

## **Paper-6: सूचना प्रणाली नियंत्रण एवं अंकेक्षण**

प्रश्न संख्या 1 अनिवार्य है

शेष छः प्रश्नों में से किन्हीं पाँच प्रश्नों के उत्तर दीजिये।

### **प्रश्न 1**

XYZ कंपनी एक खुदरा श्रृंखला गृह है जिसकी शाखाएँ संचालन के लिए विभिन्न स्थानों में स्थित हैं। इसकी व्यावसायिक प्रक्रियाएँ बोझिल और थकाऊ हैं क्योंकि इसकी खरीद और आपूर्ति के स्थलों के अनेक स्रोत हैं।

कंपनी के मुख्य कार्यकारी अधिकारी का मानना है कि मौजूदा सूचना प्रणाली अपनी वर्तमान आवश्यकताओं को पूरा नहीं करती। वह सभी प्रमुख संसाधनों के बीच तालमेल कायम करने के लिए उच्च अंतिम समाधान और संचालन प्रक्रियाओं को एकीकृत करना चाहता है। आगे वह उम्मीद करता है कि नई प्रणाली एक संरचित वातावरण प्रदान करे जिसमें माँग, आपूर्ति, संचालन, कार्मिक, वित्त, रसद आदि से संबंधित निर्णय पूर्ण रूप से सटीक और विश्वसनीय जानकारी द्वारा समर्थित हो।

कंपनी प्रणाली के विकास जीवन चक्र (SDLC) की सर्वोत्तम प्रथाओं का अनुसरण करती है, जिसमें प्रारंभिक अन्वेषण से लेकर कार्यान्वयन पश्चात् की समीक्षा, नियंत्रण और सुरक्षा पहलुओं तक विभिन्न चरण शामिल होते हैं।

कंपनी के मुख्य कार्यकारी अधिकारी ने तीन व्यक्तियों की एक समिति नियुक्त की है जिसमें एक सूचना प्रणाली विशेषज्ञ हैं, दूसरा सुरक्षा विशेषज्ञ है और तीसरा कंपनी का लेखा परीक्षक है, जिन्हें निम्नलिखित सुझाव देने हैं :

(अ) **DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES** जाने वाली  
**SEARCH ---> "STUDENTS OF CA AND CS"** (5 अंक)

- (ब) उपयोगकर्ता नियंत्रण में कौन-सी सीमा नियंत्रण तकनीक का इस्तेमाल किया जाना चाहिए ? (5 अंक)
- (स) यदि समिति उद्यम संसाधन नियोजन (ERP) लागू करने का फैसला करती है तो, ERP पैकेज का कार्यान्वयन शुरू करने से पहले आप कौन-से सामान्य दिशा-निर्देश का सुझाव देना चाहेंगे ? (5 अंक)
- (द) व्यापार निरंतरता योजना के लिए सुरक्षा नीति का आलेख तैयार करते हुए किन पहलुओं को शामिल किया जाना चाहिए ? (5 अंक)

उत्तर

- (अ) प्रणाली आवश्यकता विश्लेषण के चरण के दौरान प्रदर्शित की जाने वाली गतिविधियों की सूची निम्नलिखित है:
- हितधारकों की पहचान और उनके परामर्श, उनकी उम्मीदों के निर्धारण और उनके विरोधाभासों का हल;
  - विरोधाभासों का पता लगाना और सही करने के लिए आवश्यकताओं का विश्लेषण और उनकी प्राथमिकताओं को निर्धारित करने के लिए;
  - सत्यापित करने के लिए आवश्यकताएँ पूरी तरह, सुसंगत, स्पष्ट, निरीक्षण, परिवर्तनीय, परीक्षण योग्य और पता लगाने योग्य है;
  - डेटा इकट्ठा करने के लिए या तथ्यों को खोजने के लिए साक्षात्कार, अनुसंधान/दस्तावेज संग्रह, प्रश्नावली, प्रेक्षण जैसे उपकरणों का प्रयोग;
  - गतिविधियों के प्रतिरूप के लिये जैसे विकास प्रतिरूप इस रूप में तैयार किये जाएँ जैसे दस्तावेजीकरण के लिए डाटा प्रवाह आरेख, ई आर आरेख, और

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

- गतिविधियों के दस्तावेज तैयार करने के लिए जैसे साक्षात्कार, प्रश्नावली, रिपोर्टें आदि और मॉडलिंग गतिविधियों के दस्तावेज के लिए एक प्रणाली की (डेटा) शब्दकोश का विकास प्रणाली विकास जीवन चक्र के इस चरण का अंतिम पहलू SRS है

(ब) सीमा प्रणाली के प्रमुख नियंत्रण अभिगम नियंत्रण तंत्र है। उपयोग नियंत्रण अभिगम नियंत्रण प्रणाली के साथ लागू किया जाता है और प्रामाणिक उपयोगकर्ताओं को अधिकृत संसाधनों के साथ जोड़ दिया जाता है, जिसके उपयोग की अनुमति उन्हें दी जाती है। उपयोग नियंत्रण तंत्र के तीन चरण हैं, पहचान, अधिकृतिकरण और प्रमाणीकरण।

मुख्य सीमा नियंत्रण तकनीक निम्न है:

- क्रिप्टोग्राफी - कोड में डेटा को बदलने के लिए कार्यक्रमों के साथ सौदे किसी के लिए भी अर्थहीन है जो प्रमाणीकरण अधिकार संबंधित प्रणाली संसाधन या फाइल का उपयोग नहीं करता है। एक क्रिप्टोग्राफिक तकनीक क्रिप्टोग्राम डेटा (स्पष्ट पाठ) में इनक्रेप्ट (गूढ़ लेख पाठ) और अपनी ताकत एक क्रिप्ट विश्लेषक द्वारा गूढ़लेख पाठ समझने के लिए समय और लागत पर निर्भर करता है। क्रिप्टोग्राफी के तीन तकनीक स्थानान्तरण प्रतिस्थापन (डेटा का एक सेट के भीतर वर्णों के क्रम खिसकाना), (एक साथ पाठ बदलने के) मुख्य पाठ और उत्पाद सिफर (स्थानान्तरण और प्रतिस्थापन के संयोजन) हैं।
- पासवर्ड - नाम, जन्म तिथि, कर्मचारी कोड, कार्य, पदनाम या इनमें से दो या अधिक का संयोजन की तरह व्यक्तिगत विशेषताओं के साथ एक प्रमाणीकरण तंत्र द्वारा उपयोगकर्ताओं की पहचान एक पासवर्ड सीमा पहुंच

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES** † अभ्यासों

**SEARCH ---> "STUDENTS OF CA AND CS"**

र रहे हैं,

न्यूनतम पासवर्ड लंबाई, आम शब्दकोश शब्दों, पासवर्ड की आवधिक परिवर्तन, पासवर्ड एन्क्रिप्शन और प्रविष्टि प्रयास की संख्या के उपयोग से बचने के लिए हैं।

- व्यक्तिगत पहचान संख्या (पिन) – व्यक्तिगत पहचान संख्या एक एन्क्रिप्टेड विशेषताओं और उपयोगकर्ता एक क्रिप्टोग्राफिक एल्गोरिथ्म का उपयोग कर, या संस्थान एक उपयोगकर्ता की पहचान के विवरण के लिए स्वतंत्र डेटाबेस में संग्रहित एक यादृच्छिक संख्या उत्पन्न, या एक ग्राहक चयनित पर आधारित एक संस्था द्वारा एक उपयोगकर्ता के लिए सौंपा पासवर्ड संख्या के समान है। इसलिए, एक पिन या एक डिजिटल हस्ताक्षर कमजोरियों को उजागर कर रहे हैं, जबकि जारी करने या वितरण, मान्यता, पारिषण और भंडारण इत्यादि।
  - पहचान कार्ड – पहचान कार्ड के लिए एक प्रमाणीकरण की प्रक्रिया में आवश्यक सूचना जमा करने के लिए उपयोग किया जाता है। ये कार्ड एक उपयोगकर्ता की पहचान के लिए प्रयोग किये जाते हैं, का नियंत्रण कार्ड का उपयोग और वापसी कार्ड या कार्ड समाप्ति चरणों का एक कार्ड तैयार करने के लिए आवेदन के माध्यम से नियंत्रित किये जा रहे हैं।
  - जीव सांख्यिकी यन्त्र – जीव सांख्यिकी पहचान जैसे : अंगूठा और या अंगूली की छाप, आँख की पुतली आदि भी सीमा नियंत्रण तकनीक के रूप में प्रयोग होते हैं।
- (स) यदि समिति उद्यम संसाधन नियोजन (ERP) लागू करने का फैसला करती है, तो ERP पैकेज का कार्यान्वयन शुरू करने से पहले निम्न सामान्य दिशा निर्देशों की पालना की जाएगी।

