यातायात व्यवस्था विभागको विद्युतीय सवारी चालक अनुमतीपत्र तथा सवारी दर्ता प्रणाली (EDLVRS) को आर्थिक वर्ष २०७५/७६ को सूचना प्रविधि लेखापरीक्षण प्रतिवेदन

परिच्छेद- १

पृष्ठभूमि

१.१ परिचय

यातायात व्यवस्था विभागले विद्युतीय सवारी चालक अनुमतिपत्र तथा सवारी दर्ता सम्बन्धी कार्यहरुलाई सजिलो ,भरपर्दो एवं विश्वसनीय रुपमा सम्पादन गर्न र चालक अनुमतिपत्रलाई स्मार्ट कार्डमा दिने व्यवस्थाको लागि विद्युतीय सवारी चालक अनुमतीपत्र तथा सवारी दर्ता प्रणाली (Electronic Driving License and Vechicle Registration System, EDLVRS) विकास गरी 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(विभागमा गई प्रणालीसँग सम्बन्धित महत्वपूर्ण कागजात एवं हार्डवेयर, सफ्टवेयर, नेटवर्क, जनशक्ति लगायतका महत्वपूर्ण पूर्वाधारको अध्ययन एवं निरिक्षण गरिएको थियो ।

१.२ लेखापरीक्षणको क्षेत्र

राष्ट्रिय विद्युतीय शासन गुरुयोजना (National E-Government Master Plan) ले सरकारी निकायहरुमा सञ्चालित सूचना प्रविधि प्रणालीको लेखापरीक्षणका लागि विशेष जोड दिएको छ । यातायात व्यवस्था 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 गर्नुपर्दछ। नियन्त्रण प्रणालीमा सूचना प्रविधिको माध्यमवाट सम्पादन गरिने कार्यहरु ,सूचना प्रविधि पूर्वाधार र विभागवाट सञ्चालित सफ्टवेयर प्रणालीको सुरक्षासँग जोडिएका विषयहरु समावेश हुन्छन् । सूचना प्रविधि लेखापरीक्षणमा विशेषगरी प्रणालीसँग सम्बन्धित निम्न विषयहरुको अध्ययन गरी विश्लेषण एवं 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

यातायात व्यवस्थापनको कार्य गर्नका लागि वि.सं. २०४१ मा यातायात व्यवस्था विभागको स्थापना भएको हो । सवारी तथा यातायात व्यवस्था ऐन २०४९ र सवारी तथा यातायात व्यवस्था नियमावली, २०५४ को नीतिगत व्यवस्था वमोजिम मानिसको आवागमन र वस्तुहरुको ओसारपसारको लागि सुरक्षित, भरपर्दो र सुलभ यातायात सेवा उपलब्ध गराउनु विभाग र मातहत कार्यालयहरुको मुख्य उद्देश्य रहेको छ । यातायात व्यवस्था विभाग सवारी चालक अनुमतिपत्र र सवारी दर्ता प्रमाणपत्र जारी गर्ने अधिकार प्राप्त निकाय हो। हाल यस विभाग मीनभवन, काठमाडौंमा अवस्थित छ । नागरिकलाई प्रदान गरिने सेवा सुविधालाई सजिलो एवं प्रभावकारी बनाउनको लागि विभागले सफ्टवेयर प्रणाली संचालनमा ल्याएको छ। प्रस्तुत EDLVRS ईन्टरनेटमा आधारित अनलाईन प्रणाली हो । यस प्रणालीमा आवेदकले इन्टरनेट भएको जुनसुकै स्थान समयमा पहुँच (Access) पाउँछन् । EDLVRS मा मूख्य दुईवटा Components रहेका छन्।

- इलेक्ट्रोनिक ड्राइभिङ् लाइसेन्स (Electronic Driving License, EDL)
- सवारी दर्ता प्रणाली (Vehicle Registration System, VRS)

EDLVRS को विकास र कार्यान्वयनको लागि विभागमा आयोजना कार्यान्वयन एकाई (Project Implementation Unit, PIU) को स्थापना गरिएको थियो। EDLVRS को विकास गरी विभागलाई हस्तान्तरण गर्नको लागि बाह्य सेवाप्रदायक (**Consultant**) सँग ४ अक्टुबर, २०१३ मा करार सम्झौता भएको र ३१ डिसेम्बर २०१८ मा आयोजना सम्पन्न भएको थियो । EDLVRS का प्रमुख विशेषताहरुमा निम्न बमोजिम रहेका छन्।

- सफ्टवेयर प्रणाली (**Application Software**)को व्यवस्थापन तथा सञ्चालन यातायात व्यवस्था विभागले गरेको छ । प्रणाली र डाटालाई **सरकारी एकीकृत डाटा सेन्टरमा** (Government Integrated Data Center, GIDC) मा रहेका विभागका वेब सर्भर र स्टोरेज सर्भरहरुमा सेटअप गरिएको छ ।
- सबै यातायात व्यवस्था कार्यालयहरु र ५ वटा यातायात व्यवस्था सेवा कार्यालयहरुमा नयाँ भर्सन (New Version) को EDL संचालनमा रहेको छ।
- हालसम्म पनि यातायात व्यवस्था कार्यालय र यातायात व्यवस्था सेवा कार्यालयहरु (सवारी) मा नयाँ भर्सन (New Version) को VRS लागू गरिएको छैन। (पुरानो भर्सन (Old Version) को VRS ३४ वटा यातायात व्यवस्था कार्यालय र यातायात व्यवस्था सेवा कार्यालयहरुमा सञ्चालनमा रहेको छ)
- अनलाइन सवारी चालक इजाजतपत्र दर्ता प्रणाली कोटा प्रणालीमा आधारित छ।

- ❖ कुनै आवेदकले कोटा उपलब्ध भएमा जुनसुकै कार्यालयमा सवारी अनुमतिपत्रको लागि निवेदन दर्ता गर्न सक्दछ।
- ❖ यातायात व्यवस्था कार्यालय र यातायात व्यवस्था सेवा कार्यालयहरु प्रदेश सरकार अन्तर्गत स्थापना भएका छन्। यातायात व्यवस्था विभाग अन्तर्गत सवारी जाँचपास केन्द्र संचालित 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, 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 रहेका छन ।

१.५.२ नीतिगत व्यवस्था

सूचना तथा सञ्चार प्रविधिसँग सम्बन्धित नीतिगत व्यवस्था अन्तर्गत सूचना तथा सञ्चार प्रविधि नीति २०७२ ,ब्रोडव्याण्ड नीति ,2071 दुरसञ्चार नीति 2060 रहेका छन् । सरकारका नीति तथा आवधिक योजनामा सूचना प्रविधिबाट प्राप्त हुने लाभांशको पहुँच ग्रामीणस्तरसम्म पुर्‍याउने, सूचना प्रविधिको माध्यमवाट 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 संवन्धित 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 कार्यालय, मन्त्रालयमा लेखापरीक्षणको प्रारम्भिक प्रतिवेदन उपलब्ध गराइनेछ र प्रतिवेदनका संवन्धमा जवाफ पेस 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 आवश्यकतानुसार सम्परीक्षण गरिनेछ ।

१.६.५ लेखापरीक्षण औजार

यस सूचना प्रविधि लेखापरीक्षणका मुख्य औजारका रूपमा लेखापरीक्षण गरिने निकायमा प्रयोग भएका सफ्टवेयर ,हार्डवेयर ,नेटवर्क ,डाटा सेन्टर आदिको स्थलगत निरिक्षण र परीक्षण तथा सम्बन्धित अधिकारीहरुसँग सूचना प्रविधि प्रणालीसँग सम्बन्धित कागजात, अभिलेख एवं प्रतिवेदनहरूको सम्बन्धमा 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 विभागीय 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।

१.६.६ लेखापरीक्षणको सीमितता (Audit Limitations)

सूचना प्रविधि प्रणालीमा गरिने आन्तरिक नियन्त्रण र परीक्षणले धेरै हदसम्म प्रणालीको सुरक्षित प्रयोगमा सघाउ पुर्‍याउँछ 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 व्यहोराको सारांश

२.१ सूचना प्रविधि सुशासन

२.१.१ व्यावसायिक आवश्यकताको पहिचान, मार्गनिर्देशन र अनुगमन

क) मूल्याङ्कनका आधार (Criteria)

- 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 (Audit Observations)

लेखापरीक्षणको क्रममा छुट्टै सूचना तथा सञ्चार प्रविधि निर्देशक समिति (ICT Steerring Committee) रहेको पाइएन। सूचना प्रविधि प्रणालीवाट प्रवाह गरिने सेवाहरुको कार्यसम्पादन अवस्था अनुगमन गरी प्रतिवेदन पेश गर्ने गरेको पाइएन ।

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

सूचना प्रविधि निर्देशक समितिको अभावमा सूचना प्रविधि सम्बद्ध स्रोतहरूको व्यवस्थापन गर्न, लक्ष्य निर्धारण गर्न; रणनीतिक र कार्यगत योजनाहरू विकास गरी लागू गर्न; व्यावसायिक आवश्यकता पूरा गर्नको लागि सूचना प्रविधिजन्य साधन श्रोतको अधिकतम उपयोग भएको छ वा छैन सुनिश्चित गर्न; र प्रणालीको नियमित एवं सुरक्षित प्रयोगको लागि अपनाईने नीतिहरू वर्तमान र भविष्यको

आवश्यकतालाई सम्बोधन गर्न सक्ने गरी प्रभावकारी छन् भन्ने सुनिश्चित गर्न व्यवस्थापनलाई कठिन हुन्छ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- सूचना प्रविधिको बढ्दो प्रयोगलाई ध्यानमा राखि विभागको सांगठनिक संरचना निर्माण गर्दा प्रविधिमा काम गर्ने दक्ष कर्मचारीको कार्यविवरण र जिम्मेवारीलाई समीक्षा गरी गरिनुपर्दछ।
- सूचना प्रविधिको विकास र कार्य सम्पादनको नियमित समीक्षा गरी व्यवस्थापनलाई प्रतिवेदन पेश गर्न, थप सुधारात्मक कार्यहरुको लागि सिफारिस गर्न तथा कार्यान्वयन गरी अनुगमन गर्न सूचना प्रविधि निर्देशक समिति गठन गर्नुपर्दछ।

ङ व्यवस्थापनको जवाफ (Management Response)

२.१.२ सूचना प्रविधि रणनीति

क) मूल्याङ्कनका आधार (Criteria)

- विभागले आँफ्नो सूचना प्रविधि रणनीतिक योजना तयार गरेको हुनुपर्छ। रणनीतिक योजनामा कार्यालयको 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) लेखापरीक्षणका व्यहोरा (Audit observations)

उच्चस्तरीय व्यवस्थापनद्वारा स्वीकृत गरी लागू गरिएको सूचना प्रविधि रणनीति योजना भएको पाइएन। व्यवस्थापनसँग भएको छलफल अनुसार EDLVRS को कार्यान्वयनका लागि आयोजना कार्यान्वयन एकाइ (PIU) गठन भए पनि हाल यो निष्क्रिय रहेको पाइयो। आयोजना कार्यान्वयन एकाइ (PIU) सँग सम्बन्धित कुनै पनि कागजात उपलब्ध गराइएन।

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

सूचना प्रविधि नीति, रणनीति र योजनाको अभावमा प्रविधिको क्षमता र यसमा गरिएको लगानीको अधिकतम उपयोग हुन सक्दैन । कार्यालयको 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)

