शहरी सहकारी बैंकों के लिए साइबर सुरक्षा के संबंध में तकनीकी विजन दस्तावेज- 2020-2023[1]

1. प्रस्तावना

1.1 बैंकों द्वारा सूचना प्रौद्योगिकी का उपयोग तेजी से बढ़ा है और अब यह बैंकों की परिचालन रणनीति का एक महत्वपूर्ण हिस्सा है। हाल के दिनों में साइबर घटनाओं/हमलों की संख्या, आवृत्ति और प्रभाव में कई गुना वृद्धि हुई है, खासकर वित्तीय क्षेत्र में जिसमें शहरी सहकारी बैंक भी शामिल हैं। इसलिए, शहरी सहकारी बैंकों की सुरक्षा स्थिति को बेहतर बनाना आवश्यक हो गया है, ताकि साइबर हमलों को रोका जा सके, उनका पता लगाया जा सके, उनका सामना किया जा सके और उनसे निपटा जा सके। इसे देखते हुए, सभी शहरी सहकारी बैंकों के लिए बुनियादी साइबर सुरक्षा नियंत्रण निर्धारित करते हुए, 19 अक्टूबर 2018 को परिपत्र डीसीबीएस.सीओ. पीसीबी.परि.सं.1/18.01.000/2018-19 जारी किया गया था।

1.2 आकार, क्षेत्रों, वित्तीय स्थिति और डिजिटल गहराई के संदर्भ में यूसीबी क्षेत्र की विविधता को ध्यान में रखते हुए, यह माना गया कि यूसीबी के लिए साइबर सुरक्षा दिशानिर्देश निर्धारित करते समय 'वन साइज फिट्स ऑल' दृष्टिकोण उपयुक्त नहीं हो सकता है। इसे ध्यान में रखते हुए, शहरी सहकारी बैंकों के लिए साइबर सुरक्षा नियंत्रणों का निरूपण निम्नलिखित सिद्धांतों द्वारा निर्देशित किया जाए:

- शहरी सहकारी बैंकों के लिए साइबर सुरक्षा नियंत्रण निर्धारित करते समय एक विभेदित स्तर-वार दृष्टिकोण का पालन किया जाएगा। यूसीबी द्वारा दी जाने वाली डिजिटल सेवाओं के संदर्भ में जोखिम एक्सपोजर के आधार पर स्तरों का फैसला किया जाएगा।
- दृष्टिकोण यह सुनिश्चित करेगा कि उच्च आईटी भेदन/और सभी भुगतान सेवाओं की पेशकश करने वाले शहरी सहकारी बैंकों को परिपक्व साइबर सुरक्षा बुनियादी ढांचे और प्रथाओं वाले अन्य बैंकों के बराबर लाया जाए।
- साइबर सुरक्षा नियंत्रणों को लागू करने की प्राथमिक जिम्मेदारी शहरी सहकारी बैंकों के बोर्ड को सौंपी जाएगी।
- यह मानते हुए कि साइबर सुरक्षा ढांचे के कार्यान्वयन की प्रक्रिया अधिक लागत की होगी अतः कार्यान्वयन, निगरानी, अनुपालन और प्रतिक्रिया की जिम्मेदारी बोर्ड स्तर से सौंपी जानी चाहिए और अंतिम उपयोगकर्ता तक पहुंचनी चाहिए। आईटी/ आईएस गवर्नेंस फ्रेमवर्क में एक मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) की नियुक्ति, गहरे डिजिटल पैठ वाले यूसीबी के लिए आईटी रणनीति समिति, आईटी संचालन समिति आदि जैसी विभिन्न समितियों की स्थापना शामिल होगी।

तदनुसार, "प्राथमिक (शहरी) सहकारी बैंकों (यूसीबी) के लिए व्यापक साइबर सुरक्षा ढांचा- एक श्रेणीबद्ध दृष्टिकोण" पर दिनांक 31 दिसंबर 2019 का परिपत्र डीओएस.सीओ/सीएसआईटीई/बीसी.4083/31.01.052/2019-20 सभी यूसीबी को जारी किया गया था और प्राथमिक शहरी सहकारी बैंकों सहित सभी विनियमित संस्थाओं को "थर्ड पार्टी एटीएम स्विच एप्लीकेशन सेवा प्रदाताओं के लिए साइबर सुरक्षा नियंत्रण" पर दिनांक 31 दिसंबर 2019 को परिपत्र डीओएस.सीओ/सीएसआईटीई/बीसी.4084/31.01.015/2019-20 जारी किया गया था।

