परिच्छेद- १
पृष्ठभूमि

१.१ परिचय

आन्तरिक राजस्व विभागले सीमा राजश्व बाहेकका राजश्वको संकलन र व्वस्थापनको लागि एकीकृत कर प्रणाली (Integrated Tax System, ITS) सञ्चालनमा ल्याएको छ । महालेखापरीक्षकको कार्यालयवाट उक्त प्रणालीको सूचना प्रविधि परीक्षण (IT Audit) गरी प्रारम्भिक प्रतिवेदन तयार पारिएको छ। यस प्रारम्भिक प्रतिवेदनमा विभागले सञ्चालनमा ल्याएको सूचना प्रविधि प्रणालीको सुरक्षित एवं व्यवस्थित प्रयोगको लागि अपनाइएको नियन्त्रण प्रणालीको अध्ययन, अनुगमन तथा मूल्यांकन समावेश गरिएको छ। सूचना प्रविधि परिक्षण गर्दा महालेखापरीक्षकको कार्यालयका कर्मचारीवाट (DFID/PFMA-2 वाट नियुक्त परामर्शदाताको सहयोगमा) मितिः २०७६।०८।१२ देखि २०७६।०८।३० सम्म विभागमा गई प्रणालीसँग सम्बन्धित महत्वपूर्ण कागजात एवं हार्डवेयर, सफ्टवेयर, नेटवर्क, जनशक्ति लगायतका महत्वपूर्ण पूर्वाधारको अध्ययन एवं निरिक्षण गरिएको थियो ।

१.२ सूचना प्रविधि लेखापरीक्षणको क्षेत्र र लेखापरीक्षणका विषयहरु

राष्ट्रिय विद्युतीय शासन गुरुयोजना (National E-Government Master Plan) ले सरकारी निकायहरुमा सञ्चालित सूचना प्रविधि प्रणाली (IT System) को लेखापरीक्षणका लागि विशेष जोड दिएको छ । आन्तरिक राजश्व विभागमा सञ्चालनमा रहेको कम्प्यूटर प्रणाली सरकारी निकायहरुवाट सञ्चालित सूचना प्रविधि प्रणाली मध्येको एक महत्वपूर्ण प्रणाली भएकोले गुरुयोजनाको कार्यान्वयनमा यसको महत्वपूर्ण भूमिका रहेको छ । प्रणालीको सफल कार्यान्वयनको लागि प्रविधिको माध्यमवाट गर्न सकिने सबै किसिमका कार्यहरु कम्प्यूटर प्रणालीमा आवद्ध गरी प्रणालीको सुरक्षित एवं भरपर्दो प्रयोग गर्न निश्चित मापदण्ड अनुरुपको नियन्त्रण प्रणाली लागू गर्नुपर्छ। नियन्त्रण प्रणालीमा सूचना प्रविधिको माध्यमवाट सम्पादन गरिने कार्यहरु, सूचना प्रविधि पूर्वाधार र कम्पनी प्रशासनको लागि सञ्चालित हार्डवेयर तथा सफ्टवेयर प्रणालीको सुरक्षासँग जोडिएका विषयहरु समावेश हुनुपर्छ । सूचना प्रविधि लेखापरीक्षणमा विशेषगरी प्रणालीसँग सम्बन्धित निम्न विषयहरुको अध्ययन, विश्लेषण गरी मूल्यांकन गरिन्छ ।

- सूचनाको विश्वसनीयता,
- सूचना प्रणाली प्रणालीको उपयुक्तता,
- सूचना प्रविधिको प्रयोग,
- सूचना तथा सञ्चार प्रविधि पूर्वाधार,

- दक्ष जनशक्तिको व्यवस्थापन,
- सफ्टवेयरको प्रभावकारिता,
- सूचना प्रविधि प्रणालीको सुरक्षित प्रयोग,
- सूचनाको गोपनीयता, विश्वसनीयता र निष्पक्षता,
- प्रणालीको उपलव्धता र निरन्तरता
- प्रणालीमा समय सापेक्ष गर्नुपर्ने सुधारका लागि आवश्यकता व्यवस्था

१.३ लेखापरीक्षणको उद्देश्य

सूचना प्रविधि प्रणालीलाई सुरक्षित एवं विश्वसनीय बनाउनका लागि अपनाईएको नियन्त्रण प्रणालीको अध्ययन, विष्लेषण एवं परीक्षण गरी सफ्टवेयरको माध्यमवाट प्रदान गरिने गुणस्तरीय सेवा सुविधा, सूचनाको विश्वसनीयता तथा प्रणालीको सुरक्षित प्रयोगको लागि अपनाईएको नियन्त्रण पद्धतिको बारेमा आश्वस्तता प्रदान गर्नु यस सूचना प्रविधि लेखापरीक्षणको मुख्य उद्देश्य रहेको छ । उल्लेखित उद्देश्य पूरा गर्ने गरी सूचना प्रविधि लेखापरीक्षणका कार्यक्षेत्रहरू निर्धारण गर्दा देहाय बमोजिमका सबै वा केही विषयमा आश्वस्तता प्रदान गर्ने प्रयत्न गरिएको छ।

- डाटा तथा सूचनाको विश्वसनीयता,
- प्रयोग भएको प्रणालीको उपयुक्तता,
- सूचना प्रविधिको सुरक्षित प्रयोग,
- सूचना तथा सञ्चार प्रविधि पूर्वाधार,
- दक्ष जनशक्तिको व्यवस्थापन,
- सफ्टवेयरको प्रभावकारिता,
- कम्प्यूटर प्रणालीको कार्यदक्षता,
- सूचना प्रणालीको निष्पक्षता र गोपनीयता,
- नियम कानूनको परिपालना,
- डाटा तथा प्रणालीको उपलब्धता र निरन्तरता

१.४ सूचना प्रविधि प्रणालीको संक्षिप्त व्यहोरा

आन्तरिक राजस्व विभाग सीमा राजश्व बाहेकका राजश्वको संकलन र व्वस्थापनको लागि गठन भएको केन्द्रीय विभाग हो । विभागले विद्युतीय माध्यमबाटै आयकर, मूल्य अभिवृद्धि कर तथा अन्तः शुल्कका विभिन्न आयामहरुको प्रशासन तथा अनुगमन गर्न विभिन्न समयमा विकास गरी लागु गरिएका सफ्टवेयर प्रणालीहरुको व्यवस्थापन र सञ्चालनमा रहेका जटिलतालाई घटाएर सरल र एकीकृत व्यवस्थापनको लागि निर्माण गरेको एकीकृत कर प्रणाली (Integrated Tax

System, ITS) आ.व. २०७०/७१ देखि सञ्चालनमा रहेको छ । वेबमा आधारित उक्त प्रणालीमा दुईवटा पोर्टल रहेका छन्। Officer Portal ले विभाग तथा कार्यालयमा कार्यरत कर्मचारीहरुले गर्नुपर्ने कार्यहरुको व्यवस्थापन गर्छ भने Taxpayer Portal ले करदाता तथा कर सहयोगीहरुले पेश गर्नुपर्ने विवरण विद्युतीय माध्यमबाट पेश गर्ने तथा आवश्यक परेको अवस्थामा सोही प्रणालीबाट प्राप्त गरी हेर्न सकिने गरी व्यवस्थापन गर्दछ । हालसम्म स्थायी लेखा नम्वर आवेदन दर्ताका साथै आयकर, अग्रिम करकट्टी विवरण, अनुमानित विवरण, मूल्य अभिवृद्धि कर, अन्तः शुल्क का नियमित कर विवरण विद्युतीय माध्यमबाटै इच्छुक करदाताहरुले पेश तथा रुजु समेत गर्नसक्ने व्यवस्था गरिएको छ । साथै यसमा इजाजत नवीकरण, स्टिकर व्यवस्थापन, विद्युतीय बिजक सफ्टवेयर सूचीकरण र राजश्व भुक्तानी समावेश छन् । आफूले तिर्नुपर्ने कर विद्युतीय माध्यमको प्रयोग गरी घरैबाट तिर्न मिल्ने गरी गत आ.व. देखि प्रणालीमा विस्तार गरिसकिएको छ । २०७५ असोज १ गतेदेखि एकीकृत करप्रणालीमै आवद्ध गरी लागु भएको उक्त प्रणाली अझ विस्तारित एवं व्यवस्थित हुने क्रममा रहेको छ । हालको लागि अधिकतम एक लाख रुपैयाँसम्म विद्युतीय भुक्तानी मार्फत् दाखिला गर्न सकिने र जतिसुकै राजश्व रकमको पनि बैंक भौचर Taxpayer Portal बाट भर्न सकिने व्यवस्था लागू गरिएका छन् । अधिकृत पोर्टल (Officer Portal), कर अधिकृतको प्रशासनिक र व्यवस्थापकीय कार्य गर्ने पोर्टल हो जसबाट प्रतिवेदन (Standard Report) तयार गर्ने व्यवस्था समेत रहेको छ। सफ्टवेयर प्रणालीको विकास मोड्युलर डिजाइन (Modular Design) मा गरिएकोले आवश्यकतानुसार उप-प्रणाली (Sub-System) थप गर्न सकिन्छ । सफ्टवेयरबाट नै डाटा तथा सूचनाको आदान प्रदान गर्न व्यावसायिक सम्बन्ध भएका अन्य सरकारी निकायहरु (जस्तैः भन्सार विभाग, कम्पनी रजिष्ट्रारको कार्यालय) को सफ्टवेयरसँग पहुँच (Access) कायम गर्न ITS मा Access Interface रहेको छ । करदाताका डाटा एवम सूचनालाई सुरक्षित एवं भरपर्दो रुपमा राख्नको लागि विभागले भवन परिसर भित्र आफ्नो छुट्टै डाटा सेन्टर र भैरहवामा डिजास्टर रिकभरी सेन्टर प्रयोगमा ल्याएको छ ।

विभागले Android भर्सनमा IRD Nepal नामक मोवाइल एप सञ्चालनमा ल्याएको छ। यसमा विभागका सूचना तथा सम्बन्धित ऐन कानूनको लिङ्क उपलब्ध गराउनुका साथै करदाता तथा कर प्रशासकहरुले आफ्नो युजरबाट लग अन गरी विभिन्न सूचना प्राप्त गर्न सक्ने व्यवस्था गरिएको छ । निकट भविष्यमै यसको IOS भर्सन समेत उपलब्ध गराउने विभागको योजना रहेको रहेको जानकारी प्राप्त भएको छ । SMS System को प्रयोग गरी करदाताले विभागमा उपलब्ध गराएका आधिकारिक मोवाइल नम्वरमा निजसँग सम्बन्धित सूचनाहरु सम्प्रेषण हुने व्यवस्था समेत मिलाइएको छ ।

१.५ सूचना प्रविधिको प्रयोगको लागि गरिएका नीतिगत तथा कानुनी व्यवस्था

१.५.१ कानुनी व्यवस्था

कानुनी व्यवस्था अन्तर्गत सूचना प्रविधि विधेयक (संसदमा छलफलमा रहेको), विद्युतीय कारोबार ऐन २०६३ तथा नियमावली २०६४, दुरसञ्चार ऐन, २०५३ रहेका छन् ।

१.५.२ नीतिगत व्यवस्था

सूचना तथा सञ्चार प्रविधि सम्बन्धी नीतिगत व्यवस्थाहरुमा सूचना तथा सञ्चार प्रविधि नीति २०७२, ब्रोडव्याण्ड नीति २०७१, दुरसञ्चार नीति २०६०, डिजिटल नेपाल फ्रेमवर्क २०७६, राष्ट्रिय विद्युतीय शासन गुरुयोजना, सरकारी निकायको वेबसाइट निर्माण तथा व्यवस्थापन सम्बन्धी निर्देशिका २०६८, नेपाल सरकार इन्टरप्राइज आर्किटेक्चर **(GEA),** नेपाल सरकारका सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिका २०७१, विद्युतीय खरिद प्रणाली सञ्चालन निर्देशिका, २०७४, आवधिक योजना आदि रहेका छन ।

सरकारका नीति तथा आवधिक योजनामा सूचना प्रविधिबाट प्राप्त हुने लाभांशको पहुँच ग्रामीणस्तरसम्म पुऱ्याउने, सूचना प्रविधिको माध्यमबाट गरिने सरकारी कामकाज र सेवा प्रवाहलाई प्रादेशिक तहसम्म विस्तार गर्ने, एकीकृत सूचना प्रविधि पूर्वाधारको विकास गरी एकरूपता र मितव्ययिता कायम गर्न सरकारी क्लाउड (Government Cloud) को सञ्चालन गर्ने, नेपाल सरकारका विभिन्न निकायहरूले सञ्चालनमा ल्याएका सूचना प्रविधि प्रणालीहरूमा एकरूपता कायम गर्ने, नेपाल सरकारका विभिन्न निकायका वेब साइटहरूलाई राष्ट्रिय पोर्टलमा आबद्ध गरी एकद्वार प्रणालीमार्फत सेवा प्रदान गर्ने, डाटा सेन्टर तथा डिजास्टर रिकभरी सेन्टर **(Data Center and Disaster Recovery Center)** को क्षमता अभिवृद्धि गर्ने लगायतका कार्यक्रमहरु उल्लेख गरिएको छ ।

१.६ लेखापरीक्षण विधि एवं प्रक्रिया

यस लेखापरीक्षण सम्पन्न गर्नको लागि निम्न बमोजिमका विधि एवं प्रक्रियाहरु अवलम्वन गरिएका छन् ।

१.६.१ सूचना संकलन

सूचना प्रविधि लेखापरीक्षण गर्नको लागि शुरुमा सम्बन्धित विभाग वा कार्यालयको बारेमा अध्ययन गरी आवश्यक डाटा एवं सूचना संकलन गर्नुपर्छ। यसको लागि विभागमा हाल भैरहेका क्रियाकलापहरु, प्रयोग भएका सफ्टवेयर, हार्डवेयर, नेटवर्क, डाटा सेन्टर, जारी गरिने प्रतिवेदन,

दैनिक कार्यसम्पादनसँग सम्बन्धित सूचना एवं आर्थिक कारोबार सम्बन्धी विवरणहरु संकलन गरिएको छ।

१.६.२ लेखापरीक्षण

महालेखापरीक्षकको कार्यालयवाट स्वीकृत योजना अनुसार लेखापरीक्षण सम्पन्न गर्न कार्यालयको सूचना प्रविधि (ICT) लेखापरीक्षण निर्देशिका अनुरुप कार्यक्रम, विधि र विस्तृत परीक्षण सूची तयार गरी टोली खटाइएको थियो।

१.६.३ प्रतिवेदन

लेखापरीक्षण सम्पन्न भएपछि सम्बन्धित विभाग, मन्त्रालयमा लेखापरीक्षणको प्रारम्भिक प्रतिवेदन उपलब्ध गराइनेछ र प्रतिवेदनका सम्वन्धमा जवाफ पेश गर्न कानूनले तोके बमोजिमको समय दिइनेछ। तोकिएको म्यादभित्र प्राप्त जवाफ समेत समावेश गरी अन्तिम प्रतिवेदन जारी गरिनेछ। प्रतिवेदनमा सम्भव भएसम्म सुझाव पेश गरिनेछ । प्रारम्भिक तथा अन्तिम प्रतिवेदनका मूख्य मूख्य वुँदाहरुलाई महालेखा परीक्षकको वार्षिक प्रतिवेदनमा समावेश गरिनेछ।

१.६.४ अनुगमन (Follow Up)

सूचना प्रविधि लेखापरीक्षणबाट दिइएका सुझाव कार्यान्वयन गर्ने जिम्मेवारी सम्बन्धित विभाग र मन्त्रालयको हुनेछ । सुझाव कार्यान्वयनको अवस्था कस्तो छ भन्ने सम्बन्धमा लेखापरीक्षण गरिएको विभाग वा कार्यालयको समय समयमा अनुगमन गरी आवश्यकता अनुसार सम्परीक्षण गरिनेछ ।

१.६.५ लेखापरीक्षण औजार (Audit Tools)

यस सूचना प्रविधि लेखापरीक्षणका मुख्य औजारका रूपमा लेखापरीक्षण गरिने निकायमा प्रयोग भएका सफ्टवेयर, हार्डवेयर, नेटवर्क, डाटा सेन्टर आदिको स्थलगत निरिक्षण र प्रणालीको व्यवस्थापन तथा सञ्चालन सम्बन्धी आधिकारिक दस्तावेज, प्रतिवेदन तथा सम्बन्धित अधिकारीहरुसँग गरिएका अध्ययन, छलफल एवं अन्तरक्रिया रहेका छन् ।

१.६.६ लेखापरीक्षण मानक र पद्धती (Audit Standards and Methodology)

सूचना प्रविधि लेखापरीक्षण सम्पन्न गर्न सर्वोच्च लेखापरीक्षण संस्थाहरूको अन्तर्राष्ट्रिय संगठन (INTOSAI), सर्वोच्च लेखापरीक्षण संस्थाहरूको एसियाली संगठन (ASOSAI) र Information Systems Audit and Control Association (ISACA) का मानक एवं सिद्धान्त लाई आधार लिइएको छ । लेखापरीक्षण योजनामा उल्लेखित विधि र प्रक्रिया अनुरुप लेखापरीक्षण गरिने निकायको सूचना प्रविधिजन्य वातावरणको अध्ययन पश्चात् सम्भावित जोखिमहरुको पहिचान गरी उपयुक्त

लेखापरीक्षण विधि अवलम्बन गरिएको छ । लेखापरीक्षणको क्रममा प्राप्त डाटा, सूचना, प्रतिवेदन लगायतका विवरणहरुको विश्वसनीयतामा आश्वस्त हुनको लागि कार्यालय प्रमुख, सूचना प्रविधि प्रणालीको व्यवस्थापन एवं सञ्चालनमा संलग्न प्राविधिक कर्मचारीहरु र सम्बन्धित अन्य पदाधिकारीहरुसँग छलफल एवं अन्तर्क्रिया गरी सूचना संकलन तथा विश्लेषण गरिएको र विभिन्न स्वरुपमा आधिकारिक दस्तावेजहरु माग गरी परीक्षण गरिएको थियो।

१.६.७ लेखापरीक्षणको सीमितता (Audit Limitations)

सूचना प्रविधि प्रणालीमा गरिने आन्तरिक नियन्त्रण र परीक्षणले धेरै हदसम्म प्रणालीको सुरक्षित प्रयोगमा सघाउ पुऱ्याउँछ तर शतप्रतिशत आश्वस्त गराउन सक्दैन। परीक्षण गरिने नमुनाको छनौट, मानवीय त्रुटि, प्राविधिक ज्ञानको कमी, सूचना प्रविधिको प्रयोगमा आउनसक्ने जटिलता एवं अनिश्चितता, पेशागत विवेकको प्रयोग, छोटो समयावधि, समयमै डाटा सूचना प्राप्त नहुनु, प्रणालीमा रहेका सबै किसिमका त्रुटी कमजोरी पत्ता नलाग्नु आदि कारणहरुले गर्दा लेखापरीक्षणमा अन्तर्निहित सीमितता रहन सक्छ ।

