखा परीक्षा करने तथा आ.वि.कं. के लिए की गई सेवाओं के सहयोग में सेवा प्रदाता पर लिए गए निर्णयों तथा किसी लेखा परीक्षा या समीक्षा रिपोर्ट की प्रतियां प्राप्त करने का अधिकार प्रदान करना।

iii. संविदात्मक करार में उचित समय के भीतर **राष्ट्रीय आवास बैंक या उसके द्वारा प्राधिकृत व्यक्तियों को आ.वि.कं. के दस्तोवेज़ों,** लेनदेन के रिकॉर्ड, तथा सेवा प्रदाता द्वारा दी गई, परिवर्तित या इकट्ठा की गई अन्य आवश्यक जानकारी **तक पहुंच** की अनुमति देने के लिए खंड शामिल करें। इसमें कागज़ या इलेक्ट्रॉनिक प्रारूप में अनुरक्षित जानकारी शामिल हैं।

7.2 अंतत: बोर्ड एवं वरिष्ठ प्रबंधन 'आउटसोर्सिंग परिचालन' एवं ऐसे आउटसोर्सिंग संबंधों में शामिल जोखिमों के प्रबंधन के लिए जिम्मेदार है। आ.वि.कं. के निदेशक मंडल सभी आउटसोर्सिंग निर्णयों के लिए जवादेही तथा आउटसोर्सिंग के प्रबंधन एवं निगरानी तथा प्रभावी समुचित सावधानी के लिए जिम्मेदार है। बोर्ड और सभी आईटी आउटसोर्स परिचालनों के लिए जोखिम प्रबंधन प्रक्रिया एवं प्रभावी शासन प्रणाली स्थापित करना आईटी कार्यनीति समिति की जिम्मेदारी है।

7.3 आउटसोर्स परिचालनों के संबंध में आईटी कार्यनीति समिति की भूमिका में निम्नलिखित शामिल हैं:

क) आउटसोर्स प्रक्रियाओं हेतु जोखिम आधारित नीति एवं प्रक्रिया युक्त उपयुक्त शासन प्रणाली स्थापित करना ताकि शुरू से अंत तक आउटसोर्स से जुड़े जोखिमों की प्रभावी रूप से पहचान, उपाय, निगरानी एवं नियंत्रण किया जा सके;

ख) आउटसोर्सिंग के जोखिम और भौतिकता की प्रकृति के आधार पर आउटसोर्सिंग के लिए अनुमोदन प्राधिकरण निर्दिष्ट करना;

ग) आउटसोर्सिंग व्यवस्था की प्रकृति, क्षेत्र और जटिलता के अनुरूप बेहतर और उत्तरदायी आउटसोर्सिंग जोखिम प्रबंधन नीतियों और प्रक्रियाओं का विकास करना;

घ) आउटसोर्सिंग कार्यनीतियों और सभी मौजूदा सामग्री आउटसोर्सिंग व्यवस्था की आवधिक समीक्षा करना;

ङ) बोर्ड द्वारा बनाए गए फ्रेमवर्क के आधार पर सभी संभावित आउटसोर्सिंग के जोखिम और भौतिकता का मूल्यांकन करना;

च) आवधिक तौर पर नीतियों और प्रक्रियाओं की प्रभावशीलता की समीक्षा करना;

छ) आवधिक आधार पर आ.वि.कं. के बोर्ड को आउटसोर्सिंग के महत्वपूर्ण जोखिमों को सूचित करना;

ज) अनुमोदित नीतियों और प्रक्रियाओं के अनुसार एक स्वतंत्र समीक्षा और लेखा परीक्षा सुनिश्चित करना;

झ) यह सुनिश्चित करना कि आकस्मिक योजनाओं का विकास और पर्याप्त रूप से परीक्षण किया गया हो;

ञ) आ.वि.कं. को यह सुनिश्चित करना चाहिए कि आउटसोर्सिंग के कारण उनके व्यवसाय निरंतरता तत्परता पर प्रतिकूल समझौता न किया जाए। आ.वि.कं. से अपेक्षित है कि वे रा.आ.बैंक द्वारा जारी बेहतर व्यवसाय

निरंतरता प्रबंधन प्रथाओं को अपनाएं और सक्रिय आश्वासन प्राप्त करे कि आउटसोर्स सेवा प्रदाता निरंतर आधार पर व्यवसाय निरंतरता के लिए तत्परता और तैयारी बनाए रखे।

भाग – ख

आ.वि.कं. के लिए संस्तुति जो ₹100 करोड़ से कम की परिसंपत्ति आकार के साथ सार्वजनिक जमा स्वीकार नहीं कर रही है

8. जो आ.वि.कं. ₹100 करोड़ से कम की परिसंपत्ति आकार की सार्वजनिक जमा स्वीकार नहीं करती, उनके पास बोर्ड अनुमोदित सूचना प्रौद्योगिकी नीति/सूचना प्रणाली नीति होगी। यह नीति नीचे दिये गए बुनियादी मानकों पर विचार करके डिज़ाइन की जा सकती है और इसे 30 सितंबर, 2019 तक रखा जाएगा। आईटी सिस्टम में निम्नलिखित शामिल होंगे:

i) सामान्य सुरक्षा पहलू जैसे भौतिक/तार्किक पहुंच और स्पष्ट पासवर्ड नीति;

ii) स्पष्ट उपयोगकर्ता की भूमिका;

iii) त्रुटि और गलत प्रयोग के जोखिम को कम करने और डेटा/सूचना की स्थिरता सुनिश्चित करने के लिए मेकर-चेकर अवधारणा;

iv) सूचना सुरक्षा और साइबर सुरक्षा;

v) डिजिटल हस्ताक्षर प्रमाणपत्र, मोबाइल फाइनेंशियल सर्विसेज और सोशल मीडिया के संबंध में आवश्यकताएं उपर्युक्त अनुच्छेद 3.8, 3.10 और 3.11 में दर्शायी गई हैं;

vi) परिचालन और परिचालनेत्तर राजस्व और व्यय, सेगमेंट/ उपांग का लागत लाभ विश्लेषण, निधि लागत आदि सहित वित्तीय स्थिति को सारांशित करने के लिए शीर्ष प्रबंधन के लिए सिस्टम जेनरेट की गई रिपोर्ट;

vii) रा.आ.बैंक (ओआरएमआईएस) को विनियामक विवरणी दायर करने हेतु पर्याप्तता;

viii) बोर्ड द्वारा विधिवत अनुमोदित बीसीपी नीति आवधिक रिपोर्ट के माध्यम से बोर्ड की नियमित निरीक्षण सुनिश्चित करती है (प्रत्येक वर्ष कम से कम एक बार);

ix) आवधिक टेस्टिंग के साथ डेटा के बेकअप की व्यवस्था।

8.1 आ.वि.कं. के परिचालन में वृद्धि और जटिलता के रूप में आईटी सिस्टम को क्रमशः बढ़ाया जाना चाहिए।

***