

			विनियमित इकाइयाँ / मध्यवर्तियाँ		
नियंत्रण संख्या	क्षेत्र	लेखा परीक्षा प्रश्नावली	श्रेणी-1	श्रेणी-2	श्रेणी-3
			सकल बीमा राजस्व: > = 50 करोड (आईएसएनपी का उपयोग करने वाले सभी बीमा मध्यवर्ती और वेब एग्रीगेटर्स इस श्रेणी के अंतर्गत आते हैं)	सकल बीमा राजस्व: > = 5 करोड और < 50 करोड	सकल बीमा राजस्व: < 5 करोड
1	विसंगतियाँ और घटनाएँ(डीई.ईई):	क्या संस्था की, अपवादों, अपवादों की अवधि, अपवादों को मंजूर करने की प्रक्रिया और स्वीकृति के प्राधिकार, अधिकारी(रियों) विशेष रूप से वरिष्ठ स्तर पर, जो व्यापार और अपवाद/दों के तकनीकी संदर्भ को समझने के लिए अच्छी तरह सक्षम हैं, द्वारा सावधिक आधार पर मंजूर किये गये अपवादों की समीक्षा के लिए प्राधिकार का औचित्य सिद्ध करने की शर्तों सहित कोई स्पष्ट रूप से परिभाषित नीति है?	बोर्ड द्वारा स्वीकृति	प्रबंध निदेशक की स्वीकृति	प्रबंध निदेशक की स्वीकृति
2	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या सुरक्षा लॉग का रखरखाव और निगरानी की जाती है?	हाँ	हाँ	हाँ
3	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या महत्वपूर्ण प्रणालियों और नेटवर्क की उपयोग क्षमता की निगरानी करने के लिए कोई कार्य पद्धति है ?	हाँ	हाँ	हाँ
4	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	प्रतिक्रिया रणनीति में निरंतर सुधार करने के लिए क्या सीखे गये सबक को गतिशील रूप से शामिल करने के लिए कोई कार्य प्रणाली है?	हाँ	हाँ	हाँ
5	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	जब उपयोगकर्ता सामान्य लॉगइन व्यवहार जैसे दिन का समय, कार्य केंद्र स्थान और अवधि से भटक जाते हैं तो तब संस्था चेतावनी देती है?	हाँ	हाँ	सीमित
6	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या, संस्था के उपयोगकर्ता या प्रणाली खाते जिनका पैठ परीक्षण प्रयोग के लिए किया जाता है, को यह सुनिश्चित करने के लिए कि उनका इस्तेमाल केवल वैध उद्देश्यों से हो, नियंत्रित या उनकी निगरानी की जानी चाहिए और परीक्षण के बाद हटा दिया जाता है या सामान्य कार्य के लिए बहाल किया जाता है।	हाँ	हाँ	हाँ
7	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था अंत प्रणालियों पर डिफाल्ट इन्कार नियम के साथ हॉस्ट आधारित फायरवॉल या पोर्ट फिल्टरिंग उपकरणों का प्रयोग करती है जो उन सेवाओं और नोटों के सिवाय, जो स्पष्ट रूप से अनुमत हैं, सारी ट्रैफिक को डाप करता है।	हाँ	हाँ	हाँ
8	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, यह जाँच करने के लिए कि, सुरक्षित कोडिंग क्रिया का, आंतरिक रूप से विकसित सॉफ्टवेयर का पालन करने के लिए किया जा रहा है, स्थित (स्टैटिक) और गतिशील उपकरणों को काम में लाती है।	हाँ	हाँ	हाँ
9	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, परिसंपत्ति वस्तु सूची में, हार्डवेयर परिसंपत्ति के लिए सक्रिय पोर्ट, सेवाओं और पोर्ट, सेवाओं और प्रोटोकाल संबद्ध करती है?	हाँ	हाँ	हाँ
10	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था निष्क्रियता की तय अवधि के बाद निष्क्रिय खातों को स्वतः निलंबित कर देती है।	हाँ	हाँ	हाँ
11	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था निष्क्रियता की मानक अवधि के बाद वर्कस्टेशन सत्र को स्वतः अवरुद्ध कर देती है।	हाँ	हाँ	हाँ
12	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, संस्था के ई-मेल गेट वे में प्रवेश करने वाले सभी ई-मेल संलग्नकों को ब्लॉक कर देती है, यदि संस्था के व्यापार के लिए फाइल प्रकार अनावश्यक हैं।	हाँ	हाँ	हाँ

13	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, उपक्रम की प्रणालियों को सफलतापूर्वक अनुचित लाभ उठा सकने के लिए इस्तेमाल की जा सकने वाली भेद्यताओं का पता लगाने के लिए नियमित बाहरी और आंतरिक पैठ परीक्षण करती और वेक्टरों पर हमला करती है।	हाँ (कम से कम अर्ध वार्षिक)	वार्षिक	वार्षिक
14	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था नेटवर्क, सुरक्षा और क्लाउड प्रणाली सहित यथासंभव कुछ केंद्रीकृत बिन्दुओं को प्रमाणीकरण के माध्यम से सभी खातों के लिए प्रवेश को आकार देती है।	हाँ	हाँ	हाँ
15	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था हटाये जाने योग्य मीडिया से अंतर्वस्तु को स्वचालित न होने के लिए उपकरणों को आकार देती है।	हाँ	हाँ	हाँ
16	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, संस्था की प्रत्येक नेटवर्क सीमाओं पर सीमा द्वारा गुजर रहे नेटवर्क को रिकार्ड करने के लिए मानीटरिंग प्रणाली को आकार देती है।	हाँ	हाँ	हाँ
17	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था वायरलेस नेटवर्क से जुड़े अप्राधिकृत वायरलेस प्रवेश बिन्दुओं पर, पता लगाने और चेतावनी के लिए नेटवर्क भेद्यता-स्कैनिंग को आकार देती है।	हाँ	हाँ	ऐच्छिक
18	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था केवल प्राधिकृत वायरलेस नेटवर्कों को प्रवेश की अनुमति देने और अन्य वायरलेस नेटवर्कों को बाधित करने के लिए उन ग्राहक मशीनों जो आवश्यक वायरलेस व्यापार उद्देश्य रखते हैं, पर वायरलेस प्रवेश को आकार देती है।	हाँ	हाँ	हाँ
19	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था व्यक्तिगत या अविश्वसनीय उपकरणों के लिए एक पृथक वायरलेस नेटवर्क का सृजन करती है। इस नेटवर्क से उपक्रम प्रवेश को अविश्वसनीय माना जाना चाहिए और तदनुसार फिल्टर और संपरीक्षित किया जाना चाहिए।	हाँ	हाँ	हाँ
20	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, विशिष्ट पैठ परीक्षणों और उत्पादन में उन तत्वों, जिनकी आमतौर पर परीक्षा नहीं की जाती, के विरुद्ध रेड टीम आक्रमण, जैसे पर्यवेक्षी नियंत्रण और डेटा अधिग्रहण और अन्य नियंत्रण प्रणालियों के विरुद्ध आक्रमण, परीक्षा मंच, जो एक उत्पादन वातावरण का अनुकरण करता है, का सृजन करती है।	हाँ	ऐच्छिक	ऐच्छिक
21	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था अंतर्वस्तु का विश्लेषण करने से पूर्व प्रतिनिधि सीमा पर सभी एन्क्रिप्ट किये गये नेटवर्क टैफिक को डिक्लिप करती है। तथापि, संस्था उन अनुमत साइटों, जिन तक बिना टैफिक को डिक्लिप किये प्राक्सी के माध्यम से पहुँचा जा सकता है, की श्वेत पत्रियों का इस्तेमाल कर सकती है।	हाँ	हाँ	ऐच्छिक
22	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था कार्यस्थल सदस्यों के सुरक्षा व्यवहार को सकारात्मक रूप से प्रभावित करने के लिए पहचाने गये कौशल-अन्तर की पूर्ति के लिए प्रशिक्षण देती है।	हाँ	हाँ	हाँ
23	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था ज्ञात दुर्भावनापूर्ण अप्रयुक्त इंटरनेट आईपी पत्तों के साथ संचार से इन्कार करती है और संस्था की प्रत्येक नेटवर्क सीमाओं पर केवल विश्वसनीय और आवश्यक आईपी पता श्रेणियों के लिए पहुँच सीमित करती है।	हाँ	हाँ	हाँ
24	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था सुरक्षा जानकारी और आकस्मिकता प्रबंधन (एसआईईएम) तैनात करती है या लॉग सहसंबंध और विश्लेषण के लिए लॉग विश्लेषणात्मक औजार तैनात करती है।	हाँ	हाँ	सीमित
25	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, आक्रमक की पार्श्विक रूप से सक्रिय होने की योग्यता को सीमित करने के लिए सभी कार्यस्थल से कार्यस्थल-संचार को निष्क्रिय करती है और पडोसी प्रणालियों के साथ निजी वीएलएन या माइक्रो सेगमेंटेशन के माध्यम से सुलभ करती है।	हाँ	हाँ	हाँ
26	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था किसी व्यापार प्रक्रिया या व्यापार स्वामी के साथ संबद्ध नहीं किये जा सकने वाले किसी खाते को निष्क्रिय करती है।	हाँ	हाँ	हाँ
27	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था उपकरणों पर उस वायरलेस प्रवेश को निष्क्रिय करती है जिनका वायरलेस प्रवेश के लिए व्यापार उद्देश्य नहीं रहता है।	हाँ	हाँ	हाँ
28	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, जब किसी व्यापार उद्देश्य के लिए ऐसे प्रवेश की आवश्यकता नहीं रहती, उपकरणों के वायरलेस परिधीय प्रवेश (जैसे ब्ल्यूटूथ और एनएफसी) को निष्क्रिय करती है।	हाँ	हाँ	हाँ

29	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, सूचना तक पहुँचने के लिए उस उपकरण का इस्तेमाल करके जिसको ऐसे द्वितीयक प्रमाणीकरण तंत्र की आवश्यकता होती है, जो परि-चालन प्रणाली से समन्वित नहीं है का इस्तेमाल कर संवेदनशील जानकारी को विश्राम अवस्था में एन्क्रिप्ट करती है।	हाँ	हाँ	हाँ
30	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, पारगमन में सभी संवेदनशील जानकारी को एन्क्रिप्ट करती है।	हाँ	हाँ	ऐच्छिक
31	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था नेटवर्क आधारित यूआरएल फिल्टर लागू करती है जो संस्था द्वारा स्वीकृत नहीं किये गये वेबसाइट को जोड़ने की प्रणाली की योग्यता को सीमित करती है। यह फिल्टरिंग संस्था की प्रत्येक प्रणालियों के लिए लागू की जाएगी चाहे वे भीतिक रूप से संस्था की सुविधाओं पर हैं या नहीं हैं।	हाँ	हाँ	हाँ
32	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था यह सुनिश्चित करती है कि नेटवर्क इंजीनियर सभी प्रशासनिक कार्यों या उन्नत पहुँच की जरूरतों वाले कार्यों के लिए एक समर्पित मशीन का इस्तेमाल करते हैं। यह मशीन संस्था के प्राथमिक नेटवर्क से खंडित की जाएगी और आन्तरिक प्रवेश के लिए अनुमति नहीं दी जाएगी। इस मशीन का इस्तेमाल ई-मेल, समिश्च दस्तावेज पढ़ने या इंटरनेट सर्फिंग के लिए नहीं किया जाएगा।	हाँ	हाँ	हाँ
33	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था सुनिश्चित करती है कि सभी खाते एक समाप्ति तिथि रखते हैं जिसकी निगरानी की जाती है और लागू किये जाते हैं।	हाँ	हाँ	हाँ
34	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था सुनिश्चित करती है कि सभी सॉफ्टवेयर विकास कार्मिकों को अपने विशिष्ट विकास परिवेश और उत्तरदायित्वों के लिए सुरक्षित कोड लिखने का प्रशिक्षण प्राप्त होता है।	हाँ	हाँ	हाँ
35	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था सुनिश्चित करती है कि विश्लेषण और समीक्षा हेतु एक केंद्रीय लॉग प्रबंधन को उपयुक्त लॉगों से समुच्चयित किया जा रहा है।	हाँ	हाँ	सहभाजित
36	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था सुनिश्चित करती है कि केवल प्राधिकृत पटकथा भाषाएँ ही सभी वेब ब्राउजरों और ई-मेल ग्राहकों में चल सकती हैं।	हाँ	हाँ	हाँ
37	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था सुनिश्चित करती है कि केवल पूरी तरह से समर्थित वेबवाइजर और ई-मेल ग्राहकों को ही संघठन में निष्पादित करने आदर्श रूप में केवल विक्रेता द्वारा उपलब्ध कराये गये नवीनतम संस्करण का इस्तेमाल करने की अनुमति दी जाती है।	हाँ	हाँ	हाँ
38	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था सुनिश्चित करती है कि संस्था का सुरक्षा जागरूकता कार्यक्रम, प्रौद्योगिकियों, खतरों, मानक और व्यापार आवश्यकताओं को संपादित करने के लिए निरंतर (वर्ष में कम से एक बार) अद्यतन किया जाता है।	हाँ	हाँ	वार्षिक
39	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, आपके सुरक्षा समूह से संपर्क करने के लिए बाह्य इकाइयों हेतु एक साधन उपलब्ध कराने के साथ-साथ, सॉफ्टवेयर भेद्यताओं की रिपोर्ट स्वीकार और संबोधित करने के लिए एक प्रोसेस स्थापित करती है।	हाँ	हाँ	हाँ
40	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था पैठ परीक्षण के लिए प्रोग्राम स्थापित करती है, जिसमें मिश्रित आक्रमण की पूरी संभावना, होती है, जैसे वायरलेस, ग्राहक आधारित और वेब अनुप्रयोग आक्रमण शामिल हैं।	हाँ	हाँ	सीमित

41	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, प्रोग्रामिंग भाषा और उपयोग में लाये जा रहे विकास परिवेश के लिए उपयुक्त सुरक्षित कोडिंग प्रथाओं की स्थापना करती है।	हाँ	हाँ	हाँ
42	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था डेटाबेस पर निर्भर होने वाले अनुप्रयोगों के लिए सख्त मानक विन्यास टेम्पलेटों का प्रयोग करती है। महत्वपूर्ण व्यापार प्रक्रियाओं का अंग होने वाली सभी प्रणालियों का भी परीक्षण किया जाना चाहिए।	हाँ	हाँ	हाँ
43	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था आन्तरिक रूप से विकसित सॉफ्टवेयर के लिए सुनिश्चित करती है कि स्पष्ट ब्रुटि-जॉब की जाती है और उसके आकार, डेटा-प्रकार और स्वीकार्य रेंजों तथा प्रारूपों सहित सभी इनपुट के लिए प्रलेखित किया जाता है।	हाँ	हाँ	हाँ
44	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, यूएसबी भंडारण उपकरण की जरूरत होने पर यह सुनिश्चित करती है कि ऐसे उपकरणों पर संग्रहित सभी डेटा को, विश्राम के समय, कूट रूप दिया जाता है।	हाँ	हाँ	संवेदनशील डेटा
45	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, नेटवर्क, अरेखों, विन्यास फाइलों, पुराने पैठपरीक्षण रिपोर्टों, ई-मेलों या पासवर्डयुक्त या प्रणाली परिचालन के लिए महत्वपूर्ण जानकारी वाले अय दस्तावेजों सहित असुरक्षित प्रणाली संबंधी जानकारी और आर्टिफैक्ट की उपस्थिति के लिए जो आक्रामकों के लिए उपयोगी होंगे, परीक्षण शामिल करती है।	हाँ	हाँ	हाँ
46	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था पारगमन में वायरलेस डेटा को कूटरूप देने के लिए उच्च एन्क्रिप्शन मानक (एईएस) का लाभ उठाती है।	हाँ	हाँ	हाँ
47	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, संभावित दुर्भावनापूर्ण गतिविधि की पहचान करने के लिए संस्था की प्रणालियों में प्रत्येक से सभी यूआरएल अनुरोधों, चाहे कार्यस्थल या मोबाइल उपकरण पर, को लॉग करती है और संभावित समझौता प्रणालियों की पहचान कर घटना संचालकों की सहायत करती है।	हाँ	हाँ	सीमित
48	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, कार्यस्थल पर या दूरस्थ सेवाप्रदाता पर, स्थित सहित, संस्था की प्रौद्योगिकी प्रणाली द्वारा संग्रहित, संसाधित या संचारित सभी संवेदनशील जानकारी की कोई सूची रखती है।	हाँ	हाँ	हाँ
49	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था वायरर द्वारा नेटवर्क से जुड़े प्राधिकृत वायरलेस प्रवेश बिन्दुओं की कोई सूची रखती है।	हाँ	हाँ	हाँ
50	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, कार्यस्थल पर या किसी दूरस्थ सेवा प्रदाता पर स्थित सहित संस्था के प्रत्येक प्रमाणीकरण प्रणालियों की एक सूची रखती है।	हाँ	हाँ	हाँ
51	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, उत्पादन और गैर-उत्पादन प्रणालियों के लिये पृथक परिवेश रखती है। डेवेलोपर्स के लिए उत्पादन परिवेशों के गैर-निगरानी वाले प्रवेश नहीं होने चाहिए।	हाँ	हाँ	हाँ
52	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था बहु-कारक प्रमाणीकरण और एन्क्रिप्टीकृत सत्रों का इस्तेमाल करते हुए सभी नेटवर्क उपकरणों का प्रबंधन करती है।	हाँ	हाँ	सीमित
53	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, पृथक बीएलएएन या अधिमानतः नेटवर्क उपकरणों के लिए प्रबंधन सत्रों हेतु पूर्ण रूप से भिन्न भौतिक संयोजकता पर आश्रित होते हुए, जो उस नेटवर्क के व्यापार इस्तेमाल से पृथक हैं, नेटवर्क संयोजन के आर-पार नेटवर्क आधारभूत संरचना का प्रबंध करती है।	हाँ	हाँ	पृथक वीएलएएन

54	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, आडिट लॉगिंग के माध्यम से निष्क्रिय खातों तक पहुँचने के प्रयासों की निगरानी करती है।	हाँ	हाँ	हाँ
55	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, विषमताओं या असामान्य घटनाओं की पहचान करने के लिए लॉगों की नियमित रूप से समीक्षा करती है।	हाँ	हाँ	हाँ
56	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, कार्यवाही करने योग्य घटनाओं की पहचान को बेहतर करने और घटना के शोर को कम करने के लिए नियमित रूप से एसआईईएम प्रणाली को सुधारती है।	हाँ	हाँ	ऐच्छिक
57	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, संस्था द्वारा विकसित सॉफ्टवेयर के लिए केवल अद्यतन और भरोसेमंद तृतीय-पक्षीय पुरजों का इस्तेमाल करती है।	हाँ	हाँ	हाँ
58	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, इस जानकारी का इस्तेमाल करते हुए आधारभूत शिक्षा रोड मैप का निर्माण करने, कार्यदल-सदस्यों द्वारा पालन नहीं किये जा रहे कौशल और आचरण को समझने के लिए कौशल के अन्तर का कोई विश्लेषण करती है।	हाँ	हाँ	दो वर्ष में एक बार
59	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, आक्रमण की पहचान करने और उसको रोकने या तुरंत और प्रभावशाली ढंग से प्रतिक्रिया करने के लिए संस्थागत तैयारी की परीक्षा करने के लिए सावधिक रेड टीम एक्सरसाइज करती है।	हाँ	हाँ	ऐच्छिक
60	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था सर्वर की ओर जा रहे ट्रैफिक की जाँच और पृष्ठीकरण के लिए किन्हीं महत्वपूर्ण सर्वरों के समक्ष अनुप्रयोग फायरवाल्स स्थापित करती है। किसी भी अप्राधिकृत ट्रैफिक को बाधित और लॉग किया जाना चाहिए।	हाँ	हाँ	सीमित
61	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, वास्तविक दुनियावी खतरे के प्रति जागरूकता और सहजता बनाये रखने घटना की प्रतिक्रिया में शामिल कार्यदल के लिए नियमित घटना, प्रतिक्रिया, अभ्यास और परिदृश्य की योजना और संचालन करती है। अभ्यासों को औजारों और उनके पास उपलब्ध डेटा का इस्तेमाल करके संचार चैनलों, निर्णय करने और घटना की प्रतिक्रिया करने वालों की तकनीकी क्षमताओं की जाँच करना चाहिए।	हाँ	हाँ	वार्षिक
62	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, सामान्य वेब अनुप्रयोग आक्रमणों के लिए वेब अनुप्रयोग की ओर जा रहे सभी ट्रैफिक का निरीक्षण करने वाले वेब अनुप्रयोग फायरवाल्स डब्ल्यूएफ को तेनाती द्वारा वेब अनुप्रयोगों की सुरक्षा करती है। जो अनुप्रयोग वेब आधारित नहीं है, के लिए विशिष्ट अनुप्रयोग फायरवाल्स तेनात किये जाने चाहिए यदि ऐसे औजार उस किस्म के अनुप्रयोग के लिए उपलब्ध हैं। यदि ट्रैफिक एंक्रिप्ट किये गये हैं तो उपकरण या तो एन्क्रिप्टन के पीछे बैठा होना चाहिए या विश्लेषण से पूर्व ट्रैफिक को डिक्लिप करने में सक्षम होना चाहिए। यदि कोई विकल्प उपयुक्त नहीं है, एक हास्ट-आधारित अनुप्रयोग फायरवेल की तेनाती की जानी चाहिए।	हाँ	हाँ	सीमित
63	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, संस्था द्वारा नियमित रूप से अभिगमित नहीं किये जाने वाले संवेदनशील डेटा या प्रणाली को नेटवर्क से हटा देती है। इन प्रणालियों का व्यापार इकाई द्वारा प्रणाली की यथाकदा की आवश्यकता के लिए केवल स्टैण्डएलोन प्रणालियों (नेटवर्क से अलग किये गये) के रूप में किया जाना चाहिए या पूरी तरह से आभासी बना दिया जाना चाहिए और जरूरत पडने तक बंद रखा जाना चाहिए।	हाँ	हाँ	हाँ
64	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था को पारगमन में डेटा को एंक्रिप्ट करने और बहु-कारक प्रमाणीकरण (एमएफए) के उपयोग के लिए संस्था के नेटवर्क के सभी दूरस्थ लॉगिन एक्सेस की आवश्यकता होती है?	हाँ	हाँ	एमएफए
65	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था को, सभी प्रणालियों, चाहे साइट पर प्रबंधित या तृतीय पक्ष-प्रदाता पर, सभी-उपयोगकर्ता खातों के लिए बहु-कारक प्रमाणीकरण की आवश्यकता होती है।	हाँ	हाँ	हाँ

