

सूचना सुरक्षा और साइबर सुरक्षा के लिए आवश्यकता प्रस्ताव (आरएफपी) हेतु बोली-पूर्व प्रश्नों के उत्तर

राष्ट्रीय आवास बैंक का लेखा-परीक्षण

(आरएफपी संदर्भ संख्या: - जीईएम/2025/बी/6767020 - एनएचबी/ऑडिट/आरएफपी/02/2025-26 दिनांक 08 अक्टूबर, 2025)

क्र. सं.	आरएफपी खंड सं.	गतिविधि/मौजूदा खंड विवरण	बोलीदाता का प्रश्न/सुझाव/टिप्पणियाँ	रा.आ.बैं. प्रतिक्रिया
1	3.11 दायित्व की सीमा	इस परियोजना के एक भाग के रूप में किए गए दायित्वों के संबंध में आईएस और सीएस लेखापरीक्षक की कुल देयता, चाहे इस परियोजना के तहत उत्पन्न हो, इस तरह की देयता को जन्म देने वाली कार्रवाई के रूप या प्रकृति की परवाह किए बिना (चाहे अनुबंध, अपकार या अन्यथा), नीचे उप-खंड (ii) में उल्लिखित परिस्थितियों के अलावा, कुल अनुबंध मूल्य के गुना तक सीमित होगी।	आईएस और सीएस लेखा परीक्षक की देयता की सटीक सीमा पर स्पष्टीकरण प्रदान करें	कुल अनुबंध मूल्य का एक गुना
2	लागू नहीं	लागू नहीं	हम ध्यान देते हैं कि आरएफपी के अंतर्गत कार्य का दायरा सुरक्षा नीति में परिवर्तन/संशोधन की सिफारिश/तैयारी/सुझाव, नीति दस्तावेजों के मूल्यांकन जैसी सेवाओं को इंगित करता है। हम समझते हैं कि ये सेवाएँ कानूनी दृष्टिकोण से नहीं, बल्कि केवल तकनीकी/व्यावसायिक दृष्टिकोण से प्रदान की जाएँगी। हम निम्नलिखित खंड को शामिल करने का प्रस्ताव करते हैं: “इसके विपरीत किसी भी बात के बावजूद, कृपया ध्यान दें कि हम प्रत्यक्ष या अप्रत्यक्ष रूप से कोई भी कानूनी सेवा प्रदान नहीं करते हैं क्योंकि हमें ऐसा करने की अनुमति नहीं है। हमारा दायरा	बोलीदाताओं को आरएफपी के नियमों एवं शर्तों को बिना किसी शर्त के स्वीकार करना होगा।

			तकनीकी/व्यावसायिक पहलू तक सीमित है, और हमारी सेवाओं में कोई भी कानूनी सेवा या कानूनी सलाह शामिल नहीं होगी। हमारे कर्मचारियों द्वारा किया गया कोई भी कार्य कानूनी सेवा/कानूनी सलाह नहीं माना जाएगा।”	
3	3.20 लेखापरीक्षा	<p>आईएस और सीएस लेखा परीक्षक राष्ट्रीय आवास बैंक, उसके अधिकृत कार्मिकों, उसके लेखा परीक्षकों (आंतरिक और बाह्य) और/या भारतीय रिजर्व बैंक/अन्य विनियामक और वैधानिक प्राधिकरणों, और उनके अधिकृत कार्मिकों को अपनी पुस्तकों और खातों का निरीक्षण और/या लेखा परीक्षा करने, सेवाओं से सीधे संबंधित आईएस और सीएस लेखा परीक्षक पर किए गए किसी भी लेखा परीक्षा या समीक्षा रिपोर्ट और निष्कर्षों की प्रतियां प्रदान करने का अप्रतिबंधित अधिकार देगा।</p> <p>यदि किसी भी सेवा को आरपी के संदर्भ में अन्य आईएस और सीएस लेखा परीक्षकों को आउटसोर्स / सौंपा / उप-अनुबंधित किया जाता है, तो यह सुनिश्चित करना आईएस और सीएस लेखा परीक्षक की जिम्मेदारी होगी कि ऊपर उल्लिखित अधिकारियों / कर्मचारियों को निरीक्षण और / या लेखा परीक्षा के लिए सभी संबंधित स्थानों तक पहुंच की अनुमति दी जाए।</p>	<p>हम निम्नलिखित खंड को शामिल करने का प्रस्ताव करते हैं:</p> <p>“कोई भी ऑडिट निम्नलिखित के अधीन होगा: (i) ऑडिट केवल अनुबंध तक ही सीमित होगा और पूर्व उचित सूचना के साथ किया जाएगा। (ii) राष्ट्रीय आवास बैंक या उसके अधिकृत प्रतिनिधि ऐसे ऑडिट से पहले एक गैर-प्रकटीकरण समझौते पर हस्ताक्षर करेंगे जो ऑडिट के संचालन और उसके किसी भी परिणाम को नियंत्रित करेगा; (iii) ऑडिट के लिए राष्ट्रीय आवास बैंक के ऑडिटर या प्रतिनिधि आईएस और सीएस ऑडिटर के प्रतिस्पर्धी नहीं होंगे; (iv) ऑडिट एक कैलेंडर वर्ष में एक से अधिक बार और पूरी तरह से दो बार नहीं किया जाएगा; और (v) ऑडिट के दौरान किसी भी निष्कर्ष को आईएस और सीएस ऑडिटर के साथ साझा किया जाएगा और इसके समापन के लिए राष्ट्रीय आवास बैंक और आईएस और सीएस ऑडिटर के बीच पारस्परिक रूप से चर्चा और सहमति होगी।”</p>	<p>बोलीदाताओं को आरएफपी के नियमों एवं शर्तों को बिना किसी शर्त के स्वीकार करना होगा।</p>

