भारतीय स्टेट बैंक

केंद्रीय भर्ती एवं पदोन्नति विभाग, कॉरपोरेट केंद्र, मुंबई
(फोन: 022-2282 0427; फैक्स: 022-2282 0411; ईमेल: crpd@sbi.co.in)

भारतीय स्टेट बैंक में विशेषज्ञ संवर्ग के अधिकारियों की नियमित आधार पर भर्ती

विज्ञापन सं. CRPD/SCO-SYSTEM/2019-20/11

1. **आवेदन का ऑनलाइन पंजीकरण और शुल्क का ऑनलाइन भुगतान: दिनांक 06.09.2019 से 25.09.2019 तक**
2. **ऑनलाइन परीक्षा की तिथि (संभावित): 20.10.2019 (केवल पद क्रं. 1 से 24 के लिए)**
3. **ऑनलाइन परीक्षा के लिए कॉल लेटर डाउनलोड करने की संभावित तिथि: 10.10.2019 से (केवल पद क्रं. 1 से 24 के लिए)**

भारतीय स्टेट बैंक निम्नलिखित विशेषज्ञ संवर्ग के अधिकारी पदों पर नियमित आधार पर नियुक्ति के लिए भारतीय नागरिकों से ऑन-लाइन आवेदन करता है.

अभ्यर्थियों से अनुरोध है कि बैंक की वेबसाइट https://bank.sbi/careers या https://www.sbi.co.in/careers में दिए गए लिंक के माध्यम से ऑन-लाइन आवेदन करें.

1. एक अभ्यर्थी केवल **एक पद** के लिए आवेदन कर सकता/सकती है.
2. पंजीकरण की प्रकिया तभी पूरी होगी जब बैंक में ऑनलाइन तरीके से शुल्क भुगतान की अंतिम तिथि को या उससे पहले जमा करवा दिया गया है.
3. आवेदन करने से पहले, अभ्यर्थियों से अनुरोध है कि वे यह सुनिश्चित करें कि वे पात्रता की तिथि को उक्त पद के लिए दिए गए मानदंडों को पूरा करते हैं.
4. अभ्यर्थियों से अपेक्षा है कि वे अपेक्षित सभी प्रलेख अपलोड करें (संक्षिप्त जीवन वृत्त, आईडी प्रमाण, आयु प्रमाण, शैक्षिक योग्यता, अनुभव आदि) ऐसा नहीं करने पर उन्हें योग्य अभ्यर्थियों की सूची में शामिल करने/ऑनलाइन लिखित परीक्षा/साक्षात्कार के लिए बुलाए जाने हेतु उनकी अभ्यर्थिता पर विचार नहीं किया जाएगा.
5. ऑनलाइन परीक्षा में प्रवेश/चयनित सूची बनाना दस्तावेजों के सत्यापन के बिना पूर्णतया अनंतिम होगा. अभ्यर्थिता सभी ब्यौरों/दस्तावेजों का मूल दस्तावेजों से सत्यापन के अधीन होगी जब अभ्यर्थी के साक्षात्कार (यदि बुलाया जाता है) के लिए रिपोर्ट करता है.
6. यदि अभ्यर्थी को साक्षात्कार के लिए बुलाया जाता है और वह पात्रता मानदंडों को पूरा नहीं करता/करती है (आयु, शैक्षिक योग्यता और अनुभव आदि) तो उसे न तो साक्षात्कार में उपस्थित होने दिया जाएगा और न ही वह यात्रा व्ययों की प्रतिपूर्ति के लिए पात्र होगा/होगी.
7. अभ्यर्थियों को सलाह दी जाती हैं कि वे बैंक की वेबसाइट https://bank.sbi/careers या https://www.sbi.co.in/careers को नियमित रूप से विवरणों और नई जानकारी हेतु देखें (इसमें छांट कर बुलाए जाने/योग्य अभ्यर्थियों की सूची शामिल है). ऑनलाइन परीक्षा के लिए कॉल लेटर और "acquaint yourself" बुकलेट रजिस्ट्रेशन नंबर तथा पासवर्ड/जन्म तिथि दर्ज करके बैंक की वेबसाइट से डाउनलोड किया जाए. साक्षात्कार के लिए कॉल लेटर, जहां अपेक्षित होगा, केवल ईमेल से भेजा जाएगा. (कोई हार्ड कॉपी नहीं भेजी जाएगी).
8. यदि एक से अधिक अभ्यर्थियों को समान अंक आते हैं जो कि फाइनल मेरिट लिस्ट में कट ऑफ अंक हैं (कट ऑफ प्वाइन्ट पर समान अंक), तो ऐसे अभ्यर्थियों को मेरिट में उनकी आयु के अवरोही क्रम में रखा जाएगा.
9. **इस कार्यालय को कागजी आवेदन** और अन्य प्रलेखों की प्रतियां न भेजें.
10. **सभी संशोधन/शुद्धि पत्र केवल बैंक की उपर्युक्त वेबसाइटों पर ही अपलोड किया जाएगा.**

क. पद (नियमित)/ग्रेड/रिक्तियां/उम्र/चयन प्रक्रिया का विवरण:

पद क्रमांक	पद	ग्रेड	रिक्तियां								30.06.2019 को उम्र	चयन प्रक्रिया
			सामा.	अ.पि.व	अ.जा.	अ.ज.जा	आ.क.व	कुल	पी.डब्ल्यू.डी			
									एल.डी.#	एच आई	अधिकतम	
1	डेव्लपर	JMGS-I	62	39	22	10	14	147	3	3	30	
2	डेव्लपर	MMGS-II	16	9	4	2	3	34	1	1	33	
3	सिस्टम/सर्वर एडमिनिस्ट्रेटर	JMGS-I	21	12	7	3	4	47	1	1	30	
4	डेटाबेस एडमिनिस्ट्रेटर	JMGS-I	14	7	4	2	2	29	1	1	30	
5	क्लाउड एडमिनिस्ट्रेटर	JMGS-I	8	3	2	1	1	15	1		30	
6	नेटवर्क इंजीनियर	JMGS-I	8	3	1	1	1	14	1		30	
7	टेस्टर	JMGS-I	3	1	–	–	–	4	1		30	
8	डब्ल्यूएएस एडमिनिस्ट्रेटर	MMGS-II	5	1	–	–	–	6	1		33	
9	इंफ्रास्ट्रक्चर इंजीनियर	MMGS-II	3	1	–	–	–	4	1		33	
10	यूएक्स डिजाइनर	MMGS-II	3	–	–	–	–	3	1		33	
11	आईटी जोखिम प्रबंधक	MMGS-II	1	–	–	–	–	1	–		33	
12	आईटी सिक्योरिटी एक्सपर्ट	MMGS-III	8	3	2	1	1	15	1		38	• ऑनलाइन लिखित परीक्षा • साक्षात्कार
13	परियोजना प्रबंधक	MMGS-III	8	3	1	1	1	14	1		38	
14	एप्लिकेशन आर्किटेक्ट	MMGS-III	4	1	–	–	–	5	1		38	
15	टेक्निकल लीड	MMGS-III	3	1	–	–	–	4	1		38	
16	इंफ्रास्ट्रक्चर आर्किटेक्ट	MMGS-III	2	–	–	–	–	2	1		38	
17	इंफ्रास्ट्रक्चर इंजीनियर	JMGS-I	2	–	–	–	–	2	1	–	30	
18	आईटी सुरक्षा विशेषज्ञ	JMGS-I	27	16	9	4	5	61	3	–	30	
19	आईटी सुरक्षा विशेषज्ञ	MMGS-II	10	4	2	1	1	18	1	–	35	
20	आईटी जोखिम प्रबंधक (आईएस डिपो)	MMGS-II	4	1	–	–	–	5	1	–	35	
21	इंफ्रास्ट्रक्चर आर्किटेक्ट	MMGS-II	2	–	–	–	–	2	1	–	35	
22	उप प्रबंधक (सायबर सिक्योरिटी- एथिकल हैकिंग)	MMGS-II	6	2	1	–	1	10	1	–	35	
23	उप प्रबंधक (सायबर सिक्योरिटी-थ्रेट हन्टिंग)	MMGS-II	3	1	–	–	–	4	1	–	35	
24	उप प्रबंधक (सायबर सिक्योरिटी-डिजिटल फॉरेन्सिक)	MMGS-II	3	1	–	–	–	4	1	–	35	
25	सिक्योरिटी एनालिस्ट	MMGS-III	8	3	1	–	1	13	1	–	38	• चयनित सूची और • साक्षात्कार
26	प्रबंधक (सायबर सिक्योरिटी-एथिकल हैंकिंग)	MMGS-III	1	–	–	–	–	1	–	–	38	
27	प्रबंधक (सायबर सिक्योरिटी-डिजिटल फॉरेन्सिक)	MMGS-III	1	–	–	–	–	1	–	–	38	
28	मुख्य प्रबंधक (वल्नेराबिलिटी मैनेजमेंट एंड पैनिट्रेशन टेस्टिंग)	SMGS-IV	1	–	–	–	–	1	–	–	40	
29	मुख्य प्रबंधक (इन्सिडेंट मैनेजमेंट एंड फॉरेन्सिक्स)	SMGS-IV	2	–	–	–	–	2	1	–	40	
30	मुख्य प्रबंधक (सिक्योरिटी एनालिटिक्स एंड ऑटोमेशन)	SMGS-IV	2	–	–	–	–	2	1	–	40	
31	मुख्य प्रबंधक (एसओसी इंफ्रास्ट्रक्चर मैनेजमेंट)	SMGS-IV	1	–	–	–	–	1	–	–	40	
32	मुख्य प्रबंधक (एसओसी गवर्नेन्स)	SMGS-IV	1	–	–	–	–	1	–	–	40	
33	मुख्य प्रबंधक (सायबर सिक्योरिटी-एथिकल हैकिंग)	SMGS-IV	3	–	–	–	–	3	1	–	40	
34	मुख्य प्रबंधक (सायबर सिक्योरिटी-डिजिटल फॉरेन्सिक)	SMGS-IV	1	–	–	–	–	1	–	–	40	
35	मुख्य प्रबंधक (सायबर सिक्योरिटी-थ्रेट हन्टिंग)	SMGS-IV	1	–	–	–	–	1	–	–	40	

ओए तथा ओएल अभ्यर्थी आवेदन कर सकते हैं.

संक्षेपाक्षर:

संवर्ग: सामा-सामान्य संवर्ग, अपिव-अन्य पिछड़ा वर्ग, अ.जा-अनुसूचित जाति, अ.ज.जा-अनुसूचित जन जाति, आ.क.व-आर्थिक कमजोर वर्ग, पी.डब्ल्यू.डी-दिव्यांग व्यक्ति, एल.डी-लोकोमोटर अक्षमता, ओ.एल-एक पैर की बाधकता, ओ.ए-एक हाथ की बाधकता, एच.आई-श्रवण बाधित, जेएमजीएस-जूनियर मैनेजमेंट ग्रेड स्केल, एमएमजीएस-मिडल मैनेजमेंट ग्रेड स्केल, एसएमजीएस-सीनियर मैनेजमेंट ग्रेड स्केल.

नोट:

1. ऐसे अभ्यर्थी जो ओबीसी श्रेणी से संबंधित हैं लेकिन 'क्रीमी लेयर' से आते हैं, वे ओबीसी आरक्षण एवं आयु छूट के लिए पात्र नहीं होंगे. उन्हें अपनी श्रेणी 'सामान्य' या सामान्य (पीडब्ल्यूडी), के रूप में दर्शाना चाहिए.
2. ऊपर उल्लिखित आरक्षित रिक्त-पदों सहित रिक्त-पदों की संख्या अनंतिम है और यह बैंक की वास्तविक आवश्यकता के अनुसार बदल सकती है.
3. बैंक के पास किसी भी समय इस भर्ती प्रक्रिया को निरस्त करने का अधिकार सुरक्षित है.
4. अजा/अजजा अभ्यर्थियों को भारत सरकार द्वारा निर्धारित प्रारूप में सक्षम प्राधिकारी द्वारा जारी किया गया जाति प्रमाण-पत्र जमा करना होगा.

5. ओबीसी श्रेणी के अंतर्गत आरक्षण माँगने वाले अभ्यर्थियों द्वारा निर्धारित प्रारूप में एक घोषणा जमा करवानी होगी कि वह 31.03.2019 को क्रीमी लेयर से नहीं है. 'नॉन क्रीमी लेयर' अनुच्छेद वाला ओबीसी प्रमाण–पत्र जो 01.04.2019 से साक्षात्कार की तिथि के दौरान जारी किया गया हो, को ऐसे अभ्यर्थियों द्वारा जमा करना चाहिए, यदि उन्हें साक्षात्कार के लिए बुलाया जाता है.
6. दिव्यांग (पीडब्ल्यूडी) अभ्यर्थी के लिए आरक्षण समस्तर है और सम्पूर्ण रिक्त–पदों (की संख्या) के अंदर है.
7. पीडब्ल्यूडी अभ्यर्थी को भारत सरकार के दिशानिर्देशों के अनुसार सक्षम प्राधिकारी द्वारा जारी प्रमाणपत्र प्रस्तुत करना होगा.
8. भर्ती में आर्थिक रूप से कमजोर वर्ग के लिए आरक्षण कार्मिक एवं प्रशिक्षण विभाग, कार्मिक मंत्रालय, लोक शिकायत एवं पेंशन, भारत सरकार के दिनांक 31.01.2019 के कार्यालय ज्ञापन सं.36039/1/2019–ईएसटीटी (आरईएस) द्वारा शासित होता है. अस्वीकरण: आर्थिक रूप से कमजोर वर्ग की रिक्तियां अंतरिम हैं तथा भारत सरकार के आगे के निदेशों और किसी भी कानून के परिणाम के अधीन हैं. नियुक्ति अनंतिम है और उचित चैनलों के माध्यम से सत्यापित किए जाने वाले आय एवं आस्ति प्रमाणपत्र के अधीन है.
9. ईडब्ल्यूएस श्रेणी के तहत आरक्षण का लाभ भारत सरकार द्वारा निर्धारित प्रारूप पर सक्षम प्राधिकारी द्वारा जारी 'आय और संपत्ति प्रमाण पत्र' के प्रस्तुतीकरण पर उठाया जा सकता है.
10. अधिकतम आयु सामान्य श्रेणी के अभ्यर्थी के लिए दर्शाई गई है. भारत सरकार के दिशानिर्देशों के अनुसार आरक्षित श्रेणी के अभ्यर्थी के लिए ऊपरी आयु सीमा में छूट उपलब्ध होगी.
11. ऐसे मामलों में जहाँ एक विशिष्ट क्षेत्र में अनुभव की आवश्यकता है, प्रासंगिक अनुभव प्रमाण पत्र में विशेष रूप से शामिल होना चाहिए कि अभ्यर्थी के पास उस विशिष्ट क्षेत्र में अनुभव है.
12. यदि डिग्री/डिप्लोमा के प्रमाणपत्र विशेषज्ञता का क्षेत्र नहीं निर्दिष्ट करते हैं, तो अभ्यर्थी को संबंधित विश्वविद्यालय/महाविद्यालय से विशेष रूप से विशेषज्ञता का उल्लेख करने वाला प्रमाणपत्र प्रस्तुत करना होगा.

(ख) शैक्षणिक अर्हता/अनुभव/तैनाती के संभावित स्थान का विवरण:

पद क्रमांक	पद एवं ग्रेड	बैसिक शैक्षणिक योग्यता (अनिवार्य) यथा 30.06.2019	अन्य योग्यता (अनिवार्य/अधिमान्य) यथा 30.06.2019	30.06.2019 को बेसिक अर्हता के पश्चात कार्य अनुभव (प्रशिक्षण तथा अध्यापन के अनुभव को पात्रता में जोड़ा नहीं जाएगा.) (पद संख्या 1 से 16 के लिए ,अनुभव ''आईटी सेक्टर'' में होना चाहिए और पद संख्या 17 से 35 के लिए अनुभव ''बीएफएसआई सेक्टर तथा/या प्रख्यात आईटी कंपनियों'' में होना चाहिए.)
1.	**डेव्लपर (जेएमजीएस-I**)	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/एम.एससी. (कम्प्यूटर साइंस)		एप्लिकेशन डेव्लपमेंट एप्लिकेशन (एप्लिकेशन/सॉफ्टवेयर की कोडिंग, टेस्टिंग तथा मेन्टेनैन्स) का अनुभव. नेट/एंगुलर JS/कोर JAVA/DB2 SQL-PL SQL/IBM वेबस्फेर MQ/J2EE/ओराकल 11g/ओराकल ADF/PHP/R प्रोग्रामिंग/SAP ABAP/वेबसर्विस के ठोस ज्ञान को प्राथमिकता दी जाएगी.
2.	**डेव्लपर (एमएमजीएस-II)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/एम.एससी. (कम्प्यूटर साइंस)		न्यूनतम अर्हता के पश्चात नेट/एंगुलर JS/कोर JAVA/DB2 SQL-PLSQL/IBM वेबस्फेर MQ/J2EE/ओराकल 11g/ओराकल ADF/PHP/R प्रोग्रामिंग/SAP ABAP/ वेबसर्विस का ठोस ज्ञान में कम से कम 5 वर्षों का अनुभव
3.	**सिस्टम/सर्वर एडमिनिस्ट्रेटर (जेएमजीएस-I)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/एम.एससी. (कम्प्यूटर साइंस)		न्यूनतम अर्हता के पश्चात आईटी सेक्टर में सिस्टम/सर्वर एडमिनिस्ट्रेशन के अनुभव को प्राथमिकता दी जाएगी. **अपेक्षित विशेष कौशल:** • नेट/AIX/IBM का ठोस ज्ञान • वेबस्फोर/LINUX/UNIX सर्वर/MCSA/ओराकल का ठोस ज्ञान अपेक्षित • वेबलॉजिक/RED HAT/विंडो सर्वर को प्राथमिकता
4.	**डेटाबेस एडमिनिस्ट्रेटर (जेएमजीएस-I)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/एम.एससी. (कम्प्यूटर साइंस)		न्यूनतम अर्हता के पश्चात आईटी सेक्टर में प्राधिमानत: डेटाबेस एडमिनिस्ट्रेशन को प्राथमिकता दी जाएगी. **अपेक्षित विशेष कौशल:** • ओराकल प्रमाणित प्रोफेशनल्स • DB2 डेटाबेस/HADOOP/MS SQL सर्वर/ओराकल DBA के ठोस ज्ञान को प्राथमिकता दी जाएगी
5.	**क्लाउड एडमिनिस्ट्रेटर (जेएमजीएस-I)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)		न्यूनतम अर्हता के पश्चात आईटी सेक्टर में प्राधिमानत: क्लाउड में अनुभव को प्राथमिकता दी जाएगी. **अपेक्षित विशेष कौशल:** • VMWARE ESX/क्लाउड कम्प्यूटिंग में ठोस ज्ञान को प्राथमिकता दी जाएगी.
6.	**नेटवर्क इंजीनियर (जेएमजीएस-I)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/एम.एससी (कम्प्यूटर साइंस)		न्यूनतम अर्हता के पश्चात आईटी सेक्टर में प्राधिमानत: बड़े कॉर्पोरेट नेटवर्क या बैंकिंग नेटवर्क के संचालन को प्राथमिकता दी जाएगी. • NET/नेटवर्क सिक्योरिटी/नेटवर्किंग कॉन्सेप्ट/सिस्को सर्टिफाइड नेटवर्क एसोशिएट (CCNA) के साथ राउटिंग, स्विचिंग प्रोटोकॉल, नेटवर्किंग डिवाइसेस के ठोस एनालिटिकल और ट्रबलशूटिंग कौशल को प्राथमिकता दी जाएगी.
7.	**टेस्टर (जेएमजीएस-I)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/एम.एससी. (कम्प्यूटर साइंस)		न्यूनतम अर्हता के पश्चात आईटी टेस्टिंग के अनुभव को प्राथमिकता दी जाएगी. • मैनुअल टेस्टर/एचपी क्विक टेस्ट प्रोफेशनल (QTP)/रिग्रेसन टेस्टर को प्राथमिकता दी जाएगी
8.	**डब्ल्यूएस एडमिनिस्ट्रेटर (एमएमजीएस-II)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)	**अधिमान्य:** सीआईएसए और सीआईएसएम प्रमाणन	न्यूनतम अर्हता के बाद आईटी बिजनेस/इंडस्ट्री में कम से कम 5 वर्षों का अनुभव, जिनमें से 2 वर्ष का व्यापक अनुभव WAS, HIS, Unix, AIX एन्वायरमेंटन्ट्स के प्रबंधन में रहे हो. **अपेक्षित विशेष कौशल:** • J2EE, IHS वेब सर्वर, वेबस्फेर एप्लिकेशन सर्वर, SSL, SOA, यूनिक्स शेल, पायथॉन तथा पर्ल आदि की जानकारी. • AIX पर यूनिक्स एडमिनिस्ट्रेशन कौशल. • IBM MQ सर्वर्स, ओराकल/SQL/DB2 सर्वर्स तथा XML, XSL और WSDL की जानकारी. • वेब तथा एप्लिकेशन सर्वर्स, वर्कफ्लो इंफ्रास्ट्रक्चर की जानकारी. • बिजनेस/ऑर्गेनाइजेशन, बैंक स्टैण्डर्ड्स, इंफ्रास्ट्रक्चर, आर्किटेक्चर तथा डिजाइन/सपोर्ट/ सॉल्यूशन्स की दृष्टि से संबंधित क्षेत्रों में टेक्नोलॉजी का कुछ ज्ञान. • ऐसे वातावरण में काम करने के लिए सहज हो, जहां मल्टीटास्किंग का उच्च स्तर मापदंड है.
9.	**इंफ्रास्ट्रक्चर इंजीनियर (एमएमजीएस-II)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस).		न्यूनतम अर्हता के पश्चात आईटी सेक्टर में वेबलॉजिक, सोलारिस/LINUX/UNIX/AIX आदि पर वेबसर्वर के इंस्टॉलेशन/माइग्रेशन/अप–ग्रेडेशन में कम से कम 5 वर्षों का अनुभव. **अपेक्षित विशेष कौशल:** वेबलॉजिक, सोलारिस/LINUX/UNIX/AIX आदि के इंस्टॉलेशन/माइग्रेशन/अप–ग्रेडेशन में अनुभव
10.	**यूएक्स डिजाइनर (एमएमजीएस-II)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)		न्यूनतम अर्हता के पश्चात आईटी सेक्टर में UX डिजाइन व डेव्लपमेंट/फोटोशॉप/कोर जावा में कम से कम 5 वर्षों का अनुभव **अपेक्षित विशेष कौशल:** UX डिजाइन व डेव्लपमेंट/फोटोशॉप/कोर जावा में अनुभव.

11.	**आईटी जोखिम प्रबंधक (एमएमजीएस-II)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)		आईटी सेक्टर में कम से कम 5 वर्षों का अनुभव, जिनमें से कम से कम 2 वर्षों का अनुभव रिस्क मैनेजमेंट में होना चाहिए. **अपेक्षित विशेष कौशल:** • रिस्क मैनेजमेंट के सभी पहलुओं में विशेषज्ञता, जिनमें शामिल हैं आइडेन्टिफिकेशन, एनालिसिस, मिटिगेशन, रिपोर्टिंग, अवेयरनेस, इन्सिडेंट मैनेजमेंट तथा रेस्पॉन्स, GRC, ऑडिट और कॉम्प्लाएन्स. • बिजनेस तथा आईटी प्रोसेसेस, BCP/DR, प्रोजेक्ट्स आदि के जोखिम आकलन का ज्ञान और उनके लिए उपयुक्त निराकरण प्लान्स. • प्रोफेशनल रिस्क/सिक्योरिटी सर्टिफिकेशन जैसे कि CRISC, CISSP, CISA,CISM को प्राथमिकता दी जाएगी. • ISO27001/2, FFIEC तथा COBIT संबधित सिक्योरिटी ढांचे का ज्ञान अनिवार्य. • वित्तीय सेवा संगठनों की मौजूदा कानूनी अपेक्षाओं की गहरी समझ होनी चाहिए. • इंफ्रास्ट्रक्चर, नेटवर्किंग, सिक्योरिटी तथा सॉफ्टवेयर डेव्लपमेंट प्रोसेसेस की जानकारी. • नेटवर्क तथा इंफ्रास्ट्रक्चर आर्किटेक्चर और सिक्योरिटी (नेटवर्क सेग्मेन्टेशन कॉन्सेप्ट्स, फायरवॉल्स, राउटर्स VPN सॉल्यूशन्स इत्यादि) • सिस्टम डेव्लपमेंट (SDLC, प्रोजेक्ट मैनेजमेंट तथा चेंज कंट्रोल्स प्रविधिया आदि.). • फिजिकल सिक्योरिटी व डेटा सेन्टर एन्वायरमेन्टल कंट्रोल्स. • हॉस्टेड व विंडोज एन्वायरमेंट्स, क्लाइंट सर्वर टेक्नोलॉजी, नेटवर्क्स, फायरवॉल्स, SIEM और ई-कॉमर्स सिक्योरिटी रिस्क्स का ज्ञान. • GRC मैनेजमेंट एप्लिकेशन के इस्तेमाल में अनुभव; RSA-आर्चर एप्लिकेशन का अनुभव.
12.	**आईटी सुरक्षा विशेषज्ञ (एमएमजीएस-III)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)	**अनिवार्य:** सीआईएसए प्रमाणन	आईटी में न्यूनतम अर्हता के बाद कम से कम 8 वर्षों का अनुभव जिनमें से कम से कम 5 वर्षों का अनुभव आईटी सिक्योरिटी में होना चाहिए. **अपेक्षित विशेष कौशल:** • रिस्क एसेसमेंट, आईटी सिक्योरिटी, आईटी प्रोडक्शन, आईटी एप्लिकेशन या आईटी ऑपरेशन्स फोकस्ड कंट्रोल फंक्शन्स में व्यावहारिक अनुभव. • बड़े कॉर्पोरेशन/BFSI में अनुभव को प्राथमिकता.
13.	**परियोजना प्रबंधक (एमएमजीएस-III)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)	**अनिवार्य** पीएमआई से प्रमाणन **अधिमान्य:** प्रतिष्ठित संस्थान से एमबीए	न्यूनतम अर्हता के पश्चात आईटी बिजनेस/इंडस्ट्री में कम से कम 8 वर्षो का अनुभव, जिसमें से कम से कम 5 वर्षों का अनुभव प्लानिंग, डेव्लपमेंट रणनीतियों/पहलकारी कदमों तथा प्रोडक्ट लाइफसाइकिल/सर्विस ओरिएन्टेशन पर केन्द्रित बिल्डिंग व लीडिंग हाई-परफॉर्मिंग एजाइल टीम का हो. **अपेक्षित विशेष कौशल:** प्लानिंग, डेव्लपमेंट रणनीतियों/पहलकारी कदमों तथा प्रोडक्ट लाइफसाइकिल/सर्विस ओरिएन्टेशन पर केन्द्रित बिल्डिंग व लीडिंग हाई-परफॉर्मिंग एजाइल टीम में अनुभव.
14.	**एप्लिकेशन आर्किटेक्ट (एमएमजीएस-III)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)		न्यूनतम अर्हता के पश्चात आईटी बिजनेस/इंडस्ट्री में कम से कम 8 वर्षो का अनुभव, जिसमें से कम से कम 3 वर्षों का अनुभव ई-चैनल्स (जैसे कि INB, ATM, मोबाइल आदि) में एप्लिकेशन तथा मिडलवेयर आर्किटेक्ट के रूप में हो. **अपेक्षित विशेष कौशल:** • ई-चैनल्स (जैसे कि INB, ATM, मोबाइल आदि) में एप्लिकेशन तथा मिडलवेयर आर्किटेक्ट के रूप में अनुभव. • AGILE प्रविधि/कोर JAVA/IBM वेबस्फेर MQ/LINUX/UNIX सर्वर में अनुभव को प्राथमिकता.
15.	**टेक्निकल लीड (एमएमजीएस-III)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)		न्यूनतम अर्हता के पश्चात आईटी बिजनेस/इंडस्ट्री में मोबाइल का ई-चैनल सॉफ्टवेयर डेव्लपमेंट लाइफसाइकिल के डेव्लपमेंट डेव्लपमेंट, टेस्टिंग तथा सपोर्ट में कम से कम 8 वर्षों का अनुभव **अपेक्षित विशेष कौशल:** • मोबाइल या ई-चैनल सॉफ्टवेयर डेव्लपमेंट लाइफसाइकिल के डेव्लपमेंट, टेस्टिंग तथा सपोर्ट में अनुभव • स्क्रम/क्लाउड कम्प्यूटिंग/जेन्किन्स का ठोस ज्ञान
16.	**इंफ्रास्ट्रक्चर आर्किटेक्ट (एमएमजीएस-III)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)		न्यूनतम अर्हता के बाद बड़े आईटी इंफ्रास्ट्रक्चर प्रोजेक्ट्स की डिजाइनिंग और बिल्डिंग में कम से कम 8 वर्षों काअनुभव. **अपेक्षित विशेष कौशल:** • हार्डवेयर, वर्च्युलाइजेशन तथा मिडलवेयर लेयर्स दोनों से युक्त बड़े आईटी इंफ्रास्ट्रक्चर प्रोजेक्ट्स की डिजाइनिंग तथा बिल्डिंग में अनुभव. • OS/(Unix), मिडलवेयर, स्टोरेज, लोड बैलेन्सर पर प्रोफेशनल सर्टिफिकेशन्स वाले अभ्यर्थियों को प्राथमिकता.
17.	**इंफ्रास्ट्रक्चर इंजीनियर (जेएमजीएस-I)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)		न्यूनतम योग्यता के पश्चात आईटी क्षेत्र में बेवलॉजिक, वेबसर्वर ऑन सोलारिस/LINUX/UNIX/AIX आदि के इंस्टॉलेशन/माइर्गेशन/अप-ग्रेडेशनम में अनुभव रखने वालों को प्राथमिकता दी जाएगी.
18.	**आईटी सुरक्षा विशेषज्ञ (जेएमजीएस-I)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)	**अधिमान्य:** सीआईएसएसपी/सीआईएसएम/ सीआईएसए प्रमाणन.	आईटी क्षेत्र में अनुभव, जिसमें से आईटी सिक्योरिटी में 2 वर्षों का अनुभव रखने वालों को प्राथमिकता दी जाएगी. **अपेक्षित विशेष कौशल:** • रिस्क एसेसमेंट, आईटी सिक्योरिटी, आईटी प्रोडक्शन, आईटी एप्लिकेशन्स या आईटी ऑपरेशन्स फोकस्ड कंट्रोल फंक्शन्स में व्यवहारिक अनुभव • बड़े कॉर्पोरेशन/बीएफएसआई में अनुभव रखने वालों को प्राथमिकता दी जाएगी.
19.	**आईटी सुरक्षा विशेषज्ञ (एमएमजीएस-II)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)	**अधिमान्य:** सीआईएसएसपी/सीआईएसएम/ सीआईएसए प्रमाणन	आईटी क्षेत्र में कम से कम 5 वर्षों का अनुभव, जिसमें से कम से कम 2 वर्ष का अनुभव आईटी सिक्योरिटी में हो. **अपेक्षित विशेष कौशल :** • रिस्क एसेसमेंट, आईटी सिक्योरिटी, आईटी प्रोडक्शन, आईटी एप्लिकेशन्स या आईटी ऑपरेशन्स फोकस्ड कंट्रोल फंक्शन में व्यवहारिक अनुभव • बड़े कॉर्पोरेशन/बीएफएमआई में अनुभव रखने वालों को प्राथमिकता दी जाएगी.