परिच्छेद- २

लेखापरीक्षण सारांश

२.१ सूचना प्रविधिको माध्यमवाट गरिने सेवा प्रवाह (IT Governance)

२.१.१ व्यावसायिक आवश्यकताको पहिचान, मार्गनिर्देशन र अनुगमन

क) मूल्यांकनका आधार

- विभागमा समय समयमा आउने व्यवसायिक तथा सूचना प्रविधिसँग सम्बन्धित नवीनतम सुधारका आवश्यकताहरुको पहिचान गर्न स्पष्ट विधि र प्रक्रिया हुनुपर्दछ । साथै पहिचान गरिएका आवश्यकताहरुको सम्बोधनको लागि निर्णय लिन अधिकार प्राप्त समिति वा पदाधिकारीसँग पर्याप्त सूचनाको उपलव्धता हुनुपर्दछ।
- कार्यसम्पादन मापनको स्पष्ट आधार तयार हुनुपर्दछ। अधिकार प्राप्त उच्चस्तरीय समितिले कार्यसम्पादनको वर्तमान अवस्थाको नियमित समीक्षा गरी सुधारको लागि प्रतिवेदन तयार गरी माथिल्लो तहमा पेश गर्नुपर्दछ । प्रतिवेदन स्वीकृत भएपछि मात्र समितिले नयाँ आवश्यकताको सम्बोधनको लागि कार्य शुरु गरी सोको नियमित अनुगमन गर्नुपर्दछ ।
- पहिचान गरिएका सुधारसँग सम्बन्धित सबै विषयहरु एकैपटक सम्बोधन गर्न नसकिने अवस्थामा तत्कालिन आवश्यकताको विश्लेषण गरी प्राथमिकीकरण गर्नुपर्दछ। सुधारका लागि उपलव्ध भएका प्रतिस्पर्धी विकल्पहरू बीच लाभ-लागत विश्लेषण गरी उपयुक्त विकल्प छनौट गर्नुपर्दछ।

ख) लेखापरीक्षणमा देखिएका विषयहरु

- विभागले आयकर ऐन, २०५८, मूल्य अभिवृद्धि कर ऐन, २०५२ र अन्तःशुल्क ऐन, २०५८ अनुसार आयकर, मु.अ. कर र अन्तःशुल्कको सङ्कलन तथा व्यवस्थापनको लागि सूचना प्रविधि प्रणालीको प्रयोग गरेको पाइयो।
- प्रणालीको कार्यसम्पादन मूल्यांकन गर्ने मापदण्ड तयार गरिएको छैन। प्रविधिको माध्यमवाट भैरहेको कार्यसम्पादनको आवधिक समीक्षा गरी व्यवस्थापनलाई नियमित प्रतिवेदन पेश गर्नका लागि छुट्टै सूचना तथा सञ्चार प्रविधि निर्देशक समिति गठन गरेको पाईएन।
- उप-महानिर्देशक (सूचना प्रविधि), निर्देशक (नीति विश्लेषण महाशाखा) र निर्देशक (करदाता सेवा कार्यालय) रहेको सूचना प्रविधि कोर समूह (IT Core Group) को गठन गरिएको छ । यस समूहले विभागवाट प्रदान गरिने सेवा सुविधालाई थप प्रभावकारी

बनाउन सूचना प्रविधि प्रणालीमा गर्नुपर्ने सुधारको सम्बन्धमा अध्ययन गरी सुझाब दिने गरेको पाईयो ।

ग) व्यवसायिक एवं प्रविधि सम्बन्धी आवश्यकताको पहिचान र अनुगमन नगर्दाको असर (Consequences)

- सूचना प्रविधि प्रणालीवाट भैरहेको कार्यसम्पादनको प्रभावकारी अनुगमन र नियन्त्रण विना प्रणालीमा भएका त्रुटि एवं कमजोरी र सुरक्षा सम्बन्धी जोखिमहरु पत्ता लगाई सुधार वा रोकथाम गर्न कठिन हुन्छ । साथै निर्देशक समिति नभएको अवस्थामा सूचना प्रविधिको माध्यमवाट हाँसिल गर्न खोजेको व्यवसायिक लक्ष्य तय गर्न, रणनीतिक र कार्यगत योजनाहरू तयार गरी लागू गर्न, सूचना प्रविधिसँग सम्बन्धित साधन श्रोतहरुको अधिकतम प्रयोग गरी व्यवसायिक आवश्यकताको समीक्षा गरी सम्बोधन गर्न तथा कार्यालयको कम्प्यूटर प्रणाली र डाटाको प्रभावकारिता एवं निरन्तरताको प्रत्याभूतिको लागि अपनाउनुपर्ने सुरक्षण नीतिहरू निर्धारण गरी सोको प्रभावकारी अनुगमन गर्न व्यवस्थापनलाई निकै कठिन हुन जान्छ।

घ) लेखापरीक्षणको सिफारिस

- विभागवाट हुने सेवा प्रवाह एवं प्रविधिसँग सम्बन्धित नवीनतम सुधारका आवश्यकताहरुको नियमित अनुगमन गरी कार्यान्वयन गर्नको लागि उच्चस्तरीय व्यवस्थापनले आवश्यक व्यवस्था मिलाउनुपर्दछ ।
- सूचना प्रविधि (हार्डवेयर, सफ्टवेयर, नेटवर्क, डाटा) को माध्यमवाट प्रवाह गरिने सेवा सुविधाको नियमित समीक्षा गरी उच्चस्तरीय व्यवस्थापन समक्ष प्रतिवेदन पेश गर्नुपर्छ । प्रतिवेदनमा प्रणालीलाई परिष्कृत गर्ने सम्बन्धमा कार्यालयवाट विभिन्न समयमा भएका निर्णय र अद्यावधिक गरिएका विषयहरु उल्लेख भएको हुनुपर्छ।
- सूचना प्रविधिको माध्यमवाट प्रवाह हुने सेवा सुविधाको नियमित समीक्षा गर्न र प्रणालीमा थप सुधार गर्नुपर्ने कार्यहरुको वारेमा व्यवस्थापन समक्ष प्रतिवेदन पेश गर्न विभागमा सूचना प्रविधि निर्देशक समिति गठन गर्नुपर्छ । सुधार गर्नुपर्ने भनी प्रतिवेदनमा उल्लेख भएका विषयहरुको स्वीकृती पश्चात कार्यान्वयनको लागि पहल गर्ने र सोको नियमित अनुगमन गर्ने जिम्मेवारी समितिको हुनुपर्छ ।
- हार्डवेयर, सफ्टवेयर र डाटालाई समेटी सूचना प्रविधि कार्य सम्पादन मापनहरु स्थापित गरी उच्च व्यवस्थापनलाई नियमित रूपमा प्रतिवेदन गरिनु पर्छ । उच्च व्यवस्थापनले विषयहरूको समाधानका लागि लिइएको निर्णय र गरिएका कार्यहरूको अभिलेख राख्नु पर्दछ।

- व्यवसाय र प्रविधि सम्बन्धी आवश्यकताको निरन्तर अनुगमन गरी सम्बोधन गर्न यस समूहको कार्य क्षेत्र विस्तार गर्नुपर्दछ । समूहमा अन्तिम प्रयोगकर्ता (End User) को प्रतिनिधित्व पनि हुनुपर्दछ ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१.२ सूचना प्रविधि रणनीति

क) मूल्याङ्कनका आधार

- विभागले आँफ्नो सूचना प्रविधि रणनीतिक योजना तयार गरेको हुनुपर्छ। रणनीतिक योजनाले विभागको व्यावसायिक उद्देश्यलाई सूचना प्रविधिको माध्यमवाट पूरा गर्नको लागि आवश्यक पर्ने हार्डवेयर, सफ्टवेयर, नेटवर्क लगायतका सूचना प्रविधि पूर्वाधारहरुको बारेमा स्पष्ट रुपमा उल्लेख गरिएको हुन्छ । यस किसिमको रणनीतिक योजनालाई समय समयमा पुनरावलोकन गरी अद्यावधिक गर्नुपर्दछ ।
- सूचना प्रविधि प्रणालीमा आउन सक्ने सम्भाव्य जोखिमहरुको पहिचान गरी न्यूनिकरण गर्न स्पष्ट नीति, योजना र साधनश्रोतको व्यवस्था गर्नुपर्दछ ।

ख) लेखापरीक्षणमा देखिएका विषयहरु

- विभागले २०१८-१९ देखि २०२२-२३ सम्मको ५ वर्षे दोस्रो रणनीतिक योजना तर्जुमा गरेको तर छुट्टै सूचना प्रविधि रणनीति वा विकास योजना तयार गरेको पाईएन। यद्यपि, दोस्रो रणनीतिक योजनाको रणनीति ४.४ (Optimised Full-Scale e-Governance System) ले सूचना प्रविधि सम्बन्धी केही विषयहरु समेटेको छ।
- जोखिम व्यवस्थापन सम्बन्धी नीति र योजना तयार गरिएको पाईएन। यद्यपि, रणनीतिक योजना कार्यान्वयनको सम्बन्धमा केही जोखिमहरू पहिचान गरिएको छ। जसमा सूचना प्रविधि प्रणाली तथा डाटाको कमजोर ब्याकअप प्रणाली र मर्मत संभारका साथै प्रणालीको आवधिक लेखापरीक्षण गर्ने, अन्तर्राष्ट्रिय मापदण्ड अनुरुप भएको प्रमाणपत्र (International Standard Certification) प्राप्त गर्ने र उच्चस्तरको सुरक्षा सञ्जाल स्थापना गर्ने जस्ता रणनीतिहरू उल्लेख गरिएको छ ।

ग) नीति, रणनीति तथा योजना नबनाई काम गर्दा आउने जोखिमहरु

सूचना प्रविधि नीति, रणनीति र योजनाको अभावमा प्रविधिको क्षमता र यसमा गरिएको लगानीको अधिकतम उपयोग हुन सक्दैन । विभागको व्यावसायिक मूल्य र मान्यतालाई दिगो रुपमा कायम राख्न सकिदैन । साथै जोखिम व्यवस्थापन नीति र योजनाको अभावमा पहिचान गरिएका

सम्भाव्य जोखिमहरूको न्यूनीकरण वा व्यवस्थापन भए नभएको जानकारी पाउन सकिदैन जसले गर्दा दुर्घटना भई ठूलो क्षति हुनसक्छ । (उदाहरणका लागिः System Hack, Server Crash, Data Corruption आदि)।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- विभागले व्यावसायिक र सूचना प्रविधिसँग सम्बन्धित नवीनतम सुधारका आवश्यकताहरूलाई पूरा गर्न दोश्रो रणनीतिक योजनालाई आधार मानि सूचना प्रविधि सम्बन्धी छुट्टै रणनीति र योजनाहरू तर्जुमा गरी कार्यान्वयन गर्नुपर्दछ।
- विभागले सूचना प्रविधि प्रणालीसँग सम्बन्धित सबै किसिमका साधन श्रोतहरुको सुरक्षित प्रयोगको लागि जोखिम व्यवस्थापन नीति र योजना तर्जुमा गरी कार्यान्वयन गर्नुपर्दछ ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१.३ सांगठनिक संरचना, नीति तथा कार्यविधि

क) मूल्याङ्कनका आधार (Criteria)

- विभागमा सूचना प्रविधिको भूमिका र जिम्मेवारीलाई उच्च प्राथमिकतामा राखि प्रविधिको माध्यमवाट सम्पादन गरिने कार्यहरुलाई स्पष्ट रुपमा परिभाषित गरिनुपर्दछ । साथै प्रमुख सूचना प्रविधि अधिकृतको नेतृत्वमा पर्याप्त दक्ष जनशक्ति सहितको सूचना प्रविधि निर्देशनालय वा महाशाखाको गठन गरी प्रविधिको सुरक्षित प्रयोगको लागि जिम्मेवार र उत्तरदायी बनाउनुपर्दछ ।
- कार्यालयको व्यावसायिक उद्देश्य अनुरुप सूचना प्रविधिको माध्यमवाट सेवा सुविधा प्रदान गर्नको लागि कार्यालयले उपयुक्त नीति तथा कार्यविधिहरु लागू गर्नुपर्दछ । नीतिहरुमा सूचना प्रविधि सुरक्षण नीति जसले प्रणालीको अनाधिकृत पहुँचलाई नियन्त्रण गर्छ, प्रणालीको नियमित सञ्चालन र विपद व्यवस्थापनको लागि उपयुक्त नीति तथा कार्ययोजना, सूचनाको गोपनियता, परामर्शदातावाट लिन सकिने कार्यहरु, हार्डवेयर, सफ्टवेयर, नेटवर्क, व्याकअप (Backup), रिमोट पहुँच (Remote Access), आपतकालिन उद्धार (Incedent Response), परिवर्तन व्यवस्थापन (Change Management), सूचना प्रविधि सम्बन्धी तालीम, प्रविधिको प्रयोगलाई स्वीकार्नुपर्ने लगायतका नीति तथा योजनाहरु हुनसक्छन् ।

ख) लेखापरीक्षणमा देखिएका विषयहरु (Audit Observation)

- सूचना प्रविधि व्यवस्थापन महाशाखाको प्रमुखमा उप-महानिर्देशकको व्यवस्था गरिएको छ।

- कार्यालयको व्यावसायिक उद्देश्य अनुरुप सूचना प्रविधिको माध्यमवाट सेवा सुविधा प्रदान गर्नको लागि आवश्यक पर्ने सूचना प्रविधि सुरक्षण नीति (जसले सूचना प्रविधि पूर्वाधारको सुरक्षा र प्रणालीको अनाधिकृत पहुँचलाई नियन्त्रण गर्छ), प्रणालीको नियमित सञ्चालन र विपद व्यवस्थापनको लागि उपयुक्त नीति तथा कार्ययोजना, सूचनाको गोपनियता, परामर्शदातावाट लिन सकिने कार्यहरु, हार्डवेयर, सफ्टवेयर, नेटवर्क, व्याकअप (Backup), रिमोट पहुँच (Remote Access), आपतकालिन उद्धार (Incident Response), परिवर्तन व्यवस्थापन (Change Management), सूचना प्रविधि सम्बन्धी तालीम, प्रविधिको प्रयोगलाई स्वीकार्नुपर्ने लगायतका नीति, योजना तथा कार्यविधिहरु तर्जुमा गरी लागू गरिएको छैन् ।

ग) सांगठनिक संरचना, नीति र कार्यविधिको अभावमा पर्नजाने असरहरु (सम्भाव्य जोखिमहरू)

कार्यालयवाट स्वीकृत भएका लिखित नीति, योजना तथा कार्यविधिहरु नहुँदा सूचना प्रविधि प्रणालीसँग सम्बन्धित हार्डवेयर, सफ्टवेयर, नेटवर्क, डाटा सेन्टर, जनशक्ति लगायतका पूर्वाधारहरुको प्रभावकारीरुपमा व्यवस्थापन एवं सञ्चालन गर्ने सम्बन्धमा स्पष्ट कार्यदिशाको अभाव हुन्छ । साथै समय समयमा गर्नुपर्ने सुधारात्मक कार्यहरुको लागि के गर्ने वा के नगर्ने भन्ने सम्बन्धमा अनिश्चितता वढाउँछ र सूचना प्रविधिको प्रभावकारिताको लागि अपनाउनुपर्ने व्यवस्थापकीय मापदण्डहरुको पालना हुन सक्दैन।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

कार्यालयको व्यावसायिक उद्देश्य अनुरुप सूचना प्रविधिको माध्यमवाट सेवा सुविधा प्रदान गर्नको लागि आवश्यक पर्ने माथि उल्लेखित नीति, योजना तथा कार्यविधिहरु तर्जुमा गरी, अधिकार प्राप्त अधिकारीवाट स्वीकृत गराई लागू गर्नुपर्छ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१.४ मानव संसाधन र स्रोतसाधन

क) मूल्याङ्कनका आधार (Criteria)

- कार्यालयको व्यावसायिक आवश्यकता (**Business Needs)** पूर्ति गर्नका लागि वर्तमान र भविष्यका आवश्यकतालाई सम्बोधन गर्ने जनशक्ति विकास योजना (**Human Resource Development Plan**) तयार हुनुपर्छ ।
- सूचना प्रविधिमा काम गर्न सक्ने दक्ष एवं अनुभवी कर्मचारीहरुको उपलव्धता सुनिश्चित गर्न तथा प्रणालीको सुरक्षित एवं व्यासायिक प्रयोगको लागि उपयुक्त जनशक्तिको विकास

र प्रयोग भएको सुनिश्चितताको लागि जनशक्ति विकास सम्बन्धी विस्तृत नीति तथा योजना लागू भएको हुनुपर्दछ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- सूचना प्रणाली व्यवस्थापन (MIS) शाखामा निर्देशक-१, कम्प्युटर इञ्जिनियर-२ र सूचना प्रविधि अधिकृत -४ तथा सूचना तथा सञ्चार प्रविधि (ICT) शाखामा निर्देशक-१, कम्प्युटर इञ्जिनियर-२, सूचना प्रविधि अधिकृत-४ पदहरू गरी जम्मा १५ पदहरु मध्ये केवल ५ जनाको मात्र पदपूर्ति भई बाँकी पदहरु रिक्त छन्।
- स्थायी सूचना प्रविधि कर्मचारीको निरन्तरता सुनिश्चित गर्न जनशक्ति विकास योजना तर्जुमा गरिएको छैन। कर्मचारीहरूबीच स्पष्ट कार्य विभाजन गरेको पाईएन।

ग) नियन्त्रण सुधार नसक्दाको परिणामहरू (सम्भावित जोखिम)

ग) जनशक्ति विकास योजना नहुँदा पर्न जाने असरहरु (सम्भाव्य जोखिमहरू)

जनशक्ति योजनाको अभावले सूचना प्रविधिको माध्यमवाट प्रदान गरिने सेवा सुविधाहरुलाई दिगो, प्रभावकारी एवं गुणस्तरीय बनाउन सकिदैन। जनशक्तिको अभाव र कार्य विभाजन स्पष्ट नहुँदा केही कर्मचारी तथा परामर्शदातामा प्रणाली एवं डाटाको अत्याधिक र अनाधिकृत पहुँच हुन गई महत्वपूर्ण र गोप्य राखिनुपर्ने डाटा वा सूचनाको चोरी, फेरवदल लगायतका अनुचित कार्यहरु हुने जोखिम बढी हुन्छ । साथै सिमित कर्मचारीहरूमा कामको बोझ बढ्न गई सेवाको गुणस्तरमा कमी आउँछ; केही कर्मचारीमा मात्र सफ्टवेयर प्रणाली निर्भर रहने र कर्मचारी सरुवा हुँदा प्रणालीको सञ्चालन एवं व्यवस्थापन नै प्रभावित हुन जान्छ ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- कार्यालयले अविलम्ब रिक्त दरवन्दीमा कर्मचारी नियुक्त गर्न उपयुक्त कदम चाल्नुपर्छ।
- सूचना प्रविधिको क्षेत्रमा काम गर्ने दक्ष जनशक्तिको व्यवस्थापनको लागि जनशक्ति विकास योजना निर्माण गरी कार्यान्वयन गर्नुपर्छ। लोक सेवा आयोगको सिफारिसमा नियुक्त हुने सूचना प्रविधिसँग सम्बन्धित दक्ष कर्मचारीहरूलाई स्पष्ट कार्यविवरण सहितको जिम्मेवारी तोकिनुपर्दछ । दक्ष कर्मचारीहरूलाई कार्यालयमा समर्पित भएर काम गर्ने (Dedicated) वातावरण मिलाउनुपर्दछ। परामर्शदातालाई कार्यालयका महत्वपूर्ण डाटा अथवा सूचना (Core Business) मा पहुँच हुने गरी काम गर्न दिनुहुँदैन ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१.५ २.१.५ तालिम तथा अभिमुखीकरण