66	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था नेटवर्क को लेबल या सर्वरों पर संग्रहित जानकारी के वर्गीकरण स्तर पर खंडित करती है, पुथक किये गये आभासी स्थानीय क्षेत्र नेटवर्क (वीएलएएन) पर सभी संवेदनशील जानकारी का पता लगाती है?	हाँ	हाँ	हाँ
67	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था सुनिश्चित करने के लिए यह स्वीकार करती है कि यूआरएल वर्गीकरण सेवाएँ हाल ही की उपलब्ध वेबसाइट श्रेणी परिभाषाओं के साथ अद्यतन है, गैरश्रेणीकृत साइट अपने आप ब्लाक किये जाएँगे?	हाँ	हाँ	ऐच्छिक
68	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था मान्य ज्ञान क्षेत्रों से जाली या रूपांतरित ई-मेलों के अवसर को कम करने के लिए ज्ञान-क्षेत्र-आधारित संदेश प्रमाणीकरण प्रेषक-पालिसी फ्रेमवर्क (एसपीएफ) और ज्ञान क्षेत्र कीज़ आइडेंटि फाइंड मेल (डीकेआईएम) मानकों को लागू करने से शुरू करके, रिपोर्टिंग और अनुरूपता (डीएमआरसी) नीति और सत्यापन लागू करती है?	हाँ	हाँ	हाँ
69	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था फिशिंग, फोन घोटाले और छद्मरूपण कॉलों, जैसे सामाजिक अभियांत्रिकी आक्रमणों के भिन्न रूपों की पहचान करने का प्रशिक्षण, कार्यदल को देती है?	हाँ	हाँ	हाँ
70	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था सुरक्षित प्रामाणीकरण को सक्रिय और प्रयुक्त करने के महत्व के संबंध में कार्यदल के सदस्यों को प्रशिक्षित करती है?	हाँ	हाँ	हाँ
71	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, कार्यदल के सदस्यों को, अपने मोबाइल उपकरणों के खोने, मेल में स्वतः पूर्ण होने के कारण गलत व्यक्ति को ई-मेल भेजने जैसे, अनैच्छिक डेटा खुलासों के कारणों से जागरूक करने के लिए प्रशिक्षण देती है।	हाँ	हाँ	हाँ
72	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, कार्यदल को, पुरालेख की पहचान करने और उचित रूप से स्टोर करने, स्थानान्तरित करने और संवेदनशील जानकारी को नष्ट करने प्रशिक्षित करती है।	हाँ	हाँ	हाँ
73	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, किसी अप्राधिकृत ब्राउजर या ई-मेल ग्राहक प्लगइन या एडऑन अनुप्रयोगों की स्थापना रद्द या निष्क्रिय करती है।	हाँ	हाँ	हाँ
74	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था नेटवर्क से जुड़े अप्राधिकृत वायरलेस प्रवेश बिन्दुओं का पता लगाने या उस पर चेतावनी देने के लिए वायरलेस अतिक्रमण पहचान प्रणाली (डब्ल्यू आईडीएस) का इस्तेमाल करती है।	हाँ	हाँ	सीमित
75	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था जब डेटा प्रणाली से कापी कर लिया गया है तब भी डेटा के प्रवेश नियंत्रण को लागू करने, मेजबान आधारित डेटा हानि रोकथाम जैसे स्वचालित औजार का इस्तेमाल करती है।	हाँ	सीमित	ऐच्छिक
76	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, ज्ञात दुर्भावनापूर्ण क्षेत्रों की पहुँच को बाधित करने में मदद के लिए डीएनएस फिल्टरिंग सेवाओं का इस्तेमाल करती है।	हाँ	हाँ	हाँ
77	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था केवल मानकीकृत और व्यापक रूप से समीक्षित एन्क्रिप्ट किये गये एलोरिडम का इस्तेमाल करती है।	हाँ	हाँ	हाँ
78	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, दुर्भावनापूर्ण व्यवहार वाले आवक ई-मेल संलग्नकों का विश्लेषण करने और उन्हें बाधित करने के लिए सेण्डबाक्सिंग का इस्तेमाल करती है।	हाँ	हाँ	ऐच्छिक
79	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था कंसर्ट में भेद्यता स्कैनिंग और पैठ परीक्षण औजारों का इस्तेमाल करती है। भेद्यता स्कैनिंग आकलनों के परिणामों का इस्तेमाल मार्गदर्शन और पैठ परीक्षण प्रयासों पर ध्यान केंद्रित करने के लिए आरंभिक बिन्दु की तरह किया जाना चाहिए।	हाँ	हाँ	हाँ
80	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, कार्य स्थल पर स्थित या दूरस्थ सेवा प्रदाता के पास स्थित सहित, संस्था की प्रौद्योगिक प्रणालियों द्वारा संग्रहित, संसाधित या संचारित सभी संवेदनशील जानकारी की पहचान करने के लिए किसी सक्रिय खोजी उपकरण का इस्तेमाल करती है और संस्था की संवेदनशील जानकारी सूची को अद्यतन करती है।	हाँ	ऐच्छिक	ऐच्छिक

81	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था सभी मोबाइल उपकरणों के हार्ड ड्राइव को एन्क्रिप्ट करने के लिए स्वीकृत संपूर्ण डिस्क एन्क्रिप्टन सॉफ्टवेयर का इस्तेमाल करती है?	हाँ	ऐच्छिक	ऐच्छिक
82	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था आपकी संस्था के बाहर से हासिल किये गये सभी सॉफ्टवेयर का संस्करण अभी भी विकासकर्ता द्वारा समर्थित है या विकासकर्ता की सुरक्षा अनुशंसाओं के आधार पर उपयुक्त रूप से सख्त बनाया गया है?	हाँ	हाँ	हाँ
83	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था, जहाँ भी संभव है सुनिश्चित करती है कि रेड टीम परिणाम का अनावृत्त मशीन-पठनीय मानकों (उदाहरण - एससीएपी) का इस्तेमाल करके दस्तावेजीकरण किया जाता है। रेड टीम अभ्यासों के परिणामों का निर्धारण करने के लिए गणना करने की विधि तैयार करें, ताकि परिणामों की समय-समय पर तुलना की जा सकती है?	हाँ	हाँ	ऐच्छिक
84	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था ने सुरक्षा से संबंधित घटना की केन्द्रीकृत और समन्वयित निगरानी और प्रबंधन के लिए एक सुरक्षा परिचालन केंद्र का क्रियान्वयन करने कोई क्रियाविधि परिभाषित और निर्धारित की है?	हाँ	हाँ	सहभाजित
85	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था ने, घटनाओं, पता लगाने के तरीकों, कर्मचारियों, विक्रेताओं और ग्राहकों द्वारा रिपोर्ट करने के तरीकों और निगरानी की सावधिकाता, खतरे की जानकारी एकत्र करने/साझा करने, ऐसे परिदृश्य/ घटना प्रकार में अपेक्षित प्रतिक्रिया, ऐसी घटनाओं की देखभाल करने/ संभालने वाले कर्मिकों के उत्तरदायित्वों, ऐसे कर्मिकों को विशिष्ट प्रशिक्षण उपलब्ध कराने, घटना के बाद समीक्षा, सावधिक रूप से घटनाओं की प्रतिक्रिया योजनाओं की परीक्षा को परिभाषित किया है?	हाँ	हाँ	हाँ
86	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था ने एमएस ऑफिस दस्तावेजों में/वीबीए/मैक्रो के इस्तेमाल के नियंत्रण, ई-मेल प्रणाली/नियंत्रण अनुमेय संलग्नक प्रकारों के लिए, उपाय लागू किये हैं?	हाँ	हाँ	हाँ
87	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था ने, संस्था के नेटवर्क से अप्राधिकृत उपकरण संपर्कों की स्वतः पहचान करने और ऐसे संपर्कों को बाधित करने के लिए क्रियाविधि लागू की है?	हाँ	हाँ	हाँ
88	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था सभी महत्वपूर्ण अनुप्रयोगों, सर्वर, नेटवर्क उपकरणों और डेटाबेसों के लिए सावधिक परीक्षण आयोजित करती है?	हाँ	हाँ	वार्षिक
89	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था विक्रेताओं को भेद्यता की सूचना देने की कोई प्रक्रिया लागू करती है?	हाँ	हाँ	हाँ
90	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था वीएपीटी के समापन और सुधारात्मक कार्यवाई के लिए ट्रैकर बनाए रखती है?	हाँ	हाँ	हाँ
91	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या उच्च उपलब्धता सुनिश्चित करने और समय पर आक्रमणों का पता लगाने को परिभाषित और उसको लागू करने की कोई नीति है?	हाँ	हाँ	हाँ
92	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या भेद्यता आकलन और पैठ परीक्षण प्रक्रिया और कैलेंडर परिभाषित किये गये हैं?	हाँ	हाँ	हाँ
93	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या, इंटरनेट समक्ष अनुप्रयोगों या आधारित संरचना घटकों का वीएपीटी सावधिक रूप से किया जाता है।	हाँ	हाँ	वार्षिक
94	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या एपीआई या वेब सेवाओं इत्यादि सहित व्यापारिक अनुप्रयोगों की सुरक्षित कूट समीक्षा सहित सावधिक रूप से और चलाने से पूर्व, वीएपीटी परीक्षण की जाती है।	हाँ	हाँ	हाँ
95	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या इंटरनेट-समक्ष सूचना परिसंपत्तियों या प्रणालियों के सभी बदलावों के लिए आयोजित अनिवार्य सुरक्षा परीक्षण और सूचित अन्तराल, उत्पादन शुरू करने से पूर्व बद कर दिये जाते हैं।	हाँ	हाँ	प्रमुख बदलाव
96	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या सभी इंटरनेट समक्ष सूचना परिसंपत्तियों पर प्रणालियों के लिए आयोजित बाह्य ब्लैक बॉक्स पैठ परीक्षण (पीटी) छह महीने में एक बार किये जाते हैं।	हाँ	हाँ	वार्षिक

97	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या वीएपीटी से रिपोर्ट किये गये उच्च जोखिम अन्तरालों को, वैधीकरण परीक्षण द्वारा, दिशा-निर्देशों के अन्तर्गत नियत समयावधि के भीतर बंद कर दिया जाता है।	हाँ	हाँ	हाँ
98	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या वीएपीटी में रिपोर्ट किये गये अकेक्षण अन्तरालों को दिशानिर्देशों में दी गयी समयावधि में बंद कर दिया जाता है?	हाँ	हाँ	हाँ
99	सुरक्षा निरंतर निगरानी और पता लगाना (डीई.सीएम):	क्या संस्था की सूचना परिसंपत्तियों का किसी एकल काल स्रोत से मिलान किया जाता है?	हाँ	हाँ	हाँ
100	पता लगाने की प्रक्रियाएँ (डीई.डीपी):	सुरागसानी के लिये भूमिकाएँ और उत्तरदायित्व, जवाबदेही सुनिश्चित अच्छी तरह से परिभाषित है?	हाँ	हाँ	हाँ
101	पता लगाने की प्रक्रियाएँ (डीई.डीपी):	क्या सुरागसानी गतिविधियाँ, सभी लागू अनुप्रयोग आवश्यकताओं का अनुपालन करती हैं?	हाँ	हाँ	हाँ
102	पता लगाने की प्रक्रियाएँ (डीई.डीपी):	क्या संस्था ने लैपटॉपों, मोबाइल फोनों, टैबलेटों इत्यादि जैसे प्राधिकृत हार्डवेयर/गतिशील उपकरणों की पहचान करने की प्रक्रिया/तंत्र की व्यवस्था की है और सुनिश्चित किया है कि उन्हें संस्था द्वारा निर्धारित सुरक्षा आवश्यकताओं को पूरा करने पर ही संयोजकता उपलब्ध करायी जाती है?	हाँ	हाँ	हाँ
103	परिसंपत्ति प्रबंधन(आईडी.एम)	क्या संस्था, संस्था के विश्वसनीय नेटवर्क के साथ हार्डवेयर परिसंपत्ति संयोजकता के प्रामाणीकरण के लिए ग्राहक प्रमाण-पत्रों/ सर्वर का इस्तेमाल करती है?	हाँ	हाँ	हाँ
104	परिसंपत्ति प्रबंधन(आईडी.एम)	क्या संस्था, यह नियंत्रण करने के लिए कि नेटवर्क को कौन-से उपकरण प्रमाणित कर सकते हैं, 802.1x मानकों का अनुपालन करते हुए पोर्ट स्तर प्रवेश का इस्तेमाल करती है? यह सुनिश्चित करने के लिए की केवल प्राधिकृत उपकरण नेटवर्क से जुड़ सकते हैं, प्रामाणीकरण प्रणाली को हार्डवेयर परिसंपत्ति सूची डेटा में सम्बद्ध किया जाएगा?	हाँ	हाँ	सीमित
105	परिसंपत्ति प्रबंधन(आईडी.एम)	क्या संस्था महत्वपूर्ण परिसंपत्तियों की, उनकी संवेदनशीलता के आधार पर, पहचान करती है?	हाँ	हाँ	हाँ
106	परिसंपत्ति प्रबंधन(आईडी.एम)	क्या संस्था अपने हार्डवेयर, सॉफ्टवेयर, सूचना परिसंपत्तियों, नेटवर्क संसाधनों के विवरण की कोई अद्यतन सूची रखती है और उन कार्मिकों का भी रिकार्ड रखती है जिन्हें ऐसी परिसंपत्तियाँ जारी की जाती हैं?	हाँ	हाँ	हाँ
107	परिसंपत्ति प्रबंधन(आईडी.एम)	क्या संस्था ने प्राधिकृत सॉफ्टवेयर/अनुप्रयोगों/पुस्तकालयों इत्यादि की अद्यतन केंद्रीकृत सूची रखी है?	हाँ	हाँ	हाँ
108	परिसंपत्ति प्रबंधन(आईडी.एम)	क्या संस्था ने, यह ध्यान में रखते हुए कि संस्था के नेटवर्क के भीतर/बाहर डेटा/जानकारी संग्रहित, संचारित, प्रसंस्कृत, अभिगमित और इस्तेमाल में लायी जाती है और डेटा/सूचना की संवेदनशीलता के आधार पर डेटा/सूचना परिसंपत्ति का प्रबंधन और सुरक्षा की है?	हाँ	हाँ	हाँ
109	परिसंपत्ति प्रबंधन(आईडी.एम)	क्या संस्था ने, महत्वपूर्ण परिसंपत्तियों के स्थान को सुरक्षित रखने के लिए, प्राकृतिक खतरों से सुरक्षा प्रदान करते हुए उचित पर्यावरणीय नियंत्रणों की व्यवस्था की है?	हाँ	हाँ	हाँ
110	परिसंपत्ति प्रबंधन(आईडी.एम)	क्या संस्था ने, किसी सशक्त समझौतों या पर्यावरणीय नियंत्रणों के उल्लंघन पर निगरानी के लिए कार्य प्रणाली की व्यवस्था की है?	हाँ	हाँ	हाँ
111	परिसंपत्ति प्रबंधन(आईडी.एम)	क्या यह सुनिश्चित किया गया है कि अप्राधिकृत संपत्तियों को या तो नेटवर्क से हटा दिया गया या अलग कर दिया गया या वस्तुसूची को समय-समय पर अद्यतन किया गया है?	हाँ	हाँ	हाँ



112	व्यापार परिवेश(आईडी.बीई)	क्या संस्थागत मिशन, लक्ष्यों और गतिविधियों, डब्ल्यू.आर.टी. साइबर सुरक्षा भूमिकाओं, उत्तरदायित्वों और जोखिम प्रबंधन निर्णयों के लिए प्राथमिकताओं को स्थापित और सूचित किया गया है?	हाँ	हाँ	हाँ
113	व्यापार परिवेश(आईडी.बीई)	क्या महत्वपूर्ण सेवाओं की सहायता सुपदंगी की तन्त्रकता आवश्यकताओं को सभी परिचालन राज्यों (उदा.बहाली के दौरान अवरोध/आक्रमण के अंतर्गत)?के लिएस्थापित किया गया है?	हाँ	हाँ	हाँ
114	व्यापार परिवेश(आईडी.बीई)	क्या संस्था ने, संस्था के नेटवर्क परिवेश को जोड़ने वाले उपकरणों सहित सभी प्रमुख सूचना प्रौद्योगिकी के लिए मानक परिचालन क्रियाविधि(एसओपी)/स्थापित की है?	हाँ	हाँ	हाँ
115	व्यापार परिवेश(आईडी.बीई)	क्या संस्था ने, संस्था स्तर पर, तार से जुड़े /वायरलेस नेटवर्कों सहित अद्यतन नेटवर्क वास्तुशास्त्रीय आरेख रखना है?	हाँ	हाँ	हाँ
116	शासन-विधि (आईडी.जीवी)	क्या सूचना सुरक्षा के शासन और निगरानी के लिए संपूर्ण उत्तरदायित्व संभालने के लिए अधिकारी पदनामित है?	नामित सीआईएसओ	नामित / आभासी सीआईएसओ	नामित / आभासी सीआईएसओ
117	शासन-विधि (आईडी.जीवी)	हर समय नीति अद्यतन रहे यह सुनिश्चित करने के लिए क्या संस्था ने एक आईएसआरएमसी गठित करती है?	आईएस आरएमसी	आईटी, विधिक, मासं,जोखिम, व्यापार परिचा	आईटी, विधिक,मासं, व्यापार परिचालन
118	शासन-विधि (आईडी.जीवी)	क्या संस्था के बोर्ड की लेखा परीक्षा समिति को वार्षिक लेखा परीक्षा योजना और रिपोर्ट प्रस्तुत की गयी है?	हाँ	हाँ	प्रबंध निदेशक
119	शासन-विधि (आईडी.जीवी)	क्या साइबर सुरक्षा पालिसी में, घटना प्रबंधन एवं अन्य उपयुक्त पुनर्प्राप्ति तंत्रों के माध्यम से घटनाओं से उबरने की प्रक्रिया शामिल है?	हाँ	हाँ	हाँ
120	शासन-विधि (आईडी.जीवी)	क्या साइबर सुरक्षा नीति में, उपयुक्त निगरानी औजारों/प्रक्रिया के जरिए घटनाओं की विषमताएँ और आक्रमण का पता लगाना शामिल है?	हाँ	हाँ	हाँ
121	शासन-विधि (आईडी.जीवी)	क्या साइबर सुरक्षा नीति में, उपयुक्त नियंत्रणों, औजारों एवं उपायों द्वारा परिसंपत्तियों की सुरक्षा के संबंध में प्रक्रिया शामिल है?	हाँ	हाँ	हाँ
122	शासन-विधि (आईडी.जीवी)	क्या साइबर सुरक्षा नीति में, घटनाओं, विषमताओं या आक्रमण की पहचान के बाद प्रतिक्रिया संबंधी प्रक्रिया शामिल है?	हाँ		हाँ
123	शासन-विधि (आईडी.जीवी)	क्या संस्था अन्तर्राष्ट्रीय मानकों जैसे आईएसओ 27001, सीओबीआईटी 5.इत्यादि से सर्वोत्तम प्रथाओं का पालन कर एपीआई के माध्यम से कोई परिचालन/प्रक्रिया/मौद्रिक लेन-देन लागू करती है?	हाँ	हाँ	हाँ
124	शासन-विधि (आईडी.जीवी)	क्या साइबर सुरक्षा भूमिकाओं और उत्तरदायित्वों का आंतरिक भूमिकाओं और बाहरी भागीदारों के साथ समन्वयन और तालमेल किया जाता है?	हाँ	हाँ	हाँ
125	शासन-विधि (आईडी.जीवी)	क्या कोई साइबर संकट प्रबंधन योजना (सीसीएमपी) उपलब्ध है? क्या साइबर संकट प्रबंधन योजना की तैयारी के लिए सर्ट-इन/एनसीआईआईपीसी दिशा-निर्देशों का इस्तेमाल किया जाता है?	हाँ	हाँ	हाँ
126	शासन-विधि (आईडी.जीवी)	क्या वहाँ कोई एसओसी सेटअप उपलब्ध है जो निरंतर निगरानी सुनिश्चित करता है ?	हाँ	हाँ	सीमित/सहभाजित