4	3.16 गैर-प्रतिस्पर्धा	आईएस एवं सीएस लेखा परीक्षक इस अनुबंध की वैधता के दौरान तथा इस अनुबंध की समाप्ति की तिथि से एक वर्ष तक एनएचबी के किसी भी कर्मचारी से प्रत्यक्ष या अप्रत्यक्ष रूप से न तो संपर्क करेगा और न ही उसके लिए कार्य का कोई प्रस्ताव रखेगा।	कृपया स्पष्ट करें कि क्या निष्क्रिय नियुक्ति की अनुमति है - उदाहरण के लिए, जब कोई कर्मचारी बिना किसी प्रत्यक्ष अनुरोध के सार्वजनिक भर्ती चैनलों के माध्यम से आवेदन करता है	बोलीदाताओं को आरएफपी के नियमों एवं शर्तों को बिना किसी शर्त के स्वीकार करना होगा।
5	सुरक्षा वास्तुकला के मौजूदा डिजाइन का मूल्यांकन	कमजोरियों और व्यावसायिक जोखिम की पहचान करने, सुरक्षा की प्रभावकारिता का आकलन करने और हमलावर के उद्देश्यों और कार्यों का अनुकरण करके पहले से मौजूद शमन नियंत्रणों की जांच करने के लिए अर्ध-वार्षिक आधार पर रेड टीम अभ्यास का संचालन करें।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. क्या आप रेड टीमिंग अभ्यासों के दायरे के बारे में विस्तृत जानकारी दे सकते हैं? क्या यह बाहरी होगा या आंतरिक? क्या कोई विशिष्ट परिदृश्य हैं जिन पर ध्यान देने की आवश्यकता है?	रेड टीमिंग अभ्यास में सामाजिक इंजीनियरिंग और भौतिक पहुंच के प्रयास शामिल होंगे। लेखा परीक्षक से बाह्य मूल्यांकन करने की अपेक्षा की जाती है।
6	अनुलग्नक-II	बैंक की आवश्यकता के अनुसार कार्य के दायरे से परे साइबर सुरक्षा घटना की फॉरेंसिक जांच सहित सौंपे गए किसी भी अतिरिक्त कार्य के लिए।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. फॉरेंसिक छवियों का औसत आकार क्या है जिन्हें लिया जाना आवश्यक है? 2. इमेजिंग के लिए उपयोग की जाने वाली हार्ड डिस्क का खर्च कौन वहन करेगा, क्योंकि यह छवि के आकार और घटना में शामिल उपकरणों की संख्या पर आधारित होगा? 2. क्या लॉग विश्लेषण के भाग के रूप में सिएम/ एसआईईएम एक्सेस दिया जाएगा, या हमें डिजिटल फॉरेंसिक भाग के भाग के रूप में लॉग विश्लेषण ऑफ़लाइन करना होगा?	फॉरेंसिक ऑडिट एक अलग कार्य है। यदि बैंक द्वारा आवश्यक हो तो फॉरेंसिक ऑडिट का कार्य लेखा परीक्षक को सौंपा जाएगा। तदनुसार विवरण साझा किया जाएगा।
7	6.1 सूचना सुरक्षा ऑडिट और साइबर सुरक्षा ऑडिट (प्रकार - सेवाएँ)	सुरक्षा वास्तुकला डिजाइन में मुख्यालय और क्षेत्रीय कार्यालय दोनों शामिल हैं, अर्थात् दोनों कार्यालयों के बीच अंतर्संबंध और राष्ट्रीय आवास बैंक नेटवर्क पर विभिन्न	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. सुरक्षा वास्तुकला डिजाइन के दायरे में कितने क्षेत्रीय कार्यालय शामिल हैं?	वर्तमान में बैंक के 17 क्षेत्रीय कार्यालय हैं।

		अनुप्रयोगों द्वारा उपयोग किए जाने वाले इंटरफेस शामिल हैं।		
8	6.1 सूचना सुरक्षा ऑडिट और साइबर सुरक्षा ऑडिट (प्रकार - सेवाएँ)	इस समस्या के समाधान के लिए राष्ट्रीय आवास बैंक के नेटवर्क और अनुप्रयोगों सहित सुरक्षा वास्तुकला का विन्यास करना।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. लगभग कितने घटकों पर कॉन्फिगरेशन समीक्षा की जानी है।	नेटवर्क डिवाइस लगभग 70, सर्वर लगभग 190, एक्टिव डायरेक्टरी, ईडीआर, डब्ल्यूएफ, प्रॉक्सी, एनएसी, डेटाबेस, सैन, बैंकअप समाधान
9	6.1 सूचना सुरक्षा ऑडिट और साइबर सुरक्षा ऑडिट (प्रकार - सेवाएँ)	उत्पादन में सभी एप्लीकेशन प्रोग्रामिंग इंटरफेस की कमजोरियों की जांच करना।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. वर्तमान में कितने एप्लीकेशन प्रोग्रामिंग इंटरफेस उत्पादन में हैं और भेद्यता मूल्यांकन के दायरे में शामिल हैं?	वर्तमान में चार अनुप्रयोगों में एप्लीकेशन प्रोग्रामिंग इंटरफेस है।
10	6.1 सूचना सुरक्षा ऑडिट और साइबर सुरक्षा ऑडिट (प्रकार - सेवाएँ)	बैंक के सुरक्षा समाधान, ओएस, अनुप्रयोगों, सर्वरों और नेटवर्क उपकरणों की सुरक्षित कॉन्फिगरेशन समीक्षा का कवरेज, लेकिन इन्हीं तक सीमित नहीं।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. कृपया सुरक्षा समाधानों, ओएस प्लेटफॉर्म, अनुप्रयोगों, सर्वरों और नेटवर्क उपकरणों की संख्या और प्रकार की पुष्टि करें।	नेटवर्क डिवाइस लगभग 70 (स्विच, फ़ायरवॉल, एनएसी, वीपीएन डिवाइस), सर्वर लगभग 190 (उबंटू, आरएचईएल, विंडोज), एक्टिव डायरेक्टरी, ईडीआर, डब्ल्यूएफ, प्रॉक्सी, एनएसी, डेटाबेस, एसएएन, बैंकअप समाधान, तीस अनुप्रयोग, डेस्कटॉप-300 (ऑडिट अवधि के दौरान बढ़ाया जा सकता है)।
11	6.1 सूचना सुरक्षा ऑडिट और साइबर सुरक्षा ऑडिट (प्रकार - सेवाएँ)	बैंक के सार्वजनिक अनुप्रयोगों का स्रोत कोड ऑडिट करना। आंतरिक रूप से विकसित अनुप्रयोगों के लिए स्रोत कोड समीक्षा की जाएगी।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. उन अनुप्रयोगों की संख्या जिनके लिए स्रोत कोड ऑडिट किया जाएगा। 2. प्रत्येक अनुप्रयोग में कोड की पंक्तियाँ।	वर्तमान में, अनुप्रयोगों की संख्या ग्यारह है, जिनके लिए स्रोत कोड ऑडिट किया जाएगा।

