

अध्याय 4 आईटी सुरक्षा

लेखापरीक्षा उद्देश्य III- आईटी सुरक्षा की समीक्षा करना ताकि यह जांच की जा सके कि किस सीमा तक वह व्यवसायिक महत्वपूर्ण सूचना और परिसम्पतियों की हानि, क्षति या दुरुपयोग का यथोचित संरक्षण करने में सक्षम है

4. रेलवे बोर्ड ने अप्रैल/मई 2008 में अपनी आधारभूत आईटी सुरक्षा नीति बनाई जिसके अनुसार क्रिस/क्षेत्रीय रेलवे/स्वतंत्र इकाईयों द्वारा सहायक प्रक्रियायें और निर्देश दिए जाने थे। आधारभूत आईटी सुरक्षा नीति में आईटी सुरक्षा के विभिन्न पहलुओं को देखा जाता है जिसमें आकस्मिक प्रबंधन योजना, अनुज्ञापित सॉफ्टवेयर का प्रयोग और इसका अद्यतन, बैक अप नीति, पासवर्ड प्रबंधन, वर्जन नियंत्रण तंत्र, वायरस/मालवेयर से सुरक्षा, आईटी सुरक्षा निगरानी टीम और घटना कार्रवाई दल का गठन, परिवेश और स्थान सुरक्षा, उपकरण सुरक्षा, भौतिक पहुँच नियंत्रण, डाटा अभिगम अधिकार, प्रयोक्ता पहचान और सुविधा प्रबंधन, एप्लीकेशन बनाना और अनुरक्षण सुरक्षा, इंटरनेट सुरक्षा आदि।

आईआर की आधारभूत सुरक्षा नीति/क्रिस आईएस सुरक्षा नीति तथा आईटी परिवेश में सर्वोत्तम प्रथाओं को देखते हुए आईसीएमएस एप्लीकेशन सुरक्षा और संबंधित मुद्दों की व्यापक लेखापरीक्षा की गई थी। लेखापरीक्षा ने विभिन्न क्षेत्रीय रेलवे के 128 स्थलों का दौरा किया और देखा कि:

4.1 भौतिक अभिगम नियंत्रण

लेखापरीक्षा द्वारा द.रे¹, द.प.रे², उ.रे³, उ.म.रे⁴, उ.पू.रे⁵ और पू.त.रे⁶ में किए गए आईसीएमएस स्थलों पर अप्राधिकृत व्यक्तियों के अभिगम पर कोई प्रतिबंध नहीं था।

4.2 तर्क संगत अभिगम नियंत्रण – उपयोगकर्ता और पासवर्ड प्रबंधन

4.2.1 यद्यपि प्रयोक्ताओं के पासवर्ड इनक्रिप्टेड रूप में दर्ज किए गए थे, यूजर खातों को फिर से चालू करने के लिए सुरक्षा प्रश्नों के उत्तर स्पष्ट रूप से दर्ज थे

¹ लेखापरीक्षा के दौरान दौरा किए गए सभी चयनित स्थल

² हुबली, मैसूर और वास्को में तीन आईसीएमएस स्थल

³ लेखापरीक्षा के दौरान दौरा किए गए दिल्ली, अम्बाला और फिरोजपुर मंडलों के सभी चयनित स्थल। दिल्ली मण्डल नियंत्रण कार्यालय में सीसीटीवी कैमरे लगाए गए थे किन्तु बायोमेट्रिक प्रणाली नहीं कर रही थी।

⁴ लेखापरीक्षा के दौरान दौरा किए गए सभी चयनित स्थल

⁵ लेखापरीक्षा के दौरान दौरा किए गए सभी चयनित स्थल

⁶ लेखापरीक्षा के दौरान दौरा किए गए दो स्थल (वाल्टेयर नियंत्रण और भुवनेश्वर (एफओआईएस) सेल)

जैसा कि चार⁷ क्षेत्रीय रेलवे में देखा गया। यहाँ तक यूजर्स के पंजीकरण पासवर्ड भी स्पष्ट रूप⁸ में थे।