127	शासन-विधि (आईडी.जीवी)	क्या पदनामित साइबर सुरक्षा अधिकारी के साथ असामान्य गतिविधियों की सूचना को सुविधाजनक बनाने के लिए रिपोर्ट करने की क्रियाविधियाँ अपनाई जा रही हैं?	हाँ	हाँ	हाँ
128	शासन-विधि (आईडी.जीवी)	क्या, कोई व्यापक साइबर सुरक्षा नीति की योजना काम कर रही है ?	हाँ	हाँ	हाँ
129	शासन-विधि (आईडी.जीवी)	क्या कोई साइबर जोखिम प्रबंधन नीति उपलब्ध है ?	हाँ	हाँ	हाँ
130	शासन-विधि (आईडी.जीवी)	क्या व्यापार निरंतरता योजना और आपदा बहाली योजना काम कर रही है?	हाँ	हाँ	मुख्य प्रणालियाँ
131	शासन-विधि (आईडी.जीवी)	क्या बोर्ड की सू.प्रौ. उपसमिति द्वारा सू.प्रौ. वास्तुकला की समीक्षा की गयी है?	हाँ	प्रबंध निदेशक	प्रबंध निदेशक
132	शासन-विधि (आईडी.जीवी)	क्या संस्था के बोर्ड ने विशेषज्ञों की कोई आन्तरिक प्रौद्योगिकी समिति गठित की है? क्या समिति साइबर सुरक्षा नीति के क्रियान्वयन की सावधिक रूप से समीक्षा करती है?	हाँ	प्रबंध निदेशक	प्रबंध निदेशक
133	शासन-विधि (आईडी.जीवी)	क्लाउड और मोबाइल तैनात करने के लिए संस्था ने, क्लाउड, मोबाइल सुरक्षा और संबंधित क्षेत्रों के लिए सर्वोत्तम प्रथाओं पर विचार किया है?	हाँ	हाँ	हाँ
134	शासन-विधि (आईडी.जीवी)	क्या वरिष्ठ प्रबंधन की प्रतिबद्धता सुनिश्चित की गयी है?	हाँ	हाँ	हाँ
135	जोखिम आकलन (आईडी.आरए)	क्या संस्था ने, संभावित साइबर जोखिमों, (खतरों और भेदताओं) ऐसे खतरों की संभावना सहित और व्यापार पर उनके प्रभाव की पहचान की है और गंभीरता को रोकने के लिए तदनुसार नियंत्रण तैनात किये हैं?	हाँ	हाँ	हाँ
136	जोखिम आकलन (आईडी.आरए)	क्या संस्था यह जानने के लिए कि सभी नेटवर्क उपकरणों को नेटवर्क सुरक्षा के वांछित स्तर तक उपयुक्त रूप से आकार दिया गया है सावधिक रूप से उनका आकलन करती है?	हाँ	हाँ	हाँ
137	जोखिम आकलन (आईडी.आरए)	क्या जोखिम प्रतिक्रियाओं की पहचान की गई और प्राथमिकता दी गयी है?	हाँ	हाँ	हाँ
138	जोखिम आकलन (आईडी.आरए)	आन्तरिक और बाहरी दोनों से पक्षों, से खतरों की पहचान की गयी और उनका दस्तावेजीकरण किया गया है?	हाँ	हाँ	हाँ
139	जोखिम प्रबंधन (आईडी.आरएम)	क्या जोखिम प्रबंधन प्रक्रियाएँ स्थापित, प्रबंधित और संस्थागत हितधारकों द्वारा सममत है?	हाँ	हाँ	हाँ
140	जोखिम प्रबंधन (आईडी.आरएम)	क्या संस्थागत जोखिम सहनशीलता अवधारित और स्पष्ट रूप से व्यक्त की गयी है?	हाँ	हाँ	हाँ

141	आपूर्ति श्रृंखला जोखिम प्रबंधन (आई.टी.एससी)	क्या विक्रेता साइबर सुरक्षा नीति में दिये गये लागू दिशा-निर्देशों का पालन करते हैं? क्या संस्था, नीति प्रावधानों का अनुपालन सुनिश्चित करने के लिए उनसे आवश्यक स्वतः प्रमाणन प्राप्त करती है?	हाँ	हाँ	हाँ
142	आपूर्ति श्रृंखला जोखिम प्रबंधन (आई.टी.एससी)	क्या विक्रेताओं ने उपयुक्त सूचना सुरक्षा नियंत्रण और साइबर सुरक्षा ढाँचे लागू किये हैं?	हाँ	हाँ	हाँ
143	आपूर्ति श्रृंखला जोखिम प्रबंधन (आई.टी.एससी)	विक्रेताओं के समझौता दस्तावेज रखे गये और अद्यतन हैं ?	हाँ	हाँ	हाँ
144	आपूर्ति श्रृंखला जोखिम प्रबंधन (आई.टी.एससी)	संरक्षित या संवेदनशील जानकारी तक तृतीय पक्ष पहुँच निगरानी के लिए कोई प्रक्रिया है?	हाँ	हाँ	हाँ
145	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पी.आर.एससी):	सीईआरटी-इन दिशाओं के अनुसार 180 दिनों की रोलिंग अवधि के लिए आईसीटी आधारभूत संरचना लॉग बनाये रखे जाते हैं?	हाँ	हाँ	हाँ
146	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पी.आर.एससी):	क्या आईसीटी आधारभूत संरचना लॉग, महत्वपूर्ण और व्यापार डेटा भारत में संग्रहित किये जाते हैं?	हाँ	हाँ	हाँ
147	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पी.आर.एससी):	क्या तृतीय-पक्ष कर्मचारियों, जिन्हें संस्था के महत्वपूर्ण प्रणालियों, नेटवर्कों और अन्य कम्प्यूटर संसाधनों तक पहुँच दी जाती है, पर कड़ी देख-रेख, निगरानी और प्रवेश नियंत्रण रखे जाते हैं?	हाँ	हाँ	हाँ
148	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पी.आर.एससी):	क्या संस्था की सभी महत्वपूर्ण प्रणालियों, जो इंटरनेट पर पहुँचे जा सकते हैं, पर दो घटक सुरक्षा (जैसे वीपीएन, फायरवाल नियंत्रण इत्यादि) होती है?	हाँ	हाँ	हाँ
149	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पी.आर.एससी):	क्या प्रणालियों, अनुप्रयोगों, नेटवर्कों और डेटाबेस तक प्रवेश के लिए प्रवेश नियंत्रण नीति सुदृढ पासवर्ड प्रबंधन नियंत्रण रखती है?	हाँ	हाँ	हाँ
150	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पी.आर.एससी):	क्या संस्था, उन उपयोगकर्ताओं के प्रवेश के विशेषाधिकारों को सक्रिय रूप से निष्क्रिय करती है जो संस्था छोड़कर जा रहे हैं या जिनके प्रवेश के विशेषाधिकार वापस ले लिये गये हैं?	हाँ	हाँ	हाँ
151	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पी.आर.एससी):	क्या संस्था ने संस्था की महत्वपूर्ण प्रणालियों तक उन्नत पहुँच पात्रताओं (जैसे विशेषाधिकार प्राप्त उपयोगकर्ता) वाले कर्मचारियों को सुरक्षा उपाय और नियंत्रण तैनात किये हैं? क्या संस्था ने विशेषाधिकार प्राप्त उपयोगकर्ताओं की संख्या को भी कम से कम तक सीमित रखा है और विशेषाधिकार प्राप्त उपयोगकर्ताओं की गतिविधियों के विरुद्ध सावधिक समीक्षा क्रियाविधि/प्रक्रिया तैनात की है? क्या ऐसे विशेषाधिकारप्राप्त उपयोगकर्ताओं की प्रणाली लॉगों की पहुँच को सीमित रखा गया है जहाँ उनकी गतिविधियों को हथिया जा रहा है?	हाँ	हाँ	हाँ
152	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पी.आर.एससी):	क्या संस्था ने सुनिश्चित किया है कि कंपनी के किसी कर्मिक को उनकी श्रेणी या पद की वजह से गोपनीय डेटा, अनुप्रयोगों, प्रणाली संसाधनों या सुविधाओं तक पहुँच के प्राकृतिक अधिकार प्राप्त नहीं हैं?	हाँ	हाँ	हाँ
153	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पी.आर.एससी):	क्या संस्था ने यह सुनिश्चित किया है कि महत्वपूर्ण उपकरणों के कक्ष/क्षेत्र की परिधि भौतिक रूप से सुरक्षित है और उनकी भौतिक, मानवीय और क्रियाविधिक नियंत्रणों, जैसे सुरक्षा गारदों, सीसीटीवी, कार्ड-प्रवेश प्रणालियों, मैन ट्रेप, बोलाडों इत्यादि द्वारा नियमित रूप से निगरानी की जाती है?	हाँ	हाँ	हाँ

154	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पीआर.एसी):	क्या संस्था ने संगठन के महत्वपूर्ण सू.प्रौ. संरचनात्म ढाँचे के भीतर इंटरनेट और इंटरनेट आधारित सेवाओं, जैसे सामाजिक मीडिया स्थलों, क्लाउड आधारित स्टोरेज स्थलों इत्यादि के इस्तेमाल की निगरानी करने और विनियमित करने के लिए कोई आंतरिक प्रवेश नीति तैयार की है?	हाँ	हाँ	हाँ
155	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पीआर.एसी):	क्या संस्था ने, उपयोग की आवश्यकता के आधार और न्यूनतम विशेषाधिकार के सिद्धांत पर सू.प्रौ. प्रणालियों, अनुप्रयोगों, डेटाबेस और नेटवर्कों तक पहुँच को लागू किया है? क्या प्रवेश सुदृढ़ प्रमाणीकरण कार्य प्रणाली का इस्तेमाल करते हुए और केवल आवश्यक होने पर ही मंजूर किया जाता है?	हाँ	हाँ	हाँ
156	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पीआर.एसी):	क्या संस्था ने ग्राहकों को, सुरक्षित प्रमाणीकरण प्रौद्योगिकी का इस्तेमाल करते हुए प्रणालियों की साझेदारी के प्रवेश के लिए पहचान और प्रमाणीकरण उपलब्ध करने के लिए नियंत्रण लागू किया है?	हाँ	हाँ	हाँ
157	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पीआर.एसी):	क्या संस्था ने अवैध लॉगइन गिनती को न्यूनतम करने, प्रस्तुत खातों को निष्क्रिय करने के लिए नियंत्रण लागू किये हैं?	हाँ	हाँ	हाँ
158	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पीआर.एसी):	क्या संस्था की महत्वपूर्ण प्रणालियों तक भौतिक प्रवेश को प्राधिकृत अधिकारियों की न्यूनतम संख्या तक सीमित किया गया है? क्या तृतीय पक्ष कर्मचारियों की कड़ाईपूर्वक निगरानी की जाती है और जब तृतीय पक्ष कर्मचारियों को महत्वपूर्ण प्रणालियों तक व्यक्तिगत रूप से प्रवेश दिया जाता है तब संस्था के प्राधिकृत कर्मचारी हर समय उनके साथ रहते हैं?	हाँ	हाँ	हाँ
159	पहचान प्रबंधन, प्रमाणीकरण और प्रवेश नियंत्रण (पीआर.एसी):	क्या संस्था की महत्वपूर्ण प्रणालियों तक व्यक्तिगत प्रवेश को जब आशयक नहीं रह जाता, तुरंत निरस्त कर दिया जाता है?	हाँ	हाँ	हाँ
160	जागरूकता एवं प्रशिक्षण (पीआर.एटी):	क्या इतिहास और प्रशिक्षणअन्तर्वस्तु के संस्करण को संभाल कर रखा जाता है?	हाँ	हाँ	हाँ
161	जागरूकता एवं प्रशिक्षण (पीआर.एटी):	क्या महत्वपूर्ण कार्मिकों के लिए लक्षित जागरूकता/प्रशिक्षण सावधिक रूप से आयोजित किया जाता है?	हाँ	वार्षिक	वार्षिक
162	जागरूकता एवं प्रशिक्षण (पीआर.एटी):	क्या प्रशिक्षण कार्यक्रम की समीक्षा की जाती है और सावधिक रूप से उसको अद्यतन किया जाता है?	हाँ	वार्षिक	वार्षिक
163	जागरूकता एवं प्रशिक्षण (पीआर.एटी):	क्या ग्राहक सूचना/डेटा सहित नेटवर्क परिसंपत्तियों के सुरक्षित और स्वीकार्य इस्तेमाल को कवर करते हुए परिभाषित की गयीं और उपयोगकर्ताओं/कर्मचारियों, विक्रेताओं और भागीदारों को सूचित की गयीं हैं और उन्हें साइबर सुरक्षा जोखिमों और उनके स्तर पर सुरक्षा उपायों के बारे में उन्हें शिक्षित करने के लिए सुरक्षा नीतियाँ है?	हाँ	हाँ	हाँ
164	जागरूकता एवं प्रशिक्षण (पीआर.एटी):	क्या उपयोगकर्ता यह दर्शाते हैं कि वे अपना उत्तरदायित्व समझते हैं?	हाँ	हाँ	हाँ
165	जागरूकता एवं प्रशिक्षण (पीआर.एटी):	क्या जागरूकता स्तर का सावधिक रूप से मूल्यांकन किया जाता है?	हाँ	वार्षिक	दो वर्ष में एक बार

166	जागरूकता एवं प्रशिक्षण (पी.आर.एटी):	सुरक्षा की घटना के अवसर पर उनकी भूमिका समझाने के लिए क्या अगुआ लोगों के लिए कोई अतिरिक्त प्रशिक्षण है?	हाँ	हाँ	हाँ
167	जागरूकता एवं प्रशिक्षण (पी.आर.एटी):	यदि उपयोगकर्ता प्रशिक्षण पूरा नहीं करता तो उस स्थिति से निपटने के लिए क्या कोई प्रक्रिया है?	हाँ	हाँ	हाँ
168	जागरूकता एवं प्रशिक्षण (पी.आर.एटी):	क्या संस्था के लिए सुरक्षा प्रशिक्षण का सृजन करने के लिए कोई उत्तरदायी है?	हाँ	हाँ	हाँ
169	जागरूकता एवं प्रशिक्षण (पी.आर.एटी):	क्या संस्था ने राष्ट्रीय/क्षेत्रीय/संगठनात्मक साइबर सुरक्षा अभ्यासों में सावधिक रूप से भाग लिया है?	हाँ	हाँ	हाँ
170	डेटा सुरक्षा (पी.आर.डीएस):	क्या नेटवर्क और प्रणाली पर कोई खुले पोर्ट हैं जो इस्तेमाल में नहीं हैं, ब्लॉक किये गये हैं?	हाँ	हाँ	हाँ
171	डेटा सुरक्षा (पी.आर.डीएस):	क्या अनुप्रयोग निष्क्रियता की पूर्वनिर्धारित अवधि के बाद किसी उपयोगकर्ता को स्वचालित रूप से लॉग ऑफ करने के लिए अनुप्रयोग सेट किया जा सकता है?	हाँ	हाँ	हाँ
172	डेटा सुरक्षा (पी.आर.डीएस):	क्या अनुप्रयोग पासवर्ड समय-सीमा समाप्ति को विवश कर सकता है और उपयोगकर्ता को पासवर्ड को पुनः इस्तेमाल करने से रोक सकता है?	हाँ	हाँ	हाँ
173	डेटा सुरक्षा (पी.आर.डीएस):	क्या प्रणाली प्रशासक पासवर्ड पालिसी और/या कम से कम लंबाई, अंक और अक्षर आवश्यकताओं और बड़ा अक्षर और छोटा अक्षर की बाधाओं इत्यादि जैसी पेचीदगियों को लागू कर सकता है?	हाँ	हाँ	हाँ
174	डेटा सुरक्षा (पी.आर.डीएस):	क्या अनुप्रयोग नये उपयोगकर्ताओं को अनुप्रयोग में पहले लॉग-इन पर उनके पासवर्ड को बदलने के लिए बाध्य कर सकता है?	हाँ	हाँ	हाँ
175	डेटा सुरक्षा (पी.आर.डीएस):	क्या अनुप्रयोग उपयोगकर्ताओं को एक ही समय पर उसी यूजर आईडी से एक से अधिक कार्य स्टेशन पर अनुप्रयोग के अन्दर लॉगिंग करने से प्रतिबंधित करता है?	हाँ	हाँ	हाँ
176	डेटा सुरक्षा (पी.आर.डीएस):	क्या अनुप्रयोग, उद्यम पहचान प्रबंधन प्रणाली के साथ एकीकरण को सहयोग करता है?	हाँ	हाँ	हाँ
177	डेटा सुरक्षा (पी.आर.डीएस):	क्या संस्था अपने सू.प्रौ. आधारभूत संरचना के भीतर, उपयुक्त वैधीकरण प्रक्रिया के माध्यम से डेटा स्टोरेज उपकरणों को प्राधिकृत करता है?	हाँ	हाँ	हाँ

178	डेटा सुरक्षा (पीआर.डीएस):	क्या वहाँ कोई प्रक्रिया है जिसके द्वारा संस्था मीडिया निपटान के प्रमाण बनाये रखता है?	हाँ	हाँ	हाँ
179	डेटा सुरक्षा (पीआर.डीएस):	क्या वहाँ डेटा-निपटान और डेटा-प्रतिधारण नीति का कार्यान्वयन किया जाता रहा है?	हाँ	हाँ	हाँ
180	डेटा सुरक्षा (पीआर.डीएस):	क्या मीडिया प्रारूपण के लिए कोई प्रक्रियाएँ हैं?	हाँ	हाँ	हाँ
181	डेटा सुरक्षा (पीआर.डीएस):	क्या वहाँ किसी ग्राहक प्रणाली की भेदताओं की पैमाइश होती है?	हाँ	ऐच्छिक	ऐच्छिक
182	डेटा सुरक्षा (पीआर.डीएस):	क्या उपयोगकर्ता प्रमाणीकरण उपयोगकर्ता के खाते और पासवर्ड या पिन के अलावा किसी अन्य माध्यम से नियंत्रित होता है?	हाँ	हाँ	हाँ
183	डेटा सुरक्षा (पीआर.डीएस):	क्या तृतीय पक्षों से डेटा साझा करने के लिए विभिन्न सुरक्षा क्रियाविधियों का इस्तेमाल किया जाता है?	हाँ	हाँ	हाँ
184	डेटा सुरक्षा (पीआर.डीएस):	क्या डेटा एन्क्रिप्ट करने के लिए विभिन्न प्रौद्योगिकियाँ लागू की गयी है?	हाँ	हाँ	सीमित
185	डेटा सुरक्षा (पीआर.डीएस):	डेटा मोबिलिटी सुरक्षा के लिये उपयुक्त प्रौद्योगिकी लागू की गयी है?	हाँ	हाँ	ऐच्छिक
186	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या कार्यस्थल के बाहर पीसी, सॉफ्टवेयर और दस्तावेजीकरण की प्रतिलिपि प्रतियाँ रखीं गयीं हैं?	हाँ	हाँ	हाँ
187	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या सॉफ्टवेयर को अलग करने और चलाने के लिए इस्तेमाल की जाने वाली प्रणालियों को जो व्यापार परिचालनों के लिए आवश्यक हैं लेकिन संस्था के लिए उच्चतर जोखिम उपचित करते हैं, भौतिक रूप से या ताकिक रूप से पृथक किया जाता है?	हाँ	हाँ	हाँ
188	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	यदि कार्यस्थल (साइट) भ्रष्ट है तो व्यवस्थित बहाली सुनिश्चित करने के लिए वेबसाइट की अन्तर्वस्तु को समर्थन दिया जाता है?	हाँ	हाँ	हाँ
189	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	व्यक्तिगत फाइलों और विभाग द्वारा साझा की गयी फाइलों में अन्य समूहों द्वारा अनाधिकृत प्रवेश रोकने के लिये कोई तरीके हैं?	हाँ	हाँ	हाँ