यूसीबी के लिए साइबर सुरक्षा के संबंध में विजन-2023

पांच-स्तंभ वाले रणनीतिक दृष्टिकोण जीयूएआरडी अर्थात - (जी) गवर्नेंस निरीक्षण, (यू) उपयोगी प्रौद्योगिकी निवेश, (ए) उचित विनियमन और पर्यवेक्षण, (आर) मजबूत सहयोग और (डी) आवश्यक आईटी, साइबर सुरक्षा कौशल सेट के विकास के माध्यम से विकसित आईटी और साइबर खतरे के माहौल के खिलाफ शहरी सहकारी बैंकिंग क्षेत्र की साइबर सुरक्षा ढांचे को विकसित करना।

[1] विजन दस्तावेज के हिंदी और अंग्रेजी पाठ में यदि कोई असंगति या अस्पष्टता पाई जाती है तो विजन दस्तावेज का अंग्रेजी पाठ मान्य होगा।

विजन को पूरा करने के लिए मिशन की स्थापना निम्नलिखित कार्रवाई बिंदुओं के साथ की गई है:

मिशन- विशिष्ट कार्रवाई बिंदु
(जी) गवर्नेंस निरीक्षण
i. साइबर सुरक्षा पर बोर्ड की निगरानी पर ध्यान देना
ii. आईटी विजन दस्तावेज
(यू) उपयोगी प्रौद्योगिकी निवेश
iii. आईटी/साइबर सुरक्षा परियोजनाओं के कार्यान्वयन के लिए आरक्षित निधि/निधि का सृजन
iv. कारोबारी आईटी आस्तियों का प्रबंधन
v. बैंकिंग सेवाओं की उपलब्धता
(ए) उचित विनियमन और पर्यवेक्षण
vi. पर्यवेक्षी रिपोर्टिंग ढांचा
vii. सुरक्षित प्रथाओं के कार्यान्वयन में उचित मार्गदर्शन
(आर) मजबूत सहयोग
viii. सर्वोत्तम प्रथाओं को साझा करने और व्यावहारिक मुद्दों और चुनौतियों पर चर्चा करने के लिए फोरम
ix. यूसीबी के लिए सीआईएसओ फोरम
x. क्लाउड सेवाओं को अपनाना- चरण I
(डी) आवश्यक आईटी, साइबर सुरक्षा कौशल सेट का विकास
xi. आईटी और साइबर सुरक्षा के प्रबंधन के लिए तकनीकी कौशल प्रदान करना
xii. साइबर सुरक्षा पर सभी शहरी सहकारी बैंकों को जागरूकता/प्रशिक्षण प्रदान करना

मिशन विवरणी में उल्लिखित कार्रवाई बिंदुओं का विवरण नीचे दिया गया है।

(जी) गवर्नेंस निरीक्षण

2.1 साइबर सुरक्षा पर बोर्ड की निगरानी पर ध्यान

जैसा कि यूसीबी के लिए जारी व्यापक साइबर सुरक्षा ढांचे में बताया गया है, निदेशक मंडल अंततः यूसीबी की सूचना सुरक्षा के लिए जिम्मेदार है और एक प्रभावी आईटी (सूचना प्रौद्योगिकी) और आईएस (सूचना सुरक्षा) गवर्नेंस सुनिश्चित करने में सक्रिय भूमिका निभाएगा। इसलिए साइबर सुरक्षा से जुड़े मामलों को बोर्ड की बैठकों में चर्चा का हिस्सा बनाने की आवश्यकता है। इस संबंध में, निदेशक मंडल को अपनी बैठकों के दौरान प्रस्तुत किए जाने वाले समीक्षाओं के कैलेंडर के भाग के रूप में विशिष्ट संकेतकों के साथ साइबर सुरक्षा स्थिति पर समीक्षा को शामिल करने के लिए बैंकों को निर्देश जारी किए जाएंगे। (**कार्रवाई**: आरबीआई: 2020)