12	6.1 सूचना सुरक्षा ऑडिट और साइबर सुरक्षा ऑडिट (प्रकार - सेवाएँ)	फायरवॉल, डब्ल्यूएफ और प्रॉक्सी के लिए कॉन्फिगरेशन समीक्षा की जानी है। फायरवॉल, डब्ल्यूएफ, प्रॉक्सी, एंटीवायरस, डीएलपी और एनएसी नियम/नीति की समीक्षा की जानी है।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. दायरे में फायरवॉल, डब्ल्यूएफ, प्रॉक्सी, एंटीवायरस, डीएलपी और एनएसी समाधानों की संख्या।	फायरवॉल-6, डब्ल्यूएफ समाधान, एनएसी -2, वीपीएन-2, प्रॉक्सी समाधान-1, ईडीआर-1, डीएलपी (ईडीआर और ऑफिस 365 के साथ अंतर्निहित)
13	6.1 सूचना सुरक्षा ऑडिट और साइबर सुरक्षा ऑडिट (प्रकार - सेवाएँ)	आईएस ऑडिटर द्वारा वार्षिक आधार पर क्रेडेंशियल आधारित एप्लिकेशन और सर्वर की भेद्यता स्कैनिंग की जाएगी।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. कृपया क्रेडेंशियल-आधारित स्कैनिंग के दायरे में आने वाले एप्लिकेशन और सर्वर की संख्या की पुष्टि करें। 2. यह स्कैनिंग साल में केवल एक बार (सालाना) की जाएगी या दो बार? इसकी आवृत्ति क्या है?	आरएफपी के दायरे में उल्लिखित सभी एप्लिकेशन और सर्वर क्रेडेंशियल-आधारित स्कैनिंग के अधीन होंगे। स्कैनिंग की आवृत्ति आरएफपी में उल्लिखित आईएस और सीएस ऑडिट की आवृत्ति के अनुसार होगी।
14	6.2 भेद्यता मूल्यांकन, विश्लेषण और समाधान	बैंक के आंतरिक अनुप्रयोगों का उनके पूरे जीवन चक्र (कार्यान्वयन से पूर्व, कार्यान्वयन के बाद, बड़े बदलावों के बाद) के दौरान वीएपीटी।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. आंतरिक आवेदनों और अनुरोधों की संख्या तथा कार्यान्वयन से पूर्व, कार्यान्वयन के बाद और प्रमुख परिवर्तनों के बाद आयोजित किए जाने वाले वीएपीटी की अनुमानित संख्या।	वर्तमान में बैंक के पास 07 आंतरिक आवेदन हैं।
15	6.2 भेद्यता मूल्यांकन, विश्लेषण और समाधान	बोलीदाता/चयनित सूचीबद्ध लेखा परीक्षक, बैंक के साथ समन्वय में तथा बैंक की आवश्यकता के अनुसार, अनुबंध अवधि के दौरान किसी भी आवेदन की पूर्व तैनाती वीएपीटी का संचालन करने के लिए जिम्मेदार होगा।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. सामान्यतः ऐसे कितने अनुप्रयोग विकसित किये जाते हैं?	विकास की भविष्यवाणी नहीं की जा सकती, हालांकि अनुमान के लिए यह लगभग दस हो सकता है।
16	6.2 भेद्यता मूल्यांकन, विश्लेषण और समाधान	आईएस ऑडिट/वीएपीटी दायरे के अंतर्गत आवेदनों की सूची तदनुसार अद्यतन रखी जाएगी।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. आरएफपी के अनुसार, अभी 25 आवेदन प्राप्त हुए हैं, और इससे ज़्यादा नए आवेदन जोड़े जा सकते हैं। उम्मीद है कि हमारा अनुमान सही है।	हां, आवेदन की सीमा बढ़ाई जा सकती है।

17	6.2 भेद्यता मूल्यांकन, विश्लेषण और समाधान	प्रवेश परीक्षण का कार्य आक्रामक सुरक्षा प्रमाणित पेशेवरों की तरह किया जाना चाहिए ताकि बैंक की आईटी सुरक्षा अवसंरचना की मजबूती का आकलन किया जा सके।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. कृपया पुष्टि करें कि क्या हमें बाहरी पीटी/ प्रवेश परीक्षण करना है। यदि हाँ, तो कृपया सार्वजनिक आईपी की संख्या की पुष्टि करें। 2. यदि इसमें किसी अन्य गतिविधि को शामिल करने की आवश्यकता है तो इसकी पुष्टि करें।	बाहरी पीटी/प्रवेश परीक्षण किया जाना है। वर्तमान में सार्वजनिक आईपी की संख्या 140 है।
18	6.4 राष्ट्रीय आवास बैंक अधिकारियों के लिए प्रशिक्षण कार्यक्रम और प्रशिक्षण सामग्री	बोलीदाता/चयनित पैनलबद्ध लेखा परीक्षक पाठ्यक्रम विकसित करेगा, प्रशिक्षण देगा, तथा राष्ट्रीय आवास बैंक अधिकारियों, राष्ट्रीय आवास बैंक प्रशासकों और अन्य संबंधित उपयोगकर्ताओं के लिए प्रशिक्षण सामग्री उपलब्ध कराएगा।	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. कृपया पुष्टि करें कि प्रशिक्षण सामग्री कितनी बार उपलब्ध कराई जानी है, साथ ही प्रशिक्षण सत्रों की आवृत्ति भी बताएं।	बैंक के कर्मचारियों, बैंक के आईटी बुनियादी ढांचे को संभालने वाले ऑन-साइट सहायक कर्मचारियों/विक्रेताओं के लिए आईटी और साइबर सुरक्षा जागरूकता प्रशिक्षण (आईटी टीम के लिए विशेष सुरक्षा प्रशिक्षण सहित) व्याख्यान, सेमिनार/वेबिनार, बातचीत और प्रस्तुतियों के रूप में लेखा परीक्षक द्वारा तिमाही आधार पर आयोजित किया जाना है।
19	आईटी और आईएस सेवाओं के विक्रेताओं का ऑडिट	आईटी और आईएस सेवाओं के विक्रेताओं का ऑडिट	कृपया निम्नलिखित प्रश्नों को स्पष्ट करें: 1. कितने विक्रेताओं के लिए ऑडिट किया जाना है, तथा इसकी आवृत्ति क्या होगी।	वर्तमान में लेखापरीक्षा विक्रेता के अधीन निम्नलिखित विक्रेता हैं। 8 - आईटी आउटसोर्स सेवाओं के लिए विक्रेता। 1 - सीआईएसओ सेवाओं के लिए विक्रेता
20	चरण 1 -I	> नेटवर्क और उपयोग में आने वाले उपकरण, फ़ायरवॉल नियम-आधारित समीक्षा। > ऑपरेटिंग सिस्टम - सेटअप, कॉन्फिगरेशन, ट्यूनिंग, लाइसेंस ऑडिट, आदि।	कृपया नेटवर्क डिवाइसों, अनुप्रयोगों (वेब फेसिंग और नॉन-वेब फेसिंग), डेटाबेस की संख्या की पुष्टि करें, जिसकी समीक्षा की जानी है	नेटवर्क डिवाइस लगभग 70 (स्विच, फ़ायरवॉल, एनएसी, वीपीएन डिवाइस), सर्वर लगभग 190 (उबंटू, आरएचईएल, विंडोज), एक्टिव