क) मूल्याङ्कनका आधार (Criteria)

सूचना प्रविधिको क्षेत्रमा पछिल्लो समय देखिएका सुरक्षा चुनौतीहरु (जस्तैः सफ्टवेयर ह्याकिङ, सूचना प्रविधि प्रणालीमा अनाधिकृत पहुँच, डाटा तथा सूचनाको चोरी आदि) को सामना गर्न सूचना प्रविधिमा दक्ष कर्मचारीहरुलाई उच्चस्तरीय प्राविधिक प्रशिक्षण (High Level Technical Training) को व्यवस्था गर्नुपर्दछ । साथै सूचना प्रविधि प्रणालीमा काम गर्ने अन्य प्रयोगकर्ताहरुको ज्ञान र क्षमताको अभिवृद्धि गर्न विभिन्न तहका तालिमहरु प्रदान गर्नुपर्दछ। यसले कर्मचारीहरुलाई प्रविधिमा काम गर्न उत्प्रेरित गर्दछ र विज्ञ कर्मचारीहरुलाई कार्यालयमा टिकाइ राख्न (Retain) मद्दत गर्दछ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

चालू आ.व.को स्वीकृत वार्षिक कार्यक्रममा सूचना प्रविधिसंग सम्वन्धित विज्ञ कर्मचारी एवं प्रयोगकर्ताहरूको लागि तालिम सञ्चालन गर्न बजेट तथा कार्यक्रमको व्यवस्था गरेको पाइएन। साथै कर्मचारीहरूलाई डाटा एवं सूचनाको सुरक्षा तथा गोपनियता सम्वन्धी तालिम तथा सचेतना कार्यक्रमहरु सञ्चालन गरेको पनि देखिएन ।

ग) तालीम तथा अभिमुखिकरण कार्यक्रम नहुँदा पर्ने असरहरु (सम्भाव्य जोखिमहरू(

सूचना प्रविधिमा काम गर्ने दक्ष कर्मचारी एवं अन्य प्रयोगकर्ताहरुको लागि दिनुपर्ने विभिन्न तहका तालीम एवं प्रशिक्षण कार्यक्रमको अभावमा प्रणालीवाट गरिने कार्यहरु प्रभावकारी हुन नसक्नुका साथै माथि उल्लेखित सुरक्षा चुनौतीहरुको सामना गर्न सकिदैन । जसले गर्दा प्रणाली ह्याक हुने, डाटा तथा सूचनामा अनाधिकृत पहुँच हुने, महत्वपूर्ण एवं गोप्य राखिनुपर्ने डाटा एवं सूचनाको चोरी, फेरबदल वा चुहावट हुने हुन्छ । त्यसैगरी प्रयोगकर्तालाई दिनुपर्ने क्षमता अभिवृद्धि तालीम एवं डाटा सूचनाको सुरक्षित प्रयोग सम्बन्धी सचेतनाको अभावमा कर्मचारीहरुले सूचना प्रविधि प्रणालीमा राम्रोसँग काम गर्न नसक्नुका साथै डाटा एवं सूचनाको सुरक्षा संवेदनशीलताको बारेमा समेत जानकार हुँदैनन् र कार्यालय छोड्ने अथवा अन्य कार्यालयमा सर्ने (Transfer) सम्भावना बढ्छ ।

घ) लेखापरीक्षणका सुझावहरु (Recommendation)

विभागले तालीम तथा प्रशिक्षण सम्बन्धी कार्यक्रमको लागि स्वीकृत कार्ययोजना र पर्याप्त बजेटको व्यवस्था गरी माथि उल्लेख गरिए बमोजिमका उच्चस्तरीय एवं प्रयोगकर्ता तहका (High-Tech and User Level) तालीम तथा अभिमूखिकरण कार्यक्रमहरु नियमित रुपमा सञ्चालन गर्नपर्छ ।

कतिपय निकायहरुमा तालीम सञ्चालन भएता पनि प्रभावकारी हुन सकेका छैनन् । यसको लागि दक्ष एवं अनुभवी प्रशिक्षक र सम्पूर्ण पूर्वाधार भएको कम्प्यूटर प्रयोगशाला (IT Lab) को व्यवस्था गरी तालीम सञ्चालन गर्नुपर्छ । कर्मचारीले तालीम लिएर सूचना प्रविधि प्रणालीमा काम गर्ने व्यवस्था अनिवार्यरुपमा लागू गर्नुपर्दछ ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१.६ जोखिम विश्लेषण र अनुपालना

क) मूल्यांकनका आधार

विभागले सूचना प्रविधिको माध्यमवाट सेवा प्रवाह गर्दा आँफ्नो व्यवसायसँग सम्बन्धित सबै किसिमका कानून, नीति, नियम एवं विधि प्रक्रियाहरुको पूर्णरुपमा पालना भएको छ भन्ने सम्बन्धमा विश्वस्त हुनका लागि उपयुक्त संयन्त्रहरु (जस्तैः गुणस्तर परीक्षण समूह, आन्तरिक लेखापरीक्षण, स्थलगत निरिक्षण र चेकजाँच आदि) मार्फत परीक्षण गर्नुपर्छ ।

ख) लेखापरीक्षणमा देखिएका विषयहरु

सूचना प्रविधिको लागि छुट्टै गुणस्तर आश्वस्तता तथा कानून, नीति, नियमको अनुपालना भए नभएको सम्बन्धमा लेखापरीक्षण गर्न छुट्टै समूह नरहेको। सूचना प्रविधि सम्वन्धी जोखिमहरूको स्वतन्त्ररुपमा विश्लेषण र मूल्याङ्कन गरी सोको प्रतिवेदन उच्च व्यवस्थापन समक्ष पेश गर्ने गरेको पाइएन । कम्प्यूटर अपरेटरले आँफुले गरेको कामको आँफैले अनुगमन गर्ने गरेको देखियो ।

ग) जोखिम विश्लेषण र कानून एवं नीतिहरुको परिपालना नहुँदाका असरहरु (सम्भाव्य जोखिमहरू)

- सूचना प्रविधिजन्य जोखिमहरूको स्वतन्त्र रुपमा मूल्यांकन नहुँदा सम्भाव्य जोखिमहरूको पहिचान गर्न सकिदैन र जोखिम नियन्त्रणको लागि अपनाईएका प्रयासहरु पनि प्रभावकारी हुन सक्दैनन् । साथै व्यावसायिक अथवा प्रविधिको समय सापेक्ष आवश्यकताहरुको सम्बोधन गर्दा आउन सक्ने नयाँ किसिमका जोखिमहरुको पनि पहिचान गरी नियन्त्रण गर्न सकिदैन ।
- विभागको व्यावसायिक उद्देश्यसँग सम्बन्धित नीति नियमहरुको पूर्णरुपमा पालना भएको छ वा छैन भन्ने सम्बन्धमा स्वतन्त्र निकाय वा संयन्त्र मार्फत परीक्षण नगर्दा सामान्य प्रयोगकर्ता कर्मचारीमा निर्भर हुनुपर्छ । जसको कारण कार्यालयमा भैरहेका वा हुनसक्ने गलत क्रियाकलापहरु, सूचना प्रविधि प्रणालीमा आउन सक्ने चुनौतीहरु एवं गर्नुपर्ने सुधारका कार्यहरुको बारेमा व्यवस्थापन सचेत हुँदैन र दुर्घटना हुन सक्छ ।

घ) लेखापरीक्षणको सिफारिस

विभागले आँफ्नो व्यवसायसँग सम्बन्धित सबै किसिमका कानून, नीति, नियम एवं विधि र प्रक्रियाहरुको पूर्णरुपमा पालना गरेको छ भन्ने सम्बन्धमा स्वतन्त्र निकाय वा संयन्त्र मार्फत मूल्याङ्कन एवं परीक्षण गराई व्यवस्थापनलाई प्रतिवेदन पेश गर्ने व्यवस्था गर्नुपर्दछ । साथै नियमित रूपमा सूचना प्रविधि प्रणालीमा आउनसक्ने सम्भाव्य जोखिमहरुको पहिचान र मूल्यांकन गरी रोकथाम एवं नियन्त्रण गर्नुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.२ सूचना प्रविधिजन्य दुर्घटना तथा समस्याको व्यवस्थापन (Comptuter Security Incident and Problem Management)

२.२.१ सूचना प्रविधिको प्रयोगमा आउन सक्ने समस्या तथा दुर्घटनाहरुको व्यवस्थापन

क) मूल्याङ्कनका आधार (Criteria)

- समय समयमा आउन सक्ने सूचना प्रविधिजन्य दुर्घटना तथा समस्याहरुको (IT Incidents and Issues) न्यूनीकरणको लागि प्रविधिमा काम गर्ने दक्ष कर्मचारी तथा प्रयोगकर्ताहरुलाई विभिन्न माध्यमवाट (जस्तैः अनलाइन शिक्षा, सूचना प्रविधिको प्रयोगसँग सम्बन्धित जिज्ञासाहरुको प्रश्नोत्तर संगालो आदि) प्रशिक्षण गर्नुपर्दछ ।
- सूचना प्रविधिको प्रयोगमा आउने समस्याहरुको सम्बन्धमा ध्यानाकर्षण गराउन, अभिलेख राख्न तथा अध्ययन अनुसञ्धान एवं विश्लेषण गरी समस्याको समाधान गर्नको लागि निश्चित प्रक्रिया निर्धारण गर्नुपर्दछ र सोको जानकारी सबै प्रयोगकर्ताहरुलाई गराउनुपर्दछ।

ख) लेखापरीक्षणमा देखिएका विषयहरु (Audit Observation)

- प्रणालीको सुरक्षित प्रयोगमा देखिएका विषय र करदाताले चाँसो राखेका विषयहरुमा केही समानता देखिन्छ । यसले प्रणालीको सुरक्षासँग जोडिएका समस्याहरुको पहिचान गर्न सहयोग पुऱ्याउँछ। यसको लागि करदाताले उठाएका विषय तथा सुरक्षासँग सम्बन्धित अन्य विषयहरुको रिपोर्टिङ गर्न, समस्याको वास्तविक कारण पहिचान गर्न र स्थायी समाधान खोज्न दक्ष प्राविधिकहरु भएको संयन्त्र गठन गर्नुपर्छ।
- विभागले अन्तिम प्रयोगकर्ता (End User) लाई करदाता पोर्टलमा रिपोर्टिङ गर्न निम्नानुसारका सुविधाहरु उपलव्ध गराएको छ ।
  - क) टोल फ्रि नं (१६६ ०० १४ ००००)
  - ख) Hunting Line : (44 15 802)
  - ग) पृष्ठपोषण फाराम
  - घ) कल सेन्टर नम्बर (४४१९१११)

ङ) विभागको सहायता कक्ष (Help Desk) ले कार्यालय समयमा करदातालाई सल्लाह सेवा प्रदान गर्छ।

- कल सेन्टरको औचित्य सूचना प्रविधि सहायता समूह (IT Support Team) तथा विभागका अन्य कर्मचारीले जवाफ दिनुपर्ने कलहरूको संख्या कम गर्नु हो। यसका लागि कल सेन्टरका कर्मचारीहरूले नियमित हुने सोधपुछलाई समाधान गर्न सक्नुपर्छ। कल सेन्टर व्यवस्थापन गर्न AMEYU सफ्टवेयर प्रयोग गरिए तापनि हाल उक्त सफ्टवेयर सञ्चालनमा नरहेको र त्रुटिहरूको लग राखेको पाईएन; स्थायी सुधारको प्रयास प्रभावकारी देखिएन । विभागको सूचना तथा सञ्चार प्रविधि सम्बन्धी कार्यसञ्चालन कार्यविधि २०१४ मा बनाईएता पनि तत्पश्चात अद्यावधिक गरिएको छैन।

ग) सूचना प्रविधिजन्य दुर्घटनाहरुको व्यवस्थापन गर्न नसक्दाको असर (सम्भाव्य जोखिमहरू(

सूचना प्रविधिजन्य दुर्घटना तथा समस्याहरुको उचित व्यवस्थापन हुन नसक्दा कार्यालयको सूचना प्रविधि प्रणालीसँग सम्बन्धित सुरक्षाका महत्वपूर्ण विषयहरुलाई सम्बोधन गर्न सकिदैन। उदाहरणको लागि सूचना प्रविधि प्रणाली वा यसको सञ्चालनमा भएका त्रुटिहरुले गर्दा डाटा एवं सूचनाको चोरी हुने, फेरबदल हुने वा नष्ट हुने हुनसक्छ जसको समयमै व्यवस्थापन गर्न सकिदैन र ठुलो क्षति हुन जान्छ । समान किसिमका दोहोरिएर आइरहने समस्याहरुको गहिरिएर विश्लेषण वा अनुसञ्धान गरी वास्तविक कारण पहिचान नगर्दा बारम्बार आउने समस्याहरुले गर्दा कार्यसम्पादन प्रभावित हुन्छ ।

घ) लेखापरीक्षणका सुझाबहरु (Recommendation)

- सूचना प्रविधि प्रणालीको समग्र कार्यक्षमता एवं विश्वसनीयतामा वृद्धि गर्नको लागि प्रविधिको प्रयोगमा देखिएका समस्याहरूको वास्तविक कारण पहिचान गरी दीर्घकालिन रुपमा समाधान गरिनुपर्दछ र यसको लागि कार्यालयले समस्याहरुको व्यवस्थापन सम्बन्धी कार्यविधि (**Problem Management Procedure**) तर्जुमा गरी लागू गर्नुपर्छ ।
- प्रथम चरणमा कलहरु कल सेन्टर मार्फत व्यवस्थापन गराइनुपर्छ। सूचना प्रविधि कर्मचारीहरूको टेलिफोन नम्बर सजिलै उपलब्ध गराउनुहुँदैन।
- कार्यसञ्चालन कार्यविधिहरु (Standard Operting Procedure) अद्यावधिक गरिनुका साथै कल सेन्टरका कर्मचारीलाई प्रणालीको प्रयोग सम्बन्धी जिज्ञासाहरुको समाधान गर्न प्रशिक्षण दिनुपर्छ।

- विभागले पहिचान गरेका तथा जानकारीमा आएका समस्याहरूको दीर्घकालिन रुपमा समाधान गरी कम्प्युटर प्रणालीको कार्य सम्पादन र नियन्त्रणमा अपेक्षित परिणाम ल्याउनुपर्छ।
- प्रत्येक पटक आएका समस्या र समाधानको लागि अपनाईएको विधि एवं प्रक्रियाको बारेमा प्रयोगकर्तालाई जानकारी गराई सोको विस्तृत विवरण अनिवार्यरुपमा अभिलेख गरी राख्नु पर्दछ । यस किसिमको विवरण भविष्यमा आउने समस्याहरुको समाधानको लागि महत्वपूर्ण हुन्छ ।

२.३ परिवर्तन व्यवस्थापन (Change Management)

क) मूल्याङ्कनका आधार (Criteria)

- सूचना प्रविधि प्रणालीसँग सम्बन्धित हार्डवेयर, सफ्टवेयर, नेटवर्क लगायतका उपकरणहरुको मर्मत संभार तथा प्रणालीको व्यवस्थापन एवं सञ्चालनको लागि अपनाईएका विधि, प्रक्रिया एवं प्रविधिको माध्यमवाट प्रदान गरिने सेवा सुविधाहरुमा कुनै किसिमको सुधार वा परिमार्जन गर्नुपरेमा औपचारिक प्रक्रिया (**Formal Change Management Procedure**) द्वारा गर्नुपर्दछ । यस अन्तर्गत सुधारको लागि माग गर्ने (**Request for Change**), बर्गिकरण गर्ने, परिणामको विश्लेषण र मूल्यांकन गर्ने, कार्य अगाडी वढाउनको लागि स्वीकृत दिने, डिजाईन गर्ने, निर्माण गर्ने, चेकजाँच गर्ने र कार्यान्वयनमा ल्याउने लगायतका सबै क्रियाकलापहरु स्पष्टरुपमा उल्लेख गरेको हुनुपर्दछ ।
- प्रणालीमा कुनै किसिमको परिवर्तन गर्दा यसको कार्यक्षमतामा पर्नसक्ने असरको बारेमा गहिरिएर विश्लेषण गर्नुपर्छ ।
- आकस्मिक रुपमा कुनै परिमार्जन वा सुधार गर्न आवश्यक भएमा सोको परीक्षण गर्ने, अभिलेखीकरण गर्ने, मूल्याङ्कन गर्ने र स्वीकृत गरी कार्यान्वयन गर्ने छुट्टै प्रक्रिया निर्धारण गर्नुपर्छ । यस्तो अवस्थामा नियमित रुपमा गरिने सुधार प्रक्रियाको अनुशरण गरिदैन।
- प्रणालीमा गरिएका सवै प्रकारका सुधार एवं परिवर्तनको अभिलेखीकरण, वर्गीकरण, प्राथमिकीकरण र परिणामको मूल्यांकन गर्नको लागि उपयुक्त Tracking System को व्यवस्था गर्नुपर्दछ। सबै किसिमका परिवर्तनहरुलाई प्रयोगकर्ताले स्वीकार्नुपर्ने भएकोले सोको लागि परीक्षण (User Acceptance Test) गरिनुपर्दछ र यसको सफल परीक्षण पछि मात्र पुर्ण रूपमा कार्यान्वयन गर्न स्वीकृति दिनु पर्दछ । परिवर्तन वा सुधारको लागि

गरिएका मागहरुको समिक्षा गर्न, स्वीकृती दिन र परिवर्तन भएका विषयहरुलाई सञ्चालनमा आउनुपूर्व आवश्यक चेकजाँच गरी स्वीकृत गर्न एक 'Change Approval Board' गठन गरिनुपर्दछ।