4.2.2 क्रिस द्वारा बनाए गए यूजरों के यूजर आईडी और पासवर्ड सीएओ/एफओआईएस कार्यालय को गोपनीय तरीके से नहीं दिए गए थे बल्कि अनुरोध पत्र पर ही लिखित रूप से दिया गया जिससे पासवर्ड सुरक्षा से समझौता किया गया।

4.2.3 आईसीएमएस के लॉगिन पेज यूजर्स द्वारा लॉगिन के प्रयासों की संख्या पर कोई प्रतिबंध नहीं था। मजबूत पासवर्ड नियंत्रण के अभाव में असीमित लॉगिन प्रयासों से रेंडर पासवर्ड जनरेटर सॉफ्टवेयर का प्रयोग करते हुए प्रणाली को भेदना आसान बनाता है।

4.2.4 भारतीय रेल की आईटी सुरक्षा नीति के अनुसार प्रणाली प्रशासन पासवर्ड कम से कम 10 अंकों का होना चाहिए और यह एल्फा संख्या तथा विशेष अंकों का संयोजन होना चाहिए। तथापि, यह देखा गया कि केंद्रीयकृत डाटा केंद्र पर सीआरआईएस आईसीएमएस समूह द्वारा अनुपालन किए जा रहे पासवर्ड मानदंड निर्धारित आईटी सुरक्षा नीति का पालन नहीं करते।

4.2.5 22 प्रयोक्ताओं की सृजन तिथि उनकी प्रारंभ तिथि से 1 से 30 दिन पहले की थी और 245 प्रयोक्ताओं की प्रारंभ तिथि उनकी सृजन तिथि से पहले की थी जोकि तर्कसंगत प्रतीत नहीं होती तथा पर्याप्त नियंत्रणों की कमी को दर्शाया।

4.2.6 प्रयोक्ता आईडी के सृजन के लिए आवेदन को उ.रे. मुख्यालय द्वारा टेलिफोन पर स्वीकार किया गया था। प्रयोक्ता आईडी और पासवर्ड तैयार करने के लिए वैधीकरण से संबंधित अभिलेख उ.रे. में क्षेत्रीय रेलवे मुख्यालय में उपलब्ध नहीं थे।

4.2.7 उ.रे. में, छह आईसीएमएस स्थानों पर आईसीएमएस प्रयोक्ताओं का सृजन आईसीएमएस टर्मिनलों तथा प्रयोक्ताओं की प्रचालन शिफ्ट की तुलना में आवश्यकता से अधिक किया गया था। नई दिल्ली में पांच प्रयोक्ता थे और दिल्ली मेन में दस प्रयोक्ता थे किंतु आईसीएमएस में 26 तथा 71 सक्रिय प्रयोक्ता सृजित किए गए थे।

4.2.8 उ.रे. तथा द.म.रे. में 47 सक्रिय प्रयोक्ताओं, जिनकी वही मोबाइल संख्या तथा जन्म तिथि थी, की दो से चार प्रयोक्ता आईडी थी। शेष विवरण जैसे सिक्रेट

⁷ पू.सी.रे, द.म.रे, म.रे, उ.रे, उ.पू.रे

⁸ उ.रे, द.म.रे, म.रे, द.पू.म.रे

क्वेश्चन, नाम, पता आदि, या तो वही थे या मामूली अंतर तथा जिससे पता चला कि विभिन्न प्रयोक्ता आईडी एक ही व्यक्ति से संबंधित थी। अतः प्रणाली में प्रत्येक प्रयोक्ता के लिए विशिष्ट आईडी के सृजन को सुनिश्चित करने हेतु नियंत्रणों की कमी थी।

4.2.9 प्रयोक्ता मास्टर तालिका में प्रयोक्ताओं का सृजन श्री एलकेओ, श्री यूएमबी, श्री डीएलएलआई, श्री सीसीएम डाटाबेस, श्री पीआरसी, श्री केसीजी, श्री सीआरएसई, श्री एचवाईबी, श्री डीआरएम-एनएजी, श्री सीटीई, श्री एसइसीआरसीएमई, श्री सीईजीई, श्री सीएसटीई, एसईसीआर आदि (स्थान/पदनाम) जैसे अस्पष्ट नामों से किया गया था (उ.रे., द.म.रे., द.पू.म.रे.)।