कार्यालयको व्यावसायिक मूल्य र मान्यतालाई दिगो र उच्च राख्न राख्न सूचना प्रविधि रणनीति तयार गरि लागू गर्नुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१.३ सांगठनिक संरचना, नीति र कार्यविधिहरू

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 ।
- व्यावसायिक उद्देश्य अनुरुप सूचना प्रविधिको माध्यमवाट सेवा सुविधा प्रदान गर्नको लागि विभागले 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) लेखापरीक्षणका व्यहोरा (Audit Observations)

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 । कुनै समस्या आएमा तत्कालको आवश्यकतालाई सम्बोधन गर्ने गरी (Ad-hoc Manner) समस्याको समाधान गर्ने गरिएको छ ।

ग) असर (Consequences)

सूचना प्रविधि प्रणाली सञ्चालनको लागि आवश्यक पर्ने नीति, योजना एवं विधि प्रक्रियाको अभावमा प्रणालीलाई प्रभावकारीरुपमा सञ्चालन गरी सजिलो, भरपर्दो एवं विश्वसनीय सेवा प्रदान गर्न सकिदैन। साथै प्रणालीसँग सम्बन्धित हार्डवेयर, सफ्टवेयर, नेटवर्क, डाटा सेन्टर, जनशक्ति लगायतका पूर्वाधारहरुको 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)

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

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१.४ मानव संसाधन र स्रोत साधन

क) मूल्याङ्कनका आधार (Criteria)

- कार्यालयको व्यावसायिक आवश्यकता (**Business Needs)** पूर्ति गर्नका लागि वर्तमान र भविष्यका आवश्यकताहरूलाई सम्बोधन गर्ने जनशक्ति विकास योजना (**Human Resource Development Plan**) तयार हुनुपर्दछ ।
- 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) लेखापरीक्षणमा देखिएका विषयहरु

- सूचना प्रविधिमा काम गर्ने स्थायी कर्मचारीहरुको निरन्तरता सुनिश्चित गर्न जनशक्ति विकास योजना तर्जुमा गरी लागू गरिएको छैन। कर्मचारीहरूबीच स्पष्ट कार्य विभाजन गरेको

देखिदैन। कम्प्युटर अधिकृतलाई सूचना प्रविधि प्रणालीका साथै प्रशासनिक कार्यहरूको पनि जिम्मेवारी दिइएको छ। सूचना प्रविधि शाखाका धेरै जसो कार्यहरु बाह्य सेवा प्रदायक (परामर्शदाता) वाट गर्ने गरेको पाइयो ।

- स्थायी सूचना प्रविधि कर्मचारीहरूलाई लोक सेवा आयोग मार्फत नियुक्ति गरिन्छ।

ग) जनशक्ति विकास योजना नहुँदा पर्नजाने असरहरु (सम्भाव्य जोखिमहरू)

जनशक्ति योजनाको अभावले सूचना प्रविधिको माध्यमवाट प्रदान गरिने सेवा सुविधाहरुलाई दिगो, प्रभावकारी एवं गुणस्तरीय बनाउन सकिदैन। कर्मचारीहरुको 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 ।

घ) लेखापरीक्षणका सुझाबहरु

सूचना प्रविधिको क्षेत्रमा काम गर्ने दक्ष जनशक्तिको व्यवस्थापनको लागि जनशक्ति विकास योजना निर्माण गरी कार्यान्वयन गर्नुपर्दछ। लोक सेवा आयोगको सिफारिसमा नियुक्त हुने सूचना प्रविधिसँग सम्बन्धित दक्ष कर्मचारीहरूलाई स्पष्ट कार्यविवरण सहितको जिम्मेवारी तोकिनुपर्दछ । दक्ष कर्मचारीहरूलाई कार्यालयमा समर्पित भएर (Dedicated) काम गर्ने 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 तालीम तथा अभिमुखीकरण

क) मूल्याङ्कनका आधार (Criteria)

विभागले वर्तमान र भविष्यका व्यावसायिक आवश्यकताहरु पूरा गर्न तालिम तथा अभिमुखीकरण योजना तथार गरी लागू गर्नुपर्दछ। योजनामा 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 काम गर्ने दक्ष कर्मचारीहरुको लागि 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)

स्थायी सूचना प्रविधि कर्मचारीहरूलाई लोकसेवा आयोग मार्फत नियुक्ति गरिन्छ। प्रणाली तथा डाटाको सुरक्षाको लागि कर्मचारीको उत्तरदायित्व र जिम्मेवारी तोकिएको छैन । पर्याप्त तालिम तथा प्रशिक्षण दिने गरेको देखिएन। विभिन्न तहका तालीमको लागि कुनै योजना भएको पाइएन। नयाँ नियुक्ति हुने कर्मचारीको प्रशिक्षणका लागि मात्र बजेट शीर्षक २.१४.१.२. मा रकम छुट्याइएको पाइयो। कर्मचारीहरूलाई डाटा एवं सूचनाको सुरक्षा तथा गोपनियता सम्वन्धी तालिम तथा सचेतना कार्यक्रमहरु सञ्चालन गरेको देखिएन ।

ग) असर (Consequences)

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

घ) लेखापरीक्षणको सिफारिस (Recommendation)

विभागले तालीम तथा प्रशिक्षण 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 गर्नपर्दछ । कतिपय कार्यालयहरुमा तालीम कार्यक्रमहरु 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 गर्नुपर्दछ । कर्मचारीहरुले तालीम लिएर सूचना प्रविधि प्रणालीमा काम गर्ने व्यवस्था अनिवार्यरुपमा लागू गर्नुपर्दछ ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१.६ जोखिम विश्लेषण र अनुपालना

क) मूल्याङ्कनका आधार (Criteria)

विभागले आँफ्नो व्यवसायसँग सम्बन्धित सबै किसिमका कानून, नीति, नियम एवं विधि र प्रक्रियाहरुको पूर्णरुपमा पालना गरेको छ भन्ने सम्बन्धमा विश्वस्त हुनका लागि उपयुक्त संयन्त्रहरु (जस्तैः गुणस्तर परीक्षण समूह, आन्तरिक लेखापरीक्षण, स्थलगत निरिक्षण र चेकजाँच आदि) मार्फत परीक्षण गर्नुपर्दछ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

सूचना प्रविधिको लागि छुट्टै गुणस्तर आश्वस्तता तथा कानून, नीति, नियमको अनुपालना भए नभएको सम्बन्धमा लेखापरीक्षण गर्न छुट्टै समूह नरहेको। सूचना प्रविधि सम्वन्धी जोखिमहरूको स्वतन्त्र रुपमा विश्लेषण र मूल्याङ्कन गरी सोको प्रतिवेदन उच्च व्यवस्थापन समक्ष पेश गर्ने गरेको पाइएन। जसले गर्दा सम्भाव्य जोखिमहरुको पहिचान गरी रोकथाम गर्ने वा नियन्त्रण गर्ने गरेको पाइएन ।

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 ।

कार्यालयको व्यावसायिक उद्देश्यसँग सम्बन्धित नीति एवं विधि र प्रक्रियाहरुको पूर्णरुपमा पालना भएको छ वा छैन भन्ने सम्बन्धमा स्वतन्त्र निकाय वा संयन्त्र मार्फत परीक्षण नगर्दा सामान्य प्रयोगकर्ता कर्मचारीमा निर्भर हुनुपर्दछ । 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 (Recommendation)

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।
- परामर्शदातासँग गरिएको सेवा करार सम्झौताको आधारमा समस्याहरुको समयमै समाधान गरी सबै सरोकारवालाहरुलाई जानकारी गराउनुपर्दछ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- विभागसँग निम्न बमोजिमका ४ वटा Incident व्यवस्थापन विधि (Interface) रहेका छन्:
  - सूचना प्रविधि कार्यान्वयन समूह (DOTM IT Implemention Group): **EDLVRS** प्रयोगकर्ताहरूद्वारा सुचना तथा जानकारी अदान-प्रदान गर्नको लागि प्रयोग गरिन्छ।

- info@dotm.gov.np यो कुनै समस्या वा जिज्ञासा पठाउने आधिकारिक ईमेल हो ।
- हेल्लो यातायात व्यवस्था विभागः फेसबुक पेज जहाँ सर्वसाधारणले उजुरी वा सुझाव दिन सक्छन् ।
- हटलाइन- ०१४४७४९२२: सामान्यतया सवारी चालक अनुमति पत्र सम्बन्धमा सोधखोज गर्न प्रयोग गरिन्छ ।

- समस्या तथा जिज्ञासाहरुलाई समाधान गर्न निश्चित कार्यविधि बनाइएको छैन।
- कार्यालयका प्राविधिक कर्मचारीद्वारा सामाधान गर्न नसकिने विषयहरूको हकमा बाह्य सेवाप्रदायकलाई ईमेल मार्फत सूचित गरिन्छ ।
- समस्या आएको मिति, समस्याको प्रकृति, समाधान गर्ने व्यक्ति र समाधान भएको मिति आदि उल्लेख गरी अभिलेख राख्ने गरेको पाइएन। यद्यपि, हटलाइन नम्बरको कार्ड सम्बन्धी समस्याहरु समाधान गरेको विवरण डाटाबेसमा राख्ने गरेको पाइयो।
- प्रयोगकर्ता र सर्वसाधारणको गुनासो सुन्न र समाधान गर्नको लागि सेवाग्राही सहायता कक्ष बनाएको पाइएन।

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

सूचना प्रविधिजन्य दुर्घटना तथा समस्याहरुको उचित व्यवस्थापन हुन नसक्दा विभागको 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 हराउने 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) लेखापरीक्षणको सिफारिस (Recommendation)

- विभागले सूचना प्रविधिजन्य दुर्घटनाको प्रभावकारी रुपमा व्यवस्थापन गर्नको लागि कार्यविधि तयार गरी लागू गर्नुपर्दछ।
- विभागले बाह्य सेवा प्रदायकद्वारा प्रदान गरिएको हेल्प डेस्क सेवाहरूको कार्य सम्पादनलाई प्रभावकारीरुपमा अनुगमन तथा निरिक्षण गर्नुपर्छ।
- प्रयोगकर्ताहरूलाई प्रणाली, डाटा तथा सूचनाको सुरक्षा सम्बन्धी विषयहरुको बारेमा माथि उल्लेख गरिए बमोजिम विभिन्न माध्यमवाट सचेत गराउनुपर्दछ।

- बाह्य सेवा प्रदायक (परामर्शदाता) लाई कार्यालयको महत्वपूर्ण डाटा वा सूचना (**Core Business**) मा पहुँच हुने किसिमका कार्यहरु गर्न दिनुहुँदैन।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.२.२ समस्या व्यवस्थापन (Problem Management)

क) मूल्याङ्कनका आधार (Criteria)

