परिशिष्ट – I
क्लाउड कंप्यूटिंग सेवाओं का उपयोग

ऐसे कई क्लाउड परिनियोजन और सेवा मॉडल हैं जो वर्तमान समय में सामने आए हैं। ये आम तौर पर प्रौद्योगिकी स्टैक की सीमा पर आधारित होते हैं जिसे उपभोक्ता इकाई द्वारा अपनाया जाएगा। इनमें से प्रत्येक मॉडल[6] में तदनुरूप सेवा, व्यावसायिक लाभ और जोखिम प्रोफाइल/ पृष्ठभूमि सम्मिलित है।

इन निदेशों में निर्धारित आईटी सेवा नियंत्रणों की आउटसोर्सिंग के अलावा, विनियमित संस्थान क्लाउड वातावरण में डेटा के भंडारण, कंप्यूटिंग और संचलन के लिए निम्नलिखित आवश्यकताओं को अपनाएंगे:

1. क्लाउड समाधान को अपनाने पर ध्यान देते समय, वर्तमान आईटी अनुप्रयोग पदचिह्न और संबंधित लागतों[7] के लिए अपनाई गई व्यावसायिक रणनीति और लक्ष्यों का विश्लेषण करना अनिवार्य है। क्लाउड एडोप्शन में, केवल गैर-व्यावसायिक महत्वपूर्ण कार्यभार को क्लाउड में स्थानांतरित करने से लेकर एसएएएस एडोप्शन जैसे महत्वपूर्ण व्यावसायिक अनुप्रयोग और बीच-बीच में विभिन्न संयोजन शामिल है, जो एक व्यावसायिक प्रौद्योगिकी जोखिम मूल्यांकन पर आधारित होना चाहिए।

2. क्लाउड सेवाओं को प्रयुक्त करने में विनियमित संस्थान, अन्य बातों के साथ-साथ यह सुनिश्चित करेंगे कि आईटी सेवाओं की आउटसोर्सिंग नीति डेटा के पूरे समय चक्र पर ध्यान देगी, यानी डेटा निर्माण से लेकर क्लाउड में इसकी शुरुआत से डेटा के स्थायी रूप से मिटने/हटने तक की पूरी अवधि को शामिल करती है। विनियमित संस्थान यह सुनिश्चित करेंगे कि निर्दिष्ट प्रक्रियाएँ व्यावसायिक आवश्यकताओं और कानूनी एवं विनियामक आवश्यकताओं के अनुरूप हैं।
3. क्लाउड सेवाओं के अभिग्रहण में, विनियमित संस्थान उचित जोखिम प्रबंधन ढांचे की स्थापना करते समय क्लाउड सेवा विशिष्ट कारकों, जैसे, बहु-उपयोगकर्ता, बहु-स्थान भंडारण/डेटा का प्रसंस्करण आदि एवं परिचारक जोखिमों को ध्यान में रखेंगे। क्लाउड सुरक्षा आरई और क्लाउड सर्विस प्रोवाइडर (सीएसपी) की एक साझी जिम्मेदारी है। विनियमित संस्थान क्लाउड सेवाओं को अपनाने में संयुक्त उत्तरदायित्व मॉडल की उपयुक्तता के अनुसार आवश्यक नियंत्रणों को लागू करने के लिए कुछ *क्लाउड सुरक्षा सर्वोत्तम प्रथाओं*[8] का उल्लेख करेंगे।