4.2.10 'डीसी और 'एससी' जैसे कई गलत/अप्रासंगिक प्रयोक्ता मास्टर तालिका¹¹⁵ में पाए गए थे जिनके डाटाबेस में इस प्रकार के प्रयोक्ता के विवरण के बिना प्रयोक्ता ब्यौरे निर्दिष्ट थे।

4.2.11 प्रयोक्ताओं, जो सेवानिवृत्ति की आयु पार कर चुके थे, को प्रणाली में सक्रिय पाया गया था। 18 वर्ष से कम आयु के प्रयोक्ता (अर्थात् 1 नवम्बर 1997 के बाद पैदा हुए और नौ से 15 वर्ष के बीच थे) भी सक्रिय थे। इससे पता चला कि प्रयोक्ताओं की जन्म तिथि के डाटा प्राप्त करते समय प्रमाणित नहीं किया गया था।

उ.रे. में आईसीएमएस स्थानों पर नमूना जांच से यह भी पता चला कि क्षेत्रीय मुख्यालयों, अम्बाला, अम्बाला नियंत्रण कार्यालय तथा नई दिल्ली में सेवानिवृत्त/स्थानांतरित अधिकारियों की प्रयोक्ता आईडी अभी भी सक्रिय थी। उ.रे. में सेवानिवृत्त सक्रिय प्रयोक्ता अनुप्रयोग प्रयोक्ता थे और इनके पास अनुप्रयोग डाटा में आशोधन का विशेषाधिकार भी था।

4.2.12 प्रयोक्ताओं के ब्यौरे अधूरे थे और राज्य, मोबाईल संख्या, रेलवे फोन संख्या, आईसीएमएस इ-मेल आईडी, पदनाम, द्वितीयक इ-मेल आईडी, पता जैसे ब्यौरे खाली छोड़े गए थे। अतः डाटा पूर्ण नहीं था और आवश्यकता पड़ने पर उपयोग करने योग्य नहीं था (उ.रे., द.म.रे., उ.पू.रे., द.पू.म.रे.)

4.2.13 एक प्रयोक्ता आईडी/पासवर्ड को जोधपुर (उ.प.रे.) में तैनात तीन गाड़ी क्लर्कों द्वारा साझा किया गया था। द.रे. के चेन्नई, चेन्नई एगमोर और बेसिन ब्रिज जंक्शन में आईसीएमएस स्थानों पर विशिष्ट कार्मिक के लिए अधिकृत प्रयोक्ता आईडी तथा संबंधित पासवर्ड को एक से अधिक व्यक्तियों द्वारा साझा किया गया

¹¹⁵ एमटी-प्रयोक्ता तालिका

था। इलाहाबाद (उ.म.रे.) के आईसीएमएस नियंत्रण कार्यालय में कार्यरत चार गाड़ी क्लर्कों के पास अलग-अलग प्रयोक्ता आईडी/पासवर्ड नहीं थे और वे एक ही लॉगइन आईडी/पासवर्ड का उपयोग कर रहे थे। उ.रे., प.म.रे. और दमपू.रे. में, 13 स्थानों¹¹⁶ में प्रत्येक में केवल एक प्रयोक्ता आईडी थी और सात स्थानों¹¹⁷ पर प्रत्येक में केवल 2 सक्रिय प्रयोक्ता आईडी थी। स्थानों के दौरे के दौरान यह देखा गया कि उ.रे. में¹¹⁸ सभी प्रयोक्ताओं के पास विशिष्ट प्रयोक्ता आईडी नहीं था। आनंद विहार में 18 अप्रैल 2016 को एक प्रयोक्ता¹¹⁹ की आईसीएमएस आईडी प्रयोग में थी, हालांकि वह प्रातः की पारी के दौरान ड्यूटी पर नहीं थी। उ.पू.रे. में, एक स्थानांतरित अधिकारी की प्रयोक्ता आईडी काठगोदाम आईसीएमएस स्थान पर प्रयोग में थी।