सूचना प्रविधिको प्रयोग गर्दा आउने समस्या एवं त्रुटिहरुको पहिचान गरी समाधान गर्न उपयुक्त कदम चाल्नुपर्दछ र सोको जानकारी सबै प्रयोगकर्ताहरूलाई दिनुपर्दछ । एकै किसिमका समस्याहरु दोहोरिन नदिन समस्याको वास्तविक कारण पहिचान (Root Cause Analysis) गरी स्थायी रुपमा समाधान गर्नुपर्दछ । सम्भव भएसम्म समस्याहरुको समाधान भन्दा समस्या आउनै नदिने कुरामा जोड दिने गरेको खण्डमा सूचना प्रविधिजन्य दुर्घटनाहरुलाई कम गर्न सकिन्छ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- विशेष प्रकृतिका समस्याहरुको मात्र तत्कालिन आवश्यकता सम्बोधन हुने गरी (Ad hoc Manner) समाधान गरेको पाईयो । विषयको गहिराईमा गई वास्तविक समस्याको पहिचान र विश्लेषण गरी स्थायी समाधान खोज्ने गरेको पाईएन । समस्या समाधान गर्न आवश्यक जनशक्ति तथा विधि र प्रक्रियाको व्यवस्था गरिएको छैन। केही समस्याहरू समान प्रकृतिका, दोहोरिरहने र एकै किसिमको कारणबाट उत्पन्न हुने गरेको पाइयो ।
- समय समयमा आउने समस्या र समाधानको बारेमा अभिलेख राख्ने गरेको पाईएन।

ग) असर (Consequences)

सूचना प्रविधिको प्रयोगमा देखिएका समस्याहरूलाई तत्कालिन आवश्यकताको मात्र सम्बोधन हुने गरी (Ad hoc Manner) समाधान गर्ने तर समस्याको गहिराईमा पुगि वास्तविक कारण पत्ता लगाउन र स्थायी समाधान खोज्न नसक्दा समस्याहरु वारम्वार आईरहन्छन । जसले गर्दा कार्य सम्पादन र नियन्त्रणमा गम्भिर असर पर्न गई गुणस्तरीय सेवा प्रदान गर्न सकिदैन ।

घ) लेखापरीक्षणको सिफारिस (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**) तयार गरी लागू गर्नुपर्दछ ।

- 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 ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.३ परिवर्तन व्यवस्थापन

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 प्रभावकारी रुपमा विश्लेषण र मूल्यांकन गर्नुपर्दछ ।
- आकस्मिक रुपमा कुनै परिमार्जन वा सुधार गर्न आवश्यक भएमा सोको परीक्षण गर्ने, अभिलेखीकरण गर्ने, मूल्याङ्कन गर्ने र स्वीकृत गरी कार्यान्वयन गर्ने छुट्टै प्रक्रिया निर्धारण गर्नुपर्दछ । यस्तो अवस्थामा नियमित रुपमा गरिने सुधार प्रक्रियाको अनुशरण गरिदैन।
- प्रणालीमा गरिएका सबै 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।

- विभागले 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 हुनुपर्दछ । 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) लेखापरीक्षणका व्यहोरा (Audit Observation)

- प्रणालीमा गर्नुपर्ने सुधार एवं परिवर्तन व्यवस्थापनका लागि कुनै मापदण्ड वा लिखित प्रक्रियाहरू निर्धारण गरेको पाईएन। लेखापरीक्षणका क्रममा सुधार गर्नुपर्ने विषयका सम्बन्धमा मौखिक वा इमेल मार्फत माग हुने जानकारी कार्यालयवाट भएको थियो।

- 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**) मा गर्ने 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।

ग) परिवर्तन व्यवस्थापन गर्न नसक्दाका असर (सम्भाव्य जोखिमहरू(

प्रणालीमा गर्नुपर्ने परिवर्तन सम्बन्धी विषयहरुको उचित व्यवस्थापन नहुँदा सुधार गर्नुपर्ने सबै विषयहरुलाई 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) लेखापरीक्षणको सिफारिस (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।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.४ व्यावसायिक निरन्तरता र विपद् व्यवस्थापन नीति) Business Continuity and Disaster Recovery Plan(

क) मूल्याङ्कनका आधार (Criteria)

- 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 कार्यालयको आवश्यकता र योजना अनुरुप कार्य गर्ने गरी सेवा करार गर्नुपर्दछ ।
- 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) लेखापरीक्षणका व्यहोरा (Audit Observation)

- कार्यालयले व्यावसायिक निरन्तरताको लागि **BCP** र विपद् व्यवस्थापनको लागि DRP लागू गरेको देखिएन। कम्प्युटर प्रणालीमा कुनै किसिमको अवरोध आएमा आवश्यकताको आधारमा तत्कालको लागि गर्न सकिने समाधान गर्ने गरेको पाइयो । Recovery Point Objective (RPO) र Recovery Time Objective (RTO) परिभाषित गरिएको छैन।
- एप्लिकेशन र डाटाबेस दुबै कार्यालका सर्भर, स्टोरेजहरुमा सेटअप गरी सरकारी एकीकृत डाटा सेन्टर (Government Integrated Data Center, GIDC), सिंहदरबारमा राखिएको छ। प्रणालीको सञ्चालन एवं मर्मत संभारको लागि कार्यालय र GIDC बीच कुनै औपचारिक सम्झौता गरेको पाइएन।
- एप्लिकेशन सर्भरलाई विभागको परिसरमा राखिएको छ। कोठा धुलाम्य भएको, केबल ट्याग नगरिएको, फायरवाल (Cyber Roam) जडान नगरिएको, बैकल्पिक एप्लिकेशन सर्भर नराखिएको, सर्भर राखिएको कोठामा आगो निभाउने उपकरण नभएको, सर्भर राखिएको सतह माथि नउठाईइको र कोठामा एउटा मात्र ढोका रहेको पाइयो। एप्लिकेशन सर्भरमा एन्टिभाइरस जडान गरिएको छैन।
- GIDC को पूर्ण लेखापरीक्षण यस लेखापरीक्षणको दायरा भन्दा बाहिर भए तापनि लेखापरीक्षण टोलीले GIDC मा डाटा सेन्टर (Data Center) र प्रकोप पूनःस्थापना सम्बन्धी व्यवस्था (Disaster Recovery Arrangements) परीक्षण गर्न डाटा सेन्टरको स्थलगत निरिक्षण गर्दा गर्दा डाटा केन्द्रको तापक्रम २६ डिग्री सेल्सियसमा राखिएको (२०-२४ डिग्री हुनुपर्ने)

पाइयो । तापमान र आर्द्रताको मापन गरिएको थिएन । काठको टेबल, तेल र ग्रीज जस्ता ज्वलन्त वस्तुहरू डाटा केन्द्रमा राखिएका थिए।

- MSP सँग गरिएको सम्झौताको बुँदा ४.७ मा डाटाबेस र एप्लिकेशन सर्भर GIDC मा हुनुपर्ने प्रावधान रहेको छ। डाटाबेस सर्भर GIDC मा मात्र राखिएको छ र एप्लिकेशन सर्भर विभागमै राखिएको छ। सम्झौताको उक्त बुँदामा डाटा र एप्लिकेसनको पहिलो प्राथमिकताको ब्याकअप (Primary Backup) GIDC मा राख्नुपर्ने र दोस्रो ब्याकअप (Secondary Backup) विभागमा हुनु पर्ने उल्लेख गरिएको छ।
- बैकल्पिक डाटासेन्टर (Alternative DC) नभएकाले गम्भीर जोखिम निम्त्याउन सक्छ।

ग) असर (Consequences)

Business Continuity Plan र **Disaster Recovery Plan** नहुँदा कार्यालयवाट सम्पादन हुने नियमित कार्यहरुमा अवरोध भएमा विभागले प्रवाह गर्ने व्यवसायसँग सम्बन्धित महत्वपूर्ण सेवा सुविधाहरु प्रभावित हुन जान्छन् । साथै सूचना प्रविधि प्रणाली एवं डाटाको समयमै पुनःस्थापना गर्न नसकिने वा कठिन हुने हुन्छ । आवश्यक तयारी नहुँदा कम्प्युटर प्रणालीको उपलव्धता नभएको अवस्थामा विभागका नियमित कार्यहरु सुचारु गर्न सकिदैन्। नष्ट भएको प्रणाली वा डाटाको समयमै पुनस्थापना (Restore) गर्न नसक्दा महत्वपूर्ण डाटा एवं तथ्यांकहरु नष्ट हुन, अनाधिकृत तवरले हेरफेर हुन वा चोरी हुन सक्छ ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- विभागले 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 प्रणाली र डाटाको सुरक्षा तथा सेवाको गुणस्तरको सम्बन्धमा लिखित रुपमा सम्झौता गर्नुपर्दछ। साथै सम्झौतामा **BCP** र **DRP** सँग सम्बन्धित विषयहरुलाई प्रष्टसँग उल्लेख गरेको हुनुपर्दछ ।

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 (Criteria)

- विभागमा डाटा एवं सूचनाको सुरक्षा सम्बन्धी जोखिमको मूल्यांकन गर्ने प्रभावकारी संयन्त्र हुनुपर्दछ ।
- जोखिम मूल्यांकन प्रक्रिया पर्याप्त सूचनामा आधारित हुनुपर्दछ । यसले विभागको आन्तरिक एवं बाह्य वातावरणको अध्ययन अनुसन्धान 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 (Audit Observation)

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 विभागले सुचना सुरक्षा (Data Security) मा देखिएका कमजोरी एवं खतराहरूबाट हुन सक्ने दुर्घघटनाहरू पहिचान गर्न र रोकथामका उपायहरू अवलम्बन गर्न सक्दैन् ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

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

ङ) व्यवस्थापनको जवाफ (Management Response)

२.५.२ सूचना सुरक्षा नीति

क) मूल्याङ्कनका आधार (Criteria)

- 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 कर्मचारीहरु र सेवा प्रदायकको भूमिका, जिम्मेवारी र कार्य विवरण स्पष्टरुपमा उल्लेख गरेको हुनुपर्दछ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

विभागले सूचना सुरक्षा नीति तयार गरेको पाईएन। डाटा एवं सूचना सुरक्षाको लागि कर्मचारी एवं सेवा प्रदायकको 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 (Recommendation)

- सञ्चार तथा सूचना प्रविधि मन्त्रालय वा सूचना प्रविधि विभागसँगको सहकार्यमा स्थापित मापदण्ड अनुरुप विभागका सूचनाको सुरक्षा सम्बन्धी विषयलाई समेटी सूचना सुरक्षा नीति तयार गर्नुपर्दछ।
- कर्मचारीहरूको कार्य विवरणमा स्पष्ट रूपमा सूचना सुरक्षा सम्वन्धि भूमिका र जिम्मेवारी तोकिनुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.५.३ प्रणालीको सुरक्षामा दक्ष जनशक्तिको प्रयोग

क) मूल्याङ्कनका आधार (Criteria)

- 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 हुनुपर्दछ।
- महत्वपूर्ण र संवेदनशील डाटा एवं सूचनामा पहुँच भएका कर्मचारीहरूको पृष्ठभूमि चेकजाँच गरी (Background Checks) र सुरक्षाको विषयमा आश्वस्त (Security Clearance) हुनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- 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 (Recommendation)

- प्रणाली एवं डाटाको सुरक्षाको लागि विभागले Data Owner, Data Custodian र डाटा प्रयोगकर्ताको भूमिका र जिम्मेवारीलाई स्पष्टरुपमा परिभाषित गरी लिखित अभिलेख राख्नुपर्दछ र सो सम्बन्धमा सबैलाई जानकारी गराउनुपर्दछ।
- विभागले कर्मचारीहरूलाई 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 (Management Response)

२.५.४ गोप्य सूचनाको संरक्षण

क) मूल्याङ्कनका आधार (Criteria)

- 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) लेखापरीक्षणका व्यहोरा (Audit Observation)