20.	**आईटी जोखिम प्रबंधक (आईएस डिपार्टमेंट) (एमएमजीएस-II)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)		न्यूनतम अर्हता के पश्चात आईटी क्षेत्र में कम से कम 5 वर्षों का अनुभव, जिसमें से कम से कम 2 वर्षों का अनुभव आईटी रिस्क मैनेजमेन्ट में हो. **अपेक्षित विशेष कौशल:** • रिस्क मैनेजमेंट के सभी पक्षों में विशेषज्ञता, जिसमें शामिल है आइडेन्टिफिकेशन, एनालिसिस, मिटिगेशन, रिपोर्टिंग, अवेयरनेस, इंसिडेन्ट मैनेजमेंट और रेस्पॉन्स, जीआरसी, ऑडिट तथा कॉम्प्लाएन्स • बिजनेस और आईटी प्रोसेसेस, बीबीपी/डीआर, प्रोजेक्ट्स आदि के रिस्क एसेसमेंट का ज्ञान और उसके लिए उचित समाधान प्लान्स विकसित करने का ज्ञान. • प्रोफेशनल रिस्क/सिक्योरिटी सर्टिफिकेशन जैसे कि सीआरआईएससी, सीआईएसएसपी, सीआईएसए, सीआईएसएम को प्राथमिकता दी जाएगी. • ISO 27001/2, FFIEC और COBIT संबंधित सिक्योरिटी फ्रेमवर्क्स का ज्ञान अनिवार्य है. • वित्तीय सेवाएं संगठनों के लिए मौजूदा कानूनी अपेक्षाओं की ठोस जानकारी अनिवार्य है. • इंफ्रास्ट्रकक्चर, नेटवर्किंग, सिक्योरिटी तथा सॉफ्टवेयर डेव्लपमेंट प्रकियाओं की जानकारी • नेटवर्क तथा इंफ्रास्ट्रक्चर आर्किटेक्चर व सिक्योरिटी (नेटवर्क सेग्मेन्टेशन कॉप्सेप्ट्स, फायरवॉल्स, राउटर्स, वीपीएन सॉल्यूशन आदि) • सिस्टम्स डेव्लपमेंट (एसडीएलसी, प्रोजेक्ट मैनेजमेंट तथा चेंज कंट्रोल मेथोडोलॉजिस सहित) • फिजिकल सिक्योरिटी व डेटा सेंटर एन्वायरमेंटल कंट्रोल्स • होस्टेड व विंडोज एन्वायरमेंट्स, क्लाइंट सर्वर टेक्नोलॉजी, नेटवर्क्स, फायरवॉल्स, एसआईईएम तथा ई-कॉमर्स सिक्योरिटी रिस्क्स आदि का ज्ञान • जीआरसी मैनेजमेंट एप्लिकेशन्स के इस्तेमाल का अनुभव; आरएसए-आर्चर एप्लिकेशन का अनुभव
21.	**इंफ्रास्ट्रक्चर आर्किटेक्ट (एमएमजीएस -II)**	किसी मान्यताप्राप्त विश्वविद्यालय/संस्थान से कम्प्यूटर साइंस/आईटी/ईसीई में इंजीनियरिंग स्नातक या एमसीए/एम.एससी. (आईटी)/ एम.एससी. (कम्प्यूटर साइंस)		न्यूनतम अर्हता के पश्चात बड़े आईटी इंफ्रास्ट्रक्चर प्रोजेक्ट्स की डिजाइनिंग और निर्माण में कम से कम 5 वर्षों का अनुभव **अपेक्षित विशेष कौशल:** • बड़े इंफ्रास्ट्रक्चर प्रोजेक्ट्स का डिजाइनिंग और निर्माण का अनुभव, जिसमें हार्डवेयर, वर्च्युलाइजशन और मिडलवेयर लेयर्स, दोनों शामिल है. • ओएस (Unix), मिडलवेयर, स्टोरेज, लोड बैलेन्सर पर प्रोफेशनल सर्टिफिकेशन रखने वाले अभ्यर्थियों को प्राथमिकता दी जाएगी.
22.	**उप प्रबंधक (साइबर सिक्योरिटी-एथिकल हैकिंग) (एमएमजीएस-II)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/ इंफॉर्मेशन टेक्नोलॉजी/इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स व टेलीकम्यूनिकेशन्स/ इलेक्ट्रॉनिक्स व कम्यूनिकेशन्स/इलेक्ट्रॉनिक्स व इंस्ट्रूमेन्टेशन्स में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीए	**अनिवार्य:** सर्टिफाइड एथिकल हैकर (सीईएच) **प्राथमिकता:** एसएएनएस जीआईएसी सर्टिफिकेशन्स/ ऑफेन्सिव सिक्योरिटी सर्टिफाइड प्रोफेशनल (ओएससीपी)/ ईसी-काउन्सिल सर्टिफाइड सिक्योरिटी एनालिस्ट (ईसीएसए) लाइसेंस्ड पेनिट्रेशन टेस्टर (एलपीटी)	न्यूनतम अर्हता के पश्चात सायबर सिक्योरिटी में कम से कम 5 वर्षों का अनुभव. 5 वर्षों के अनुभव में से कम से कम तीन (3) वर्ष एथिकल हैकिंग/एप्लिकेशन या मोबाइल सिक्योरिटी टेस्टिंग/रेड टीम एक्सरसाइजेज में हो. **अपेक्षित विशेष कौशल:** • वेब एप्लिकेशन सिक्योरिटी टेस्टिंग, मोबाइल एप्प सिक्योरिटी टेस्टिंग,नेटवर्क,सिस्टम व एप्लिकेशन वल्नेराबिलिटी एसेसमेन्ट व पेनिट्रेशन टेस्टिंग, आईसीएस/एलओटी डिवाइस सिक्योरिटी टेस्टिंग तथा रेड टीम एक्सरसाइजेज में अनुभव. • वेब एप्लिकेशन सिक्योरिटी की समस्याओं, जैसे कि जिनका उल्लेख ओडब्ल्यूएएसपी टॉप 10 अटैक्स में किया गया है, के समाधान में व्यापक अनुभव. • सॉफ्टवेयर लाइफसायकल तथा डेवसेक्ऑप्स में एप्लिकेशन सिक्योरिटी का ठोस ज्ञान • कॉमन एप्लिकेशन, नेटवर्क सिक्योरिटी टूल्स जैसे कि ओपन सोर्स या कमर्शियल टेस्टिंग टूल्स जैसे कि काली Linux, मेटास्प्लॉइट, बर्प सूट, फॉर्टिफाई, एप्पस्कैन, वेबल्न्स्पेक्ट आदि के साथ काम करने का अनुभव • विभिन्न स्क्रिप्टिंग लैग्वेजेज जैसे कि पायथॉन, पर्ल, बैश आदि का इस्तेमाल • अतिउत्तम मौखिक, एनालिटिकल तथा लिखित संचार कौशल
23.	**उप प्रबंधक (सायबर सिक्योरिटी-थ्रेड हन्टिंग) (एमएमजीएस-II)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/इंफॉर्मेशन टेक्नोलॉजी/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स व टेलीकम्यूनिकेशन्स/इलेक्ट्रॉनिक्स व कम्यूनिकेशन्स/इलेक्ट्रॉनिक्स व इंस्ट्रूमेन्टेशन्स में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/एम.एससी. (आईटी)/एमसीए	**अधिमान्य:** सर्टिफाइड थ्रेट इंटेलिजेंस एनालिस्ट (सीटीआईए)/घटना पर प्रतिक्रिया और जोखिम के क्षेत्रों पर एसएएनएस जीआईएसी प्रमाणन/सर्टिफाइड इन्फॉर्मेशन सिस्टम्स सिक्योरिटी प्रोफेशनल (सीआईएसएसपी)	न्यूनतम अर्हता के पश्चात सायबर सिक्योरिटी में कम से कम 5 वर्षों का अनुभव. 5 वर्षों के अनुभव में से कम से कम दो (2) वर्ष थ्रेट हंटिंग/मलवेयर एनालिसिस तथा रिवर्स इंजीनियरिंग में होने चाहिए **अपेक्षित विशेष कौशल:** • नियमित आधार पर थ्रेट हंटिंग करना • जांच और एनालिसिस कार्य के लिए आवश्यकता अनुसार मलवेयर पर रिवर्स इंजीनियरिंग करना • संदिग्ध बायनरीज को कैरेक्टेरासज करना तथा ट्रेट्स, C2 की पहचान करने में समर्थ होना एवं नेटवर्क तथा होस्ट -आधारित IOCs विकसित करना. • मेमरी डम्प्स, लॉग्स तथा पॉकेट कैप्चर्स से संभावित दुभावनापूर्ण गतिविधि की पहचान करना • थ्रेट हंटिंग के लिए स्क्रिप्टिंग लिखना. • अतिउत्तम मौखिक, एनालिटिकल तथा लिखित संचार कौशल
24.	**उप प्रबंधक (सायबर सिक्योरिटी-डिजिटल फॉरेन्सिक) (एमएमजीएस-II)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/इंफॉर्मेशन टेक्नोलॉजी/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स व टेलीकम्यूनिकेशन्स/इलेक्ट्रॉनिक्स व कम्यूनिकेशन्स/इलेक्ट्रॉनिक्स व इंस्ट्रूमेन्टेशन्स में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीए	**अनिवार्य:** ईसी-काउंसिल से कंप्यूटर हैकिंग फोरेंसिक इनवेस्टिगेटर (सीएचएफआई)/एनकेस सर्टिफाइड एक्जामिनर (एनसीई) **अधिमान्य:** सर्टिफाइड थ्रेट इंटेलिजेंस एनालिस्ट (सीटीआईए)/घटना पर प्रतिक्रिया और जोखिम के क्षेत्रों पर एसएएनएस जीआईएसी प्रमाणन/सर्टिफाइड इन्फॉर्मेशन सिस्टम्स सिक्योरिटी प्रोफेशनल (सीआईएसएसपी)	न्यूनतम अर्हता के पश्चात सायबर सिक्योरिटी में कम से कम 5 वर्षों का अनुभव. 5 वर्षों के अनुभव में से कम से कम 3 वर्षों का अनुभव डिजिटल फॉन्सिक एनालिसिस में होना चाहिए. **अपेक्षित विशेष कौशल:** • डिजिटल फारेन्सिक एनालिसिस तथा फॉरेन्सिक टूल्स (कमर्शियल व ओपन सोर्स टूल्स) जैसे कि एन्कैश फॉरेन्सिक टूल किट्स (एफटीके) आदि में अनुभव • डिजिटल तथा अन्य एविडेन्सेस की फॉरेन्सिक परीक्षा करना तथा फॉरेन्सिक जांचों के लिए इंसिडेन्ट्स को एनालाइज करने की क्षमता. • नेटवर्क, सिस्टम्स, एप्लिकेशन्स, मोबाइल एप्स आदि की सिक्योरिटी पर ठोस तकनीकी ज्ञान • अतिउत्तम मौखिक, एनालिटिकल तथा लिखित संचार कौशल

25.	**सिक्योरिटी एनालिस्ट (एमएमजीएस-III)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/ इंफॉर्मेशन टेक्नोलॉजी/इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स व टेलीकम्यूनिकेशन्स/ इलेक्ट्रॉनिक्स व कम्यूनिकेशन्स/इलेक्ट्रॉनिक्स व इंस्ट्रूमेन्टेशन्स में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीए	**अनिवार्य:** • सीईएच **अधिमान्य:** • सीआईएसएसपी/सीआईएसए/ सीआईएसएम • एसआईईएम/यूईबीए/ एसओएआर/वीएम/डीएएम/ पीसीएपी/एनबीए जैसे ओईएम से एसओसी सिक्योरिटी टेक्नोलॉजी सर्टिफिकेशन	न्यूनतम अर्हता के पश्चात आईटी/आईटी सिक्योरिटी/इफॉर्मेशन सिक्योरिटी में कम से कम 7 वर्षों का अनुभव जिसमें से कम से कम 2 वर्ष एसओसी ऑपरेशन्स में हो. • सिक्योरिटी टेक्नोलॉजी और सॉल्यूशन्स में अनुभव (कम से कम एक अनिवार्य है) • एसआईईएम–इवेन्ट एनालिसिस, रूल क्रिएशन, ऑटोमेशन, एसेट इंटिग्रेशन • वल्नेराबिलिटी मैनेजमेंट तथा पेनिट्रेशन टेस्टिंग ओडब्ल्यूएएसपी वल्नेराबिलिटीज तथा एप्लिकेशन सिक्योरिटी रिस्क्स • यूजर तथा नेटवर्क विहेवियर एनालिसिस, पैकेट–कैप्चर व पैकेट फ्लोज़ एनालिसिस • डेटाबेस एक्टिविटी मॉनिटरिंग सिक्योरिटी पॉलिसी क्रिएशन्स तथा डेटाबेस इंटिग्रेशन • लॉग्स डिकोडिंग/पार्सिंग तथा कोरिलेशन टेक्नीक्स, कोरिलेशन क्रॉस–आईटी टेक्नोलॉजिस लॉग्स, उपरोक्त एसओसी टेक्नोलॉजिस के डिप्लायमेंट की विधियों, एसओपी टेक्नेलॉजिस के सब–कंपोनेंट्स, डैश–बोर्डिंग, एसओपी, एसओसी टेक्नोलॉजिस से लॉग्स का प्रत्येक अन्य 360 डिग्री कोरिलेशन में इन्जेस्चन, आईओसीएस के लिए थ्रेट हन्टिंग तथा थ्रेट इंटिलिजेन्स, डेटा माइनिंग आदि की लेवरेजिंग आदि की गहरी जानकारी • आईटी इंफ्रास्ट्रक्चर टेक्नोलॉजिस तथा आर्किटेक्चर की समझ ताकि इसका इस्तेमाल एसओसी फाइन–टूनिंग के लिए किया जा सके. • आईटी सिक्योरिटी टेक्नोलॉजिस जैसे कि फायरवॉल्स, IPS, WAF, AV, AD, DLP, LB, PIMS, ITAM, IAM, RASP, VPN, Anti-APT और नेटवर्किंग प्रोटोकॉल्स तथा टेक्नोलॉजियों जैसे कि राउटर्स, स्विचेज, SDN का ज्ञान ताकि कोरिलेशन के लिए इनका इस्तेमाल किया जा सके. • उभरती टेकनोलॉजियों जैसे कि AI/ML, ब्लॉकचेन, RPA, IOT, क्लाउड का ज्ञान • डिजिटल फॉरेन्सिक जांच • सिस्टम एडमिन नॉलेज (विंडोज/Linux) • प्रोग्रामिंग का ज्ञान–पायथॉन/पर्ल/शेल/PHP
26.	**प्रबंधक (सायबर सिक्योरिटी–एथिकल हैकिंग (एमएमजीएस-III)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/इंफॉर्मेशन टेक्नोलॉजी/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स व टेलीकम्यूनिकेशन्स/इलेक्ट्रॉनिक्स व कम्यूनिकेशन्स/इलेक्ट्रॉनिक्स व इंस्ट्रूमेन्टेशन्स में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीए	**अनिवार्य:** ऑफेंसिव सिक्योरिटी सर्टिफाइड प्रोफेशनल (ओएससीपी)/सर्टिफाइड इन्फॉर्मेशन सिस्टम्स सिक्योरिटी प्रोफेशनल (सीआईएसएसपी)/ एप्लिकेशन पर एसएएनएस जीआईएसी प्रमाणन/मोबाइल/नेटवर्क सिक्योरिटी असेसमेंट या टेस्टिंग एरियाज **अधिमान्य:** ऑफेंसिव सिक्योरिटी सर्टिफाइड प्रोफेशनल (ओएससीपी)/ ईसी–काउंसिल सर्टिफाइड सिक्योरिटी एनालिस्ट (ईसीएसए)/लाइसेंस्ड पेनिट्रेशन टेस्टर (एलपीटी)	न्यूनतम अर्हता के पश्चात कम से कम सायबर सिक्योरिटी में 7 वर्षों का अनुभव. 7 वर्षों के इस अनुभव में से कम से कम तीन (3) वर्ष एथिकल हैकिंग/एप्लिकेशन या मोबाइल सिक्योरिटी टेस्टिंग/रेड टीम एक्सरसाइजेज में होने चाहिए **अपेक्षित विशेष कौशल:** • वेब एप्लिकेशन सिक्योरिटी टेस्टिंग, मोबाइल एप्प सिक्योरिटी टेस्टिंग, नेटवर्क, सिस्टम तथा एप्लिकेशन वल्नेराबिलिटी एसेसमेंट व पेनिट्रेशन टेस्टिंग, आईसीएस/IOT डिवाइस सिक्योरिटी टेस्टिंग में अनुभव • वेब एप्लिकेशन सिक्योरिटी की समस्याओं, जैसे कि जिनका उल्लेख ओडब्ल्यूएएसपी टॉप 10 अटैक्स में किया गया है, के समाधान का व्यापक ज्ञान सॉफ्टवेयर लाइफसायकिल तथा डेवसेक्ऑप्स में एप्लिकेशन सिक्योरिटी का ठोस ज्ञान • कॉमन एप्लिकेशन, नेटवर्क सिक्योरिटी टूल्स जैसे कि ओपन सोर्स या कमर्शियल टेस्टिंग टूल्स जैसी कि काली Linux, मेटास्प्लॉइट, बर्प सूट, फॉर्टिफाई, एप्पस्कैन, वेबल्न्स्पेक्ट आदि के साथ काम करने का अनुभव • विभिन्न स्क्रिप्टिंग लैग्वेजेज जैसे कि पायथॉन, पर्ल, बैश आदि का इस्तेमाल • इंफॉर्मेशन तथा सायबर सिक्योरिटी डोमेन में ठोस पृष्टभूमि के साथ विषयवस्तु की गहरी विशेषज्ञता/ज्ञान • एंटरप्राइज सिक्योरिटी आर्किटेक्चर तथा इंफॉर्मेशन/सायबर सिक्योरिटी क्षेत्रों जैसे कि आइडेंटिफाई तथा एक्सेस मैनेजमेंट, डेटा प्रोटेक्शन, वल्नेराबिलिटी मैनेजमेन्ट, एप्लिकेशन सिक्योरिटी, इंफ्रास्ट्रक्चर सिक्योरिटी तथा सिक्योरिटी मॉनिटरिंग और रेस्पॉन्स का अनुभव. • इंफॉर्मेशन तथा सायबर सिक्योरिटी में मुख्य विनियमों/विकासों की ताजा जानकारी • अतिउत्तम मौखिक, एनालिटिकल तथा लिखित संचार कौशल
27.	**प्रबंधक (सायबर सिक्योरिटी–डिजिटल फॉरेन्सिक) (एमएमजीएस-III)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/ इंफॉर्मेशन टेक्नोलॉजी/इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स व टेलीकम्यूनिकेशन्स/ इलेक्ट्रॉनिक्स व कम्यूनिकेशन्स/इलेक्ट्रॉनिक्स व इंस्ट्रूमेन्टेशन्स में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीए	**अनिवार्य:** ईसी–काउंसिल से कंप्यूटर हैकिंग फोरेंसिक इनवेस्टिगेटर (सीएचएफआई)/एनकेस सर्टिफाइड एक्जामिनर (एनसीई)/घटना की प्रतिक्रिया के क्षेत्र पर एसएएनएस जीआईएसी प्रमाणन **अधिमान्य** सर्टिफाइड इन्फॉर्मेशन सिस्टम्स सिक्योरिटी प्रोफेशनल (सीआईएसएसपी)	न्यूनतम अर्हता के पश्चात सायबर सिक्योरिटी में कम से कम 7 वर्षों का न्यूनतम अनुभव. 7 वर्षों के अनुभव में से कम से कम तीन (3) वर्ष डिजिटल फॉरेन्सिक एनालिसिस में होने चाहिए. **अपेक्षित विशेष कौशल** • डिजिटल फारेन्सिक एनालिसिस तथा फॉरेन्सिक टूल्स (कमर्शियल व ओपन सोर्स टूल्स) जैसे कि एन्कैश फॉरेन्सिक टूल किट्स (एफटीके) आदि में अनुभव • डिजिटल तथा अन्य एविडेन्स की फॉरेन्सिक परीक्षा करना तथा फॉरेन्सिक जांचों के लिए इंसिडेन्ट्स को एनालाइज करने की क्षमता. • नेटवर्क, सिस्टम्स, एप्लिकेशन्स, मोबाइल एप्स आदि की सिक्योरिटी पर ठोस तकनीकी ज्ञान • अतिउत्तम मौखिक, एनालिटिकल तथा लिखित संचार कौशल