4.2.14 सीआरआईएस लेखों में सृजित किए गए 26 सक्रिय आईसीएमएस प्रयोक्ताओं, जिनके पास प्रशासनिक विशेषाधिकार हैं, में से 25 सक्रिय विशिष्ट प्रयोक्ता¹²⁰ थे। इन प्रयोक्ताओं में वह भी शामिल है जिनका सीआरआईएस आईसीएमएस ग्रुप से अन्य सीआरआईएस ग्रुप में स्थानांतरण हो गया था, किंतु विशिष्ट प्रयोक्ता विशेषाधिकार के साथ यह अब भी सक्रिय आईसीएमएस प्रयोक्ता थे। प्रशासनिक विशेषाधिकार वाले विशिष्ट प्रयोक्ताओं में दो जाली प्रयोक्ता भी शामिल थे जिन्हें आईसीएमएस आईआरसीए तथा पीआरएससी एचएआरटी के नाम से बनाया गया था। इससे पता चला कि प्रयोक्ताओं के निर्धारित कार्यों/उत्तरदायित्वों/कर्तव्यों के अनुपालन में आईसीएमएस तक पहुंच को रोकने के लिए कोई नियंत्रण नहीं था। यह आईटी सुरक्षा नीति के उल्लंघन में था।

4.2.15 आईसीएमएस प्रयोक्ता के पंजीकरण डाटा के विश्लेषण से पता चला कि 335 प्रयोक्ताओं को प्रणाली तक एक्सेस हेतु बिना प्रयोक्ता आईडी के पंजीकृत कोड आबंटित किए गए थे। इनमें से 330 प्रयोक्ताओं को आवेदन स्तर/रिपोर्ट स्तर की एक्सेस दी गई थी और 253 प्रयोक्ताओं के पास आईसीएमएस के एक या अधिक मॉड्यूलों के डाटा में आशोधन का विशेषाधिकार था। प्रयोक्ता मास्टर डाटा की समीक्षा से पता चला कि नौ प्रयोक्ताओं के पास पंजीकरण कोड नहीं था जिसमें सक्रिय प्रयोक्ता और सेवानिवृत्त प्रयोक्ता शामिल थे।

¹¹⁶ मेरठ, पानीपत, पटियाला, आलमबाग (उ.रे.) और द.पू.म.रे. के छह स्थान, प.म.रे. के तीन स्थान

¹¹⁷ जगाधरी कार्यशाला, जम्मू तवी, हुसैनपुर (उ.रे.), द.पू.म.रे. के तीन स्थान, प.म.रे. का एक स्थान

¹¹⁸ आनंद विहार, अम्बाला (सीपीआरसी तथा सीटीएलसी), दिल्ली नियंत्रण (कोचिंग स्टॉक तथा सीटीएलसी), जगाधरी कार्यशाला, जम्मू तवी, दिल्ली सराय रोहिल्ला

¹¹⁹ सुश्री सुषमा

¹²⁰ विशेषाधिकार रखने वाला प्रयोक्ता जिसे नए/ मौजूदा प्रयोक्ताओं के सृजन/ प्रबंधन का अधिकार है

4.2.16 147 मामलों¹²¹ में, विभिन्न आईसीएमएस में प्रयोक्ता लॉग इन समय 3 दिनों में 523 दिन पूराना था और प्रयोक्ताओं ने आईसीएमएस से लॉग आऊट नहीं किया था। आगे यह देखा गया कि आईसीएमएस में डाटा उन प्रयोक्ताओं द्वारा भरा जा रहा था जिन्होंने आईसीएमएस में लॉग इन तो किया किंतु लम्बे समय तक लॉग आऊट नहीं किया और उनका पासवर्ड भी समाप्त हो चुका था। हालांकि यह देखा गया कि आईसीएमएस द्वारा विशेष निष्क्रियता अवधि के पश्चात प्रयोक्ता को स्वतः लॉग आऊट कर दिया जाता था, आईसीएमएस डाटाबेस के अनुसार इन प्रयोक्ताओं को 3 से 523 दिनों की अवधि तक आईसीएमएस में लॉग इन के बाद भी स्वचालित रूप से लॉग आऊट नहीं किया गया था।

प्रयोक्ताओं के सेशन ब्यौरों के साथ साथ पिछले लॉग-इन ब्यौरों के संबंधित डाटा¹²² के विश्लेषण से उन मामलों का पता चला जहां प्रयोक्ता लॉग आऊट समय प्रयोक्ता के लॉग इन समय से पहले का था। (उ.रे., उ.पू.रे., प.म.रे., द.म.रे.)