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES** मझते हुए  
**SEARCH ---> "STUDENTS OF CA AND CS"** चयन;

- कार्यान्वयन शुरू करने के पहले व्यापार प्रक्रिया के नये स्वरूप का अभ्यास;
  - संगठन में अच्छे संचार नेटवर्क की स्थापना;
  - एक मजबूत और प्रभावी नेतृत्व प्रदान करना जिससे नीचे के लोग अच्छी तरह से प्रेरित हो सके;
  - कुशल और सक्षम परियोजना प्रबंधक खोजना;
  - कार्यान्वयन सलाहकारों की संतुलित टीम बनाना, जो कि एक साथ टीम के रूप में काम कर सकें;
  - सिंदुर अनुकूलन के साथ अच्छी कार्यान्वयन पद्धति का चयन;
  - अंतिम उपयोगकर्ताओं को प्रशिक्षण; और
  - नई प्रणाली के अनुकूल ढलना और काम करने के वातावरण में आवश्यक बदलाव करना ताकि भवष्य में इस प्रणाली का प्रभावी उपयोग किया जा सके।
- (द) व्यापार निरंतरता योजना के लिए सुरक्षा नीति का आलेख तैयार करने में निम्न मुख्य पहलुओं को शामिल किया जाना चाहिए;
- व्यापार निरंतरता योजना को बनाए रखना, परीक्षण करना और यदि आवश्यक हो तो उसका उद्यतन किया जाना चाहिए। सभी कर्मचारियों को इसके बारे में पता होना चाहिए।
  - व्यापार निरंतरता और प्रभाव आकलन प्रतिवर्ष आयोजित किया जाना चाहिए।
  - नेटवर्क सेवाओं के आपूर्तिकर्ताओं को अनुबंध द्वारा पूर्ण निर्धारित न्यूनतम सेवा स्तर प्रदान करने के लिए बाध्य किया जाना चाहिए।

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

इकाईयों

थित होना

चाहते हैं, तो उन्हें संबंधित मानकों के अनुरूप हार्डवेयर, सॉफ्टवेयर, नीतियों और संबंधित प्रक्रियाओं को लागू करना चाहिए।

- कम्प्यूटर संचालन प्रबंधन को जानकारी संसाधन विभाजन वसूली प्राथमिकता के आधार पर करने के लिए एक तार्किक ढांचे की स्थापना और उपयोग करना चाहिए। बदले में यह सबसे महत्वपूर्ण संसाधनों को पहले वसूलने की अनुमति दे देगा। सूचना प्रणाली आकस्मिक योजना तैयार करते समय सभी विभागों को समान ढांचे का उपयोग करना चाहिए।
- इसके अतिरिक्त, सभी आवेदनों की वसूली प्राथमिकता भी अनुप्रयोगों के तहत्व के आकंलन द्वारा परिभाषित की जानी चाहिए। आगे, आवेदन महत्व के लिए वर्गीकरण भी किया जा सकता है।
- प्रबंधन को समय-समय पर अद्यतन तैयार करना होगा, और नियमित रूप से आपातकालीन प्रतिक्रिया योजनाओं और आपदा सुधार योजना का परीक्षण करना होगा जो सभी महत्वपूर्ण कम्प्यूटर प्रणालियों के प्रसंस्करण और जारी रखने की अनुमति देगा और व्यवधान की स्थिति में या सेवा की गिरावट की स्थिति में और बड़े नुकसान होने की स्थिति में, जैसे: बाढ़, भूकम्प में उपलब्ध होगा।

## प्रश्न-2

- (अ) सॉफ्टवेयर विकास के प्रोटोटाइप प्रतिरूप दृष्टिकोण का लक्ष्य क्या है? इस प्रतिरूप की क्षमता की विवेचना करें। (अंक 6)
- (ब) व्यवस्था में बदलाव में कौन-सी गतिधियाँ शामिल हैं? संक्षेप में समझाएँ। (अंक 6)
- (स) **DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES** है? (अंक 4)  
**SEARCH ---> "STUDENTS OF CA AND CS"**

## उत्तर

(अ) प्रोटोटाइप प्रतिरूप का लक्ष्य एक छोटे या प्रायोगिक संस्करण के किसी भाग या पूरी प्रणाली जिसे प्रोटोटाइप बुलाया जाता है, को विकसित करना है। प्रोटोटाइप उपयोग किये जा सकने वाली एक ऐसी व्यवस्था या घटक है जिसे बनाने में अधिक समय नहीं लगता और इस पर लागत भी कम आती है। इसको बाद में पूर्ण सक्रिय व्यवस्था में बदल दिया जाता है या इसी में वांछित बदलाव कर दिये जाते हैं।

उपयोगकर्ता इसमें सुधार करने के सुझाव देते हैं। इन सुझावों पर काम करके एक नया प्रोटोटाइप बनाया जाता है, जिसका इस्तेमाल और मूल्यांकन किया जाता है। अन्ततः जब ऐसा प्रोटोटाइप तैयार हो जाता है, जो सबकी अपेक्षाओं पर खरा उतरने वाला होता है तो या तो यह परिष्कृत होता है और इसे अन्तिम व्यवस्था के रूप में स्वीकार कर लिया जाता है या रद्द कर दिया जाता है। यदि इसे रद्द किया जाता है तो इसको बनाने से हुआ ज्ञानार्जन वास्तविक व्यवस्था को बनाने में काम आता है।

प्राटोटाइपिंग प्रतिरूप की प्रमुख विशेषताएँ निम्नलिखित हैं:-

- प्रोटोटाइप प्रतिरूप हितधारकों की प्रणाली विकास में भागीदारी और विश्लेषकों के साथ संप्रेषण को बेहतर बनाता है।
- यह विशेष रूप से अस्पष्ट उद्देश्यों को हल करने उपयोगकर्ता की आवश्यकताओं को विकसित करने विभिन्न डिजाइन समाधानों के साथ प्रयोग या तुलना, या प्रदर्शन और मानव कम्प्यूटर इंटरफेस दोनों की जाँच करने में उपयोगी है।
- प्रारम्भिक आइटरेशन से प्राप्त जानकारी का उपयोग बाद में विकसित

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

- भ्रमकारी या कठिन क्रियाओं का अविद्यमान कार्यो को सरलता से चिह्नित करने में सहायता करता है।
  - उत्पादन एप्लीकेशन के लिए विवरण उत्पन्न कर सकता है।
  - अभिनव एवं लोचपूर्ण डिजायन को बढ़ावा देता है।
  - अपूर्ण, लेकिन कार्यक्षम एप्लीकेशन का तेज कार्यान्वयन उपलब्ध करता है।
  - प्रोटोटाइपिंग में प्रयोगकर्ता के सघन जुड़ाव की आवश्यकता होती है। इसलिए पारंपरिक प्रणाली विकास दृष्टिकोण की तुलना में यह विशिष्ट तौर पर प्रयोगकर्ता की आवश्यकता एवं जरूरतों के निर्धारण में अच्छा परिणाम परक होता है।
  - प्रोटोटाइप का विकास प्रयोग शुरू करने के लिए सामान्यता बहुत कम समय (जैसे: एक सप्ताह) की आवश्यकता होती है। यह संक्षिप्त समयावधि प्रणाली प्रयोगकर्ताओं को प्रस्तावित प्रणाली बदलावों को तुरन्त मूल्यांकित करने की सुविधा देती है।
  - क्योंकि प्रणाली प्रयोगकर्ता एक इंटरैक्टिव प्रोसेस द्वारा प्रोटोटाइप के प्रत्येक संस्करण का परीक्षण करते हैं, अतः गलतियों को विकास प्रक्रिया के दौरान जल्दी ही खोज कर उनको दूर कर दिया जाता है। परिणामस्वरूप पारंपरिक प्रणाली विकास प्रक्रिया के कार्यान्वयन की तुलना में, अंततः कार्यान्वित यह सूचना प्रणाली विकास करने में अधिक विश्वसनीय एवं कम खर्चीली होती है।
- (ब) बदलाव में वे सभी गतिविधियाँ शामिल होती हैं जिन्हें वर्तमान व्यवस्था से नयी सूचना व्यवस्था में परिवर्तन के लिए सफलतापूर्वक पूरा कर लिया गया होता है। ये निम्नलिखित हैं :-