		> डेटाबेस, सिस्टम और एप्लिकेशन (वेब-फेसिंग और नॉन-वेब-फेसिंग) - सेटअप, कॉन्फिगरेशन, ट्यूनिंग, डेटाबेस ऑडिट, आदि।		डायरेक्टरी, ईडीआर, डब्ल्यूएफ, प्रॉक्सी, एनएसी, डेटाबेस, एसएएन, बैकअप समाधान, तीस अनुप्रयोग, डेस्कटॉप-300 (ऑडिट अवधि के दौरान बढ़ाया जा सकता है)।
21	चरण 1 -I	> बैंक द्वारा निर्धारित समय-सीमा के भीतर केआरआई रिटर्न का पूर्व-लेखापरीक्षा/सत्यापन। > निर्धारित समय-सीमा के भीतर सार्वजनिक अनुप्रयोगों और डेटाबेस का पूर्व-लेखापरीक्षा/सत्यापन। > साइबर सुरक्षा घटना सारांश का पूर्व-लेखापरीक्षा/सत्यापन। > भारतीय रिजर्व बैंक को प्रस्तुत किए जाने वाले किसी भी अन्य रिटर्न का पूर्व-लेखापरीक्षा/सत्यापन।	सफल बोलीदाता रिटर्न की समीक्षा करेगा, लेकिन उसे सत्यापन प्रदान करना आवश्यक नहीं है। कृपया हमारी सहमति की पुष्टि करें।	लेखा परीक्षक को रिटर्न की समीक्षा और सत्यापन करना होगा।
22	चरण 1 -I	साइबर सुरक्षा सेट-अप	कृपया "साइबर सुरक्षा सेट-अप" में शामिल किए जाने वाले क्षेत्रों और नियंत्रणों को निर्दिष्ट करें	लेखा परीक्षक को मौजूदा साइबर सुरक्षा व्यवस्था के सभी क्षेत्रों की समीक्षा करनी होगी।
23	चरण 1 -I	भारतीय रिजर्व बैंक को प्रस्तुत करने के लिए आवश्यक किसी अन्य रिटर्न का पूर्व-लेखापरीक्षा/सत्यापन।	कृपया समीक्षा हेतु आवश्यक रिटर्न की संख्या निर्दिष्ट करें	रिटर्न की संख्या निर्दिष्ट नहीं की जा सकती क्योंकि यह भारतीय रिजर्व बैंक की अपेक्षा है
24	चरण 1 -I	मौजूदा सुरक्षा संरचना का मूल्यांकन, परिवर्तन सिफारिशें / नए डिजाइन / लेआउट, और सुरक्षा वास्तुकला का दस्तावेजीकरण ताकि भारतीय रिजर्व बैंक दिशानिर्देशों, अंतर्राष्ट्रीय	कृपया बताएं कि भारतीय रिजर्व बैंक के किन दिशानिर्देशों, अंतर्राष्ट्रीय मानकों पर विचार किया जाना है।	कृपया समय-समय पर भारतीय रिजर्व बैंक द्वारा आईटी प्रणालियों, अवसंरचना आदि पर जारी मास्टर परिपत्रों/निर्देशों/दिशानिर्देशों का अवलोकन करें। इसके अतिरिक्त,

		मानकों और उद्योग-व्यापी स्वीकृत सर्वोत्तम प्रथाओं के अनुरूप हो।		लेखा परीक्षक को यह सुनिश्चित करना होगा कि अनुपालन प्रमाणपत्र/अन्य नियामक निर्देशों के अनुसार हो।
25	चरण 1 -I	कमजोरियों और व्यावसायिक जोखिम की पहचान करने, सुरक्षा की प्रभावकारिता का आकलन करने और हमलावर के उद्देश्यों और कार्यों का अनुकरण करके पहले से मौजूद शमन नियंत्रणों की जांच करने के लिए अर्ध-वार्षिक आधार पर रेड टीम अभ्यास का संचालन करें।	सफल बोलीदाता पहचानी गई कमजोरियों के लिए नियंत्रण लागू करने के लिए जिम्मेदार नहीं होगा। कृपया हमारी सहमति की पुष्टि करें।	लेखा परीक्षक सिफारिशों और सहायता प्रदान करेगा। सिफारिशों के आधार पर, बैंक कमियों को दूर करेगा।
26	चरण 1 -I	कम्प्यूटरीकृत प्रक्रियाओं के लिए वर्तमान परिचालन प्रक्रिया और सुरक्षा नीति का मूल्यांकन। इन प्रक्रियाओं के लिए परिचालन प्रक्रिया और सुरक्षा नीति की अनुशंसा और रूपरेखा तैयार करना।	कृपया समीक्षा की जाने वाली तथा तैयार की जाने वाली नीतियों/प्रक्रियाओं की संख्या की पुष्टि करें।	बैंक परियोजना से संबंधित सभी आंतरिक नीतियों और मानक संचालन प्रक्रिया (एसओपी) की प्रतियाँ उपलब्ध कराएगा। इसके अलावा, लेखा परीक्षक को यह सुनिश्चित करना होगा कि अनुपालन भारतीय रिज़र्व बैंक/प्रमाणपत्र/अन्य नियामक निर्देशों के अनुसार हो।
27	चरण 1 -I	वेब एप्लिकेशन कॉन्फ़िगरेशन का मूल्यांकन और कमियों/कमजोरियों/सुधारों (यदि कोई हो) की परीक्षण रिपोर्टिंग। इनसे निपटने के लिए समाधान/शमनकारी रणनीतियाँ सुझाना।	कृपया कवर किए जाने वाले वेब अनुप्रयोगों/आवेदनों की संख्या की पुष्टि करें	वर्तमान में, लगभग तीस वेब आवेदनों /अनुप्रयोगों को कवर किया जाना है।
28	चरण 1 -I	बैंक के आंतरिक अनुप्रयोगों/आवेदनों और पोर्टलों (ऑडिट अवधि के दौरान विकसित अनुप्रयोगों और पोर्टलों सहित) का सॉफ्टवेयर ऑडिट करना।	कृपया कवर किए जाने वाले आवेदनों/अनुप्रयोगों और पोर्टलों की संख्या की पुष्टि करें	वर्तमान में, लगभग तीस वेब अनुप्रयोगों/ आवेदनों को कवर किया जाना है।

29	सामान्य	लागू नहीं	कृपया उस स्थान की पुष्टि करें जहां से परियोजना को क्रियान्वित किया जाना है।	मुख्य /आधार स्थान जहाँ से ऑडिट किया जाना है, वह दिल्ली स्थित राष्ट्रीय आवास बैंक का मुख्यालय है। नमूना आधारित ऑन-साइट ऑडिट केवल क्षेत्रीय कार्यालयों के लिए स्वीकार्य है।
30	6	लेखा परीक्षक लेखापरीक्षा गतिविधियाँ संचालित करेंगे और विभिन्न कार्यों के लिए अलग-अलग लेखापरीक्षा रिपोर्ट प्रस्तुत करेंगे। रिपोर्टों के अतिरिक्त, लेखा परीक्षक अनुपालन प्रमाणपत्र भी प्रदान करेंगे।	कृपया उन क्षेत्रों की पुष्टि करें जिनके लिए अनुपालन प्रमाणपत्र आवश्यक है।	कृपया आरएफपी के डिलिवरेबल्स अनुभाग को देखें।
31	वाणिज्यिक बोली का प्रारूप (आवरण पत्र के साथ प्रस्तुत किया जाना है)	वाणिज्यिक बोली का प्रारूप (आवरण पत्र के साथ प्रस्तुत किया जाना है)	वाणिज्यिक बोली अनुलग्नक को जीईएम पोर्टल पर अपलोड करने की आवश्यकता नहीं है तथा बोली राशि जीईएम पर ही प्रस्तुत की जानी चाहिए। कृपया हमारी सहमति की पुष्टि करें।	वाणिज्यिक बोली अनुलग्नक को जीईएम पोर्टल पर आरएफपी में उल्लिखित अन्य दस्तावेजों के साथ प्रस्तुत करना आवश्यक है।
32	अनुलग्नक VIII	बैंक गारंटी का प्रारूप	बैंक गारंटी केवल सफल बोलीदाता द्वारा ही जमा की जानी है। कृपया हमारी सहमति की पुष्टि करें।	बैंक गारंटी केवल सफल बोलीदाता द्वारा ही प्रस्तुत की जाएगी।
33	अनुलग्नक X	गोपनीयता सह एनडीए	गोपनीयता सह एनडीए केवल सफल बोलीदाता द्वारा ही प्रस्तुत किया जाना है। कृपया हमारी सहमति की पुष्टि करें।	गोपनीयता सह एनडीए केवल सफल बोलीदाता द्वारा प्रस्तुत किया जाना है।
34	सामान्य	लागू नहीं	हम आपसे विनम्र अनुरोध करते हैं कि कृपया बोली जमा करने की तिथि 29 अक्टूबर 2025 से बढ़ाकर 07 नवंबर 2025 कर दी जाए।	वित्तीय बोली प्रस्तुत करने की अंतिम तिथि 29.10.2025 है।