4.2.17 प्रयोक्ताओं के पिछले लॉग-इन ब्यौरे दर्शाने वाली तालिका में 407 सक्रिय प्रयोक्ताओं¹²³ के लॉग इन/ लॉग आऊट के कोई अभिलेख नहीं थे।

4.2.18 लेखापरीक्षा जांच की प्रतिक्रिया में सीआरआईएस ने वैयक्तिक अधिकारी के कर्तव्यों और जिम्मेदारियों के ब्यौरों की बजाय सीआरआईएस आईसीएमएस दल के पदनाम वार कर्तव्य और जिम्मेदारियां उपलब्ध कराई थी। अतः यह सुनिश्चित नहीं किया जा सका कि क्या प्रत्येक अधिकारी के कर्तव्यों तथा जिम्मेदारियों को पृथक/अलग रूप से परिभाषित किया गया था।

4.3 परिवर्तन प्रक्रिया/प्रबंधन

आईटी सुरक्षा नीति के अनुसार, सभी आईटी दलों से अनुप्रयोग सॉफ्टवेयर में परिवर्तनों के लिए प्रक्रियाएं विकसित करना अपेक्षित था। तथापि, आईसीएमएस दल ने आईसीएमएस सॉफ्टवेयर में परिवर्तन करने के लिए प्रक्रियाएं विकसित/निश्चित नहीं की थी। आईसीएमएस में किए गए परिवर्तनों से संबंधित सीआरआईएस अभिलेखों की नमूना जांच के अनुसार ऑनलाइन परिवेश में आईसीएमएस में किए गए परिवर्तनों को बताने से पूर्व उचित अनुमोदन प्राप्त करने हेतु कोई प्रणाली/प्रक्रिया नहीं पाई गई थी।

4.4 आईसीएमएस प्रलेखन

¹²¹ उ.रे.-84 प.म.रे.-15, द.म.रे.-48

¹²² डीटी-सेशन तथा डीटी-लास्ट-लॉग इन-इनफो

¹²³ द.म.रे.-80, द.पू.म.रे.-5, उ.रे.-207, उ.पू.रे.-115

सीआरआईएस द्वारा दी गई सूचना के अनुसार सीआरआईएस के पास आईसीएमएस पर प्रयोक्ता नियमपुस्तक, सीओआईएस पर सॉफ्टवेयर आवश्यकता विनिर्देश (एसआरएस) और सीओआईएस पर प्रणाली डिजाइन एवं विकास (एसडीडी) है। पीएम तथा सीओआईएस के लिए प्रयोक्ता आवश्यकता विनिर्देश पर सीआरआईएस ने कोई प्रलेखन उपलब्ध नहीं कराया। सीआरआईएस पीएम के लिए एसआरएस भी उपलब्ध नहीं कराता। यहां तक कि सीओआईएस पर एसडीडी में भी सीओआईएस मॉड्यूल में उपयोग की गई सभी तालिकाओं जिसमें उनकी तालिका संरचना, विभिन्न तालिकाओं के बीच लिंकेज, आईसीएमएस तालिकाओं के विभिन्न फील्ड्स के विवरण, विभिन्न फील्ड्स के लिए प्रयुक्त मूल्यों के विवरण शामिल है, के पूर्ण ब्यौरे निर्दिष्ट नहीं किए गए थे। प्रयोक्ता नियमपुस्तक दिसम्बर 2014 तक अद्यतित थी और यह अधूरी पाई गई थी क्योंकि इसमें आईसीएमएस द्वारा सृजित विभिन्न रिपोर्टों के ब्यौरे नहीं थे जिसमें उनका फार्मेट, विभिन्न रिपोर्टों में उपयोग किए गए कोड के ब्यौरे, अवधि, जिसके लिए विभिन्न रिपोर्टों में प्रयोक्ता आदि के लिए आईसीएमएस डाटा उपलब्ध कराया गया था, शामिल है (उ.रे., पूम.रे.)।