2.2 आईटी विजन दस्तावेज

आज, लगभग हर यूसीबी डिजिटल डिलीवरी चैनलों पर अपने पदचिह्न का विस्तार करने सहित प्रौद्योगिकी अपनाने के किसी न किसी चरण में है: कोर बैंकिंग समाधान (सीबीएस), या डिजिटल डिलीवरी चैनल जैसे इंटरनेट बैंकिंग, मोबाइल बैंकिंग और एटीएम। वित्तीय समावेशन को आगे बढ़ाने में शहरी सहकारी बैंक महत्वपूर्ण भूमिका निभा सकते हैं। यूसीबी सहित बैंकिंग क्षेत्र के लिए अपने ग्राहकों को अपनी सेवाएं प्रदान करने लिए प्रौद्योगिकी तेजी से प्रमुख कारोबारी सहायक बन रही है। इसलिए, शहरी सहकारी बैंकों को अपने कारोबार में सुरक्षित तरीके से आईटी समाधानों को शामिल करने हेतु अपनी योजनाओं की रूपरेखा तैयार करने के लिए अपना स्वयं प्रौद्योगिकी विजन दस्तावेज विकसित करने की आवश्यकता है। यह विज़न दस्तावेज ऐसे दिशानिर्देश प्रदान करेगा जिनका उपयोग बैंकों द्वारा न केवल एक संगठनात्मक क्षमता के रूप में बल्कि एक रणनीतिक संपत्ति के रूप में आईटी संचालन को डिजाइन, विकसित और कार्यान्वित करने के लिए किया जा सकता है। वांछित परिणाम प्राप्त करने के लिए विजन दस्तावेज़ में अनिवार्य रूप से समय सीमा का उल्लेख होना चाहिए। आवधिक आधार पर विनियामक द्वारा किए गए अनिवार्य परिवर्तनों को शामिल करने के लिए बैंकों को समय-समय पर विजन दस्तावेज की समीक्षा करने के लिए एक तंत्र स्थापित करना चाहिए। (**कार्रवाई:** स्तर 2 से 4 के यूसीबी के लिए : 2021; स्तर 1 के यूसीबी के लिए: 2022)

(यू) उपयोगी प्रौद्योगिकी निवेश

2.3 आईटी/साइबर सुरक्षा परियोजनाओं के कार्यान्वयन के लिए आरक्षित निधि/निधि का सृजन

यह मानते हुए कि साइबर सुरक्षा नियंत्रणों का कार्यान्वयन करने में अधिक पूंजी लगेगी, अतः शहरी सहकारी बैंक आईटी/साइबर सुरक्षा परियोजनाओं को लागू करने के लिए आरक्षित निधि/निधि के सृजन पर विचार कर सकते हैं। यह आरक्षित निधि समयावधि में अपने वार्षिक निवल लाभ में से बनाई जा सकती है। सबसे पहले, चरण-I में एनएएफसीयूबी और यूसीबी के संघों द्वारा एक प्रस्ताव पत्र लाया जा सकता है और चरण II में निधि सृजित की जा सकती है।

(**कार्रवाई**: चरण I –एनएएफसीयूबी और यूसीबी के संघ: सभी यूसीबी: 2022)

2.4 कारोबारी आईटी आस्तियों का प्रबंधन

शहरी सहकारी बैंकों को अपनी आईटी आस्तियों, हार्डवेयर और सॉफ्टवेयर दोनों के जीवनचक्र की उचित निगरानी करनी चाहिए, ताकि अप्रचलित हार्डवेयर/सॉफ्टवेयर के कारण जोखिम न हो। इसलिए, शहरी सहकारी बैंक सहायक आईटी अवसंरचना और सुविधाओं के साथ अपनी आईटी सूची को निवेश और अपग्रेड करने का प्रयास करेगें ताकि यह सुनिश्चित हो सके कि अप्रचलित हार्डवेयर/सॉफ्टवेयर के कारण आईटी अवसंरचना जोखिम के संपर्क में तो नहीं है। इसके अलावा, यूसीबी द्वारा सॉफ्टवेयर लाइसेंस प्रबंधन (एसएलएम) के लिए एक व्यापक प्रक्रिया लागू की जाएगी। यूसीबी द्वारा कम से कम वार्षिक आधार पर आईटी आस्तियों (गंभीरता, विशेषाधिकार पहुंच, पासवर्ड नीति, आदि) की समीक्षा और मूल्यांकन किया जा सकता है।