35	5	<p>इसके अलावा, बैंक के क्षेत्रीय कार्यालय अहमदाबाद, बेंगलुरु, भोपाल, भुवनेश्वर, चंडीगढ़, चेन्नई, दिल्ली, गुवाहाटी, हैदराबाद, जयपुर, लखनऊ, कोलकाता, मुंबई, पटना, रायपुर, रांची और तिरुवनंतपुरम में हैं, जो मुख्यालय स्थित केंद्रीकृत डेटा सेंटर से जुड़े हैं। आईएस और सीएस ऑडिट इन कार्यालयों के लिए लागू किए गए एक्सेस कंट्रोल मैकेनिज्म को भी कवर करेगा।</p>	<p>1. कृपया पुष्टि करें कि क्या प्रवेश प्रबंधन केंद्रीय रूप से किया जाता है और</p> <p>2. क्या क्षेत्रीय कार्यालयों की यात्रा आवश्यक है?</p>	<p>पहुँच प्रबंधन केंद्रीय स्तर पर किया जाता है। क्षेत्रीय कार्यालयों तक यात्रा आवश्यकता के आधार पर की जाती है।</p>
36	चरण I - I - सी	<p>आईएस एवं सीएस लेखा परीक्षक को बैंक के सभी विभागाध्यक्षों (एचओडी) के साथ बातचीत करनी चाहिए ताकि बैंक द्वारा उठाए गए सूचना सुरक्षा एवं साइबर सुरक्षा उपायों के बारे में उनके विचार/प्रतिक्रिया प्राप्त की जा सके तथा उनकी प्रतिक्रिया के आधार पर कमियों (यदि कोई हो) का मूल्यांकन किया जा सके।</p>	<p>राष्ट्रीय आवास बैंक लेखापरीक्षा के दौरान लेखापरीक्षकों, विभागाध्यक्षों और अन्य राष्ट्रीय आवास बैंक हितधारकों के बीच समन्वय को सुगम बनाने के लिए एक एसपीओसी नियुक्त करेगा। कृपया हमारी सहमति की पुष्टि करें।</p>	<p>राष्ट्रीय आवास बैंक, लेखापरीक्षा के दौरान लेखापरीक्षकों, विभागाध्यक्षों और अन्य एनएचबी हितधारकों के बीच समन्वय को सुगम बनाने के लिए एक विशेष कार्यकारी अधिकारी (एसपीओसी) की नियुक्ति करेगा। हालाँकि, लेखापरीक्षक को बैंक के सभी विभागाध्यक्षों (एचओडी) के साथ बातचीत करके बैंक द्वारा उठाए गए सूचना सुरक्षा और साइबर सुरक्षा उपायों पर उनके विचार/प्रतिक्रियाएँ प्राप्त करनी होंगी और कमियों का मूल्यांकन करना होगा।</p>
37	चरण II-II	<p>अनुपालन समीक्षा पूरी होने पर, आईएस एवं सीएस लेखा परीक्षक को इस आशय का आईएस लेखा परीक्षा एवं सीएस लेखा परीक्षा</p>	<p>कृपया ड्राफ्ट ऑडिट रिपोर्ट प्रस्तुत करने के बाद अनुपालन समीक्षा आरंभ करने की समयसीमा की पुष्टि करें।</p>	<p>कृपया आरएफपी के परियोजना अनुसूची अनुभाग को देखें।</p>

		अनुपालन दस्तावेज/रिपोर्ट उपलब्ध करानी होगी।		
38	10.25	सफल बोलीदाता को सेवा आदेश दिए जाने के 30 दिनों के भीतर या बैंक द्वारा निर्धारित विस्तारित अवधि के भीतर राष्ट्रीय आवास बैंक के साथ अनुबंध IX, X और अनुबंध XI के अनुसार सेवा स्तर समझौते, गोपनीयता सह गैर-प्रकटीकरण समझौते और पूर्व-अनुबंध अखंडता समझौते पर हस्ताक्षर करना होगा।	बोली जमा करते समय अनुलग्नक IX, X और अनुलग्नक XI के अनुसार सेवा स्तर समझौता, गोपनीयता सह गैर-प्रकटीकरण समझौता और अनुबंध-पूर्व सत्यनिष्ठा संधि की आवश्यकता नहीं है। सफल बोलीदाता को इसे जमा करना होगा। कृपया हमारी सहमति की पुष्टि करें।	बोलीदाता को आरएफपी में उल्लिखित अन्य सभी आवश्यक दस्तावेजों के साथ पूर्व-अनुबंध सत्यनिष्ठा समझौता प्रस्तुत करना होगा।
39	खंड 5 – कार्यक्षेत्र	आईएस और सीएस ऑडिट में मुख्यालय, डीआर साइट और 17 क्षेत्रीय कार्यालय शामिल होंगे	कृपया पुष्टि करें कि क्या सभी क्षेत्रीय कार्यालयों के लिए प्रत्यक्ष निरीक्षण आवश्यक है या अन्य कार्यालयों के लिए दूरस्थ सत्यापन के साथ नमूना-आधारित ऑन-साइट ऑडिट स्वीकार्य है। वह आधार स्थान क्या है जहाँ से ऑडिट किया जाना है?	आधार स्थान जहाँ से ऑडिट किया जाना है, वह दिल्ली स्थित राष्ट्रीय आवास बैंक का मुख्यालय है। नमूना आधारित ऑन-साइट ऑडिट केवल क्षेत्रीय कार्यालयों के लिए स्वीकार्य है।
40	खंड 5(ए) – आईटी अवसंरचना	कवरेज में मुख्य कार्यालय, डीआर साइट, क्षेत्रीय कार्यालय शामिल हैं	ऑडिट प्रयास के अनुमान के लिए नेटवर्क/सुरक्षा उपकरणों (फ़ायरवॉल, राउटर, स्विच, सर्वर, एंडपॉइंट) की अनुमानित संख्या और प्रकार का अनुरोध करें।	नेटवर्क डिवाइस लगभग 70 (स्विच, फ़ायरवॉल, एनएसी, वीपीएन डिवाइस), सर्वर लगभग 190 (उबंटू, आरएचईएल, विंडोज), एक्टिव डायरेक्टरी, ईडीआर, डब्ल्यूएएफ, प्रॉक्सी, एनएसी, डेटाबेस, एसएएन, बैकअप समाधान, तीस अनुप्रयोग, डेस्कटॉप-300 (ऑडिट अवधि के दौरान बढ़ाया जा सकता है)।