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

का पूर्ण  
हिए। यह



कम्प्यूटर परिचालन तथा कार्यक्षेत्रों के परिचालन पर समान रूप से लागू होता है। कोई भी समानान्तर या बदलाव की गतिविधि शुरू करने से पहले उन कार्यक्षेत्रों के लिए परिचालन प्रक्रियाएँ स्पष्ट होनी चाहिए, विधियों, प्रक्रियाओं, आउटपुट और आंतरिक नियंत्रणों से सम्बद्ध सूचना सामान्य पाठक के लिए सरल, संक्षिप्त तथा समझ में आने वाली भाषा में होनी चाहिए। व्यवस्था परिवर्तन प्रशिक्षण सत्रों के दौरान मौखिक संवाद के अलावा लिखित परिचालन प्रक्रियाओं का होना भी जरूरी है।

- **फाइलों में बदलाव :** चूंकि बड़ी फाइलों को एक से दूसरे माध्यम में बदलना होता है, इसलिए यह काम प्रोग्रामिंग तथा जांच-पड़ताल पूरी होने से काफी पहले शुरू कर देना चाहिए। यदि बदलावों को यथा सम्भव सटीक लागू करना है तो फाइलों में बदलाव के काम का विस्तृत परीक्षण करना आवश्यक है। पर्याप्त नियंत्रण, जैसे कि रिकॉर्ड काउंट्स व कंट्रोल टोटल बदलाव प्रोग्राम की आउटपुट के रूप में होने चाहिए। वर्तमान कम्प्यूटर फाइलों को तब तक रखना होगा जब तक बैक-अप के लिए पर्याप्त फाइलें एकत्र न हो जाएं। उन परिस्थितियों में तो यह और भी आवश्यक हो जाता है, जब बदलाव की प्रक्रिया के दौरान फाइलों में पाई गई किसी त्रुटि को दूर करके उसको पुनः बनाया जाता है।
- **प्रणाली में बदलाव :** ऑनलाइन तथा ऑफलाइन फाइलों में बदलाव तथा कार्यक्षेत्रों में सिस्टम की विश्वसनीयता सुनिश्चित हो जाने के बाद दैनिक के स्तर पर की जाने वाली प्रोसेसिंग को पुरानी व्यवस्था से नई व्यवस्था पर डाला जाता है। इसके बाद सभी कार्य नई व्यवस्था पर किया जाता है। पुरानी व्यवस्था के कुछ और समय तक काम करने पर भी विचार

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

- कार्मिकों और उपकरणों का कार्य निर्धारण : व्यवस्था प्रबन्धक के लिए नई सूचना व्यवस्था में पहली बार डेटा प्रोसेसिंग कार्य का निर्धारण करना कठिन होता है। जैसे-जैसे कर्मचारी नई व्यवस्था से परिचित हो जाते हैं, यह समस्या हल होती जाती है। विभागाध्यक्षों से सलाह कर व्यवस्था प्रबन्धक को उस उपकरण से जुड़े कार्यक्षेत्रों के लिए समय का निर्धारण करना चाहिए।
  - किसी उपकरण के खराब हो जाने पर वैकल्पिक व्यवस्था : उपकरण के काम न कर पाने की स्थिति में वैकल्पिक व्यवस्था सक्रिय हो जानी चाहिए। उन कामों को वरीयता दी जानी चाहिए जो संस्थान के लिए महत्वपूर्ण है, जैसे - बिलिंग, पेरोल व इन्वेंटरी। जब तक उपकरण ठीक नहीं हो जाता अत्यन्त महत्वपूर्ण कार्यों को मानवीय रूप में पूरा किया जा सकता है।
- (स) कार्यकारी सूचना प्रणाली कई मायनों में पारंपरिक सूचना प्रणाली से भिन्न है। निम्न तालिका विभिन्न आयामों पर भिन्नता प्रस्तुत करती है:

अंतर का आधार	कार्यकारी सूचना प्रणाली	पारंपरिक सूचना प्रणाली
प्रबन्ध का स्तर	उच्च व उसके निकटतम कार्यकारी	निम्न श्रेणी कर्मियों के लिए
सूचना को प्राप्त करने का स्वरूप	विशिष्ट मामले/समस्याएँ और सामूहिक रिपोर्ट	वस्तु स्थिति की रिपोर्ट
प्राप्त सूचना की प्रकृति	ऑनलाइन टूल्स व विश्लेषण	वस्तु स्थिति की ऑफलाइन रिपोर्ट
सूचना के स्रोत	बाह्य अधिक, आंतरिक कम	आंतरिक
विवरण के जाँच पड़ताल की सुविधा	उपलब्ध	उपलब्ध नहीं
सूचना का स्वरूप	ग्राफिकल के साथ टेक्स्ट	तालिका रूप में

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES** रिपेटर द्वारा

**SEARCH ---> "STUDENTS OF CA AND CS"**

प्रश्न 3

- (अ) आवेदन प्रणाली के आउटपुट नियंत्रण का दायरा क्या है? विभिन्न प्रकार के आउटपुट नियंत्रण के सुझाव दीजिए जो गोपनीयता, अखंडता और आउटपुट में स्थिरता के लिए लागू किये जा सकें। (6 अंक)
- (ब) विशेषज्ञ व्यवस्था क्या है? उन गुणों की सूची बनाइए जो कि आवेदन को विशेषज्ञ प्रणाली विकास के लिए अर्हत करती है। (6 अंक)
- (स) पैकेट फिल्टर फायरवॉल से क्या तात्पर्य है? इसकी प्रमुख कमजोरियाँ बताइए। (4 अंक)

उत्तर

- (अ) आउटपुट नियंत्रण का आवेदन प्रणाली के लिए दायरा निम्न रूप में प्रस्तुत है :

ऐसे फंक्शन उपलब्ध करवाना जो उपयोगकर्ताओं के लिए उपलब्ध डेटा सामग्री, डेटा स्वरूप, समयबद्धता निर्धारित करें और डेटा कैसे तैयार किया गया है तथा उपयोगकर्ताओं में किस प्रकार पहुँचाया जाये इसका निर्धारण करें।

विभिन्न प्रकार के आउटपुट नियंत्रण सुझाव, जो जिनसे गोपनीयता, अखंडता और आउटपुट में स्थिरता लागू की जा सके निम्न है :

- संवेदनशील लॉगिंग और भंडारण और, महत्वपूर्ण रूप : अनाधिकृत विनाश या हटाने और उपयोग को रोकने के लिए पूर्व मुद्रित स्टेशनरी सुरक्षित संग्रहित किया जाना चाहिए। केवल अधिकृत व्यक्तियों को सुरक्षा रूपों,

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES** अनुमति दी

**SEARCH ---> "STUDENTS OF CA AND CS"**

- उत्पादन कार्यक्रम कार्यान्वयन को लॉग इन करना : जब डेटा के उत्पादन के लिए कार्यक्रमों को क्रियान्वित किया जाता है, और तब इसकी लॉग इन और निगरानी की जानी चाहिए। इस तरह के आउटपुट कार्यान्वयन पर नियंत्रण के अभाव में, डेटा की गोनीयता से समझौता किया जा सकता है।
- स्पूलींग/कतार : यह प्रक्रिया सुनिश्चित करती है कि प्रिंट ऑपरेशन पूरा होने से पहले भी उपयोगकर्ता काम जारी रखने में सक्षम है। फाइल को जब मुद्रित किया जाना होता है, ऑपरेटिंग प्रणाली डेटा को जो प्रिंट के लिये जाना है उसको एक अस्थायी फाइल में हार्ड डिस्क में जमा कर लेती है।

इस फाइल को फिर प्रिंटर पर 'स्पूल' किया जाता है जैसे ही प्रिंटर डेटा को लेने के लिए तैयार हो जाता है। आउटपुट के इस मध्यवर्ती भण्डारण से अनाधिकृत प्रकटीकरण और/या संशोधन हो सकता है। कतार दस्तावेजों की सूची है जो की किसी विशेष प्रिंटर पर मुद्रित होने के इंतजाम में है। कतार अनाधिकृत संशोधनों के अधीन नहीं होनी चाहिए।

- मुद्रण पर अधिक नियंत्रण : यह सुनिश्चित होना चाहिए कि मुद्रित सूचना का अनाधिकृत प्रकटीकरण रोका गया है। उपयोगकर्ताओं को सही प्रिंटर का चरन करने का प्रशिक्षण दिया जाना चाहिए तथा वर्कस्टेशन पर पहुँच प्रतिबंध लगा देने चाहिए जो कि मुद्रण के लिए इस्तेमाल किये जा सकें।
- रिपोर्ट वितरण और संग्रह पर नियंत्रण : रिपोर्ट का वितरण सुरक्षित होना चाहिए ताकि डेटा का अनाधिकृत प्रकटीकरण न हो सके। लॉग तैयार