28.	**मुख्य प्रबंधक (वल्नेराबिलिटी मैनेजमेंट एंड पैनिट्रेशन टेस्टिंग) (एसएमजीएस-IV)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/ इंफॉर्मेशन टेक्नोलॉजी में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीए	**अनिवार्य:** सीवीए/सीपीटी **अधिमान्य** सीपीईएन/ओएससीपी/ सीआईएसएम/सीआईएसएसपी/ सीआरआईएससी/जीपीईएन प्रमाणन वीएम, डीएएम, एसआईईएम जैसे ओईएम से एसओसी सिक्योरिटी टेक्नेलॉजी प्रमाणन	न्यूनतम अर्हता के पश्चात आईटी और आईटी/इंफॉर्मेशन सिक्योरिटी में कम से कम 9 वर्षों का अनुभव. 9 वर्षों के अनुभव में से कम से कम 5 वर्षों का अनुभव वल्नेराबिलिटी मैनेजमेंट व पेनिट्रेशन टेस्टिंग क्षेत्रों में होना चाहिए. • सरफेस, इंटूसिव तथा ऑफेन्सिव एक्सटर्नल व इंटरनल सिक्योरिटी टेस्टिंग जैसे कि वल्नेराबिलिटी एसेसमेंट, पेनिट्रेशन टेस्टिंग, एप्लिकेशन सिक्योरिटी टेस्टिंग, कोड रिव्यू तथा सिक्योरिटी कॉन्फिगुरेशन वेरिफिकेशन में ठोस अनुभव. • ग्लोबल सिक्योरिटी टेस्टिंग प्रैक्टिसेस, फ्रेमवर्क्स तथा मेथोडोलॉजिक्स पर आधारित आईटी इंफ्रास्ट्रक्चर, वेब एप्लिकेशन्स, मोबाइल प्लेटफॉर्म्स और क्लाउड प्लेटफॉर्म्स पर डीप वल्नेराबिलिटी एसेसमेंट व पेनिट्रेशन टेस्टिंग कौशल. • कमर्शियल, ओपन सोर्स सिक्योरिटी तथा एनालिसिस टूल्स (काली,मेटास्प्लॉइट, बर्प सूट, वायरशार्क, वेबइंस्पेक्ट, एचपी फॉर्टिफाई, एनमैप आदि) तथा कॉमन वल्नेराबिलिटी स्कैपिंग टूल्स (क्वॉलिस, नेसुस, एप्पस्कैन आदि) पर व्यावहारिक अनुभव • कॉमन वल्नेराबिलिटी फ्रेमवर्क्स (सीवीएसएस, ओडब्ल्यूएएसपी), एनवीडी तथा सीवीईएस का ठोस ज्ञान • स्क्रिप्टिंग ज्ञान: पायथॉन/बर्ल, शैल, बैश • इंफ्रास्ट्रक्चर आर्किटेक्चर डिजाइन, नेटवर्किंग तथा सॉफ्टवेयर आर्किटेक्चर, सिक्योरिटी और नेटवर्किंग प्रोटोकॉल्स का ठोस ज्ञान • सिस्टम, एप्लिकेशन तथा डेटाबेस हार्डनिंग टेक्नीक्स और बेस्ट प्रैक्टिसेस की अच्छी जानकारी • ओडब्ल्यूएएसपी टॉप 10 वल्नेराबिलिटीज़ जैसे कि एक्सएसएस, एसक्यूएल इंजेक्शन्स, सीएसआरएफ आदि की पहचान के लिए व्यवहारिक तकनीकों का इस्तेमाल करते हुए एप्लिकेशन सिक्योरिटी एसेसमेन्ट्स करने में अनुभव. **प्राथमिकता प्राप्त कौशल:** • डिजिटल तथा सायबर इकोसिस्टम, सोशियल इकोसिस्टम, प्लेटफॉर्म्स, ब्लॉकचेन, एआई/एमएल, आईओटी, क्लाउड आदि जैसे प्लेटफॉर्म्स के संचालन में अनुभव • रेड व ब्लू टीमिंग एक्टिविटीज तथा ईमेल फिशिंग अटैक सिमुलेटर्स/टूल्स • एनालिटिकल तथा संचार कौशल
29.	**मुख्य प्रबंधक (इन्सिडेंट मैनेजमेंट एंड फॉरेन्सिक्स) (एसएमजीएस-IV)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/ इंफॉर्मेशन टेक्नोलॉजी में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीए	**अनिवार्य:** • ईसी–काउंसिल से कंप्यूटर हैकिंग फोरेंसिक इनवेस्टिगेटर (सीएचएफआई)/एनकेस सर्टिफाइड एक्जामिनर (एनसीई)/डिजिटल फोरेंसिक्स पर एसएएनएस जीआईएसी सर्टिफिकेशन/घटना की प्रतिक्रिया के क्षेत्र पर एसएएनएस जीआईएसी प्रमाणन **अधिमान्य:** • ईसीआईएच/जीसीआईएच/ सीआईएसएसपी/सीआरआईएससी /सीआईएसए/सीआईएसएम प्रमाणन • डीएएम, एसआईईएम, यूईबीए, एसओएआर जैसे ओईएम से एसओसी सिक्योरिटी टेक्नोलॉजी प्रमाणन अधिमान्य होगा	न्यूनतम अर्हता के पश्चात आईटी/इंफॉर्मेशन सिक्योरिटी में कम से कम 9 वर्षों का अनुभव. 9 वर्षों के अनुभव में से कम से कम 5 वर्ष का अनुभव एसओसी इमेनेटिंग इंसिडेन्ट मैनेजमेंट तथा फॉरेन्सिक और एनालिसिस में होना चाहिए. • विभिन्न एसआईईएम/यूईबीए/डीएएम/एसओएआर/एनबीए/पीसीएपी प्लेटफॉर्म्स तथा इंसिडेन्ट मैनेजमेंट टूल्स पर कार्य अनुभव • ISO 27035, एनआईएसटी, आईटीआईएल तथा सीओबीआईटी फ्रेमवर्क्स से अच्छी तरह जानकार • आईटी तथा इंफॉर्मेशन सिक्योरिटी में इंसिडेंट मैनेजमेंट लाइफ साइकल में व्यावहारिक अनुभव • सायबर–अटैक किल चेन पर टेक्नोलॉजी तथा प्रोसेसेस की ठोस जानकारी, जिसमें शामिल है इनिशियल एक्सेस, एग्जिक्यूशन पर्सिसटेन्स, प्रिविलेज एसकेलेशन, डिफेन्स इवेशन, क्रिडेन्शियल एक्सेस, डिस्कवरी, लेटरल मूवमेंट, कलेक्शन कमाण्ड तथा कंट्रोल, एक्सफिल्ट्रेशन आदि. • इंसिडेंट एनालिसिस, रिकवरी तथा इंपैक्ट एनालिसिस सहित सायबर सिक्योरिटी इंसिडेंट रेस्पॉन्स में गहरा अनुभव. • आईटी एसेट्स के एसओसी के साथ इंटिग्रेशन, विभिन्न एसेट्स जैसे कि फायरवॉल्स, आईपीएस, डब्ल्यूएएफ, ओएस, आरडीबीएमएस, डीएलपी, एडी, एवी, लोड बैलेन्सर्स, आईटीएएम, पीआईएमएस, आईएम आदि के लॉग्स का कोरिलेशन तथा एनालिसिस. • विभिन्न एसआईईएम/यूईबीए/डीएएम/एसओएआर प्लेटफॉर्म्स तथा इंसिडेंट मैनेजमेंट टूल्स पर कार्य अनुभव • इंफ्रास्ट्रक्चर आर्किटेक्चर डिजाइन, नेटवर्किंग व सॉफ्टवेयर आर्किटेक्चर, विंडोज और UNIX ऑपरेटिंग सिस्टम्स, सिक्योरिटी तथा नेटवर्किंग प्रोटोकॉल्स का ठोस ज्ञान • उभरती टेक्नोलॉजियों और समकक्ष सिक्योरिटी थ्रेट्स की गहरी समझ **प्राथमिकता प्राप्त कौशल:** • विभिन्न आईटी सिक्योरिटी समाधानों जैसे कि एंटीवायरस, डीएलपी, डब्ल्यूएएफ, आईडीएस, आईपीएस/आईपीएस, पीआईएमएस, एंटी–एप्ट, ईडीआर सॉल्यूशन्स आदि में अनुभव • नेक्स्ट जेन एसओसी टेक्नोलॉजियों जैसे कि यूईबीए, एसओएआर, सिक्योर बिग डेटा लेक, थ्रेट इंटेल प्लेटफॉर्म्स रेड एंड ब्लू टीमिंग टूल्स में अनुभव • एनालिटिकल तथा संचार कौशल
30.	**मुख्य प्रबंधक (सिक्योरिटी एनालिटिक्स एंड ऑटोमेशन) (एसएमजीएस-IV)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/इंफॉर्मेशन टेक्नोलॉजी में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीएस	**अनिवार्य** • सीआईएसएसपी **अधिमान्य:** • सीआरआईएससी/सीआईएसए/ सीआईएसएम प्रमाणन • डीएएम, एसआईईएम, यूईबीए, एसओएआर जैसे ओईएम से एसओसी सिक्योरिटी टेक्नोलॉजी प्रमाणन अधिमान्य होगा.	न्यूनतम अर्हता प्राप्त करने के पश्चात आईटी/आईटी सिक्योरिटी/इंफॉर्मेशन सिक्योरिटी में कम से कम 9 वर्षों का अनुभव. 9 वर्षों के इस अनुभव में से कम से कम 5 वर्ष का अनुभव ऑटोमेशन तथा सिक्योरिटी एनालिटिक्स में होना चाहिए. • स्क्रिप्टिंग ज्ञान: पायथॉन/पर्ल. शैल/ बैश • विभिन्न आईटी तथा एसओसी सिस्टम्स के साथ एपीआई इंटिग्रेशन. • विभिन्न एसआईईएम/यूईबीए/सिक्योरिटी बिग डेटा लेक, एसओएआर प्लेटफॉर्म्स और इंसिडेंट मैनेजमेंट टूल्स • विभिन्न रोबोटिक्स प्रोसेस ऑटोमेशन (आरपीए) के फ्रेमवर्क्स, मशीन लर्निंग, पैटर्न एनालिसिस तथा एसओसी में मॉडलिंग/इंफॉर्मेशन सिक्योरिटी डोमेन. • डिजाइनिंग व कस्टमाइजिंग सिक्योरिटी इंसिडेंट प्लेबुक्स • दिन–प्रतिदिन के मैन्युअल ऑपरेशन्स का कस्टमाइजेशन तथा ऑटोमेटिंग जैसे कि एनालिटिक्स वर्कफ्लोज, इंसिडेंट रीमेडिएशन/रेस्पॉन्सेस का ऑटोमेशन, थ्रेट इंटेलिजेन्स का ऑपरेशनलाइजेशन आदि. • सिक्योरिटी एनालिटिक्स टूल्स तथा डिस्परेट डेटा सेट्स को इंटिग्रेट व कोरिलेट करने की टेक्नोलॉजियां • 2 या अधिकटूल्स व टेक्नोलॉजियों के आउटपुट का इस्तेमाल करते हुए सिक्योरिटी की कोरिलेटिंग तथा कॉन्टेक्स्टुलाइजिंग • रनबुक्स की रचना तथा उनकी इंसिडेन्ट रेस्पॉन्स वर्कफ्लोज पर मैपिंग • ऑटोमेशन तथा आर्केस्ट्रेशन प्लेटफार्म्स, सिक्योरिटी एनालिटिक्स के लिए एआई/एमएल टेक्नोलॉजियों का डिप्लॉयमेंट • उभरती टेक्नोलॉजिस जैसे कि ब्लॉकचेन, आईओटी/एआई/एमआई आदि समकक्ष सिक्योरिटी थ्रेट्स की गहरी समझ **प्राथमिकता प्राप्त कौशल:** • ओपन सोर्स एनालिटिकल टूल्स.

31.	**मुख्य प्रबंधक (एसओसी इंफ्रास्ट्रक्चर मैनेजमेंट) (एसएमजीएस-IV)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/ इंफॉर्मेशन टेक्नोलॉजी में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीए	**अनिवार्य:** • सीआईएसएसपी/आईटीआईएल एक्सपर्ट/प्रमाणित लीड इंप्लीमेंटर प्रोफेशनल **अधिमान्य:** • आईएसओ 27001 लीड ऑडिटर सर्टिफिकेशन	न्यूनतम अर्हता के पश्चात आईटी/आईटी सिक्योरिटी/ इंफॉर्मेशन सिक्योरिटी में कम से कम 9 वर्षों का अनुभव. 9 वर्षों के अनुभव में से कम से कम 5 वर्ष का अनुभव ऐंड टू ऐंड आईटी इंफ्रास्ट्रक्चर की मैनेजिंग में होना चाहिए. • एसओसी इंफ्रा मैनेजमेंट में ठोस अनुभव • एसओसी टेक्नोलॉजियों जैसे कि एसआईईएम, यूईबीए, एमओएआर, डीएएम, वीएम, थ्रेट इंटेलिजेन्स तथा सर्विसेस जैसे कि एंटी–फिशिंग, एक्सटर्नल पेनिट्रेशन टेस्टिंग की समझ • इंप्लिमेंटिंग पैचेज, एसओसी इंडिया सेट में वर्जन के अपग्रेडेशन के द्वारा सेटिंग्स/ हार्डनिंग के सिक्योर्ड कॉन्फिगुरेशन पर इंप्लिमेंटेशन, वल्नेराबिलिटीज की क्लोजिंग • ओएस, एप्लिकेशन्स, आरडीबीएमएस, वेब सर्वर, ओपन सोर्स टेक्नोलॉजियों का इंस्ट्रॉलेशन तथा कॉर्पोरेट की ज़रूरतों के अनुसार उन्हें कॉन्फिगर करना. • आईटी इंफ्रास्ट्रक्चर का पीआईएमएस, आईएम, एसएसओ, एडी, एवी, आईटीएएम, आईटीएसएम, डीएलपी, एनएसी के साथ इंटिग्रेशन • सिक्योरिटी टेक्नोलॉजियों जैसे कि फायरवॉल्स, आईपीएस, डब्ल्यूएएफ आदि डिप्लॉय करके आईटी इंफ्रास्ट्रक्चर की सिक्योरिटी • अपटाइम मैनेजमेंट, मैनेज एलएएन तथा कॉर्पोरेट नेटवर्क के साथ इंटिग्रेशन • क्रिडेन्शियल/यूजर मैनेजमेंट, रोल्स तथा ग्रुप्स मैनेजमेंट, आईटी/एसओसी इंफ्रास्ट्रक्चर पर एडमिनिस्ट्रेटिव गतिविधियों को पूरा करना • कई वेन्डर्स तथा ओईएम्स के साथ आईटी इंफ्रा संबंधित एसएलए मैनेजमेंट • बिजनेस निरंतरता और डीआर प्लान बनाना • सिक्योर्ड कम्यूनिकेशन, प्रोसेसिंग तथा डेटा के स्टोरेज के लिए एन्क्रिप्शन हैशिंग तकनीकों पर अमल • प्रमुख आईटी आर्किटेक्चर सिद्धान्तों जैसे कि क्लाइंट–सर्वर एप्लिकेशन्स, मल्टी–टियर वेब एप्लिकेशन्स, रिलेशनल और नॉन–रिलेशनल डेटाबेसेस, फायरवॉल्स, वीपीएन्स, आईपीएस की समझ • आमतौर पर इस्तेमाल किए जाने वाले इंटरनेट तथा नेटवर्किंग प्रोटोकॉल्स टीसीपी/आईपी एसएमटीपी, एचटीटीपी, एफटीपी, एसएनएमपी, पीओपी, एलडीएपी आदि की समझ • आईटी इंफ्रास्ट्रक्चर मैनेजमेंट क्लाउड मैनेजमेंट • पैचेस का रोल आउट, आईटी इंफ्रा पर बग फिक्सेस, बैकअप और रिकवरी, यूजर एक्सेस मैनेजमेंट, आईटी एसेट्स का विभिन्न सिक्योरिटी टेक्नोलॉजियों जैसे कि पीआईएमएस, आईएम, एडी, एवी, आईटीएसएम, आईटीएएम आदि के साथ इंटिग्रेशन **प्राथमिकता प्राप्त कौशल:** • एसओसी के लिए प्राइवेट क्लाउट या कोई मल्टीटेनेन्ट क्लाउड्स सेटअप करना या मैनेज करना • बिग डेटा लेक या सिक्योरिटी बिग डेटा लेक सेटअप करना या उसे मैनेज करना. • विभिन्न आईटी सिक्योरिटी सॉल्यूशन्स जैसे कि एंटीवायरस, डीएलपी, डब्ल्यूएएफ, आईडीएम/आईपीएस, पीआईएमएस, एंटी–एप्ट, ईडीआर सॉल्यूशन्स आदि में अनुभव.
32.	**मुख्य प्रबंधक (एसओसी गवर्नेन्स) (एसएमजीएस-IV)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/इंफॉर्मेशन टेक्नोलॉजी में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीए	**अनिवार्य:** • सीआईएसए **अधिमान्य:** • सीआईएसएसपी/आईएसओ 27001 लीड ऑडिटर सर्टिफिकेशन	न्यूनतम अर्हता पाने के पश्चात आईटी/आईटी सिक्योरिटी/इंफॉर्मेशन सिक्योरिटी में कम से कम 9 वर्षों का अनुभव. इस 9 वर्षों के अनुभव में से कम से कम 5 वर्ष का अनुभव एसओसी/इंफॉर्मेशन सिक्योरिटी गवर्नेन्स में होना चाहिए. • आईटी/एमओसी गवर्नेन्स में ठोस अनुभव • ISO 27001/27002, एनआईएसटी, आईटीआईएल तथा सीओबीआईटी फ्रेमवर्क्स की अच्छी जानकारी • एसओसी टेक्नोलॉजियों जैसे कि एसआईईएम, यूईबीए, एमओएआर, डीएएम, वीएम, थ्रेट इंटेलिजेन्स तथा सर्विसेस जैसे कि एंटी–फिनिश, एक्सटर्नल पेनिट्रेशन टेस्टिंग की समझ • एसओसी या समान एस्टाबिलशमेंट में इंफॉर्मेशन सिक्योरिटी पॉलिसी तथा प्रोसिजर्स, एसओपीज़ पर अमल • ISO27001 आईएसएमएस स्टैण्डर्ड्स पर अमल/ऑडिटिंग में व्यावहारिक अनुभव • पहचान, सुरक्षा, खोज, प्रतिसाद तथा पुन:प्राप्ति क्षेत्रों के लिए एनआईएसटी के साथ एलाइनिंग आईटी/इंफॉर्मेशन सिक्योरिटी ऑपरेशन्स पर व्यावहारिक अनुभव • पैच, वर्जन, यूजर एक्सेस तथा चेंज मैनेजमेंट रणनीतियों व तकनीकों, इ्यूटीज़ के सेग्रिगेशन, शिफ्ट मैनेजमेंट की पूरी समझ. • विभिन्न डोमेस्टिक तथा ग्लोबल वैधानिक व विनियामक रिपोर्टिंग • बिजनेस निरंतरता और डीआर प्लान बनाना • प्रमुख आईटी आर्किटेक्चर सिद्धान्तों जैसे कि क्लाइंट–सर्वर एप्लिकेशन्स, मल्टी–टियर वेब एप्लिकेशन्स, रिलेशनल और नॉन–रिलेशनल डेटाबेसेस, फायरवॉलल्स, वीपीएन्स, आईपीएस की समझ • सामान्य रूप से प्रयुक्त इंटरनेट और नेटवर्किंग प्रोटोकॉल्स टीसीपी/आईपी, एसएमटीपी, एचटीटीपी, एफटीपी, एसएनएमपी, पीओपी, एलडीएपी इ. की समझ **प्राथमिकता प्राप्त कौशल** डोमेस्टिक तथा फॉरेन डेटा सिक्योरिटी कानूनों और उनके अमल की गहरी समझ. सीओबीआईटी, एनआईएसटी, एचआईपीएए, पीसीआई टीएसएस,एंक्रिप्शन विधियां आदि
33.	**मुख्य प्रबंधक (सायबर सिक्योरिटी–एथिकल हैकिंग) (एसएमजीएस-IV)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/इंफॉर्मेशन टेक्नोलॉजी में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीए	**अनिवार्य:** ऑफेंसिव सिक्योरिटी सर्टिफाइड प्रोफेशनल (ओएससीपी)/सर्टिफाइड इन्फॉर्मेशन सिस्टम्स सिक्योरिटी प्रोफेशनल (सीआईएसएसपी)/ एप्लिकेशन पर एसएएनएस जीआईएसी प्रमाणन/मोबाइल/नेटवर्क सिक्योरिटी असेसमेंट या टेस्टिंग एरिया **अधिमान्य:** ऑफेंसिव सिक्योरिटी सर्टिफाइड एक्सपर्ट (ओएससीई)/ ईसी–काउंसिल सर्टिफाइड सिक्योरिटी एनालिस्ट (ईसीएसए)/लाइसेंस्ड पेनिट्रेशन टेस्टर (एलपीटी)	न्यूनतम अर्हता प्राप्त करने के पश्चात सायबर सिक्योरिटी में कम से कम 9 (नौ) वर्षों का अनुभव. इन 9 वर्षों में से कम से कम 5 वर्षों का अनुभव एथिकल हैकिंग/एप्लिकेशन या मोबाइल सिक्योरिटी टेस्टिंग/रेड टीम एक्सरसाइजेज में होना चाहिए **अपेक्षित विशेष कौशल :** • वेब एप्लिकेशन सिक्योरिटी टेस्टिंग, मोबाइल एप्प स्यिोरिटी टेस्टिंग, नेटवर्क, सिस्टम तथा एप्लिकेशन वल्नेराबिलिटी एसेसमेंट व पेनिट्रेशन टेस्टिंग, आईसीएस/IOT डिवाइस सिक्योरिटी टेस्टिंग, रेड टीम एक्सरसाइजेज में अनुभव. • वेब एप्लिकेशन सिक्योरिटी की समस्याओं,जैसे कि जिनका उल्लेख ओडब्ल्यूए एसपीटॉप 10 अटैक्स में किया गया है, के समाधान का व्यापक अनुभव. • सॉफ्टवेयर लाइफसायकिल तथा डेवसेक्ऑप्स में एप्लिकेशन सिक्योरिटी का ठोस ज्ञान • कॉमन एप्लिकेशन, नेटवर्क सिक्योरिटी टूल्स जैसे कि ओपन सोर्स या कमर्शियल टेस्टिंग टूल्स जैसे कि काली, Linux, मेटास्प्लॉइट, बर्प सूट, फॉर्टिफाई, एप्पस्कैन, वेबल्न्स्पेक्ट आदि के साथ काम करने का अनुभव • विभिन्न स्क्रिप्टिंग लैग्वेजेज जैसे कि पायथॉन, पर्ल, बैश आदि का इस्तेमाल • इंफॉर्मेशन तथा सायबर सिक्योरिटी डोमेन में ठोस पृष्टभूमि के साथ विषयवस्तु की गहरी विशेषज्ञता/ज्ञान • सिक्योरिटी कोड रिव्यूज में अनुभव • अतिउत्तम मौखिक, एनालिटिकल तथा लिखित संचार कौशल

34.	**मुख्य प्रबंधक (सायबर सिक्योरिटी-डिजिटल फॉरेन्सिक) (एसएमजीएस-IV)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/इंफॉर्मेशन टेक्नोलॉजी में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीए	**अनिवार्य** ईसी-काउंसिल से कंप्यूटर हैकिंग फोरेंसिक इनवेस्टिगेटर (सीएचएफआई)/एनकेस सर्टिफाइड एक्जामिनर (एनसीई)/ डिजिटल फोरेंसिक्स पर एसएएनएस जीआईएसी सर्टिफिकेशन/घटना की प्रतिक्रिया के क्षेत्र पर एसएएनएस जीआईएसी प्रमाणन **अधिमान्य:** सर्टिफाइड इन्फॉर्मेशन सिस्टम्स सिक्योरिटी प्रोफेशनल (सीआईएसएसपी)	न्यूनतम अर्हता के पश्चात सायबर सिक्योरिटी में कम से कम 9(नौ) वर्षों का अनुभव 9 वर्षों के अनुभव में से कम से कम 5 वर्षों का अनुभव डिजिटल फॉरेन्सिक एनालिसिस में होना चाहिए. **अपेक्षित विशेष कौशल :** • डिजिटल फारेन्सिक एनालिसिस तथा फॉरेन्सिक टूल्स (कमर्शियल व ओपन सोर्स टूल्स) जैसे कि एन्कैश फॉरेन्सिक टूल किट्स (एफटीके) आदि में अनुभव • डिजिटल तथा अन्य एविडेन्स की फॉरेन्सिक परीक्षा करना तथा फॉरेन्सिक जांचों के लिए इंसिडेन्ट्स को एनालाइज करने की क्षमता. • नेटवर्क, सिस्टम्स, एप्लिकेशन्स, मोबाइल एप्स आदि की सिक्योरिटी पर ठोस तकनीकी ज्ञान • थ्रेट हंटिंग, इंडिकेटर्स ऑफ कम्प्रोमाइस (आईओसी) एनालिसिस और मलवेयर एनालिसिस और रिवर्स इंजीनियरिंग • डिजिटल फॉरेन्सिक एनालिसिस में अनुभव • अतिउत्तम मौखिक, एनालिटिकल तथा लिखित संचार कौशल
35.	**मुख्य प्रबंधक (सायबर सिक्योरिटी-थ्रेट हन्टिंग) (एसएमजीएस-IV)**	कंप्यूटर साइंस/कंप्यूटर एप्लिकेशन्स/इंफॉर्मेशन टेक्नोलॉजी में बी.ई./बी.टेक या सरकार द्वारा मान्यता प्राप्त विश्वविद्यालय या संस्थान से एम.एससी. (कंप्यूटर साइंस)/ एम.एससी. (आईटी)/एमसीए	**अनिवार्य:** सर्टिफाइड थ्रेट इंटेलिजेंस एनालिस्ट (सीटीआईए)/घटना पर प्रतिक्रिया और जोखिम के क्षेत्रों पर एसएएनएस जीआईएसी प्रमाणन **अधिमान्य:** सर्टिफाइड इन्फॉर्मेशन सिस्टम्स सिक्योरिटी प्रोफेशनल (सीआईएसएसपी)	न्यूनतम अर्हता के पश्चात सायबर सिक्योरिटी में कम से कम 9(नौ) वर्षों का अनुभव 9 वर्षों के अनुभव में से कम से कम 3 वर्षों का अनुभव थ्रेट हंटिंग/मलवेयर एनालिसिस और रिवर्स इंजीनियरिंग में होना चाहिए. **अपेक्षित विशेष कौशल:** • नियमित आधार पर थ्रेट हंटिंग करना • इंवेस्टिगेशन तथा एनालिसिस कार्य के लिए अपेक्षित मलवेयर पर रिवर्स इंजीनियरिंग करना • संदिग्ध बायनरीज को कैरेक्टेरासज करना तथा ट्रेट्स, C2 की पहचान करने में समर्थ होना एवं नेटवर्क तथा होस्ट -आधारित IOCs विकसित करना. • मेमरी डम्प्स, लॉग्स तथा पॉकेट कैप्चर्स से संभावित दुभावनापूर्ण गतिविधि की पहचान करना • थ्रेट हंटिंग के लिए स्क्रिप्टिंग लिखना. • अतिउत्तम मौखिक, एनालिटिकल तथा लिखित संचार कौशल • थ्रेट हंटिंग, इंडिकेटर्स ऑफ कम्प्रोमाइस (आईओसी) एनालिसिस और मलवेयर एनालिसिस और रिवर्स इंजीनियरिंग • अतिउत्तम मौखिक, एनालिटिकल तथा लिखित संचार कौशल

पद संख्या 1 से 16 के लिए, अनुभव ''आईटी सेक्टर'' में होना चाहिए और पद संख्या 17 से 35 के लिए अनुभव ''बीएफएसआई सेक्टर तथा/या प्रख्यात आईटी कंपनियों'' में होना चाहिए.
तैनाती का स्थान : मुंबई/नवी मुंबई (पद के आधार पर). तैनाती का स्थान केवल सांकेतिक है. चुने गए अभ्यर्थी को भारत में कहीं भी तैनात किया जा सकता है.