(**कार्रवाई:** स्तर 2 से 4 के यूसीबी के लिए: 2021; स्तर 1 के यूसीबी के लिए: 2022)

2.5 बैंकिंग सेवाओं की उपलब्धता

अनपेक्षित परिस्थितियां कभी-कभी बड़े परिचालन व्यवधान उत्पन्न करती हैं जिससे शहरी सहकारी बैंकों के निरंतर परिचालन और कामकाज के लिए पर्याप्त जोखिम पैदा होता है। जोखिम से प्रभावी ढंग से निपटने के लिए, शहरी सहकारी बैंकों के पास सभी प्रक्रियाओं के लिए एक कारोबारी निरंतरता योजना (बीसीपी) होनी चाहिए जिसमें केवल

बैकअप सिस्टम की उपलब्धता के अलावा अन्य पहलू भी शामिल हों और यह सुनिश्चित करें कि वह अच्छी तरह से संप्रेषित है, उसका अच्छी तरह से पूर्वाभ्यास किया गया है और समय-समय पर उसकी समीक्षा की जाती है। आवश्यकता के आधार पर, यह एक सुरक्षित लोचदार डिजिटल कार्यस्थल की स्थापना को आवश्यकता के आधार पर अपनाने पर भी चर्चा करेगा, क्योंकि बीसीपी मौजूदा विनियामक अनुदेशों के अनुपालन में अन्य बातों के साथ-साथ कारोबार, तकनीकी और मानवीय पहलुओं को शामिल करेगा। कारोबार को सुचारू रूप से और सुरक्षित रूप से संचालित करने के लिए उनके महत्व के संदर्भ में प्रणालियों और प्रक्रियाओं को प्राथमिकता देने पर ध्यान केंद्रित किया जा सकता है।

(**कार्रवाईः** स्तर 2 से 4 के यूसीबी के लिए: 2021; स्तर 1 के यूसीबी के लिए: 2022)

(ए) उचित विनियमन और पर्यवेक्षण

2.6 पर्यवेक्षी रिपोर्टिंग ढांचा

मौजूदा अनुदेशों के अनुसार, शहरी सहकारी बैंकों को सूचित किया गया है कि वे सभी असामान्य साइबर सुरक्षा घटनाओं (चाहे वे सफल हों या मात्र प्रयास) को अन्य संबंधित प्राधिकरणों के अलावा भारतीय रिज़र्व बैंक को तत्काल रिपोर्ट करें। इसके अलावा, बड़ी संख्या में शहरी सहकारी बैंकों को ध्यान में रखते हुए, साइबर सुरक्षा दिशानिर्देशों के संबंध में शहरी सहकारी बैंकों के अनुपालन की निगरानी के लिए और साथ ही यूसीबी सेक्टर की साइबर सुरक्षा की स्थिति की समग्र और अद्यतन जानकारी के लिए शहरी सहकारी बैंकों का एक प्रभावी ऑफसाइट पर्यवेक्षण आयोजित किया जाएगा।

(**कार्रवाईः** आरबीआईः 2021)

संबंधित विनियमों की पूर्व निर्धारित व्याख्या के आधार पर और सीधे मानक प्रारूप में विनियामक को रिपोर्ट करते हुए स्वचालन के लिए डिजिटल विनियामक रिपोर्टिंग का अन्वेषण किया जाएगा।

(**कार्रवाईः** आरबीआईः 2022)