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

की है और  
को स्वयं



**PLEASE VISIT [WWW.STUDENTSOFCAANDCS.COM](http://WWW.STUDENTSOFCAANDCS.COM) FOR MORE UPDATES**

रिपोर्ट एकत्र करनी है वह स्वयं समय पर रिपोर्ट एकत्र करने के लिए जिम्मेदार होने चाहिए खासकर अगर रिपोर्ट सार्वजनिक क्षेत्र में छापी है। एक लॉग बनाना चाहिए जिसमें कौन-सी रिपोर्ट मुद्रित हुई है और उनमें से कौ-सी एकत्रित कर ली गई है होना चाहिए। असंग्रहित रिपोर्ट को सुरक्षित रूप से संग्रहित किया जाना चाहिए।

- रिटेंशन नियंत्रण : रिटेंशन नियंत्रण उस अवधि पर विचार करता है जिसमें आउटपुट नष्ट करने से पहले रखा जाना चाहिए। ऐसे माध्यम के प्रकार पर विचार करना चाहिए जिसमें आउटपुट को जमा किया जा सके। रिटेंशन नियंत्रण के लिए आवश्यक है एक तिथि प्रत्येक आउटपुट आइटम के उत्पादन के लिए निर्धारित की जाए।
  - स्थिति/सुधार नियंत्रण : इनकी आवश्यकता आउटपुट के खो जाने या नष्ट हो जाने की स्थिति में आउटपुट को ठीक करने के लिए पड़ती है। यदि आउटपुट को स्पूल फाइलों या रिपोर्ट फाइलों पर लिखा गया है और उन्हें रखा गया है, तो उसकी वापसी तथा नया उत्पादन आसन और सीधा है।
- (ब) विशेषज्ञ व्यवस्था : यह एक उच्च विकसित निर्णय समर्थन प्रणाली (DSS) है, जो किसी समस्या को हल करने के लिए विशेषज्ञ के पास संचित जानकारी (ज्ञान) का उपयोग करता है। विशेषज्ञ व्यवस्था ऐसा सॉफ्टवेयर सिस्टम है जो मानव विशेषज्ञों की तार्किक प्रोसेसिंग की नकल करता है और निर्णय लेने वालों को ऐसी जानकारी उपलब्ध कराता है, जो उन्हें ऐसी विशेषज्ञ व्यवस्था से मिल सकती थी। उदाहरणार्थ, निवेश पोर्टफोलियो प्रबन्धन के क्षेत्र में विशेषज्ञ व्यवस्था प्रयोगकर्ता से किसी निवेशकर्ता के सम्बन्ध में प्रश्न पूछ सकती है, जैसे - कितना धन निवेश करना है ?

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES** रुचि है

**SEARCH ---> "STUDENTS OF CA AND CS"**

विशेषज्ञ व्यवस्था में शामिल होने के लिए किसी एप्लीकेशन में निम्नलिखित गुणों का होना आवश्यक है :

- उपलब्धता : एक या अधिक व्यक्ति यह तय करने में सक्षम होते हैं कि वे समस्या को हल करने के लिए क्या प्रक्रिया अपनाएंगे जिसके लिए विशेषज्ञ व्यवस्था लागू की जाएगी।
  - जटिलता : किस समस्या के हल के लिए विशेषज्ञ व्यवस्था अपनाई जाएगी, वह एक जटिल कार्य है। इसमें तार्किक अनुमान प्रोसेसिंग की आवश्यकता होती है, जो पारंपरिक सूचना प्रोसेसिंग से कर पाना संभव नहीं है।
  - विषय क्षेत्र : किसी समस्या का विषय क्षेत्र स्पष्ट समस्या क्षेत्र की तुलना में अपेक्षाकृत छोटा और सीमित होता है।
  - दक्षता : समस्या के समाधान के लिए दक्ष लोगों के प्रयासों की आवश्यकता होती है। आवश्यक योग्यता, तकनीक अनुभव व अन्तर्ज्ञान रखने वाले लोग कठिनता से मिलते हैं।
  - संरचना : समाधान प्रक्रिया को इस प्रकार का होना चाहिए कि वह बेतरतीब संरचना, अनिश्चित, छूटे हुए तथा परस्पर विरोधी डेटा के साथ गतिशील समस्या समाधान परिस्थितियों में काम कर सके।
- (स) पैकेट फिल्टर फायरवॉल्ल्स : पैकेट फिल्टर फायरवॉल्ल्स प्रत्येक इनकमिंग एवं आउटगोइंग पैकेट के हेडर्स का मूल्यांकन यह सुनिश्चित करने के लिए करता है कि इसका एक वैध इन्टरनेट एड्रेस है, यह अनुमति प्राप्त एप्लीकेशन से आया है एक अलग मोबाइल या सर्विस से
- DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**
- SEARCH ---> "STUDENTS OF CA AND CS"**
- मति प्राप्त

ट्रैफिक के लिए पूर्व निर्धारित नीति से मैच नहीं करता, तो फायरवॉल पैकेट को ड्रॉप कर देता है।

पैकेट फिल्टर फायरवॉल्स की प्रमुख कमजोरियाँ निम्न हैं:

- प्रणाली की आवेदन विशिष्ट कमजोरियों और कार्यों शोषण के हमले को रोकने में असमर्थ है क्योंकि पैकेट फिल्टर पैकेट की सामग्री की जाँच नहीं करता है।
- लॉगिंग कार्यक्षमता उसी जानकारी तक सीमित है जो अभिगम नियंत्रण बनाने के लिए इस्तेमाल की जाती है।
- ज्यादातर पैकेट फिल्टर फायरवॉल्स सर्वाधिक उन्नत उपयोगकर्ता प्रमाणीकरण योजनाओं का समर्थन नहीं करते।
- फायरवॉल आमतौर पर ऐसे हमलों और शोषण का शिकार होते रहते हैं जो नेटवर्क प्रोटोकॉल से लाभ लेने की चेष्टा करते हैं।
- फायरवॉल्स को अविन्यास करना आसान है, जिससे जो यातायात अवरुद्ध किया जाना चाहिए वह पारित हो जाता है।

#### प्रश्न 4

- (अ) 'प्रणाली नियंत्रण लेखापरीक्षण समीक्षा फाइल' (SCARF) से आप क्या समझते हैं? SCARF के द्वारा लेखा परीक्षक किस प्रकार की सूचना एकत्रित कर सकते हैं? (6 अंक)
- (ब) व्यावसायिक प्रभाव विश्लेषण क्या है? इस अंकेक्षण में कौन-कौन से

DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES

SEARCH ---> "STUDENTS OF CA AND CS"

- (स) सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 की धारा 22 के तहत इलेक्ट्रॉनिक हस्ताक्षर प्रमाण पत्र जारी करने हेतु लाइसेंस के लिए आवेदन करने की प्रक्रिया का वर्णन कीजिये। (4 अंक)

उत्तर

- (अ) प्रणाली नियंत्रण लेखापरीक्षण समीक्षा फाइल (SCARF)-SCARF तकनीक एक मेजबान अनुप्रयोग प्रणाली के भीतर लेखा परीक्षण सॉफ्टवेयर मॉड्यूल एम्बेडेड शामिल प्रणाली के लेनदेन की सतत् निगरानी प्रदान करने के लिए है। एकत्रित सूचना एक विशेष लेखापरीक्षण फाइल SCARF मास्टर फाइल पर लिखी जाती है। इसके बाद लेखा परीक्षक इस फाइल पर निहित सूचना की जाँच करता है यह देखने के लिए कि अनुप्रयोग प्रणाली को फोलो आप की आवश्यकता तो नहीं। कई मायनों में SCARF तकनीक स्नैपशॉट तकनीक के साथ-साथ अन्य डेटा संग्रह की क्षमताओं की तरह है।

लेखा परीक्षक SCARF का उपयोग निम्नलिखित प्रकार की सूचना एकत्र करने के लिए कर सकते हैं :

- अनुप्रयोग प्रणाली अशुद्धियाँ - SCARF लेखापरीक्षण दिनचर्या प्रणाली के प्रसंस्करण की गुणवत्ता पर एक स्वतंत्र जाँच प्रदान करता है कि क्या वहाँ कोई भी डिजाइन और प्रोग्रामिंग के रूप में अशुद्धियाँ हैं जो प्रणाली में पायी जा सकती हैं जब इसमें संशोधित और देखभाल की गयी हो।
- नीति और प्रक्रियात्मक विचलन - संगठनों को उन संगठनों और उद्योगों की नीतियों, प्रक्रियाओं और मानकों का पालन करना पड़ेगा जिससे वे जड़े हाग हैं। SCARF ऑडिट रूटिन नीतियों, प्रक्रियाओं और मानकों की