गोप्य राख्नुपर्ने सूचनाको संरक्षण गर्न आवश्यक नीति तयार गरेको पाईएन। साथै गोपनीयताको स्तरअनुसार तथ्यांकको वर्गीकरण गरिएको छैन।

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

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

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- विभागले 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 (Management Response)

२.६ सञ्चार र सञ्जाल (Communication and Network)

२.६.१ सुरक्षा प्याच (Security Patches)

क) मूल्याङ्कनका आधार (Criteria)

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 (Audit Observation)

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।

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

- कार्यालयले सुरक्षा प्याच (Security Patch) व्यवस्थापन नीति तयार गर्नुपर्दछ । यसमा कर्मचारीको भूमिका निर्धारण गरी कार्यान्वयन गर्नुपर्दछ।
- 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 (Management Response)

२.६.२ एन्टिभाइरस र एन्टिमालवेयर (Anti-Malware)

क) मूल्याङ्कनका आधार (Criteria)

सूचना प्रविधि प्रणालीलाई बाह्य जोखिमवाट वचाउन तथा जोखिम पहिचान गर्न उपयुक्त एन्टिमालवेयर / एन्टिभाइरस सफ्टवेयरको प्रयोग गर्नुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

ESET node 32 एन्टि-भाइरस सफ्टवेयर सेटअप गरिएको छ। एकान्तकुना विभागमा सेटअप गरिएको एन्टिभाइरस सफ्टवेयरको म्याद समाप्त भइसकेको छ।

ग) Antivirus प्रयोग नगर्दाको असर (सम्भाव्य जोखिमहरू)

सूचना प्रविधिमा विकास भएका खराब एप्लिकेशनहरु (Malwares) ले प्रणालीसँग सम्बन्धित उपकरण, सफ्टवेयर र डाटालाई Damage, Lost वा Modify गर्न सक्छन् ।

घ) लेखापरीक्षणको सिफारिस

एप्लिकेशन सर्भर, डाटावेस सर्भर र प्रयोगकर्ता कम्प्यूटर सबैमा Active Antivirus or Anti-Maleware सेटअप गरी समय समयमा अद्यावधिक गर्नुपर्दछ ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.६.३ Intrusion पहिचान गरी रोकथाम गर्न फायरवाल (Firewall) को प्रयोग गर्ने

क) मूल्याङ्कनका आधार (Criteria)

सफ्टवेयर प्रणालीको सुरक्षाको लागि प्रणालीमा हुनसक्ने Intrusion पत्ता लगाई सोको रोकथाम गर्ने उपकरण वा एप्लिकेशन (जस्तैः फायरवाल) प्रयोग गरिएको हुनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- विभागमा DAX फायरवाल प्रयोग गरेको पाइयो। सेवाप्रदायक (Madras Security Printing, MSP) सँग भएको सम्झौताको शर्त अनुसार १८ महिनासम्म फायरवाल निगरानी गर्न सेवाप्रदायक नै जिम्मेवार रहेको देखियो। तर, १८ महिना बितिसकेपछि पनि कुनै कर्मचारीलाई फायरवाल निगरानीको लागि तोकिएको छैन।
- वेभ सर्भर, HTTP प्रोटोकलमा चलिरहेको हुनाले सुरक्षित नरहेको पाइयो। सम्झौतामा (Secure Socket Layer) को प्रयोग गर्नुपर्ने प्रवधान रहेको छ। कुनै पनि कम्प्यूटरवाट Team Vewer मार्फत रिमोट पहुँच (Remote Access) दिने गरेको पाइयो। फायरवाल जडान गरिएता पनि एन्टिभाइरस जडान गरिएको पाइएन। असुरक्षित प्रोटोकल (TELNET) सार्वजनिक नेटवर्क (Public Network) मा चलिरहेको पाइयो।

ग) नियन्त्रणमा सुधार गर्न नसक्दाको असर (सम्भाव्य जोखिमहरू)

कम्प्युटर नेटवर्कमा Malicious Attack हुने सम्भावना बढि हुन्छ ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- फायरवाल सेटअपका नियमहरू (Firewall Rules) लाई समयसापेक्ष अद्यावधिक गर्नुपर्छ ।
- कर्मचारीलाई फायरवाल निगरानीको लागि जिम्मेवारी दिनुपर्छ।

- कुनै पनि किसिमको सञ्चार (Communication) गर्नुपर्दा सुरक्षित नेटवर्कबाट मात्र गरिनुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

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 हुनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

Configuration Management का लागि लिखित दस्तावेज छैन । नेटवर्क र कन्फिगरेशन (Configuration) को विस्तृत विवरण लेखापरीक्षणका क्रममा माग गरिए पनि उपलब्ध गराइएन। Wi-Fi बाट इन्टरनेटको प्रयोग गरिएको छ तर यो Ethernet Cable मार्फत हुनुपर्दछ।

ग) सूचना सुरक्षाको लागि उपयुक्त Configuration Management नगर्दा हुने असर (सम्भाव्य जोखिमहरू)

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

घ) लेखापरीक्षणको सिफारिस (Recommendation)

कार्यालयले प्रणालीसँग सम्बन्धित System and Configuration का आवश्यकताहरू पहिचान गरी बाह्य सेवाप्रदायकबाट भैरहेका कार्यहरुको प्रभावकारी अनुगमन गर्नुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.६.५ प्रणालीको कार्यसम्पादन

क) मूल्याङ्कनका आधार (Criteria)

- कम्प्युटर प्रणालीले तोकिएका सबै कार्यहरु प्रभावकारी रुपमा सम्पादन गर्नुपर्दछ। कार्य सम्पादन मापनमा Result/Output दिने समय (Response Time), सेवा प्रवाह (Throughput), सूचना प्रविधिजन्य साधनस्रोतको उपयोग, सफ्टवेयर एप्लिकेशनको उपलब्धता, Data Compression And Decompression, ईन्टरनेट Bandwidth को उपयोग जस्ता विषयहरु समावेश गरिनुपर्दछ ।

- इन्टरनेटमा समस्या आई सफ्टवेयर प्रणाली संचालन नहुने अवस्थालाई रोकथाम गर्न वैकल्पिक इन्टरनेट जडान गरिनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- कार्यालयमा कम्प्युटर प्रणालीले तोकिएका सबै कार्यहरु सम्पादन गर्न सकेको छैन। नेटवर्क सेवाहरू बाह्य सेवा प्रदायकबाट लिएको भनिएता पनि नियमित रूपमा नेटवर्क अनुगमन तथा मूल्यांकन प्रतिवेदन लिने गरिएको छैन। लेखापरीक्षण टोलीलाई नेटवर्क कहिले कहिले बन्द (**Network Down**) भएको थियो सोको प्रतिवेदन र सफ्टवेयर एप्लिकेशन मार्फत सम्पादन गरिएका कार्यहरुको अनुगमन तथा मूल्यांकन प्रतिवेदन उपलब्ध गराइएन।
- लेखापरीक्षणका क्रममा भएका छलफलबाट सेवा ग्राहिलाई प्रदान गरिने सेवा सुविधा मा अवरोध भएको (प्रणालीमा समस्या आई) समयावधि (**System** Down time) उल्लेखनीय भएको पाइयो। लेखापरीक्षण अवधिमा अनलाईन सूचना प्रविधि प्रणाली (**Online IT System**) पुरै एक दिनभर सञ्चालनमा आएको थिएन। यस्तो समस्या बारम्बार दोहोरिने भए तापनि समस्याको वास्तविक कारण पहिचान हुन सकेको छैन।
- विभागलाई र यातायात व्यवस्था कार्यालयहरुसँग L2 Connection द्वारा जडान गरिएको छ र Multiprotocol Label Switching (MLPS) VPN मार्फत सुरक्षित गरिएको छ।

ग) कार्यसम्पादन राम्रो नहुँदा पर्ने असर (सम्भाव्य जोखिमहरू)

- सूचना प्रविधि प्रणाली मार्फत प्रवाह गरिने सेवा प्रभावकारी भएन भने यसमा गरेको लगानी खेर व्यर्थ हुन जान्छ। साथै प्रणाली सञ्चालनमा समय समयमा अवरोध आयो भने Incomplete Data Input को कारणले Data Integrity जोखिम बढाउँछ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- प्रणालीको प्रभावकारी कार्यसम्पादन र निर्बाध उपलब्धताको नजिकबाट अनुगमन गर्न, प्रणालीमा बारम्बार आउने समस्याको वास्तविक कारण पहिचान गर्न र सुधारका दीर्घकालिन उपायहरुको कार्यान्वयनको लागि सूचना प्रविधिमा काम गर्ने कर्मचारीहरूलाई नियमित प्रतिवेदन उपलब्ध गराउनुपर्दछ ।
- पहिलो प्राथमिकताको (**Primary**) इन्टरनेट जडानमा केही समस्या हुँदा कार्यसम्पादन सुचारु राख्नको लागि वैकल्पिक व्यवस्थाको रुपमा दोस्रो प्राथमिकता (**Secondary**) को इन्टरनेट जडान गरिनुपर्दछ ।

ङ) व्यवस्थापनको जवाफ (Management Response)

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 राखिनुपर्दछ।
- कुनैपनि उपकरणहरुको बिक्री तथा लिलामीको लागि आवश्यक अख्तियारी हुनुपर्दछ।
- आवश्यक नभएका उपकरणहरु सुरक्षित तवरले बिक्री गरिनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- प्रणालीसँग सम्बन्धित हार्डवेयर र सफ्टवेयरको अभिलेख लेखा तथा भण्डारण प्रयोजनको लागि राखिएको भएता पनि सूचना प्रविधिजन्य उपकरण एवं सफ्टवेयरको विस्तृत सूची राखिएको छैन।
- हार्डवेयरहरू पुनः जडान गर्दा वा लिलामी गर्दा डाटा सुरक्षित रूपमा मेटाइएको कुरा सुनिश्चित गर्न कुनै नीति वा प्रक्रिया निर्धारण गरिएको छैन।
- लिलामी पूर्व सुरक्षित रूपमा डाटा धुल्याउने प्रक्रिया अपर्याप्त छ। अनुपयोगी उपकरणहरु लिलामी गर्न समिति गठन गरिएको छ।
- हार्डवेयर उपकरणहरु प्रतिस्थापन गर्ने योजना तर्जुमा गरिएको छैन।
- एकान्तकुनाको कार्यालयमा Window OS Genuine रहेको पाईएन।

ग) सूचना प्रविधिजन्य साधनश्रोतको व्यवस्थापन नगर्दाको असर (सम्भाव्य जोखिमहरु)

सूचना प्रविधि सम्बन्धी उपकरण तथा सफ्टवेयरहरु पूर्ण रूपमा सुरक्षित नहुन सक्छन। कार्यालयलाई यसको बारेमा जानकारी नहुन सक्छ ।

घ) लेखापरीक्षणको सिफारिस

विभागले सूचना प्रविधि सम्बन्धी हार्डवेयर, सफ्टवेयर, डाटा, नेटवर्क लगायतका सम्पूर्ण पूर्वाधारको मर्मत सम्भारको लागि उपयुक्त नीति र प्रक्रियाहरू अपनाउनु पर्दछ र हार्डवेयर पुनः जडान वा लिलाम गर्नुभन्दा पहिले त्यहाँ भएका तथ्यांकलाई स्थायी रुपले मेटाउने अथवा धुल्याउने गर्नुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.८ भौतिक सुरक्षा