ग. कार्य की रूपरेखा तथा केआरए

पद क्रमांक	पद और ग्रेड	जॉब प्रोफाइल और प्रमुख कार्यनिष्पादन क्षेत्र:
1.	**डेव्लपर (जेएमजीएस-I)**	• डेवलपमेंट का कार्य करना • व्यावसायिक आवश्यकताओं के संबंध में विभिन्न आईटी-संबंधित संभावनाओं की पहचान करना और उनका मूल्यांकन करना • समाधान की प्रयोज्यता और कार्य-निष्पादन सुनिश्चित करना • सिस्टम क्षेत्र के विकास को संचालित करने के प्रयासों में भाग लेना • व्यावसायिक मूल्य को अधिकतम करने के लिए डिज़ाइन किए गए समाधान विकसित करना • किसी दिए गए डोमेन का ज्ञान तेजी से हासिल करने में सक्षम • प्रचलित समाधान और मान्यताओं को चुनौती स्वीकार करना • यह सुनिश्चित करने में प्रभावी होना कि डिलिवरेबल्स सिस्टम आर्किटेक्चर और विकास के मानकों के अनुरूप हैं. • कारोबारी इकाई के लक्ष्य और ध्येय की प्राप्ति के लिए सक्रिय रूप से योगदान करना • कई कार्य के साथ कुशलता से सामना करना और एक उच्च मानक प्रदान करता है • आंतरिक ग्राहकों और व्यावसायिक भागीदारों के साथ कुशलतापूर्वक और उद्देश्यपूर्ण ढंग से संवाद करना • परिस्थितियों के अनुसार लचीलापन और अनुकूलन क्षमता प्रदर्शित करना • सक्रिय रूप से दूसरों को विकसित करने में सहायता करना, उदा. ज्ञान का संचार करना और पेशेवर नेटवर्क में भाग लेना • स्वयं के काम की गुणवत्ता पर ध्यान बनाए रखें, जैसे यूनिट टेस्ट लेकर.
2.	**डेव्लपर (एमएमजीएस-II)**	• डेवलपमेंट का कार्य करना • व्यावसायिक आवश्यकताओं के संबंध में विभिन्न आईटी-संबंधित संभावनाओं की पहचान करना और उनका मूल्यांकन करना • समाधान की प्रयोज्यता और कार्य-निष्पादन सुनिश्चित करना • सिस्टम क्षेत्र के विकास को संचालित करने के प्रयासों में भाग लेना • व्यावसायिक मूल्य को अधिकतम करने के लिए डिज़ाइन किए गए समाधान विकसित करना • किसी दिए गए डोमेन का ज्ञान तेजी से हासिल करने में सक्षम • प्रचलित समाधान और मान्यताओं को चुनौती स्वीकार करना • यह सुनिश्चित करने में प्रभावी होना कि डिलिवरेबल्स सिस्टम आर्किटेक्चर और विकास के मानकों के अनुरूप हैं. • कारोबारी इकाई के लक्ष्य और ध्येय की प्राप्ति के लिए सक्रिय रूप से योगदान करना • कई कार्य के साथ कुशलता से सामना करना और एक उच्च मानक प्रदान करता है • आंतरिक ग्राहकों और व्यावसायिक भागीदारों के साथ कुशलतापूर्वक और उद्देश्यपूर्ण ढंग से संवाद करना • परिस्थितियों के अनुसार लचीलापन और अनुकूलन क्षमता प्रदर्शित करना • सक्रिय रूप से दूसरों को विकसित करने में सहायता करना, उदा. ज्ञान का संचार करना और पेशेवर नेटवर्क में भाग लेना • स्वयं के काम की गुणवत्ता पर ध्यान बनाए रखें, जैसे यूनिट टेस्ट लेकर.
3.	**सिस्टम/सर्वर एडमिनिस्ट्रेटर (जेएमजीएस-I)**	• सिस्टम/सर्वर स्थापना, विन्यास और निगरानी • कंप्यूटर सिस्टम/सर्वर/स्टोरेज/नेटवर्क की स्थापना, समर्थन और रखरखाव के लिए जिम्मेदार • पैच अपडेशन/अपग्रेडेशन और माइग्रेशन • नए कंप्यूटर सिस्टम, सिस्टम और सर्वर के कार्य-निष्पादन को डिज़ाइन करना • निर्धारित रखरखाव के माध्यम से सर्वर डाउनटाइम से बचना, सर्वर सुरक्षा सुनिश्चित करना और सर्वर से जुड़ने में कर्मचारियों की सहायता करना. • सिस्टम कार्य-निष्पादन की निगरानी और सुधार • प्रक्रियाओं का अनुकूलन और अग्रता प्रक्रिया में सुधार • कर्मचारियों और उपयोगकर्तायों क्रेडेंशियल्स और फ्रेमवर्क को प्रबंधित करना • तकनीकी समस्याओं का निवारण • कर्मचारियों के लिए प्रशिक्षण तैयार करना और कार्यान्वित करना • फ़ायरवॉल और नेटवर्क सिस्टम की स्थापना/कॉन्फ़िगरेशन के लिए समन्वय करना तथा समर्थन प्रदान करना. • सिस्टम/सर्वर/नेटवर्क सुरक्षा निगरानी और क्षमता नियोजन • जोखिम न्यूनीकरण योजना • डीसी/डीआर सर्वर कॉन्फ़िगरेशन सेट-अप और रखरखाव

4.	**डेटाबेस एडमिनिस्ट्रेटर (जेएमजीएस-I)**	• सॉफ्टवेयर स्थापना, कॉन्फ़िगरेशन और रखरखाव: □ नए ओरेकल, एसक्यूएल सर्वर आदि की प्रारंभिक स्थापना और कॉन्फ़िगरेशन पर सहयोग करना □ हार्डवेयर सेट करने के लिए और डेटाबेस सर्वर के लिए ऑपरेटिंग सिस्टम लगाना □ मौजूदा सिस्टम से डेटा को नए प्लेटफॉर्म/डेटा माइग्रेशन पर स्थानांतरित करना • डेटा निष्कर्षण, परिवर्तन और बड़ी मात्रा में डेटा आयात करके कुशलतापूर्वक लोडिंग जो कई सिस्टम से डेटा वेयरहाउस वातावरण में निकाला गया है. • विशिष्ट डेटा हैंडलिंग: एक बहुत बड़े डेटाबेस (VLDB) के प्रबंधन के लिए उच्च स्तर के कौशल और अतिरिक्त निगरानी और दक्षता बनाए रखने की आवश्यकता हो सकती है • डेटाबेस बैकअप और रिकवरी: □ उद्योग की सर्वोत्तम प्रथाओं के आधार पर बैकअप और रिकवरी योजनाओं और प्रक्रियाओं का निर्माण करना □ डेटा की सुरक्षा के लिए आवश्यक सावधानी बरतने के लिए लागत, समय और धन का बैकअप और प्रबंधन करे उसके लिए राजी करना • सुरक्षा: जोखिम को कम करने के लिए सर्वोत्तम प्रथाओं को लागू करना और निगरानी करना. • प्रमाणीकरण: कर्मचारी पहुंच स्थापित करना डेटाबेस सुरक्षा का एक महत्वपूर्ण पहलू है (नियंत्रण जिनके पास पहुंच है और उन्हें किस प्रकार की पहुंच की अनुमति है). • क्षमता आयोजना • कार्य–निष्पादन की निगरानी : कार्य–निष्पादन के मुद्दों के लिए डेटाबेस की निगरानी करना और सॉफ्टवेयर में कॉन्फ़िगरेशन परिवर्तन करना या अतिरिक्त हार्डवेयर क्षमता जोड़ना • डेटाबेस सुरक्षा: किसी समस्या के विकसित होने तक प्रतीक्षा करने के बजाय अनुप्रयोग और उपयोग के आधार पर एक प्रणाली को नियमित रूप से ट्यून करें. • समस्या निवारण : जब समस्याएं उत्पन्न होती हैं तो उन समस्याओं को जल्दी समझना और उन पर अनुक्रिया करना. • डीसी/डीआर सर्वर कॉन्फ़िगरेशन सेट–अप, रखरखाव और क्षमता आयोजना.
5.	**क्लाउड एडमिनिस्ट्रेटर (जेएमजीएस-I)**	• बैंक के क्लाउड वातावरण की स्थापना, कॉन्फ़िगरेशन और रखरखाव. • आभासी शाखा शिकायत प्रबंधन. • क्लाउड प्लेटफॉर्म के लिए डीसी/डीआर की स्थापना • कैटलॉग आइटमों के लिए मूल्य निर्धारण सेट करना • प्रावधान नियमों को परिभाषित और सक्रिय करना • टैगिंग नियमों को परिभाषित और सक्रिय करना • क्लाउड संसाधनों के लिए परिवर्तन नियंत्रण मापदंडों को परिभाषित करना • उपयोगकर्ता अनुभव को अनुकूलित करना, नियमों और यूआई नीतियों का प्रावधान करना • बिलिंग डेटा डाउनलोड करने के लिए अनुसूची को परिभाषित करना. • क्लाउड संसाधन में संशोधनों के साथ जुड़े परिवर्तन अनुरोधों को अनुमोदित करना • क्लाउड संसाधनों के लिए लंबित अनुमोदनों को देखना • क्लाउड संसाधनों के नियोजन पर सारांश डेटा देखना और विश्लेषण करना • क्लाउड संसाधनों के लिए अनुरोधों और प्रमुख मेट्रिक्य की पिगासपी करना • गतिरोध की रोकथाम और पहचान • डिबगिंग मुद्दे • एसक्यूएल कार्यों, डेटा निर्यात और आयात, डेटाबेस प्रतिकृति, एन्क्रिप्शन, ईएलबी, ईसीबी, एस 3, क्लाउड फ्रंट, अरोरा का प्रबंधन और निगरानी • IIS, Apache, पीएचपी साइट्स, नेट साइट्स, एफटीपी साइट्स, एसएमटीपी, लिनक्स सर्वर, बैकअप रिस्टोर, मल्टीपल वीपीएन बनाए रखना • प्रश्नों, तालिका संरचना, अनुक्रमण को अनुकूलित करना • ग्राहक/परियोजना की आवश्यकताओं के अनुसार सुरक्षित वातावरण सेटअप करना • क्षमता आयोजना
6.	**नेटवर्क इंजीनियर (जेएमजीएस-I)**	• नेटवर्क डिवाइसों की स्थापना और क्षमता आयोजना • सिस्टम कॉन्फ़िगरेशन को डिज़ाइन करके नेटवर्किंग वातावरण की स्थापना करना; निर्देशन प्रणाली की स्थापना; दस्तावेज़ीकरण को परिभाषित करना, और सिस्टम मानकों को लागू करना • कार्य–निष्पादन की निगरानी के द्वारा नेटवर्क के कार्य–निष्पादन को अधिकतम करना, नेटवर्क समस्याओं और समस्याओं का निवारण; शेड्यूलिंग अपग्रेड; नेटवर्किंग पर नेटवर्क के साथ सहयोग कर अनुकूलन. • नीतियों को स्थापित और लागू करके तथा पहुंच को परिभाषित और उसकी निगरानी करके नेटवर्क प्रणाली को सुरक्षित करना. • शैक्षिक अवसरों में भाग लेकर कार्य संबंधी ज्ञान अद्यतन करना, पेशेवर प्रकाशन पढ़ना; व्यक्तिगत नेटवर्क बनाए रखना; पेशेवर संगठनों में भाग लेना. • संबंधित परिणामों को आवश्यकतानुसार पूरा करके सूचना प्रणाली और संगठन के लक्ष्यों को पूरा करना • सूचना को एकत्रित करके प्राथमिकता तय करके और परियोजनाओं का प्रबंधन करके नेटवर्क परिचालन की स्थिति की रिपोर्ट करना. • कौशल: ट्रैकिंग बजट खर्च, परियोजना प्रबंधन, समस्या समाधान, लैन ज्ञान, प्रॉक्सी सर्वर, नेटवर्किंग ज्ञान, नेटवर्क डिजाइन और कार्यान्वयन, नेटवर्क समस्या निवारण, नेटवर्क हार्डवेयर कॉन्फ़िगरेशन, नेटवर्क कार्य–निष्पादन ट्यूनिंग.
7.	**टेस्टर (जेएमजीएस-I)**	• परीक्षण स्क्रिप्ट और मामलों को परिभाषित करना • परीक्षण स्क्रिप्ट/मामलों का निष्पादन • परीक्षण स्क्रिप्ट में सुधार और परीक्षण मामलों की रिपोर्ट की निरंतरता • सफेद–बॉक्स, ग्रे–बॉक्स और ब्लैक–बॉक्स परीक्षण • परीक्षण के परिणाम का दस्तावेजीकरण • सुनिश्चित करना कि परीक्षण की शुरुआत से पहले एक विस्तृत परीक्षण स्क्रिप्ट/मामले, परिदृश्य और निर्देश उपलब्ध हैं. • सुनिश्चित करना कि यूएटी के दौरान पहचाने गए मुद्दे परीक्षण लॉग में लॉग किए गए हैं • सुनिश्चित करना कि परीक्षण सहमत समय सीमा के भीतर होता है • व्यावसायिक आवश्यकताओं और कार्यात्मक विनिर्देश दस्तावेजों की समझ • दोष वर्गीकरण और रिपोर्टिंग में सहायता • स्थिति रिपोर्ट तैयार करने के लिए आवश्यक डेटा का प्रावधान • स्वचालन परीक्षण उपकरण की अच्छी समझ • दिन के अंत में दैनिक स्थिति रिपोर्ट में दैनिक गतिविधियों को अद्यतन करना.
8.	**डब्ल्यूएएस एडमिनिस्ट्रेटर (एमएमजीएस-II)**	• डब्ल्यूएएस की स्थापना, कॉन्फ़िगरेशन और रखरखाव • कई मध्यम वेयर उत्पादों के साथ बड़े पैमाने पर डब्ल्यूएएस इंफ्रास्ट्रक्चर का समर्थन करना • AIX में डब्ल्यूएएस और आईएचएस की स्थापना, डब्ल्यूएएस और समस्या निवारण • एसएसएल कॉन्फ़िगरेशन, लोड बैलेंसर की स्थापना • J2EE, आईएचएस वेब सर्वर, वेबस्पेयर एप्लिकेशन सर्वर, एसएसएल, एसओए, यूनिक्स शेल, पायथन और पर्ल आदि की स्थापना. • आईबीएम एमक्यू सर्वर, ओरेकल/एसक्यूएल/डीबी 2 सर्वर और एक्सएमएल, एक्सएसएल, और डब्ल्यूएसडीएल की स्थापना • वेब और एप्लिकेशन सर्वर, वर्कफ़्लो इन्फ्रास्ट्रक्चर और समस्या निवारण स्थापित करना • कार्य–निष्पादन ट्यूनिंग और सुधार • क्षमता आयोजना
9.	**इंफ्रास्ट्रक्चर इंजीनियर (एमएमजीएस-II)**	• सोलारिस/लाइनक्स/यूनिक्स पर वेबलॉजिक का इंस्टालेशन/माइग्रेशन/अपग्रेडेशन • हार्डवेयर आकार निर्धारण, क्षमता आयोजना, मूल्यांकन और खरीद. • नए उपकरणों की स्थापना, हार्डवेयर स्वैप–आउट और कम्पोनेंट प्रतिस्थापन (सर्वर, नेटवर्क उपकरण और भंडारण) • वर्चुअलाइजेशन का कार्यान्वयन • बिजली की आपूर्ति और उपकरणों की स्थापना और रखरखाव. नेटवर्क पैचिंग जैसे संबंधित बुनियादी ढांचे की स्थापना • नेटवर्क केबलिंग और परीक्षण • आपूर्तिकर्ता संपर्क – बुनियादी ढांचे के विक्रेताओं के साथ ऑर्डर और डिलीवरी की व्यवस्था करना • कंसोल और कमांड लाइन का उपयोग करके वेबलॉग पर वेब एप्लिकेशन नियोजन का अनुभव • वेब सर्वर/एप्लिकेशन सर्वर और डीबी सर्वर का एकीकरण • वेबसर्वर/ऐप सर्वर पर एसएसएल सीट्स का प्रबंधन

		• लॉग्स की समस्या निवारण, विभिन्न टीमों से मांग पर लॉग प्रदान करना (आर्किटेक्ट, डेवलपर्स और सत्यापन) • आवश्यकता के अनुसार थ्रेड/हीप डंप प्रदान करना • शेल स्क्रिप्टिंग का उपयोग करके कार्यों के उत्पादन परिनियोजन स्वचालन के दौरान विभिन्न टीमों के साथ काम करना • समय–समय पर स्वास्थ्य जांच सुनिश्चित करना और उच्च उपलब्धता के लिए उचित कदम उठाना. • सुनिश्चित करना कि पूर्वनिर्धारित एसएलए को बनाए रखा गया है • सुनिश्चित करना कि सभी मामलों में 100% बीसीपी का प्रावधान है • आईटीआईएल/आईटीएसएम उपकरण (न्यूनतम मैनुअल हस्तक्षेप) के कार्यान्वयन के लिए जिम्मेदार • इंफ्रा रोडमैप पर आईटी साझेदारों के साथ नियमित रूप से बातचीत करना और सभी अंशधारकों को रिपोर्ट देना • बैंक की आईटी/आईएस नीति के अनुसार पैच प्रबंधन के लिए जिम्मेदार • उपरोक्त मामलों पर आवेदन मालिकों के साथ नियमित सवाद • पूरे आर्किटेक्चर डिजाइन और मूल्यांकन कार्य का प्रलेखन सुनिश्चित करना • नई प्रणालियों में माइग्रेशन, क्षमता आयोजना, कार्य–निष्पादन की निगरानी और सुधार.
10.	**यूएक्स डिजाइनर (एमएमजीएस-II)**	• यूएक्स डिजाइन में उद्योग की सर्वोत्तम प्रथाओं का अध्ययन करना. • वायरफ्रेम वेबसाइटों और मोबाइल एप्लिकेशनों को डिजाइन करना • वेबसाइट की सामग्री का मिलान करने और प्रोग्राम के विकास का प्रबंधन करने के लिए आंतरिक डिजाइन और प्रोग्रामिंग टीम के साथ मिलकर काम करना. • उपयोगकर्ताओं की आवश्यकताओं की पहचान करने और उपयोगकर्ता सामग्री का उपभोग और उसे नेविगेट कैसे करते हैं, यह समझने के लिए उत्पाद टीम के साथ मिलकर काम करना. • मौजूदा सूचना आर्किटेकट का आकलन करना और सामग्री के आविष्कार और ऑडिट सहित सुधार के लिए क्षेत्रों की पहचान करना. • वेबसाइट या अनुप्रयोगों के लिए सूचना की योजना तथा डिजाइन बनाना. • उपयोग के मामले बनना और आरेख बनाना और सूचना पदानुक्रम को परिभाषित करना • सूचना की लेबलिंग • वायरफ्रेम और टैक्सोनॉमी बनाना. • साक्षात्कार, उपयोगकर्ता सर्वेक्षण, कार्ड छंटाई और प्रयोज्यता परीक्षण की योजना बनाना और उसका आयोजन • उपयोगकर्ता के व्यवहार और दृष्टिकोण के अध्ययन का डिजाइन तैयार करना और निष्पादित करना • अन्वेषणात्मक मूल्यांकन का संचालन करना • उपयोगकर्ता व्यक्तित्व को परिभाषित और परिष्कृत करने में मदद करना • दीर्घकालिक उत्पाद रणनीति को आकार देने में मदद करने के लिए अंतर्दृष्टि प्रस्तुत और संप्रेषित करना. • उपयोगकर्ता अनुसंधान और प्रतियोगी विश्लेषण की योजना बनाना और संचालन करना • डेटा और गुणात्मक प्रतिक्रिया की व्याख्या करना • उपयोगकर्ता कहानियां, व्यक्ति और कहानीबोर्ड बनाना. • सूचना आर्किटक्चर का निर्धारण करना और साइटमैप बनाना. • प्रोटोटाइप और वायरफ्रेम बनाना • प्रयोज्यता परीक्षण का संचालन करना.
11.	**आईटी जोखिम प्रबंधक (एमएमजीएस-II)**	• प्रक्रिया, प्रौद्योगिकी, साइबर सुरक्षा, लेखा परीक्षा, कानूनी और नियामक अनुपालन सहित आईटी जोखिम की पहचान करने के लिए जिम्मेदार. अभ्यर्थी व्यावसायिक जोखिमों सहित समग्र –संगठन स्तर पर जोखिम प्रबंधन प्रक्रियाओं का प्रबंधन और संचालन करने के लिए प्रमाणित नेतृत्व क्षमता के साथ आईटी जोखिम प्रबंधन पर एक विषय वस्तु विशेषज्ञ होना चाहिए. • उद्यम वार आईटी जोखिम प्रबंधन ढांचा डिजाइन करना और कार्यान्वयन में सहायता करना. संगठन में आईटी जोखिम की निगरानी करना. • प्राथमिक इंटरफ़ेस व्यवसाय इकाई, डेटा, प्रक्रिया और नियंत्रण मालिकों के साथ आगे नियोजन के साथ सूचना प्रौद्योगिकी के भीतर होगा. इस भूमिका में स्थापित नियमों और संगठन मानकों के अनुसार जोखिम विश्लेषण शामिल होना चाहिए, लेकिन यह सूचना प्रणाली, स्वाम्य अनुप्रयोग, व्यावसायिक प्रक्रिया, आस–पास के अनुप्रयोग, भौतिक वातावरण, तीसरे पक्ष के सेवा प्रदाता, सूचना सुरक्षा उपकरण और रणनीति, साथ ही साथ व्यापार की निरंतरता और आपदा वसूली क्षमताओं तक सीमित नहीं है. • आईटी संपत्तियों, स्वाम्य अनुप्रयोगों, विक्रेता आधारित समाधान, व्यापार प्रक्रियाओं और तीसरे पक्ष के साथ संबंधों के समक्ष स्वतंत्र जोखिम आकलन करके सूचना प्रौद्योगिकी जोखिम की निरंतर पहचान, आकलन, माप, दस्तावेज और निगरानी करना. • जोखिम मालिकों के साथ जोखिम–आधारित सुधारात्मक कार्य योजनाओं को विकसित करने और उनके निष्पादन और पूर्णता में निगरानी प्रदान करके जोखिम विश्लेषण के परिणामस्वरूप जोखिम प्रबंधन पहलों के साथ सहायता करना. • तकनीकी और संरचनात्मक समीक्षा, प्रौद्योगिकी परियोजनाओं, नई व्यवसाय प्रक्रिया और परिवर्तन प्रबंधन गतिविधियों के लिए एक प्रमुख परियोजना और जोखिम–केंद्रित संसाधन के रूप में कार्य करना. • प्रबंधन को प्रस्तुत जोखिम प्रबंधन से संबंधित मैट्रिक्स और स्थिति की निगरानी और रिपोर्टिंग में सहायता करना. • वार्षिक आईटी रिस्क यूनिवर्स और शेड्यूल के विकास में भाग लेना, जोखिम रजिस्टर रखना, नए जोखिम खतरों का मूल्यांकन करना और डेटा, गोपनीयता, अखंडता और उपलब्धता के नुकसान को कम करने के लिए नियंत्रण सिफारिशें स्थापित करना. • वर्तमान पहचान जोखिम प्रबंधन के लिए निष्कर्ष निकालना और सुझाई कार्य योजनाओं पर बातचीत • कमजोरियों, सुरक्षा उल्लंघनों या दुर्भावनापूर्ण हमलों से संबंधित सूचना प्रौद्योगिकी के सभी क्षेत्रों में वर्तमान प्रगति की जानकारी रखना. • नवीनतम जोखिम न्यूनीकरण उपकरण/तकनीकों और उनके कार्यान्वयन की समझ;
12.	**आईटी सुरक्षा विशेषज्ञ (एमएमजीएस-III)**	• सूचना एकत्र करके और योजनाएं विकसित करके आईटी धमकियों को कम करना. सुरक्षा उल्लंघनों के मामलों में निगरानी नेटवर्क, सुरक्षा प्रोटोकॉल पर प्रशिक्षण उपयोगकर्ताओं, सर्वोत्तम प्रथाओं और सुरक्षा मानकों को विकसित करना, सुरक्षा सुधार के लिए आईटी को चालू रखने के लिए आपदा वसूली प्रक्रियाओं का निर्माण और परीक्षण करना. • उत्पादन वातावरण में लगाए जाने से पहले आंतरिक रूप से विकसित अनुप्रयोगों की समीक्षा के लिए जिम्मेदार • संभावित दुर्भावनापूर्ण हैकर द्वारा उपयोग की जा सकने वाली कमजोरियों को पहचान करना. • अनुप्रयोग के मूल्यांकन में उपकरण आधारित परीक्षण और मैन्युअल रूप से वेब ब्राउज़र या नामित क्लाइंट सॉफ़्टवेयर के साथ परीक्षण शामिल हैं. • क्षेत्रों में वीएपीटी, इनपुट सत्यापन, अभिगम नियंत्रण, पासवर्ड नीति, सत्र प्रबंधन, प्रमाणीकरण, एन्क्रिप्शन शामिल हैं, किंतु इन्हीं तक सीमित नहीं. • नवीनतम आईटी सुरक्षा उपकरणों/तकनीकों को समझना • कॉर्पोरेट आवश्यकताओं को पूरा करने के लिए नेटवर्क सुरक्षा मानकों और मार्गदर्शक नेटवर्क डिजाइन का विकास करना • नेटवर्क सुरक्षा आकलनों का संचालन और डीडीओ, डब्ल्यूएएफ, आईडीएस, फ़ायरवॉल और सिएम सिस्टम की निगरानी करना. • यह सुनिश्चित करने पर आंतरिक और बाहरी व्यापार भागीदारों के साथ काम करना कि आईटी बुनियादी ढांचा वैश्विक नेटवर्क सुरक्षा मानकों को पूरा करता है. • हमारे एप्लिकेशनों और नेटवर्क में सुरक्षा भेद्यता, मुद्दों की रिपोर्टिंग और संभावित समाधानों का वर्णन करने के सक्रिय रूप से नजर रखना. • हमारे सुरक्षा इंफ्रास्ट्रक्चर को डिजाइन करना और बनाए रखना. • सुरक्षा संबंधी खबरों से अवगत रहना, नवीनतम कमजोरियों और क्षेत्र में उभरने वाले उपचारों पर नज़र रखना.. • सभी स्रोत कोडों के पूरी तरह से स्वचालित परीक्षण के माध्यम से (जैसे, परीक्षण–प्रेरित विकास के माध्यम से) सक्रिय संरचना सुनिश्चित करने के लिए विकास टीम के साथ सक्रिय रूप से संपर्क करना. • हमारी वर्तमान सेवाओं और नवीनतम परिवर्तनों के साथ–साथ हमारी आंतरिक प्रथाओं का लेखा–जोखा करने वाली नियमित रिपोर्ट प्रदान करना. • हमारे सर्वर ट्रैफ़िक, टिकटिंग और असामान्य पैकेट की रिपोर्टिंग करना. • आंतरिक उत्पादों और सूचनाओं की सुरक्षा सुनिश्चित करने के लिए सुरक्षा उपकरणों और सॉफ्टवेयर का विकास और डिजाइन करना. • एक नेटवर्क प्रणाली के भीतर सूचना प्रौद्योगिकी प्रणाली के लिए सुरक्षा उपायों का प्रबंधन करना • सुरक्षा अपडेट के लिए सिस्टम और नेटवर्क प्रक्रियाओं का नियमित निरीक्षण करना • सुरक्षा और सुरक्षा उपायों और रणनीतियों को शुरू करने के लिए ऑडिट प्रक्रिया का संचालन करना • नियमों और आवश्यकता के अनुसार सूचना तक पहुँच को अनुकूलित करना • मानक सूचना सुरक्षा नीति, प्रक्रिया और सेवाओं को बनाए रखना्