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**



- प्रणाली अपवाद - SCARF का उपयोग अनुप्रयोग प्रणाली अपवाद की विभिन्न प्रकार की निगरानी के लिए किया जा सकता है। जैसे - सेल्समैन को कीमतों में कुछ छूट दी जा सकती है जो वह ग्राहकों से वसूल कर सके। SCARF यह देखने के लिए इस्तेमाल किया जा सकता है कि सेल्समैन कितनी बार मानकों की अवहेलना करता है।
  - सांख्यिकीय नमूना - कुछ एम्बेडेड लेखापरीक्षण रूटीन सांख्यिकीय नमूना हो सकते हैं, SCARF एक फाइल पर एक साथ सभी नमूना सूचना को एकत्र करने का सुविधाजनक तरीका प्रदान करता है और वहाँ पर विश्लेषणात्मक समीक्षा उपकरण का उपयोग करता है।
  - स्नैपशॉट और विस्तारित रिकॉर्ड - स्नैपशॉट और विस्तारित रिकॉर्ड SCARF फाइल में लिखा जा सकता है और जब आवश्यक हो मुद्रित किया जा सकता है।
  - रूपरेखा डेटा-लेखा परीक्षक एम्बेडेड रूटीन का उपयोग उपयोगकर्ताओं की प्रोफाइल निर्माण के लिए डेटा एकत्रित करने में कर सकते हैं। प्रोफाइल से विचलन त्रुटियों या अनियमितताओं का संकेत हो सकता है।
- (ब) व्यावसायिक प्रभाव विश्लेषण : व्यावसायिक प्रभाव विश्लेषण (BIA) एक ऐसी विधि है जो विभिन्न घटनाओं से होने वाले सम्भावित खतरों पर व्यवस्थित रूप से आकलन करती है। व्यावसायिक निरंतरता में लगी टीम को इससे महत्वपूर्ण व्यवस्थाओं, प्रक्रियाओं और कार्यों, घटनाओं और खतरों से होने वाले आर्थिक प्रभाव (जो सिस्टम, सेवाओं) व सुविधाओं को एक्सेस न कर पाने की स्थिति में व्यावसायिक इकाईयाँ कितने समय तक काम पर पाएंगी आदि को समझने में मदद मिलती है।
- इस विश्लेषण में किए जाने वाले प्रमुख कार्य, निम्न रूप से दिये गये

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

- संस्थानिक जोखिमों की पहचान - इसमें संरचनात्मक जोखिम व एक बिन्दु पर असफलता शामिल है। इसका उद्देश्य जोखिमों और अवसरों की पहचान व साथ ही उन संभावित कारणों को पहचानना है, जो किसी खतरे का कारण बन सकते हैं।
  - जटिल व्यावसायिक प्रक्रियाओं की पहचान।
  - कार्य व्यवधान तथा आर्थिक प्रभाव के सन्दर्भ में महत्वपूर्ण व्यावसायिक कार्यों को हो सकने वाले खतरों/जोखिमों की पहचान।
  - महत्वपूर्ण व्यावसायिक प्रक्रियाओं पर निर्भर कार्य और वह क्रम जिसमें इन्हें पुनः शुरु किया जाएगा।
  - प्रत्येक व्यावसायिक प्रक्रिया के लिए निष्क्रिय रहने का अधिकतम समय।
  - रिकवरी के लिए आवश्यक संसाधनों का प्रकार व मात्रा, जैसे - मेज, कुर्सियाँ, फैक्स, फोटोकॉपीज, डेस्कटॉप, प्रिन्टर इत्यादि।
  - खतरा आ पड़ने की स्थिति में संस्थान पर उसका पडने वाला प्रभाव, जैसे वित्तीय साख इत्यादि।
- (स) सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 की (धारा 22) के लाइसेंस के लिए आवेदन:
- (1) लाइसेंस जारी करने के लिए प्रत्येक आवेदन को केन्द्र सरकार द्वारा निर्धारित प्रारूप में होना चाहिए।
  - (2) लाइसेंस जारी करने के लिए आवेदन के साथ निम्न को संलग्न होना चाहिए -
    - (क) एक अभ्यास प्रमाणीकरण विवरण,
    - (ख) एक विवरण जिसमें कि आवेदक की पहचान से संबंधित प्रक्रिया को

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

(ग) फीस का भुगतान, पच्चीस हजार रुपये से अधिक नहीं जैसा कि केन्द्र सरकार द्वारा निर्धारित किया गया हो,

(घ) अन्य दस्तावेज जैसा कि केन्द्र सरकार के द्वारा निर्धारित किया गया हो।

प्रश्न 5

(अ) सूचना सुरक्षा, प्रबंधन प्रणाली में 'सम्पत्ति का वर्गीकरण और नियन्त्रण' की संक्षेप में वर्णन कीजिये। (6 अंक)

(ब) जोखिम मूल्यांकन को उद्देश्य क्या है? जोखिम मूल्यांकन के लिए उपलब्ध कुछ तकनीकें बताइए। (6 अंक)

(स) सूचना सुरक्षा नीति क्या है? इसे कौन-से मुद्दों को संबोधित करना चाहिए? (4 अंक)

उत्तर

(अ) 'सम्पत्ति का वर्गीकरण और नियंत्रण' सूचना सुरक्षा प्रबंधन प्रणाली (ISMS):

विस्तृत नियंत्रण और उद्देश्य नीचे दिए गए हैं:

- सूचना वर्गीकरण : यह सुनिश्चित करने के लिए कि सूचना संपत्ति को उचित स्तर का संरक्षण प्राप्त है।
- संपत्ति के लिए जवाबदेही : संगठनात्मक परिसम्पत्ति की उचित सुरक्षा बनाए रखने के लिए।

इनका संक्षेप में वर्णन निम्न प्रकार है :

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

- (1) सूचना वर्गीकरण : सबसे कठिन लेकिन एक आवश्यक कार्य सूचना प्रौद्योगिकी परिसंपत्ति की स्कन्ध प्रबन्धन का जो कि जानकारी परिसंपत्ति, सॉफ्टवेयर परिसंपत्ति, भौतिक परिसंपत्ति या अन्य समान सेवा हो सकती है। इन जानकारी परिसंपत्तियों के वर्गीकरण की आवश्यकता सुरक्षा की डिग्री को इंगित करने के लिए है। वर्गीकरण का परिणाम उपयुक्त जानकारी को लेबल करना होना चाहिए जो इंगित करे कि वह संवेदनशील या महत्वपूर्ण है और कौन-सी प्रक्रिया, जानकारी परिसंपत्ति की प्रतिलिपि, संग्रह और संचारित या विनाश के लिए उपयुक्त है।
- (2) परिसंपत्ति के लिए जवाबदेही : यह सूचना परिसम्पत्ति रजिस्टर अनुबंध रजिस्टर के उपयोग द्वारा प्राप्त किया जा सकता है। एक सूचना परिसंपत्ति रजिस्टर (IAR) संगठन के भीतर हर जानकारी परिसंपत्ति के विवरण के साथ बनाया जाना चाहिए। उदाहरण: डेटाबेस, कर्मियों के रिकॉर्ड, पैमाने के मॉडल, प्रोटोटाइप, परीक्षण के नमूने, अनुबंध, सॉफ्टवेयर लाइसेंस, प्रचार सामग्री। जानकारी परिसंपत्ति रजिस्टर में वर्णन होना चाहिए, 'प्रत्येक जानकारी परिसंपत्ति के लिए कौन जिम्मेदार है' और 'क्या वहाँ गोपनीयता, अखंडता या उपलब्धता की कोई विशेष आवश्यकता है'। प्रशासनिक सुविधा के लिए, सूचना परिसंपत्ति रजिस्टर विषय के शीर्ष के तहत अलग रजिस्टर रखा जा सकता है। उदाहरण के लिये 'मीडिया रजिस्टर' सॉफ्टवेयर के स्टॉक और उसके लाइसेंस का विवरण रखता है।

इसी प्रकार, अनुबंध रजिस्टर में अनुबंध के हस्ताक्षर तथा इस प्रकार के अन्य विवरण शामिल होंगे। इसका प्रभाव यह होगा कि मात्र एक रजिस्टर के रखरखाव से निगम की बहुमूल्य संपत्ति पर नियंत्रण

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

(ब) जोखिम मूल्यांकन का उद्देश्य है :

- विफलताओं और खतरों की संभावनाओं की पहचान।
- जोखिम का परिकलन यानी, परिसंपत्ति को क्षति या हानि
- लागत लाभ विश्लेषण को ध्यान में रखते हुए नियंत्रण सिफारिशें करना।

जोखिम मूल्यांकन के लिए उपलब्ध प्रमुख तकनीकें निम्नलिखित हैं :