- सूचना प्रविधि प्रणालीमा भएका सुधार एवं परिवर्तनका सम्बन्धमा प्रयोगकर्ताहरूलाई पूर्णरुपमा जानकारी गराउनुपर्दछ तथा प्रणाली एवं प्रणालीसँग सम्बन्धित दस्तावेजहरुमा सोही वमोजिम अद्यावधिक गरिनुपर्दछ।
- कार्यालयले सूचना प्रविधि प्रणालीको विकास, डाटा **Migration,** परिमार्जन एवं परीक्षण लगायतका क्रियाकलापहरु प्रणाली सञ्चालनमा रहेको (**Live Environment**) वातावरण भन्दा छुट्टै वातावरणमा गर्नुपर्दछ । प्रणाली विकास र प्रणाली सञ्चालन (**System Development and System Running**) का वीचमा कुनै किसिमको पहुँच (**Both Physical and Logical Access**) हुन नदिन कडा किसिमले नियमन गरिएको हुनुपर्छ । सफ्टवेयर प्रणाली विकास गर्ने, गुणस्तर एवं कार्यालयको आवश्यकता बमोजिम भए नभएको चेकजाँच गर्ने र प्रणालीको सञ्चालन गर्ने वातावरण छुट्टाछुट्टै हुनुपर्दछ। साथै एउटा वातावरणमा काम गरेको प्राविधिक जनशक्तिले अर्को वातावरणमा काम गर्नुहुँदैन । प्रयोगकर्ताहरुले संचालनमा रहेको सफ्टवेयर प्रणाली (**Live System**) मा मात्रै काम गर्नुपर्दछ ।

ख) लेखापरीक्षणमा देखिएका विषयहरु (Audit Observation)

- प्रणालीमा गर्नुपर्ने सुधार एवं परिवर्तन व्यवस्थापनका लागि कुनै मापदण्ड वा लिखित प्रक्रियाहरू निर्धारण गरेको पाईएन।
- प्रणालीमा कुनै किसिमको परिवर्तन गर्दा पर्ने प्रभावको मूल्यांकन एवं विश्लेषण गरी सोको अभिलेख राख्ने गरिएको छैन।
- आकस्मिक रुपमा गर्नुपर्ने कुनै किसिमको सुधार वा परिवर्तनको लागि छुट्टै प्रक्रिया निर्धारण गरेको देखिएन। तत्कालको आवश्यकता सम्बोधन गर्ने गरी (**AD-hoc Manner**) गरेको पाईयो । सेवा प्रदायक (**Consultant**) ले प्रणालीमा परिवर्तन (**Update**) गरेपछि सोको बारेमा व्यवस्थापनलाई मौखिक रूपमा जानकारी गराउने गरेको पाइयो। आकस्मिक रुपमा गरिएका सुधार एवं परिवर्तनहरुको अभिलेख राख्ने गरेको पाइएन।
- प्रणालीमा भए गरेका सुधार एवं परिवर्तनहरुको अभिलेखिकरण, वर्गीकरण, प्राथमिकीकरण एवं प्रभाव मूल्यांकनका लागि कुनै Tracking System रहेको पाइएन। प्रयोगकर्ताले परिवर्तनलाई स्वीकार गरेको परीक्षण (User Acceptance Test, UAT) को लिखित

प्रतिवेदन पेश नभएकोले **UAT** गरिएको पुष्टि गर्न सकिएन। सुधार गर्नुपर्ने मागको समीक्षा गर्न, सुधारको लागि स्वीकृती दिन र चेकजाँच गरी सञ्चालनमा ल्याउने अनुमति दिनको लागि Change Approval Board गठन गरिएको छैन।

- नयाँ मोड्युल प्रयोगमा ल्याउनु (**Live**) अघि परीक्षण वातावरण (Test Environment) मा परीक्षण गरिन्छ। सञ्चालन गर्नुपूर्व नीति विश्लेषण तथा व्यवस्थापन महाशाखाले प्रणालीमा भएका सुधार वा परिवर्तनहरुको समीक्षा गरी स्वीकृति दिनुपर्छ ।

ग) परिवर्तन व्यवस्थापन गर्न नसक्दाका असर (सम्भाव्य जोखिमहरू)

प्रणालीमा गर्नुपर्ने परिवर्तन सम्बन्धी विषयहरुको उचित व्यवस्थापन कार्यविधि नहुँदा सुधार गर्नुपर्ने सबै विषयहरु समेट्न सकिदैन। अनाधिकृत परिवर्तनहरु हुन सक्छन्। साथै सफ्टवेयर प्रणालीमा गरिएका सुधारका कार्यहरु (Update /Upgrade) को राम्रोसँग परीक्षण (Test) नगरी सञ्चालनमा ल्याएको अवस्थामा विभिन्न किसिमका त्रुटि एवं समस्याहरु देखापर्न सक्छन्। सुधार गरिएका विषयहरुको UAT नगर्दा प्रयोगकर्ताहरूको आवश्यकतालाई सम्बोधन गरे नगरेको एकीन गर्न सकिदैन।

घ) लेखापरीक्षणका सुझाबहरु (Recommendation)

- विभागले सूचना प्रविधि प्रणालीमा गर्नुपर्ने सुधार एवं परिवर्तनको लागि गरिने सम्पूर्ण कार्यहरुको लागि निश्चित विधि र प्रक्रियाहरू तर्जुमा गरी लागू गर्नुपर्दछ।
- आकस्मिक रुपमा गर्नुपर्ने कार्यहरुको लागि बाह्य सेवा प्रदायकलाई प्रणालीमा सिधा पहुँच उपलब्ध गराउनुपर्ने भएमा कार्यालयले आँफ्ना कर्मचारी र परामर्शदाता बीच कार्य विभाजन गरी जोखिम व्यवस्थापन गर्नुपर्दछ।

२.४ व्यवसाय निरन्तरता नीति (BCP)/(प्रकोप पुनःस्थापना योजना) DRP(

क) मूल्याङ्कनका आधार

- विभागले सूचना प्रविधिको माध्यमवाट प्रदान गर्ने सेवा सुविधामा कुनै किसिमको रोकावट हुन नदिई प्रणालीको निरन्तर सञ्चालनको व्यवस्था मिलाउनको लागि आवश्यक **Business Continuity Policy** बनाई लागू गर्नुपर्दछ । आकस्मिक वा अन्य कुनै कारण विशेषले (जस्तैः विद्युत आपुर्ती नहुनु, ईन्टरनेटमा समस्या आउनु आदि) केही समयको लागि कम्प्यूटर प्रणाली सञ्चालन हुन नसक्ने भएमा सोको लागि प्रणालीको सुरक्षित प्रयोगको लागि अपनाईएको नियन्त्रण प्रणालीमा कुनै असर नपर्ने गरी वैकल्पिक व्यवस्था गर्नुपर्दछ ।

- विभागले सूचना प्रविधि प्रणाली सञ्चालनका लागि सेटअप गरिएका सर्भर, डाटा स्टोरेज, नेटवर्क लगायतका उपकरणहरु राखिएको डाटा सेन्टरमा कुनै पनि बेला भुकम्प, बाढी जस्ता ठूला प्रकोपहरु (**Disaster**) आउन सक्छन् । जसले गर्दा महत्वपूर्ण डाटा, सूचना लगायत सम्पूर्ण प्रणालीनै नष्ट (**Lost**) हुनसक्ने भएकोले यसवाट बचाउनको लागि Disaster Recovery **Plan** सहितको नीति कार्यान्वयन गर्नुपर्दछ । जसले प्रकोपको कारण सम्पूर्ण प्रणालीमा अवरोध आएको खण्डमा छिटो र सुरक्षित तवरले प्रणाली एवं डाटालाई उक्त डाटा सेन्टर भन्दा टाढा रहेको **Disaster Recovery Center** मा सेटअप गरिएका सर्भर, स्टोरेजवाट पुन:स्थापना गर्न सहयोग पुऱ्याउँछ ।

- **Business Continuity Plan** र **Disaster Recovery Plan** को लागि बाह्य सेवा प्रदायक (**Consultant**) नियुक्त गरिएको भए सेवा प्रदायकसँग व्यवसायिक निरन्तरता र विपद् व्यवस्थापनको लागि विभागको आवश्यकता अनुरुप कार्य गर्ने गरी सेवा करार गर्नुपर्छ ।

- विपद् वा अन्य कुनै कारणले डाटा सेन्टरमा डाटा नष्ट भएको अवस्थामा कार्यालयले वैकल्पिक व्याकअप (Backup) को व्यवस्था गरेको हुनुपर्दछ । जसबाट नष्ट भएको वा समस्या आएको डाटालाई पुनः स्थापित **(Restore)** गर्न सकिन्छ ।

ख) लेखापरीक्षणमा देखिएका विषयहरु

बिभागको डाटासेन्टर विभाग रहेको भवन परिसरमा र त्यसको वैकल्पिक डाटा सेन्टर GIDC सिंहदरबारमा तथा विपद् व्यवस्थापन केन्द्र (**DRP**) भैरहवामा राखिएको छ। GIDC मा प्रकोप पुनः स्थापना सम्बन्धी व्यवस्था (Disaster Recovery Arrangements) परीक्षण गर्दा डाटा सेन्टरको तापक्रम २६ डिग्री सेल्सियसमा राखिएको (२०-२४ डिग्री हुनुपर्ने) पाइयो । तापमान र आर्द्रताको मापन गरिएको थिएन ।काठको टेबल, तेल र ग्रीज जस्ता प्रज्वलनशील वस्तुहरू डाटा

सेन्टरमा देखिएका थिए। सर्भर कोठाको अग्नि नियन्त्रण यन्त्रको म्याद २०७४.११.१४ मा समाप्त भएको पाइयो ।

ब्याकअप मिडियाको पर्याप्त मात्रामा नियन्त्रण गरिएको छैन। लेखापरिक्षणको क्रममा डाटा ब्याकअपको बाह्य हार्ड डिस्कमा ५ जना स्टाफलाई पहुँच प्रदान गरिएको पाइयो। ब्याकअप मिडियाको पूर्णरुपमा नियन्त्रण गर्न निति तर्जुमा गरी अभिलेखिकरण गर्नुपर्छ ।

ग) BCP र DRP नहुँदाको असर (सम्भाव्य जोखिमहरू(

Business Continuity Plan र **Disaster Recovery Plan** नहुँदा विभागवाट सम्पादन हुने नियमित कार्यहरुमा अवरोध भएमा विभाग वा कार्यालयले प्रवाह गर्ने महत्वपूर्ण सेवा सुविधाहरु प्रभावित हुन जान्छन् । कुनै कारणले प्रणाली एवं डाटामा समस्या आएमा समयमै पुनःस्थापना गर्न नसकिने वा कठिन हुने हुन्छ जसले गर्दा महत्वपूर्ण डाटा एवं तथ्यांकहरु नष्ट हुने, अनाधिकृत तवरले हेरफेर हुने वा चोरी हुने सम्भाबना बढ्छ । साथै आवश्यक तयारी नहुँदा कम्प्युटर प्रणालीको उपलव्धता नभएको अवस्थामा विभागका नियमित कार्यहरु सुचारु गर्न सकिदैन् ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- कार्यालयले कम्प्युटर प्रणालीको निरन्तर प्रयोगमा आउन सक्ने जोखिमहरुको न्यूनीकरणका लागि **Business Continuity Plan** र **Disaster Recovery Plan** तर्जुमा गरी लागू गर्नुपर्दछ।
- कार्यालयले **एप्लिकेशन र डाटाको सुरक्षाको लागि** GIDC सँग सुरक्षा तथा सेवाको गुणस्तरको सम्बन्धमा लिखित सम्झौता गर्नुपर्छ। साथै सम्झौतामा **BCP** र **DRP** सँग सम्बन्धित विषयहरुलाई प्रष्टसँग उल्लेख गरेको हुनुपर्छ ।
- विभागको Data Center **मा** Dual Factor Authentication लागू गर्नुपर्छ, दुइवटा ढोका राखिनुपर्छ, स्वचालित अग्नि नियन्त्रण उपकरण जडान गरिनुपर्छ, छतको उचाइ पर्याप्त हुनुपर्छ, कर्मचारी निरन्तर खटाइनुपर्छ, उपयुक्त किसिमले तार विच्छ्याइनु पर्छ, ओसिलो भित्ताको मर्मत गर्नुपर्छ र निषेध गरिएका वस्तुहरु जस्तै खाना, पेय पदार्थ, धूम्रपान निषेध आदि संकेतहरु राख्नुपर्छ। डाटा सेन्टरको नियमित रुपमा परीक्षण गर्नुपर्छ। हिंस्रक जनावर र कीट नियन्त्रणको व्यवस्था गर्नुपर्छ ।
- भैरहवामा भएको डाटा सेन्टरको छुट्टै लेखापरीक्षण गर्नुपर्छ।
- हार्ड ड्राइभमा भएको ब्याकअपको गतिविधिको लग (Log) राख्नुपर्छ ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.५ डाटा तथा सूचनाको सुरक्षा (Information Security)

२.५.१ डाटा एवं सूचनाको सुरक्षा सम्बन्धी जोखिम मुल्यांकन

क) मूल्याङ्कनका आधार

- विभागमा डाटा एवं सूचनाको सुरक्षा सम्बन्धी जोखिमको मूल्यांकन गर्ने प्रभावकारी संयन्त्र हुनुपर्छ ।
- जोखिम मूल्यांकन प्रक्रिया पर्याप्त सूचनामा आधारित हुनुपर्दछ । यसले विभागको आन्तरिक एवं बाह्य वातावरणको अध्ययन अनुसञ्धान एवं विश्लेषण गरी महत्वपूर्ण जोखिमहरूको पहिचान र मूल्यांकन गर्नुपर्दछ। डाटा एवं सूचनाको सुरक्षा सम्बन्धी पहिचान गरिएका जोखिमहरुको रोकथाम गर्न वा दीर्घकालिन रुपमा समाधान गर्न निश्चित प्रक्रिया निर्धारण गरेको हुनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा

विभागसँग लिखित रुपमा सूचना सुरक्षा सम्बन्धी जोखिम मूल्यांकन गर्ने संयन्त्र रहेको देखिएन। जसले गर्दा जोखिमहरुको व्यवस्थापन गर्ने संयन्त्र र विधि प्रक्रियाहरू कार्यान्वयन भएको पाइएन।

ग) सूचना सुरक्षा सम्बन्धी जोखिम व्यवस्थापन नगर्दाको असर (सम्भाव्य जोखिमहरू(

सूचना सुरक्षा सम्बन्धी जोखिम मूल्यांकन र व्यवस्थापनको अभावमा कार्यालयले सुचना सुरक्षा (Data Security) मा देखिएका कमजोरी एवं खतराहरूवाट हुन सक्ने दुर्घघटनाहरू पहिचान गर्न र रोकथामका उपायहरू अवलम्बन गर्न सक्दैन् ।

घ) लेखापरीक्षणको सिफारिस

विभागले व्यवस्थित र नियमित रूपमा सूचना सुरक्षा सम्बन्धी जोखिमहरुको विश्लेषण र मूल्याङ्कन गर्ने व्यवस्था गर्नुपर्दछ।

ङ) व्यवस्थापनको जवाफ

२.५.२ सूचना सुरक्षा नीति

क) मूल्याङ्कनका आधार

- विभागले सूचना सुरक्षा नीति तर्जुमा गरी लागू गरेको हुनुपर्दछ, जसले प्रणालीको व्यवस्थापन तथा सञ्चालनमा आउनसक्ने जोखिमहरूलाई न्यनूनिकरण गर्नुका साथै महत्वपूर्ण व्यावसायिक सूचनाहरूलाई नष्ट हुन वा दुरुपयोग हुनवाट जोगाउँदछ ।

- सूचना सुरक्षाका लागि जिम्मेवार बनाउन यससँग सम्बन्धित प्राविधिक एवं अन्य कर्मचारी र सेवा प्रदायकको भूमिका, जिम्मेवारी र कार्य विवरण स्पष्टरुपमा उल्लेख गरेको हुनुपर्दछ ।

ख) लेखापरीक्षणका व्यहोरा

कार्यालयले सूचना सुरक्षा नीति तयार गरेको पाईएन। डाटा एवं सूचना सुरक्षाको लागि कर्मचारी एवं सेवाप्रदायकको भूमिका र जिम्मेवारी तोकेको पाईएन।

ग) सूचना सुरक्षा नीति नहुँदाका असर (सम्भाव्य जोखिमहरू)

सूचना सुरक्षा (Data Security) सम्बन्धी जोखिमहरू पहिचान गर्न सकिदैन। महत्वपूर्ण र संवेदनशील डाटा एवं सूचनाहरू नष्ट हुन वा दुरुपयोग हुन सक्छन्।

घ) लेखापरीक्षणको सिफारिस

- सञ्चार तथा सूचना प्रविधि मन्त्रालय वा सूचना प्रविधि विभागसँगको सहकार्यमा स्थापित मापदण्ड अनुरुप कार्यालयका सूचनाको सुरक्षा सम्बन्धी विषयलाई समेटी सूचना सुरक्षा नीति तयार गरी लागू गर्नुपर्छ।
- कर्मचारीहरूको कार्य विवरणमा स्पष्ट रूपमा सूचना सुरक्षा सम्वन्धी भूमिका र जिम्मेवारी तोकिनुपर्छ।

ङ) व्यवस्थापनको जवाफ

२.५.३ प्रणालीको सुरक्षामा दक्ष जनशक्तिको प्रयोग

क) मूल्यांकनका आधार

- सूचना प्रविधिका दक्ष एवं प्रयोगकर्ता कर्मचारीहरुलाई प्रणाली एवं डाटाको सुरक्षित प्रयोग सम्बन्धी कर्तव्य र जिम्मेवारीका बारेमा पूर्णरुपमा जानकार गराउनुपर्दछ ।
- कर्मचारीसँग आँफ्नो कर्तव्य र जिम्मेवारीलाई पूर्णरुपमा पालना गर्नको लागि उपयुक्त सीप र दक्षता हुनुपर्छ।
- महत्वपूर्ण र संवेदनशील डाटा एवं सूचनामा पहुँच भएका कर्मचारीहरूको पृष्ठभूमि चेकजाँच गरी (Background Checks) र सुरक्षाको विषयमा आश्वस्त (Security Clearance) हुनुपर्छ ।

ख) लेखापरीक्षणका व्यहोरा

- कर्मचारीको भूमिका र जिम्मेवारीलाई स्पष्टसँग परिभाषित गरिएको कुनै लिखित दस्तावेज छैन।
- सूचना प्रविधि प्रणालीको विकास र सञ्चालनमा खटिएका दक्ष कर्मचारी तथा सेवा प्रदायक (**Consultant**) को क्षमता र कार्यकुशलता पर्याप्त छ वा छैन भन्ने सम्बन्धमा चेकजाँच गर्ने कुनै मापदण्ड तय गरिएको पाईएन।
- सूचना सुरक्षा सम्वन्धि पर्याप्त तालिमको अभाव रहेको छ। कम्प्युटर प्रणाली सुरक्षित हुनका लागि **Physical, Logical, Technical** र प्रशासकीय नियन्त्रणको सन्तुलित संयोजन गरेको हुनुपर्दछ। **Physical and Logical Securities** जति नै मजबुत भए तापनि कमजोर सुरक्षा अभ्यास (**User Security Practices**) ले यसलाई कमजोर पार्न सक्छन् । (जस्तैः प्रयोगकर्ताको युजरनेम र पासवर्ड (**Username and Password**) एक अर्का बीच आदान प्रदान गर्दा प्रणालीको सुरक्षामा जटिलता आउँछ ।
- कर्मचारीको पृष्ठभूमि जाँच (**Background Checks**) गर्ने व्यवस्था सुदृढ गर्नुपर्ने देखिन्छ। स्थायी कर्मचारीहरूको पृष्ठभूमि जाँच लोकसेवा आयोगद्वारा गरिन्छ। कार्यालयले सेवा प्रदायकद्वारा खटाईएका कर्मचारीहरुको पृष्ठभूमि जाँच गरेको पाइएन । साथै यदि सेवा प्रदायक स्वयंले पृष्ठभूमि जाँच गरेको भए सोको प्रतिवेदन माग गरिएको छैन। वाह्य सेवा प्रदायकसँगको सम्झौता अनुसार **Core Business** को लागि आँफ्ना कर्मचारी र **Supporting Business** को लागि परामर्शदाताको सुचि तयार गरी अनुमोदन गर्नुपर्नेमा त्यस्तो गरेको पाइएन।