क) मूल्याङ्कनका आधार (Criteria)

- भवन परिसर र सूचना प्रविधि क्षेत्रमा हुने पहुँच न्यायोचित, अधिकारिक, अभिलेख (**Log**) राखिएको र अनुगमन गरिएको हुनुपर्दछ। यो विषय परिसरमा प्रवेश गर्ने सबै व्यक्तिहरू जस्तैः स्थायी र अस्थाई दुवै कर्मचारी, सेवा प्रदायक, सेवा ग्राही, आगन्तुक वा तेस्रो पक्ष सबैमा लागू हुनुपर्दछ ।
- अनाधिकृत व्यक्तिहरूले हेर्न र प्रयोग गर्न नसक्ने गरी संवेदनशील डाटा एवं सूचनाको प्रयोग गरिने स्थानहरुलाई सुरक्षित गराउनु पर्दछ।
- 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 गरिनुपर्दछ।
- सूचना तथा सूचना प्रसोधन गर्ने उपकरणहरू (**Data and Data Processing Equipment**) भएका स्थानहरूलाई सुरक्षा घेरा भित्र राखिनुपर्दछ।
- अनधिकृत व्यक्ति प्रवेश गर्न सक्ने स्थानहरु (**Doors**) लाई नियन्त्रण गरिनुपर्दछ। सम्भव भएसम्म अनधिकृत पहुँचबाट बच्न सूचना प्रशोधन कार्य (**Data Processing Service**) लाई छुट्टै र केही दुरीमा राखिनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- भौतिक सुरक्षा मापदण्ड/कार्यविधि तर्जुमा गरिएको छैन ।
- परिसरमा प्रवेश गर्ने व्यक्तिको अभिलेख राख्ने गरिएको छैन ।
- विभाग तथा कार्यालयमा टर्मिनलहरू (कम्प्युटरमा पहुँच हुने किवोर्ड र स्क्रिन सहितको विद्युतीय उपकरण) सुरक्षितरूपमा (प्रयोगकर्ता बाहेक अरुले नदेख्ने गरी) राखेको पाइएन। यसवाट अनाधिकृत व्यक्तिले टर्मिनलमा हेरी तथ्यांक चोरी गर्न सक्छन्।

ग) भौतिक सुरक्षा नहुँदाको असर (सम्भाव्य जोखिमहरू)

कमजोर भौतिक सुरक्षा र नियन्त्रणले विभागले सूचना प्रविधिसँग सम्बन्धित उपकरण, सफ्टवेयर र डाटामा नोक्सानी पुऱ्याउन सक्दछ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- परिसरमा प्रवेश गर्ने व्यक्तिको अभिलेख राखिनुपर्दछ।

- गोप्य तथ्यांक प्रशोधन (Sensitive Data Manipulation) गर्ने टर्मिनलहरूको स्क्रिन अनाधिकृत व्यक्तिले नदेख्ने गरी राख्नुपर्दछ ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.९ पहुँच नियन्त्रण (Access Control)

२.९.१ सूचना प्रविधि पहुँच नीति

क) मूल्याङ्कनका आधार (Criteria)

प्रयोगकर्ताको जिम्मेवारी अनुसार प्रणालीमा पहुँच सुनिश्चित गर्नको लागि पहुँच नियन्त्रण सम्बन्धमा स्पष्ट नीति हुनुपर्दछ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

कार्यालयमा सूचना प्रविधि पहुँच सम्बन्धी नीति वा प्रक्रियाको निर्धारण गरिएको छैन। प्रणालीमा लग इन गर्नको लागि पासवर्ड र बायोमेट्रिक आवश्यक पर्ने Two Factor Authentication को व्यवस्था गरेको पाईयो।

ग) असर (Consequences)

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 गर्नुपर्दछ। विभिन्न तहका कर्मचारीलाई दिईने सबै किसिमका पहुँच (Access) हरू स्वीकृत गरी कार्य विवरणमा तोकिएको र आवश्यक पर्ने मात्र पहुँच प्रदान गरिनुपर्दछ ।

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 गर्नुपर्दछ।

- कर्मचारी सरुवा भएर जाँदा सरुवा रमाना दिँदानै साविकमा दिइएको पहुँचलाई हटाएर मात्र दिनुपर्दछ । सरुवा भएर आउँदा माथिल्लो तहको निर्देशन लिएर मात्र अभिलेख राखि आवश्यकता बमोजिम बढी अधिकार नहुने गरी प्रणालीमा पहुँच दिनुपर्दछ ।
- अवकाश हुने कर्मचारीहरूको पहुँच अधिकार पुनः सक्रिय गर्न नमिल्ने गरी निष्क्रिय गर्नुपर्दछ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- यातायात व्यवस्था कार्यालयको लागि प्रशासनिक अधिकारी (Administrative User) विभागका कम्प्युटर इन्जिनियरद्वारा सृजना गरिन्छ। त्यस पश्चात कार्यालय प्रमुखद्वारा कर्मचारीका लागि प्रयोगकर्ता (Username and Password) सृजना गरिन्छ। नियुक्ति पत्र रुजु गरी केन्द्रीय कार्यालयमा सर्वाधिकार प्रयोगकर्ताले (Superuser) नयाँ कर्मचारीको भूमिका तोक्दछ।
- एउटा कार्यालयवाट अर्को कार्यालयमा सरुवा भएमा प्रणालीबाट पहुँच निस्क्रिय गराई कर्मचारीले पदबहाली गर्ने कार्यालयमा रमाना पत्रको आधारमा पहुँच प्रदान गरिन्छ। यद्यपि, सरुवा भएको एउटा कर्मचारीको पहुँच कायम नै रहेको पाइयो।
- व्यक्तिगत प्रयोगकर्ताको पहुँच र सुविधाहरूको सेट-अप, परिमार्जन र निस्क्रियता पूर्ण रूपमा अभिलेखिकरण गरेको देखिएन।

ग) पहुँच नियन्त्रण हुँदा पर्ने असर (सम्भाव्य जोखिमहरू)

प्रयोगकर्ताको नाम र पासवर्ड (User Name and Password Combination) साझा हुने गरी प्रयोगकर्ताहरूलाई धेरै अधिकारहरु प्रदान गरिनु हुँदैन जसले तथ्यांकको फेरवदल हुने सम्भावना बढाउँछ र फेरबदल कसले गऱ्यो भन्ने पत्ता लगाउन गाह्रो हुन्छ। पहुँच र सुविधाहरू कार्यालय प्रमुखले स्वीकृत गरे पश्चात लिखित रूपमा अभिलेख राखेर मात्र प्रदान गरिनुपर्दछ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- कार्यालय प्रमुखद्वारा प्रयोगकर्तालाई अधिकार र सुविधाहरूको पहुँच प्रदान गर्न, संशोधन गर्न वा हटाउन उपयुक्त फारामको प्रयोग गरी अभिलेख राख्नुपर्दछ ।
- सूचना प्रविधिमा काम गर्ने कर्मचारीले प्रयोगकर्तालाई दिईएको पहुँच र सुविधाको विवरण स्वीकृत भए नभएको चेकजाँच गरी सोही बमोजिम प्रणालीमा पहुँच उपलव्ध गराई फाइलिङ गर्नुपर्दछ ।

- नयाँ कार्यालयमा सरुवा भएपछि विभागले अनिवार्य रुपमा प्रयोगकर्तालाई लाई निष्क्रिय गराउनुपर्दछ ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.९.३ पासवर्ड (Password)

क) मूल्याङ्कनका आधार (Criteria)

- प्रणाली प्रशासक (System Administrator) र सामान्य प्रयोगकर्ताहरुको लागि पासवर्ड नीति तयार गरी लागु गरेको हुनुपर्दछ। प्रयोगकर्ताहरूका लागि सुरक्षित पासवर्ड अभ्यास वारे सबै कर्मचारीलाई जानकारी गराउनुपर्दछ।
- मजबुत पासवर्ड राख्ने र समय समयमा पासवर्ड परिवर्तन गर्ने नीति लागू गर्नुपर्दछ ।
- हार्डवेयर र सफ्टवेयरमा सेट भएका (Saved) पासवर्डहरू परिवर्तन गरिनु पर्दछ।
- सफ्टवेयर, सर्भर र डाटामा सबै अधिकार सहितको पहुँच (System Administrator Access) को लागि Token वा Smart Card जस्ता Multifactor Authentication (MFA) प्रयोग गर्नुपर्दछ ।
- पासवर्ड सेट गर्दा सजिलो अक्षरहरु (Plane Text) र चलन चल्तिमा प्रयोग भैरहने नाम, शव्दहरु राखिनु हुँदैन।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

विद्यमान पासवर्ड अभ्यासहरूमा निम्न कमजोरीहरू पहिचान गरिएको थियोः

- पासवर्ड सम्बन्धी नियम तयार गरी लागु गरेको पाईएन।
- बलियो पासवर्ड (**Strong Password**) को लागि आवश्यक ढाँचा (**Format**) निर्धारण गरेको पाईएन।
- नयाँ प्रयोगकर्ता सेटअप गर्दा प्रयोगकर्ताले राख्नुपर्ने पासवर्ड कमजोर हुँदा पनि **System** ले स्वीकार गरेको पाइयो। **Complex Password** मात्रै लिने (**Accept**) गरेको पाईएन। सुरक्षित पासवर्ड ढाँचा लागू नगरेको र पासवर्ड पुनःसुनिश्चित (**Re-Confirm**) गर्ने व्यवस्था प्रणालीमा गरेको पाईएन।
- प्रयोगकर्ताले पहिलो पटक **System** मा **Log In** गर्दा पासवर्ड परिवर्तन गर्न अनुरोध गर्ने प्रक्रियालाई अनिवार्य गरिएको छैन।

ग) असर (Consequences)

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

घ) लेखापरीक्षणको सिफारिस (Recommendation)

विभागले अन्तर्राष्ट्रिय उत्तम अभ्यास अनुशरण गर्ने पासवर्ड नीति अपनाउनु पर्दछ । पासवर्डहरू गैर-विषयगत हुनुपर्दछ, सजिलै अनुमान योग्य हुनुहुँदैन र बलियो ढाँचाको हुनुपर्दछ। पासवर्डहरू निम्नलिखित ढाँचामा हुनुपर्दछः

- कम्तीमा आठ अक्षरहरू भएको।
- निम्नमध्ये एक वा बढी समावेश हुनुपर्दछः
    - lower-case letter
    - upper-case letter
    - number
    - punctuation mark.
- Administrator पासवर्ड लामो हुनुपर्दछ। क्रमरहित (Random) शब्दहरू सँगै राखी झट्ट हेर्दा उस्ताउस्तै देखिने वर्णहरू समावेश हुनुपर्दछ ।
- अत्यधिक संवेदनशील प्रणाली र डाटाको लागि विशेष पहुँच हुने स्थानमा Multi-Factor Authentication, जस्तै टोकन वा स्मार्ट कार्डहरू प्रयोग गर्नुपर्दछ।
- पासवर्ड नियन्त्रणमा मजबूत पासवर्ड, दोहोरो ईन्ट्री (Re-Confirm), पहिलो प्रयोगमा पासवर्डको अनिवार्य परिवर्तन जस्ता मापदण्ड राखिनुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.९.४ प्रणाली भित्रको Log In

क) मूल्याङ्कनका आधार (Criteria)