- (1) विवेक एवं अन्तर्ज्ञान - कई स्थितियों में, ऑडिटर्स को जोखिम आकलन हेतु अपने विवेक एवं अन्तर्ज्ञान का प्रयोग करना होता है। यह मुख्यतया ऑडिटर्स के वैयक्तिक एवं व्यवसायिक अनुभव और उनके सिस्टम एवं उनके पर्यावरण के बारे में समझ कर निर्भर करता है। इसके साथ-साथ क्रमिक शिक्षण एवं चालू पेशेवर अपडेटिंग की भी आवश्यकता होती है।
- (2) डेल्टा दृष्टिकोण - इस तकनीक का प्रयोग एक समान राय प्राप्त करने के लिए किया जाता है। विशेषज्ञों का एक पैनल इस कार्य में लगाया जाता है और प्रत्येक विशेषज्ञ से लिखित एवं स्वतन्त्र रूप में अपनी राय देने को कहा जाता है। वे लागत लाभ का अनुमान एवं एक खास, सिस्टम को क्यों चुना जाना चाहिए, उसके कारण एवं सिस्टम के जोखिम एवं अरक्षितताओं की सूची बनाते हैं। इन अनुमानों को तब एक साथ एकत्रित किया जाता है। वे अनुमान जो पूर्व निर्धारित स्वीकृत रेंज में आते हैं, उन्हें ले लिया जाता है। प्रक्रिया को रेंज से परे के अनुमानों को संशोधित करने के लिए प्रक्रिया को चार बार दोहराया जा सकता है। सभी अनुमानों को ग्राफ पर पॉइन्ट के रूप में लेकर एक वक्र खींचा

गाना जाता  
**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

- (3) क्रमबद्धता दृष्टिकोण - इस अप्रोच में सिस्टम के जोखिम और उनके सम्बन्धित एक्सपोजर्स को सूचीबद्ध किया जाता है। तीव्रता, घटित होने पर प्रभाव एवं शामिल व्यय के अनुसार, जोखिम एवं एक्सपोजर को भार दिया जाता है। एक्सपोजर भार के साथ जोखिम भार का प्रत्येक विशिष्ट में उत्पाद भारित स्कोर प्रदान करता है। इन भारित स्कोर का जोड़ सिस्टम का जोखिम एवं एक्सपोजर भार प्रस्तुत कर रहा है। उसके बाद स्कोर के अनुसार सिस्टम के जोखिम एवं एक्सपोजर को क्रमबद्ध किया जाता है।
- (4) मात्रात्मक तकनीक - मात्रात्मक तकनीक में सालाना नुकसान मूल्य का परिकलन करना शामिल है जो कि घटना की सम्भाव्यता एवं अनुमानित व्यय के संदर्भ में एक्सपोजर पर आधारित है। यह संगठन को लागत प्रभावी समाधान चुनने में मदद करता है। यह, प्रतिकूल घटनाओं के घटित होने की स्थिति में, इस बात का ध्यान रख कर कि कितनी बार ऐसी घटना हो सकती है, सम्भावित क्षति का उल्लंघन है।
- (5) गुणात्मक तकनीक - जोखिम विश्लेषण के लिए इस्तेमाल की गई तकनीक में से यह तकनीक अब तक सबसे व्यापक रूप में इस्तेमाल की गई है। संभावित डेटा की आवश्यकता नहीं है और केवल अनुमान संभावित नुकसान प्रयोग किया जाता है। अधिकांश गुणात्मक जोखिम के तरीके बहुत से अंतर्संबंधित तत्वों का मुख्यतः खतरों, कमजोरियों और नियंत्रण का उपयोग करते हैं।
- (स) सूचना सुरक्षा नीति: यह नीति एक योजना अथवा कार्यो का नियम होती है जिसे निर्णयों, कार्यो और अन्य बातों को प्रभावित करने और निर्धारित

तयमों और  
केस प्रकार  
**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**  
**SEARCH ---> "STUDENTS OF CA AND CS"**

**PLEASE VISIT [WWW.STUDENTSOFCAANDCS.COM](http://WWW.STUDENTSOFCAANDCS.COM) FOR MORE UPDATES**

संपत्तियों जिसमें संवेदनशील सूचनाएँ भी शामिल हैं, को नियंत्रित, सुरक्षित और संस्थान के प्रयोगकर्ताओं के बीच आवंटित किया जाए।

सूचना सुरक्षा नीति अनेक बातों जैसे प्रकटीकरण, संबंधित अखंडता और उपलब्धता, किसके पास कौन-सी सूचनाएँ और किस प्रकार से पहुँच रही है, वह आधार जिन पर अभिगम्यता के निर्णय लिए गए, कम से कम सुविधाएँ बनाम अनुकूलतम लाभ की सहभागिता, कर्तव्यों का खण्डन, सूचनाओं का अधिकार किसके पास है और कौन उन्हें नियंत्रित करता है, और अधिकार के मामले का पता लगाती है।

प्रमुख मुद्दे जो इस नीति को संबंधित करने चाहिए:

- सूचना सुरक्षा की परिभाषा
- सूचना सुरक्षा का संस्थान के लिए महत्वपूर्ण होने के कारण, इसके लक्ष्य और सिद्धान्त,
- सुरक्षा नीति, सिद्धान्त, स्तरों, अनुकूलता की आवश्यकता पर संक्षिप्त व्याख्या,
- सभी प्रासंगिक सूचना सुरक्षा उत्तरदायित्वों की परिभाषा,
- दस्तावेजीकरण का समर्थन करने के लिए संदर्भ।

प्रश्न 6

(अ) सूचना प्रौद्योगिकी संरचना लाइब्रेरी (ITIL) ढांचे के तहत, निम्नलिखित के महत्व पर चर्चा करें :

(i) विमोचन (Release) प्रबंधन

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

(अंक 6)

- (ब) मिस्टर A को अपने सेलफोन पर मिस्टर B के बारे में कुछ जानकारी प्राप्त हुई है। वह जानते हैं कि यह जानकारी प्रेषक द्वारा चुराई गई है। उन्होंने न सिर्फ उस जानकारी को अपने पास रखा बल्कि इसे मिस्टर B और उनके मित्रों को भी भेज दिया। इस कृत्य से मिस्टर B नाराज है और उनकी जान को भी खतरा है।

मिस्टर B आपसे सुझाव लेना चाहते हैं, कि सूचना प्रौद्योगिकी (संशोधन) अधिनियम कि किस धारा के अन्तर्गत वे पुलिस में FIR दर्ज करवा सकते हैं? मिस्टर B को अधिनियम के लागू होने वाली धाराओं का ब्यौरा देते हुए सलाह दें।

(अंक 6)

- (स) 'हर कंपनी जो कि उद्यम संसाधन नियोजन लागू करना चाहता है उसे एक या अन्य रूप में अपनी प्रक्रियाओं की पुर्नअभियान्त्रिकी करनी होगी।' इस कथन के प्रकाश में, किन्हीं चार प्रक्रियाओं का वर्णन करें जिनमें पुर्नअभियान्त्रिकी की जा सकती है।

(अंक 6)

उत्तर

- (अ) (i) विमोचन (रिलीज) प्रबन्धन आई टी आई एल में: रिलीज प्रबन्धन सॉफ्टवेयर और हार्डवेयर के स्वतन्त्र और स्वचालित वितरण को प्लेटफॉर्म देने के लिए किया जाता है, जिसमें पूरे आईटी ढाँचे में लाइसेन्स नियन्त्रण भी शामिल है। उचित सॉफ्टवेयर और हार्डवेयर नियन्त्रण लाइसेन्सयुक्त, परीक्षित और संस्करण - प्रमाणित सॉफ्टवेयर व हार्डवेयर

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES** सही ढंग  
**SEARCH ---> "STUDENTS OF CA AND CS"** के विकास



और क्रियान्वयन के दौरान गुणवत्ता नियन्त्रण भी रिलीज प्रबन्धन की जिम्मेदारी है। यह इस बात को सुनिश्चित करता है कि सभी सॉफ्टवेयरों को व्यावसायिक प्रक्रियाओं की माँगों की पूर्ति करने के लिए संकल्पनात्मक रूप से अनुकूल बनाया जा सकता है। रिलीज प्रबन्धन के लक्ष्य निम्न हैं -

- सॉफ्टवेयर जारी करने की योजना बनाना,
- आईटी प्रणालियों में परिवर्तनों के वितरण और संस्थापन के लिए पद्धतियों की रचना और क्रियान्वयन,
- नए विमोचनों की योजना बनाने और उन्हें जारी करते समय ग्राहकों की अपेक्षाओं को प्रभावी ढंग से सम्प्रेषित करना,
- आईटी प्रणालियों के परिवर्तनों के वितरण और संस्थापन को नियंत्रित करना।