ग) दक्ष जनशक्तिको प्रयोगमा नियन्त्रण नगर्दाको असर (सम्भाव्य जोखिमहरू(

डाटाको स्वामित्व हुने (Data Owner), हेरविचार गर्ने (Data Custodians) र प्रयोगकर्ताहरूलाई दिईने सुरक्षा सम्बन्धी तालीम पर्याप्त नहुँदा सुरक्षा नियमको उल्लंघन भई डाटामा अनधिकृत पहुँच र हेरफेर हुने जोखिम बढन जान्छ ।

घ) लेखापरीक्षणको सिफारिस

- प्रणाली एवं डाटाको सुरक्षाको लागि कार्यालयले Data Owner, Data Custodian र डाटा प्रयोगकर्ताको भूमिका र जिम्मेवारीलाई स्पष्टरुपमा परिभाषित गरी लिखित अभिलेख राख्नुपर्दछ र सो सम्बन्धमा सबैलाई जानकारी गराउनुपर्दछ।
- विभागले कर्मचारीलाई उनीहरूको सुरक्षा जिम्मेवारी सम्बन्धी तालीम दिनुपर्छ।

- कार्यालयले स्थायी कर्मचारी र सेवा प्रदायकको पृष्ठभूमि जाँच गर्नुपर्दछ। कार्यालयका कर्मचारीलाई Core Business को र सेवा प्रदायकलाई Supporting Business को कार्य गर्न दिनुपर्छ ।

ङ) व्यवस्थापनको जवाफ

२.५.४ गोप्य सूचनाको संरक्षण

क) मूल्याङ्कनका आधार

- सूचनाको सुरक्षा र गोपनीयताको लागि कार्यालयमा आवश्यकता अनुसार कर्मचारी एवं सेवा प्रदायकसँग सम्झौता गरेको हुनुपर्दछ।
- बाह्य सेवा प्रदायक (जस्तैः उपकरणहरुको मर्मत संभार गर्ने, सफ्टवेयर आपूर्तिकर्ता आदि) को पहुँचमा रहेका डाटा एवं सूचनाको सुरक्षा एवं गोपनियताको पूर्ण प्रत्याभूतिको लागि आवश्यक व्यवस्था मिलाउनुपर्दछ ।

ख) लेखापरीक्षणमा देखिएका विषयहरु

- गोप्य राख्नुपर्ने सूचनाको संरक्षण गर्न आवश्यक नीति तयार गरेको पाईएन। साथै गोपनीयताको स्तरअनुसार तथ्यांकको वर्गीकरण गरिएको छैन।
- सम्झौताका शर्त बमोजिम सेवा प्रदायकद्वारा गोपनीयता कायम राखिनुपर्छ भन्ने उल्लेख गरिएको छ । यद्यपि, तीनवटा सेवा प्रदायकहरूसँग गरिएको सम्झौताको गोपनीयता खण्डमा "सम्झौताको म्याद सकिएपछि २ बर्षको लागी मान्य छ" भन्ने उल्लेख गरिएको छ। साथै तीन वटै सेवा प्रदायकसँग गरिएको सम्झौताले तिनका कर्मचारिहरुलाई कार्य सम्पादन गर्न निर्बाध रुपमा पहुँच प्रदान गर्ने उल्लेख गरिएको छ, जसका कारण अनाधिकृत पहुँच भई गोपनियता भङ्ग हुन सक्छ ।

ग) गोप्य सूचनाको संरक्षण गर्न नसक्दाको असर (सम्भाव्य जोखिमहरू(

विद्यमान व्यवस्थाले गोप्य तथ्यांकमा हुनसक्ने अनाधिकृत पहुँचको जोखिमलाई पूर्ण रूपमा नियन्त्रण र व्यवस्थापन गर्न सक्दैन।

घ) लेखापरीक्षणको सिफारिस

- कार्यालयले गोप्य सूचनाको सुरक्षाको लागि नीति तर्जुमा गरी लागू गर्नुपर्दछ। सर्वप्रथम, डाटा एवं सूचनाको संवेदनशीलता र गोपनीयतालाई लाई बिचार गरेर सूचनाको वर्गीकरण

गर्नुपर्दछ। सबै डाटालाई गर्नुपर्ने सुरक्षाको न्यूनतमस्तर कायम गरी बढी संवेदनशील र गोपनीय तथ्यांकको लागि थप नियन्त्रण प्रणाली लागू गर्नुपर्दछ।

- भविष्यमा हुने सम्झौता वा विद्यमान सम्झौताको गोपनीयताको खण्डमा संशोधन गरी अनन्त कालसम्म गोपनीयता कायम राख्नुपर्ने शर्तहरू लागू गरिनुपर्दछ।
- सूचना प्रविधि सुरक्षा नीति लागू हुनासाथ सोही अनुरुप हुने गरी सम्झौतामा समेत आवश्यक संशोधन गरी सेवा प्रदायकलाई समेत सोको पालना गराउनुपर्छ।

ङ) व्यवस्थापनको जवाफ

२.६ सञ्चार र सञ्जाल (Communication and Network)

२.६.१ सुरक्षा प्याच (Security Patches)

क) मूल्याङ्कनका आधार

सूचना प्रविधि प्रणालीसँग सम्बन्धित सफ्टवेयर एप्लिकेशन तथा डाटाबेसको सुरक्षा गर्न ठाउँ ठाउँमा **Security Patches** (समस्याको पहिचान र समाधानको लागि राखिने **Supporting Words**) हरू राख्नुपर्दछ ।

ख) लेखापरीक्षणका व्यहोरा

कार्यालयले Patch व्यवस्थापन नीति तथा प्रक्रिया निर्धारण गरेको छैन। प्याच व्यवस्थापनको लागि कर्मचारीको भूमिका तोकिएको छैन। सुरक्षा Patch व्यवस्थापन आवश्यकताको आधारमा तदर्थ रूपमा गरेको पाईयो। लागू गरिएका सुरक्षा Patch को अभिलेख (Log) राखेको देखिएन। वैकल्पिक फायरवाल नभएको कारणले पनि सुरक्षा प्याच सेटअप लगाइएको छैन ।

ग) सुरक्षा प्याच प्रयोग गर्न नसक्दाको असर (सम्भाव्य जोखिमहरू(

पछिल्लो समय विकास भएका Security Patches लागू गर्न नसक्दा प्रणाली Hack भई डाटामा अनाधिकृत पहुँच हुने, Data हेरफेर हुनसक्ने तथा समग्र सफ्टवेयर प्रणालीनै अवरुद्ध हुने जोखिम बढाउँछ।

घ) लेखापरीक्षणको सिफारिस

- विभागले सुरक्षा प्याच (Security Patch) व्यवस्थापन नीति तयार गर्नुपर्छ । यसमा कर्मचारीको भूमिका निर्धारण गरी कार्यान्वयन गर्नुपर्छ।
- व्यवस्थापनले हाल सञ्चालित अपरेटिङ सिस्टम, सफ्टवेयर एप्लिकेशन र डाटावेश नयाँ **भर्सन** (New Version) मा छन् वा छैनन् यकीन गरी पुरानो भर्सन (**Old Version**) मा भए हुनसक्ने कमजोरी र जोखिमहरुको मूल्यांकन गरी रोकथाम गर्नुपर्दछ।

ङ) व्यवस्थापनको जवाफ

२.६.२ नेटवर्क कन्फिगरेसन (Network Configuration)

क) मूल्याङ्कनका आधार (Criteria)

व्यवसायिक डाटा एवं सूचनाको सुरक्षण गर्न उपयुक्त नेटवर्क विभाजन गरेको हुनुपर्छ ।

ख) लेखापरीक्षणका व्यहोरा

- कर कार्यालयहरू मध्ये १३ वटा कर कार्यालयलाई इन्ट्रानेट लाइन २ (**L2)** मार्फत जडान गरिएको छ। अन्य कर कार्यालयहरूलाई ईन्टरनेट सेवा प्रदायकबाट **Static IP Address** मार्फत जडान गरिएको छ। नेटवर्क सञ्चार गर्दा **SSL Encryption** को प्रयोग गरिएको छ ।
- विभागमा नेटवर्क विभाजन (LAN Segregation) लाई सुधार गर्नुपर्ने देखिन्छ। सुचना प्रविधि शाखा र डाटा सेन्टर एउटै नेटवर्कमा रहेका छन्। अन्य कार्यालयहरूसँग ईन्टरनेटको माध्यमवाट जडान गर्दा VPN गरेको पाइएन।

ग) नियन्त्रणमा सुधार गर्न नसक्दाको असर (सम्भाव्य जोखिमहरू)

नेटवर्क विभाजन नहुँदा डाटा सेन्टर नेटवर्कमा अत्यधिक पहुँच हुनसक्छ। ईन्टरनेट मार्फत एप्लिकेशनको प्रयोगमा VPN नगर्दा नेटवर्क सञ्चार असुरक्षित हुनसक्छ ।

घ) लेखापरीक्षणको सिफारिस

कार्यालयले नेटवर्क विभाजन (LAN segregation) मा सुधार गर्नुपर्छ जसले गर्दा तोकिएका IP Address वाट मात्र डाटा सेन्टर नेटवर्कमा पहुँच हुने व्यवस्था गर्न सकिन्छ । ईन्ट्रानेटको प्रयोग गर्न नसकेको अवस्थामा VPN को प्रयोग गर्नुपर्छ।

ङ) व्यवस्थापनको जवाफ

२.६.३ एन्टिभाइरस / एन्टिमालवेयर (Anti – Malware) को सेटअप

क) मूल्याङ्कनका आधार (Criteria)

सूचना प्रविधि प्रणालीलाई बाह्य जोखिमवाट वचाउन उपयुक्त एन्टिमालवेयर / एन्टिभाइरस सफ्टवेयरको प्रयोग गर्नुपर्छ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

ESET ३२ एन्टिभाइरस सफ्टवेयर (0७-03-2020 सम्म मान्य (Valid) रहेको) सेटअप गरिएको छ। यसले डेस्कटप PC र सर्भरहरूको सुरक्षा गर्छ। सफ्टवेयर स्वतः अद्यावधिक हुन्छ।

ग) एन्टिभाइरस / एन्टिमालवेयरको प्रयोग नगर्दा हुने असर (सम्भावित जोखिम)

सूचना प्रविधिको प्रयोगमा सक्रिय हुनसक्ने खराब एप्लिकेशन (Malwares) हरुले प्रणालीसँग सम्बन्धित उपकरण, सफ्टवेयर र डाटालाई नष्ट वा हेरफेर गर्न सक्छन् ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

एन्टिमालवेयर / एन्टिभाइरस सफ्टवेयरको प्रयोगलाई निरन्तरता दिनुपर्छ ।

२.६.३ Intrusion पत्ता लगाई रोकथाम गर्न फायरवाल (Firewall) को प्रयोग गर्ने

क) मूल्याङ्कनका आधार (Criteria)

सफ्टवेयर प्रणालीको सुरक्षाको लागि प्रणालीमा हुनसक्ने Intrusion पत्ता लगाई सोको रोकथाम गर्न फायरवाल उपकरण वा एप्लिकेशन सेटअप गर्नुपर्छ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- कार्यालयमा फायरवाल नीति/मार्गदर्शन छैन।
- **Intrusion Detection System** फायरवालहरूमा सक्रिय गरिएको छैन।
- हाल निम्ना बमोजिमका दुईवटा फायरवालहरू प्रयोगमा रहेका छन् ।
    - Firewall 1: Juniper SRX firewall (IRD-WALL) – JunOS 12.1 X44-D30.4
    - Firewall 2: SRX (IRD-SRX-WALL 2) – JUNOS 12.1X44-D35.5
- लेखापरीक्षणको क्रममा धेरै कमजोरीहरू पहिचान गरिएको छ।

ग) फायरवालको प्रयोग नगर्दाको असर (सम्भावित जोखिम)

फायरवालको उपयुक्त सेटअप गर्न नसक्दा जानकारीमा भएका र पहिचान गर्न सकिने Malicious Attacks वाट नेटवर्कलाई बचाउन सकिदैन।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

फायरवाल कन्फिगरेसन मजबुत गरिनुका साथै निम्न सुधारात्मक कदम चालिनुपर्छः

- Loopback Address को प्याकेट Claim गरी कुनै नेटवर्क वा फायरवालवाट भित्र जान खोज्ने प्याकेटहरूलाई ब्लक गर्न फायरवाल फिल्टरहरू राखिनुपर्छ (Firewall filters be established to block any attempt from the firewall or any network to pass any packets claiming to be from a loopback address) ।
- पहुँच नियन्त्रण (Access Control) गर्न र प्रयोगकर्ताहरुको केन्द्रीय रूपमा (Centrally) व्यवस्थापन गर्न छुट्टै AAA सर्भर सेटअप गरी फायरवाललाई प्रमाणित (Authenticate)

गरिनुपर्छ (A separate AAA server be introduced to authenticate the firewall(s), this will make it easier to control permissions and manage users centrally)।

- फायरवाल नियमहरू (Rules) समय सापेक्ष अद्यावधिक गरिनुपर्छ।
- आवश्यकता अनुसार फायरवालको अनुगमन गर्न र Configure गर्न कर्मचारी खटाइनुपर्छ।

२.६.४ डाटा एवं सूचनाको सुरक्षा लागि Configuration Management

क) मूल्याङ्कनका आधार (Criteria)

सूचना प्रविधि प्रणालीको प्रयोग एवं डाटाको सञ्चार गर्दा डाटा एवं सूचनाको सुरक्षाको लागि स्पष्ट एवं सुव्यवस्थित (Clear and Well-Managed) Configuration System हुनुपर्छ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- प्रणाली एवं डाटाको प्रयोग र सञ्चार गर्दा अपनाउनुपर्ने सूचना सुरक्षा सम्बन्धी नीति तयार गरिएको छैन।
- ठूला करदाता कार्यालयमा ईन्टरनेटको दोहोरो लाइन जडान गरेको तर दुबै लाइनहरु एउटै सेवा प्रदायक र समान बिन्दुबाट जडान भएको पाइयो।
- ठूला करदाता कार्यालयमा नेटवर्क सम्बन्धी उपकरणहरूको लागि पर्याप्त पावर-ब्याकअपको व्यवस्था गरिएको छैन। यसकारण विद्युत कटौतीको समयमा उपकरणहरू सञ्चालन गर्न जेनेरेटरमा निर्भर रहेको पाइयो। उच्च भोल्टेजका कारण उपकरणमा हुनसक्ने क्षतिलाई न्यूनीकरण गर्न यूपीएस वा पावर कन्ट्रोल उपकरण (Stabilizer) को प्रयोग गरेको पाईएन।

ग) नियन्त्रण सुधार नसक्दाको परिणामहरू (सम्भावित जोखिम)

आन्तरिक नीति, निर्देशन र निगरानी बिना लागू गरिएको सुरक्षा प्रणालीले विभाग वा कार्यालयको आवश्यकतालाई पूरा गर्न सक्दैनन् । प्रणाली एवं डाटामा क्षति हुनसक्छ ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

पहिलो र दोस्रो प्राथमिकताका ईन्टरनेट सेवा जडान गर्दा फरक फरक ISP तथा फरक फरक बिन्दु (Internet Access Point) बाट जडान गरिनुपर्छ।

२.७ सूचना प्रविधिजन्य साधनश्रोत (सूचना प्रविधि सम्पत्ति) को व्यवस्थापन

क) मूल्याङ्कनका आधार (Criteria)

- सूचना प्रविधि सम्बन्धी सबै किसिमका साधनश्रोत (हाडवेयर, सफ्टवेयर, नेटवर्क, डाटा, लिखित दस्तावेज आदी) हरुको अभिलेख राखिनुपर्छ।
- कुनैपनि उपकरणहरुको बिक्री तथा लिलामीको लागि आवश्यक अख्तियारी हुनुपर्दछ।
- आवश्यक नभएका उपकरणहरु सुरक्षित तवरले बिक्री गरिनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- सूचना प्रविधि सम्पत्ति प्रतिस्थापन योजना तर्जुमा गरिएको छ जसमा सूचना प्रविधि उपकरणहरूको विस्तृत सूची समावेश गरिएको छ।
- सूचना प्रविधि सम्बन्धी उपकरणहरुको लिलाम गर्नुभन्दा पहिले सुरक्षित तवरले सम्पूर्ण डाटा धुल्याएको सुनिश्चित गर्ने व्यवस्था गरेको पाइएन।
- महत्वपूर्ण सर्भर तथा सफ्टवेयरको प्रयोग गर्दा आधिकारिक अनुमतिपत्र (License) लिएको पाइएनः

क. लाइसेन्स नलिएका DC Server:

Ref. No.	Model Name	OS
1	Dell Power Edge 2900	WINDOWS SERVER 2008 R2 STANDARD x64
2	Dell Power Edge 2950	Windows Server 2008 R2 Enterprise x64
3	Dell Power Edge 2950	Windows Server 2008 R2 Enterprise x64
4	Dell Power Edge 2950	**Faulty**

5	Dell Power Edge1950	WINDOWS SERVER 2008 R2 STANDARD x64
6	Dell Power Edge1950	**Faulty**
7	Dell PowerEdge 820	VMware vSphere 5.5
8	HpProliant DL580	VMware vSphere 5.5

ख. लाइसेन्स नलिएका सफ्टवेयरः

S.N.	Software	Quantity	Use	Procurement Year
1	Oracle Database with RAC	4	ITS Database	2076
2	VMware VSphere/Vcenter	8	For creation and operation of 22 virtual machines in two physical servers	2076
3	Microsoft Windows Server 2012	40	For 19 virtual machines running on Windows	2076
4	Microsoft Office 2016	100	For Microsoft Office package for computer and Laptop running in IRD	2076
5	Microsoft Active Directory	100 cal	For active directory management of computer and Laptop running in IRD	2076
6	IRedAdmin Email Server	300 users	For Email server of IRD with 300 users	2076