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

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- Log-In/ Log-Out नीति तयार गरी कार्यान्वयन गरेको पाईएन।
- तोकिए भन्दा बढीपटक असफल Log-In Attempt पछि प्रयोगकर्ताको User Account स्वतः निस्क्रिय हुने व्यवस्था लागु गरिएको छैन जसले गर्दा प्रणालीमा Brute Force Attack जस्ता जोखिम रहने देखिन्छ ।

ग) असर (Consequences)

विभागको प्रणालीमा अनाधिकृत व्यक्तिहरूले पहुँच प्राप्त गरी डाटाको गोपनीयता र Data Integrity कायम नरहन सक्छ ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- विभागले 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

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

ख) लेखापरीक्षणका व्यहोरा

Administrator तथा अधिकार प्राप्त प्रयोगकर्ताहरूले उच्चस्तरीय तथा विशेषाधिकार पहुँच प्राप्त गर्ने हुनाले यस्ता पहुँचलाई कडाइका साथ नियन्त्रण गरिनुपर्दछ। लेखापरीक्षणका क्रममा निम्न विषयहरू देखिए:

- Administrator अधिकारलाई पर्याप्त कडाइका साथ नियन्त्रण नगरिएको र फायरवाल कन्फिगरेसनको कार्य बाह्य सेवाप्रदायक मार्फत गराईएको छ। यद्यपि, अन्य सेवाप्रदायकहरुलाई पनि फायरवालमा पहुँच भएको पाइयो।
- Administrator अधिकार प्रदान गर्नको निमित्त एउटा **Username** बनाई सोही **Username** सबै प्रयोगकर्ताहरूद्वारा साझा प्रयोग गरेको पाइयो। तसर्थ, कुन व्यक्तिले कुन कामको जवाफदेहिता लिने भन्ने स्पष्ट भएन ।

ग) नियन्त्रणमा सुधार गर्न नसक्दाको असर (सम्भाव्य जोखिमहरु)

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

घ) लेखापरीक्षणको सिफारिस

- कार्यको प्रभावकारितको लागि पहुँच अत्यावश्यक भए मात्र उच्चस्तरीय Administrator पहुँच दिइनुपर्दछ। सो पहुँच अनावश्यक भएमा तुरुन्त खारेज गरिनुपर्दछ।
- Administrator पहुँच प्रदान गर्न **Generic Username** प्रयोग गर्ने कार्य तुरुन्त स्थगित गरिनुपर्दछ। यसको सट्टा, व्यक्तिपिच्छे फरक **Username** सेट गरी **Administrator** अधिकार दिइनुपर्छ। यी प्रयोगकर्ताहरूको गतिविधिको अभिलेख राखिनुपर्छ र स्वतन्त्र व्यक्तिबाट नियमित रूपमा समीक्षा गरी मूल्यांकन गरिनुपर्छ।

ङ) व्यवस्थापनको जवाफ

२.१० बाह्य सेवा **(Out Sourcing)**

२.१०.१ बाह्यसेवा प्राप्ति नीति

क) मूल्याङ्कनका आधार (Criteria)

कार्यालयले बाह्य सेवा प्रदायक (Outsourcing) वाट सेवा लिने कार्यका सम्बन्धमा स्पष्ट कार्यविवरण र जिम्मेवारी सहितको नीति हुनुपर्दछ । कार्यालयका महत्वपूर्ण डाटा तथा सूचनामा पहुँच हुने गरी (Core Business को लागि) बाह्य सेवा प्रदायकवाट सेवा लिनुहुँदैन। Support and Maintenance जस्ता Supporting Business को लागि मात्र बाह्य सेवा प्रदायक नियुक्त गर्नुपर्दछ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

विभागले आउटसोर्सिङ गर्न आवश्यक नीति बनाएको देखिएन। यसको बाबजुद कम्प्युटर प्रणालीको विकास र संचालनका लागि बाह्य सेवाप्रदायकसँग कार्यालय अत्यधिक मात्रामा निर्भर रहेको छ। तथापि आउटसोर्सिङ प्राप्त गर्दा सार्वजनिक खरिद ऐन, २०६३ को पालना गरी खरिद गरिएका छन्। विदेशी सेवा प्रदायकवाट बाह्य सेवा प्राप्त गर्ने सम्बन्धी नीति रहेको पाईएन ।

ग) नियन्त्रण सुधार गर्न असफलताको परिणामहरू (सम्भावित जोखिम)

बाह्य सेवामा अधिक निर्भरताका कारण जोखिम बढ्दै जान्छ ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

कार्यालयले आउटसोर्सिङ सम्बन्धी स्पष्ट नीति अख्तियार गरी बाह्य निर्भरता कम गर्दै लैजानु पर्दछ । बाह्य सेवा आवश्यक भएमा Supporting Business को लागि सम्झौता गरी लिइने सेवामा नियन्त्रण र कार्यसम्पादन समेत उल्लेख गरिनुपर्दछ। (उदाहरणका लागि सुरक्षा, डाटा अधिकार, कार्यसम्पादन प्रतिवेदन, जरिवाना आदि)

ङ) व्यव्यवस्थापनको जवाफ (Management Response)

२.१०.२ सेवा प्रदायक र करार अनुगमन

क) मूल्याङ्कनका आधार (Criteria)

- प्रत्येक सेवा प्रदायकसँग करार संझौता गरिएको हुनुपर्दछ।
- आवश्यक पर्ने सेवाहरूको तह पहिचान गरी सेवा सम्झौता गरिनुपर्दछ।
- सेवा प्रदायकसँग लिईने सेवाहरूको अनुगमनको व्यवस्था हुनुपर्दछ।
- सम्झौता मार्फत सेवाको गुणस्तर सुनिश्चितता गरिएको हुनुपर्दछ।
- सेवा सम्झौताका प्रावधानहरू कार्यान्वयन नहुँदा उचित कारबाहीको व्यवस्था गर्नुपर्दछ ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- EDLVRS को निर्माण गर्न विदेशी सेवाप्रदायकसँग बाह्यसेवा प्राप्त गरिएको छ। सेवा करार सम्झौताको खण्ड ४.२ को कार्यसम्पादन मानकमा, सेवाको कार्य सम्पादनको मापन (Performance Matrix) तोकिएको छ। यद्यपि, सोको अनुगमन गरी सुधारात्मक कदम चालिएको छैन।

- EDLVRS को लागि सेवा सम्झौता (Service Level Agreement- SLA) सेप्टेम्बर २०१३ मा गरिएको थियो। सो सम्झौताको करार अवधि १५ महिनाको रहेको थियो । पटक पटक नवीकरण भई EDL खण्डको आधिकारिक स्वीकृति प्रदान गरिएको छ। सम्झौताको VRS खण्ड अझै अपूरो छ। करारको खण्ड २८ बमोजिम क्षतिपूर्ति दाबी गरिएको छैन।
- अनुसूची १ को बुँदा १ मा डाटा माईग्रेशनमा EDLVRS को व्यावसायिक र कार्यगत आवश्यकताको आधारमा सेवा प्रदायकले हालको प्रणालीबाट डाटा माईग्रेशन गर्नुपर्छ र म्यानुअल प्रणालीमा रहेका डाटा प्रविष्ट गर्नुपर्छ भनी उल्लेख गरिएको छ तर डाटा माइग्रेशन कार्य पूरा भएको छैन।
- सेवा सम्झौताको खण्ड ५.२.८ मा Wide-Area नेटवर्क अनुसार सेवाको उपलब्धता ९९.९९% हुनुपर्छ भनी उल्लेख गरिएको छ तर यसको कुनै अनुगमन गरिएको छैन।
- सेवा सम्झौताको खण्ड ५.२.८ अनुसार एन्टिभाइरस, एडवेयर र एन्टिमालवेयर सफ्टवेयर सर्भरमा सेटअप गर्नुपर्ने भनी उल्लेख गरिएता पनि एप्लिकेशन सर्भरमा एन्टिभाइरस सेटअप गरिएको छैन।
- सेवा सम्झौताको खण्ड ४.६ मा प्रणाली सञ्चालनमा अवरोध आउन सक्ने अधिकतम समय (Maximum Down-Time) र सोको उल्लंघन भएमा दण्डको व्यवस्था गरिएता पनि Down-Time को अनुगमन गरिएको छैन।
- सेवा सम्झौताको खण्ड ४.७ अनुसार डाटाबेस र एप्लिकेशन सर्भर GIDC मा र डाटाबेस तथा एप्लिकेशनको सेकेन्डेरी व्याकअप विभागमा हुनुपर्ने व्यवस्था छ। तर, डाटाबेस सर्भर GIDC मा मात्र रहेको छ भने एप्लिकेशन सर्भर कार्यालयमा मात्र रहेको छ।
- स्मार्ट कार्ड छपाई गर्न प्रिन्टर तथा सवारी चालक अनुमतिपत्रको लागि स्मार्ट कार्डको आपूर्ति, सेटअप, जडान, वितरण र कमिसनिङ गर्न बाह्य सेवाप्रदायक (Madras Security Printing, MSP) संग ३० अप्रिल २०१९ मा सेवा करार सम्झौता गरिएको थियो र सम्झौता भएको मितिबाट ७५ दिनभित्र सेटअप तथा जडान पूरा गरिसक्नुपर्ने भनिएको थियो तर प्रिन्टरलाई EDLVRS सफ्टवेयरसँग Integrate/Configure नभएकाले अनुमतिपत्र कार्डहरु छपाई गर्न सुरू भएको पाईएन।

ग) नियन्त्रण सुधार गर्न असफलताको परिणामहरू (सम्भावित जोखिम)

कार्यालयको सूचना प्रविधि प्रणालीको विकास, सञ्चालन तथा व्यवस्थापन प्रभावकारी बनाउन सकिदैन। प्रणालीको नियन्त्रण गर्न र कार्यसम्पादन व्यवस्थापन गर्न विभाग असक्षम हुनसक्छ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- कार्यालयले सेवाप्रदायकलाई सम्झौता भएका प्रमुख कार्यहरुको कार्य सम्पादन मापन (KPIs) को प्रतिवेदन नियमित बुझाउन लगाउनुपर्छ र उच्च कार्यसम्पादन स्तर कायम गर्नका लागि अनुगमन, आन्तरिक रिपोर्टिङ र सुधारात्मक व्यवस्थाहरूको कार्यान्वयन गर्नुपर्दछ। बाह्य सेवा प्राप्त गर्न आवश्यक नीति तथा कार्यविधि तर्जुमा गरिनुपर्दछ ।
- सम्झौताका सर्तहरु सम्झौता अवधि भित्र पूरा गराईनुपर्दछ र कार्य सम्पादन नभएको अवस्थामा क्षतिपूर्ति दाबी गरिनुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१०.३ दक्ष जनशक्तिको टिकाउ (Retaining)

क) मूल्याङ्कनका आधार (Criteria)