13.	**परियोजना प्रबंधक (एमएमजीएस-III)**	• कारोबार, अनुप्रयोग, डेटा और प्रौद्योगिकी संरचना पर केंद्रित उच्च प्रदर्शन, फुर्तीली टीम बनाना और उसका नेतृत्व करना • अंतरराष्ट्रीय स्तर पर स्थापित मानकों के अनुसार एंटरप्राइज एंड टेक आर्किटेक्चर (ई एंड टीए) का निर्माण करना और उसे अद्यतन रखना. • बैंक में E & TA आर्किटेक्चर को संचालित करने के लिए गवर्नेंस की स्थापना करना. सुनिश्चित करना कि जोखिम प्रमाणित प्रथाओं के अनुसार प्रबंधित किए जाते हैं. • परिवर्तन प्रबंधन प्रक्रिया में उद्यम आर्किटेक्चर का निर्माण • टीम के प्रदर्शन और कार्य–सिपुर्दगी की समीक्षा करना और यह सुनिश्चित करना कि प्रदर्शन हितधारकों की अपेक्षाओं को पूरा करता है. हितधारकों का ज्ञान उन्नयन सुनिश्चित करें. • कारोबारी जरूरतों और उद्देश्यों के साथ संरेखण में उत्पादों/सेवाओं को वितरित करना. उद्यम के भीतर कई टीमों या विभागों के लिए जिम्मेदार. • आईटी योजना, रणनीतियों/पहल और उत्पाद जीवनचक्र/सेवा अभिविन्यास के विकास में योगदान; आईटी इको–सिस्टम की वर्तमान और भविष्य की जरूरतों को निर्धारित करना. • विदेशी पोर्टफोलियो/प्रोग्राम/प्रोजेक्ट मैनेजमेंट जिम्मेदारियां. वित्तीय प्रबंधन और जोखिम प्रबंधन क्षमताओं को निर्देशित करना. • स्थिर और सुरक्षित वातावरण, घटना प्रबंधन, उत्पाद स्वास्थ्य/पैचिंग और परिसंपत्ति प्रबंधन जीवनचक्र में योगदान करना. • सभी संबंधित हितधारकों को शामिल करने और तकनीकी व्यवहार्यता सुनिश्चित करने के लिए परियोजना के दायरे और उद्देश्यों की परिभाषा में सहायता करना. • प्रगति की निगरानी और ट्रैक करने के लिए एक विस्तृत परियोजना योजना विकसित करना . • उपयुक्त उपकरणों और तकनीकों का उपयोग करके परियोजना के प्रदर्शन को मापना. • ग्राहक और सभी हितधारकों के साथ संबंध का सफलतापूर्वक प्रबंधन करना. परियोजनाओं के निर्दोष निष्पादन के लिए आंतरिक संसाधनों और तृतीय पक्षों/विक्रेताओं का समन्वय करना. बुनियादी ढांचे, प्रौद्योगिकियों और समर्थन की उपलब्धता सुनिश्चित करने के लिए विक्रेताओं, आपूर्तिकर्ताओं और कार्यपालक प्रबंधन के साथ संवाद करना. • समय–समय पर परियोजना प्रबंधन और परियोजना प्रबंधन संबंधित अवधारणाओं पर आवधिक प्रशिक्षण देना. • क्रियाशील आधार पर परियोजनाओं के लाभ का मूल्यांकन और उचित हितधारकों को रिपोर्ट करना. • सुनिश्चित करना कि सभी परियोजनाओं को समय पर, दायरे में और बजट के भीतर निष्पादित किया जाए. • संबंधित हितधारकों के लिए परियोजनाओं और रिपोर्ट का विश्लेषण जारी रखना • व्यापक परियोजना प्रलेखन तैयार करना और उसे रखना. • परियोजना जोखिमों को कम करने के लिए जोखिम प्रबंधन करना. • आवश्यकतानुसार प्रबंधन को रिपोर्ट करना और उसे पहुंचाना. • उचित सत्यापन तकनीकों का उपयोग करके परियोजना के दायरे, परियोजना अनुसूची और परियोजना लागत में परिवर्तन का प्रबंधन करना. • संसाधन उपलब्धता और आवंटन सुनिश्चित करना • मजबूत लिखित, मौखिक और प्रस्तुति कौशल होना चाहिए.
14.	**एप्लिकेशन आर्किटेक्ट (एमएमजीएस-III)**	• एप्लिकेशन आर्किटेक्ट डिजाइन, मिडलवेयर ऑर्किटेक्चर डिजाइन और अन्य प्रौद्योगिकी आर्किटेक्चर तैयार करना और उसे वैधीकृत करना. • डिजाइन के प्रयासों का अनुमान लगाना, विस्तृत कार्यक्रम निर्धारित करना, प्रौद्योगिकियों का मूल्यांकन करना, प्रोटोटाइप विकसित करना, आर्किटेक्ट डिजाइन करना. • व्यवसाय की आवश्यकता और प्रौद्योगिकी में परिवर्तन के अनुसार आर्किटेक्चर बदलना. • आर्किटेक्ट सिद्धांतों, प्रक्रियाओं, उनके मानकों और दिशानिर्देशों को समझना और लागू करना • गुणवत्ता और समयबद्धता के अनुसार सौंपे गए कार्य का पूर्ण दायित्व लेना. • एप्लीकेशन लेयरिंग डिपेंडेंसीज़ (यूज़र–इंटरफ़ेस, परिनियोजन, पब्लिक इंटरफ़ेस, एप्लीकेशन डोमेन, एप्लीकेशन इन्फ्रास्ट्रक्चर, टेक्निकल फ्रेमवर्क, और प्लेटफ़ॉर्म) और एप्लिकेशन कंपोनेंट की निर्भरताओं को समझना, दस्तावेज़ीकृत करना और निगरानी करना. • मौजूदा तकनीकी और नेटवर्क वातावरण के बीच निर्भरता के प्रभावों को समझना और उसकी निगरानी करना. • प्रस्तावित संरचनात्मक अंतःक्रियाओं के लिए अवधारणा के प्रत्यक्ष और परिभाषित कार्यों को निर्धारित करना तथा दिशानिर्देशित करना. • अनुपालन और तत्परता के लिए सॉफ्टवेयर उत्पाद, सहायक उपकरण, और प्लेटफॉर्म लाइसेंसिंग वर्गीकरण का निगरानी करना. • पैकेज्ड या आवश्यकतानुरूप अनुप्रयोगों का समर्थन करने के लिए सहायक तकनीकों को परिभाषित करना, योजना बनाना, प्रस्ताव करना और चयन करना. • विभिन्न आर्किटेक्ट विकल्पों के प्रौद्योगिकी विकल्पों, जोखिमों और प्रभावों को सूचीबद्ध करने वाले दृष्टिकोण पत्र तैयार करना. • विभिन्न अनुप्रयोगों और अनुप्रयोग घटकों के बीच, और उनमें डेटा निर्भरता को परिभाषित करना. • विभिन्न अनुप्रयोगों और अनुप्रयोग घटकों के बीच और बीच में डेटाबेस के उदाहरणों के बीच समन्वय निर्धारित करना और प्रत्यक्ष समन्वय करना. • दस्तावेज़ और तकनीकी आर्किटेक्चर, नेटवर्क आर्किटेक्चर, एप्लिकेशन आर्किटेक्चर, और तकनीकी अनुप्रयोग आर्किटेक्चर आरेख और विवरण बनाए रखना, जिसमें रिलीज़ और सॉफ़्टवेयर के संस्करण शामिल हैं. • संदर्भ आरेख, कार्यात्मक आर्किटेक्चर, डेटा आर्किटेक्चर को दस्तावेजीकृत करना और बनाए रखना तथा आर्किटेक्चर आरेख और विवरण का प्रेषित करना. • सुनिश्चित करना कि आर्किटेक्ट घटक व्यावसायिक आवश्यकताओं को बेहतर ढंग से संबोधित करते हैं. • तकनीकी और बुनियादी ढांचे की आवश्यकताओं, इंजीनियरिंग पहलों में नेतृत्व करना/भाग लेना. • अन्य आर्किटेक्टों, परियोजना प्रबंधकों के साथ समन्वय करना और टीम सिस्टम मॉडल से विकास को सुनिश्चित करने में अग्रणी रहे. • आईटी ऊर्ध्वाधर में आर्किटेक्ट दृष्टिकोण और मानकों की व्यापक समझ सुनिश्चित करने के लिए ईएंडवाई के साथ गतिविधियों को समन्वित करना. • आर्किटेक्चर जोखिम न्यूनीकरण योजना को परिभाषित करना. • वर्तमान प्रयासों की दिशा में प्रयोज्यता का मूल्यांकन करने के लिए उत्पाद विक्रेताओं से उभरती प्रौद्योगिकियों और तकनीकी नमोन्मेषणों की निगरानी करना.
15.	**टेक्निकल लीड (एमएमजीएस-III)**	• नई आवश्यकता और समर्थन टिकट से संबंधित ग्राहक के साथ समन्वय. साप्ताहिक स्थिति कॉल, कार्य आवंटन और निगरानी टीम के सदस्यों का नेतृत्व करना. • ग्राहक कोड विकास और बग फिक्सिंग कोड समीक्षा और गुणवत्ता परीक्षण मानव संसाधन कार्यात्मक सेट अप (कोर एचआर, बिक्री सेवा) के लिए दैनिक स्थिति अपडेट • परियोजना की सर्वोत्तम प्रथाओं, कोडिंग मानकों/सुरक्षित कोडिंग प्रथाओं का उपयोग करना. • डिजाइन, कोडिंग और यूनिट परीक्षण तैयार करने के लिए टीम तैयार करें और मदद करें. • प्रोजेक्ट आर्किटेक्चर की बहुत अच्छी समझ होनी चाहिए . • सहकर्मी समीक्षा का संचालन करना और फीडबैक देना. • स्प्रिंट स्तर पर जोखिम और मुद्दों की पहचान करने के लिए सटीक जानकारी के साथ अपडेट ट्रैकर • परियोजना स्तर पर पीएम के साथ परियोजना जोखिम पहचान और न्यूनीकरण कार्रवाई योजना का संचालन करना. • प्रक्रिया जाँच मास्टर – यह सुनिश्चित करने के लिए कि उसकी टीम सभी सूचीबद्ध प्रक्रियाओं का पालन कर रही है. • अवशिष्ट को खत्म करके टीम के वेग/उत्पादकता को बढ़ाने के तरीकों की निरंतर तलाश करना. • लोक प्रबंधन और तकनीकी प्रबंधन • परियोजना समन्वय/प्रबंधन में परियोजना प्रबंधक की सहायता करना • अलार्म, स्पष्टीकरण और समाधान के साथ स्थिति रिपोर्ट करना. • रिपोर्टिंग प्रबंधक को समस्याओं से तुरंत अवगत कराना, मुद्दों को ट्रैक करना और उनका समाधान करना. • सॉफ्टवेयर विकास परियोजना जीवनचक्र के विकास, परीक्षण और समर्थन में एक टीम के माहौल में सहयोग करना. • वेब इंटरफेस और अंतर्निहित व्यावसायिक लॉजिक विकसित करना • कोई भी आवश्यक तकनीकी दस्तावेज तैयार करना • दैनिक और साप्ताहिक गतिविधियों को ट्रैक और रिपोर्ट करना • संहिता समीक्षा और संहिता ठीक करने में भाग लेना. • उचित इकाई परीक्षण और स्वचालन प्रदर्शित तथा विकसित करना • क्यूए या उत्पाद समर्थन द्वारा खोजी गई अनुसंधान समस्याएं और समस्याओं का समाधान विकसित करना • व्यावसायिक आवश्यकताओं के अनुसार और प्रबंधन द्वारा निर्देशित अतिरिक्त कर्तव्यों का पालन करना.
16.	**इंफ्रास्ट्रक्चर आर्किटेक्ट (एमएमजीएस-III)**	• आर्किटेक्चरल मापनीयता को डिजाइन करना, सर्वांग बनाना और कार्यान्वित करना • इष्टतम बुनियादी ढांचे के डिजाइन को सुनिश्चित करने के लिए एप्लिकेशन आर्किटेक्ट के साथ घनिष्ठ सहयोग में काम करना. • एक दीर्घकालिक उद्यम स्तर आईटी इन्फ्रास्ट्रक्चर योजना बनाना • सुनिश्चित करना कि डिजाइन में उपलब्धता की आवश्यकता पूरी होती हों. • सभी इन्फ्रास्ट्रक्चर परिवर्तन को मान्य करना और सक्षम प्राधिकारी से आवश्यक अनुमोदन प्राप्त करना. • आईटी भागीदारों, परामर्शदाताओं के साथ बातचीत • प्रौद्योगिकी, उद्योग के रुझान का मूल्यांकन करना और व्यापार पर संभावित प्रभाव की पहचान करना. • कारोबार और आईटी रणनीतियों के आधार पर प्रचलित उद्यम आर्किटेक्चर अभिशासन संरचना विकसित करना और उसके प्रबंधन में भाग लेना. • आईटी इंफ्रास्ट्रक्चर समाधान विकसित करने के लिए आईटी सलाहकार और व्यापारिक नेताओं के रूप में कार्य करना. • कारोबार और आईटी विभागों के लिए संगठन ऑर्किटेक्चर प्रक्रिया और परिणामों को बढ़ावा देना • इंफ्रास्ट्रक्चर ऑर्किटेक्चर के समतुल्य निर्णय लेने के लिए अधिशासी सिद्धांतों को तैयार करने के लिए नेतृत्व और निर्देश देना. • आईटी रणनीतियों और व्यावसायिक आवश्यकताओं के आधार पर इंफ्रास्ट्रक्चर ऑर्किटेक्चर के लिए कार्यान्वयन योजना बनाना. • इष्टतम अभिशासन संरचना सुनिश्चित करना और इंफ्रास्ट्रक्चर ऑर्किटेक्चर पालन से संबंधित गतिविधियों का अनुपालन करना • इंफ्रास्ट्रक्चर आर्किटेक्चर निष्पादन के साथ–साथ चल रहे न्यूनीकरण कार्यों को लागू करना • आईटी भागीदारों के साथ इंफ्रास्ट्रक्चर आर्किटेक्चर के मानकों का चयन और मूल्यांकन

		• इंफ्रास्ट्रक्चर ऑर्किटेक्चर कार्य को फिट करने के लिए परियोजना टीमों से परामर्श करना और परियोजना की आवश्यकताओं को प्राप्त करने के लिए बुनियादी ढांचे आर्किटेक्चर को संशोधित करने की आवश्यकता है • इन्फ्रास्ट्रक्चर आरकी जरूरतों को शामिल करने के लिए तकनीकी आर्किटेक्चर को बदलने की आवश्यकता की पहचान करना • स्वस्थ आर्किटेक्चर इन्फ्रास्ट्रक्चर को प्राप्त करने के लिए इन्फ्रास्ट्रक्चर ऑर्किटेक्चर के विकास की परियोजना टीमों के साथ परामर्श देना. • इन्फ्रास्ट्रक्चर आर्किटेक्चर का समर्थन करने के लिए अवसंरचना और संसाधनों की आवश्यकताओं की पहचान करना . • पूरे आर्किटेक्चर डिजाइन और मूल्यांकन कार्य के प्रलेखन सुनिश्चित करना. • इन्फ्रास्ट्रक्चर आर्किटेक्चर के लिए शिक्षा योजना विकसित और निष्पादित करना.
17.	**इंफ्रास्ट्रक्चर इंजीनियर (जेएमजीएस–I)**	• सोलारिस/लाइनक्स/यूनिक्स पर वेबलॉजिक का इंस्टालेशन/माइग्रेशन/अपग्रेडेशन • हार्डवेयर आकार निर्धारण, क्षमता आयोजना, मूल्यांकन और खरीद. • नए उपकरणों की स्थापना, हार्डवेयर स्वैप–आउट और कम्पोनेंट प्रतिस्थापन (सर्वर, नेटवर्क उपकरण और भंडारण) • वर्चुअलाइजेशन का कार्यान्वयन • बिजली की आपूर्ति और उपकरणों की स्थापना और रखरखाव. नेटवर्क पैचिंग जैसे संबंधित बुनियादी ढांचे की स्थापना • नेटवर्क केबलिंग और परीक्षण • आपूर्तिकर्ता संपर्क – बुनियादी ढांचे के विक्रेताओं के साथ ऑर्डर और डिलीवरी की व्यवस्था करना • कंसोल और कमांड लाइन का उपयोग करके वेबलॉग पर वेब एप्लिकेशन नियोजन का अनुभव • वेब सर्वर/एप्लिकेशन सर्वर और डीबी सर्वर का एकीकरण • वेबसर्वर/ऐप सर्वर पर एसएसएल सीट्स का प्रबंधन • लॉग्स की समस्या निवारण, विभिन्न टीमों से मांग पर लॉग प्रदान करना (आर्किटेक्ट, डेवलपर्स और सत्यापन) • आवश्यकता के अनुसार थ्रेड/हीप डंप प्रदान करना • शेल स्क्रिप्टिंग का उपयोग करके कार्यों के उत्पादन परिनियोजन स्वचालन के दौरान विभिन्न टीमों के साथ काम करना • समय–समय पर स्वास्थ्य जांच सुनिश्चित करना और उच्च उपलब्धता के लिए उचित कदम उठाना. • सुनिश्चित करना कि पूर्वनिर्धारित एसएलए को बनाए रखा गया है • सुनिश्चित करना कि सभी मामलों में 100% बीसीपी का प्रावधान है • आईटीआईएल/आईटीएसएम उपकरण (न्यूनतम मैनुअल हस्तक्षेप) के कार्यान्वयन के लिए जिम्मेदार • इंफ्रा रोडमैप पर आईटी साझेदारों के साथ नियमित रूप से बातचीत करना और सभी अंशधारकों को रिपोर्ट देना • बैंक की आईटी/आईएस नीति के अनुसार पैच प्रबंधन के लिए जिम्मेदार • उपरोक्त मामलों पर आवेदन मालिकों के साथ नियमित सवाद • पूरे आर्किटेक्चर डिजाइन और मूल्यांकन कार्य का प्रलेखन सुनिश्चित करना • नई प्रणालियों में माइग्रेशन, क्षमता आयोजना, कार्य–निष्पादन की निगरानी और सुधार.
18.	**आईटी सुरक्षा विशेषज्ञ (जेएमजीएस-I)**	• सूचना एकत्र करके और योजनाएं विकसित करके आईटी धमकियों को कम करना. सुरक्षा उल्लंघनों के मामलों में निगरानी नेटवर्क, सुरक्षा प्रोटोकॉल पर प्रशिक्षण उपयोगकर्ताओं, सर्वोत्तम प्रथाओं और सुरक्षा मानकों को विकसित करना, सुरक्षा सुधार के लिए आईटी को चालू रखने के लिए आपदा वसूली प्रक्रियाओं का निर्माण और परीक्षण करना. • उत्पादन वातावरण में लगाए जाने से पहले आंतरिक रूप से विकसित अनुप्रयोगों की समीक्षा के लिए जिम्मेदार • संभावित दुर्भावनापूर्ण हैकर द्वारा उपयोग की जा सकने वाली कमजोरियों को पहचान करना. • अनुप्रयोग के मूल्यांकन में उपकरण आधारित परीक्षण और मैन्युअल रूप से वेब ब्राउज़र या नामित क्लाइंट सॉफ़्टवेयर के साथ परीक्षण शामिल हैं. • क्षेत्रों में वीएपीटी, इनपुट सत्यापन, अभिगम नियंत्रण, पासवर्ड नीति, सत्र प्रबंधन, प्रमाणीकरण, एन्क्रिप्शन शामिल हैं, किंतु इन्हीं तक सीमित नहीं. • नवीनतम आईटी सुरक्षा उपकरणों/तकनीकों को समझना • कॉर्पोरेट आवश्यकताओं को पूरा करने के लिए नेटवर्क सुरक्षा मानकों और मार्गदर्शक नेटवर्क डिजाइन का विकास करना • नेटवर्क सुरक्षा आकलनों का संचालन और डीडीओ, डब्ल्यूएएफ, आईडीएस, फ़ायरवॉल और सिएम सिस्टम की निगरानी करना. • यह सुनिश्चित करने पर आंतरिक और बाहरी व्यापार भागीदारों के साथ काम करना कि आईटी बुनियादी ढांचा वैश्विक नेटवर्क सुरक्षा मानकों को पूरा करता है. • हमारे एप्लिकेशनों और नेटवर्क में सुरक्षा भेद्यता, मुद्दों की रिपोर्टिंग और संभावित समाधानों का वर्णन करने के सक्रिय रूप से नजर रखना. • हमारे सुरक्षा इंफ्रास्ट्रक्चर को डिजाइन करना और बनाए रखना. • सुरक्षा संबंधी खबरों से अवगत रहना, नवीनतम कमजोरियों और क्षेत्र में उभरने वाले उपचारों पर नज़र रखना.. • सभी स्रोत कोडों के पूरी तरह से स्वचालित परीक्षण के माध्यम से (जैसे, परीक्षण–प्रेरित विकास के माध्यम से) सक्रिय संरचना सुनिश्चित करने के लिए विकास टीम के साथ सक्रिय रूप से संपर्क करना. • हमारी वर्तमान सेवाओं और नवीनतम परिवर्तनों के साथ–साथ हमारी आंतरिक प्रथाओं का लेखा–जोखा करने वाली नियमित रिपोर्ट प्रदान करना. • हमारे सर्वर ट्रैफ़िक, टिकटिंग और असामान्य पैकेट की रिपोर्टिंग करना. • आंतरिक उत्पादों और सूचनाओं की सुरक्षा सुनिश्चित करने के लिए सुरक्षा उपकरणों और सॉफ्टवेयर का विकास और डिजाइन करना. • एक नेटवर्क प्रणाली के भीतर सूचना प्रौद्योगिकी प्रणाली के लिए सुरक्षा उपायों का प्रबंधन करना • सुरक्षा अपडेट के लिए सिस्टम और नेटवर्क प्रक्रियाओं का नियमित निरीक्षण करना • सुरक्षा और सुरक्षा उपायों और रणनीतियों को शुरू करने के लिए ऑडिट प्रक्रिया का संचालन करना • नियमों और आवश्यकता के अनुसार सूचना तक पहुँच को अनुकूलित करना • मानक सूचना सुरक्षा नीति, प्रक्रिया और सेवाओं को बनाए रखना्
19.	**आईटी सुरक्षा विशेषज्ञ (एमएमजीएस-II)**	• सूचना एकत्र करके और योजनाएं विकसित करके आईटी धमकियों को कम करना. सुरक्षा उल्लंघनों के मामलों में निगरानी नेटवर्क, सुरक्षा प्रोटोकॉल पर प्रशिक्षण उपयोगकर्ताओं, सर्वोत्तम प्रथाओं और सुरक्षा मानकों को विकसित करना, सुरक्षा सुधार के लिए आईटी को चालू रखने के लिए आपदा वसूली प्रक्रियाओं का निर्माण और परीक्षण करना. • उत्पादन वातावरण में लगाए जाने से पहले आंतरिक रूप से विकसित अनुप्रयोगों की समीक्षा के लिए जिम्मेदार • संभावित दुर्भावनापूर्ण हैकर द्वारा उपयोग की जा सकने वाली कमजोरियों को पहचान करना. • अनुप्रयोग के मूल्यांकन में उपकरण आधारित परीक्षण और मैन्युअल रूप से वेब ब्राउज़र या नामित क्लाइंट सॉफ़्टवेयर के साथ परीक्षण शामिल हैं. • क्षेत्रों में वीएपीटी, इनपुट सत्यापन, अभिगम नियंत्रण, पासवर्ड नीति, सत्र प्रबंधन, प्रमाणीकरण, एन्क्रिप्शन शामिल हैं, किंतु इन्हीं तक सीमित नहीं. • नवीनतम आईटी सुरक्षा उपकरणों/तकनीकों को समझना • कॉर्पोरेट आवश्यकताओं को पूरा करने के लिए नेटवर्क सुरक्षा मानकों और मार्गदर्शक नेटवर्क डिजाइन का विकास करना • नेटवर्क सुरक्षा आकलनों का संचालन और डीडीओ, डब्ल्यूएएफ, आईडीएस, फ़ायरवॉल और सिएम सिस्टम की निगरानी करना. • यह सुनिश्चित करने पर आंतरिक और बाहरी व्यापार भागीदारों के साथ काम करना कि आईटी बुनियादी ढांचा वैश्विक नेटवर्क सुरक्षा मानकों को पूरा करता है. • हमारे एप्लिकेशनों और नेटवर्क में सुरक्षा भेद्यता, मुद्दों की रिपोर्टिंग और संभावित समाधानों का वर्णन करने के सक्रिय रूप से नजर रखना. • हमारे सुरक्षा इंफ्रास्ट्रक्चर को डिजाइन करना और बनाए रखना. • सुरक्षा संबंधी खबरों से अवगत रहना, नवीनतम कमजोरियों और क्षेत्र में उभरने वाले उपचारों पर नज़र रखना.. • सभी स्रोत कोडों के पूरी तरह से स्वचालित परीक्षण के माध्यम से (जैसे, परीक्षण–प्रेरित विकास के माध्यम से) सक्रिय संरचना सुनिश्चित करने के लिए विकास टीम के साथ सक्रिय रूप से संपर्क करना. • हमारी वर्तमान सेवाओं और नवीनतम परिवर्तनों के साथ–साथ हमारी आंतरिक प्रथाओं का लेखा–जोखा करने वाली नियमित रिपोर्ट प्रदान करना. • हमारे सर्वर ट्रैफ़िक, टिकटिंग और असामान्य पैकेट की रिपोर्टिंग करना. • आंतरिक उत्पादों और सूचनाओं की सुरक्षा सुनिश्चित करने के लिए सुरक्षा उपकरणों और सॉफ्टवेयर का विकास और डिजाइन करना. • एक नेटवर्क प्रणाली के भीतर सूचना प्रौद्योगिकी प्रणाली के लिए सुरक्षा उपायों का प्रबंधन करना • सुरक्षा अपडेट के लिए सिस्टम और नेटवर्क प्रक्रियाओं का नियमित निरीक्षण करना • सुरक्षा और सुरक्षा उपायों और रणनीतियों को शुरू करने के लिए ऑडिट प्रक्रिया का संचालन करना • नियमों और आवश्यकता के अनुसार सूचना तक पहुँच को अनुकूलित करना • मानक सूचना सुरक्षा नीति, प्रक्रिया और सेवाओं को बनाए रखना्