ग. लाइसेन्स नलिएका फायरवालः

S.N	Brand	Model Name	Serial No.	OS
1	Juniper	SSG350	JN119785AADE	screen os
2	Juniper	SSG350	JN119867CADE	screen os
3	Juniper	SRX-550	AL2414AK0041	JUNOS Software Release [12.1X44-D30.4]
4	Juniper	SRX-	AL4914AK0124	JUNOS Software Release [12.1X44-D30.4]

		550		

ग) असर (सम्भावित जोखिम)

सामान्यतया उत्पादकले इजाजतपत्र बिनाको उपकरण र सफ्टवेयरलाई स्वीकार गर्दैन। परिणाम स्वरुप प्रतिलिपि अधिकारको उल्लंघन सम्बन्धी कानूनी कारबाही हुनसक्छ। प्राविधिकरुपमा पनि ईजाजतपत्र विनाका सफ्टवेयरमा समस्या आउनसक्छ ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- सबै सूचना प्रविधि प्रणाली उपकरण र सफ्टवेयरको आधिकारिक अनुमतिपत्र (License) लागि लाइसेन्स प्राप्त गर्नुपर्छ।
- हार्डवेयर पुनः जडान वा लिलामी गर्नुभन्दा पहिले डाटा सुरक्षित रूपमा धुल्याउनुपर्छ।

२.८ भौतिक सुरक्षा

क) मूल्याङ्कनका आधार (Criteria)

- भवन परिसर र सूचना प्रविधि क्षेत्रमा हुने पहुँच न्यायोचित, अधिकारिक, अभिलेख (**Log**) राखिएको र अनुगमन गरिएको हुनुपर्छ। यो विषय परिसरमा प्रवेश गर्ने सबै व्यक्तिहरू जस्तैः स्थायी र अस्थाई दुवै कर्मचारी, सेवा प्रदायक, सेवा ग्राही, आगन्तुक वा तेस्रो पक्ष सबैमा लागू हुनुपर्छ ।
- अनाधिकृत व्यक्तिले हेर्न र प्रयोग गर्न नसक्ने गरी संवेदनशील डाटा एवं सूचनाको प्रयोग हुने स्थानहरुलाई सुरक्षित गराउनुपर्छ।
- सम्भव भएसम्म आगो, बाढी, भूकम्प, विस्फोट, हुलदङ्गा र प्राकृतिक वा मानवीय कारणले हुनजाने विपत् वा यस्तै प्रकारका अन्य क्षतिहरू हुन नदिन भौतिक सुरक्षाको राम्रो व्यवस्था गरिनुपर्छ।
- सूचना वा सूचना प्रसोधन गर्ने उपकरणहरू (**Data and Data Processing Equipment**) भएका स्थानलाई सुरक्षा घेरा भित्र राखिनुपर्दछ।
- अनधिकृत व्यक्ति प्रवेश गर्न सक्ने स्थानहरु (**Doors**) लाई नियन्त्रण गरिनुपर्छ। सम्भव भएसम्म अनधिकृत पहुँचबाट बच्न सूचना प्रशोधन कार्य (**Data Processing Service**) लाई छुट्टै र केही दुरीमा राखिनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- विभागको डाटा सेन्टरमा वातावरणीय नियन्त्रणको मूल्यांकन खण्ड २.४ मा समावेश गरेको पाइयो।
- विभागका प्रमुख गेटहरूमा पहरा दिएको पाइयो। आगन्तुकहरूको अभिलेख राख्ने गरेको पाईएन। यसलाई सुधार गर्नुपर्ने देखिन्छ।
- विभागमा प्रयोगकर्ताले काम गर्ने टर्मिनलहरू (कम्प्युटरमा पहुँच प्रदान गर्ने किवोर्ड, माउस र स्क्रिन) सुरक्षित रूपमा राखेको पाइएन। यसवाट अनाधिकृत व्यक्तिले तथ्यांक चोरी गर्न सक्छन्।
- अनुगमन र निगरानीका लागि सि.सि. क्यामेरा जडान गरिएको छ।
- लेखापरीक्षण क्रममा विभागको केन्द्रीय कार्यालयमा अवस्थित डाटा सेन्टरको स्थलगत निरिक्षण गर्दा निम्न अनुसारको अवस्था देखियो :
    - डाटा सेन्टर आगन्तुक अभिलेख राखेको पाइएन,
    - दोहोरो प्रमाणीकरण (Doul Factor Authentication) लागू गरिएको छैन,
    - डाटा सेन्टरमा प्रवेश निषेध गरिएको, खाना, पेय, र धूमपान निषेध गरिएको जस्ता संकेतहरु उल्लेख गरेको पाईएन,
    - ढोका अग्नि प्रतिरोधक छैन। डाटा सेन्टरमा एउटा मात्र ढोका रहेको छ;
    - स्वचालित अग्नि नियन्त्रण उपकरण जडान गरिएको पाइएन,
    - ताप फैलावट (Heat Dispersal) को लागि छतको उचाइ पर्याप्त छैन,
    - रातको समयमा डाटा सेन्टरको रेखदेखका लागि सेन्टरको प्रवेश कार्ड इलेक्ट्रिसियनलाई हस्तान्तरण गर्ने गरेको पाइयो। चमेना गृहको कर्मचारीलाई पनि डाटा सेन्टरमा पहुँच भएको पाइयो,
    - प्लास्टिक जस्ता प्रज्वलनशील वस्तुहरू डाटा सेन्टर कोठामा भएको पाइयो,
    - वातानुकूलक (Air Conditioner) सुविधा स्वचालित नभई Mannually गर्नुपर्ने पाइयो,
    - उपकरण जडान गरिएका तारहरु अव्यवस्थित र लेबल (Lebel) नगरेको पाइयो,
    - भित्ता ओसिलो भएको पाइयो,
    - डाटा सेन्टरको परीक्षण नियमित रुपमा गरिएको छैन,
    - कर्मचारीको ड्युटी रोस्टर (Duty Roster) डाटा सेन्टरमा राखेको पाइएन,
    - हिंस्रक जिव र कीट नियन्त्रणका लागि अवश्यक व्यवस्था गरेको पाइएन,

- डाटा सेन्टरमा १०० mbps लाइन १०० mbps राउटरसँग जडान गरिएकाले ब्याण्डविड्थको पूर्ण उपयोग नहुने देखिन्छ।

ग) नियन्त्रण सुधार नसक्दाको परिणामहरू (सम्भावित जोखिम)

भौतिक सुरक्षाको कमजोर व्यवस्थापन तथा नियन्त्रणले विभागको सम्पत्ति, डाटा र गोपनीयता मा नोक्सानी पुऱ्याउन सक्छ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- विभाग परिसरमा प्रवेश गर्ने व्यक्तिको अभिलेख राखिनुपर्छ।
- गोप्य तथ्यांक प्रशोधन (Sensitive Data Manipulation) गर्ने टर्मिनलहरूको स्क्रिन अनाधिकृत व्यक्तिले नदेख्ने गरी राख्नुपर्दछ ।
- विभागको डाटा सेन्टरमा वातावरणीय नियन्त्रणलाई सुदृढ पार्नुपर्छ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.९ पहुँच नियन्त्रण (Access Control)

२.९.१ सूचना प्रविधि पहुँच नीति

क) मूल्याङ्कनका आधार (Criteria)

कर्मचारीको कार्य विवरण अनुसार मात्र प्रणालीमा पहुँच सुनिश्चित गर्नको लागि पहुँच नियन्त्रण सम्बन्धमा स्पष्ट नीति हुनुपर्छ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

विभागमा प्रणालीको पहुँच नीति वा प्रक्रियाको अभिलेख राखिएको छैन। करदाता बाहेक सूचना प्रविधि प्रणालीमा निम्नलाई अनुमति दिइएको छः

- कर अधिकृत (अफिसर पोर्टल मार्फत)
- भन्सार विभाग (प्यान सूचना र आयात/निर्यात डाटा)
- कम्पनी रजिष्टारको कार्यालय (For PAN Reservation)
- महालेखा नियन्त्रक कार्यालय
- राजस्व सूचना व्यवस्थापन प्रणाली
- राजस्व अनुसन्धान विभाग
- नेपाल चार्टर्ड एकाउन्टेन्ट्स संस्था
- राष्ट्रिय सूचना प्रविधि केन्द्र, GIDC
- वाणिज्य बैंकहरू (ऋण प्रशोधनका लागि)

प्रणालीमा लग इन गर्न पासवर्ड आवश्यक हुन्छ तर दुई फ्याक्टर अथेन्टिकेसन (Two Factor Authentication) अनिवार्य छैन। कर्मचारीलाई भूमिकामा आधारित (Role Based) कार्य विवरण तोकिएको छ।

ग) पहुँच नियन्त्रण नहुँदाका असर (सम्भावित जोखिम)

अनधिकृत व्यक्तिको प्रणालीमा पहुँच बढ्न सक्छ । आधिकारिक व्यक्तिले पनि चाहिनेभन्दा बढी पहुँच पाउन सक्छन्। यी दुवैको कारणले तथ्यांकको गोपनीयता र Intigrity जोखिममा पर्न सक्छ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

Access Control Policy तयार गरी लागु गर्नुपर्छ। विभिन्न तहका कर्मचारीलाई दिईने सबै किसिमका पहुँच (Access) हरू स्वीकृत गरी कार्य विवरणमा तोकेको र आवश्यक पर्ने पहुँच मात्र प्रदान गरिनुपर्छ ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.९.२ नियुक्ति, सरुवा र अवकाश

क) मूल्याङ्कनका आधार (Criteria)

- नयाँ कर्मचारी नियुक्ति वा पदस्थापन हुँदा शुरुमै अभिलेख राख्ने, स्वीकृत गर्ने र प्रणालीमा पहुँच दिने गर्नुपर्छ।
- कर्मचारी सरुवा भएर जाँदा साविकमा दिइएको पहुँचलाई हटाएर मात्र रमाना दिनुपर्छ । सरुवा भएर आउँदा माथिल्लो तहको निर्देशन लिएर मात्र अभिलेख राखि आवश्यकता बमोजिम बढी अधिकार नहुने गरी प्रणालीमा पहुँच दिनुपर्छ ।
- अवकाश हुने कर्मचारीहरूको पहुँच अधिकार पुनः सक्रिय गर्न नमिल्ने गरी निष्क्रिय गर्नुपर्दछ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- कर कार्यालयमा नयाँ प्रयोगकर्ता सिर्जना गर्दा केन्द्रीय कार्यालयको सूचना प्रविधि सहायता एकाई (IT Support Unit) ले गर्ने गरेको पाइयो। कार्यालय प्रमुखले औपचारिक रूपमा नयाँ प्रयोगकर्ताको खाता सिर्जना गर्न अनुरोध गर्छन्। तत्पश्चात् सूचना प्रविधि सहायता एकाईले प्रत्येक कर्मचारीको आईडी अघि 'पी' (क्यापिटल) अक्षर

तोक्छ। प्रयोगकर्ताहरूलाई लिखित रूपमा नयाँ प्रयोगकर्ताको नाम सेटअप गरिएको बारे जानकारी गराउने गरेको पाइयो।

- पहिलो पटक लग इन गर्न प्रयोगकर्ताको एउटै (Same) युजरनेम र पासवर्ड दिईन्छ। पहिलो लगइन पछि सिस्टमले नै प्रयोगकर्ताको पासवर्ड परिवर्तन गर्न अनिवार्य गर्छ। लग इन नगर्ने नयाँ प्रयोगकर्ताले आफ्नो पासवर्ड परिवर्तन नगर्दा सुरक्षा जोखिम बढ्न सक्छ ।
- कर्मचारी सरुवा भएमा कार्यालय प्रमुखले कर्मचारीको खाता निष्क्रिय गर्ने गरेको पाइयो। सरुवा भएपछि प्रमुखले कर्मचारी खाता पुनः सक्रिय गर्न अनुरोध गर्ने गरेको पाइयो। एक कर कार्यालयबाट अर्को कर कार्यालयमा सरुवा गर्दा कर्मचारीको खाता कार्यालय प्रमुखले निष्क्रिय बनाउने गरेको पाइयो।
- कर्मचारीको अवकाशको समयमा सूचना प्रविधि प्रणालीमा प्रयोगकर्ता खाताको पहुँच निस्क्रिय गर्ने गरेको पाइयो।

ग) नियन्त्रण नगर्दाको असर (सम्भावित जोखिम)

अनावश्यक रुपमा खोलिएका प्रयोगकर्ता खाताहरू (User Accounts) ले प्रणालीको कार्यक्षमता र डाटामा अनधिकृत पहुँच बढाउँछ । नयाँ प्रयोगकर्ता खाता (Username and Password) सजिलै अनुमान गर्न सकिने भएकाले अनधिकृत व्यक्तिले वास्तविक प्रयोगकर्ताले प्रयोग गर्नु अगावै पहिलो पटक लगइन गरी कारोबार गर्नसक्छ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- कार्यालय प्रमुखद्वारा प्रयोगकर्तालाई अधिकार र सुविधाहरूको पहुँच प्रदान गर्न, संशोधन गर्न तथा हटाउन उपयुक्त फारामको तर्जुमा गर्नुपर्छ ।
- निश्चित अवधिभित्र प्रारम्भिक पासवर्ड परिवर्तन नगरिएका नयाँ प्रयोगकर्ताको खातालाई (New User Account) निष्क्रिय गरिनुपर्छ ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.९.३ पासवर्ड

क) मूल्याङ्कनका आधार (Criteria)

- प्रणाली प्रशासक (System Administrator) र सामान्य प्रयोगकर्ताहरुको लागि पासवर्ड नीति तयार गरी लागु गरेको हुनुपर्छ। प्रयोगकर्ताहरूका लागि सुरक्षित पासवर्ड अभ्यास वारे सबै कर्मचारीलाई जानकारी गराईनुपर्छ।

- मजबुत पासवर्ड राख्ने र समय समयमा परिवर्तन गर्ने नीति लागू गर्नुपर्छ ।
- हार्डवेयर र सफ्टवेयरमा सेट (Save) भएका (Saved) पासवर्डहरू परिवर्तन गरिनुपर्छ।
- सफ्टवेयर, सर्भर र डाटामा सर्वाधिकार पहुँच (System Administrator Access) प्राप्त गर्न टोकन वा स्मार्ट कार्ड जस्ता Multifactor Authentication (MFA) को प्रयोग गरिनुपर्छ।
- पासवोर्ड सादा अक्षर (Plain Text) मा राखिनु हुँदैन ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

विद्यमान पासवर्ड अभ्यासहरूमा निम्न कमजोरीहरू पहिचान गरिएको थियोः

- पासवर्डसँग सम्बन्धित नियम तयार गरी लागू गरेको पाईएन।
- बलियो पासवर्ड (**Strong Password**) को लागि आवश्यक ढाँचा (**Format**) निर्धारण गरेको पाईएन।
- नयाँ प्रयोगकर्ताको लागि आँफनो पासवर्ड राख्न अनिवार्य गरेपनि कमजोर पासवर्ड लाई पनि स्वीकार गरेको पाइयो।
- विशेषाधिकार प्राप्त प्रयोगकर्तालाई Two Factor Authentications अनिवार्य गरिएको छैन।
- लेखापरीक्षणको क्रममा छलफल गर्दा कार्यालयको प्रमुखले आँफ्नो युजरनेम र पासवर्ड कम्प्यूटर अधिकृतलाई दिने (Share) गरेको पाइयो ।

ग) वलियो पासवर्ड नहुँदाको असर (सम्भावित जोखिम)

सुरक्षित पासवर्ड अभ्यासको अभावले अनधिकृत पहुँच र प्रणाली एवं डाटाको असुरक्षा हुन जान्छ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

कार्यालयले अन्तर्राष्ट्रिय उत्तम अभ्यास अनुसरण गर्ने पासवर्ड नीति अपनाउनु पर्दछ । पासवर्डहरू गैर-विषयगत हुनुपर्दछ, सजिलै अनुमान योग्य हुनुहुँदैन र बलियो ढाँचाको हुनुपर्छ। पासवर्डहरू निम्नलिखित ढाँचामा हुनुपर्छः

- कम्तीमा आठ अक्षरहरू भएको र निम्नमध्ये एक वा बढी समावेश भएको हुनुपर्छ।
    - lower-case letter
    - upper-case letter
    - number
    - punctuation mark.