2.7 सुरक्षित प्रथाओं के कार्यान्वयन में उचित मार्गदर्शन

सभी सहकारी बैंकों के लिए एक समान 'साइबर सिक्योरिटी हाइजीन' दस्तावेज जारी किया जाएगा। यह दस्तावेज़ अनिवार्य रूप से प्रिविलेज एक्सेस मैनेजमेंट, नेटवर्क सेगमेंटेशन, सुरक्षित कॉन्फ़िगरेशन, सुरक्षा घटना और इवेंट मैनेजमेंट सहित विभिन्न क्षेत्रों के पर्यवेक्षित संस्थाओं में देखी जाने वाली विभिन्न सर्वोत्तम प्रथाओं को कवर करेगा, जिनका उपयोग यूसीबी द्वारा लागू नियंत्रणों को लागू करने के लिए संदर्भ दस्तावेज़ के रूप में किया जा सकता है। इसके अलावा, कभी-कभी बदलते खतरे के परिदृश्य का प्रभावी ढंग से मुकाबला करने और समग्र यूसीबी साइबर लचीलापन में सुधार के लिए 'साइबर सिक्योरिटी हाइजीन' को लगातार बढ़ाने के लिए समय-समय पर इसकी समीक्षा की जाएगी।

(**कार्रवाईः** आरबीआईः 2021)

(आर) मजबूत सहयोग

2.8 सर्वोत्तम प्रथाओं को साझा करने और व्यावहारिक मुद्दों और चुनौतियों पर चर्चा करने के लिए फोरम

शहरी सहकारी बैंक राज्य/क्षेत्रीय स्तर पर एक फोरम स्थापित करने की संभावना की तलाश कर सकते हैं जिसमें विभिन्न बैंकों और अन्य संबंधित हितधारकों (जैसे तीसरे पक्ष के प्रदाता) के प्रमुख कर्मचारी और/या प्रबंधन समय-समय पर साइबर सुरक्षा पहलुओं पर बातचीत और समन्वय कर सकते हैं। यह फोरम शहरी सहकारी बैंकों के लिए समकक्षों के साथ अपने अभ्यासों को बेंचमार्क करने, खतरे की खुफिया जानकारी साझा करने, साइबर खतरों से निपटने में उनकी ताकत और कमजोरियों की खोज करने के लिए एक मंच के रूप में भी कार्य कर सकता है। फोरम शुरुआती तौर पर,

सर्वोत्तम प्रथाओं को साझा करने और व्यावहारिक मुद्दों और नियंत्रणों को अपनाने और कार्यान्वयन की चुनौतियों पर चर्चा करने के लिए कम से कम छमाही आधार पर बैठक कर सकता है।

(**कार्रवाई**: यूसीबी के सभी संघ: 2021)

2.9 यूसीबी के लिए सीआईएसओ फोरम

प्रौद्योगिकी परिवर्तनों पर नज़र रखना और साइबर सुरक्षा प्रक्रियाओं को विकसित करना आवश्यक है। नई तकनीकों और अवधारणाओं का पता लगाने की आवश्यकता है, ताकि यह पता लगाया जा सके कि क्या वे पर्याप्त कारोबारी लाभ देते हैं। इस आशय के लिए, जैसा कि वाणिज्यिक बैंकों के मामले में होता है, आईडीआरबीटी शहरी सहकारी बैंकों के साथ अधिक निकटता से जुड़ने के लिए एक अलग सीआईएसओ फोरम स्थापित कर सकता है। यूसीबी की संख्या को ध्यान में रखते हुए, शुरू में, इसे स्तर 3 और 4 यूसीबी (व्यापक साइबर सुरक्षा ढांचे के अनुसार वर्गीकृत) के लिए स्थापित किया जा सकता है और कम से कम तिमाही आधार पर उनके साथ नियुक्त किया जा सकता है।

(**कार्रवाई**: आईडीआरबीटी: 2021)

2.10 क्लाड सेवाओं को अपनाना - चरण I[2]