4.5 कारोबार निरंतरता योजना

4.5.1 सीआरआईएस केंद्रीयकृत डाटा केंद्रों पर कारबार निरंतरता योजना

आईसीएमएस के केंद्रीयकृत अनुप्रयोग है और सभी सर्वरों (डाटाबेस, सर्वर, अनुप्रयोग सर्वर, वैब सर्वर आदि) को सीआरआईएस मुख्यालय, चाणक्यपुरी, नई दिल्ली में प्रतिष्ठापित किया गया था। आईसीएमएस प्रचालनों की निरंतरता को सुनिश्चित करने के लिए सीआरआईएस ने 2011-12 के दौरान कारबार निरंतरता योजना के कार्यान्वयन की प्रक्रिया शुरू की थी। नवम्बर 2015 में, सीआरआईएस ने रेलवे बोर्ड के लिए ₹ 12.04 करोड़ की लागत पर आईसीएमएस अनुप्रयोग के आपदा बहाली (डीआर) सैट अप के लिए काल्पनिक अनुमान प्रस्तुत किया था। 31 मार्च 2016 तक डीआर सैट-अप के लिए प्रक्रिया अभी चल रही है।

लेखापरीक्षा पूछताछ पर प्रतिक्रिया में सीआरआईएस ने बताया (फरवरी 2016) कि अक्टूबर 2015 में प्रतिष्ठापित नई प्रणाली के लिए आईसीएमएस डाटा बैकअप सुरक्षा नीति प्रगतिशील थी और इसकी समीक्षा चल रही थी। आगे यह देखा गया कि यद्यपि आईसीएमएस द्वारा दैनिक आधार पर डाटा लिया जा रहा था फिर भी आईसीएमएस के किसी ऑफलाइन/रिमोट साइट बैकअप का सीआरआईएस आईसीएमएस ग्रुप द्वारा अनुरक्षण नहीं किया जा रहा था।

4.5.2 क्षेत्रीय स्तर पर कारबार निरंतरता योजना

द.प.रे., उ.म.रे., द.म.रे., पू.म.रे., पू.त.रे., पू.रे., प.रे., उ.पू.रे., दपू.रे., उ.म.रे., तथा द.रे. में कोई प्रलेखित कारबार निरंतरता योजना उपलब्ध नहीं थी। सीआरआईएस ने फरवरी 2015 में नए आईसीएमएस सर्वर खरीदे थे। यद्यपि सर्वर को अक्टूबर 2015 में ऑनलाइन कर दिया गया था फिर भी प्रतिष्ठापन प्रक्रिया अभी पूरी की जानी थी (मार्च 2016)। लेखापरीक्षा में जांच किए गए आईसीएमएस स्थानों पर निम्नलिखित कमियां देखी गई थी:

- (i) प.रे., द.रे., उ.रे. और उ.पू.रे. के आईसीएमएस स्थानों पर थिन क्लाउंट के बजाय व्यक्तिगत कम्प्यूटरों/डेस्कटॉप का उपयोग हो रहा था। उ.म.रे. और पू.म.रे. में प्रारंभ में थिन क्लाउंटस उपलब्ध कराए जा रहे थे किंतु बाद में इनको डेस्कटॉप कम्प्यूटरों से बदल दिया गया था जिससे एन्टी वायरस के अभाव में प्रणाली सुरक्षा जोखिमों तथा वायरस के लिए सुभेघ हो दी गई।
- (ii) उ.पू.रे. तथा उ.रे.¹²⁴ में लेखापरीक्षा दल द्वारा दौरा किए गए अधिकतर आईसीएमएस स्थानों पर एन्टीवायरस सॉफ्टवेयर उपयोग में नहीं था और म.रे. में एन्टीवायरस सॉफ्टवेयर अद्यतित नहीं पाया गया था।
- (iii) आईसीएमएस प्रणालियों को द.म.रे., द.रे., उ.रे.¹²⁵ में वार्षिक अनुरक्षण ठेका के अंतर्गत कवर नहीं किया गया था। पू.म.रे. में, छह पीसीज (17 में से) की वारंटी अवधि 31 मार्च 2016 को पहले ही समाप्त हो चुकी है और लेखापरीक्षा की तिथि तक किसी एजेंसी के साथ इन छह पीसीज के लिए एएमसी कार्यान्वित नहीं की गई थी। थिन क्लाउंटस 31 मार्च 2016 को समाप्त हो चुके थे और इन थिन क्लाउंटस को बदलने की प्रक्रिया अभी शुरू की जानी थी।
- (iv) उ.म.रे. (5)¹²⁶, द.रे.¹²⁷, पू.रे.¹²⁸, द.म.रे.¹²⁹, उ.रे.¹³⁰ और उ.पू.रे.¹³¹ में आईसीएम स्थानों पर धुंआ संसूचक, अग्निशामक नहीं पाए गए थे।
- (v) कचरा/कुड़ादान (अग्नि जोखिम) परिसर हाऊसिंग सिस्टम के अंदर रखे पाए गए थे जिन पर आईसीएमएस प्रतिष्ठापित किए गए थे और चालू थे। शोर्ट सर्किट, शार्प एनर्जी वेरिएशन आदि के कारण आग की घटना होने पर आग