20.	**आईटी जोखिम प्रबंधक (आईएस डिपार्टमेंट) (एमएमजीएस-II)**	• प्रक्रिया, प्रौद्योगिकी, साइबर सुरक्षा, लेखा परीक्षा, कानूनी और नियामक अनुपालन सहित आईटी जोखिम की पहचान करने के लिए जिम्मेदार. अभ्यर्थी व्यावसायिक जोखिमों सहित समग्र –संगठन स्तर पर जोखिम प्रबंधन प्रक्रियाओं का प्रबंधन और संचालन करने के लिए प्रमाणित नेतृत्व क्षमता के साथ आईटी जोखिम प्रबंधन पर एक विषय विशेषज्ञ होना चाहिए. • उद्यम वार आईटी जोखिम प्रबंधन ढांचा डिजाइन करना और कार्यान्वयन में सहायता करना. संगठन में आईटी जोखिम की निगरानी करना. • प्राथमिक इंटरफ़ेस व्यवसाय इकाई, डेटा, प्रक्रिया और नियंत्रण मालिकों के साथ आगे नियोजन के साथ सूचना प्रौद्योगिकी के भीतर होगा. इस भूमिका में स्थापित नियमों और संगठन मानकों के अनुसार जोखिम विश्लेषण शामिल होना चाहिए, लेकिन यह सूचना प्रणाली, स्वाम्य अनुप्रयोग, व्यावसायिक प्रक्रिया, आस–पास के अनुप्रयोग, भौतिक वातावरण, तीसरे पक्ष के सेवा प्रदाता, सूचना सुरक्षा उपकरण और रणनीति, साथ ही साथ व्यापार की निरंतरता और आपदा वसूली क्षमताओं तक सीमित नहीं है. • आईटी संपत्तियों, स्वाम्य अनुप्रयोगों, विक्रेता आधारित समाधान, व्यापार प्रक्रियाओं और तीसरे पक्ष के साथ संबंधों के समक्ष स्वतंत्र जोखिम आकलन करके सूचना प्रौद्योगिकी जोखिम की निरंतर पहचान, आकलन, माप, दस्तावेज और निगरानी करना. • जोखिम मालिकों के साथ जोखिम–आधारित सुधारात्मक कार्य योजनाओं को विकसित करने और उनके निष्पादन और पूर्णता में निगरानी प्रदान करके जोखिम विश्लेषण के परिणामस्वरूप जोखिम प्रबंधन पहलों के साथ सहायता करना. • तकनीकी और संरचनात्मक समीक्षा, प्रौद्योगिकी परियोजनाओं, नई व्यवसाय प्रक्रिया और परिवर्तन प्रबंधन गतिविधियों के लिए एक प्रमुख परियोजना और जोखिम–केंद्रित संसाधन के रूप में कार्य करना. • प्रबंधन को प्रस्तुत जोखिम प्रबंधन से संबंधित मैट्रिक्स और स्थिति की निगरानी और रिपोर्टिंग में सहायता करना. • वार्षिक आईटी रिस्क यूनिवर्स और शेड्यूल के विकास में भाग लेना, जोखिम रजिस्टर रखना, नए जोखिम खतरों का मूल्यांकन करना और डेटा, गोपनीयता, अखंडता और उपलब्धता के नुकसान को कम करने के लिए नियंत्रण सिफारिशें स्थापित करना. • वर्तमान पहचान जोखिम प्रबंधन के लिए निष्कर्ष निकालना और सुझाई कार्य योजनाओं पर बातचीत • कमजोरियों, सुरक्षा उल्लंघनों या दुर्भावनापूर्ण हमलों से संबंधित सूचना प्रौद्योगिकी के सभी क्षेत्रों में वर्तमान प्रगति की जानकारी रखना. • नवीनतम जोखिम न्यूनीकरण उपकरण/तकनीकों और उनके कार्यान्वयन की समझ;
21.	**इंफ्रास्ट्रक्चर आर्किटेक्ट (एमएमजीएस -II)**	• वास्तुकला मापनीयता को डिजाइन करना, सर्वांग बनाना और कार्यान्वित करना • इष्टतम बुनियादी ढांचे के डिजाइन को सुनिश्चित करने के लिए एप्लिकेशन आर्किटेक्ट के साथ घनिष्ठ सहयोग में काम करना. • एक दीर्घकालिक उद्यम स्तर आईटी इन्फ्रास्ट्रक्चर योजना बनाना • सुनिश्चित करना कि डिजाइन में उपलब्धता की आवश्यकता पूरी होती हों. • सभी इन्फ्रास्ट्रक्चर परिवर्तन को मान्य करना और सक्षम प्राधिकारी से आवश्यक अनुमोदन प्राप्त करना. • आईटी भागीदारों, परामर्शदाताओं के साथ बातचीत • प्रौद्योगिकी, उद्योग के रुझान का मूल्यांकन करना और व्यापार पर संभावित प्रभाव की पहचान करना. • कारोबार और आईटी रणनीतियों के आधार पर प्रचलित उद्यम आर्किटेक्चर अभिशासन संरचना विकसित करना और उसके प्रबंधन में भाग लेना. • आईटी अवसंरचना समाधान विकसित करने के लिए आईटी सलाहकार और व्यापारिक नेताओं के रूप में कार्य करें • कारोबार और आईटी विभागों के लिए संगठन आर्किटेक्चर प्रक्रिया और परिणामों को बढ़ावा देना • बुनियादी ढांचे की संरचना के समतुल्य निर्णय लेने के लिए अभिशासन सिद्धांतों को तैयार करने के लिए नेतृत्व करना और निर्देश देना. • आईटी रणनीतियों और व्यावसायिक आवश्यकताओं के आधार पर बुनियादी ढांचे की संरचना के लिए कार्यान्वयन योजना बनाना. • इष्टतम अभिशासन संरचना सुनिश्चित करना और बुनियादी ढांचे आर्किटेक्चर पालन से संबंधित गतिविधियों का अनुपालन करना. • आईटी इंफ्रास्ट्रक्चर समाधान विकसित करने के लिए आईटी सलाहकार और व्यापारिक नेताओं के रूप में कार्य करना. • बुनियादी ढांचे के आर्किटेक्चर निष्पादन के साथ–साथ चल रहे परिष्करण कार्यों को निष्पादित करना • आईटी भागीदारों के साथ बुनियादी ढाँचे के मानकों का चयन और मूल्यांकन • इंफ्रास्ट्रक्चर आर्किटेक्चर कार्य को फिट करने के लिए परियोजना टीमों से परामर्श करना और परियोजना की आवश्यकताओं को प्राप्त करने के लिए इंफ्रास्ट्रक्चर आर्किटेक्चर को संशोधित करने की आवश्यकता की पहचान करना. • बुनियादी सुविधाओं की जरूरतों को शामिल करने के लिए तकनीकी आर्किटेक्चर को बदलने की आवश्यकता को पहचान करना. • स्वस्थ आर्किटेक्चर बुनियादी ढांचे को प्राप्त करने के लिए बुनियादी ढांचे के विकास की परियोजना टीमों के साथ परामर्श देना. • इंफ्रास्ट्रक्चर आर्किटेक्चर का समर्थन करने के लिए इंफ्रास्ट्रक्चर और संसाधनों की आवश्यकताओं की पहचान करना . • पूरे आर्किटेक्चर डिजाइन और मूल्यांकन कार्य के प्रलेखन सुनिश्चित करना. • इन्फ्रास्ट्रक्चर आर्किटेक्चर के लिए शिक्षा योजना विकसित और निष्पादित करना.
22.	**उप प्रबंधक (साइबर सिक्योरिटी–एथिकल हैकिंग) (एमएमजीएस-II)**	• वेब एप्लिकेशन सुरक्षा परीक्षण, मोबाइल ऐप सुरक्षा परीक्षण, नेटवर्क, सिस्टम और एप्लिकेशन भेद्यता आकलन और पैठ परीक्षण, आईसीएस/आईओटी डिवाइस सुरक्षा परीक्षण सहित आवधिक आंतरिक एथिकल हैकिंग और रेड टीम अभ्यास करना. • हितधारकों के साथ सक्रिय रूप से जुड़ना, कारोबार के प्रबंधन और लेखा परीक्षकों के साथ मजबूत संबंधों का निर्माण, भेद्यता खोज और सुधारात्मक प्रयासों को सुविधाजनक बनाना. • सुरक्षा जोखिम का आकलन करना जो व्यावसायिक आवश्यकताओं का समर्थन करते हैं, और जोखिम, कमजोरियों और साइबर संकटों को दूर करने के लिए न्यूनीकरण और प्रति–उपायों की सलाह देते हैं. • एप्लिकेशन सुरक्षा आकलन में भाग लेना. • नेटवर्क सुरक्षा आकलन और सुरक्षा कॉन्फ़िगरेशन समीक्षा करना. • एनआईएसटी मानकों, उद्योग सर्वोत्तम प्रथाओं और अनुपालन नियमों के आधार पर सूचना/साइबर सुरक्षा प्रबंधन नीतियों, प्रक्रियाओं और मानकों के विकास और कार्यान्वयन में सहायता करना.
23.	**उप प्रबंधक (सायबर सिक्योरिटी–थ्रेड हन्टिंग) (एमएमजीएस-II)**	• नियमित आधार पर थ्रेट हन्टिंग का कार्य किया हो. • स्क्रिप्टिंग कौशल वांछनीय हैं • जांच और विश्लेषण की सुविधा के लिए मैलवेयर पर रिवर्स इंजीनियरिंग का कार्य करना. • फीड्स, एकत्र की गई घटनाओं का आकलन करना और जैसा उपयुक्त हो नियमों को परिष्कृत करना. • संदिग्ध बाइनरियों को वर्गीकृत करना और ट्रेट्स, C2 की पहचान करने में सक्षम होना चाहिए और नेटवर्क और होस्ट–आधारित आईओसी विकसित करने में सक्षम होना चाहिए. • मेमोरी डंप, लॉग और पैकेट कैप्चर से संभावित दुर्भावनापूर्ण गतिविधि की पहचान करना • संगठन के भीतर अन्य खोजी टीमों से संवाद करना और उनकी सहायता करना. • समन्वित प्रतिक्रियाओं और सुरक्षा घटनाओं के बाद के उपशमन पर तकनीकी विशेषज्ञों की एक घनिष्ठ टीम के हिस्से के रूप में भाग लेना.
24.	**उप प्रबंधक (सायबर सिक्योरिटी–डिजिटल फॉरेन्सिक) (एमएमजीएस-II)**	• डिजिटल और अन्य साक्ष्यों की फॉरेंसिक जाँच करना और फॉरेंसिक टूल्स (वाणिज्यिक और ओपन सोर्स टूल्स) का उपयोग करके फोरेंसिक जांच के लिए घटनाओं का विश्लेषण करना. • एनआईएसटी मानकों, उद्योग की सर्वोत्तम प्रथाओं और अनुपालन आवश्यकताओं के आधार पर सूचना/साइबर सुरक्षा प्रबंधन नीतियों, प्रक्रियाओं और मानकों के विकास और कार्यान्वयन में सहायता करना.
25.	**सिक्योरिटी एनालिस्ट (एमएमजीएस-III)**	• एक वरिष्ठ/एल 3 स्तर का सुरक्षा विश्लेषक बनना और इंसीडेंट मैनेजमेंट, वीएपीटी, इंफ्रास्ट्रक्चर मैनेजमेंट आदि जैसे एसओसी परिचालनो के विभिन्न शिफ्टों का शिफ्ट प्रभारी बनना. • दैनंदिन परिचालनों के लिए आपको सौंपे जाने वाले एसओसी क्षेत्रों का विषय विशेषज्ञ (एसएमई) बनना. • खतरा प्रबंधन, खतरा मॉडलिंग, खतरे वाले वैक्टर की पहचान करना और सुरक्षा निगरानी के लिए उपयोग के मामलों का विकास करना. • थ्रेट हंटिंग गतिविधियों, इंसीडेंट मैनेजमेंट और फोरेंसिक विश्लेषण की अगुवाई करना • तीसरी पार्टी, नियामकों और शासी निकाय से प्राप्त सभी खतरे की खुफिया जानकारियों को क्यूरेट और प्रचालित किया जाता है. • घटना निर्माण के लिए लॉग विश्लेषण में एसओसी में एल 1 और एल 2 स्तर के अधिकारियों को गाइड करना, एप्लिकेशन/परिसंपत्ति स्वामी (एओ) द्वारा घटनाओं में सुधार की परिशुद्धता की पुष्टि करना, उचित उपचार के लिए एओ का मार्गदर्शन करना और एओ के साथ वृद्धि का प्रबंधन करना. • ऑडिट के लिए उचित रिकॉर्ड के साथ शिफ्ट टेकओवर और हैंडओवर गतिविधियों को प्रबंधित करना. • लोगों, प्रक्रियाओं और प्रौद्योगिकी के दृष्टिकोण से एसओसी में एसओपी को लागू करना. • सुनिश्चित करना कि एसओसी प्रौद्योगिकियां बेहतर, सुरक्षित और विश्वसनीय तरीके से चलाने के लिए कारगर बनाई गई हैं. • सीआरएम/यूईबीए/डीएएम/एनबीए आदि (जैसा लागू हो) के साथ सभी मानक और गैर मानक मानकों के एकीकरण के लिए ज़िम्मेदार. • सहज ज्ञान युक्त डैशबोर्ड बनाना, नियम, हस्ताक्षर, डिकोडर/पार्सर, मॉडल, पैटर्न बनाना. • आईटी और अन्य हितधारकों के साथ सहयोग और समन्वय करना, निर्माण और उनके साथ सकारात्मक कामकाजी संबंधों को बनाए रखना. • साइबर हमले के उपकरणों, तकनीकों और प्रक्रियाओं को समझना, अनधिकृत व्यवहार और गतिविधियों का पता लगाने के प्रयास में सुरक्षा लॉग का गहन विश्लेषण करना. • प्रबंधन और विनियामक रिपोर्ट, एम.आई.एस. तैयार करना. • एसओसी संबंधित परिचालन और सामरिक दृष्टिकोण के लिए दैनंदिन आईटी और अन्य में हितधारकों के साथ घनिष्ठ सहयोग करना.

		• अपने एसओसी ऑपरेशंस के डोमेन में नियोजन, एकीकरण, लॉग्स पार्सिंग/डिकोडिंग तकनीक, रिपोर्टिंग, विश्लेषण, रीमेडिएशन, डैश–बोर्डिंग, क्वेरी और एमआईएस तकनीकों की सिफारिश करना. • वैयक्तिक योगदानकर्ता के रूप में पी1 और पी2 घटनाओं को उत्पन्न करने के लिए सीधे तौर पर जिम्मेदार. • खतरा प्रबंधन, खतरा मॉडलिंग, खतरे वाले वैक्टर की पहचान करना और सुरक्षा निगरानी के लिए उपयोग के मामलों का विकास करना. • थ्रेट हंटिंग गतिविधियों, इंसीडेंट मैनेजमेंट और फोरेंसिक विश्लेषण में वैयक्तिक योगदानकर्ता • एसओसी में दैनंदिन शिफ्टों का प्रबंधन करने के लिए शिफ्ट प्रभारी • सुनिश्चित करना कि एसओसी सेटअप स्वयं सुरक्षित किला बना हुआ है • महत्वपूर्ण घटनाओं, न्यूनीकरण, निगरानी, वृद्धि आदि का विश्लेषण • उपरोक्त क्षेत्रों में एल 1 और एल 2 कार्मिक संसाधनों की क्षमताओं को बढ़ाना
26.	**प्रबंधक (सायबर सिक्योरिटी–एथिकल हैकिंग (एमएमजीएस-III)**	• समय–समय पर आंतरिक एथिकल हैकिंग अभ्यास और थ्रेट हंटिंग गतिविधियों का प्रबंध करना और उसका नेतृत्व करना. • हितधारकों के साथ सक्रिय रूप से जुड़ना, कारोबार के प्रबंधन और लेखा परीक्षकों के साथ मजबूत संबंधों का निर्माण, भेद्यता खोज और सुधारात्मक प्रयासों को सुविधाजनक बनाना. • सुरक्षा जोखिम का आकलन करना जो व्यावसायिक आवश्यकताओं का समर्थन करते हैं, और जोखिम, कमजोरियों और साइबर संकटों को दूर करने के लिए न्यूनीकरण और प्रति–उपायों की सलाह देते हैं. • मानक संचालन प्रक्रियाएं (एसओपी) और सुरक्षा समाधान दस्तावेज करना. • एप्लिकेशन सुरक्षा आकलन में भाग लेना. • नेटवर्क सुरक्षा आकलन और सुरक्षा कॉन्फ़िगरेशन की समीक्षा करना. • आंतरिक एथिकल हैकिंग और रेड टीम (IEHRT) अभ्यास का प्रदर्शन और नेतृत्व करना. • साइबर सुरक्षा आकलन और सूचना प्रणाली के ऑडिट का समय पर अनुपालन सुनिश्चित करना • एनआईएसटी मानकों, उद्योग की सर्वोत्तम प्रथाओं और अनुपालन नियमों के आधार पर सूचना/साइबर सुरक्षा प्रबंधन नीतियों, प्रक्रियाओं और मानकों के विकास और कार्यान्वयन में सहायता करना. • बैंक में साइबर सुरक्षा परिपक्वता मूल्यांकन के विकास, कार्यान्वयन और निगरानी में सहायता करना. • आईएस नीति, साइबर सुरक्षा नीति आदि से संबंधित गतिविधियों में सहायता करना.
27.	**प्रबंधक (सायबर सिक्योरिटी–डिजिटल फॉरेन्सिक) (एमएमजीएस-III)**	• डिजिटल फोरेंसिक विश्लेषण गतिविधियों का प्रबंध करना और नेतृत्व करना. • डिजिटल और अन्य साक्ष्यों की फॉरेंसिक जाँच करना और फॉरेंसिक टूल्स (वाणिज्यिक और ओपन सोर्स टूल्स) का उपयोग करके फोरेंसिक जांच के लिए घटनाओं का विश्लेषण करना. • हितधारकों के साथ सक्रिय रूप से जुड़ना, कारोबार के प्रबंधन और लेखा परीक्षकों के साथ मजबूत संबंधों का निर्माण, भेद्यता खोज और सुधारात्मक प्रयासों को सुविधाजनक बनाना.
28.	**मुख्य प्रबंधक (वल्नेराबिलिटी मैनेजमेंट एंड पैनिट्रेशन टेस्टिंग) (एसएमजीएस-IV)**	**कार्य की रूपरेखा:** • वीएपीटी टीम का नेतृत्व करना जो भेद्यता आकलन, पेनिट्रेशन, ऐप सुरक्षा, कोड रिव्यू, और कॉन्फ़िगरेशन रिव्यू का संचालन करती है, साथ ही फिशिंग, मोबाइल रॉग ऐप्स, फिशिंग साइट्स की निगरानी और रिपोर्ट भी करती है. • रणनीतिक दिशा निर्धारित करना और वैश्विक उत्कृष्ट प्रथाओं और विभिन्न घरेलू और वैश्विक विनियामक निर्देशों के साथ तालमेल बनाए रखना और बैंक के पीएपीटी प्रोग्राम को बढ़ाने के लिए उन्हें निष्पादित करना. • आईटी इन्फ्रा, अनुप्रयोग, प्रक्रिया, नेटवर्किंग और सुरक्षा सेटअप में कमजोरियों की पहचान करना और उसे बंद करने के लिए निर्देश प्रदान करना. • वीएपीटी टूल में प्लग–इन और हस्ताक्षर जैसी भेद्यताओं का अद्तन रिकॉर्ड रखना. • शून्य–दिवस की भेद्यताओं पर ध्यान केंद्रित करना और बैंक के वातावरण में उनकी उपस्थिति की जांच करना, हितधारकों के साथ उनके सुधार के लिए सहयोग करना और उसे सत्यापित करना. • आईटी, बिजनेस, विनियामक, लेखापरीक्षक जैसे विभिन्न आंतरिक और बाहरी हितधारकों के साथ सक्रिय रूप से जुड़ाव रखना ताकि यह सुनिश्चित किया जा सके कि भेदयताओं के निवारण को कारोबार और नियामक उद्देश्यों के साथ संरेखित किया गया है. • कमजोरियों का पता लगाने और सुधारे जाने सहित वीएपीटी प्रोग्राम के लिए एसओपी तैयार करना. • कॉन्फ़िगरेशन का विश्लेषण करने और नेटवर्क, ऑपरेटिंग सिस्टम, एप्लिकेशन, डेटाबेस, और अन्य सूचना प्रणाली घटक के लिए वैधानिक, विनियामक आवश्यकताओं, दिशानिर्देशों और सुरक्षा सर्वोत्तम प्रथाओं के अनुसार कॉन्फ़िगरेशन का विश्लेषण करने और सेटिंग्स को लागू करने की सुविधा के लिए भेद्यताओं/खामियों के अनुपालन/सुधारात्मक सत्यापन का नेतृत्व करना. • सभी तकनीकी और प्रक्रिया मुद्दों के विस्तार के लिए पहला संपर्क बिंदु. भेद्यताओं के समय पर समाधान और न्यूनीकरण के लिए आईटी विभागों द्वारा जहां कहीं भी आवश्यक हो, तकनीकी विषयगत विशेषज्ञता प्रदान करना. • वीएपीटी दृष्टिकोण से वैश्विक और नियामक मानकों के अनुसार विभिन्न नीतियों सूचना सुरक्षा नीति, साइबर सुरक्षा नीति और संबंधित प्रक्रियाओं को संरेखित करने के लिए सुझाव देना. • वीएपीटी टीम के कार्य और कार्यभार का प्रबंधन करना और 24X7X365 एसओसी संचालन के लिए शिफ्ट हैंड–ऑफ गतिविधियों का प्रबंधन करना. • प्रशिक्षण और कार्यशालाओं के माध्यम से वीएपीटी टीम की क्षमता बढ़ाना • 24X7X365 दिनों के आधार संचालन के लिए वीएपीटी टीम के शिफ्टों को प्रबंधित करना. **मुख्य दायित्व क्षेत्र (केआरए):** • बैंक में पीएपीटी प्रोग्राम का पर्यवेक्षण तथा प्रबंधन और बैंक की सूचना सुरक्षा नीति और देशी और विदेशी नियामक संस्थाओं जैसी विभिन्न नीतियों का अनुपालन सुनिश्चित करना. • भेद्यताओं/कमजोरियों का समय पर पता लगाना और उन्हें बंद करने के लिए हितधारकों का मार्गदर्शन करना. • उपकरण, तकनीक, विधियों, प्रक्रियाओं सहित वैश्विक सर्वोत्तम प्रथाओं को अपनाना और तदनुसार बैंक के पीएपीटी प्रोग्राम को संरेखित करना. • झूठी सकारात्मक भेद्यताओं/कमजोरियों को कम करना. • शून्य–दिवस की भेद्यताओं/कमजोरियों पर हितधारकों को समय पर सलाह जारी करना. उसका पता लगाना और उसके बंद होने का सत्यापन करना. • उपकरणों, तकनीकों, विधियों और प्रक्रियाओं के माध्यम से भेद्यताओं/कमजोरियों का पता लगाने और बंद करने के लिए वीएपीटी प्रक्रियाओं को स्वचालन करना. • डैशबोर्ड के माध्यम से प्रबंधन रिपोर्टिंग विश्लेषण • वीए/पीटी प्रयासों को मात्रात्मक और गुणात्मक रूप से प्रबंधित करने और मापने के लिए मैट्रिक्स को डिजाइन और कार्यान्वित करना. •.सुनिश्चित करना कि एसओसी सेटअप स्वयं सुरक्षित किला बना हुआ है. • दैनंदिन एसओसी संबंधित रणनीतिक, परिचालनात्मक और युक्तिपरक दृष्टिकोणों के लिए आईटी में हितधारकों तथा अन्य के साथ घनिष्ठ रूप से सहयोग करना.
29.	**मुख्य प्रबंधक (इन्सिडेंट मैनेजमेंट एंड फॉरेन्सिक्स) (एसएमजीएस-IV)**	**कार्य की रूपरेखा:** • बैंक की सूचना/साइबर सुरक्षा नीतियों, प्रक्रियाओं और वैश्विक मानकों के अनुसार एसओसी के भीतर सूचना और साइबर सुरक्षा घटना प्रबंधन (आईएम) टीम के परिचालन का नेतृत्व करना. • बैंक की नीतियों, साइबर संकट प्रबंधन योजना (CCMP), नियामक आवश्यकताओं और एनआईएसटी ढांचे के अनुरूप आईएम टीम के लिए रणनीतिक दिशा–निर्देश निर्धारित करना. • असमान आईटी प्रणालियों से प्राप्त लॉग के लिए सहसंबंध नियम बनाना, एसओसी को प्रति दिन प्राप्त होने वाले अरबों लॉग पर विश्लेषणात्मक और पैटर्न विश्लेषण मॉडल विकसित और लागू करना. • लॉग सहसंबंध, घटना निर्माण, रिपोर्टिंग, सुधारात्मक, वृद्धि और समापन सत्यापन के स्वचालन के लिए प्लेबुक बनाना. • सुरक्षा, निगरानी और पता लगाने की सुसंगत और गुणवत्ता निष्पादन में टीम की सहायता करने के लिए मानक ऑपरेटिंग प्रक्रियाओं (एसओपी), वर्कफ़्लोज़ और प्रक्रियाओं को परिभाषित और अनुकूलित करना. • वास्तविक समय के सहसंबंध और संभावित सुरक्षा घटना की रिपोर्टिंग के लिए विभिन्न आंतरिक और बाहरी स्रोतों से प्राप्त होने वाली खुफिया जानकारी को एसओसी में मिलाना. • आईएसओ 27035 मानकों के समक्ष बेंचमार्क एसओसी घटना प्रबंधन प्रक्रियाएं. • सुरक्षा घटनाओं से प्रतिक्रिया और पुनर्प्राप्त करने के लिए आईटी और व्यावसायिक इकाइयों के साथ सहयोग करना. • थ्रेट हन्टिंग, निगरानी, पहचान, विश्लेषण और घटना प्रतिक्रिया और प्रतिक्रिया क्षमताओं और प्रक्रियाओं का निरंतर विकास सुनिश्चित करना. • खतरा आसूचना निविष्टियों का उपयोग करने के लिए उभरते खतरों और कमजोरियों और संरचित विश्लेषणात्मक कार्यप्रणाली के विकास पर अनुसंधान. • साइबर हमलों के प्रति बैंक की रक्षात्मक और उत्तरदायी क्षमताओं को मापने के लिए बैंक के महत्वपूर्ण बुनियादी ढांचे पर योजनाबद्ध अंतराल पर रेड टीम/ब्लू टीम अभ्यास का आयोजन. • गहन जांच और रूट साइबर एक्शन एनालिसिस (RCA) करने के लिए L1 और L2 घटना संचालकों को तकनीकी घटना अनुक्रिया दिशानिर्देश प्रदान करना ताकि पूरी साइबर किलर चेन की स्थापना की जा सके. • एसओसी द्वारा एकत्र किए गए लॉग का विश्लेषण और सहसंबंध करके फोरेंसिक जांच में भाग लेना. • प्रबंधन के लिए विश्लेषणात्मक डैशबोर्ड और रिपोर्ट की संकल्पना करना, तैयार करना और प्रदर्शित करना. • विनियामक विवरणियों का समय पर प्रस्तुतन सुनिश्चित करना • बैंक और नियामकों द्वारा आयोजित साइबर अभ्यास, तालिका शीर्ष अभ्यास में प्रभावी रूप से भाग लेना. • आईएम टीम के कार्य और कार्यभार का प्रबंधन करना और 24X7X365 एसओसी परिचालनों के लिए शिफ्ट हैंड–ऑफ गतिविधियों का प्रबंध करना. • प्रशिक्षण और कार्यशालाओं के माध्यम से आईएम टीम की क्षमता बढ़ाना