190	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	एलएएन और नेटवर्क परिचालन सॉफ्टवेयर के प्रवेश को सीमित करने के लिए कोई क्रियाविधियाँ हैं?	हाँ	हाँ	हाँ
191	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या वेबसाइट के अद्यतन स्वतंत्र रूप से समीक्षित, स्वीकृत और परीक्षित किये जाते हैं?	हाँ	हाँ	हाँ
192	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या सूचना सुरक्षा नीति में, उपकरणों जैसे मोबाइल फोनों, फैक्सों, फोटो कॉपियरों, स्कैनरों इत्यादि के इस्तेमाल को उनके महत्वपूर्ण सू.प्रौ. संरचनात्मक ढाँचे के भीतर, जिनको संवेदनशील डेटा प्राप्त करने और संचरित करने के लिए किया जा सकता है, शामिल किया जाता है?	हाँ	हाँ	हाँ
193	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या संस्था, सभी परिसंपत्तियों पर, यह सुनिश्चित करने के लिए कि केवल प्राधिकृत सॉफ्टवेयर निष्पादन करते हैं और सभी अनधिकृत सॉफ्टवेयर को परिसंपत्तियों को निष्पादन करने के लिए रोकने के लिए वाइट लिस्टिंग प्रौद्योगिकी अनुप्रयोग का इस्तेमाल करती है?	हाँ	हाँ	हाँ
194	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या संस्था, व्यापार प्रणालियों पर सभी सॉफ्टवेयर के दस्तावेजीकरण को स्वचालित करने के लिए संस्था में सर्वत्र सॉफ्टवेयर इन्वेंटरी उपकरण इस्तेमाल करती है?	हाँ	हाँ	सीमित
195	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या संस्था के पास प्रमुख हार्डवेयर या सॉफ्टवेयर की विफलता की स्थिति में महत्वपूर्ण कार्यों के प्रसंस्करण के लिए आपदा बहाली योजना का कोई दस्तावेज है?	हाँ	हाँ	हाँ
196	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या संस्था का अनुप्रयोग वाइटलिस्टिंग सॉफ्टवेयर सुनिश्चित करता है कि केवल प्राधिकृत सॉफ्टवेयर पुस्तकालय (जैसे *.dll, *.ocx, *.so, इत्यादि.) को ही प्रणाली प्रक्रिया में लोड करने की अनुमति दी जाती है?	हाँ	हाँ	हाँ
197	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या संस्था के अनुप्रयोग वाइटलिस्टिंग सॉफ्टवेयर को ही सुनिश्चित करना चाहिए कि केवल प्राधिकृत डिजिटल रूप से हस्ताक्षरित आलेख (जैसे *.ps1, *.py, macros, इत्यादि) को ही प्रणाली पर चलाये जाने के लिए अनुमति दी जाती है?	हाँ	हाँ	हाँ
198	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या संस्था सावधिक सूची यह जाँच करने के लिए ली जाती है कि उपयुक्त बैकअप फाइलों को रखा जा रहा है?	हाँ	हाँ	हाँ
199	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या उपयुक्त हार्डवेयर बैकअप उपलब्ध है?	हाँ	हाँ	हाँ
200	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या यह सुनिश्चित किया गया है कि केवल वही सॉफ्टवेयर अनुप्रयोग या परिचालन प्रणालियाँ जो वर्तमान में सॉफ्टवेयर विक्रेता द्वारा समर्थित हैं, संस्था की प्राधिकृत सॉफ्टवेयर सूची में जोड़ी जाती हैं। अप्राधिकृत सॉफ्टवेयर को सूची प्रणाली में असमर्थित के रूप में टैग (नली) किया जाना चाहिए?	हाँ	हाँ	हाँ
201	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या यह सुनिश्चित किया गया है कि सॉफ्टवेयर सूची प्रणाली को हार्डवेयर परिसंपत्ति सूची में बाँधा जाना चाहिए ताकि सभी उपकरण और सहबद्ध सॉफ्टवेयर को एक ही स्थान से ट्रैक किया जाता है?	हाँ	हाँ	हाँ

202	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	दूरस्थ प्रवेश सॉफ्टवेयर प्रतिबंधित किया गया है?	हाँ	हाँ	हाँ
203	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या डेटा, प्रोग्राम, हार्डवेयर और प्रणाली की जरूरतों के व्यौरे का दस्तावेज तैयार किया गया है?	हाँ	हाँ	हाँ
204	सूचना संरक्षण प्रक्रियाएँ एवं क्रियाविधियाँ (पीआर.आईपी):	क्या सुरक्षा के भिन्न स्तरों पर महत्वपूर्ण जानकारी के संरक्षण के लिए नीतियों और क्रियाविधियों का इस्तेमाल किया जा रहा है?	हाँ	हाँ	हाँ
205	रख-रखाव (पीआर.एमए):	क्या यह तय करने के लिए कोई प्रक्रिया है कि पहचान के कितने दिनों बाद पैचों को बंद किया जाएगा?	हाँ	हाँ	हाँ
206	रख-रखाव (पीआर.एमए):	क्या संस्था की परिसंपत्तियों के दूरस्थ रख-रखाव को इस तरह से मंजूर, लॉग और निष्पादित किया गया है जो अनधिकृत प्रवेश की रोकथाम करते हैं?	हाँ	हाँ	हाँ
207	रख-रखाव (पीआर.एमए):	पैचों को स्थापित करने की जरूरत को प्राथमिकता देने के लिए परिभाषित प्राचल लिये गये हैं?	हाँ	हाँ	हाँ
208	रख-रखाव (पीआर.एमए):	संस्था की परिसंपत्तियों के रख-रखाव और मरम्मत जब भी निष्पादित किए जाते हैं, स्वीकृत और नियंत्रित उपकरणों के साथ लागू किये गये हैं?	हाँ	हाँ	हाँ
209	रख-रखाव (पीआर.एमए):	महत्वपूर्ण पैचों को परीक्षण परिवेशों में तैनात करने के लिए क्या कोई प्रक्रिया है?	हाँ	हाँ	हाँ
210	रख-रखाव (पीआर.एमए):	क्या स्वीकृत पैच प्रबंधन नीति लागू की गयी है?	हाँ	हाँ	हाँ
211	रख-रखाव (पीआर.एमए):	पैचों के वर्गीकरण के लिए परिधियों को परिभाषित किया गया है?	हाँ	हाँ	हाँ
212	सुरक्षात्मक प्रौद्योगिकी (पीआर.पीटी):	क्या मौद्रिक लेन-देनों के अनुप्रयोगों/प्रक्रिया को चलाने के लिए सर्वरों की संयोजकर्ता और परिधि को पृथक और सुरक्षित रखने के लिए पर्याप्त उपाय किय गये हैं?	हाँ	हाँ	हाँ
213	सुरक्षात्मक प्रौद्योगिकी (पीआर.पीटी):	क्या संस्था विभिन्न विक्रेताओं /ओईएम, सीईआरटी-इन द्वारा जारी /परामशों और अन्य समान एजेंसियों द्वारा जारी पैचों की निरंतर निगरानी करती है और पैच प्रबंध नीति के अनुसार सुरक्षा पैच लागू करती है?	हाँ	हाँ	हाँ



214	सुरक्षात्मक प्रौद्योगिकी (पी.आर.पीटी):	क्या संस्था ने, वायरस/मालवेयर/रेंसमवेयर आक्रमणों को रोकने के लिए, हॉटस्पॉट/नेटवर्क/अनुप्रयोग आधारित आईडीएस प्रणालियाँ, लाइनव्स के लिए अनुकूलित केमैल्स एंटी वायरस और एंटी मालवेयर सॉफ्टवेयर इत्यादि जैसे नियंत्रण तैनात किये हैं?	हाँ	हाँ	हाँ
215	सुरक्षात्मक प्रौद्योगिकी (पी.आर.पीटी):	क्या संस्था ने, संस्था के भागीदारों एवं विक्रेताओं द्वारा इस्तेमाल किये जा रहे सहित, जिसमें ई-मेल-स्पूफिंग, एक जैसे मेल ज्ञान क्षेत्र, संलग्नकों के संरक्षण, दुर्भावनपूर्ण कडियों को रोकने के उपाय शामिल हैं, सुरक्षित मेल और संदेश प्रणालियाँ प्रलेखित और क्रियान्वित की गई है?	हाँ	हाँ	हाँ
216	सुरक्षात्मक प्रौद्योगिकी (पी.आर.पीटी):	क्या संस्था ने अपने सू.प्रौ. परिवेश के भीतर परिचालन प्रणालियों, डेटाबेसों, नेटवर्क उपकरणों और उद्यम के मोबाइल उपकरणों के लिए सुरक्षा विन्यासों के निरंतर अनुप्रयोग को सरल बनाने के लिये बेसलाइन मानक स्थापित किया है?	हाँ	हाँ	हाँ
217	सुरक्षात्मक प्रौद्योगिकी (पी.आर.पीटी):	क्या संस्था ने, अंतिम उपयोगकर्ता निजी कम्प्यूटरों, कार्य स्टेशनों, सर्वरों, मोबाइल उपकरणों इत्यादि पर सॉफ्टवेयर/अनुप्रयोगों की स्थापना को नियंत्रित करने के लिए कार्यप्रणाली और ऐसे उपकरणों, प्रणालियों पर अनधिकृत सॉफ्टवेयर/अनुप्रयोग स्थापित करने और चलाये जाने का पता लगाने, उसको बाधित करने/रोकने के लिए कोई कार्य प्रणाली लागू की है?	हाँ	हाँ	हाँ
218	सुरक्षात्मक प्रौद्योगिकी (पी.आर.पीटी):	क्या संस्था ने, अपने सू.प्रौ. संरचनात्मक ढाँचे, को जोकि इंटरनेट के संपर्क में होते हैं, आंतरिक और बाह्य स्रोतों से उत्पन्न होने वाले सुरक्षा एक्सपोजर्स से सुरक्षित रखने के लिए नेटवर्क सुरक्षा उपकरणों, जैसे फायरवालों, परोक्षी सर्वरों, अतिक्रमण-सुरागसानी और रोकथाम प्रणाली की स्थापना की है?	हाँ	हाँ	हाँ
219	संचार (आरसी.सी.ओ):	क्या बहाली गतिविधियों की जानकारी आन्तरिक और बाहरी हितधारकों और साथ ही साथ कार्यपालक और प्रबंधन दल को दी गयी है?	हाँ	हाँ	हाँ
220	सुधार (आरसी.आईएम):	क्या बहाली रणनीति को सावधिक रूप से अद्यतन किया जाता है?	हाँ	हाँ	हाँ
221	सुधार (आरसी.आईएम):	क्या सीखे गये पाठों को बहाली योजना में शामिल किया जाता है?	हाँ	हाँ	हाँ
222	बहाली योजना (आरसी.आरपी):	क्या बहाली योजना का निष्पादन किसी साइबर सुरक्षा घटना के दौरान या बाद में किया जाता है?	हाँ	हाँ	हाँ
223	विश्लेषण (आरएस.एएन)	क्या आन्तरिक और बाह्य स्रोतों द्वारा संस्था को भेदताओं के खुलासे को प्राप्त, विश्लेषण और प्रतिक्रिया करने के लिए प्रक्रियाएँ स्थापित की गयी हैं? (उदा. आन्तरिक परीक्षण, सुरक्षा बुलेटिन या सुरक्षा अनुसंस्थानकर्ता)	हाँ	हाँ	हाँ
224	विश्लेषण (आरएस.एएन)	क्या संस्था के पास सुनिश्चित करने के लिए कि किसी घटना के प्रभाव का विश्लेषण किया गया है, कोई क्रियाविधि है?	हाँ	हाँ	हाँ
225	विश्लेषण (आरएस.एएन)	क्या संस्था के पास यह सुनिश्चित करने कोई क्रियाविधि है, जिससे सुरागसानी प्रणालियों से अधिसूचनाओं की जाँच की जाती है?	हाँ	हाँ	हाँ

226	विश्लेषण (आरएस.एन):	क्या संस्था के पास सुनिश्चित करने के लिए कोई क्रियाविधि है जिससे न्याय संबंधी कार्यों का निष्पादन किया जाता है?	हाँ	हाँ	हाँ
227	संचार (आरएस.सीओ):	क्या साइबर आक्रमण से संबंधित घटनाओं को वश में किया जाता और लॉग किया जाता है?	हाँ	हाँ	हाँ
228	संचार (आरएस.सीओ):	क्या साइबर से संबंधित घटना की, उच्चाधिकारियों को, जानकारी दी जाती है?	हाँ	हाँ	हाँ
229	संचार (आरएस.सीओ):	क्या साइबर घटनाओं की रिपोर्ट, ऐसी घटनाओं को नोटिस करने या नोटिस में लाये जाने के छह घंटे के भीतर सीईआरटी-इन को दी जाती है?	हाँ	हाँ	हाँ
230	संचार (आरएस.सीओ):	क्या तृतीय पक्षों के लिए संविदात्मक रूप से अनिवार्य है कि वे उनसे साझा की जाने वाली जानकारी को एक घटना के अंग के रूप में सुरक्षित रखें?	हाँ	हाँ	हाँ
231	संचार (आरएस.सीओ):	क्या घटना समाधानों के लिए एनसीआईआईपीसी और सीईआर टी-इन जैसी एजेंसियों, मंत्रालयों, हितधारकों, विक्रेताओं के संपर्क विवरण अद्यतन और प्रलेखित हैं?	हाँ	हाँ	हाँ
232	संचार (आरएस.सीओ):	क्या आईआरडीएआई, सीईआरटी-इन सहित बाह्य संस्थाओं को घटनाओं की रिपोर्ट करने के लिए समय-सीमा निर्धारित की गयी है?	हाँ	हाँ	हाँ
233	संचार (आरएस.सीओ):	क्या घटना के मूल कारण विश्लेषण और की गयी कार्रवाई की रिपोर्ट संबंधित बीमाकर्ता को माँगने पर प्रस्तुत की जाती है?	हाँ	हाँ	हाँ
234	सुधार (आरएस.आईएम):	क्या प्रतिक्रिया रणनीति को सावधिक रूप से अद्यतन किया जाता है?	हाँ	हाँ	हाँ
235	सुधार (आरएस.आईएम):	क्या बोर्ड के सदस्यों को सु.प्रौ. जोखिम/साइबर सुरक्षा जोखिम संबंधी प्रशिक्षण कार्यक्रम उपलब्ध कराये जाते हैं और इस संबंध में सर्वोत्तम प्रथाओं का विकास किया जाता है ताकि वर्ष में कम से कम एक बार बोर्ड के सभी सदस्यों को शामिल किया जा सके?	हाँ	प्रबंध निदेशक	प्रबंध निदेशक
236	सुधार (आरएस.आईएम):	क्या सर्वोच्च प्रबंधन को सावधिक रूप से विभिन्न प्रौद्योगिक घटनाक्रमों और साइबर सुरक्षा से संबंधित घटनाक्रमों के संबंध में संवेदनशील बनाया जाता है?	हाँ	वार्षिक	वार्षिक
237	सुधार (आरएस.आईएम):		हाँ	हाँ	हाँ

238	शमन (आरएस.एमआई):	क्या संस्था ने घटना प्रबंधन प्रतिक्रिया क्रियाविधि को परिभाषित किया है ?	हाँ	हाँ	हाँ
239	शमन (आरएस.एमआई):	क्या नयी पहचानी गयी भेदताओं का अल्पीकरण किया गया या स्वीकार्य जोखिमों के रूप में प्रलेखित किया गया है?	हाँ	हाँ	हाँ
240	शमन (आरएस.एमआई):	क्या वीएपी में सभी पहचानी गयी भेदताओं के लिए सुधारात्मक कार्यवाही क्रियाविधि हैं?	हाँ	हाँ	हाँ
241	प्रतिक्रिया योजना (आरएस.आरएपी):	प्रबंधन को शामिल करने और बैकअप से पुनर्प्राप्त करने क्या योजना को तिमाही रूप में परीक्षित किया जाता है?	हाँ	वार्षिक	वार्षिक
242	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या संस्था इस्तेमाल में प्रत्येक नेटवर्क उपकरण के लिए परिभाषित स्वीकृत सुरक्षा विन्यासों के विरुद्ध सभी नेटवर्क उपकरण विन्यासों की तुलना करती है और जब कोई विचलन पाया जाता है तो चेतावनी देती है?	हाँ	हाँ	हाँ
243	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या संस्था यह सुनिश्चित करती है कि सभी बैकअपों में कम से कम एक बैकअप गंतव्य ऐसा हो जो कि परिचालन प्रणाली कॉल/ऑफ लाइन बैकअप के माध्यम से निरंतर रूप से पता करने योग्य नहीं हो?	हाँ	हाँ	संवेदनशील डेटा
244	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या संस्था यह सुनिश्चित करती है कि संस्था की सभी मूल/महत्वपूर्ण प्रणालियाँ, इमेजिंग जैसी प्रक्रियाओं के माध्यम से एक संपूर्ण प्रणाली के रूप में समर्थित हैं ताकि एक संपूर्ण प्रणाली को तुरंत बहाल किया जा सके?	हाँ	हाँ	हाँ
245	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या संस्था सभी नेटवर्क उपकरणों पर किसी सुरक्षा से संबंधित अद्यतन के नवीनतम स्थायी संस्करण को स्थापित करती है?	हाँ	हाँ	हाँ
246	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या संस्था सभी प्राधिकृत नेटवर्क उपकरणों के लिए प्रलेखित सुरक्षा विन्यास मानक बनाये रखती है?	हाँ	हाँ	हाँ
247	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या संस्था, सुनिश्चित करने के लिए कि बैकअप ठीक से काम कर रहा है, नियमित रूप से एक डेटा बहाली प्रक्रिया करके बैकअप मीडिया पर डेटा अखंडता की जाँच करती है?	द्वि-वार्षिक	द्वि-वार्षिक	वार्षिक
248	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या व्यापार प्रभाव विश्लेषण आयोजित किया गया है?	हाँ	हाँ	हाँ
249	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या संस्था ने व्यापार निरंतरता योजना और क्रियाविधि परिभाषित की है?	हाँ	हाँ	हाँ

250	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या संस्था ने यह सुनिश्चित किया है कि आरपीओ (पुनर्प्राप्ति बिन्दु उद्देश्य) और आरटीओ (पुनर्प्राप्ति बिन्दु उद्देश्य) नीति के अनुकूल हैं?	हाँ	हाँ	हाँ
251	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या घटनाओं की प्रतिक्रिया और विश्लेषण किया गया है?	हाँ	हाँ	हाँ
252	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या सुरक्षा घटनाओं का विश्लेषण किया गया और निरंतर सुधार के लिए सुधारात्मक कार्रवाईयों को लागू किया गया है ?	हाँ	हाँ	हाँ
253	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या पुनर्प्राप्ति योजना समझी गयी और सभी सुरक्षा प्रशिक्षण के माध्यम से बतायी गयी है? क्या कर्मचारियों के उत्तरदायित्वों और भूमिकाओं को योजना में सुस्पष्ट रूप से कहा गया और बताया गया है?	हाँ	हाँ	हाँ
254	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या वहाँ स्पष्ट रूप से परिभाषित भूमिकाओं और उत्तरदायित्वों वाला कोई घटना प्रतिक्रिया/संकट काल दल है?	हाँ	हाँ	हाँ
255	प्रतिक्रिया योजना (आरएस.आरएपी):	क्या साइबर संकट-काल योजना को लागू किया गया, उसका अभ्यास किया गया या सांविधिक रूप से उसका रिहर्सल किया गया है?	हाँ	हाँ	वार्षिक
256	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या बोर्ड द्वारा मंजूर साइबर सुरक्षा नीति, विनियमित इकाई की (नीति), दूरस्थ स्थान से कार्य करना (डब्ल्यू एफआरएल) जोखिमों से जुड़े जोखिमों का समाधान करती है?	हाँ	प्रबंध निदेशक	प्रबंध निदेशक
257	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या नीति, सुदृढ़ नयाचारों के साथ सुरक्षित नेटवर्क और दूरस्थ स्थान पर वाइफाई पासवर्डों के इस्तेमाल की पुष्टि करती है?	हाँ	हाँ	हाँ
258	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या यह सांविधिक रूप से पासवर्डों के बदलावों का अधिदेश करती है?	हाँ	हाँ	हाँ
259	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या उपयोगकर्ताओं को संस्था के प्राधिकृत परिसंपत्तियाँ उपलब्ध करायी गयी हैं, जो कि सुदृढ़ पासवर्ड प्रमाणीकरण के लिये सुरक्षा नीति के अनुसार कठोर हैं?	हाँ	हाँ	हाँ
260	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या सर्वर, अनुप्रयोग और नेटवर्क कठोर और मानकीकृत सुरक्षा नीति समायोजनों के अनुसार सुरक्षित हैं?	हाँ	हाँ	हाँ
261	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या प्रशासन स्तर प्रवेश, अप्राधिकृत अधिष्ठापनों या सॉफ्टवेयर में बदलावों, यूएसबी और अन्य मीडिया, बाह्य उपकरणों को बाधित करने के लिए, उपयोगकर्ता प्रणालियों और सूचना तथा संचार प्रौद्योगिकी (आईसीटी) संरचनात्मक ढाँचे पर उपकरण नियंत्रण लागू किये गये हैं?	हाँ	हाँ	हाँ