- Administrator पासवर्ड लामो हुनुपर्दछ। क्रमरहित (Random) शब्दहरू सँगै राखी झट्ट हेर्दा उस्ताउस्तै देखिने वर्णहरू समावेश गर्नुपर्छ।
- अत्यधिक संवेदनशील प्रणाली, सेवा र डाटाको लागि पहुँच हुने खातामा Multi-factor Authentication जस्तै टोकन वा स्मार्ट कार्डहरू प्रयोग गर्नुपर्छ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.९.४ लग इन (Log-In)

क) मूल्याङ्कनका आधार (Criteria)

- प्रणालीको सुरक्षा गर्न Log-In/Log-out प्रक्रिया निर्धारण गरेको हुनुपर्छ र प्रयोगकर्ताहरूलाई उनीहरूको जिम्मेवारी र उत्तरदायित्वका सम्बन्धमा जानकारी गराएको हुनुपर्छ ।
- कुनै प्रयोगकर्ताले तोकिएको भन्दा बढी पटक प्रणालीको पहुँच (Log-In/Log-on) पाउन असफल प्रयास गरेमा उक्त प्रयोगकर्तालाई स्वतः निस्क्रिय गराईनुपर्छ। यस्ता प्रयासहरुको अभिलेख प्रणालीमा स्वतः दर्ता हुने व्यवस्था गरी समय समयमा समीक्षा गरिनुपर्छ ।
- केही समय किबोर्ड निष्क्रिय भएमा निर्धारित समयपश्चात् प्रणालीले प्रयोगकर्ताको Account लाई स्वतः Log-Out गर्नुपर्छ। उदाहरणका लागिः ५ वा १० मिनेट।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- Log-out/ Log-in नीति तयार गरी कार्यान्वयन गरेको पाईएन।
- तोकिएभन्दा बढीपटक असफल Log-in पछि प्रयोगकर्ताको User Account स्वतः निस्क्रिय हुने व्यवस्था लागु गरेको पाईयो। निष्क्रिय समय अवधि ३०० सेकेन्ड भनेता पनि परीक्षण गर्दा ३०० सेकेन्डपछि लग आउट भएन।

ग) नियन्त्रण सुधार नसक्दाको परिणामहरू (सम्भावित जोखिम)

कार्यालयको प्रणालीमा अनाधिकृत व्यक्तिहरूले पहुँच प्राप्त गरी डाटाको गोपनीयता र Data Integrity कायम नहुन सक्छ ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- कार्यालयले सबै प्रयोगकर्ताहरूलाई जानकारी गराई स्पष्ट Log-In/Log-Out कार्यविधि बनाएर लागू गर्नुपर्दछ। केही पटक असफल Log-In प्रयासपछि प्रयोगकर्तालाई स्वतः

निष्कृय हुने सूचना सहित स्वचालित इमेल (Automatic E-mail) जाने व्यवस्था हुनुपर्छ र निश्चित समय निष्क्रिय भएपछि फेरि Log-In गर्नसक्ने व्यवस्था प्रणालीमा हुनुपर्दछ ।

- प्रणालीमा धेरै पटक असफल Log-In को प्रयासपछि प्रयोगकर्ता खाताहरू स्वतः निस्क्रिय पारिनुपर्दछ। खाता निस्क्रिय गरिएको अवस्थामा सूचना प्रविधि कर्मचारीले प्रयोगकर्ताहरूलाई व्यवस्थापनसँग स्वीकृति लिएर मात्र उनीहरूको खाता पुनः सक्रिय गर्नुपर्दछ।
- सबै प्रयोगकर्ताहरूमा निष्क्रिय समय अवधि **(Idel Time)** लागू गरिनुपर्छ र संवेदनशील पहुँचका लागि साधारण उपयोगकर्ताहरूको भन्दा छोटो समय हुनुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.९.५ Administrator र विशेषाधिकार प्राप्त प्रयोगकर्ताहरूको अधिकार

क) मूल्याङ्कनका आधार (Criteria)

- Administrator अधिकार आवश्यकता अनुसार सीमित व्यक्तिलाई मात्र प्रदान गर्नुपर्छ।
- System Administrator र अन्य विशेषाधिकार प्राप्त प्रयोगकर्ताहरूको गतिविधि प्रणालीमा अभिलेख (Log) राखी आवधिक रूपमा समीक्षा गरेको हुनुपर्छ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

Administrator तथा उच्च अधिकार प्राप्त प्रयोगकर्ताहरूले उच्च स्तरीय तथा विशेषाधिकार पहुँच प्राप्त गर्ने हुनाले यस्ता पहुँचलाई कडाइका साथ नियन्त्रण गरिनुपर्छ। System Administrator र अन्य विशेषाधिकार प्राप्त प्रयोगकर्ताहरूको गतिविधि प्रणालीमा अभिलेख (Log) राखी आवधिक रूपमा समीक्षा गरेको पाईएन।

ग) नियन्त्रण सुधार नसक्दाको परिणामहरू (सम्भावित जोखिम)

Administrator को विशेषाधिकारको दुरुपयोगले हिनामिनाको जोखिम वढाउनुका साथै गोपनीयता भङ्ग हुने, Data Integrity गुम्ने र प्रणाली अवरुद्ध हुने जस्ता गम्भीर किसिमका खतराहरु आउन सक्छन्।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- प्रभावकारी रूपमा कार्य गर्न पहुँच आवश्यक भए मात्र उच्च अधिकार सहितको Administrator पहुँच दिइनुपर्छ। सो पहुँच अनावश्यक भएमा तुरुन्त खारेज गरिनुपर्छ।

- System Administrator र अन्य विशेषाधिकार प्राप्त प्रयोगकर्ताहरूको गतिविधिको अभिलेख राखिनुपर्छ र स्वतन्त्र व्यक्तिबाट नियमित रूपमा समीक्षा गरिनुपर्छ।

२.१० बाह्य सेवा प्रदायक (Outsourcing)

क) मूल्याङ्कनका आधार (Criteria)

- कार्यालयले बाह्य सेवा प्रदायक (Outsourcing) वाट सेवा लिने कार्यका सम्बन्धमा स्पष्ट कार्यविवरण र जिम्मेवारी सहितको नीति हुनुपर्छ ।
- विभागको नीतिमा बाह्य सेवा प्राप्त गर्ने र सूचना प्रविधि सेवाहरूको खरिद गर्ने सम्बन्धमा आवश्यक प्रावधानहरू रहेको हुनुपर्छ।
- सेवा प्रदायकसँग करार सम्झौता गरेको हुनुपर्छ। सेवा प्रदायकसँग करार सम्झौता गर्दा सेवाको गुणस्तर निर्धारण गर्ने, कार्यसम्पादन मापन गर्ने, सुरक्षा सम्बन्धी जोखिमको पहिचान गरी व्यवस्थापन गर्ने तथा सेवा प्रवाहको अनुगमन गर्ने व्यवस्था सुनिश्चित गर्नुपर्छ। करार सम्झौता अनुसारको सेवा प्रवाह नगरेमा आवश्यक कारबाहीको व्यवस्था गरिनुपर्छ।
- डाटा सुरक्षा र पहुँच अधिकार सम्वन्धि व्यवस्था सेवा करारमा समावेश हुनुपर्छ। सेवा सम्झौता बमोजिमका प्रावधानहरु बाह्यसेवा प्रदायकद्वारा पालना भैरहेका छन् भन्ने सुनिश्चित गर्ने संयन्त्र हुनुपर्दछ। बाह्य सेवा प्रदायकलाई महत्वपूर्ण र संवेदनशील डाटा एवं सूचनामा पहुँच दिनु हुँदैन । Support and Maintenance जस्ता Supporting Business को लागि मात्र बाह्य सेवा प्रदायक नियुक्त गर्नुपर्दछ ।
- सेवाप्रदायकले सेवा दिन असमर्थ भएमा पनि महत्वपूर्ण कार्यहरू सञ्चालन गर्न सकिने गरी बिभाग भित्रै व्यावसायिक ज्ञान भएका जनशक्तिको व्यवस्था गरी सेवा निरन्तरताको सुनिश्चितता गर्नुपर्दछ। बाह्य सेवा प्रदायकको निर्भरता कम गर्दै लग्नुपर्छ ।
- बाह्य सेवा लिने सम्बन्धमा यथार्थ परक लागत लाभ विश्लेषण गरी सोको आधारमा कार्यक्रम व्यवस्थापन र नियन्त्रण गरिनुपर्छ।
- विभागले बाह्य सेवा प्रदायकवाट हुनसक्ने सुरक्षा जोखिम पहिचान गर्नुपर्छ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- विभागको बाह्यसेवा प्रदायकद्वारा कार्य गराउनका लागि आवश्यक नीति तर्जुमा गरेको छैन। आउटसोर्स गरिएका सेवाहरू सार्वजनिक खरिद ऐन, २०६३ (२००७) को पालनामा खरिद गरिएका छन्।
- सेवा प्रदायकसँगको सेवा सम्झौताको गोपनीयता सम्बन्धी खण्ड २३ मा सेवा अवधि समाप्त भएको २ वर्षसम्म मात्र गोपनीयता कायम रहने उल्लेख गरिएको छ।

- विभागको आँफ्नो जनशक्ति (In House Team) सक्षम रहेता पनि बाह्य सेवा प्रदायकद्वारा कार्य गराउने परिपाटीलाई प्रतिस्थापन गर्न स्थायी कर्मचारीहरू पर्याप्त रहेको पाईएन।
- विदेशी एजेन्सीवाट सेवा प्राप्त गर्ने सम्वन्धमा अवश्यक नीतिगत प्रावधान रहेको पाइएन।
- सम्झौता बमोजिम सेवा उपलव्ध नभएको खण्डमा प्रतिघण्टा रु २०,०००।- जरिवाना तिर्नुपर्ने प्रावधान रहेको छ। तर, कार्य सम्पादन डाटाको अपर्याप्ततले गर्दा सोको कार्यान्वयन गर्न असम्भव देखिन्छ।
- सेवा प्रदायकवाट सेवा लिँदा हुन सक्ने जोखिम व्यवस्थापनको लागि सम्झौतामा उल्लेख गरेको पाइएन ।
- सेवा प्रदायकद्वारा एप्लिकेशन, डाटा र सेवाको लागि व्यवसाय निरन्तरता योजना (BCP) /प्रकोप पुनर्स्थापना योजना (DRP) को सुनिश्चित गर्नेबारे सम्झौतामा कुनै व्यवस्था गरेको पाइएन।

ग) नियन्त्रणहरू सुधार नसक्दाका परिणामहरू

बाह्य सेवामा अधिक निर्भरताका कारण विभागको आन्तरिक विज्ञता तथा नियन्त्रण गुम्ने, गोपनीयता र डाटाको शुद्धता घट्ने जस्ता जोखिमहरु हुनसक्छ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- विभागले बाह्य सेवा प्रदायकद्वारा कार्य गराउने नीतिको तर्जुमा गरी लागू गर्नुपर्छ।
- सेवा प्रदायकको कार्य सम्पादन अनुगमनको अभिलेखिकरण हुनुपर्छ र आवश्यकता अनुसार क्षतिपूर्तिको दाबी गरिनुपर्छ।
- बाह्य सेवा प्रदायकद्वारा कार्य गराउन आवश्यक भएमा सेवा करार सम्झौतामा सेवाको गुणस्तर, नियन्त्रण र कार्य सम्पादनका मापदण्ड समावेश गर्नुपर्छ।(उदाहरणका लागिः सुरक्षा, डाटा अधिकार, कार्य सम्पादन प्रतिवेदन, जरिवाना आदि)।
- बाह्य सेवा प्रदायकद्वारा कार्य गराउन आपूर्तिकर्तासँगको सम्झौताको गोपनीयताको खण्डमा डाटाको गोपनीयता २ वर्षका लागि मात्र सुरक्षित नभई अनन्त कालसम्म सुरक्षित रहने गरी संशोधन गरिनुपर्छ।
- सेवा सम्झौतामा सेवा प्रदायकबाट प्राप्त गरिएका डाटा, एप्लिकेशन र सेवाहरूमा व्यवसाय निरन्तरता योजना (BCP) /प्रकोप पुनर्स्थापना योजना (DRP) को सुनिश्चित हुनुपर्ने व्यवस्था समावेश गर्नुपर्छ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.११ सामान्य एप्लिकेशन नियन्त्रण (Generic Application Controls)

२.११.१ इनपुट तथा त्रुटि व्यवस्थापन (Input And Error Handling)

क) मूल्याङ्कनका आधार (Criteria)

- प्रयोगकर्ताले बुझ्ने गरी डाटा प्रविष्टि गर्ने अनलाईन फारम (Interface) हुनुपर्छ। प्रयोगकर्ताले सफ्टवेयर प्रणालीमा विवरण प्रविष्टि (Entry) गर्दा प्रणालीवाट नै नियन्त्रण गर्न सकिने विषयहरु जस्तैः कारोबारको आधिकारिक श्रोत, सूचनाको आधिकारिकता, पूर्णता, दोहोरोपना र शुद्धता जाँच गर्ने व्यवस्था (Input Control System) हुनपर्दछ।
- कारोवारहरु आधिकारिक स्रोतबाट मात्र भएको हुनुपर्छ। शुरुवाटै कारोवारमा त्रुटी नहुनेगरी नियन्त्रण कायम गरिनुपर्छ।
- एप्लिकेशनमा डाटा प्रविष्टि हुनु अघि उचित लगिङ (Logging) र स्रोत कागजातहरू (Source Document) को रेकर्ड राखेको हुनुपर्छ। हरेक कारोवारलाई युनिक क्रमसंख्या (Unique Sequential Number) प्रदान गरिनुपर्छ। कागजातहरू कानूनी मापदण्डद्वारा निर्धारण गरिएको समय सम्मको लागि राखिनुपर्छ।
- कारोबार पूर्णरूपमा म्यानुअल वा इलेक्ट्रोनिक माध्यमद्वारा प्रमाणित गरिएको हुनुपर्छ। इनपुटको लागि समय तालिका निर्धारण गरी पालना गरिएको हुनुपर्छ। इनपुट गर्ने र प्रमाणित गर्ने कार्यको स्पष्ट कार्य विभाजन गरिएको हुनुपर्छ। कारोबारको लागि प्रमाणित गर्ने पदाधिकार (वा प्रत्यायोजित अधिकार) निर्धारण गरी उचित नियन्त्रण गरिएको हुनुपर्छ । कर्तव्यहरूको निर्धारण सम्भव नहुने मुद्दाहरूको लागि (Compensating Control) लागू गरिनुपर्छ। प्रशोधनको लागि मापक र अन्य स्थायि डfटा (Standing Deta) कडाइका साथ पालना गरिनुपर्दछ। इनपुटको लागि समय तालिका निर्धारण गरी पालना गरिएको हुनुपर्दछ।
- प्रत्येक त्रुटिलाई हल गर्न र समस्याहरूको सञ्चार गर्न स्पष्ट कार्यविधि हुनुपर्छ। कारोबार प्रशोधन हुनुभन्दा पहिले त्रुटिलाई सच्चाउनुपर्छ। लगहरूको समय समयमा अनुमगन र समीक्षा गरी आवश्यक सुधारात्मक कदमहरु चालिनुपर्छ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- सूचना प्रविधि प्रणाली इनपुट 'Four Eyes' सिद्धान्तमा आधारित छ। डाटा प्रविष्ट गरेपश्चात कारोबारको स्क्रिन जाँच र स्वतन्त्र प्रमाणीकरण गरी डाटाबेश अपडेट गरिन्छ।
- स्वीकृतिकर्ताले आफ्नो यूजरनेम र पासवर्ड डाटा प्रवृष्टि गर्ने कर्मचारीलाई अदान-प्रदान नगरेको अवस्थामा मात्र यो प्रक्रिया प्रभावकारी हुन्छ।

- कर अधिकृतले कर लेखापरीक्षणको लागि करदाता चयन गरी विस्तृत पुष्टीकरणका लागि कागजातहरूको माग गर्दा म्यानुअल रूपमा कर कार्यालयमा पेश गरिन्छ। करदाताहरुले कागजातहरू इलेक्ट्रोनिक रूपमा अपलोड गर्ने व्यवस्था गरिएको छैन।
- आय विवरणको अनुसूचि १३ नभरे पनि वा पूर्णरुपमा नभरेको अबस्थामा समेत आय बिबरण भिडान (Verify) हुन्छ । करदाताले विगत वर्ष र यस वर्षका बिभिन्न कागजातमा फरक फरक तथ्याङ्क पेश गरेपनि प्रणालीले पहिचान गर्दैन ।
- अनुगमनको लागि आबश्यक न्युनतम कागजातहरु पेश गर्नुपर्ने व्यवस्थालाई अनिवार्य गरिएको छैन। पेश गर्नुपर्ने भनि तोकिएका कागजातहरु पेश नभएको अबस्थामा समेत Verify भएका उदाहरणहरु प्रशस्त छन्। कागजातहरु पेश नगरेको र इलेक्ट्रनिक रूपमा अपलोड गर्ने सुविधा पनि नभएको अवस्थामा पेश भएको कागजातको कुनै Trail नरहन सक्दछ ।
- कर भुक्तानी पोर्टलमा 'गत आ.व. बाट जिम्मेवारी सारेको व्यवसायको नोक्सानीको' जाँच हुने ब्यबस्था छैन । यसबाट गलत नतिजा निस्कने, कर निर्धारणमा समस्या हुने तथा करदाताको अनुगमन गर्न र करदाता बीचका कारोबार एक आपसमा भिडान गर्न समस्या पर्ने देखिन्छ ।

ग) ईनपुट तथा त्रुटि व्यवस्थापन नगर्दाका परिणामहरू

वैधिकरण (Validation) को अभावले गलत डाटा प्रविष्टिको सम्भावना बढाउँछ। कागजातहरू इलेक्ट्रनिक रूपमा अपलोड गर्ने व्यवस्था नहुँदा कागजातको कुनै Trail नरहन सक्छ ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- कर भुक्तानी पोर्टलमा 'गत आ.व. बाट जिम्मेवारी सारेको व्यवसायको नोक्सानीको वैधिकरण जाँच लागू गर्नुपर्छ।
- अनुगमनको लागि न्युनतम कागजात पेश नभएसम्म Verify नहुने ब्यबस्था गर्नुपर्छ ।सबै कागजात PDF फरम्याटमा अपलोड गर्ने नभै सिस्टममा नै प्रबिष्टि गर्ने ब्यबस्था मिलाउनुपर्छ ।
- कर अधिकृतले माग गरेका कागजातहरूको प्रणालीमा इलेक्ट्रोनिक अपलोड गर्न मिल्ने व्यवस्था गर्नुपर्छ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.११.२ प्रशोधन (प्रोसेसिङ)

क) मूल्याङ्कनका आधार (Criteria)

- व्यावसायिक नीति, नियम र विधि प्रक्रियाको पालना हुने गरी सफ्टवेयर एप्लिकेशनले डाटाको Processing गर्नुपर्छ र प्रविष्ट भएका डाटा, सूचना तथा कागजातको Processing सफलतापूर्वक सम्पन्न भएको पुष्टि गर्नुपर्छ।
- सेवा लिने क्रममा केहि त्रुटि भई प्रक्रिया अवरुद्ध हुन गएमा पूनः प्राप्ति वा पूनः पेश गर्ने व्यवस्था प्रणालीमा हुनुपर्छ। एप्लिकेशनले प्रशोधनको क्रममा डाटाको पूर्णता, सत्यता, वैधता र विश्वसनीयता चेकजाँच गर्नुपर्दछ । असङ्गत डाटालाई एप्लिकेशनले स्वीकार गर्नुहुँदैन। वैधिकरण मापदण्ड समयानुकूल, उपयुक्त र आधिकारिक तवले अद्यावधिक गर्नुपर्छ।
- प्रयोगकर्ता र कर्मचारीले बुझ्ने किसिमको स्पष्ट प्रशोधन सूची (Processing List) तयार गरेको हुनुपर्छ । वैधिकरण नियमहरू सम्पूर्ण डाटालाई समेटने, अभिलेखिकरण गरिएको र एप्लिकेशनको इन्ट्री Interfaces मा लागू गरिएको हुनुपर्छ; डाटा प्रविष्टिका बिभिन्न विधि प्रक्रियाहरु Interface मा लागू गरिएको हुनुपर्छ; असङ्गत डाटालाई एप्लिकेसनले अस्वीकार गर्नुपर्छ; वैधिकरण मापदण्ड समयानुकूल, उपयुक्त र आधिकारिक तवरले अपडेट गर्नुपर्छ। Overriding Input Controls भएको अवस्थामा लग (Log) र स्वीकृति (Authorisation) नियम जस्ता पूरक नियन्त्रणहरू हुनुपर्छ। Application Interface का लागि उपयुक्त नियन्त्रण र अभिलेखिकरण भएको हुनुपर्छ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- सूचना प्रविधि प्रणालीमा कर कानुनी प्रक्रिया अनुरुप मिलान भएको देखिन्छ।
- कतिपय कानुनी ब्यबस्थाहरु सिस्टममा समाबेश छैनन । जस्तै करदाताले ढिला बिबरण बुझाएको अबस्थामा आयकर ऐन २०५८ को दफा ११७, ११८ र ११९ बमोजिमको शुल्क र व्याज स्वतः गणना हुँदैन र करदाताहरुद्वारा प्रविष्टी गरिएका रकमको चेकजाँच हुने गरेको छैन।
- कर निर्धारण भैसकेपछि स्वचालितरुपमा आफै बक्यौता कायम हुने र RMIS मार्फत कर चुक्ता गरेपछि बक्यौता घटदै जाने बिशेषता सिस्टममा छैन । एकीकृत कर प्रणाली र बक्यौताको सफ्टबेयर बेग्ला बेग्लै रहेको र ईन्टरफेस समेत नहुदाँ यस्तो स्थिति देखिएको छ ।
- करदाताको प्रकृति अनुसार आबश्यक फारमहरुको ब्यबस्था गरिएको छैन । राजस्वसँग सम्बन्धित आबश्यक सबै म ले प फारमहरु सिस्टममा राखिएका छैनन् ।