¹²⁴ अम्बाला (सीटीएलसी) को छोड़कर, जहां एन्टी वायरस का नि-शुल्क वर्जन उपयोग में था।

¹²⁵ अम्बाला (सीपीआरसी), दिल्ली (सीटीएलसी), जगाधरी कार्यशाला, जम्मू तवी और अमृतसर

¹²⁶ हालांकि सभी स्थानों पर धुआ संसूचक उपलब्ध नहीं थे, फिर भी सभी स्थानों पर अग्निशामक पाए गए थे।

¹²⁷ दौरा किए गए सभी स्थानों पर धुंआ संसूचक और अग्निशामक उपलब्ध नहीं हैं।

¹²⁸ दौरा किए गए सभी स्थानों पर धुआ संसूचक उपलब्ध नहीं थे और एचडब्ल्यूएच/टीएनसी पर अग्निशामक उपलब्ध नहीं थे।

¹²⁹ 2 स्थानों पर फायर अलार्म/धुआं संसूचक उपलब्ध थे और अग्निशामक सभी स्थानों पर उपलब्ध थे।

¹³⁰ यूएमबी नियंत्रण कार्यालय को छोड़कर

¹³¹ लेखापरीक्षा द्वारा दौरा किए गए सभी स्थानों पर धुआं संसूचक नहीं पाए गए थे

को बुझाने के लिए कोई अग्निशामक उपलब्ध नहीं थे जिससे कि सूचना प्रणाली परिसम्पतियों (द.रे.) को बचाया जा सके।

- (vi) रेलवे बोर्ड आदेशों/अनुदेशों के अनुसार निरंतर और सुगम प्रचालनों को सुनिश्चित करने के लिए सभी एफओआईएस परियोजनाओं में मीडिया और रूट विविधता उपलब्ध कराई जानी है। उ.रे. में लेखापरीक्षा द्वारा दौरा किए गए लगभग सभी स्थानों पर एफओआईएस नेटवर्क¹³² द्वारा आईसीएमएस कनेक्टिविटी उपलब्ध कराई गई थी किंतु किसी भी स्थान पर स्टैंड बाय/अतिरेक लाइन उपलब्ध नहीं कराई गई थी। प्रयोक्ताओं ने कनेक्टिविटी समस्याओं की सूचना दी। उ.रे.¹³³ और म.रे.¹³⁴ में लिंक/कनेक्टिविटी खराबी/समस्याओं के लिए अभिलेखों का रख-रखाव नहीं किया गया था। द.रे. में यद्यपि नमूना जांच किए गए आईसीएमएस स्थानों पर खराबी रिपोर्ट रजिस्ट्रों का अनुरक्षण किया जा रहा था और रजिस्ट्रों में नेटवर्क खराबी, प्रणाली खराबी आदि के बारे में सूचना निर्दिष्ट की गई थी, फिर भी प्रणाली की खराबियों के परिशोधन, वास्तविक डाऊन टाइम से संबंधित ब्यौरे रजिस्टर में उपलब्ध नहीं थे।
- (vii) चार आईसीएमएस टर्मिनलों¹³⁵ पर कोई यूपीएस उपलब्ध नहीं थे। पांच स्थानों¹³⁶ पर उपलब्ध कराए गए यूपीएस खराब थे/ कोई पावर बैकअप नहीं था। पर्याप्त और उचित फर्नीचर उपलब्ध¹³⁸ नहीं कराया गया था।
- (viii) उ.रे., द.म.रे., ओर म.रे. में 12 स्थानों¹³⁹ पर धूल रहित परिवेश नहीं था और 11¹⁴⁰ स्थानों पर एयर कंडिशनर उपलब्ध नहीं थे।
- (ix) नई दिल्ली दिल्ली मेन में ट्रेन ब्रांच और उ.रे. के अमृतसर स्थान और