262	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या उपयोगकर्ता प्रणालियों को, एण्टीवायरस, एंड पाइंट सुरक्षा नियंत्रणों, डेटा कूटलेखन (एन्क्रिप्टन) और डेटा हानि रोकथाम कार्य प्रणालियों से सक्षम बनाया गया है?	हाँ	हाँ	हाँ
263	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या ये नियंत्रण, सभी उपयोगकर्ताओं को सभी कार्यकलापों में सभी जगह व्याप्त होते हैं?	हाँ	हाँ	हाँ
264	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या उपयोगकर्ता प्रणालियाँ और संस्था को आईसीटी संरचनात्मक ढाँचा सुरक्षा पैचों और फिक्सों के साथ नियमित रूप से अद्यतन की जानी है (लेखा परीक्षक नवीनतम अद्यतन तिथि का उल्लेख करें)?	हाँ	हाँ	हाँ
265	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या कार्य प्रवाह मंजूरीयाँ, विचलन या अपवादों को परिवर्तन प्रबंधन क्रियाविधियों के अनुसार अधिकृत किया गया है?	हाँ	हाँ	हाँ
266	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या आभासी निजी नेटवर्क (वीपीएन), इंटरनेट परोक्षी (प्रॉक्सी) या आभासी उपकरण अन्तराफलक (इंटरफेस)(वीडीआई) की कार्य प्रणाली का, डब्ल्यूएफआरएल उपयोगकर्ता प्रवेश संस्थागत डेटा परिसंपत्तियों और अनुप्रयोगों के लिए प्रावधानीकरण किया गया है?	हाँ	हाँ	हाँ
267	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या अनधिकृत प्रवेश जोखिमों और साइबर खतरों के लिए एक नियंत्रण के रूप में संस्थागत आईसीटी संरचनात्मक ढाँचे पर अंकेक्षण लॉग निगरानी और विश्लेषण का प्रावधानीकरण किया गया है?	हाँ	हाँ	हाँ
268	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या उपयोगकर्ताओं को, सुदृढ़ पासवर्ड प्रामाणीकरण के लिए बीमाकर्ता द्वारा प्राधिकृत परिसंपत्तियाँ उपलब्ध करायी गयी है जिन्हें बीमाकर्ता सुरक्षा नीति व्यवस्थाओं के अनुसार कठोर किया गया है?	हाँ	हाँ	हाँ
269	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या नीति, संस्थागत डेटा परिसंपत्तियों और उपयोगकर्ता के निजी उपकरणों, जैसे मोबाइल फोनों, टैबलेटों या बीमाकर्ता के अन्य, अपने निजी उपकरण लाएं (बीवाईओडी) से अनुप्रयोगों के सुरक्षित प्रवेश से संबंधित नियंत्रणों और क्रियाविधियों के बारे में सूचित करती है?	हाँ	हाँ	हाँ
270	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या, जब बीमाकर्ता द्वारा डब्ल्यू एफआरएल की अनुमति दी गयी है उस अवधि के दौरान डेटा के साथ छेड़छाड़ और खो गये मोबाइल/टैबलेट उपकरणों का दुरुपयोग रोकने के लिये डेटा कंटेनरीकरण, बहुकारकीय प्रामाणीकरण और दूरस्थ डेटा सफाई की गयी है?	हाँ	हाँ	सीमित
271	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या उपयोगकर्ता को, संस्था की प्रणालियों में सुरक्षित स्थानों पर सावधिक रूप से महत्वपूर्ण डेटा बैकअप करने के लिए अधिदिष्ट किया गया है?(नीति सावधिक रूप से अधिदिष्ट करेगी)	हाँ	हाँ	हाँ
272	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	डब्ल्यूएफआरएल पर परिचालन आरंभ करने की अनुमति देने से पूर्व और गोपनीयता डेटा सुरक्षा के संबंध में कर्मचारी/परामर्शदाता/तृतीय-पक्ष विक्रेता के साथ गैर-प्रकटन समझौते/वचनपत्र पर हस्ताक्षर किये गये हैं?	हाँ	हाँ	हाँ
273	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या उपयोगकर्ताओं को बीमाकर्ता द्वारा प्राधिकृत परिसंपत्तियाँ उपलब्ध करायी गयी और सुरक्षा नीति व्यवस्थाओं और सुदृढ़ पासवर्ड प्रामाणीकरण के अनुसार उन्हें कठोर बनाया गया है?	हाँ	हाँ	हाँ

274	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या, प्रशासकीय उद्देश्यों से लिये गये विशेषाधिकार प्राप्त उपयोगकर्ता पहचान प्रवेश प्रामाणिकरण का कोई अंकेक्षण होता है?	हाँ	हाँ	हाँ
275	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या वहाँ, कोई सुरक्षा जानकारी का अंकेक्षण और अंकेक्षण लॉग विश्लेषण की घटनाओं की निगरानी और घटना प्रतिक्रिया होती है?	हाँ	हाँ	सीमित
276	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या अप्राधिकृत प्रवेश, दुर्भावनापूर्ण कूट निष्पादन, संदिग्ध गतिविधियों या व्यवहार, सार्व की चोरी, अग्रिम निरन्तर खतरों जैसे दूरस्थ प्रवेश टूल किटों और संस्थागत आईसीटी आधारभूत संरचना को ऐसे साइबर जोखिमों की पहचान करने के लिए नियंत्रणों की व्यवस्था की गयी है?	हाँ	हाँ	हाँ
277	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	सैम, जाली मेलों और मैलवेयर फिल्टरिंग की रोकथाम के लिए ई-मेल सेवाएँ सुरक्षित हैं?	हाँ	हाँ	हाँ
278	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	सैम, फिशिंग घोटाले और छलपूर्ण ई-मेलों से निपटने के लिए उपयोगकर्ताओं को प्रशिक्षित किया गया है?	हाँ	हाँ	हाँ
279	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या इंटरनेट पर संदिग्ध या दुर्भावनापूर्ण कार्यक्षेत्रों को, नेटवर्क, फायरवाल, वेब प्राक्सी फिल्टरिंग, अतिक्रमण की रोकथाम प्रणालियों की पहचान की गयी और उनको बाधित किया या है?	हाँ	हाँ	हाँ
280	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	अप्राधिकृत इंटरनेट कार्यक्षेत्रों, अप्राधिकृत सॉफ्टवेयर अधिष्ठापनों या विन्यासों, यूएबी और अन्य मीडिया बाह्य उपकरणों में बदलावों को बाधित करने के लिए, उपयोगकर्ता प्रणालियों और आईसीटी आधारभूत संरचना प्रणालियों के संबंध में उपकरण नियंत्रणों को लागू किया गया है?	हाँ	हाँ	हाँ
281	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या उपयोगकर्ता प्रणालियों और संस्था की आईसीटी आधारभूत संरचना को, सुरक्षा पैचों और फिक्सों के साथ अद्यतन किया जाता है? (नवीनतम अद्यतन तिथि का उल्लेख करें)	हाँ	हाँ	हाँ
282	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	लेखा परीक्षिती और लेखा परीक्षक संस्थाओं की सुरक्षित और कठोर की गयी प्रणालियों पर स्वीकृत दूरस्थ प्रवेश सॉफ्टवेयर का इस्तेमाल करते हुए पूर्वाभ्यास और साक्षात्कार जैसी गतिविधियों की जाती हैं?	हाँ	हाँ	हाँ
283	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या प्रमाणों और कलाकृतियों का वर्गीकरण, किया गया और संबंधित हितधारकों को उनका सुरक्षित रूप से प्रदर्शन किया गया और उन्हें प्राधिकृत कार्यक्षेत्र के बाहर साझा नहीं किया गया है?	हाँ	हाँ	हाँ
284	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या परियोजना कार्यान्वयन कार्यक्रम दस्तावेजों, एनआईएस रिपोर्टों को वर्गीकृत किया जाता और जानने की आवश्यकता के आधार पर साझा किया जाता है?	हाँ	हाँ	हाँ
285	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या संस्था द्वारा, साइबर सुरक्षा घटना प्रतिक्रिया और संकट प्रबंधन गतिविधियों के लिये, योजनाओं और क्रियाविधियों की व्यवस्था की गयी है?	हाँ	हाँ	हाँ

286	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या साइबर सुरक्षा परियोजना प्रबंधन दूर से पूरा किया जाता है?	हाँ	हाँ	हाँ
287	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	पुष्टि करें कि क्या, प्रणालियों की जाँच / स्कैन करने के लिए कठोर क्रियाविधियों को कार्यालय में वापस लाया गया है?	हाँ	हाँ	हाँ
288	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	पुष्टि करें कि क्या सभी पैचों, एबी, अंतिम बिन्दु संरक्षण, डेटा कूट लेखन-कार्यप्रणालियों की उनका उपयुक्त कामकाज सुनिश्चित करने के लिए जाँच कर ली गयी है?	हाँ	सीमित	सीमित
289	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या उपयोगकर्ता प्रणालियाँ और संस्था की आईसीटी आधारभूत संरचना प्रणालियाँ, सुरक्षा पैचों और फिक्सों के साथ नियमित रूप से अद्यतन की जाती हैं?	हाँ	हाँ	हाँ
290	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या सुरक्षा घटना लेखा परीक्षा लॉग निगरानी और विश्लेषण का, बीमाकर्ता आईसीटी आधारभूत संरचना पर प्रावधानीकरण किया गया है?	हाँ	हाँ	हाँ
291	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या सेवाओं के वितरित नकार (डीडीओएस) आक्रमणों की रोकथाम के लिए आईसीटी आधारभूत संरचना पर सुरक्षा पैच अद्यतनों की समीक्षा की गयी और (उनको) सावधिक रूप से लागू किया गया?	हाँ	हाँ	हाँ
292	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	विच्छेद की स्थिति में, क्या पोर्टल, हेल्पडेस्क (फोन) या ई-मेल के माध्यमों से या कार्यालय जाकर निवेश अनुप्रयोगी उपयोगकर्ता द्वारा आईटी समर्थन तक पहुँचा जा सकता है?	हाँ	हाँ	हाँ
293	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	बन्द रहने के समय के प्रभाव को कम करने के लिए सावधिक रूप से बैकअप की समीक्षा और कार्य प्रणालियों को संरक्षित किया जाता है?	हाँ	हाँ	हाँ
294	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	व्यापार निरन्तरता मैट्रिक्स का पालन सुनिश्चित करने के लिए डीआर अभ्यास किया जाता है? (डीआर अभ्यास सामान्य कार्य दिवस पर किया जाना चाहिए।)	हाँ	वार्षिक	वार्षिक
295	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या बैकअपों की अखंडता सुनिश्चित करने के लिए क्या आवधिक आधार पर डेटा बहाली परीक्षण किया जाता है?	द्वि-वार्षिक	द्वि-वार्षिक	वार्षिक
296	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या, व्यापार निरन्तरता के अंग के रूप में वैकल्पिक कार्यस्थल विकल्पों और संसाधन उपलब्धता की योजना बनायी गयी और उनका परीक्षण किया गया है?	हाँ	हाँ	हाँ
297	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या द्वितीयक नेटवर्क संयोजकर्ता और सू.प्रौ. आधारभूत संरचना का प्रावधान किया गया और महत्वपूर्ण अनुप्रयोगों और सेवाओं के लिए उनकी परीक्षा की गयी है?	हाँ	हाँ	हाँ

298	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या उपयोगकर्ता प्रामाणीकरण के बिना प्रामाणीकरण से बच करके प्रणालियों तक प्रवेश करना संभव है? (लेखा परीक्षक विशेष रूप से यह पुष्टि करेगा कि उपयोगकर्ता सुरक्षा से बचकर नहीं निकल सकता)?	हाँ	हाँ	हाँ
299	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या अनुप्रयोग, सुरक्षित वीपीएन या वीडिआई प्रवेश के माध्यम से केवल प्राधिकृत उपयोगकर्ताओं के लिए सुगम है?	हाँ	हाँ	हाँ
300	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या उपयोगकर्ता कार्यक्षेत्र नीति सर्वर द्वारा प्रामाणीकृत और प्राधिकृत हैं?	हाँ	हाँ	हाँ
301	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या अनुप्रयोग सू.प्रौ. आधारभूत संरचना के लॉग 24X7 सुरक्षा परिचालन केंद्र (एसओसी) दल द्वारा संगृहीत और विश्लेषित हैं?	हाँ	हाँ	सहभाजित
302	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या, उपयोगकर्ताओं द्वारा अप्राधिकृत लॉग इन/लॉग आउट प्रवेश उल्लंघनों इत्यादि की समीक्षा करने के लिए आईटी लॉगों की निरंतर (लेखा परीक्षक सावधिक अन्तराल के संबंध में विशेष रूप से टिप्पणी करेगा) निगरानी, सुरक्षा सूचना और घटना निगरानी (एसआईईएम) की जाती है और सुरक्षा परिचालन केंद्र (एसओसी) द्वारा उस पर नजर रखी जाती है?	हाँ	हाँ	सहभाजित
303	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या, एसओसी दल द्वारा 24X7 आधार पर, उद्यम वार, सूचना सुरक्षा घटनाओं की निगरानी की जाती है?	हाँ	हाँ	सहभाजित
304	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या आईसीटी आधारभूत संरचना लॉगों को विनियामक दिशा-निर्देशों के अनुसार रखा जाता है?	हाँ	हाँ	हाँ
305	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या अनुमोदित सॉफ्टवेयर और उपयोग्यताओं के अधिष्ठापन को केन्द्रीय रूप से लागू नीति द्वारा बाधित किया जाता है?	हाँ	हाँ	हाँ
306	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या, उपयोगकर्ता केवल संस्था द्वारा अनुमोदित सहकार्यता सॉफ्टवेयर इस्तेमाल कर रहे हैं?	हाँ	हाँ	हाँ
307	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या फायरवेल/नेटवर्क सुरक्षा उपकरणों पर अप्राधिकृत सहयोग औजारों को बाधित करने के लिए कोई निरोधक नियंत्रण है?	हाँ	हाँ	हाँ
308	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या, साइबर सुरक्षा जागरूकता परिपत्र और परामर्श, कर्मचारियों, तृतीय पक्ष विक्रेता और परीमर्शदाताओं को नियमित रूप से भेजे जाते हैं।	हाँ	हाँ	हाँ
309	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या संस्था के पास डब्ल्यूएफआरएल के दौरान व्यवहार गतिविधियों पर निरीक्षण को संचालित करने के लिए कोई व्यवहार कक्ष नीति और मानक परिचालन नीति है?	हाँ	हाँ	हाँ



310	दूरस्थ स्थान से कार्य (डब्ल्यूएफआरएल)	क्या तृतीय पक्ष के साथ सभी प्रबंधन/दस्तावेज विशेष औजर का इस्तेमाल करते हुए डिजिटल तरीके से हस्ताक्षरित किये जाते हैं?	हाँ	हाँ	ऐच्छिक
311	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या रिकार्ड की गयी लाइने काम कर रही है और अच्छी हालत में रखी गयी हैं?	हाँ	हाँ	हाँ
312	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या, मध्यकार्यालय मानक परिचालन क्रियाविधि (एसओपी) में परिभाषित प्रक्रिया के अनुसार आवाज रिकार्डिंग की जाँच करता है?	हाँ	हाँ	हाँ
313	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या, ब्रोकरों को कॉल करने के लिए डब्ल्यूएफएच के दौरान कोई समर्पित और सुरक्षित रिकार्डिंग लाइन उपलब्ध करायी जाती है?	हाँ	हाँ	हाँ
314	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	कार्यालय स्थान से किये गये कॉलों की रिकार्डिंग के लिये वायस लॉगर का इस्तेमाल किया जाता है?	हाँ	हाँ	हाँ
315	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या, लेन-देन के प्रमाण के अंग के रूप में कॉल रिकार्डिंग के बैकअप/स्टोरेज को सक्रिय किया जाता है, जिन तक किसी भी समय पहुँचा जा सकता है?	हाँ	हाँ	हाँ
316	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या एसओपी डीलरों और दलालों के बीच संचार संपर्कों में अवरोध से निपटने के लिए प्रक्रिया परिभाषित करता है?	हाँ	हाँ	हाँ
317	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या ऐसे संचारों को लॉग /रिकार्ड किया जाता है?	हाँ	हाँ	हाँ
318	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या मध्यवर्ती कार्यालय इन लॉगों / रिकार्डों की स्वतंत्र रूप से समीक्षा करते हैं?	हाँ	हाँ	हाँ
319	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या ऐसे लेन-देनों की प्रक्रिया करने के लिए उपयुक्त पूर्व अनुमोदन / प्राधिकार प्राप्त किए गये हैं?	हाँ	हाँ	हाँ
320	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या डीलर एएलएल लेन-देन केवल रिकार्ड किये गये टेलीफोन लाइनों के माध्यम से किये जाते हैं?	हाँ	हाँ	हाँ
321	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या सभी केवल प्राधिकृत ब्लूमबर्ग टर्मिनल /ब्लूमबर्ग कहीं भी आईडी /एनडीएस टर्मिनल/टीआरईपीएस टर्मिनल/ई-मेल्स हैं और एसएमएस / चैट सुविधाओं के लिये पूरी तरह से निष्क्रिय किये गये हैं?	हाँ	हाँ	हाँ

322	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	पुष्टि करें कि ब्लूमबर्ग टर्मिनल बहुकारक (मल्टी फैक्टर) प्रामाणीकरण के माध्यम से प्रवेश योग्य हैं और एसएमएस / चैट सुविधाओं के लिये निष्क्रिय किये गये हैं?	हाँ	हाँ	हाँ
323	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	संचार संपर्क के विच्छेद की स्थिति में उपयुक्त अनुमोदनों के साथ लेन-देन प्रक्रिया करने निवेश कार्य के अधिकारियों का मार्गदर्शन करने के लिए क्या कोई परिभाषित नीतियाँ/प्रक्रियाएँ हैं?	हाँ	हाँ	हाँ
324	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	यह विशेष रूप से पुष्टि करें कि निवेश लेन-देन, अपेक्षित अनुमदनों सहित डीलिंग रूम कार्य प्रवाह / एसओपी के एक अंग के रूप में परिभाषित सभी अधिदेशों के साथ, निष्पादित किये जाते हैं?	हाँ	हाँ	हाँ
325	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या डीलर, केवल रिकार्ड की गयी टेलीफोन लाइनों या प्राधिकृत ब्लूमबर्ग टर्मिनल, ब्लूमबर्ग कहीं पर भी आईडी / एडीएस टर्मिनलों / एनडीएस टर्मिनलों/टीआरडीपीएस टर्मिनलों/ई-मेलों के माध्यम से सभी लेन-देन निष्पादित करते हैं?	हाँ	हाँ	हाँ
326	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	विशेष रूप से पुष्टि करें कि डीलर रिकार्ड किये गये लाइनों के अतिरिक्त केवल सूचीबद्ध दलालों के माध्यम से, केवल एसओपी/डीलिंग कक्ष नीति के अनुसार प्राधिकृत संचार माध्यमों से आर्डर देते हैं?	हाँ	हाँ	हाँ
327	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या प्रासंगिकता नीतियाँ और योजनाएँ, एक प्रभावी व्यापार निरंतरता के लिए आवधिक रूप संशोधित और परीक्षित किये जाते हैं?	हाँ	हाँ	हाँ
328	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या द्वितीयक नेटवर्क संयोजनकता और सू.प्रौ. आधारभूत संरचना का महत्वपूर्ण अनुप्रयोगों और सेवाओं के लिए प्रावधान किया गया है? किसी एसपीओएफएस-विफलता के एक बिन्दु (सिंगल पॉइंट ऑफ फ़ेल्युर) के लिए जाँच करें।	हाँ	हाँ	हाँ
329	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या, अनुप्रयोगों, प्रक्रियाओं और संसाधनों की दूरस्थ बैकअप स्थल पर उपलब्धता को परखने के लिये आपदा बहाली(डीआर) अभ्यास किये जाते हैं? क्या डीआर परीक्षण करने के दौरान समस्याओं का पता लगाया गया है?	द्वि-वार्षिक	द्वि-वार्षिक	वार्षिक
330	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या, सू.प्रौ. सहायता निवेश अनुप्रयोग उपयोगकर्ताओं द्वारा पोर्टल, हेल्पडेस्क के माध्यम से या कार्यालय पहुँच कर अभिगमित की जाती है?	हाँ	हाँ	हाँ
331	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या बैकअप/वैकल्पिक स्थान और संसाधन की पहचान, व्यापार निरंतरता सुनिश्चित करने के लिए, निवेश कार्य के भीतर की जाती है?	हाँ	हाँ	हाँ
332	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या, ई-मेल सुविधा सूचीबद्ध दलाल, काउण्टर पार्टियों, अभिरक्षक इत्यादि द्वारा सक्रिय की जाती है?	हाँ	हाँ	हाँ
333	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या, ई-मेल केवल प्राधिकृत कंपनी के माध्यम से संबंधित काउण्टर पार्टियों के साथ पंजीकृत ई-मेल पत्तों पर साझा की जाती है?	हाँ	हाँ	हाँ