41	खंड 5(ए) – साइबर सुरक्षा ढांचा	इसमें सीएसओसी और साइबर सुरक्षा तैयारी संकेतक शामिल हैं	कृपया पुष्टि करें कि क्या सीएसओसी सेटअप (एसआईईएम, ईडीआर, एसओसी संचालन) को विस्तृत कॉन्फिगरेशन समीक्षा और मॉनिटरिंग लॉग सत्यापन में शामिल किया जाएगा।	कृपया आरएफपी का अनुलग्नक I देखें
42	खंड 5 – रेड टीमिंग अभ्यास	सार्वजनिक अनुप्रयोगों पर अर्ध-वार्षिक रेड टीमिंग	कृपया स्पष्ट करें कि क्या रेड टीमिंग में सोशल इंजीनियरिंग और भौतिक पहुंच के प्रयास शामिल हैं या केवल नेटवर्क/वेब शोषण तक सीमित है। क्या हमसे आंतरिक और बाह्य दोनों तरह के मूल्यांकन करने की अपेक्षा की जाती है?	रेड टीमिंग में सोशल इंजीनियरिंग और भौतिक पहुंच के प्रयास शामिल होंगे। लेखा परीक्षक से दोनों बाहरी मूल्यांकन करने की अपेक्षा की जाती है।
43	खंड 5(बी) – चरणबद्ध लेखापरीक्षा दृष्टिकोण	चरण I – मूल्यांकन, चरण II – संचार, चरण III – समीक्षा और प्रमाणन	स्पष्ट करें कि क्या प्रत्येक चरण को स्वीकृति हस्ताक्षर के साथ अलग से निर्धारित किया जाएगा या सभी चरण एक ही लेखापरीक्षा चक्र के भीतर लगातार चलेंगे।	परियोजना के लक्ष्यों का उल्लेख आरएफपी के डिलिवरेबल्स और परियोजना अनुसूची अनुभाग में किया गया है।
44	खंड 5(डी) – वेब फेसिंग अनुप्रयोग	25+ अनुप्रयोग सूचीबद्ध (एसएपी, क्रैमिस, पीएमएवाई-सीएलएसएस, ग्रिड्स, यूआईडीएफ, आदि)	कृपया पुष्टि करें कि इनमें से कौन से अनुप्रयोग बाह्य-उन्मुख हैं और कौन से आंतरिक हैं; साथ ही, क्या परीक्षण यूआरएल या यूएटी इंस्टैंस प्रदान किए जाएंगे।	सफल बोलीदाता के साथ साझा किया जाएगा
45	खंड 5(डी) – स्रोत कोड समीक्षा	सार्वजनिक अनुप्रयोगों के स्रोत कोड का ऑडिट	उन अनुप्रयोगों की संख्या की पुष्टि करें जिनके लिए स्रोत कोड साझा किया जाएगा, भाषा/स्टैक (जावा, .NET, पीएचपी, आदि) और क्या पहुंच स्थानीय या दूरस्थ होगी।	लगभग 13. वर्तमान में सभी आवेदन डॉट नेट पर हैं
46	खंड 5(डी) – एपीआई सुरक्षा समीक्षा	उत्पादन परिवेश में एपीआई की समीक्षा	कृपया एपीआई की सांकेतिक संख्या बताएं तथा बताएं कि क्या पोस्टमैन संग्रह/एपीआई दस्तावेज परीक्षण के लिए साझा किए जाएंगे।	वर्तमान में चार अनुप्रयोगों में एपीआई है।
47	खंड 5(डी) – मोबाइल एप्लिकेशन का ऑडिट	बैंक में क्रियान्वित सभी अनुप्रयोग और पोर्टल	स्पष्ट करें कि क्या कोई एंड्रॉइड या आईओएस मोबाइल ऐप दायरे में है; यदि हां, तो कृपया एपीके/आईपीए एक्सेस और परीक्षण वातावरण विवरण की पुष्टि करें।	एंड्रॉइड और आईओएस दोनों के लिए 1 ऐप

48	खंड 5 – आईटी अवसंरचना का मूल्यांकन	डीसी (दिल्ली) और डीआर साइट (नवी मुंबई)	कृपया पुष्टि करें कि क्या दोनों साइटों का प्रबंधन राष्ट्रीय आवास बैंक की आंतरिक टीमों द्वारा किया जाता है या किसी डेटा-सेंटर सेवा प्रदाता को आउटसोर्स किया जाता है, और क्या विक्रेता समन्वय की सुविधा प्रदान की जाएगी।	दोनों साइटों का प्रबंधन आउटसोर्स सेवा प्रदाता के समन्वय से राष्ट्रीय आवास बैंक की आंतरिक टीम द्वारा किया जाता है।
49	खंड 5 – साइबर सुरक्षा मूल्यांकन	अर्ध-वार्षिक आधार पर रेड टीम अभ्यास का संचालन करना	पुष्टि करें कि क्या रेड टीम की सहभागिता उत्पादन या पृथक प्रतिकृति वातावरण पर निष्पादित की जाएगी।	रेड टीम की सहभागिता को प्रतिरूपित वातावरण में क्रियान्वित किया जाएगा।
50	खंड 5 – जोखिम मूल्यांकन	केआरआई रिटर्न और आरबीआई प्रस्तुतियों की समीक्षा	कृपया सत्यापित किए जाने वाले केआरआई की सूची तथा आरबीआई को रिपोर्टिंग चक्र (मासिक/तिमाही) स्पष्ट करें।	केआरआई भारतीय रिज़र्व बैंक रिटर्न के अनुसार हैं और आवृत्ति त्रैमासिक है।
51	खंड 5(सी) – प्रणाली कार्यान्वयन का मूल्यांकन	एसएपी, क्रैमिस, पीएमएवाई-सीएलएसएस, ग्रीड्स, यूआईडीएफ, आदि।	पुष्टि करें कि क्या एसएपी सिस्टम ऑडिट में कार्यात्मक पहुँच नियंत्रण और बेसिस कॉन्फिगरेशन समीक्षा दोनों शामिल हैं।	हाँ। एसएपी सिस्टम ऑडिट में कार्यात्मक पहुँच नियंत्रण और बेसिस कॉन्फिगरेशन समीक्षा दोनों शामिल हैं।
52	खंड 5(सी) – विभागीय बातचीत	आईएस और सीएस लेखा परीक्षक को सभी विभागाध्यक्षों के साथ बातचीत करनी चाहिए	साक्षात्कार सत्रों की योजना बनाने के लिए विभागों/हितधारकों की अनुमानित संख्या का अनुरोध करें।	बैंक के मुख्यालय में 22 विभाग और सत्रह क्षेत्रीय कार्यालय हैं। आईएस और सीएस लेखा परीक्षकों का मुख्य संपर्क आईटीएस, सीईओ और लेखा परीक्षा विभाग के साथ होता है।
53	खंड 5 – आउटसोर्स सेवाएँ	आईटी और आईएस सेवाओं के विक्रेताओं का ऑडिट	कृपया दायरे में आने वाले विक्रेताओं की संख्या बताएं (उदाहरण के लिए: एएमसी, एसओसी, क्लाउड, डीआर, या नेटवर्क विक्रेता)।	वर्तमान में निम्नलिखित विक्रेता विक्रेता लेखापरीक्षा के अधीन हैं। 8 - आईटी आउटसोर्स सेवाओं के लिए विक्रेता। 1 - सीआईएसओ सेवाओं के लिए विक्रेता