(ii) आई टी आई एल में आईसीटी संरचना प्रबन्धन - आईसीटी संरचना प्रबन्धन प्रक्रियाएँ आवश्यकताओं के विश्लेषण, नियोजन, रचना, तैनाती, प्रबन्धन के चल रहे कार्यकलाप व आई सी टी संरचना की तकनीकी सहायता की अनुशंसा करती है। संरचना प्रबन्धन प्रक्रियाएँ आईटीआईएल के अन्तर्गत उन प्रक्रियाओं का वर्णन करती है जो सीधे उन आईसीटी उपकरणों और सॉफ्टवेयर से सम्बन्धित है, जो ग्राहकों को आईसीटी सेवाएँ प्रदान करने में लगे हैं, ये निम्नलिखित हैं:

- आईसीटी रचना व नियोजन,
- आईसीटी तैनाती,

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

(ब) यह साफ नहीं है कि मिस्टर B FIR मिस्टर A के खिलाफ करवाना चाहते हैं या प्रेषक के खिलाफ जिसने जानकारी चुराई है या दोनों के खिलाफ।

सबसे व्यावहारिक धारणा पर विचार करते हुए यदि यह मान ले कि मिस्टर B मिस्टर A के खिलाफ FIR दर्ज करवाते हैं तो वह सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 के निम्न खण्ड के अंतर्गत फाइल कर सकते हैं :

- धारा 66 A : आपत्तिजनक संदेश संचार सेवा आदि के माध्यम से भेजने पर सजा,
- धारा 66 B : असत्यनिष्ठा द्वारा कंप्यूटर संसाधन या संचार उपकरण की चोरी करने पर सजा, और
- धारा 66 E : गोपनीयता के उल्लंघन के लिए सजा,  
इस संबंध में लागू धाराओं को निम्न रूप में दिया गया है:

(धारा 66A) : संचार सेवा के माध्यम से आपत्तिजनक संदेश आदि भेजने के लिए सजा

कोई भी व्यक्ति यदि कम्प्यूटर संसाधन या संचार उपकरण के माध्यम से सूचना भेजता है -

(अ) मोटे तौर पर आक्रमक या किसी भी प्रकार की खतरनाक चरित्र की जानकारी, या

(ब) ऐसी सूचना जो उसे पता है झूठी है, लेकिन झुंझलाहट, असुविधा, खतरा, नुकसान या अपमान जैसी आर्थिक क्षति या नुकसान पैदा करने

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

ग उपयोग

(स) कोई इलेक्ट्रॉनिक मेल या इलेक्ट्रॉनिक मेल संदेश इसके प्राप्तकर्ता को झुंझलाहट या असुविधा या प्राप्तकर्ता को संदेशों की उत्पत्ति के बारे में गुमराह करने के उद्देश्य से भेजा जाए तो यह तीन साल तक के कारावास और जुर्माने तक दण्डनीय होगा।

स्पष्टीकरण : इस धारा के प्रयोजन के लिए, मर्दे “इलेक्ट्रॉनिक मेल” और “इलेक्ट्रॉनिक मेल संदेश” का अर्थ एक संदेश या निर्मित सूचना या प्रेषित या कम्प्यूटर द्वारा प्राप्त, कम्प्यूटर सिस्टम, कम्प्यूटर संसाधन या संचार उपकरण में अनुलग्नक सहित पाठ, छवि, ऑडियो, वीडियो और कोई भी अन्य इलेक्ट्रॉनिक रिकॉर्ड।

(धारा 66B) धोखेबाजी द्वारा चोरी से कम्प्यूटर संसाधन अथवा संप्रेषण यंत्र को प्राप्त करने की सजा

जो कोई बेईमानी से किसी चोरी किए हुए कम्प्यूटर संसाधन अथवा संप्रेषण यंत्र को प्राप्त करता है अथवा अपने पास यह जानते हुए धारण करता है कि उक्त कम्प्यूटर अथवा संप्रेषण यंत्र चोरी का है तो वह व्यक्ति सजा का पात्र बन जाता है इसके लिए उसे तीन वर्ष तक की सजा और एक लाख रुपये तक का जुर्माना अथवा दोनों भुगतने पड़ सकते हैं।

(धारा 66E) निजता की गोपनीयता का उल्लंघन करने की सजा

कोई भी व्यक्ति जब किसी दूसरे व्यक्ति की अनुमति के बिना उसके व्यक्तिगत क्षेत्र को जानबूझकर तस्वीरों में कैद करता है, प्रकाशित करता है अथवा संप्रेषित कर उसकी गोपनीयता को खंडित करता है तो उस व्यक्ति को सजा का पात्र बन जाता है इसके लिए उसे तीन वर्ष तक की सजा और एक लाख रुपये तक का जुर्माना अथवा दोनों भुगतने पड़ सकते हैं।

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

हालांकि, उत्तर अन्य दो धारणाओं के आधार पर भी दिया जाता सकता है।

(स) प्रश्न में दिये गये वाक्य कि रोशनी में, निम्न मुख्य प्रक्रियाएँ हैं जहाँ पुर्नअभियान्त्रिकी की आवश्यकता है :

- भविष्यवाणी : लम्बी अवधि के दौरान बिक्री, निधि के प्रवाह आदि को दर्शाती है, जैसे दो वर्षों के दौरान।
- निधि का प्रबन्धन : निधियों की आवश्यकता और इन निधियों के संचय का तरीका। अनिश्चितता और जोखिम जैसे तत्वों पर विचार करना होता है। 'यदि ऐसा हो तो' जैसे प्रश्नों से अनुकृति - निर्माण भी शामिल है।
- मूल्य नियोजन : उन कीमतों का निर्धारण जिन पर उत्पाद उपलब्ध करवाए जाते हैं। इसके अन्तर्गत वाणिज्यिक डेटाबेस सेवाओं जैसी तकनीक मूल्य निर्धारण के लिए लागू की जाती है। प्रतिक्रिया और संवेदनशीलता विश्लेषण भी इसमें शामिल है।
- बजट आवंटन : विभिन्न कार्यों के लिए आवंटित निधियों के वांछित मिश्रण का अनुमान लगाने के लिए कम्प्यूटरीकृत अलगोरिथम का इस्तेमाल।
- सामग्री आवश्यकता का नियोजन : कच्चे माल से नए उत्पादों के निर्माण प्रक्रिया, जिसमें समयबद्धन और आवश्यकता नियोजन शामिल है। साथ ही, वास्तविक उत्पादन के निरीक्षण व नियोजन की गतिविधियाँ भी शामिल है।
- गुणवत्ता नियंत्रण : यह उन गतिविधियों का ध्यान रखता है ताकि उत्पादन वांछित गुणवत्ता बनायी जा सके।

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**

प्रश्न 7

निम्न में से किन्हीं चार पर संक्षिप्त टिप्पणी करें :

- (अ) सूचना प्रणाली लेखा परीक्षण नीति के उद्देश्य। (4 अंक)
- (ब) आपदा रिकवरी योजना बनाने के लिए प्रयोग में आने वाले अंकक्षण उपकरण और तकनीक। (4 अंक)
- (स) जोखिम का आकलन (4 अंक)
- (ड) उद्यम संसाधन नियोजन की विफलता के कारण (4 अंक)
- (घ) (धारा 19) सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 के अन्तर्गत विदेशी प्रमाणीकरण प्रधिकरणों की मान्यता। (4 अंक)

उत्तर

- (अ) सूचना प्रणाली परीक्षण नीति के उद्देश्य : लेखा परीक्षण नीति का उद्देश्य ऑडिट टीम को आई टी अवसंरचना प्रणाली आधारित लेखा परीक्षा का संचालन करने के लिए दिशा निर्देश प्रदान करना है। लेखा परीक्षण पूरी प्रणाली सामान्य से सामान्य सुरक्षा खतरों से रक्षा करने के लिए किया जाता है जैसे गोपनीय डेटा तक पहुँच, विभाग के कम्प्यूटर का अनाधिकृत उपयोग, पासवर्ड प्रकटीकरण समझौता, वायरस के संक्रमण, सेवा हमलों के इनकार आदि।

लेखा परीक्षण सूचना और संसाधनों की अखंडता, गोपनीयता और उपलब्धता सुनिश्चित करने के लिए आयोजित किया जा सकता है। सूचना प्रणाली लेखा परीक्षण नीति को लेखा परीक्षण के उद्देश्य और उसके दायरे