- करदाताको कर परीक्षण प्रतिबेदन सिस्टममा अपलोड गरिदैन जसले गर्दा कुन करदाताको कहिले कर परीक्षण भयो यकिन गर्न र छुटेकालाई छनौट गर्न समस्या पर्ने देखिन्छ ।
- करको दर छनौट गर्दा Drop-Down विकल्पमा '०', '७.५%' दर भएको पाइएन।
- सूचना प्रविधि प्रणालीमा कम्प्युटर बील, संशोधित विवरण र अनलाइन खरिदको भ्याट फिर्ता दाबी गर्ने मोड्युलहरू रहेका छैन।

ग) नियन्त्रणहरू सुधार नसक्दाका परिणामहरू

- ब्याबसायिक आबश्यकता पुरा नहुदाँ सिस्टमले प्रभाबकारी ढंगले नियन्त्रण प्रदान गर्न सक्दैन । प्रयोगकर्ताहरूका लागि अनलाईन ईनपुट प्रणाली असहज भएमा अनलाइन रजिष्ट्रेशन कार्य निरुत्साहित हुन जान्छ। भविष्यमा प्रणालीको स्तरोन्नति गर्दा आवश्यक सुविधा प्रदान गर्नुपर्छ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- विभागले भविष्यमा सुचना प्रविधि प्रणालीको स्तरोन्नति गर्दा नियन्त्रित कम्प्युटराइज्ड बिजक, संशोधित विवरण दाखिला र अनलाइन खरिदको भ्याट फिर्ता दाबी गर्ने सुविधा प्रदान गर्नुपर्छ।
- करको दर छनौट गर्दा Drop-Down विकल्पमा '०', '७.५%' दर उपलब्ध गराउनुपर्छ।
- भविष्यमा प्रणालीको स्तरोन्नति गर्दा आवश्यक सुविधा प्रदान गर्नुपर्छ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.११.३ नतिजा (Output)

क) मूल्याङ्कनका आधार (Criteria)

- नतिजाको लागि जिम्मेबार कर्मचारीले नतिजाको पूर्णता सुनिश्चित गर्नुपर्दछ; नतिजाको उपयोगिता समीक्षा गर्नुपर्दछ। एप्लिकेशनवाट सृजना हुने नतिजाको पूर्णता र शुद्धता जाँच गरेपछि मात्र अनुगमन **(Follow up)** प्रक्रियामा समावेश गर्नुपर्छ।

- सबै कारोवारको स्रोतको जानकारी राखिएको हुनुपर्छ। नतिजाको स्पष्ट रूपमा पहिचान हुने र पूर्णता दर्शाउने किसिमको जानकारी समावेश हुनुपर्छ।
- नतिजा **(Output)** वितरण गर्दा सम्बन्धित प्रयोगकर्ताले मात्र पाउने गरी गोपनीयता कायम गरिनुपर्छ। विद्यमान नियम कानूनमा तोकिएको अवधिसम्म नतिजा सुरक्षित राखिनुपर्छ।

- Interface नियन्त्रण मापदण्ड अनुरूप फाइल निर्यात, उत्पन्न, हिसाब मिलान, सञ्चार र आयातित गरिनुपर्दछ। एक वित्तीय प्रणालीबाट अर्को वित्तीय प्रणालीमा रेकर्डहरू पोस्ट गरिँदा दोस्रोका Input पहिलेको Output सँग मिल्ने हुनुपर्दछ। प्रणालीहरूबीच तथ्यांक स्थानान्तरण हुँदा नमिल्ने सुचना तथा तथ्यांकलाई पहिचान अनुसन्धान र सुधार गरिनु पर्दछ।
- एक वित्तीय प्रणालीबाट अर्को वित्तीय प्रणालीमा डाटा पोष्ट गर्दा दोस्रोको ईनपुट डाटा पहिलेको डाटासँग मिल्नुपर्छ। प्रणाली प्रणालीका बीचमा तथ्यांक आदान प्रदान हुँदा मिलान नभएका तथ्यांकलाई पहिचान गरी सुधार गर्नुपर्छ। विभागको कम्प्युटर प्रणालीबाट जारी भएका नतिजामा नियन्त्रण तथा सुधार गरिनुपर्छ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- केही प्रतिवेदन असंगत छन् । उदाहरणका लागि: करदातालाई डेबिट रिपोर्ट र नन् फाइलर दुबै सूची देखाइएको छ । नतिजाको मिलान गरिइएको छैन। उदाहरणको लागि बिभागको कम्प्युटर प्रणालीबाट उपलब्ध विवरण र राजस्व व्यवस्थापन सूचना प्रणाली (**RMIS**) को संकलन तथ्यांकमा फरक देखिन्छ तर भिडान गर्ने सिस्टम छैन। अनलाईन कम्प्युटर प्रणालीवाट प्राप्त हुने तथ्यांक उपलव्ध नभएकोले राजस्व व्यवस्थापन सूचना प्रणाली (**RMIS**) को तथ्यांक संग मिलान भए नभएको यकिन हुन सकेन ।
- विभागको सफ्टवेयरबाट राजस्व संकलन बक्यौता लगायतका तथ्याङ्कको आधारमा स्वचालित तबरले बित्तिय बिबरण तयार हुने ब्यबस्था छैन जसले गर्दा सिस्टमको असुली र बक्यौता लगत बित्तिय बिबरणसंग भिडान हुदैन र सोको हिसाब मिलान पनि गरिएको हुदैन । फलस्वरुप लेखापरीक्षणबाट बित्तिय बिबरणको यथार्थता यकिन गर्न कठिन छ ।
- ठूला करदाता कार्यालय भ्रमणको क्रममा प्रणालीको कार्यसम्पादनमा केही समस्याहरु रहेको पाइयो। उदाहरणका लागि रिपोर्ट आउन ढिलाइ हुने वा रिपोर्ट आउनुपूर्व नै सेसन लग आउट हुने गरेको पाइयो।

ग) नियन्त्रण सुधार नसक्दाको परिणामहरू (सम्भावित जोखिम)

विभागको कम्प्युटर प्रणालीबाट उत्पन्न नतिजा नियन्त्रणमा सुधार गरिनुपर्छ। राजस्व सूचना व्यवस्थापन प्रणालीको अभिलेख र वित्तीय विवरणमा देखाइएको अभिलेख जाँच गर्ने प्रणालीको कमी रहेको पाइयो।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- नियन्त्रण संरचना निर्माण गर्ने उद्देश्यले विभागले कम्प्युटर प्रणालीबाट प्राप्त नतिजा समीक्षा गरी इनपुटलाई स्वीकृत र प्रोसेसिङ गरी अपेक्षित आउटपुट भए नभएको पुष्टि गर्नुपर्छ ।
- विभागको कम्प्युटर प्रणाली र राजस्व सूचना व्यवस्थापन प्रणालीले संकलन गरेको डाटाको दैनिक रुपमा हिसाब मिलान गरिनुपर्छ;
- एकिकृत कर प्रणाली र राजस्व सूचना व्यवस्थापन प्रणाली वीचमा देखिएको असन्तुलनको विवरण तयार गरी घटी/बढी भएमा विभागले अनुसन्धान गरी उक्त असन्तुलनलाई कम गर्न आवश्यक कदम चाल्नुपर्छ। बित्तिय बिबरण समेत सिस्टमबाट तयार हुने र एक आपसमा भिडान हुने ब्यबस्था मिलाउनुपर्दछ ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.११.४ अडिट ट्रायल (Audit Trial)

क) मूल्याङ्कनका आधार (**Criteria)**

- Audit Trail ले महत्वपूर्ण कारोबारको सम्पादन, Overrides र प्रमाणीकरणका लगहरू प्राप्त गर्नुपर्छ।
- अनाधिकृत गतिविधि निगरानीको लागि अडिट ट्रायलको समय समयमा समीक्षा गरिनुपर्छ।
- अडिट ट्रायल फाइल वा रिपोर्टहरू पूर्ण हुनुपर्छ। अडिट ट्रायललाई निष्क्रिय गरेमा सोको विवरण समावेश हुनुपर्छ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

कम्प्युटर प्रणालीबाट Audit Trail/Activity Trail प्रतिवेदन प्राप्त गरेको पाईयो तर यी प्रतिवेदनहरूको नियमित समीक्षा गर्ने गरेको पाइएन।

ग) अडिट ट्रायल प्रभावकारी नहुँदाको परिणाम (सम्भावित जोखिम)

प्रयोगकर्ताद्वारा भएका अनाधिकृत पहुँच/गतिविधिहरू पत्ता नलाग्न सक्छ ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

Audit Trail Report तयार गरी नियमित रूपमा समीक्षा गरिनुपर्छ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१२ कार्यालयको वेबसाइट

२.१२.१ सि.सि.टी.भी जडान तथा सञ्चालन सम्बन्धी कार्यविधि, २०७२ को अनुपालना नभएको

क) मूल्याङ्कनका आधार (Criteria)

- CCTV जडान तथा सञ्चालन सम्बन्धी कार्यविधि, २०७२ को बुँदा ३(क)(१) अनुसार CCTV जडान बारे नजिकको प्रहरी इकाई वा सम्बन्धित जिल्ला प्रशासन कार्यालयलाई लिखित जानकारी दिनुपर्छ।
- CCTV जडान तथा सञ्चालन सम्बन्धी कार्यविधि, २०७२ को बुँदा ३(क)(५) अनुसार CCTV मार्फत खिचिएका दृश्यहरु कम्तीमा तीन महिनासम्म सुरक्षित रहने गरी राख्नुपर्छ।
- CCTV जडान तथा सञ्चालन सम्बन्धी कार्यविधि, २०७२ को बुँदा ३(घ) अनुसार CCTV जडान भएको क्षेत्रमा CCTV जडान भएको सूचना अनिवार्य रुपमा राख्नुपर्छ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- विभागमा CCTV जडान गरिए तापनि CCTV जडान तथा सञ्चालन सम्बन्धी कार्यविधि, २०७२ को अनुपालना गरेको पाइएन।
- CCTV जडानबारे नजिकको प्रहरी इकाई वा सम्बन्धित जिल्ला प्रशासन कार्यालयलाई लिखित जानकारी गरेको पाइएन साथै, CCTV मार्फत खिचिएका दृश्यहरु कम्तीमा तीन महिनासम्म सुरक्षित रहने नीति तर्जुमा गरेको पाइएन। CCTV जडान भएको क्षेत्रमा CCTV जडान भएको सूचना उल्लेख गरेको पाइएन।

ग) CCTV को प्रभावकारी व्यवस्थापन नहुँदाको परिणाम (सम्भावित जोखिम)

CCTV जडान तथा सञ्चालन सम्बन्धी कार्यविधि, २०७२ को पालना नहुन सक्छ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

CCTV जडान तथा सञ्चालन सम्बन्धी कार्यविधि, २०७२ को पुर्ण पालना गर्नुपर्छ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१२.२ कार्यालयको वेबसाइटको अपडेट

क) मूल्याङ्कनका आधार (Criteria)

वेबसाइटको नियमित रूपमा समीक्षा गरी अद्यावधिक गरिनुपर्छ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- कार्यालयको वेबसाइटको नियमित समीक्षा गरिएको पाइएन।
- विभिन्न उप-मेनुहरू (उदाहरणका लागि, "हाम्रो बारेमा/कार्यक्रम" र "सूचना/सेवा डेलिभरी म्यानुअल") खाली रहेको पाइयो।
- केही सामग्री अद्यावधिक गरिनुपर्छ (उदाहरणका लागि, "कर कानुन/आर्थिक ऐन" र "कर ऐन/परिपत्र")।

ग) वेबसाईटको प्रभावकारी रुपमा सञ्चालन र व्यवस्थापन नहुँदाको परिणाम (सम्भावित जोखिम)

कार्यालयको वेबसाइटमा राखिएका सूचना पुरानो हुन सक्छन्। वेबसाइटमा आवश्यक र नयाँ सामग्रीको अभावले सार्वजनिक सेवा प्रदान गर्न सकिदैन।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

कार्यालयको वेबसाइट नियमित रूपमा अद्यावधिक हुनुपर्छ र सामग्री (Contents) पूर्ण रुपमा राखिनुपर्छ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१३ सम्परीक्षण

क) मूल्याङ्कनका आधार (Criteria)

लेखापरीक्षण प्रतिवेदनमा उल्लेखित सुझाव तथा सिफारिसहरू समयमै कार्यानवयन गरिनुपर्छ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

विभागमा सञ्चालित सफ्टवेयर प्रणालीको तेस्रो पक्षद्वारा सूचना प्रविधि लेखापरीक्षण गरी १ डिसेम्बर २०१६ मा प्रतिवेदन पेश गरेको थियो। सो लेखापरीक्षण प्रतिवेदनमा सिफारिस निम्न बमोजिमका २९ सुझाबहरुको प्रभावकारीरुपमा कार्यान्वयन भएको पाईएन।

S.I. No.	Original Ref. no.	Audit Focus Areas
1	1	Documented Policies and Procedures
2	2	Technology Risk Management
3	3	Awareness, Training and Education
4	5	Secure Disposal of Equipment
5	6	Protecting Against External and Environmental Threats

6	7	Cabling Security
7	8	Cabling Security
8	11	Planning Disaster Recovery
9	17	Audit Trails and Event Logging
10	20	System Security Testing
11	25	Information Management
12	35	Review of User Access Rights
13	36	User of Secret Authentication Information
14	37	Audit Trails and Event Logging
15	38	Supporting Utilities
16	39	Protecting Against External and Environmental Threats
17	40	Working in Secure Area
18	42	Protecting Against External and Environmental Threats
19	44	Removal of Assets
20	45	Protecting Against External and Environmental Threats
21	46	Responsibilities and Procedures
22	47	Verify, Review and Evaluate Service Continuity
23	48	Clear Desk and Clear Screen Policy
24	50	Audit Trails and Event Logging
25	51	Protection of Log Information
26	52	Clock Synchronization
27	53	Protecting Services Transactions
28	54	Protecting Services Transactions
29	56	Security of Equipment and Assets Off-Premises

ग) नियन्त्रण सुधार नसक्दाको परिणामहरू (सम्भावित जोखिम)

लेखापरीक्षण सुझावको पूर्णरुपमा कार्यान्वयन नगर्दा प्रणालीमा भएका जोखिम एवं कमि कमजोरीहरुको समयमै रोकथाम वा नियन्त्रण हुँदैन र दुर्घटना हुन गई ठूलो क्षती हुनसक्छ ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

लेखापरीक्षणमा दिईएका सुझावहरुको यथाशिघ्र पूर्णरुपमा पालना गर्नुपर्छ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१४ वित्तीय जानकारीमा परेका असरका केही उदाहरणहरु

क) मूल्याङ्कनका आधार (Criteria)

आन्तरिक नियन्त्रण प्रणालीमा भएका कमि कमजोरीले गर्दा सारभुत वित्तीय नोक्सानी हुनुहुदैन।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

आन्तरिक नियन्त्रण प्रणालीमा भएको कमजोरीको कारण वित्तीय आँकडा गलत हुन सक्छन्। वित्तीय आँकडा सारभूत रुपमा गलत गराउन सक्ने आन्तरिक नियन्त्रण प्रणालीका कमजोरीलाई निम्नानुसार उल्लेख गर्न सकिन्छः

- करदाताहरुद्वारा दाबी गरिएका स्रोतमा कर कट्टी (TDS) को जाँच गरिएको छैन। परिणाम स्वरुप TDS को अधिक दाबी हुनाले सरकारलाई राजस्व घाटा हुन सक्छ। दफा ११७, ११८ र ११९ को शुल्क र व्याज स्वतः गणना हुँदैन र करदाताहरुद्वारा प्रवृष्टि गरिएका रकमको जाँच हुने गरेको छैन।
- केन्द्रीकृत बिलिङ व्यवस्थापन प्रणाली (CBMS) सुरुवात गरिएको छ। मु.अ.क दर्ता भएका २,१२,४९३ करदाताहरु र प्यान दर्ता भएका ११,७२,४४५ करदाताहरुमध्ये केवल ९२ करदाताहरु सो प्रणालीमा समावेश गरिएका छन्।
- प्रशासनिक पुनरावलोकनबापत धरौटी रकम दायित्व भए तापनि राजस्व भनेर लेखाङ्कन गरिएको छ। यसले गर्दा राजस्वको अधिक रिपोर्टिङ भएको देखिन्छ। आ.व. २०७५/७६ मा मू.अ.क. रु. ४५,८०,९६,३३७ र आयकर रु. ५,९७,७२,३८,०५३ गरी जम्मा विवादित रकम रु ६,४३,५३,३४,३९० रहेकोमा सोको २५ प्रतिशत रकम रु. १,६०८,८३३,५९७.५० अधिक राजस्व रिपोर्टिङ भएको देखिन्छ।
- मु.अ.क को लागि प्रशासनिक पुनरावलोकनका लागि जम्मा गरिएको धरौटी रकम ATR फाराममा 'हेल्ड' भनेर चिन्ह लगाइने गरिन्छ। यद्यपि, केही धरौटी रकम 'Held' भनेर चिन्ह लगाइएको छैन। परिणामतः सरकारलाई ब्याज र जरिवाना कम संकलनभई राजस्व घाटा हुन्छ।
- पुनरावेदन व्यवस्थापन प्रणालीको नियमित समीक्षा र आवश्यकता अनुसार अद्यावधिक गरिएको छैन।

- फाइलहरू कर परीक्षणका लागि चयन हुँदा र कर परीक्षण सम्पन्न हुँदा EMIS मा अद्यावधिक गरिनुपर्दछ। यद्यपि, कर परीक्षणका लागि चयन गरिएका सबै फाइलहरू सफ्टवेयरमा अभिलेख गरिएका छैनन्। परिणाम स्वरूप चयन नगरिएका फाइलहरूको कर परीक्षण भएको अवस्था सृजना भएको छ ।

ग) नियन्त्रण सुधार नसक्दाको परिणामहरू (सम्भावित जोखिम)

आन्तरिक नियन्त्रण प्रणालीमा भएको कमजोरीको कारण राज्यलाई आर्थिक घाटा हुन सक्छ । लेखा परीक्षकलाई वित्तीय तथ्यांकको शुद्धताको बारेमा आश्वस्तता प्रदान गर्दैन।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

यस प्रतिवेदनको दफा २.१४ (ii) मा उल्लेखित विषयहरुका जोखिम निर्धारण गरी रोकथाम गर्न, पत्ता लगाउन र सुधार गर्न उपयुक्त नियन्त्रणका उपाय अपनाउनुपर्छ ।

ङ) व्यवस्थापनको जवाफ (Management Response)