334	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या आवाज रिकार्डिंग विश्लेषण और दूर स्कैन नियमित रूप से व्यापार और लेन-देन डीलिंग कक्ष नीति में यथा परिभाषित कीमत पर किया जाता है?	हाँ	हाँ	हाँ
335	दूरस्थ स्थान से कार्य-निवेश (डब्ल्यूएफआरएल.इन)	क्या, वहाँ कोई पर्यवेक्षी निगरानी प्रक्रिया चेक लिस्ट है, जिसमें लेन-देन कीमत निगरानी और व्यापार निगरानी इत्यादि शामिल है?	हाँ	हाँ	हाँ
336	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	क्या, मध्यवर्ती ने, अपने वेबसाइट, मोबाइल आधारित अनुप्रयोग या दोनों पर जैसी भी स्थिति हो, प्रमुख रूप से, किसी व्यक्ति द्वारा उसके कंप्यूटर संसाधन तक प्रवेश या इस्तेमाल के लिए नियम और विनियम, निजता नीति और उपयोगकर्ता करार प्रकाशित किया है?	हाँ	हाँ	हाँ
337	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	क्या, उसके कंप्यूटर संसाधन उपयोगकर्ता को, नियम और विनियम, निजी नीति या मध्यवर्ती के उपयोगकर्ता करार में यह सूचित किया गया है कि उस जानकारी की मेजबानी, प्रदर्शित, अपलोड, संशोधन, प्रकाशन संचरण एकर, अद्यतन या साझा न करें जो (i) किसी अन्य व्यक्ति से संबंधित है और जिस पर उपयोगकर्ता का कोई अधिकार नहीं है; (ii) अपमानसूचक, अश्लील, कामोद्दीपक, शारीरिक गोपनीयता सहित किसी अन्य की गोपनीयता-आक्रमण लिंग के आधार पर अपमानजनक या छेड़छाड़ करने वाला, निंदात्मक, नस्लीय या जातीय रूप से आपत्तिजनक, कालेधन या द्यूत-क्रीडा को वैध बनाने से संबंधित या प्रोत्साहित करने वाला या प्रचलित कानून से अन्यथा असंगत और विपरीत है; (iii) बच्चे के लिए हानिकारक है; (iv) किसी पेटेंट, ट्रेडमार्क, कॉपी राइट या अन्य मालिकाना अधिकारों का उल्लंघन है; (v) वर्तमान में लागू किसी कानून का उल्लंघन करता है; (vi) संदेश के उद्गम के संबंध में पत्र पाने वाले को धोखा देता है या जानबूझ कर या इरादतन ऐसी जानकारी देना जोकि साफ तौर पर असत्य या गुमराह करने की प्रकृति की है किन्तु यथोचित रूप से सत्य प्रतीत होती है; (vii) किसी अन्य व्यक्ति का प्रतिरूपण करना; (viii) भारत की एकता, अखंडता, रक्षा और सुरक्षा या सार्वभौमिकता विदेशी राज्यों से मैत्री संबंध, या सार्वजनिक व्यवस्था, को खतरे में डालना, किसी संज्ञेय अपराध के कृत्य को उकसाने का कारण बनता, या किसी अपराध की जाँच पड़ताल को रोकता या अन्य राष्ट्र के लिए अपमानजनक; (ix) जिसमें सॉफ्टवेयर वायरस, या कोई अन्य कोड, फाइल और या प्रोग्राम है जिसको किसी कम्प्यूटर संसाधन की कार्यक्षमता को अवरुद्ध, नष्ट या सीमित करने के लिए तैयार किया गया है; (x) पेटेंट रूप से गलत और असत्य है और किसी व्यक्ति को गुमराह करने या सताने, संस्था या एजेंसी को वित्तीय लाभ के लिए या किसी व्यक्ति को कोई चोट पहुँचाने के इरादे से लिखा या किसी रूप में प्रकाशित किया गया है;	हाँ	हाँ	हाँ
338	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	क्या, मध्यवर्ती ने आवधिक रूप से उपयोगकर्ता को वर्ष में कम से कम एक बार सूचित किया है कि नियमों और विनियमों, गोपनीयता नीति या प्रवेश के लिए उपयोगकर्ता या ऐसे मध्यवर्ती के कम्प्यूटर संसाधन के इस्तेमाल के लिए उपयोगकर्ता करार का अनुपालन करने की स्थिति में उसको यह अधिकार है कि कम्प्यूटर संसाधन के प्रवेश या इस्तेमाल के उपयोगकर्ता के अधिकारों को तुरंत समाप्त करे या अनुपालन सूचना को हटा दे या दोनों जैसी भी स्थिति हो	हाँ	हाँ	हाँ
339	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	क्या, मध्यवर्ती ने, जिसके कंप्यूटर संसाधन पर जानकारी संग्रहित की जाती है, प्रकाशित सक्षम क्षेत्राधिकार के न्यायालय द्वारा किसी आदेश के रूप में वास्तविक सूचना प्राप्त होने पर या उपयुक्त सरकार या उसकी एजेंसी द्वारा अधिनियम की धारा 79 की उपधारा(3) के खंड(ख) के अंतर्गत अधिसूचित होने पर कि ऐसी कोई गैर-कानूनी सूचना प्रकाशित न करें जो वर्तमान में लागू किसी कानून के अंतर्गत प्रतिबंधित है, जो भारत की सार्वभौमिकता और अखंडता के हित के संबंध में राज्य की सुरक्षा, विदेशी राष्ट्रों के साथ मैत्रीपूर्ण संबंधों, सार्वजनिक व्यवस्था, शालीनता और नैतिकता, न्यायालय की अवमानना के संबंध में, मानहानि, उपरोक्त से संबंधित किसी अपराध के लिए उकसाना, या कोई जानकारी जो वर्तमान में लागू किसी कानून के अंतर्गत प्रतिबंधित है; हॉस्ट या प्रकाशित की है?	हाँ	हाँ	हाँ
340	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	क्या मध्यवर्ती ने, आवधिक रूप से और एक वर्ष में कम से कम एक बार, उपयोगकर्ता को अपने नियम और विनियम, गोपनीयता नीति या उपयोगकर्ता करार या नियमों और विनियमों, गोपनीयता नीति या उपयोगकर्ता करार, में बदलाव जैसी भी स्थिति है, के बारे में सूचित किया है?	हाँ	हाँ	हाँ

341	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	यदि मध्यवर्ती ने उपयोगकर्ता से कंप्यूटर संसाधन पर पंजीकरण के लिए जानकारी एकत्र की है, क्या उसने, उसके पंजीकृत रद्दीकरण या वापसी के बाद, जैसी भी स्थिति है, एक सौ अस्सी दिनों के लिए उसकी जानकारी संभाल कर रखी है;	हाँ	हाँ	हाँ
342	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	क्या मध्यवर्ती ने, सूचना प्रौद्योगिकी (उचित सुरक्षा अभ्यास और क्रियाविधियाँ और संवेदनशील व्यक्तिगत जानकारी) नियम, 2011 में निर्धारित उचित सुरक्षा अभ्यासों और क्रियाविधियों का पालन करते हुए, अपने कंप्यूटर प्राप्त करने के लिए सभी उचित उपाय किये हैं	हाँ	हाँ	हाँ
343	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	क्या मध्यवर्ती, आदेश के प्राप्त होने पर यथासंभव शीघ्र किन्तु 72 घंटे के भीतर, वह जानकारी, जो उसके नियंत्रण या अधिकार में है, उपलब्ध कराता है या सरकारी एजेंसी को सहायता उपलब्ध कराता है, जो अपराधों की पहचान की जाँच या रोकथाम, सुरागसानी, जाँच-पड़ताल या अभियोजना के उद्देश्यों से उस समय लागू किसी कानून के अंतर्गत या साइबर सुरक्षा घटनाओं की तहकीकात संबंधी या रक्षात्मक या साइबर सुरक्षा गतिविधियों के लिए कानूनी रूप से प्राधिकृत है;	हाँ	हाँ	हाँ
344	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	क्या मध्यवर्ती ने साइबर सुरक्षा घटनाओं की रिपोर्ट की है और संबंधित जानकारी, सूचना प्रौद्योगिकी (भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल और कार्य और कर्तव्य पूरा करने की प्रणाली) नियम 2013, में उल्लिखित नीतियों और क्रिया विधि के अनुसार भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल के साथ साझा की है।	हाँ	हाँ	हाँ
345	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	क्या मध्यवर्ती को मालूम है कि वह कंप्यूटर संसाधन के तकनीकी विन्यास को जानबूझ कर प्रसारित या स्थापित या संशोधित नहीं करेगा या ऐसे किसी कृत्य का भागीदार नहीं बनेगा जो कंप्यूटर संसाधन के परिचालन की सामान्य प्रक्रिया को बदल सकता है या बदलने की क्षमता रखता है, जिससे वर्तमान में लागू किसी कानून की प्रवचना होती है, बजाय इसके कि उसको क्या करना है?	हाँ	हाँ	हाँ
346	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	क्या मध्यवर्ती ने, अपने वेबसाइट, मोबाइल आधारित अनुप्रयोग या दोनों पर जैसी भी स्थिति है, शिकायत अधिकारी का नाम और उसके संपर्क विवरण, साथ ही साथ प्रक्रिया, जिसके द्वारा उपयोगकर्ता या कोई पीडित इस नियम के प्रावधानों के उल्लंघन या इसके द्वारा उपलब्ध कराये गये कंप्यूटर संसाधन से संबंधित किसी अन्य मामले के विरुद्ध, शिकायत कर सकता है, प्रमुख रूप से अपने वेबसाइट पर प्रकाशित की है और शिकायत अधिकारी; (i) शिकायत की प्राप्ति के चौबीस घंटों के भीतर शिकायत प्राप्ति की सूचना देगा और ऐसी शिकायत का उसकी प्राप्ति की तिथि से पंद्रह दिन की अवधि के भीतर निपटान करेगा, (ii) उपयुक्त सरकार किसी सक्षम प्राधिकारी या सक्षम अधिकार क्षेत्र के न्यायालय द्वारा जारी कोई आदेश, नोटिस या निर्देश प्राप्त करेगा और प्राप्ति सूचना देगा।	हाँ	हाँ	हाँ
347	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	क्या मध्यवर्ती ने, किसी व्यक्ति या व्यक्ति द्वारा अपनी ओर से, इस उप-नियम के अंतर्गत, किसी अन्तर्वस्तु, जो कि प्रथम दृष्टया किसी ऐसी सामग्री की प्रकृति की है जो ऐसे व्यक्ति के निजी क्षेत्र को उजागर करता है, ऐसे व्यक्ति को पूर्ण या आंशिक नग्नता में दर्शाता है या ऐसे व्यक्ति को किसी लैंगिक कृत्य या आचरण में दर्शाता या चित्रित करता है या इलेक्ट्रॉनिक रूप से छदम रूपण प्रकृति में है, ऐसे व्यक्ति की कृत्रिम रूप से रूपांतरित छवियों सहित, के संबंध में की गयी किसी शिकायत की प्राप्ति के चौबीस घंटों के भीतर ऐसी सामग्री, जो कि उसके द्वारा दिखायी, संग्रहित प्रकाशित या प्रसारित की गयी है, को हटाने के लिए सभी तर्कसंगत और व्यवहार्य उपाय किए हैं?	हाँ	हाँ	हाँ
348	सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 (आईजीडीएम)	क्या मध्यवर्ती ने, इस उप-नियम की धारा (बी) के अंतर्गत जो किसी एक व्यक्ति या व्यक्ति को विवरण उपलब्ध कराने के योग्य बनाता है, ऐसी अन्तर्वस्तु या संचार संपर्क के संबंध में आवश्यक हो सकता है, शिकायत प्राप्त करने के लिए क्रियाविधि कोई लागू की है?	हाँ	हाँ	हाँ

			Regulated Entities / Intermediaries		
Control No.	Area	Audit Questionnaire	Cat-1	Cat-2	Cat-3
			Gross Insurance Revenue: > = 50 Crs (All Insurance Intermediaries using ISNP and Web Aggregators will fall under this category)	Gross Insurance Revenue: > = 5 Cr and < 50 Cr	Gross Insurance Revenue: < 5 Crs
1	Anomalies and Events (DE.AE):	Does the organization have a clearly defined policy including requirements justifying the exceptions, duration of exceptions, process of granting exceptions, and authority for approving, authority for review of exceptions granted on a periodic basis by officer(s) preferably at senior levels who are well equipped to understand the business and technical context of the exception(s) ?	Board Approved	MD Approval	MD Approval
2	Security Continuous Monitoring & Detection (DE.CM):	Are the security logs maintained and monitored?	Yes	Yes	Yes
3	Security Continuous Monitoring & Detection (DE.CM):	Are there any procedure to monitor capacity utilization of critical systems and networks ?	Yes	Yes	Yes
4	Security Continuous Monitoring & Detection (DE.CM):	Are there mechanism to dynamically incorporate lessons learnt to continually improve the response strategies?	Yes	Yes	Yes
5	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Alert when users deviate from normal login behaviour, such as time-of-day, workstation location and duration.	Yes	Yes	Limited
6	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	Yes	Yes	Yes
7	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Yes	Yes	Yes
8	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.	Yes	Yes	Yes
9	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Associate active ports, services and protocols to the hardware assets in the asset inventory.	Yes	Yes	Yes
10	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Automatically disable dormant accounts after a set period of inactivity.	Yes	Yes	Yes
11	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Automatically lock workstation sessions after a standard period of inactivity.	Yes	Yes	Yes
12	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Block all e-mail attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.	Yes	Yes	Yes
13	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.	Yes (atleast half yearly)	Annual	Annual
14	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	Yes	Yes	Yes
15	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure devices to not auto-run content from removable media.	Yes	Yes	Yes
16	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	Yes	Yes	Yes
17	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	Yes	Yes	Optional
18	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.	Yes	Yes	Yes
19	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.	Yes	Yes	Yes
20	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	Yes	Optional	Optional
21	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Decrypt all encrypted network traffic at the boundary proxy prior to analysing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	Yes	Yes	Optional
22	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Deliver training to address the skills gap identified to positively impact workforce members' security behaviour.	Yes	Yes	Yes
23	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.	Yes	Yes	Yes
24	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	Yes	Yes	Limited
25	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighbouring systems, through technologies such as Private VLANs or micro segmentation.	Yes	Yes	Yes
26	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable any account that cannot be associated with a business process or business owner.	Yes	Yes	Yes
27	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable wireless access on devices that do not have a business purpose for wireless access.	Yes	Yes	Yes
28	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.	Yes	Yes	Yes
29	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Encrypt sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	Yes	Yes	Yes
30	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Encrypt all sensitive information in transit.	Yes	Yes	Optional
31	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	Yes	Yes	Yes

32	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	Yes	Yes	Yes
33	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that all accounts have an expiration date that is monitored and enforced.	Yes	Yes	Yes
34	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.	Yes	Yes	Yes
35	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	Yes	Yes	Shared
36	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that only authorized scripting languages are able to run in all web browsers and email clients.	Yes	Yes	Yes
37	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	Yes	Yes	Yes
38	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.	Yes	Yes	Annual
39	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	Yes	Yes	Yes
40	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.	Yes	Yes	Limited
41	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Establish secure coding practices appropriate to the programming language and development environment being used.	Yes	Yes	Yes
42	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	Yes	Yes	Yes
43	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	Yes	Yes	Yes
44	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation If USB storage devices are required, ensure all data stored on such devices must be encrypted while at rest.	Yes	Yes	Sensitive Data
45	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.	Yes	Yes	Yes
46	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	Yes	Yes	Yes
47	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	Yes	Yes	Limited
48	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.	Yes	Yes	Yes
49	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain an inventory of authorized wireless access points connected to the wired network.	Yes	Yes	Yes
50	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.	Yes	Yes	Yes
51	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.	Yes	Yes	Yes
52	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Manage all network devices using multi-factor authentication and encrypted sessions.	Yes	Yes	Limited
53	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	Yes	Yes	Seperated VLANs
54	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Monitor attempts to access deactivated accounts through audit logging.	Yes	Yes	Yes
55	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation On a regular basis, review logs to identify anomalies or abnormal events.	Yes	Yes	Yes
56	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation On a regular basis, tune SIEM system to better identify actionable events and decrease event noise.	Yes	Yes	Optional
57	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Only use up-to-date and trusted third-party components for the software developed by the organization.	Yes	Yes	Yes
58	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Perform a skills gap analysis to understand the skills and behaviours workforce members are not adhering to, using this information to build a baseline education roadmap.	Yes	Yes	Once in 2 years
59	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	Yes	Yes	Optional
60	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	Yes	Yes	Limited



61	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Plan and conduct routine incident, response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.	Yes	Yes	Annual
62	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	Yes	Yes	Limited
63	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	Yes	Yes	Yes
64	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication (MFA).	Yes	Yes	MFA
65	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.	Yes	Yes	Yes
66	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).	Yes	Yes	Yes
67	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.	Yes	Yes	Optional
68	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail(DKIM) standards.	Yes	Yes	Yes
69	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.	Yes	Yes	Yes
70	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Train workforce members on the importance of enabling and utilizing secure authentication.	Yes	Yes	Yes
71	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	Yes	Yes	Yes
72	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.	Yes	Yes	Yes
73	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	Yes	Yes	Yes
74	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.	Yes	Yes	Limited
75	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.	Yes	Limited	Optional
76	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use DNS filtering services to help block access to known malicious domains.	Yes	Yes	Yes
77	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use only standardized and extensively reviewed encryption algorithms.	Yes	Yes	Yes
78	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use sandboxing to analyse and block inbound email attachments with malicious behaviour.	Yes	Yes	Optional
79	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	Yes	Yes	Yes
80	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.	Yes	Optional	Optional
81	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	Yes	Optional	Optional
82	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.	Yes	Yes	Yes
83	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.	Yes	Yes	Optional
84	Security Continuous Monitoring & Detection (DE.CM):	Has the organization defined and set a procedure to implement a Security Operations Centre for centralised and coordinated monitoring and management of security related incident?	Yes	Yes	Shared
85	Security Continuous Monitoring & Detection (DE.CM):	Has the organization defined incidents, method of detection, methods of reporting incidents by employees, vendors and customers and periodicity of monitoring, collection/sharing of threat information, expected response in each scenario/incident type, allocate and communicate clear roles and responsibilities of personnel manning/handling such incidents, provide specialised training to such personnel, post incident review, periodically test incident response plans?	Yes	Yes	Yes
86	Security Continuous Monitoring & Detection (DE.CM):	Has the organization implemented measures to control use of VBA/macros in MS office documents, control permissible attachment types in email systems?	Yes	Yes	Yes
87	Security Continuous Monitoring & Detection (DE.CM):	Has the organization implemented mechanism to automatically identify unauthorised device connections to the organization's network and block such connections?	Yes	Yes	Yes
88	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation conduct periodic tests for all the critical application, server, network devices and data bases?	Yes	Yes	Annual
89	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation implement a process to communicate vulnerabilities to vendors?	Yes	Yes	Yes
90	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation maintain tracker for closure and corrective action of VAPT?	Yes	Yes	Yes