		मुख्य दायित्व क्षेत्र (केआरए): • एसओसी के भीतर घटना प्रबंधन कार्यों का प्रबंधन करना और वैधानिक और नियामक आवश्यकताओं के लिए प्रक्रिया अनुपालन सुनिश्चित करना. • सुरक्षा घटनाओं के लिए पता लगाने, प्रतिक्रिया और पुनप्राप्ति की प्रक्रियाओं का स्चचालन करना. • आईएसओ 27035 के समक्ष बेंच मार्किंग हासिल करना. • तात्कालिक सक्रिय खतरे का पता लगाने और संभावित सुरक्षा घटना की रोकथाम के लिए एसओसी में खतरे की जानकारी अंतर्निहित करना. • सुरक्षा ऑर्केस्ट्रेशन, स्वचालन और प्रतिक्रिया के लिए प्लेबुक को लागू करने के लिए आईटी सेटअप को व्यवस्थित करने में आईटी और कारोबार के साथ सहयोग करना. • झूठी सकारात्मक सुरक्षा घटनाओं को कम करना • P0, P1, P2, P3 (P0 साइबर संकट और P3 कम गंभीरता वाला) में घटनाओं को प्राथमिकता देना. • व्यक्तिगत योगदानकर्ता के रूप में P0 एवं P1 घटनाओं को उत्पन्न करने के लिए सीधे जिम्मेदार. • एसओसी निगरानी और पहचान क्षमताओं को मजबूत करने के लिए शिक्षण को कार्यान्वित करना. • नियामकों और आंतरिक हितधारकों को समय पर विभिन्न रिपोर्ट प्रस्तुत करना सुनिश्चित करना • एसओसी द्वारा मिलाए गए सहसंबद्ध और विश्लेषित लॉग का उपयोग करते हुए फोरेंसिक जांच में प्रभावी रूप से भाग लेना. सुरक्षा घटनाओं के आरसीए पर पहुंच. • सुनिश्चित करें कि एसओसी सेटअप स्वयं सुरक्षित किला बना हुआ है • दैनंदिन एसओसी संबंधित रणनीतिक, परिचालनात्मक और युक्तिपरक दृष्टिकोणों के लिए आईटी में हितधारकों तथा अन्य के साथ घनिष्ठ रूप से सहयोग करना.
30.	**मुख्य प्रबंधक (सिक्योरिटी एनालिटिक्स एंड ऑटोमेशन) (एसएमजीएस-IV)**	**कार्य की रूपरेखा:** • सामान्य L1 / L2 गतिविधियों जैसे अलर्ट ट्राइज, संदर्भ और संवर्धन, लाइव थ्रेड फीड्स, घटना प्रतिक्रिया आदि के स्वचालन के प्रयासों का नेतृत्व करते हुए, एसओसी परिवर्तन के लिए जिम्मेदार. • सुरक्षा निगरानी और एनालिटिक्स स्वचालन रणनीति और पहचानने की प्रक्रिया जो अधिकतम एसओसी दक्षता और प्रभावशीलता सुनिश्चित करने के लिए स्वचालित और योजनाबद्ध हो सकती है. • उपयोगकर्ताओं, नेटवर्क, होस्ट और सामग्री की विसंगतियों का पता लगाने में सहायता के लिए उपयोगकर्ताओं और संस्थाओं का सांख्यिकीय विश्लेषण. • दुर्भावनापूर्ण उपयोगकर्ता या समझौता किए गए सिस्टमों/उपयोगकर्ता क्रेडिन्शियल्स द्वारा संभावित आंतरिक खतरे पर पहुंचने के लिए उपयोगकर्ता और इकाई व्यवहार विश्लेषण पर मजबूत उपयोग के मामलों का निर्माण करने के लिए पीआईएमएस, आईएएम, डीएलपी और सीबीएस, एचआरएमएस आदि जैसे विभिन्न आईटी प्रणालियों के लिए गैर–आईटी प्रासंगिक डेटा का लाभ उठाना. • थ्रेट इंटेलिजेंस क्यूरेशन और इसे एसओसी मॉनिटरिंग टूल के उपभोग के लिए स्वचालित करना. • ऑटोमेशन और ऑर्केस्ट्रेशन क्षमताओं को समझने, परिभाषित करने, विकसित करने और एकीकृत करने के लिए आईटी विभागों, थ्रेट इंटेलिजेंस, घटना प्रबंधन और फोरेंसिक टीमों के साथ मिलकर काम करना. • नए प्रयोग के मामलों की समीक्षा और सत्यापन के लिए सुरक्षा घटना प्लेबुक के निर्माण और अनुकूलन का प्रबंधन करना. • सुरक्षा घटनाओं के लिए प्रतिक्रियाशील समय का पता लगाने (एमटीटीआर) और प्रत्युत्तर देने में माध्य समय (एमटीटीआर) में मापने योग्य कमी लाना. • अन्य डोमेन में उसी प्रकार की होने वाली घटनाओं से बचने के लिए घटनाओं पर आधारित सलाह जारी करना. • सक्रिय कदम उठाने के लिए बाहरी खतरे की आसूचना के आधार पर आईटी और कारोबार में हितधारकों को सलाह जारी करना. • प्रतिक्रियाशील से प्रागाक्ति एसओसी के लिए क्षमताओं को बढ़ाना. • सुरक्षा घटना प्रबंधन पर एसओसी और आईटी टीमों के भीतर विशेषज्ञता विकसित करना • घटनाओं, शिक्षण, विश्लेषण के ज्ञान भंडार को बनाए रखना. • किसी भी नए एसओसी समाधान/कार्यात्मक मॉड्यूल की अवधारणा का प्रमाण (पीओसी). • सुरक्षा विश्लेषिक उपयोग मामले तैयार करना, उभरते खतरों और प्रौद्योगिकियों का अनुसंधान और विकास, थ्रेड इंटेलिजेंस संग्रहण, उत्पाद इंजीनियरिंग और प्रक्रिया में सुधार के लिए अन्य एसओसी टीम की सहायता करना. **मुख्य दायित्व क्षेत्र (केआरए):** • एल 1 और एल 2 एसओसी विश्लेषकों के नियमित अलर्ट/घटनाओं की रिपोर्टिंग का स्वचालन. • प्लेबुक के माध्यम से सुरक्षा ऑर्केस्ट्रेशन, स्वचालन और प्रतिक्रिया गतिविधियों को स्वचालित करना • एमटीटीढी और एमटीटीआर में मापने योग्य कमी लाना. • नए उपयोग मामलों की समीक्षा और सत्यापन करना. • एसओसी द्वारा मिलान की गई लाखों घटनाओं का लाभ उठाते हुए सुरक्षा विश्लेषिकी मॉडल की परिकल्पना और विकास करना. • एसओसी को प्रतिक्रियाशील से प्रागोक्ति एसओसी में रुपांतरित करना. • सर्वर के साथ विवेचनात्मक रूप से पूर्ण महत्वपूर्ण सुरक्षा घटनाओं को उत्पन्न करने के लिए एसओसी की क्षमताओं को बढ़ाना. • सुरक्षा विश्लेषिक उपयोग मामले तैयार करना, उभरते खतरों और प्रौद्योगिकियों का अनुसंधान और विकास, थ्रेड इंटेलिजेंस संग्रहण, उत्पाद इंजीनियरिंग और प्रक्रिया में सुधार के लिए अन्य एसओसी टीम की सहायता करना. • सुनिश्चित करें कि एसओसी सेटअप स्वयं सुरक्षित किला बना हुआ है • दैनंदिन एसओसी संबंधित रणनीतिक, परिचालनात्मक और युक्तिपरक दृष्टिकोणों के लिए आईटी में हितधारकों तथा अन्य के साथ घनिष्ठ रूप से सहयोग करना.
31.	**मुख्य प्रबंधक (एसओसी इंफ्रास्ट्रक्चर मैनेजमेंट) (एसएमजीएस-IV)**	**कार्य की रूपरेखा:** • यूएटी और उत्पादन वातावरण में एसओसी इंफ्रा की स्थापना, एकीकरण, प्रोविजनिंग, डी–प्रोविजनिंग सहित एसओसी इंफ्रास्ट्रक्चर के आद्योपांत प्रबंधन के लिए जिम्मेदार. • सेटिंग्स/हार्डनिंग के सुरक्षित विन्यास का कार्यान्वयन, पैचों को लागू करके भेद्यताओं/कमजोरियों को बंद करना, एसआईआर इंफ्रा सेटअप में संस्करण का उन्नयन. • ओएस, एप्लिकेशन, आरडीबीएमएस, वेब सर्वर, ओपन सोर्स टेक्नोलॉजीज की स्थापना और उन्हें कॉर्पोरेट आवश्यकताओं के अनुसार कॉन्फ़िगर करना. • पीआईएमएस, आईएएम, एसएसओ, एडी, एवी, आईटीएएम, आईटीएसएम, डीएलपी, एनएसी के साथ आईटी इंफ्रास्ट्रक्चर का एकीकरण • फायरफॉल्स, आईपीएस, डब्ल्यूएएफ आदि जैसी सुरक्षा तकनीकों को लगाकरआईटी इन्फ्रास्ट्रक्चर की सुरक्षा • अपटाइम प्रबंधन, लैन का प्रबंधन और कॉर्पोरेट नेटवर्क के साथ एकीकरण, • क्रेडेंशियल/उपयोगकर्ता प्रबंधन, भूमिकाएं और समूह प्रबंधन, आईटी/एसओसी बुनियादी ढांचे पर प्रशासनिक गतिविधियां शुरू करना. • कई विक्रेताओं और ओईएम के साथ आईटी इन्फ्रा संबंधित एसएलए प्रबंधन • व्यवसाय निरंतरता और डीआर योजना का विकास करना और विभिन्न डीआर ड्रिलों में भाग लेना • सुनिश्चित करना कि एसओसी सेटअप आरटीओ और आरपीओ से उचित रूप से स्वीकार्य है. • सुनिश्चित करना कि एसओसी सेटअप बैंक की नीतियों और विनियामक और वैधानिक आवश्यकताओं के अनुसार है. • डेटा के सुरक्षित संचार, प्रसंस्करण और भंडारण के लिए एन्क्रिप्शन, हैशिंग तकनीक का कार्यान्वयन. **मुख्य दायित्व क्षेत्र (केआरए):** • यूएटी और उत्पादन वातावरण में एसओसी परिसंपत्तियों के शिपमेंट/प्लेसमेंट/प्रतिस्थापन और प्रोविजनिंग/डीप्रोविजनिंग सहित आद्योपांत एसओसी इंफ्रास्ट्रक्चर का प्रबंध करना. • कॉर्पोरेट आवश्यकता के अनुसार अपटाइम का प्रबंध करना. • एसओसी इन्फ्रा को सिक्योर कॉन्फिगरेशन डॉक्यूमेंट (एससीडी) को लागू करके सुरक्षित रखना और संपूर्ण एसओसी इन्फ्रास्ट्रक्चर में भेद्यता मूल्यांकन का अनुपालन. • सभी प्रौद्योगिकियों में संस्करण उन्नयन/पैच प्रबंधन और कंट्रोल बनाए रखना. • सुनिश्चित करना कि एसओसी सेटअप स्वयं सुरक्षित किला बना हुआ है • एसओसी की क्षमता योजना (बुनियादी ढांचे–हार्डवेयर का उन्नयन). • बैकअप/पुन: स्थापन, टेप उपकरण संचलन, आईएसएमएस प्रक्रिया के अनुसार बैकअप/पुन: स्थापन का परीक्षण • स्वीकार्य आरटीओ और आरपीओ का प्रबंध करना • विभिन्न माध्यमों से और बैंक के विभिन्न डीआर बीसीपी ड्रिल के दौरान एसओसी आरटीओ तथा आरपीओ को सिद्ध करना. • दैनंदिन एसओसी संबंधित रणनीतिक, परिचालनात्मक और युक्तिपरक दृष्टिकोणों के लिए आईटी में हितधारकों तथा अन्य के साथ घनिष्ठ रूप से सहयोग करना.
32.	**मुख्य प्रबंधक (एसओसी गवर्नेन्स) (एसएमजीएस-IV)**	**कार्य की रूपरेखा:** • अभिशासन टीम का नेतृत्व करना और सूचना सुरक्षा नीति, साइबर सुरक्षा नीति, डेटा अभिशासन नीति और संबंधित प्रक्रियाओं सहित विभिन्न नीतियों को लागू करने के लिए जिम्मेदार होगा. • आईएसओ 27001, 27002, 27035 मानकों को लागू करना. • नीतियों, मानकों, प्रक्रिया और दिशानिर्देशों के साथ संरेखित एसओसी संचालन के लिए विभिन्न एसओपी की अवधारणा, विकास और समीक्षा करना. • एसओसी इंफ्रास्ट्रक्चर और परिचालनों में सुरक्षा सुनिश्चित करने के लिए रणनीति विकसित करना, तकनीकों का प्रयोग करना

		• ओईएम द्वारा जारी किए गए विभिन्न एसओसी इंफ्रास्ट्रक्चर और अनुप्रयोगों के नए संस्करणों और पैच की खोज करना और यह सुनिश्चित करना कि उन्हें निर्धारित समय सीमा के भीतर एसओसी द्वारा लगाया जाए. • इंफ्रास्ट्रक्चर और प्रक्रिया स्तर की भेद्यताओं को बंद करने के लिए एसओसी इंफ्रा टीम को मार्गदर्शन प्रदान करना • सुनिश्चित करना कि एसओसी का मुख्य उद्देश्यों का सही सकारात्मक घटनाओं को शामिल करने के लिए पालन किया जाता है/आईटी, कारोबार और व्यक्तिगत उपयोगकर्ताओं जैसे भी लागू हो, हितधारकों को अलर्ट भेजा जाता है. • सुनिश्चित करना कि एसओसी हर गतिविधि का केन्द्र बिन्दु बने जो बैंक की सुरक्षा को प्रभावित कर सके . • परिवर्तन, पैच, उपयोगकर्ता, एसओडी, अपटाइम प्रबंधन की समीक्षा करना. • एसओसी बुनियादी ढांचे की चौबीसों घंटे स्वास्थ्य निगरानी. • एसएलए के अनुसार एसओसी डिवाइसों को सुनिश्चित करना. • बैंक की आवश्यकताओं के अनुसार डीआर बीसीपी ड्रिल का प्रबंध करना. • सुनिश्चित करना कि सभी वैधानिक और नियामक रिपोर्टिंग समयबद्ध तरीके से किये जाते हैं. • सुनिश्चित करना कि बैंक के सभी कर्मचारी सदस्य और विक्रेता साझेदार सूचना सुरक्षा से संबंधित नीतियों, मानकों, प्रक्रियाओं, दिशानिर्देशों और एसओपी से अच्छी तरह वाकिफ हैं• और दिन-प्रतिदिन के कार्यों का पालन कर रहे हैं. • दैनंदिन एसओसी संबंधित रणनीतिक, परिचालनात्मक और युक्तिपरक दृष्टिकोणों के लिए आईटी में हितधारकों तथा अन्य के साथ घनिष्ठ रूप से सहयोग करना. **मुख्य दायित्व क्षेत्र (केआरए) :** • सुनिश्चित करना कि एसओसी परिचालन विभिन्न नीतियों के अनुपालन में हैं. • आईएसओ 27001, 27002, 27035 को प्राप्त करना और उसे बनाए रखना • एनआईएसटी ढांचे, निर्धारणों, डेटा सुरक्षा कानूनों को लागू करना • सुनिश्चित करना कि एसओसी सेटअप स्वयं सुरक्षित किला बना हुआ है. • यह सुनिश्चित करने के लिए एसओपी विकसित करना कि एसओसी संचालन सुरक्षित तरीके से प्रबंधित किए जाते हैं. • सांविधिक और नियामक रिपोर्टें समय पर प्रस्तुत करना.
33.	**मुख्य प्रबंधक (सायबर सिक्योरिटी-एथिकल हैकिंग) (एसएमजीएस-IV)**	• बैंक के भीतर साइबर सुरक्षा कार्यक्रम के लिए समग्र पर्यवेक्षण और रणनीतिक दिशा देना. • समय-समय पर आंतरिक एथिकल हैकिंग अभ्यास गतिविधियों का प्रबंध और नेतृत्व करना. • हितधारकों के साथ सक्रिय रूप से जुड़ना, कारोबार के प्रबंधन और लेखा परीक्षकों के साथ मजबूत संबंधों का निर्माण, भेद्यता खोज और सुधारात्मक प्रयासों को सुविधाजनक बनाना. • एप्लिकेशन सुरक्षा आकलन में भाग लेना. • नेटवर्क सुरक्षा आकलन और सुरक्षा कॉन्फ़िगरेशन समीक्षा करना • आंतरिक नैतिक हैकिंग और लाल टीम (IEHRT) अभ्यास का पर्यवेक्षण करना.
34.	**मुख्य प्रबंधक (सायबर सिक्योरिटी-डिजिटल फॉरेन्सिक) (एसएमजीएस-IV)**	• बैंक के भीतर साइबर सुरक्षा कार्यक्रम के लिए समग्र पर्यवेक्षण और रणनीतिक दिशा देना. • डिजिटल फॉरेंसिक विश्लेषण गतिविधियों का प्रबंधन, लोड और पर्यवेक्षण करना. • डिजिटल और अन्य साक्ष्यों की फॉरेंसिक जाँच करना और फॉरेंसिक टूल्स (वाणिज्यिक और ओपन सोर्स टूल्स) का उपयोग करके फोरेंसिक जांच के लिए घटनाओं का विश्लेषण करना. • हितधारकों के साथ सक्रिय रूप से जुड़ना, कारोबार के प्रबंधन और लेखा परीक्षकों के साथ मजबूत संबंधों का निर्माण, भेद्यता खोज और सुधारात्मक प्रयासों को सुविधाजनक बनाना. • मानक संचालन प्रक्रियाओं (एसओपी) और सुरक्षा समाधान दस्तावेज तैयार करना.
35.	**मुख्य प्रबंधक (सायबर सिक्योरिटी-थ्रेट हन्टिंग) (एसएमजीएस-IV)**	• बैंक के भीतर साइबर सुरक्षा कार्यक्रम के लिए समग्र पर्यवेक्षण और रणनीतिक दिशा देना. • डिजिटल फॉरेंसिक विश्लेषण गतिविधियों का प्रबंधन, लोड और पर्यवेक्षण करना. • डिजिटल और अन्य साक्ष्यों की फॉरेंसिक जाँच करना और फॉरेंसिक टूल्स (वाणिज्यिक और ओपन सोर्स टूल्स) का उपयोग करके फोरेंसिक जांच के लिए घटनाओं का विश्लेषण करना. • हितधारकों के साथ सक्रिय रूप से जुड़ना, कारोबार के प्रबंधन और लेखा परीक्षकों के साथ मजबूत संबंधों का निर्माण, भेद्यता खोज और सुधारात्मक प्रयासों को सुविधाजनक बनाना. • मानक संचालन प्रक्रियाओं (एसओपी) और सुरक्षा समाधान दस्तावेज तैयार करना.

टिप्पणी : उपर्युक्त जॉब प्रोफाइल और केआरए के अतिरिक्त, बैंक द्वारा किसी भी पद के लिए समय-समय पर भूमिकाएँ सौंपी जा सकती हैं.

(घ) पुष्टि प्रक्रिया: चयनित अभ्यर्थी के प्रदर्शन का मूल्यांकन मूल्यांकन प्रणाली के माध्यम से किया जाएगा और बैंक में केवल सफल अभ्यर्थियों की पुष्टि की जाएगी.

(ङ) पारिश्रमिक:

क्रमांक	ग्रेड	वेतनमान
1	जूनियर मैनेजमेंट ग्रेड स्केल I (जेएमजीएस I)	23700-980/7-30560-1145/2-32850-1310/7-42020
2	मिडल मैनेजमेंट ग्रेड स्केल II (एमएमजीएस II)	31705-1145/1-32850-1310/10-45950
3	मिडल मैनेजमेंट ग्रेड स्केल III (एमएमजीएस III)	42020-1310/5-48570-1460/2-51490
4	सीनियर मैनेजमेंट ग्रेड स्केल IV (एमएमजीएस-IV)	50030-1460/4-55870-1650/2-59170

यहां, विभिन्न ग्रेड को लागू वेतनमान दिया गया है. अधिकारी समय-समय पर प्रभावी महंगाई भत्ता, मकान किराया भत्ता, नगर प्रतिपूर्ति भत्ता, भविष्य निधि, अंशदायी पेंशन फ़ंड, एलएफसी, चिकित्सा सुविधा आदि पाने के पात्र होंगे

च. आवेदन कैसे करें:

अभ्यर्थियों का मान्य ईमेल आईडी हो जिसे परिणाम घोषित होने तक सक्रिय रखा जाए. इससे उसे अपना कॉल लेटर/साक्षात्कार संबंधी सूचना आदि ईमेल के माध्यम से प्राप्त करने में सहायता होगी.

ऑनलाइन आवेदन करने के लिए दिशा-निर्देश:

i. अभ्यर्थी एसबीआई की वेबसाइट **https://bank.sbi/careers** या **https://www.sbi.co.in/careers** पर उपलब्ध लिंक के माध्यम से अपना ऑनलाइन पंजीकरण करेंगे.

ii. अभ्यर्थी पहले तो अपने हाल के फोटो और हस्ताक्षर स्कैन करें. ऑनलाइन आवेदन तब तक पंजीकृत नहीं होगा जब तक कि अभ्यर्थी अपनी फोटो और हस्ताक्षर ऑनलाइन पंजीकरण पेज पर बताए अनुसार ('आवेदन कैसे करें' के अंतर्गत) नहीं कर देता/देती.

iii. अभ्यर्थी आवेदन को ध्यानपूर्वक पढ़ें. आवेदन पूरी तरह से भरने के बाद तो अभ्यर्थी इसे प्रस्तुत करें. यदि एक बार में अभ्यर्थी आवेदन नहीं भर पाता है, तो वह पहले से प्रविष्ट जानकारी को सेव कर सकता/सकती है. जब जानकारी/आवेदन को सेव किया जाएगा तो एक अनंतिम पंजीकरण नंबर और पासवर्ड सिस्टम द्वारा बन कर आ जाएगा और यह स्क्रीन पर दिखेगा. **अभ्यर्थी इस पंजीकरण नंबर और पासवर्ड को अपने पास लिख कर रखे लें.** वे इस सेव किए हुए आवेदन को पंजीकरण नंबर और पासवर्ड का प्रयोग कर फिर से खोल सकते हैं और यदि आवश्यक हो तो दिए गए विवरण में संशोधन कर सकते हैं. सेव की गई जानकारी को इस तरह से बदल कर संशोधन करने की अनुमति मात्र तीन बार तक करने के लिए ही होगी. आवेदन जब पूरी तरह से भरा जाएगा तब अभ्यर्थी को चाहिए कि वह इसे प्रस्तुत करें और ऑनलाइन शुल्क का भुगतान करें.

iv. ऑनलाइन पंजीकरण हो जाने के बाद, अभ्यर्थियों को यह सलाह दी जाती है कि वे सिस्टम के बनाए ऑनलाइन आवेदन प्रपत्रों का प्रिन्ट आउट ले लें.

शुल्क के भुगतान के लिए दिशा-निर्देश:

i. सामान्य/ओबीसी/ईडब्ल्यूएस अभ्यर्थियों के लिए आवेदन शुल्क और सूचना शुल्क (अप्रतिदेय) ₹750/- है (सात सौ पचास रुपए मात्र) और अनुसूचित जाति/अनुसूचित जनजाति/दिव्यांग व्यक्ति के अभ्यर्थियों के लिए सूचना शुल्क ₹125/- है (एक सौ पच्चीस रुपए मात्र).

ii. शुल्क का भुगतान उपलब्ध भुगतान गेटवे के माध्यम से ऑनलाइन ही करना होगा.

iii. आवेदन पत्र के विवरण सही हैं यह सुनिश्चित कर लेने के बाद अभ्यर्थी द्वारा आवेदन के साथ समेकित रूप से भुगतान गेटवे के माध्यम से शुल्क का भुगतान करना होगा. **इसके बाद आवेदन में कोई परिवर्तन/संशोधन की अनुमति नहीं दी जाएगी.**

iv. भुगतान डेबिट कार्ड/क्रेडिट कार्ड/इन्टरनेट बैंकिंग आदि द्वारा स्क्रीन पर बताई जानकारी के अनुसार किया जा सकता है. ऑनलाइन भुगतान करते समय यदि कोई लेनदेन शुल्क लागू हो तो वह अभ्यर्थियों को ही वहन करना होगा.

v. भुगतान कार्य सफलतापूर्वक हो जाने के बाद अभ्यर्थी द्वारा प्रस्तुत किए जाने की तारीख के साथ ई-रसीद और आवेदन फॉर्म बनेगा जिसे प्रिन्ट कर अभ्यर्थी अपने पास रख ले.

vi. यदि पहली बार में शुल्क का भुगतान नहीं हो पाता है, तो ऑनलाइन भुगतान के लिए फिर से प्रयास करें.

vii. शुल्क विवरणों सहित ई-रसीद और आवेदन फॉर्म का प्रिन्ट फिर से करने का भी प्रावधान है.

viii. भुगतान किया गया आवेदन शुल्क किसी भी तरह से वापस **नहीं** लौटाया जाएगा, **न** ही इसे किसी अन्य परीक्षा या फिर भावी चयन के लिए समायोजित किया जाएगा.

छ. प्रलेखों को अपलोड कैसे करें:

अ. अपलोड किए जाने वाले प्रलेखों का विवरण:

i. संक्षिप्त रेस्यूम (पीडीएफ)
ii. आईडी प्रमाण (पीडीएफ)
iii. जन्म तिथि का प्रमाण (पीडीएफ)
iv. शैक्षणिक योग्यता: संगत अंक तालिका/डिग्री प्रमाणपत्र (पीडीएफ)
v. अनुभव प्रमाणपत्र (पीडीएफ)
vi. जाति प्रमाण–पत्र/ओबीसी प्रमाण–पत्र/ईडब्ल्यूएस प्रमाण–पत्र, यदि लागू हो (पीडीएफ)
vii. पीडब्ल्यूडी प्रमाणपत्र, यदि लागू हो (पीडीएफ)

ब. फोटोग्राफ फाइल टाइप/साइज़:

i. पासपोर्ट आकार की हाल में खिंची हुई रंगीन फोटो.
ii. फाइल का आकार 20 केबी–50 केबी और आयाम 200X230 पिक्सल तक होना चाहिए.
iii. यह सुनिश्चित कर लें कि फोटो रंगीन है, और सफेद या हल्के रंग की पृष्ठभूमि में लिया गया हो.
iv. तनावमुक्त होकर कैमरे में सामने की ओर देखें.
v. फोटो यदि धूप में ली गई हो तो सूरज आपके पीछे रहे या आप छाया में हों ताकि आपकी नज़र में तिरछापन न आए या फिर कोई भारी छाया न पड़े.
vi. यदि आपको फ्लैश का प्रयोग करना होता है, तो आप यह सुनिश्चित करें कि इसमें रैड–आई नहीं है.
vii. यदि आप चश्मा लगाते हैं, तो यह सुनिश्चित करें कि कोई परछाई नहीं पड़ रही है और आपकी आंखें साफ देखी जा सकती हैं.
viii. टोपी, हैट और गहरे रंग का चश्मा लगाया जाना स्वीकार्य नहीं है. धार्मिक प्रतीक पगड़ी आदि बांध सकते हैं लेकिन इससे आपका चेहरा न ढकने पाए.
ix. यह सुनिश्चित करें कि स्कैन किया गया चित्र 50 केबी से अधिक का नहीं है. फाइल का आकार यदि 50 केबी से अधिक का है, तो स्कैनिंग की प्रक्रिया के दौरान डीपीआई रिजोल्यूशन, रंगों की संख्या आदि जैसी बातें स्कैनर पर सेट करके समायोजित कर लें.

स. हस्ताक्षर फाइल का प्रकार/आकार:

i. आवेदक सफेद कागज पर काली स्याही के पैन से हस्ताक्षर करें.
ii. हस्ताक्षर आवेदक स्वयं करे न कि कोई अन्य व्यक्ति.
iii. कॉल लेटर तथा जहां आवश्यक होंगे वहां आपके हस्ताक्षर का प्रयोग किया जाएगा.
iv. यदि परीक्षा के समय उत्तर पुस्तिका पर आवेदक के हस्ताक्षर कॉल लेटर के हस्ताक्षर से मेल नहीं खाते तो आवेदक अयोग्य हो जाएगा/जाएगी.
v. फाइल का आकार 10 केबी–20 केबी के बीच का हो और आयाम 140X60 पिक्सल (अधिमानत:) हो.
vi. यह सुनिश्चित करें कि स्कैन किए गए चित्र का आकार 20 केबी से अधिक नहीं है.
vii. अंग्रेज़ी के बड़े अक्षरों में किए गए हस्ताक्षर स्वीकार्य नहीं होंगे.

द. प्रलेख की फाइल का प्रकार/आकार:

i. सभी प्रलेख पीडीएफ प्रारूप में होने चाहिए.
ii. प्रलेख के पेज का आकार ए4 का हो.
iii. फाइल का आकार 500 केबी से अधिक का न हो.

प्रलेख की फाइल का प्रकार/आकार (जारी.....)

iv. प्रलेख को यदि स्कैन किया जा रहा है तो आप यह सुनिश्चित करें कि इसे पीडीएफ के रूप में सेव कर लिया गया है और इसका आकार पीडीएफ के तौर पर 500 केबी से अधिक का नहीं है. फाइल का आकार यदि 500 केबी से अधिक का है तो स्कैनर की सेटिंग की प्रक्रिया के दौरान डीपीआई का रिज़ोल्यूशन, रंगों की संख्या आदि समायोजित करें. यह सुनिश्चित कर लें कि अपलोड किए गए प्रलेख साफ और पढ़े जा सकने लायक हैं.