54	खंड 6 – डिलिवरेबल्स	डिलिवरेबल्स की सूची (आईएस ऑडिट, सीएस ऑडिट, वीएपीटी, रेड टीम, विक्रेता ऑडिट, प्रशिक्षण)	स्पष्ट करें कि क्या प्रत्येक वितरण योग्य वस्तु के लिए अलग प्रमाणन पत्र या समेकित रिपोर्ट प्रस्तुत करने की आवश्यकता है।	प्रत्येक वितरण योग्य वस्तु के लिए अलग प्रमाणीकरण/रिपोर्ट की आवश्यकता होती है।
55	खंड 6.1 – आईएस और सीएस ऑडिट	फ़ायरवॉल, डब्ल्यूएफ, प्रॉक्सी, डीएलपी, एनएसी नीति समीक्षा	कृपया पुष्टि करें कि क्या लेखा परीक्षकों को केवल पढ़ने के लिए प्रशासनिक पहुंच दी जाएगी या स्क्रीनशॉट/लॉग के साथ अवलोकन-आधारित समीक्षा दी जाएगी।	लेखा परीक्षकों को रीड-ओनली की प्रशासनिक पहुंच दी जाएगी।
56	खंड 6.1 – कॉन्फ़िगरेशन समीक्षा	एंटीवायरस, एडी, पैच, उपयोगकर्ता पहुंच प्रबंधन	पुष्टि करें कि क्या सत्यापन के लिए नेसस/क्वालिस, माइक्रोसॉफ्ट बेसलाइन एनालाइजर या आंतरिक स्क्रिप्ट जैसे उपकरणों का उपयोग किया जा सकता है।	लेखा परीक्षक दोनों उपकरणों का उपयोग कर सकता है।
57	खंड 6.2 – वीएपीटी	तिमाही वीएपीटी और उपचारोत्तर सत्यापन	पुष्टि करें कि क्या पुनः परीक्षण को तिमाही डिलिवरेबल्स का हिस्सा माना जाएगा या इसे अलग प्रयास के रूप में माना जाएगा।	पुनःपरीक्षण तिमाही वीएपीटी अभ्यास का हिस्सा है। इसके अलावा, आरएफपी में उल्लिखित अन्य कार्यों के लिए, पुनःपरीक्षण दायरे के अनुसार किया जाएगा।
58	खंड 6.2 – वीएपीटी	सर्वरों की क्रेडेंशियल-आधारित स्कैनिंग	कृपया पुष्टि करें कि क्या विंडोज, लिनक्स और डीबी सर्वर के लिए क्रेडेंशियल स्कैन आवश्यक हैं; और क्या स्थानीय एडमिन क्रेडेंशियल साझा किए जाएंगे।	हाँ
59	खंड 6.2 – पैच समीक्षा	तिमाही पैच और सुरक्षा अद्यतन समीक्षा	पुष्टि करें कि पैच समीक्षा केवल ओएस और अनुप्रयोगों को कवर करती है या इसमें फर्मवेयर/नेटवर्क डिवाइस भी शामिल हैं।	पैच समीक्षा में फ़र्मवेयर/नेटवर्क डिवाइस भी शामिल हैं
60	खंड 6.2 – ईमेल सुरक्षा परीक्षण	डीकेआईएम, एसपीएफ, डीएमएआरसी नियंत्रणों की जाँच करें	पुष्टि करें कि क्या राष्ट्रीय आवास बैंक अनुमोदन के साथ ईमेल स्पूफ़िंग परीक्षण किया जा सकता है।	हाँ
61	खंड 6.2 – एपीआई परीक्षण	विकसित/अनुकूलित एपीआई के लिए वीएपीटी	एपीआई की संख्या और अपेक्षित प्रमाणीकरण विधियों (जेडब्ल्यूटी, ओ ऑथ, बेसिक ऑथ, आदि) पर पुष्टि का अनुरोध करें।	वर्तमान में चार अनुप्रयोगों में एपीआई है।
62	खंड 6.3 – रिपोर्टिंग	आईएस/सीएस ऑडिट रिपोर्ट: विस्तृत निष्कर्ष, अनुपालन, ज्ञान हस्तांतरण	स्पष्ट करें कि क्या बैंक को वरिष्ठ प्रबंधन के लिए अलग कार्यकारी सारांश और आईटी टीम के लिए तकनीकी रिपोर्ट की आवश्यकता है।	कृपया आरएफपी के डिलिवरेबल्स अनुभाग को देखें।