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES** किया जाता

**SEARCH ---> "STUDENTS OF CA AND CS"**

- सूचना प्रणाली परिसंपत्ति/संसाधनों की रक्षा के लिए,
- डेटा की अखण्डता बनाए रखने के लिए,
- सिस्टम के प्रभाव बनाए रखने के लिए,
- प्रणाली दक्षता सुनिश्चित करने के लिए, और
- सूचना प्रणाली से संबंधित नीतियों, दिशा-निर्देशों, परिपत्रों और किसी भी अन्य निर्देशों की अनुपालना हेतु।

(ब) आपदा रिकवरी योजना के लिए अंकेक्षण उपकरण और तकनीक : सबसे अच्छा लेखा परीक्षा उपकरण और तकनीक आपदा का आवधिक अनुकरण है। अन्य अंकेक्षण तकनीकों में निगरानी, साक्षात्कार चेकलिस्ट, पूछताछ, बैठकें, प्रश्नावलियाँ और दस्तावेजीकरण का पुनर्वलोकन शामिल है। इन्हें निम्नानुसार वर्गीकृत किया जा सकता है:

- स्वचालित उपकरण - इनका प्रयोग कर बड़ी कम्प्यूटर व्यवस्था के कई दोषों के लिए जाँच बहुत कम समय में की जा सकती है। ये खतरों की पहचान करने व खतरों की संभावनाओं का पता लगाने का काम करते हैं, जैसे : कमजोर एक्सेस नियंत्रण, कमजोर पासवर्ड, सिस्टम सॉफ्टवेयर में एकात्मकता का अभाव।
- आंतरिक नियंत्रण अंकेक्षण - इसमें पूछताछ, निगरानी और जाँच शामिल है। यह प्रक्रिया अवैध कार्यों, गलतियों, अनियमितताओं या कानूनन तथा नियम का पालन न करने की स्थितियों की पहचान करती है।
- आपदा और सुरक्षा जाँच सूची - जाँच सूची का प्रयोग व्यवस्था का अंकेक्षण करने के लिए किया जा सकता है। जाँच सूची का आधार आपदा रिकवरी की नीतियाँ और कार्य होते हैं. जो नीव का काम करते हैं। जाँच

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES** सत्यापित

**SEARCH ---> "STUDENTS OF CA AND CS"**

- प्रभाव का परीक्षण - इसका प्रयोग व्यवस्था को होने वाले संभावित खतरों को पहचानने के लिए होता है।

(स) जोखिम का आंकलन : जोखिम मूल्यांकन गतिविधि एक प्रभावी दृष्टिकोण प्रदान कर सकता है, जो आपदाओं से बचने के लिए नींव के रूप में कार्य करता है। आपदा और व्यापार निरंतरता योजना में यह एक महत्वपूर्ण चरण है। एक सुपरिक्षित आकस्मिकता योजना विकसित करने के लिए जोखिम का आंकलन आवश्यक है। जोखिम आकलन संसाधनों (परिसम्पत्तियों) को खतरों का विश्लेषण, एवं उनको पर्याप्त रूप से सुरक्षित रखने के लिए आवश्यक सुरक्षा की मात्रा का निर्धारण है, ताकि आपदा की स्थिति में, महत्वपूर्ण सिस्टम्स, परिचालन एवं सेवाओं को अपर्याप्त परीक्षण के कारण हो सकता है।

सूचना की अनुपलब्धता की स्थिति में, शामिल जोखिमों का निर्धारण करने हेतु जोखिम आकलन एप्लीकेशन्स के प्राथमिकीकरण, आरक्षितता चिन्हित करने एवं रिकवरी परिदृश्य विकसित करने हेतु एक महत्वपूर्ण तकनीक है।

(द) उद्यम संसाधन नियोजन परियोजनाओं की विफलता के कारण : अपने सरलतम स्तर पर उद्यम संसाधन नियोजन आपकी कम्पनी के विभागों में विभिन्न उत्तरदायित्वों के निर्वाह के लिए सर्वश्रेष्ठ तौर-तरीकों का एक समुच्चय है। इन दायित्वों में वित्त, उत्पादन और गोदाम भी शामिल है। सॉफ्टवेयर से अधिकतम लाभ प्राप्त करने के लिए आपको अपनी कंपनी के लोगों को सॉफ्टवेयर में बताए गए कामकाज के तौर-तरीके अपनाने के लिए तैयार करना होगा। उद्यम संसाधन नियोजन का प्रयोग करने जा रहे अलग-अलग विभागों के लोग यदि इस बात पर सहमत नहीं होते हैं

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES** तौर-तरीके  
**SEARCH ---> "STUDENTS OF CA AND CS"** ऐसे में वे

PLEASE VISIT [WWW.STUDENTSOFCAANDCS.COM](http://WWW.STUDENTSOFCAANDCS.COM) FOR MORE UPDATES

आईटी से यह माँग करेंगे कि उस सॉफ्टवेयर को बदला जाय ताकि वह उनके वर्तमान तौर-तरीकों से मेल खाए। यहीं पर ईआरपी परियोजनाए टूटने लगती हैं।

सॉफ्टवेयर कैसे स्थापित होगा, अथवा स्थापित होगा या नहीं, इसे लेकर दफ्तर के अंदर अक्सर जमकर राजनीति और उठापटक भी होती है। कुछ शक्तिशाली व्यावसायिक चौधरियों की इच्छाओं से मेल खाने के लिए ईआरपी सॉफ्टवेयर को संशोधित करने के लम्बे और खर्चीले अनुकूलन प्रयासों में आईटी अक्सर उलझकर रह जाता है। इस प्रकार के अनुकूलन सॉफ्टवेयर को और अस्थिर बनाते हैं। जब सॉफ्टवेयर जीवन्त होता है, तब ऐसे प्रयोगों के कारण उसका रखरखाव भी कठिन होता है। चूंकि ईआरपी व्यवसाय के कार्यकलापों का अच्छा-खासा हिस्सा समेटता है, सॉफ्टवेयर की असफलता कम्पनी को बिल्कुल ठप्प कर सकती है।

कम्पनियाँ अक्सर एक ओर गलती कर बैठती हैं। वे यह मान लेती हैं कि सॉफ्टवेयर के अनुकूलन की तुलना में लोगों की आदतें बदलना ज्यादा आसान है। दरअसल ऐसा नहीं है। आपकी कम्पनी के लोगों को अपने कामकाज के तौर-तरीकों में सुधार के लिए सॉफ्टवेयर के इस्तेमाल के लिए राजी करना ज्यादा कठिन चुनौती है। यदि लोग परिवर्तन का प्रतिरोध करने की प्रवृत्ति रखते हैं, तो ईआरपी प्रकल्प की विफलता की सम्भावना ज्यादा है।

- (घ) (धारा 19) विदेशी प्रमाणीकरण प्राधिकरणों की मान्यता : धारा 19 को नियंत्रक की शक्तियाँ जिन्हें पहले से ही केन्द्र सरकार की स्वीकृति प्राप्त होती है, जिससे विदेशी प्रमाणीकरण प्राधिकरण को विनियमों द्वारा लागू

DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES है। सूचना  
SEARCH ---> "STUDENTS OF CA AND CS"



तकनीक अधिनियम संशोधन, 2008 के अनुसार, धारा 19 निम्न प्रकार से है -

- (1) इस अधिनियम के उद्देश्य के लिए विनियमों द्वारा संभवतः लागू की गई शर्तों व नियमों का विषय, नियंत्रक संभवतः केन्द्र सरकार द्वारा प्रदान की गई पिछली स्वीकृति के साथ और आधिकारिक राजपत्र में अधिसूचना के द्वारा, किसी भी विदेशी प्रमाणीकरण प्राधिकरण के तौर पर मान्यता दी जाती है।
- (2) जहाँ पर कोई भी प्रमाणीकरण प्राधिकरण को उपधारा (1) अंतर्गत मान्यता प्रदान की जाती है, इस प्रकार का प्रमाणीकरण प्राधिकरण जारी इलेक्ट्रॉनिक हस्ताक्षर प्रमाण पत्र इस अधिनियम के लिए वैध होता है।
- (3) नियंत्रक यदि इस बात से संतुष्ट हो जाता है कि प्रमाणीकरण प्राधिकरण को उपधारा (1) की जिन शर्तों व नियमों के आधार पर प्रमाण पत्र जारी किया गया था उनमें से किसी का उल्लंघन प्रमाणीकरण प्राधिकरण के द्वारा किया गया है तो वह इस कारण रिकॉर्ड में लिखित रूप में रखने के लिए आधिकारिक राजपत्र में अधिसूचना के द्वारा जारी कर मान्यता को रद्द कर सकता है।

**DOWNLOAD OUR ANDROID APP FROM PLAYSTORE TO GET UPDATES**

**SEARCH ---> "STUDENTS OF CA AND CS"**