91	Security Continuous Monitoring & Detection (DE.CM):	Whether a policy to ensure high availability and timely detection of attacks is defined and implemented ?	Yes	Yes	Yes
92	Security Continuous Monitoring & Detection (DE.CM):	Whether vulnerability assessment and penetration testing procedure and calendar are defined ?	Yes	Yes	Yes
93	Security Continuous Monitoring & Detection (DE.CM):	Is VAPT of internet-facing applications or infrastructure components conducted periodically	Yes	Yes	Annual
94	Security Continuous Monitoring & Detection (DE.CM):	Does Business applications including APIs or Web Services etc. undergo VAPT Testing including secure code review periodically & before go live.	Yes	Yes	Yes
95	Security Continuous Monitoring & Detection (DE.CM):	Is mandatory security testing conducted for all changes to internet facing information assets or systems and reported gaps closed before moving into production.	Yes	Yes	Major Changes
96	Security Continuous Monitoring & Detection (DE.CM):	Is External Blackbox Penetration Testing (PT) conducted for all internet facing information assets or systems once in a 6 months.	Yes	Yes	Annual
97	Security Continuous Monitoring & Detection (DE.CM):	Are High risk gaps, reported from the VAPT closed within the time period prescribed under guidelines followed by validation test.	Yes	Yes	Yes
98	Security Continuous Monitoring & Detection (DE.CM):	Are audit gaps reported in VAPT closed within the timeframe provided in the guidelines.	Yes	Yes	Yes
99	Security Continuous Monitoring & Detection (DE.CM):	Is the organizations information assets synchronized with a singular time source?	Yes	Yes	Yes
100	Detection Processes (DE.DP):	Are roles and responsibilities for detection well defined to ensure accountability?	Yes	Yes	Yes
101	Detection Processes (DE.DP):	Do detection activities comply with all applicable requirements?	Yes	Yes	Yes
102	Detection Processes (DE.DP):	Has the organization put in place processes/mechanism to identify authorised hardware / mobile devices like Laptops, mobile phones, tablets, etc. and ensure that they are provided connectivity only when they meet the security requirements prescribed by the organization?	Yes	Yes	Yes
103	Asset Management (ID.AM)	Does the Organisation use client certificates/server to authenticate hardware assets connecting to the organization's trusted network?	Yes	Yes	Yes
104	Asset Management (ID.AM)	Does the organisation Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network? The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	Yes	Yes	Limited
105	Asset Management (ID.AM)	Does the organization identify critical assets based on their sensitivity?	Yes	Yes	Yes
106	Asset Management (ID.AM)	Does the organization maintain an up-to-date inventory of its hardware, software, information assets, details of network resources and also maintain records of those personnel who are issued such assets?	Yes	Yes	Yes
107	Asset Management (ID.AM)	Has organization maintained an up-to-date centralised inventory of authorised software/applications/libraries, etc. ?	Yes	Yes	Yes
108	Asset Management (ID.AM)	Has the organization managed and protected data/information asset considering how the data/information are stored, transmitted, processed, accessed and put to use within/outside the organization's network, and level of risk they are exposed to depending on the sensitivity of the data/information?	Yes	Yes	Yes
109	Asset Management (ID.AM)	Has the organization put in place appropriate environmental controls for securing location of critical assets providing protection from natural threats?	Yes	Yes	Yes
110	Asset Management (ID.AM)	Has the organization put in place mechanism for monitoring any potential compromises or breach to environmental controls?	Yes	Yes	Yes
111	Asset Management (ID.AM)	Is it ensured that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner?	Yes	Yes	Yes
112	Business Environment (ID.BE)	Are Priorities for organizational mission, objectives, and activities w.r.t cybersecurity roles, responsibilities, and risk management decisions established and communicated?	Yes	Yes	Yes
113	Business Environment (ID.BE)	Are Resilience requirements to support delivery of critical services are established for all operating states? (e.g. under duress/attack, during recovery, normal operations)	Yes	Yes	Yes
114	Business Environment (ID.BE)	Has the organization established Standard Operating Procedures (SOP) for all major IT activities including for connecting devices to the network environment of the organization?	Yes	Yes	Yes
115	Business Environment (ID.BE)	Has the organization maintained up-to-date network architecture diagram at the organization level including wired/wireless networks?	Yes	Yes	Yes
116	Governance (ID.GV)	Is official designated to assume overall responsibility for governance and monitoring of Information Security	Designated CISO	Designated / Virtual CISO	Designated / Virtual CISO
117	Governance (ID.GV)	Does the organization form an IS RMC which shall be responsible to ensure that the policy remains updated at all times?	IS RMC	IT, Legal, HR, Risk, Business Ops	IT, Legal, HR, Business Ops
118	Governance (ID.GV)	Is the annual audit plan and the reports presented to the Audit Committee of the Board of the organization?	Yes	Yes	MD
119	Governance (ID.GV)	Does Cyber Security Policy include process of recovering from incidents through incident management & other appropriate recovery mechanisms?	Yes	Yes	Yes
120	Governance (ID.GV)	Does Cyber Security Policy include process on detecting incidents, anomalies and attacks via appropriate monitoring tools/process?	Yes	Yes	Yes
121	Governance (ID.GV)	Does Cyber Security Policy include process on protecting assets by deploying suitable controls, tools & measures?	Yes	Yes	Yes
122	Governance (ID.GV)	Does Cyber Security Policy include process on responding after identification of the incident, anomaly or attack?	Yes		Yes
123	Governance (ID.GV)	Does the organization implement any operation/process/monetary transactions through API follow best practices from international standards like ISO 27001, COBIT 5, etc? Are such practices periodically reviewed?	Yes	Yes	Yes
124	Governance (ID.GV)	Are cybersecurity roles and responsibilities coordinated and aligned with internal roles and external partners?	Yes	Yes	Yes



125	Governance (ID.GV)	Is there a Cyber Crisis Management Plan (CCMP) available? Are Cert-In / NCIIPC guidelines used for preparing Cyber Crisis Management Plan?	Yes	Yes	Yes
126	Governance (ID.GV)	Is there a SOC setup available which ensures continuous surveillance ?	Yes	Yes	Limited/Shared
127	Governance (ID.GV)	Are the reporting procedures being taken to facilitate communication of unusual activities with designated Cyber Security officer ?	Yes	Yes	Yes
128	Governance (ID.GV)	Whether a comprehensive Cyber Security Policy is in place ?	Yes	Yes	Yes
129	Governance (ID.GV)	Whether a cyber risk management policy is available ?	Yes	Yes	Yes
130	Governance (ID.GV)	Whether Business Continuity Plan and Disaster Recovery Plan is in place ?	Yes	Yes	Core Systems
131	Governance (ID.GV)	Whether IT architecture has been reviewed by the IT Sub Committee of the board ?	Yes	MD	MD
132	Governance (ID.GV)	Whether the Board of the organization formed an internal technology committee of experts? Does the committee periodically review implementation of the Cyber Security policy ?	Yes	MD	MD
133	Governance (ID.GV)	For Cloud and Mobile deployment has the organisation considered the best practices relating to Cloud, Mobile Security and related areas?	Yes	Yes	Yes
134	Governance (ID.GV)	Is the commitment of Senior Management ensured?	Yes	Yes	Yes
135	Risk Assessment (ID.RA)	Does the organization identify potential cyber risks (threats and vulnerabilities) along with the likelihood of such threats and impact on the business and deploy controls accordingly to suppress the criticality?	Yes	Yes	Yes
136	Risk Assessment (ID.RA)	Does the organization periodically assess whether all the network devices are configured appropriately to the desired level of network security?	Yes	Yes	Yes
137	Risk Assessment (ID.RA)	Are risk responses identified and prioritized?	Yes	Yes	Yes
138	Risk Assessment (ID.RA)	Are threats from both internal and external parties identified and documented?	Yes	Yes	Yes
139	Risk Management (ID.RM)	Are Risk management processes established, managed, and agreed to by organizational stakeholders?	Yes	Yes	Yes
140	Risk Management (ID.RM)	Is Organizational risk tolerance is determined and clearly expressed?	Yes	Yes	Yes
141	Supply Chain Risk Management (ID.SC)	Does vendors adhere to the applicable guidelines provided in the Cyber Security policy? Does the organization obtains the necessary self-certifications from them to ensure compliance with the policy provisions?	Yes	Yes	Yes
142	Supply Chain Risk Management (ID.SC)	Has the vendors implemented appropriate information security controls and cybersecurity framework?	Yes	Yes	Yes
143	Supply Chain Risk Management (ID.SC)	Vendors agreement documents are maintained and updated ?	Yes	Yes	Yes
144	Supply Chain Risk Management (ID.SC)	Are there process for monitoring third - party access to protected or sensitive information?	Yes	Yes	Yes
145	Identity Management, Authentication and Access Control (PR.AC):	Are ICT infrastructure logs maintained for a rolling period of 180 days as per CERT-In directions?	Yes	Yes	Yes
146	Identity Management, Authentication and Access Control (PR.AC):	Are ICT infrastructure logs, Critical and Business data stored in India?	Yes	Yes	Yes
147	Identity Management, Authentication and Access Control (PR.AC):	Are third-party staff who are given access to the organization's critical systems, networks, and other computer resources subjected to strict supervision, monitoring, and access restrictions?	Yes	Yes	Yes
148	Identity Management, Authentication and Access Control (PR.AC):	Do all critical systems of the organization that is accessible over the internet have two-factor security (Such as VPNs, Firewall Controls, etc.)?	Yes	Yes	Yes
149	Identity Management, Authentication and Access Control (PR.AC):	Does the access control policy address strong password management control for access to systems, applications, networks and databases?	Yes	Yes	Yes
150	Identity Management, Authentication and Access Control (PR.AC):	Does the organization proactively deactivate access of privileges of users who are leaving the organization or whose access privileges have been withdrawn?	Yes	Yes	Yes
151	Identity Management, Authentication and Access Control (PR.AC):	Has the organization deployed security measures and controls to supervise staff with elevated access entitlements (Such as privileged users) to organization's critical systems? Has the organization also restricted the no. of privileged user to the least number and deployed periodic review mechanism/process against privileged users' activities? Are such privileged users restricted of access to system logs where their activities are being captured?	Yes	Yes	Yes
152	Identity Management, Authentication and Access Control (PR.AC):	Has the organization ensured that no personnel in the company have natural rights to access confidential data, applications, system resources or facilities by virtue of rank or position?	Yes	Yes	Yes
153	Identity Management, Authentication and Access Control (PR.AC):	Has the organization ensured that the perimeter of the critical equipment's room/area are physically secured and continuously monitored by employing physical, human, and procedural controls such as security guards, CCTVs, Card access systems, mantrap, bollards, etc?	Yes	Yes	Yes
154	Identity Management, Authentication and Access Control (PR.AC):	Has the organization formulated an internet access policy to monitor and regulate the use of internet & internet based services such as social media sites, cloud-based storage sites, etc. within the organization's critical IT infrastructure?	Yes	Yes	Yes

155	Identity Management, Authentication and Access Control (PR.AC):	Has the organization implemented access to IT systems, applications, databases and networks on a need-to-use basis and the principle of least privilege? Is the access granted using strong authentication mechanisms and only when it is required ?	Yes	Yes	Yes
156	Identity Management, Authentication and Access Control (PR.AC):	Has the organization implemented controls for providing identification and authentication of customers for access to partner systems using secure authentication technologies?	Yes	Yes	Yes
157	Identity Management, Authentication and Access Control (PR.AC):	Has the organization implemented controls to minimize invalid login counts, deactivate dormant accounts?	Yes	Yes	Yes
158	Identity Management, Authentication and Access Control (PR.AC):	Is physical access to the critical systems of the organization restricted to the minimum number of authorized officials? Are third party staffs strictly monitored and physically accompanied all the time by the authorized employee of the organization while third party staff has been given physical access to critical systems ?	Yes	Yes	Yes
159	Identity Management, Authentication and Access Control (PR.AC):	Is physical access to the critical systems of the organization revoked immediately if the same is no longer required?	Yes	Yes	Yes
160	Awareness and Training (PR.AT):	Are the history and versions of training content maintained?	Yes	Yes	Yes
161	Awareness and Training (PR.AT):	Are the targeted awareness/training for key personnel conducted periodically?	Yes	Annual	Annual
162	Awareness and Training (PR.AT):	Are the training programs reviewed and updated periodically?	Yes	Annual	Annual
163	Awareness and Training (PR.AT):	Are security policy/ies covering secure and acceptable use of network/assets including customer information/data defined and communicated to users/employees, vendors & partners , and also educating them about cybersecurity risks and protection measures at their level.	Yes	Yes	Yes
164	Awareness and Training (PR.AT):	Do users indicate that they understand their responsibilities?	Yes	Yes	Yes
165	Awareness and Training (PR.AT):	Is awareness level evaluated periodically?	Yes	Annual	Once in 2 years
166	Awareness and Training (PR.AT):	Is there additional training for leaders to understand their roles in the event of a security incident?	Yes	Yes	Yes
167	Awareness and Training (PR.AT):	Is there a process to handle if a-user does not complete the training?	Yes	Yes	Yes
168	Awareness and Training (PR.AT):	Is someone responsible for creating the security training for the organization?	Yes	Yes	Yes
169	Awareness and Training (PR.AT):	Has the Organization periodically participated in national/ sectoral/ organisational Cyber Security Exercises?	Yes	Yes	Yes
170	Data Security (PR.DS):	Are open ports on network and systems which are not in use blocked ?	Yes	Yes	Yes
171	Data Security (PR.DS):	Can the application be set to automatically log a user off the application after a predefined period of inactivity?	Yes	Yes	Yes
172	Data Security (PR.DS):	Can the application force password expiration and prevent users from reusing a password?	Yes	Yes	Yes
173	Data Security (PR.DS):	Can the system administrator enforce password policy and/or complexity such as minimum length, numbers and alphabet requirements, and upper and lower case constraint, etc.?	Yes	Yes	Yes
174	Data Security (PR.DS):	Does the application force "new" users to change their password upon first login into the application?	Yes	Yes	Yes
175	Data Security (PR.DS):	Does the application prohibit users from logging into the application on more than one workstation at the same time with the same user ID?	Yes	Yes	Yes
176	Data Security (PR.DS):	Does the application support integration with the enterprise identity management system?	Yes	Yes	Yes
177	Data Security (PR.DS):	Does the organization authorize data storage devices within their IT infrastructure through appropriate validation process?	Yes	Yes	Yes
178	Data Security (PR.DS):	Is there a process by which the organization maintains the evidence of media disposal?	Yes	Yes	Yes
179	Data Security (PR.DS):	has there been a implementation of a data-disposal and data-retention policy?	Yes	Yes	Yes
180	Data Security (PR.DS):	Are there processes for media formatting?	Yes	Yes	Yes
181	Data Security (PR.DS):	Is there measurement a client system's vulnerabilities?	Yes	Optional	Optional

182	Data Security (PR.DS):	Is user authentication controlled by means other than user account and password or PIN?	Yes	Yes	Yes
183	Data Security (PR.DS):	Are various security mechanism used to share the data with third parties?	Yes	Yes	Yes
184	Data Security (PR.DS):	are the different technologies implemented for the encryption of data?	Yes	Yes	Limited
185	Data Security (PR.DS):	Are appropriate technologies implemented for data mobility security?	Yes	Yes	Optional
186	Information Protection Processes and Procedures (PR.IP):	Are duplicate copies of PC software and documentation maintained off-location?	Yes	Yes	Yes
187	Information Protection Processes and Procedures (PR.IP):	Are Physically or logically segregated systems used to isolate and run software that is required for business operations but incur higher risk for the organization.	Yes	Yes	Yes
188	Information Protection Processes and Procedures (PR.IP):	Are the contents of the Web site backed-up to ensure an orderly recovery if the site is corrupted?	Yes	Yes	Yes
189	Information Protection Processes and Procedures (PR.IP):	Are there methods to prevent unauthorized access by other groups into individual files and department-shared files?	Yes	Yes	Yes
190	Information Protection Processes and Procedures (PR.IP):	Are there procedures for limiting access to LAN and network operating software?	Yes	Yes	Yes
191	Information Protection Processes and Procedures (PR.IP):	Are updates to the Web site independently reviewed, approved and tested?	Yes	Yes	Yes
192	Information Protection Processes and Procedures (PR.IP):	Does information security policy cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data?	Yes	Yes	Yes
193	Information Protection Processes and Procedures (PR.IP):	Does the organisation utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.?	Yes	Yes	Yes
194	Information Protection Processes and Procedures (PR.IP):	Does the organisation utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	Yes	Yes	Limited
195	Information Protection Processes and Procedures (PR.IP):	Does the organization have a documented disaster recovery plan for processing critical jobs in the event of a major hardware or software failure?	Yes	Yes	Yes
196	Information Protection Processes and Procedures (PR.IP):	Does the organization's application whitelisting software ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.	Yes	Yes	Yes
197	Information Protection Processes and Procedures (PR.IP):	Does the organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system.	Yes	Yes	Yes
198	Information Protection Processes and Procedures (PR.IP):	Is a periodic inventory taken to verify that the appropriate backup files are being maintained?	Yes	Yes	Yes
199	Information Protection Processes and Procedures (PR.IP):	Is appropriate hardware backup available?	Yes	Yes	Yes
200	Information Protection Processes and Procedures (PR.IP):	Is it ensured that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory? Unsupported software should be tagged as unsupported in the inventory system.	Yes	Yes	Yes
201	Information Protection Processes and Procedures (PR.IP):	Is it ensured that the software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location?	Yes	Yes	Yes
202	Information Protection Processes and Procedures (PR.IP):	Is the use of remote access software restricted?	Yes	Yes	Yes
203	Information Protection Processes and Procedures (PR.IP):	Is there documentation describing data, programs, hardware, and system requirements?	Yes	Yes	Yes
204	Information Protection Processes and Procedures (PR.IP):	Are policies and procedures being used to protect critical information at different layers of security?	Yes	Yes	Yes
205	Maintenance (PR.MA):	Is there a process to determine after how many days of identification, patches would be fixed?	Yes	Yes	Yes
206	Maintenance (PR.MA):	Are remote maintenance of organizational assets approved, logged, and performed in a manner that prevents unauthorized access?	Yes	Yes	Yes
207	Maintenance (PR.MA):	Are Defined parameters taken for prioritizing the patches need to be installed?	Yes	Yes	Yes

208	Maintenance (PR.MA):	Are maintenance and repair of organizational assets logged whenever performed, with approved and controlled tools?	Yes	Yes	Yes
209	Maintenance (PR.MA):	Is there a process to deploy critical patches in a test environment?	Yes	Yes	Yes
210	Maintenance (PR.MA):	Are the approved patch management policy have been implemented?	Yes	Yes	Yes
211	Maintenance (PR.MA):	Have perimeters been defined for classifying patches?	Yes	Yes	Yes
212	Protective Technology (PR.PT):	Are adequate measures taken to isolate and secure the perimeter and connectivity of the servers running monetary transactions applications/process?	Yes	Yes	Yes
213	Protective Technology (PR.PT):	Does the organization Continuously monitor the release of patches by various vendors / OEMs, advisories issued by CERT-in and other similar agencies and expeditiously apply the security patches as per the patch management policy?	Yes	Yes	Yes
214	Protective Technology (PR.PT):	Has the organization deployed controls like host / network / application based IDS systems, customized kernels for Linux, anti-virus and anti-malware software etc., to prevent from virus / malware / ransomware attacks?	Yes	Yes	Yes
215	Protective Technology (PR.PT):	Has the organization documented and implemented secure mail and messaging systems, including those used by organization's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.?	Yes	Yes	Yes
216	Protective Technology (PR.PT):	Has the organization established baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment? Are LAN and wireless networks secured within organizations premises by deploying proper controls?	Yes	Yes	Yes
217	Protective Technology (PR.PT):	Has the organization implemented mechanism to control installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. and mechanism to block /prevent and identify installation and running of unauthorised software/applications on such devices/systems?	Yes	Yes	Yes
218	Protective Technology (PR.PT):	Has the organization installed network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources?	Yes	Yes	Yes
219	Communications (RC.CO):	Are recovery activities communicated to internal and external stakeholders as well as executive and management team?	Yes	Yes	Yes
220	Improvements (RC.IM):	Are recovery strategies updated periodically?	Yes	Yes	Yes
221	Improvements (RC.IM):	Does recovery plans incorporate lessons learned?	Yes	Yes	Yes
222	Recovery Planning (RC.RP):	Is recovery plan executed during or after a cybersecurity incident?	Yes	Yes	Yes
223	Analysis (RS.AN)	Are processes established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources? (e.g. internal testing, security bulletins, or security researchers)	Yes	Yes	Yes
224	Analysis (RS.AN)	Does the organisation have a process to ensure that impact of an incident analysed?	Yes	Yes	Yes
225	Analysis (RS.AN)	Does the organisation have a process to ensure that Notifications from detection systems are investigated ?	Yes	Yes	Yes
226	Analysis (RS.AN)	Does the organisation have a process to ensure that forensics are performed?	Yes	Yes	Yes
227	Communications (RS.CO):	Are all the cyber attacks related incidents captured and logged?	Yes	Yes	Yes
228	Communications (RS.CO):	Are the cyber related incident reported to higher authority on periodic basis?	Yes	Yes	Yes
229	Communications (RS.CO):	Are cyber incidents reported to CERT-In within 6 hours of noticing or being brought to notice about such incidents?	Yes	Yes	Yes
230	Communications (RS.CO):	Are third parties contractually required to protect the information that is shared with them as part of an incident?	Yes	Yes	Yes
231	Communications (RS.CO):	Are Contact details of Ministries, stakeholders, vendors and agencies like NCIIPC & CERTIn for incident resolutions up to date and documented?	Yes	Yes	Yes
232	Communications (RS.CO):	Are the timelines prescribed for reporting incidents to external organizations including IRDAI, CERT-IN strictly adhered to?	Yes	Yes	Yes
233	Communications (RS.CO):	Is root cause analysis of the incident and Action taken report submitted to the concerned insurer on demand.	Yes	Yes	Yes