शहरी सहकारी बैंकों की सीमित पूंजी को देखते हुए साइबर सुरक्षा नियंत्रणों को लागू करने की लागत एक बाधा हो सकती है। क्लाउड आधारित सेवाओं (अधिमानतः समुदाय) जैसे लागत प्रभावी प्रौद्योगिकियों का उपयोग उचित जोखिम मूल्यांकन करने और मौजूदा विनियामक अनुदेशों का अनुपालन करने के बाद आईटी समाधानों और साइबर सुरक्षा नियंत्रणों को लागू करने के लिए किया जा सकता है। क्लाउड सेवाओं को अपनाने का नेतृत्व यूसीबी के संघों और/या किसी अन्य समकक्ष द्वारा किया जा सकता है जो भविष्य में उभर सकता है। प्रथम चरण में, सहयोगात्मक दृष्टिकोण के माध्यम से, शहरी सहकारी बैंकों के लिए क्लाउड सेवाओं को अपनाने के लिए एक ब्लू-प्रिंट तैयार किया जा सकता है। मार्गदर्शन के लिए ReBIT/IDRBT/IFTAS से परामर्श किया जा सकता है।

(**कार्रवाई**: यूसीबी के फेडरेशन। समयसीमा: 2022)

(डी) आवश्यक आईटी, साइबर सुरक्षा कौशल सेट का विकास

2.11 आईटी और साइबर सुरक्षा के प्रबंधन के लिए तकनीकी कौशल प्रदान करना

आईटी प्रणालियों के प्रबंधन में शहरी सहकारी बैंकों[3] में आईटी परिपक्वता का स्तर न्यूनतम है। इसलिए, उन्हें निर्धारित साइबर सुरक्षा नियंत्रणों को लागू करने और निरंतर आधार पर उनका प्रबंधन और निगरानी करने के लिए पर्याप्त सहयोग की आवश्यकता है। विभिन्न श्रेणियों के शहरी सहकारी बैंकों को न केवल समयबद्ध तरीके से नए ढांचे के साथ गति प्रदान करने के लिए बल्कि बदलते और चुनौतीपूर्ण परिदृश्य में आईटी और सुरक्षा उपायों का प्रबंधन करने के लिए लक्षित कौशल-उन्मुख प्रशिक्षण और प्रमाणन कार्यक्रम तैयार किए जाएंगे। क्षेत्रीय भाषाओं में इस तरह का प्रशिक्षण प्रदान करने के लिए देश भर में प्रतिष्ठित विभिन्न संस्थानों/विश्वविद्यालयों में उपलब्ध विशेषज्ञता का लाभ उठाने के उपाय किए जाएंगे।

(**कार्रवाई –** आरबीआई: 2021)

---

[2] इसके पूरा होने पर, चरण 2 दूसरे स्तंभ के तहत कार्यान्वयन के बारे में चर्चा करेगा - (यू) उपयोगिता प्रौद्योगिकी निवेश

[3] मुख्य रूप से स्तर 1 और स्तर 2 के यूसीबी में (31 दिसंबर, 2019 के परिपत्र के अनुसार ग्रेड)

2.12 साइबर सुरक्षा पर सभी शहरी सहकारी बैंकों को जागरूकता/प्रशिक्षण प्रदान करना

निदेशक मंडल, वरिष्ठ प्रबंधन और शहरी सहकारी बैंकों के कर्मचारियों के लिए प्रमाणन:

शहरी सहकारी बैंकों में हितधारकों (बोर्ड से कर्मचारी) के कार्यों/जिम्मेदारियों के लिए जागरूकता/प्रमाणन कार्यक्रम विकसित और अनुकूलित किए जाएंगे। ये कार्यक्रम आरबीआई के विभिन्न प्रशिक्षण संस्थानों और आरबीआई द्वारा स्वीकृत अन्य प्रतिष्ठित संस्थानों की सहायता से प्रदान किए जाएंगे। इस पहल का उद्देश्य, अन्य बातों के अलावा, जागरूकता पैदा करना और मुख्य रूप से साइबर सुरक्षा और सामान्य नियंत्रण की बेहतर समझ के लिए स्थानीय भाषा में आईटी/साइबर सुरक्षा चुनौतियों और विनियामक अपेक्षाओं को संप्रेषित करना है ताकि अपने दिन-प्रतिदिन के कार्यों में एक सुरक्षित और सुदृढ़ आईटी वातावरण सुनिश्चित किया जा सके।

(**कार्रवाई –** आरबीआई: 2021)

****