¹³² नई दिल्ली, दिल्ली नियंत्रण कार्यालय (सीपीआरसी), आनंद विहार, अम्बाला नियंत्रण कार्यालय (सीपीआरसी), दिल्ली सराय रोहिल्ला, जम्मू तवी

¹³³ म.रे. के मुम्बई सीएसटी और मझगांव में और दिल्ली तथा आनंद विहार की ट्रेन ब्रांच को छोड़कर उ.रे. लेखापरीक्षा दल द्वारा दौरा किए गए स्थान

¹³⁴ मुम्बई सीएसटी/और मझगांव

¹³⁵ दिल्ली नियंत्रण कार्यालय, आनंद विहार, जम्मू तवी, अमृतसर की ट्रेन ब्रांच

¹³⁶ दिल्ली सराय रोहिल्ला, नई दिल्ली, दिल्ली, अम्बाला और मझगांव की ट्रेन ब्रांच

¹³⁸ अम्बाला, दिल्ली के नियंत्रण कार्यालय (कोचिंग सैक्शन), आनंद विहार, अम्बाला, जम्मू तवी, दिल्ली, दिल्ली सराय रोहिल्ला, अमृतसर, मझगांव यार्ड की ट्रेन ब्रांच

¹³⁹ आनंद विहार, दिल्ली सराय रोहिल्ला, दिल्ली, अम्बाला, जगाधरी कार्यशाला, सिक्ंदराबाद, विजयवाड़ा, गुंटकल, गुंटूर, मुम्बई सीएसटी, दादर टर्मिनल, मझगांव की ट्रेनिंग ब्रांच

¹⁴⁰ आनंद विहार, दिल्ली सराय रोहिल्ला, दिल्ली, अम्बाला, जगाधरी कार्यशाला, जम्मू तवी, अमृतसर, मुम्बई सीएसटी, दादर टर्मिनल, लोकमान्य तिलक टर्मिनल, मझगांव

द.म.रे. के गुंटुल में जल रिसाव की समस्या देखी गई थी जोकि सुगम आईसीएमएस प्रचालनों को प्रतिकूल रूप से प्रभावित कर सकती थी।

अतः आईटी सुरक्षा त्रुटिपूर्ण थी तथा प्रत्यक्ष एवं तर्कसंगत एक्सेस नियंत्रणों को सुदृढ़ करने की आवश्यकता थी परिवर्तन प्रबंधन का आईटी सर्वोत्तम पद्धतियों के अनुसार प्रलेखन नहीं किया गया था और कारबार निरंतरता योजना को अभी पूर्ण रूप से कार्यान्वित किया जाना था।

एक्जिट कॉन्फ्रेंस (अक्टूबर 2016) के दौरान रेलवे ने सहमति दी कि एक्सेस नियंत्रण एक दुर्बल क्षेत्र है और उन्हे इसको सुदृढ़ करने पर कार्य करने की आवश्यकता है। रेलवे बोर्ड लेखापरीक्षा अभ्युक्तियों पर भी सहमत था। लेखापरीक्षा सिफारिशों के संबंध में रेलवे बोर्ड ने बताया कि लेखापरीक्षा सिफारिशें उपयोगी है और प्रणाली को सुधारने के लिए रेलवे इन पर कार्य करेगी।