234	Improvements (RS.IM):	Are Response strategies updated periodically?	Yes	Yes	Yes
235	Improvements (RS.IM):	Are the Board members provided with training programmes on IT Risk / Cybersecurity Risk and evolving best practices in this regard so as to cover all the Board members at least once a year.	Yes	MD	MD
236	Improvements (RS.IM):	Are top management sensitised on various technological developments and cyber security related developments periodically?	Yes	Annual	Annual
237	Improvements (RS.IM):	Are lessons learned captured and shared?	Yes	Yes	Yes
238	Mitigation (RS.MI):	Has the organization defined the incident management response procedure ?	Yes	Yes	Yes
239	Mitigation (RS.MI):	Are newly identified vulnerabilities are mitigated or documented as accepted risks?	Yes	Yes	Yes
240	Mitigation (RS.MI):	Are the corrective action procedure for all the vulnerabilities identified in VAPT?	Yes	Yes	Yes
241	Response Planning (RS.RP):	Are the plans tested quarterly to include management and recovering from backups?	Yes	Annual	Annual
242	Response Planning (RS.RP):	Does the organisation Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.	Yes	Yes	Yes
243	Response Planning (RS.RP):	Does the organisation Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls / offline backup ?	Yes	Yes	Sensitive Data
244	Response Planning (RS.RP):	Does the organisation Ensure that all of the organization's key / critical systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	Yes	Yes	Yes
245	Response Planning (RS.RP):	Does the organisation Install the latest stable version of any security-related updates on all network devices.	Yes	Yes	Yes
246	Response Planning (RS.RP):	Does the organisation Maintain standard, documented security configuration standards for all authorized network devices.	Yes	Yes	Yes
247	Response Planning (RS.RP):	Does the organisation Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	Bi-annually	Bi-annually	Annual
248	Response Planning (RS.RP):	Has the business impact analysis conducted?	Yes	Yes	Yes
249	Response Planning (RS.RP):	Has the organization defined the business continuity plan and procedure?	Yes	Yes	Yes
250	Response Planning (RS.RP):	Has the organization ensured that RPO(Recovery point objective) and RTO (Recovery point objective) are inline with the policy?	Yes	Yes	Yes
251	Response Planning (RS.RP):	Are the incidents responded and analysed?	Yes	Yes	Yes
252	Response Planning (RS.RP):	Are the security incidents analysed and corrective actions implemented for continual improvement ?	Yes	Yes	Yes
253	Response Planning (RS.RP):	Is the recovery plan understood and communicated through all security training? Are employee responsibilities and roles explicitly stated in the plan and communicated?	Yes	Yes	Yes
254	Response Planning (RS.RP):	Is there an incident response / crisis team with clearly defined roles and responsibilities?	Yes	Yes	Yes
255	Response Planning (RS.RP):	Is Cyber Crisis plan implemented and exercised or rehearsed periodically	Yes	Yes	Annual
256	Work From Remote Location (WFRL)	Does the Board approved Cyber Security Policy (Policy) of Regulated Entity address risks associated with Work From Remote Location (WFRL) risks?	Yes	MD	MD
257	Work From Remote Location (WFRL)	Does the Policy confirms use of secure network with strong protocols and Wi-Fi passwords at remote location?	Yes	Yes	Yes
258	Work From Remote Location (WFRL)	Does it mandates passwords change periodically?	Yes	Yes	Yes
259	Work From Remote Location (WFRL)	Are users provided with authorized assets of the organization which are hardened as per security policy for strong password authentication?	Yes	Yes	Yes

260	Work From Remote Location (WFRL)	Are servers, applications and networks hardened and secured as per standardized security policy settings?	Yes	Yes	Yes
261	Work From Remote Location (WFRL)	Are device controls implemented on user systems and Information and Communication Technology (ICT) infrastructure systems to block admin level access, unauthorized installation or changes to software, USB and other media, peripherals?	Yes	Yes	Yes
262	Work From Remote Location (WFRL)	Are user systems enabled with Antivirus, Endpoint protection controls, data encryption and Data Loss Prevention mechanisms?	Yes	Yes	Yes
263	Work From Remote Location (WFRL)	Does these controls pervade across all the users from all functions	Yes	Yes	Yes
264	Work From Remote Location (WFRL)	Are user systems and organization ICT infrastructure regularly updated with security patches and fixes. (Auditor to mention the latest update date)	Yes	Yes	Yes
265	Work From Remote Location (WFRL)	Are workflow approvals, deviations or exceptions captured as per Change Management Procedures.	Yes	Yes	Yes
266	Work From Remote Location (WFRL)	Are secure remote access mechanisms of Virtual Private Network (VPN), Internet Proxy or Virtual Device Interface (VDI) provisioned for WFRL users accessing organizational data assets and applications?	Yes	Yes	Yes
267	Work From Remote Location (WFRL)	Is the audit log monitoring and analysis provisioned on organizational ICT infrastructure as a control for unauthorized access risks and cyber threats?	Yes	Yes	Yes
268	Work From Remote Location (WFRL)	Are users provided with assets authorized by the Insurer which are hardened as per the Insurers security policy settings for strong password authentication?	Yes	Yes	Yes
269	Work From Remote Location (WFRL)	Does the policy, spell controls and procedures related to secure access of organizational data assets and applications from user-owned devices like mobile phones, tablets or other Bring Your Own Device (BYOD) of the Insurer?	Yes	Yes	Yes
270	Work From Remote Location (WFRL)	Do data containerization, Multifactor authentication and remote data wipe have been done to prevent data tampering and misuse of lost mobile/tablet devices during the period when WFRL has been permitted by the Insurer?	Yes	Yes	Limited
271	Work From Remote Location (WFRL)	Are users mandated to back-up critical data periodically (Policy shall mandate periodicity) on secure location in organization systems?	Yes	Yes	Yes
272	Work From Remote Location (WFRL)	Are Non-disclosure agreements / Undertaking on data security and confidentiality signed at the time of employee/ consultant/ third-party vendor on boarding before permitting Operations to be commenced at WFRL?	Yes	Yes	Yes
273	Work From Remote Location (WFRL)	Are users provided with assets authorized by the Insurer and are hardened as per security policy settings and strong password authentication?	Yes	Yes	Yes
274	Work From Remote Location (WFRL)	Is there an audit of Privileged user identity access authentication taken for administrative purposes?	Yes	Yes	Yes
275	Work From Remote Location (WFRL)	Is there an Audit of security information and events monitoring of audit logs analysis and incident response in place?	Yes	Yes	Limited
276	Work From Remote Location (WFRL)	Are controls in place to identify unauthorized access, malicious code execution, suspicious activities or behaviour, credential theft, presence of advance persistent threats like remote access toolkits and such cyber risks to organizational ICT infrastructure?	Yes	Yes	Yes
277	Work From Remote Location (WFRL)	Are email services secured to prevent spam, spoofed mails and malware filtering?	Yes	Yes	Yes
278	Work From Remote Location (WFRL)	Are users trained to handle spam, phishing scam and fraudulent emails?	Yes	Yes	Yes
279	Work From Remote Location (WFRL)	Are suspicious or malicious domains on the internet detected and blocked on network firewall, web proxy filtering, intrusion prevention systems?	Yes	Yes	Yes
280	Work From Remote Location (WFRL)	Are device controls implemented on user systems and ICT infrastructure systems to block unauthorized internet domains, unauthorized software installation or changes to configuration, USB and any other media, peripherals?	Yes	Yes	Yes
281	Work From Remote Location (WFRL)	Are user systems and organization ICT infrastructure regularly updated with security patches and fixes? (Auditor to mention the latest update date)	Yes	Yes	Yes
282	Work From Remote Location (WFRL)	Are activities like walkthrough and interviews performed using approved remote access software over secure and hardened systems of auditee and auditor organizations?	Yes	Yes	Yes
283	Work From Remote Location (WFRL)	Are evidences and artefacts classified, securely demonstrated to concerned stakeholders and not shared out of authorized domains?	Yes	Yes	Yes
284	Work From Remote Location (WFRL)	Are project implementation documents, MIS reports classified and shared on Need-to-know basis?	Yes	Yes	Yes
285	Work From Remote Location (WFRL)	Are plans and procedures set in place by the organization for Cybersecurity incident response and Crisis management activities?	Yes	Yes	Yes

286	Work From Remote Location (WFRL)	Is Cyber Security Project management performed remotely?	Yes	Yes	Yes
287	Work From Remote Location (WFRL)	Confirm whether there are hardening procedures to check / scan systems brought back to Office?	Yes	Yes	Yes
288	Work From Remote Location (WFRL)	Confirm whether if all patches, AV, End Point Protection, Data Encryption mechanisms are checked to ensure its appropriate functioning?	Yes	Limited	Limited
289	Work From Remote Location (WFRL)	Are user systems and organization ICT infrastructure systems regularly updated with security patches and fixes?	Yes	Yes	Yes
290	Work From Remote Location (WFRL)	Is the security event audit log monitoring and analysis provisioned on Insurers ICT infrastructure?	Yes	Yes	Yes
291	Work From Remote Location (WFRL)	Are security patch updates reviewed and periodically applied on ICT infrastructure to prevent Distributed Denial of Services(DDoS) attacks?	Yes	Yes	Yes
292	Work From Remote Location (WFRL)	In the case of disruption can IT support be accessed by investment application users through portal, help desk (phone) or email or visit to office?	Yes	Yes	Yes
293	Work From Remote Location (WFRL)	Are backups reviewed periodically and procedures aligned to minimize downtime impact?	Yes	Yes	Yes
294	Work From Remote Location (WFRL)	Is DR Drill performed to ensure adherence to Business Continuity metrics? (DR Drill should have been done on a normal working day)	Yes	Annual	Annual
295	Work From Remote Location (WFRL)	Is data restoration testing performed on periodic basis to ensure integrity of backups?	Bi-annually	Bi-annually	Annual
296	Work From Remote Location (WFRL)	Are alternative site options and resource availability planned as a part of Business Continuity and tested for same?	Yes	Yes	Yes
297	Work From Remote Location (WFRL)	Are Secondary Network Connectivity and IT infrastructure is provisioned and tested for the critical applications and services?	Yes	Yes	Yes
298	Work From Remote Location (WFRL)	Is it possible to <u>access</u> systems without user authentication or by-passing authentication? (Auditor shall specifically confirm that that users cannot bypass security)	Yes	Yes	Yes
299	Work From Remote Location (WFRL)	Are applications accessible ONLY to authorised users through a secured VPN or VDI access?	Yes	Yes	Yes
300	Work From Remote Location (WFRL)	Are users authenticated and authorised by a domain policy server?	Yes	Yes	Yes
301	Work From Remote Location (WFRL)	Are Logs of application IT infrastructure are collected and analysed by 24X7 Security Operation Centre (SOC) team?	Yes	Yes	Shared
302	Work From Remote Location (WFRL)	Is Continuous (Auditor shall specifically comment on the Periodicity interval) monitoring of IT logs to review unauthorized Login/Logout by users, access violations etc. done through Security Information and Event Monitoring (SIEM) and monitored by Security Operations Centre (SOC)?	Yes	Yes	Shared
303	Work From Remote Location (WFRL)	Are Enterprise wide monitoring of Information security incidents done by SOC team on 24X7 basis?	Yes	Yes	Shared
304	Work From Remote Location (WFRL)	Are ICT infrastructure logs maintained as per regulatory guidelines?	Yes	Yes	Yes
305	Work From Remote Location (WFRL)	Are Installation of unapproved software and utilities barred by centrally enforced policy?	Yes	Yes	Yes
306	Work From Remote Location (WFRL)	Are users using only Organization approved collaboration software?	Yes	Yes	Yes
307	Work From Remote Location (WFRL)	Is there a preventive control to block Unauthorized Collaboration tools on the firewall/network security devices?	Yes	Yes	Yes
308	Work From Remote Location (WFRL)	Are Cybersecurity awareness circulars and advisories regularly sent to employees, third party vendor and consultants.	Yes	Yes	Yes
309	Work From Remote Location (WFRL)	Does the Organization has a Dealing room policy and Standard operating policy to supervise controls over the dealing activities during WFRL?	Yes	Yes	Yes
310	Work From Remote Location (WFRL)	Are all agreements/documents with third parties digitally signed using a special tool?	Yes	Yes	Optional
311	Work From Remote Location - Investment (WFRL.IN)	Are Recorded lines working and and well-maintained condition?	Yes	Yes	Yes



312	Work From Remote Location - Investment (WFRL.IN)	Does Mid-office check voice recording as per a defined process in Standard Operating Procedure (SOP)?	Yes	Yes	Yes
313	Work From Remote Location - Investment (WFRL.IN)	Are Dealers provided with a dedicated and secured recording line during WFH for placing the calls to the brokers.	Yes	Yes	Yes
314	Work From Remote Location - Investment (WFRL.IN)	Is Voice logger used for recording of calls made from office location?	Yes	Yes	Yes
315	Work From Remote Location - Investment (WFRL.IN)	Is Back up/storage of call recordings enabled as a part of proof of transaction that can be accessed anytime?	Yes	Yes	Yes
316	Work From Remote Location - Investment (WFRL.IN)	Does the SOP define process to handle disruption in communication links between the dealers and brokers?	Yes	Yes	Yes
317	Work From Remote Location - Investment (WFRL.IN)	Are such communications logged /recorded?	Yes	Yes	Yes
318	Work From Remote Location - Investment (WFRL.IN)	Does the Mid-Office independently review these logs / records ?	Yes	Yes	Yes
319	Work From Remote Location - Investment (WFRL.IN)	Are appropriate prior approvals / authorisations taken to process such transactions?	Yes	Yes	Yes
320	Work From Remote Location - Investment (WFRL.IN)	Do Dealers execute ALL transactions only through recorded telephone lines?	Yes	Yes	Yes
321	Work From Remote Location - Investment (WFRL.IN)	Are all authorized Bloomberg terminals / Bloomberg anywhere ID's / NDS terminals/TREPS Terminals/Emails only and are completely disabled for SMS / Chat facilities?	Yes	Yes	Yes
322	Work From Remote Location - Investment (WFRL.IN)	Confirm that Bloomberg terminals are accessible through multi factor authentication and are disabled for SMS / Chat facilities.	Yes	Yes	Yes
323	Work From Remote Location - Investment (WFRL.IN)	In the event of disruption of communication link, are there defined policies / processes to guide the officials of the Investments Function to process transactions with appropriate approvals?	Yes	Yes	Yes
324	Work From Remote Location - Investment (WFRL.IN)	Confirm specifically that investment transactions are executed with all mandates defined as a part of Dealing room Work flow / SOP with requisite approvals	Yes	Yes	Yes
325	Work From Remote Location - Investment (WFRL.IN)	Do Dealers execute all transactions via recorded telephone lines or authorized Bloomberg terminals / Bloomberg anywhere ID's / NDS terminals/TREPS terminals/Emails only?	Yes	Yes	Yes
326	Work From Remote Location - Investment (WFRL.IN)	Confirm specifically that in addition to the recorded lines the dealers places the orders only through empanelled brokers ONLY through authorized communication modes as per SOP/Dealing room policy?	Yes	Yes	Yes
327	Work From Remote Location - Investment (WFRL.IN)	Are Contingency policy and plans, revised and tested periodically for an effective business continuity?	Yes	Yes	Yes
328	Work From Remote Location - Investment (WFRL.IN)	Is Secondary network connectivity and IT infrastructure provisioned and tested for the critical applications and services? Check for are any SPoFs - Single Point of Failure	Yes	Yes	Yes
329	Work From Remote Location - Investment (WFRL.IN)	Are Disaster Recovery (DR) Drills performed to verify the availability of applications, processes and resources at remote backup site. Are issues identified during DR testing addressed?	Bi-annually	Bi-annually	Annual
330	Work From Remote Location - Investment (WFRL.IN)	Is IT support accessed by Investment application users by way of portal, helpdesk or visit to office.	Yes	Yes	Yes
331	Work From Remote Location - Investment (WFRL.IN)	Are Backup/Alternative locations and resources identified within Investment function to ensure business continuity?	Yes	Yes	Yes
332	Work From Remote Location - Investment (WFRL.IN)	Is Email facility enabled with empanelled broker, counter parties, custodian etc.	Yes	Yes	Yes
333	Work From Remote Location - Investment (WFRL.IN)	Are Emails shared ONLY through authorized company email addresses registered with concerned counterparties?	Yes	Yes	Yes
334	Work From Remote Location - Investment (WFRL.IN)	Is Voice recording analysis and rate scan done on a regular basis to supervise trades and transaction price as defined in dealing room policy?	Yes	Yes	Yes
335	Work From Remote Location - Investment (WFRL.IN)	Is there a supervisory monitoring process check list which includes transaction price monitoring and trade monitoring etc.?	Yes	Yes	Yes
336	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary prominently published on its website, mobile based application or both, as the case may be, the rules and regulations, privacy policy and user agreement for access or usage of its computer resource by any person?	Yes	Yes	Yes



337	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the rules and regulations, privacy policy or user agreement of the intermediary informed the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that (i) belongs to another person and to which the user does not have any right; (ii) is defamatory, obscene, pornographic, paedophilic, invasive of another privacy including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force; (iii) is harmful to child; (iv) infringes any patent, trademark, copyright or other proprietary rights; (v) violates any law for the time being in force; (vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact; (vii) impersonates another person; (viii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation; (ix) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource; (x) is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person;	Yes	Yes	Yes
338	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary periodically informed its users, at least once every year, that in case of non-compliance with rules and regulations, privacy policy or user agreement for access or usage of the computer resource of such intermediary, it has the right to terminate the access or usage rights of the users to the computer resource immediately or remove non-compliant information or both, as the case may be	Yes	Yes	Yes
339	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the Act, not host, store or publish any unlawful information, which is prohibited under any law for the time being in force relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force:	Yes	Yes	Yes
340	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary periodically, and at least once in a year, informed its users of its rules and regulations, privacy policy or user agreement or any change in the rules and regulations, privacy policy or user agreement, as the case may be	Yes	Yes	Yes
341	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	If the intermediary collected information from a user for registration on the computer resource, has it retained his information for a period of one hundred and eighty days after any cancellation or withdrawal of his registration, as the case may be;	Yes	Yes	Yes
342	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary taken all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011	Yes	Yes	Yes
343	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Does the intermediary, as soon as possible, but not later than seventy two hours of the receipt of an order, provide information under its control or possession, or assistance to Government agency which is lawfully authorised for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents:	Yes	Yes	Yes
344	Information Technology	Has the intermediary reported cyber security incidents and share related information with the Indian Computer Emergency Response Team in accordance with the policies and procedures as mentioned in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.	Yes	Yes	Yes
345	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Is the intermediary aware that it shall not knowingly deploy or install or modify technical configuration of computer resource or become party to any act that may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force	Yes	Yes	Yes
346	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary prominently published on its website, mobile based application or both, as the case may be, the name of the Grievance Officer and his contact details as well as mechanism by which a user or a victim may make complaint against violation of the provisions of this rule or any other matters pertaining to the computer resources made available by it, and the Grievance Officer shall - (i) acknowledge the complaint within twenty four hours and dispose off such complaint within a period of fifteen days from the date of its receipt; (ii) receive and acknowledge any order, notice or direction issued by the Appropriate Government, any competent authority or a court of competent jurisdiction.	Yes	Yes	Yes
347	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it:	Yes	Yes	Yes
348	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary implemented a mechanism for the receipt of complaints under clause (b) of this sub-rule which may enable the individual or person to provide details, as may be necessary, in relation to such content or communication link	Yes	Yes	Yes