- कार्यालयले बाह्य सेवाप्रदायकले सेवा प्रदान गर्न असमर्थ भएमा पनि महत्वपूर्ण एवं संवेदनशील कार्यहरू सञ्चालन गर्न सकिने गरी कार्यालय भित्रै व्यावसायिक ज्ञान भएको जनशक्तिको व्यवस्था गर्नुपर्दछ।
- व्यावसायिक प्रक्रियाको स्वामित्व कार्यालयमै रहनुपर्दछ।
- कार्यालयले बाह्य सेवाप्रदायकले सेवा प्रदान गर्न असमर्थ भएमा पनि महत्वपूर्ण एवम् संवेदनशील कार्यहरू सञ्चालन गर्न सकिने गरी कार्यालय भित्रै व्यावसायिक ज्ञान भएको जनशक्तिको व्यवस्था गर्नुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- बाह्य सेवाप्रदायकहरूले कार्यसम्पादन नगर्दा वा कार्यसम्पादन गर्न असक्षम भएको खण्डमा विभागले आन्तरिक रूपमा कार्यहरू सञ्चालन गर्न सक्ने व्यावसायिक ज्ञान भएको जनशक्ति व्यवस्था गरेको पाईएन। व्यवसायिक ज्ञान भएको जनशक्ति टिकाईराख्नका लागि कुनै विशेष नीति अख्तियार गरेको देखिएन।
- EDLVRS प्रणालीको को सोर्स कोड (Source Code) अझै विभागलाई हस्तान्तरण गराइएको छैन। सेवा करार सम्झौतामा विश्वसनीय तेस्रो पक्षको Escro Account मा सोर्स कोड राख्ने बारे कुनै प्रावधान रहेको छैन।

ग) नियन्त्रणमा सुधार गर्न नसक्दाको परिणामहरू (सम्भावित जोखिम)

सेवाप्रदायकहरूसँग सम्झौताहरू रद्द भएमा वा सेवाप्रदायकहरूले सेवा आपूर्ति गर्न असक्षम भएमा विभागको कम्प्युटर प्रणाली दिगो र प्रभावकारी रुपले सञ्चालन हुन सक्दैन।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- प्रमुख कार्यहरु संचालन गर्न विभागले आन्तरिक सूचना प्रविधि क्षमताको सुदृढीकरण गर्नुपर्दछ।
- सेवा सम्झौतामा Escro Account मा सोर्स कोडको भण्डारणको लागि प्रावधान राखिनुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१०.४ बाह्य सेवा प्रदायकबाट लिईएका सेवाको व्यवसाय निरन्तरता नीति(BCP) /प्रकोप पुनर्स्थापना योजना(DRP)

क) मूल्याङ्कनका आधार (Criteria)

- बाह्य सेवा प्रदायकले करारमा व्यवस्था भएको व्यवसाय निरन्तरता नीति (BCP) /प्रकोप पुनर्स्थापना योजना(DRP) सम्बन्धी प्रावधानहरूको पालना गर्नुपर्दछ ।
- बाह्य सेवा प्रदायकले आफ्ना प्रक्रियाहरू आवधिक रूपमा परीक्षण गर्नुका साथै BCP/DRP सम्वन्धि आवश्यकताहरू पूरा भएको पुष्टि गर्नका लागि स्वतन्त्र वा आन्तरिक लेखा परीक्षण प्रतिवेदन उपलब्ध गराउनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

सेवाप्रदायकहरूसँगको करार संझौतामा डाटा र सेवाहरूको लागि व्यवसाय निरन्तरता नीति (BCP) प्रकोप पुनर्स्थापना योजना (DRP) को व्यवस्था उल्लेख गरेको पाइएन।

ग) नियन्त्रणमा सुधार गर्न नसक्दाका परिणामहरू (सम्भावित जोखिम)

सेवाप्रदायकका कारण सेवा अवरुद्ध हुने तथा सही तथ्यांक प्राप्त नहुन सक्दछ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

सेवाप्रदायकसंग बाह्यसेवा प्राप्त गर्न भविष्यमा हुने सबै करार संझौतामा पर्याप्त रूपमा व्यवसाय निरन्तरता नीति (BCP) /प्रकोप सुधार योजना (DRP) को सुनिश्चितता गराउनुपर्ने सर्त उल्लेख भएको हुनुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.११ Generic Application Controls

२.११.१ इनपुट (Input)

क) मूल्याङ्कनका आधार (Criteria)

- कारोवारहरु मान्यता प्राप्त स्रोतबाट मात्र भएको हुनुपर्दछ। सुरुवातबाटै कारोवारहरुमा त्रुटी नहुनेगरी नियन्त्रण कायम गरिनुपर्दछ। डाटा तयारी प्रक्रियाहरू पूर्ण रूपमा अभिलिखित र प्रयोगकर्ताहरूले बुझ्ने हुनुपर्दछ। ऐप्लिकेशनमा डाटा प्रविष्टि हुनु अघि उचित लगिङ (Logging) र स्रोत कागजातहरू (Source Document) को रेकर्ड राखेको हुनुपर्दछ। हरेक कारोवारको विशेष क्रम संख्या प्रदान गरिनुपर्दछ। सक्कल स्रोत कागजातहरू कानूनी मापदण्ड वा नीतिहरूद्वारा निर्धारण गरिएको समय सम्मको लागि राखिनुपर्दछ।
- कारोबार स्पष्ट रूपमा म्यानुअल वा इलेक्ट्रोनिक माध्यमद्वारा प्रमाणीत गरिएको हुनुपर्दछ। इनपुट गर्ने र प्रमाणीत गर्ने कार्यको स्पष्ट कार्य विभाजन गरिएको हुनुपर्दछ। कारोबारको लागि प्रमाणीत गर्ने पदियस्तर निर्धारण गरिएको हुनुपर्दछ, प्रतिनिधिमण्डलको सहमतिपूर्ण योजनाको साथ उचित नियन्त्रण लागू गरिएको हुनुपर्दछ। कर्तव्यहरूको निर्धारण सम्भव नहुने मुद्दाहरूको लागि (Compensating Control) लागूगरिनुपर्दछ। प्रशोधनको लागि मापक र अन्य स्थायि डfटा (Standing Deta) कडाइका साथ पालना गरिनुपर्दछ। इनपुटको लागि समय तालिका निर्धारण गरी पालना गरिएको हुनुपर्दछ।
- प्रयोगकर्ता र संचालन कर्मचारीहरूले बुझ्ने किसिमको स्पष्ट प्रशोधन सूची तयार गरेको हुनु पर्दछ । वैधिकरण नियमहरू विस्तृत र अभिलिखित भई एप्लिकेसन इन्ट्री Interfaces मा लागू गरिएको हुनुपर्दछ; डाटा प्रविष्टिका बिभिन्न विधिहरू र Interfaces अभिलिखित हुनुपर्दछ; असङ्गत डाटालाई एप्लिकेसनले अस्वीकार गर्नुपर्दछ; वैधिकरण मापदण्ड समयानुकूल, उपयुक्त र आधिकारीक तरिकाले अपडेट गर्नुपर्दछ। इनपुट नियन्त्रण परिसीमित (Overriding) भएको अवस्थामा लग (Log) र स्वीकृति (Authorisation) नियम जस्ता पूरक नियन्त्रणहरू हुनुपर्दछ। Application Interface का लागि उपयुक्त नियन्त्रणहरू र अभिलेख रहेको हुनुपर्दछ।
- प्रत्येक प्रकारको त्रुटिको लागि तत्काल सुधारात्मक कार्यहरू गर्न समस्याहरूको संचार गर्न स्पष्ट र कम्प्याक्ट (Compact) त्रुटि सन्देश प्रणाली हुनुपर्दछ। कारोबार प्रशोधन हुनुभन्दा पहिले त्रुटिहरूको सुधार वा उचित ओभरराइड (Override) गरिनुपर्दछ। लगहरू आवधिक रूपमा समीक्षा तथा आवश्यक सुधारात्मक कार्य गरिनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- Application ID विशेष प्रकारको भए तापनि, एउटै एप्लिकेसनबाट धेरै प्रकारका प्रविष्टिहरू गरिएका छन्।
- पहिले नै प्रणालीमा लग इन गरेका प्रयोगकर्ताले अर्को कम्प्यूटवाट प्रणालीमा पूनः लग इन गर्दा सो प्रयोगकर्ताको अघिल्लो सत्रको) Session (निष्क्रिय हुदैन।
- नागरिकता लगायत विशेष परिचय पत्रको आधारमा जाँचपश्चात मात्र दर्ता गर्न अनुमति दिनुपर्दछ। एउटा आवेदकले एकै समयमा दुई पटक दुई पटक प्रणालीमा दर्ता गरेको देखियो ।

- वैधिकरण जाँचहरु उचित रुपमा Configure गरिएको छैन। उदाहरणको लागी अशोक महर्जनको रिपोर्टले इजाजत पत्र जारी भएको मिति २०६१।६।१२ देखाउँछ तर लाइसेन्स नवीकरण २०६०।०५।२४ मा देखाउँछ।

ग) नियन्त्रण सुधार गर्न असफलताको परिणामहरू (सम्भावित जोखिम)

गलत/अनुचित डाटा प्रणालीमा प्रविष्ट गर्न सकिने हुनाले प्रणालीले लक्षित उद्देश्य प्राप्त गर्न सक्दैन।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- वैधिकरण नियन्त्रणहरु प्रभावकारी बनाइनु पर्दछ।
- इनपुटमा नियन्त्रणको लागि सत्र (Session) लग आउट उचित रुपले राखिएको हुनुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.११.२ प्रशोधन (Processing)

क) मूल्याङ्कनका आधार (Criteria)

ऐप्लिकेशनमा व्यावसायिक प्रक्रिया (सेवा प्राप्त गर्ने प्रकृया) र आवश्यकता मिलान गरिनुपर्दछ। प्रोग्रामले प्रक्रिया सफलतापूर्वक सम्पन्न भएको पुष्टि गर्नुपर्दछ । सेवा प्राप्त गर्ने क्रममा सेवा प्राप्त गर्ने प्रकृयाको असामान्य समाप्ति (Process Termination) भएको खण्डमा पुन प्राप्ति र पुनः पेश गर्ने प्रक्रिया प्रणाली अद्यावधिक गरेको हुनुपर्दछ। एप्लिकेशनले पूर्णता, डाटा सत्यता, वैधता र विश्वसनीयता प्रदान गर्नुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- यातायात व्यवस्थापन कार्यविधि निर्देशिकाको खण्ड १२.१३ मा एक पटक प्रयोगात्मक परीक्षामा अनुत्तीर्ण भएका परीक्षार्थीले लिखित परीक्षा उत्तीर्ण भएको ९० दिनभित्र पुनः दुई पटक तोकिएको दस्तुर तिरी प्रयोगात्मक परीक्षा दिन पाउनेछ भनी उल्लेख गरिएको छ। तर, प्रणालीले सो समयावधि प्रयोगकर्ताले दर्ता गरेको मितिदेखि गणना गर्दछ।
- इजाजतपत्र ५ वर्षसम्म नवीकरण नगरिएमा प्रणालीले स्वत :सो इजाजतपत्र रद्द गरिनु पर्दछ। तथापि, प्रणालीमा सो सम्बन्धी कुनै व्यवस्था रहेको देखिएन।
- सफ्टवेयरमा अंकगणितिय हिसाबमा त्रुटि देखिएको छ। उदाहरणका लागि, २*५०० लाई ५०० देखाउँदछ।
- नयाँ दर्ता श्रेणी ए मा गरिएको भए तापनि रसिदमा) बिल (श्रेणी बी देखियो।

ग) नियन्त्रण सुधार गर्न असफलताको परिणामहरू (सम्भावित जोखिम)

गलत डाटा प्रशोधनले प्रणालीको विश्वसनीयता घटाउँदछ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