य. फोटो/हस्ताक्षर/प्रलेखों को स्कैन करने हेतु दिशा–निर्देश:

i. स्कैनर के रिज़ोल्यूशन को कम से कम 200 डीपीआई (डॉट्स प्रति इन्च) पर रखें.
ii. कलर को ट्रू कलर पर सेट करें.
iii. फोटो/हस्ताक्षर के किनारे तक क्रॉप करके फोटो को स्कैन करें फिर फोटो को अंतिम आकार (जैसा ऊपर बताया गया है) देने के लिए क्रॉप करने हेतु अपलोड एडिटर का प्रयोग करें.
iv. फोटो/हस्ताक्षर की फाइल जेपीजी या जेपीईजी प्रारूप में हो (यानी फाइल का नाम image01.jpg या image01.jpeg दिखाई दे)
v. इमेज के आयाम फोल्डर/फाइल की लिस्टिंग कर जांचे जा सकते हैं या फिर फाइल इमेज के आयकॅन पर माउस को घुमाकर इसे जांचा जा सकता है
vi. जो अभ्यर्थी एमएस विन्डोज़/एमएस ऑफिस का प्रयोग करते हैं, वे आसानी से फोटो और हस्ताक्षर जेपीईजी फार्मेट में पा सकते हैं जो कि क्रमश: 50 केबी और 20 केबी से अधिक न होगी, इसके लिए एमएस पेन्ट या एमएस ऑफिस पिक्चर मैनेजर का प्रयोग करना होगा. स्कैन किया गया फोटो या हस्ताक्षर किसी भी फार्मेट सें जेपीजी (jpg) फार्मेट में सेव किए जा सकते हैं. इसके लिए फाइल मेन्यू में 'सेव ऐज़' के विकल्प का प्रयोग करना होगा. इमेज मेन्यू द्वारा क्रॉप और रिसाइज़ (बिंदु 1 और 2 ऊपर देखें जो कि पिक्स्ल आकार के लिए दिया हुआ है) विकल्प चुनकर फाइल के आकार को 50 केबी (फोटो) और 20 केबी (हस्ताक्षर) से कम कराया जा सकता है. इसी तरह से अन्य फोटो एडीटर में भी विकल्प उपलब्ध हैं.
vii. ऑनलाइन आवेदन फार्म भरते समय अभ्यर्थी को एक लिंक उपलब्ध करवाया जाएगा ताकि वह अपने फोटो और हस्ताक्षर को अपलोड कर सके.

र. प्रलेख अपलोड करने की प्रक्रिया:

i. हर प्रलेख को अपलोड करने हेतु अलग से लिंक दिए गए हैं.
ii. ''अपलोड'' का संबंधित लिंक क्लिक करें.
iii. ब्राउज़ करके उस जगह को चुनें जहां कि जीपीजी या पीडीएफ, डीओसी या डीओसीएक्स फाइल को सेव किया गया है.
iv. फाइल पर क्लिक कर इसे चुनें और अपलोड का बटन क्लिक करें.
v. आवेदन सबमिट करने से पहले प्रलेख अपलोड हो गया है और सही तरह से खुल रहा है, इस बात की पुष्टि करने के लिए प्रिव्यू क्लिक करें. यदि फाइल का आकार और प्रारूप बताए अनुसार नहीं है तो इसमें त्रुटि का संदेश आएगा.
vi. प्रलेख अपलोड हो जाने के बाद/प्रस्तुत कर दिए जाने के बाद संशोधित/परिवर्तित नहीं हो सकेंगे.
vii. ऑनलाइन आवेदन फार्म में फोटो/हस्तातक्षर अपलोड कर दिए जाने के बाद अभ्यर्थी जांच लें कि फोटो साफ हैं और ये ठीक तरह से अपलोड हुए हैं. फोटो या हस्ताक्षर स्पष्ट रूप से यदि नहीं दिखें तो अभ्यर्थी अपने आवेदन को संशोधित कर सकता/सकती है और अपने फोटो या हस्ताक्षर आवेदन फार्म प्रस्तुत किए जाने से पहले फिर से अपलोड कर सकता/सकती है. फोटो से चेहरा या हस्ताक्षर यदि स्पष्ट नहीं हैं तो अभ्यर्थी का आवेदन अस्वीकार किया जाएगा.

नोट: यदि फोटो में चेहरा या हस्ताक्षर अस्पष्ट है, तो अभ्यर्थी का आवेदन खारिज कर किया जा सकता है. यदि फोटो या हस्ताक्षर प्रमुख रूप से दिखाई नहीं देते हैं, तो अभ्यर्थी अपने आवेदन को संपादित कर सकता है और केएम प्रस्तुत करने से पहले अपने फोटोग्राफ या हस्ताक्षर को फिर से लोड कर सकता है.

ज. चयन प्रक्रिया: (पद क्र.सं; 1 से 24 के लिए):

पद क्र.सं. 1 से 24 के लिए अभ्यर्थियों का चयन ऑनलाइन लिखित परीक्षा और साक्षात्कार के बाधार पर किया जाएगा.

ऑनलाइन लिखित परीक्षा: ऑनलाइन लिखित परीक्षा अनंतिम रूप से 20.10.2019 को आयोजित की जाएगी. परीक्षा का कॉल लेटर बैंक की वेबसाइट पर अपलोड किया जाएगा और अभ्यर्थियों को एसएमएस और ई–मेल के माध्यम से भी सूचित किया जाएगा. अभ्यर्थियों को कॉल लेटर डाउनलोड करने की आवश्यकता होगी. परीक्षा गुंटूर, कुरनूल, विजयवाड़ा, विशाखापट्टनम, गुवाहाटी, सिलचर, भागलपुर, दरभंगा, मुजफ्फरपुर, पटना, चंडीगढ़/मोहाली, रायपुर, भिलाई, बिलासपुर, दिल्ली/नई दिल्ली, फरीदाबाद, गाजियाबाद, ग्रेटर नोएडा, गुरुग्राम, पणजी, अहमदाबाद, वडोदरा, अंबाला, हिसार, हमीरपुर, शिमला, धनबाद, जमशेदपुर, रांची, बेंगलुरु, हुबली, मंगलौर, कोच्चि, तिरुवनंतपुरम, भोपाल, इंदौर, औरंगाबाद, मुंबई/ठाणे/नवी मुंबई, नागपुर, पुणे, इम्फाल, शिलांग, आइजोल, कोहिमा, भुवनेश्वर, संबलपुर, पुदुचेरी, जालंधर, लुधियाना, मोहाली, पटियाला, जयपुर, उदयपुर, बर्दांग/गंगटोक, चेन्नई, मदुरै, तिरुनेलवेली, हैदराबाद, वारंगल, अगरतला, इलाहाबाद, कानपुर, लखनऊ, मेरठ, वाराणसी, देहरादून, आसनसोल, ग्रेटर कोलकाता, कल्याणी, सिलीगुड़ी केंद्रों में आयोजित की जाएगी.

अभ्यर्थी को वह केन्द्र चुनना चाहिए जहां वह परीक्षा के लिए बैठना चाहता/चाहती है. चुने गए परीक्षा केन्द्र में किसी परिवर्तन पर विचार नहीं किया जाएगा. तथापि बैंक किसी भी केन्द्र को जोड़ने या हटाने और अभ्यर्थी को उसके द्वारा चुने गए केन्द्र से भिन्न कोई अन्य केन्द्र आबंटित करने का अधिकार अपने पास सुरक्षित रखता है.

ऑनलाइन लिखित परीक्षा का पैटर्न:

क्रमांक	परीक्षण		प्रश्नों की संख्या	अंक	समय
1	सामान्य अभिरुचि*	तर्कशक्ति परीक्षण	50	50*	90 मिनट
2		मात्रात्मक अभिरुचि	35	35*	
3		अंग्रेजी भाषा	35	35*	
4	व्यावसायिक ज्ञान (PK)	सामान्य आईटी ज्ञान	25	50	70 मिनट
		भूमिका आधारित ज्ञान	50	100	

* मेरिट निकालने के लिए अर्हता की प्रकृति और उसमें अंक की गणना नहीं की जाएगी.

(क) व्यावसायिक ज्ञान (पीके) प्रश्नपत्र को छोड़कर, अन्य प्रश्न–पत्र प्रकृति में अर्हता के होंगे. इन प्रश्नपत्रों में अभ्यर्थियों को न्यूनतम अर्हताअंक प्राप्त करने होंगे. न्यूनतम अर्हता अंक तय किए जाएंगे या बैंक के विवेक पर माफ किए जा सकते हैं. प्रश्न द्विभाषी अर्थात हिंदी और अंग्रेजी में होंगे. अभ्यर्थियों के पास हिंदी या अंग्रेजी में प्रश्नों का उत्तर देने का विकल्प होगा (अंग्रेजी भाषा की परीक्षा को छोड़कर).

(ख) साक्षात्कार के लिए चयनित सूची में शामिल किए जाने के लिए पात्र होने के लिए, अभ्यर्थियों को व्यावसायिक ज्ञान परीक्षा के लिए बैंक द्वारा तय किए जाने वाले कट–ऑफ अंकों के बराबर या उससे अधिक अंक प्राप्त करने होंगे, इसके अलावा अन्य परीक्षणों में न्यूनतम योग्यता अंकों के बराबर या उससे अधिक अंक प्राप्त करने होंगे.

ऑनलाइन लिखित परीक्षा ऑनलाइन आयोजित की जाएगी. यदि आवेदनों की संख्या कम है, तो बैंक ऑनलाइन लिखित परीक्षा और साक्षात्कार के बजाय, चयनित सूची बनाने और साक्षात्कार के माध्यम से अभ्यर्थी के चयन पर विचार करने का अधिकार सुरक्षित रखता है.

साक्षात्कार: बैंक द्वारा तय किए गए अभ्यर्थियों की पर्याप्त संख्या को ऑनलाइन लिखित परीक्षा में प्रदर्शन के आधार पर साक्षात्कार के लिए बुलाया जाएगा. साक्षात्कार 25 अंकों का होगा. साक्षात्कार में अर्हक अंक बैंक द्वारा तय किए जाएंगे.

मेरिट सूची: व्यावसायिक ज्ञान परीक्षण (150 अंकों में से) और साक्षात्कार (25 अंकों में से) के अंकों को मिलाने के बाद अंतिम मेरिट सूची तैयार की जाएगी. अंको का भार इस प्रकार होगा:

ग्रेड	भारिता स्वरूप
जेएमजीएस I, एमएमजीएस II और एमएमजीएस III (पद क्र.सं; 1 से 24 के लिए)	• लिखित परीक्षा: 70% • साक्षात्कार 30%
चयन प्रत्येक श्रेणी में शीर्ष मेरिट रैंक वाले अभ्यर्थियों से किया जाएगा. नोट:– यदि एक से अधिक अभ्यर्थी कट–ऑफ अंक (कट–ऑफ पॉइंट पर सामान्य अंक) प्राप्त करते हैं, तो ऐसे अभ्यर्थी का चयन सूची में अवरोही क्रम में उनकी आयु के अनुसार किया जाएगा.	

चयन प्रक्रिया:

(पद क्र. सं. 25 से 35 के लिए):

पद क्रम संख्या 25 से 35 तक के अभ्यर्थियों का चयन चयनित सूची और साक्षत्कार के आधार पर होगा.

चयनित सूची बनाना: केवल न्यूनतम योग्यता और अनुभव पूरा करना ही किसी अभ्यर्थी को साक्षात्कार के लिए बुलाये जाने का अधिकार नहीं देता है. बैंक द्वारा गठित शॉर्ट लिस्टिंग समिति चयनित सूची बनाने के लिए मानदंड तय करेगी और उसके बाद पर्याप्त संख्या में अभ्यर्थियों, जैसा कि बैंक द्वारा तय किया गया है, की चयनित सूची तैयार की जाएगी और साक्षात्कार के लिए बुलाया जाएगा. साक्षात्कार के लिए अभ्यर्थियों को बुलाने का बैंक का निर्णय अंतिम होगा. इस संबंध में कोई पत्राचार नहीं किया जाएगा. .

साक्षात्कार: साक्षात्कार 100 अंकों का होगा. साक्षात्कार में अर्हक अंक बैंक द्वारा तय किए जाएंगे. इस संबंध में कोई पत्राचार नहीं किया जाएगा.

मेरिट सूची: चयन के लिए मेरिट सूची केवल साक्षात्कार में प्राप्त अंकों के आधार पर अवरोही क्रम में तैयार की जायेगी. एक से अधिक अभ्यर्थियों द्वारा निर्दिष्ट अंक प्राप्त करने पर (निर्दिष्ट सीमा पर एक समान अंक होने पर), ऐसे अभ्यर्थियों की मेरिट में उनकी आयु के आधार पर अवरोही क्रम में रेंक प्रदान की जायेगी.

झ. ऑनलाइन परीक्षा/साक्षात्कार के लिए कॉल लेटर :

क. ऑनलाइन परीक्षा: अभ्यर्थियों को अपने ऑनलाइन परीक्षा के लिए कॉल लेटर तथा स्वयं जाने नामक पुस्तिका अपना पंजीकरण नंबर तथा पासवर्ड/जन्म तिथि दर्ज करके बैंक की वेबसाइट से डाउनलोड करें. **कॉल लेटर/स्वयं जानें नामक पुस्तिका की प्रति डाक से नहीं भेजी जाएगी.**

ख. साक्षात्कार: साक्षात्कार के लिए घोषणा/कॉल लेटर ई-मेल द्वारा भेजे जाएंगे या बैंक की वेबसाइट पर अपलोड किये जायेंगे. कोई हार्ड प्रति नहीं भेजी जायेगी.

ञ. परीक्षा के समय परिचय का प्रमाण प्रस्तुत करना:

अभ्यर्थियों को पासपोर्ट/आधार/पैनकार्ड/ड्राइविंग लाईसेंस/मतदाता कार्ड/मूल प्रति में विधिवत् सत्यापित फोटो के साथ बैंक पासबुक जैसे एक फोटो पहचान प्रमाण और साथ ही उसकी एक स्व-सत्यापित फोटोकॉपी लानी होगी. परीक्षा हॉल में परीक्षकों को पहचान प्रमाण की एक फोटोप्रति कॉल लेटर के साथ प्रस्तुत की जानी चाहिए, ऐसा न करने पर या फिर यदि अभ्यर्थी की पहचान संबंधी संदेह होने पर अभ्यर्थी को परीक्षा में बैठने नहीं दिया जाएगा.

ट. कदाचार के दोषी पाए गए अभ्यर्थियों **के विरुद्ध कार्रवाई :**

अभ्यर्थियों को यह चेतावनी दी जाती है कि ऐसा कोई विवरण न दें/संलग्न न करें जो असत्य, जाली/बनावटी हो या आवेदनपत्र भरते समय किसी भी महत्वपूर्ण सूचना को न छिपाएँ.

यदि लिखित परीक्षा/साक्षात्कार के समय कोई अभ्यर्थी निम्नलिखित बातों का दोषी पाया जाता है :

(i) परीक्षा के दौरान अनुचित साधनों का प्रयोग करना या (ii) छद्म व्यक्ति बनकर छद्म व्यक्ति द्वारा परीक्षा देना या (iii) परीक्षा हॉल में दुर्व्यवहार करना या (iv) अभ्यर्थी के रूप में अपने चयन हेतु किसी अनियमित या अनुचित साधन का आश्रय लेना या (v) अपनी अभ्यर्थिता के संबंध में किसी भी अनुचित साधन की सहायता लेना, तो ऐसे अभ्यर्थी के विरुद्ध कानूनी कार्यवाही तो होगी ही, साथ ही:

अ) जिस परीक्षा में भाग ले रहे होंगे, उसमें उसे अयोग्य घोषित किया जाएगा.

ब) भारतीय स्टेट बैंक द्वारा संचालित भर्ती के लिए किसी भी परीक्षा से स्थायी रूप से या किसी निश्चित अवधि के लिए वंचित कर दिया जाएगा.

बैंक अभ्यर्थी के जवाबों का परीक्षा में शामिल अन्य अभ्यर्थियों के जवाबों के साथ समानता ढूँढ़ने के लिए विश्लेषण करता है. इस विश्लेषण के आधार पर यदि यह पाया जाता है कि जवाब एक जैसे हैं, और प्राप्त अंक यथार्थ/वैध नहीं है, तो बैंक के पास उम्मीदवारिता रद्द करने का अधिकार सुरक्षित है.

ठ. अभ्यर्थियों **को मोबाइल फोन, पेजर, कैलक्यूलेटर या ऐसे उपकरण का उपयोग करने की अनुमति नहीं है.**

(i) जहां परीक्षा आयोजित की जा रही है, उस परिसर में मोबाइल फोन, पेजर्स या कोई भी संचार उपकरण लाने की अनुमति नहीं है. इन अनुदेशों का पालन न करने वाले अभ्यर्थियों की अभ्यर्थिता रद्द कर दी जाएगी और भावी परीक्षाओं में शामिल होने की अनुमति न मिलने के साथ उन पर अनुशासनिक कार्रवाई भी की जाएगी.

(ii) अभ्यर्थियों को उनके हित में यह सूचना दी जाती है कि वे मोबाइल फोन/पेजर्स जैसी निषिद्ध वस्तुएं परीक्षा परिसर में न लाएं क्योंकि इन चीजों के सुरक्षित रखरखाव का आश्वासन नहीं दिया जा सकता.

(iii) अभ्यर्थियों को परीक्षा परिसर में कैलक्यूलेटर या कम्यूनिकेशन के अन्य कोई भी साधन लाने या उसका उपयोग करने की अनुमति नहीं है.

ड. बायोमेट्रिक सत्यापन:

बैंक विभिन्न चरणों में अभ्यर्थियों के अंगूठे की निशानी अभ्यर्थियों की वास्तविकता के बायोमेट्रिक सत्यापन के लिए डिजिटल प्रारूप में प्राप्त कर सकता हैं. अभ्यर्थी यह सुनिश्चित करेंगे कि अंगूठे की सही निशानी विभिन्न चरणों में ली गई है और किसी भी असंगति से उम्मीदवारी को अस्वीकार कर दिया जाएगा. यदि कोई अभ्यर्थी वास्तविक नहीं पाया जाता है, तो उसके खिलाफ कानूनी कार्रवाई करने के अलावा, उसकी अभ्यर्थिता रद्द कर दी जाएगी. इस प्रकार उन्हें सलाह दी जाती है कि अपने हाथों पर मेहंदी, स्याही, रासायनिक आदि जैसे किसी बाहरी पदार्थ को न लगाएं.

ढ. सामान्य जानकारी:

i. पद के लिए आवेदन करने से पहले आवेदक को यह सुनिश्चित करना चाहिए कि वह पद के लिए उपर्युक्तवर्णित योग्यता और अन्य मानदंडों को निर्दिष्ट तारीख को पूरा करता/करती है और कि उसके द्वारा प्रस्तुत ब्यौरा सभी प्रकार से सही है.

ii. भर्ती की किसी भी अवस्था में यदि ऐसा पता चलता है कि कोई अभ्यर्थी पात्रता मानदंडों को पूरा नहीं करता/करती है, तो और/या यह कि उसने गलत/झूठी जानकारी दी है या उसने कोई महत्वपूर्ण जानकारी (रियां) छिपाई हैं तो उसकी अभ्यर्थिता को निरस्त कर दिया जाएगा. इनमें से यदि कोई बात उसकी नियुक्ति के बाद भी पता चलती है, तो उसकी सेवाएं समाप्ति की जा सकती है.

iii. आवेदक को सुनिश्चित करना चाहिए कि आवेदन पूरी तरह से निर्धारित प्रारूप के अनुसार है और सही एवं पूरी तरह से भरा गया है.

iv. चयनित अभ्यर्थी की नियुक्ति इस शर्त पर होगी कि वह बैंक की आवश्यकता के अनुसार चिकित्सीय रूप से उपयुक्त हो. यह नियुक्ति बैंक में इस पद हेतु बैंक में कार्यभार संभालते समय जो भी सेवा और आचरण नियम लागू होंगे उनके अध्यधीन होगी.

v. अभ्यर्थियों को सूचित किया जाता है कि वे संप्रेषण जैसे कॉल लेटर/साक्षात्कार की तारीख की सूचना, आदि प्राप्त करने के लिए अपने ई-मेल को सक्रिय रखें.

vi. किसी पत्र के मिलने में विलंब होने या न मिलने के लिए बैंक की कोई जिम्मेदारी नहीं होगी.

vii. आरक्षित श्रेणी के अभ्यर्थी, जिनके लिए किसी आरक्षण का वर्णन नहीं किया गया है सहित, अनारक्षित श्रेणी के लिए घोषित रिक्त पदों के लिए आवेदन करने के लिए स्वतंत्र हैं बशर्ते वे अनारक्षित श्रेणी के लिए लागू पात्रता की सभी शर्तें पूरी करते हों.

viii. जो अभ्यर्थी सरकार/अर्ध-सरकारी कार्यालयों, बैंकों और वित्तीय संस्थानों सहित सार्वजनिक क्षेत्र के प्रतिष्ठानों में कार्यरत हैं, उन्हें सलाह दी जाती है कि वे साक्षात्कार के समय अपने नियोक्ता से लेकर अनापत्ति प्रमाणपत्र प्रस्तुत करें ऐसा न करने पर उनकी अभ्यर्थिता पर विचार नहीं किया जाएगा और वे यदि किसी यात्रा व्यय की प्रतिपूर्ति के लिए पात्र होंगे, तो उन्हें उसका भुगतान नहीं किया जाएगा.

ix. चयन की दशा में, अभ्यर्थी से अपेक्षा होगी कि वह नियुक्ति प्राप्त करते समय अपने नियोक्ता का उचित कार्यमुक्ति प्रमाणपत्र प्रस्तुत करें.

x. अभ्यर्थियों को उन्हीं के हित के लिए यह सलाह दी जाती है कि वे अंतिम तारीख से पहले समय रहते ही ऑनलाइन आवेदन प्रस्तुत कर दें और वे अंतिम तारीख का इंतज़ार न करते रहें क्योंकि बाद में हो सकता है कि वेबसाइट को लॉग ऑन करने में डिसकनेक्शन/अक्षमता/फेलियर की स्थिति बन जाए इन्टरनेट पर हैवी लोड या फिर वेबसाइट जाम होने के कारण ऐसा हो जाए. यदि पूर्वोक्त कारणों से यदि एसबीआई के नियंत्रण से बाहर के किसी भी कारण से यदि अभ्यर्थी अपना आवेदन समय रहते नहीं कर पाते हैं, तो इसके लिए एसबीआई किसी भी तरह से जिम्मेदार नहीं होगा.

xi. पात्रता, साक्षात्कार आयोजित किए जाने, अन्य. परीक्षाएं और चयन के सभी मामलों में बैंक के निर्णय अंतिम और सभी अभ्यर्थियों के लिए बाध्यकारी होंगे. इस संबंध में किसी अभ्यावेदन पर विचार नहीं जाएगा और न ही इस संबंध में कोई पत्र-व्यवहार किया जाएगा.

xii. आवेदन में दी गई जानकारी बाद में गलत पाए जाने पर आवेदक पर दीवानी/फौजदारी मुकदमा किया जा सकता है.

xiii. जहां भर्ती बिना लिखित परीक्षा के और केवल साक्षात्कार लेकर की जाती है, वहां मात्र पात्रता मानदंडों को पूरा करने पर ही यह पर्याप्त नहीं होता है कि अभ्यर्थी को साक्षात्कार के लिए बुलाया जाए. बैंक के पास यह अधिकार सुरक्षित रहता है कि वह अभ्यर्थी की आयु, योग्यता, अनुभव, उपयुक्तता आदि के संदर्भ के अनुसार आरंभिक स्क्रीनिंग/छंटाई के बाद ही साक्षात्कार के लिए अभ्यर्थियों की अपेक्षित संख्या में ही उन्हें बुलाए.

xiv. एक ही पद के लिए कई आवेदन होने की स्थिति में, अंतिम मान्य (भरा हुआ) आवेदन को ही रखा जाएगा और अन्य पंजीकरण हेतु भुगतान किये गए आवेदन शुल्क/इन्टीमेशन शुल्क को ज़ब्त कर लिया जाएगा. ऑनलाइन लिखित परीक्षा/साक्षात्कार में एक पद के लिए एक अभ्यर्थी द्वारा एकाधिक उपस्थिति पूर्णत: अस्वीकृत कर दी जाएगी/अभ्यर्थिता रद्द कर दी जाएगी.

xv. इस विज्ञापन और/या इसके जवाब में आए आवेदन के कारण किसी दावे या विवाद की दशा में कानूनी कार्यवाहियां मात्र मुंबई और मुंबई स्थित न्यायालयों/न्यायाधिकरणों/मंचों पर ही की जा सकती हैं. किसी भी मुकदमे/विवाद की सुनवाई का एकल व अनन्य अधिकार क्षेत्र मुंबई ही होगा.

xvi. लिखित परीक्षा/चयनित सूची में अर्हता प्राप्त करने के बाद साक्षात्कार के लिए बुलाए गए बाहरी अभ्यर्थियों को भारत में सबसे छोटे मार्ग के लिए एसी-III टियर (केवल मेल/एक्सप्रेस) के यात्रा किराया या वास्तविक खर्च (जो भी कम हो) की प्रतिपूर्ति की जाएगी. स्थानीय परिवहन व्यय की प्रतिपूर्ति नहीं की जायेगी. अभ्यर्थी के पद के लिए अयोग्य पाये जाने पर उन्हें साक्षात्कार के लिए उपस्थित होने की अनुमति नहीं दी जायेगी और किसी प्रकार के किराये की प्रतिपूर्ति नहीं की जायेगी.

xvii. बैंक को अधिकार होगा कि वह किसी भी अवस्था में पूरी भर्ती प्रक्रिया को रद्द कर दे.

xviii. परीक्षा के संचालन में कुछ समस्या होने की संभावना को पूरी तरह से खारिज नहीं किया जा सकता है, जो परीक्षण देना और/या जनरेट होने वाला परिणाम प्रभावित हो सकता है. ऐसी स्थिति में, इस तरह की समस्या को सुधारने के लिए हर संभव प्रयास किया जाएगा, जिसमें आवश्यक होने पर दूसरी परीक्षा का आयोजन शामिल हो सकता है.

xix. साक्षात्कार के समय, अभ्यर्थी को उसके विरुध्द लंबित आपराधिक मामलों (यदि कोई हों) का विवरण देना आवश्यक होगा. बैंक अन्य बातों के साथ-साथ पुलिस रिकॉर्ड के सत्यापन सहित स्वतंत्र सत्यापन भी कर सकता है. बैंक ऐसे प्रकटनों और/या सत्यापन के आधार पर नियुक्ति से इनकार करने को अधिकार अपने पास सुरक्षित रखता है.

किसी पूछताछ के लिए, कृपया हमसे लिंक "CONTACT US/post your query" लिंक के ज़रिए लिखें,जो कि बैंक की वेबसाइट **URL-https://bank.sbi/careers** या **https://www.sbi.co.in/careers** पर उपलब्ध है.

किसी विवाद की स्थिति में अंग्रेजी में जारी विज्ञापन मान्य होगा. प्रिंटिंग में यदि कोई त्रुटि हो, तो बैंक इसके लिए ज़िम्मेदार नहीं होगा.

मुंबई
दिनांक: 06.09.2019

महाप्रबंधक
(सीआरपीडी)