63	खंड 6.4 – प्रशिक्षण कार्यक्रम	तिमाही कर्मचारी जागरूकता प्रशिक्षण	कृपया अपेक्षित श्रोता संख्या, भाषा वरीयता (अंग्रेजी/हिंदी) तथा यह भी बताएं कि क्या राष्ट्रीय आवास बैंक ऑन-साइट सत्र रिकॉर्डिंग या एलएमएस अपलोड की अपेक्षा करता है।	प्रशिक्षण द्विभाषी होगा तथा ऑनलाइन आयोजित किया जाएगा।
64	खंड 7 – परियोजना अनुसूची	ऑडिट रिपोर्ट जमा करने की समयसीमा (15 जनवरी 2026 और 30 जुलाई 2026)	स्पष्ट करें कि क्या वीएपीटी, रेड टीम और विक्रेता ऑडिट डिलिवरेबल्स के लिए अलग-अलग समय-सीमाएं लागू होती हैं या एक ही तिथि का पालन किया जाता है।	हाँ। समय-सीमा के लिए, कृपया आरएफपी के परियोजना अनुसूची अनुभाग देखें।
65	खंड 7 – तिमाही वितरण	वीएपीटी रिपोर्ट तिमाही के अंतिम दिन से 45 दिनों के भीतर प्रस्तुत की जानी है	कृपया पुष्टि करें कि क्या राष्ट्रीय आवास बैंक रिपोर्ट प्रस्तुत करने की अपेक्षा करता है, भले ही सुधार कार्य जारी हो या समापन सत्यापन के बाद।	वीएपीटी के लिए अनुमत अधिकतम समय-सीमा लेखापरीक्षा के अंतर्गत तिमाही की अंतिम तिथि से 45 दिन है।
66	खंड 6 – भेद्यता शोषण	प्रवेश परीक्षण का दायरा	कृपया पुष्टि करें कि पहचानी गई कमजोरियों को सत्यापित करने के लिए नियंत्रित शोषण की अनुमति है या नहीं।	उत्पादन सेवाओं के निर्बाध संचालन को सुनिश्चित करते हुए इसकी अनुमति दी जा सकती है।
67	खंड 6 – उपकरण और स्वचालन	लेखा परीक्षक उद्योग-स्वीकृत उपकरणों का उपयोग करेगा	पुष्टि करें कि क्या लाइसेंस प्राप्त उपकरणों के साथ ओपन-सोर्स उपकरणों (जैसे, एनमैप, निकटो, एसक्यूएलमैप) के उपयोग की अनुमति है।	हाँ
68	खंड 6 – पुनः परीक्षण	सुधार के बाद सत्यापन	कृपया प्रति तिमाही शामिल पुनः परीक्षण चक्रों की संख्या (एक या एकाधिक) की पुष्टि करें।	बैंक द्वारा प्रस्तुत सभी अनुपालनों का सत्यापन आवश्यक है।
69	खंड 5 - कार्य का दायरा (I - जोखिम मूल्यांकन और सुरक्षा आवश्यकताओं की पहचान)	भारतीय रिजर्व बैंक को प्रस्तुत करने के लिए आवश्यक किसी भी अन्य रिटर्न का पूर्व-लेखा परीक्षा / सत्यापन	यहाँ किन विशिष्ट रिटर्न का उल्लेख किया जा रहा है? क्या इसमें दक्ष पोर्टल पर प्रस्तुत अनुपालन रिपोर्ट शामिल हैं?	हाँ

70	खंड 5 - कार्य का दायरा (I - जोखिम मूल्यांकन और सुरक्षा आवश्यकताओं की पहचान)		कृपया स्पष्ट करें कि क्या बैंक आईएस-आरएमएफ की समीक्षा के लिए औपचारिक जोखिम मूल्यांकन पद्धति (जैसे, आईएसओ 27001) का पालन किए जाने की अपेक्षा करता है?	हाँ
71	खंड 6 - डिलिवरेबल्स आईएस-आरएमएफ और जोखिम रजिस्ट्रों की समीक्षा	सूचना सुरक्षा - जोखिम प्रबंधन ढांचा (आईएस-आरएमएफ) दस्तावेज की समीक्षा और बैंक के आईएस-आरएमएफ के आधार पर सूचना सुरक्षा जोखिम रजिस्टर का निर्माण।	कृपया स्पष्ट करें कि क्या डिलीवरेबल में एक नया जोखिम रजिस्टर टेम्पलेट बनाना शामिल होना चाहिए या केवल ऑडिट निष्कर्षों के आधार पर बैंक के मौजूदा आईएस-आरएमएफ रजिस्टर को भरना चाहिए।	बैंक के आईएस-आरएमएफ पर आधारित एक नया जोखिम रजिस्टर टेम्पलेट बनाना आवश्यक है।
72	खंड 5 - कार्यक्षेत्र (I. जोखिम मूल्यांकन और सुरक्षा आवश्यकताओं की पहचान, उप-धारा सी. बैंक में प्रणाली कार्यान्वयन का मूल्यांकन)		कृपया स्पष्ट करें कि वर्तमान परिचालन प्रक्रियाओं और सुरक्षा नीतियों का मूल्यांकन किन विशिष्ट विनियमों, दिशानिर्देशों या सुरक्षा मानकों के आधार पर किया जाना है।	बैंक परियोजना से संबंधित सभी आंतरिक नीतियों और मानक संचालन प्रक्रिया (एसओपी) की प्रतियाँ उपलब्ध कराएगा। इसके अलावा, लेखा परीक्षक को यह सुनिश्चित करना होगा कि अनुपालन भारतीय रिजर्व बैंक/प्रमाणपत्र/अन्य नियामक निर्देशों के अनुसार हो।
73	कार्य का दायरा (II. सुरक्षा अंतराल का विवरण)	सभी आउटसोर्स गतिविधियों और सेवाओं का ऑडिट	कृपया पुष्टि करें कि क्या विक्रेता ऑडिट के लिए भारतीय रिजर्व बैंक आईटी आउटसोर्सिंग दिशानिर्देश (2023) के अनुसार मूल्यांकन की आवश्यकता होगी और क्या विक्रेता स्व-प्रमाणन / तृतीय-पक्ष एसओसी 2 रिपोर्ट को साक्ष्य के रूप में स्वीकार किया जा सकता है।	Yes

74	<p>खंड 6 - वितरण योग्य,</p> <p>उप- खंड 6.3 आईएस ऑडिट और सीएस ऑडिट रिपोर्ट (प्रकार - दस्तावेजीकरण)</p>		<p>कृपया ज्ञान हस्तांतरण रिपोर्ट के अपेक्षित दायरे और विषय-वस्तु की पुष्टि करें। क्या इसमें मुख्य रूप से आयोजित जागरूकता सत्रों और प्रतिभागियों की प्रतिक्रिया का दस्तावेजीकरण होना चाहिए?</p>	<p>यह रिपोर्ट सम्पूर्ण परियोजना कार्यान्वयन के दौरान की गई विस्तृत बातचीत पर आधारित होगी।</p>
75	<p>खंड 6 - वितरण योग्य,</p> <p>उप- खंड 6.3 आईएस ऑडिट और सीएस ऑडिट रिपोर्ट (प्रकार - दस्तावेजीकरण)</p>		<p>आईएस और सीएस ऑडिट के लिए भारतीय रिज़र्व बैंक के कौन से विशिष्ट दिशानिर्देश हैं?</p>	<p>कृपया समय-समय पर आईटी प्रणालियों, बुनियादी ढांचे आदि पर भारतीय रिज़र्व बैंक द्वारा जारी मास्टर परिपत्रों/निर्देशों/दशानिर्देशों का संदर्भ लें।</p>
76	<p>खंड 6. डिलिवरेबल्स उप-खंड 6.2 भेद्यता मूल्यांकन, विश्लेषण और समाधान (प्रकार - दस्तावेजीकरण और सेवा)</p>	<p>उन कमियों को ठीक करना/समाधान करना जिन्हें तत्काल दूर किया जा सकता है।</p>	<p>क्या हमसे यह अपेक्षा की जाती है कि हम कमजोरियों को भी ठीक करें या केवल सिफारिशों और सहायता प्रदान करें?</p>	<p>लेखा परीक्षक सिफारिशों और सहायता प्रदान करेगा। सिफारिशों के आधार पर, बैंक कमजोरियों को दूर करेगा।</p>