असंगतिहरू सुधार गर्नका लागि EDLVRSको प्रयोगकर्ता स्विकार्य परीक्षण (User Acceptance Test-UAT) \ सफ्टवेयर लेखापरीक्षण गराउनु पर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.११.३ आउटपुट (Output)

क) मूल्याङ्कनका आधार (Criteria)

- आउटपुटको लागि जिम्मेदार कर्मचारीले आउटपुटको पूर्णताको सुनिश्चितता गर्नुपर्दछ। आउटपुटहरूको उपयोगिताको समीक्षा गरिनु पर्छ । एपलिकेसनवाट सृजना हुने आउटपुटको पूर्णता र शुद्धता जाँच गरेपछि मात्र अनुवर्ती **(Follow up)** प्रक्रियामा समावेश गर्नु पर्दछ। सबै कारोवारको स्रोतको जानकारी राखिएको हुनुपर्दछ। आउटपुटको स्पष्ट रूपमा पहिचान गरी पूर्णता दर्शाउने जानकारी समावेश हुनुपर्दछ। कर्मचारीहरू नतिजाको पूर्णता र व्यावहारिकता सुनिश्चित गर्न जिम्मेवार वनाईनु पर्दछ ।
- नतिजा **(Output)** वितरणवाट Output सही स्थान/प्रयोगकर्ताहरूमा पुग्ने र गोपनीयता कायम रहेको सुनिश्चितता गरिनु पर्दछ।
- विद्यमान कानून र नियमहरु अनुसार आवश्यक अवधिको लागि पर्याप्त Output राखिएको हुनुपर्दछ।
- 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।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

- एप्लिकेशनको रिपोर्टिंग प्रणाली कमजोर रहेको पाइयो।
- सुपर प्रशासक (Super Admin)ले युजर लगइन(User Login) आदिको अडिट ट्रेल हेर्नका लागि एप्लिकेशनमा व्यवस्था नहुदा अडिट ट्रेल निगरानी सक्दैनन् । खोजी गर्दा (सर्च अप्सन) नाम वा मापदण्ड बहुउदाहरणहरूसँग मेल खाए पनि केवल १० रेकर्डहरू मात्र देखाइन्छ र अन्य मेल खाने रेकर्डहरू देखाईँदैन।
- प्रयोगकर्ता (User) अनुसार खाता रिपोर्टले नयाँ अनलाइन दर्ता गरिएको हो वा पुनः ट्रायल दर्ता (रेजिष्ट्रेसन) हो भनी देखाउँदैन।

- रिपोर्टमा विषयहरूको दोहोरोपना भएको पाइयो। उदाहरणको लागि कुनै ड्राइभर परीक्षा उत्तीर्ण भएमा उनको नाम ट्रायल परीक्षाको तालिकामा दुई पटक भएको पाईयो । लिखित परीक्षाको तालिकामा पनि दोहोरो नाम रहेको पाईयो।
- अनलाईन सफ्टवेयर र RIMS बीच हिसाब मिलान गरेको पाइएन।
- राजस्व संकलनको एकीकृत रिपोर्ट प्रणालीबाट प्राप्त गर्न सकिँदैन।
- परीक्षाको विवरणमा एउटै व्यक्ति विभिन्न मितिमा दुई पटक पास भएको देखिन्छ । साथै यसको परीक्षा मिति खण्ड खाली रहेको छ।

ग) नियन्त्रण सुधार गर्न असफलताको परिणामहरू (सम्भावित जोखिम)

कमजोर रिपोर्टिंगले सेवा/कार्यक्षमतालाई अप्रभावी तुल्याउँदछ। संकलन भएको राजस्व र RIMS का रेकर्डहरु मिलान गर्ने प्रणालीको अभाव हुंदा यकिन नहुने तथा हिनामिन हुनसक्ने अवस्था देखियो।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

निम्न सुझावहरुको टिप्पणी गरिएको छः

- प्रणालीको रिपोर्टिङमा सुधार गरिनु पर्दछ।
- प्रणाली र राजस्व सूचना व्यवस्थापन प्रणाली (RIMS) को आँकडाको हिसाब मिलान गरिनु पर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.११.४ अडिट ट्रेल

क) मूल्याङ्कनका आधार (Criteria)

- Audit Trail ले महत्वपूर्ण कारोबारको सम्पादन, Overrides र प्रमाणीकरणका लगहरू प्राप्त गर्नुपर्दछ।
- अनाधिकृत गतिविधि निगरानीको लागि अडिट ट्रेलको समय समयमा समीक्षा गरिनुपर्दछ।
- Audit Trail सुरक्षित हुनुपर्दछ। प्रत्येक कारोबारलाई फरक किसिमको र अनुक्रमिक संख्या वा संकेत तोकिएको हुनुपर्दछ। Audit Trail फाईल वा रिपोर्टहरू पूर्ण हुनुपर्दछ। Audit Trail लाई निष्क्रिय गरेमा सोको विवरण समावेश हुनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

महत्वपूर्ण कारोबारको लागि सम्पादन, Overrides र प्रमाणीकरणका लगहरूको अडिट ट्रायल उपलब्ध भएन र Audit Trail अनुगमन गरिएको सम्बन्धमा अभिलेखन गरिएको छैन।

ग) नियन्त्रण सुधार गर्न असफलताको परिणामहरू (सम्भावित जोखिम)

Audit Trail अनुगमनको अभावमा व्यवस्थापनलाई अनधिकृत गतिविधि भए वा नभएको बारे आश्वासन दिन सकिँदैन।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

विभागमा उचित Audit Trail बनाउनु पर्दछ र नियमित समीक्षा गरिनु पर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१२ वेबसाइट निर्माण तथा व्यवस्थापन सम्बन्धी निर्देशिकाको अनुपालना

क) मूल्याङ्कनका आधार (Criteria)

इन्टरनेट वेबसाइटले सरकारी निकायको वेबसाइट निर्माण तथा व्यवस्थापनसम्बन्धी निर्देशिका, २०६८ बमोजिमका व्यवस्थाको पालना गरेको हुनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

सरकारी निकायको वेबसाइट निर्माण तथा व्यवस्थापनसम्बन्धी निर्देशिका, २०६८ को बुँदा ६(च) मा बुँदा ६(छ) निर्माण गरिएको वेबसाइटको सुरक्षण जोखिमताको परीक्षण (Security Vulnerability Audit) गरिएको हुनुपर्ने तथा बुँदा ८ मा प्रत्येक वेबसाइटलाई विशेष आगन्तुक, धेरै पटक अवलोकन गरिएका पृष्ठहरू, Bandwidth उपयोग इत्यादिको आधारमा मूल्याङ्कन गर्ने प्रावधान रहेको छ। त्यसैगरी बुँदा ९ मा प्रत्येक कार्यालयमा वेबमास्टर खटाइने र बुँदा १२ मा प्रत्येक सरकारी कार्यालयले सरकारी इमेल प्रयोग गर्नुपर्ने प्रावधान रहेको छ। विभागले वेबसाइटको सुरक्षा जोखिम लेखापरीक्षण गराइएको देखिएन र निर्धारित मापदण्ड अनुरुप वेबसाइटको मूल्यांकन नगरिएको, वेबमास्टर नखटाइएको र स्वीकृत इमेल प्रणाली प्रयोग नगरिएको देखियो।

ग) नियन्त्रण सुधार गर्न असफलताको परिणामहरू (सम्भावित जोखिम)

सरकारी निर्देशिकाको उल्लघंन हुने ।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

सरकारी निकायको वेबसाइट निर्माण तथा व्यवस्थापन सम्बन्धी निर्देशिका, २०६८ को सबै प्रावधानहरूको पालना गर्नुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१३ Vulnerability Assessment and Penetration Test) VAPT(

क) मूल्याङ्कनका आधार (Criteria)

विभागले नेटवर्क र प्रणालीहरूको Vulnerability Assessment and Penetration Test (VAPT) नियमित रूपमा गर्नुपर्दछ। VAPT मार्फत पहिचान भएका जोखिम र कमजोरीहरू कम गर्न र समाधान गर्न सुधारात्मक कदम चालिनु पर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

Vulnerability Assessment and Penetration Test) VAPT (गरेको पाइएन। सूचना प्रविधि शाखाद्वारा Vulnerability Assessment परीक्षण गराइएको भए तापनि सोको प्रतिवेदन लेखापरीक्षण टोलीलाई उपलब्ध गराइएन।

ग) नियन्त्रण सुधार गर्न असफलताको परिणामहरू (सम्भावित जोखिम)

VAPTको अभावमा सबै सुरक्षा जोखिमहरू पत्ता लगाउन सकिँदैन र सुरक्षा जोखिम आउनुभन्दा अगावै निरोधात्मक उपायहरू लागू गर्न सकिँदैन।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

VAPT परीक्षणबाट जोखिम पहिचान गरी समाधान वा जोखिम कम गर्नुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१४ प्रयोगकर्ता स्वीकृति परीक्षण

क) मूल्याङ्कनका आधार (Criteria)

- सबै नयाँ कम्प्युटर प्रणालीहरूको स्वीकृति अघि User Acceptance Test (UAT) भएको हुनपर्दछ।
- अन्तिम प्रयोगकर्ताहरू सक्रिय रूपमा परीक्षण प्रक्रियामा संलग्न रहेको हुनुपर्दछ र अन्तिम प्रयोगकर्ताहरूले स्वीकृति औपचारिक रूपमा लिएको हुनुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

विभागको सफ्टवेयर स्वीकृत हुनुभन्दा पहिले प्रयोगकर्ता स्वीकृति जाँच (User Acceptance Test-UAT) गराइएको पाईएन।

ग) नियन्त्रणहरू सुधार गर्न असफलताको परिणामहरू (सम्भावित जोखिम)

User Acceptance Test-UAT) को अभावमा लागू गरिएको प्रणालीले प्रयोगकर्ता तथा सेवाग्रहीका आवश्यकता पूरा गर्दैन र सुरक्षित नियन्त्रण वातावरण प्रदान गर्दैन।

घ) लेखापरीक्षणको सिफारिस (Recommendation)

- सफ्टवेयर परिवर्तन र स्तरोन्नतिका लागि प्रयोगकर्ता स्वीकृति जाँच (UAT) गरिनुपर्दछ।
- प्रयोगकर्ता स्वीकृति जाँच (UAT) बाट उत्पन्न हुने सुधारात्मक कार्यहरूको कार्यान्वयन गर्न परिवर्तन व्यवस्थापन प्रक्रियाहरू लागू गरिनुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)

२.१५ 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 दिनुपर्दछ।
- CCTV जडान तथा सञ्चालन सम्बन्धी कार्यविधि, २०७२ को बुँदा ३(क)(५) अनुसार CCTV मार्फत खिचिएका दृश्यहरु कम्तीमा तीन महिनासम्म सुरक्षित रहने गरी राख्नुपर्दछ।
- CCTV जडान तथा सञ्चालन सम्बन्धी कार्यविधि, २०७२ को बुँदा ३(घ) अनुसार CCTV जडान भएको क्षेत्रमा CCTV जडान भएको सूचना अनिवार्य रुपमा राख्नुपर्दछ।

ख) लेखापरीक्षणका व्यहोरा (Audit Observation)

CCTV जडान बारे नजिकको प्रहरी ईकाई 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) नियन्त्रण सुधार गर्न असफलताका परिणामहरू (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 गर्नुपर्दछ।

ङ) व्यवस्थापनको जवाफ (Management Response)