---

[6] उदाहरण के लिए, कुछ क्लाउड सेवा और परिनियोजन मॉडल हैं: ए) एक सेवा के रूप में बुनियादी ढांचा (आईएएएस): यह सेवा गणना, भंडारण, नेटवर्क और अन्य बुनियादी संसाधन प्रदान करती है ताकि ग्राहक अपने अनुप्रयोगों को विकसित और परिनियोजित कर सके। बी) एक सेवा के रूप में प्लैटफ़ार्म (पीएएएस): यह सेवा ग्राहक को बुनियादी ढांचे के साथ अनुप्रयोग, मिडलवेयर, डेटाबेस, विकास वातावरण और अन्य उपकरणों के निर्माण के लिए सॉफ्टवेयर प्रदान करती है। सी) एक सेवा के रूप में सॉफ्टवेयर (एसएएएस): ग्राहक क्लाउड इंफ्रास्ट्रक्चर पर सेवा प्रदाता द्वारा प्रदान किए गए अनुप्रयोग (ओं) का उपयोग करता है। (घ) अनुप्रयोग सेवाओं के अलावा, क्लाउड सेवा प्रदाता (सीएसपी) तीन सामान्य सेवाओं यथा किसी सेवा के रूप में डेटाबेस, किसी सेवा के रूप में सुरक्षा, सेवा और अन्य के रूप में संग्रहण के अतिरिक्त अलग-अलग जोखिम स्तर वाली कई प्रकार की सेवाएँ भी प्रदान करता है। परिनियोजन मॉडल: क्लाउड सेवाएं निजी क्लाउड, पब्लिक क्लाउड, हाइब्रिड क्लाउड, कम्युनिटी क्लाउड जैसे लोकप्रिय मॉडल के माध्यम से उपलब्ध करवाई जाती हैं।

[7] उदाहरण के लिए, क्लाउड से संबंधित व्यय के विभिन्न शीर्ष अनुप्रयोग रिफैक्टरिंग, एकीकरण, परामर्श, प्रवासन, कार्यभार के आधार पर अनुमानित आवर्ती व्यय आदि हो सकते हैं।

[8] i.) एनआईएसटी एसपी 800-210 क्लाउड सिस्टम के लिए सामान्य पहुंच नियंत्रण दिशानिर्देश - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf
ii) एमईआईटीवाई का क्लाउड सुरक्षा सर्वोत्तम प्रथाएं दस्तावेज़ - https://www.meity.gov.in/writereaddata/files/2.%20WI3_Cloud%20Security%20Best%20Practices_06112020.pdf

4. **क्लाउड गवर्नेंस:** विनियमित संस्थान समुचित रूप से स्थापित और प्रलेखित क्लाउड अभिग्रहण नीति को अभिग्रहीत और प्रदर्शित करेंगे। इस तरह की नीति को अन्य बातों के साथ-साथ उन गतिविधियों की पहचान करनी चाहिए, जिन्हें क्लाउड में हस्तांतरित किया जा सकता है; विभिन्न हितधारकों के हितों की सुरक्षा को सक्षम और समर्थित करना चाहिए, गोपनीयता, सुरक्षा, डेटा संप्रभुता, पुनर्प्राप्ति और डेटा भंडारण आवश्यकताओं सहित डेटा वर्गीकरण के समकक्ष विनियामक आवश्यकताओं का अनुपालन सुनिश्चित करना चाहिए। यह नीति सीएसपी से जुड़े जोखिमों के प्रबंधन और सतत निगरानी के लिए समुचित सावधानी से संबंधित उपाय करेगी।

5. **क्लाउड सेवा प्रदाता (सीएसपी)**

सीएसपी के चयन के लिए विचार: विनियमित संस्थान आरई यह सुनिश्चित करेंगे कि सीएसपी का चयन सीएसपी के व्यापक जोखिम मूल्यांकन पर आधारित है। विनियमित संस्था केवल सीएसपी के साथ अनुबंध में प्रवेश करेगी जो उन अधिकार क्षेत्रों के अधीन होगा जो डेटा भंडारण, डेटा संरक्षण और गोपनीयता जैसे पहलुओं से संबंधित अधिकारों सहित विनियमित संस्था के लिए उपलब्ध अधिकारों और करारों की प्रवर्तनीयता को बनाए रखते हैं।

6. **क्लाउड सेवा प्रबंधन और सुरक्षा विचार**

ए) सेवा और प्रौद्योगिकी अवरचना: विनियमित संस्थान यह सुनिश्चित करेंगे कि क्लाउड-आधारित अनुप्रयोग समर्थित सेवा और प्रौद्योगिकी अवरचना विश्व स्तर पर मान्यता प्राप्त संरचना सिद्धांतों और मानकों के अनुपालन में बनाई गई है। विनियमित संस्थान ऐसी प्रौद्योगिकी संरचना को प्राथमिकता देंगे जो सुरक्षित कंटेनर-आधारित डेटा प्रबंधन प्रदान करती है, जहां एन्क्रिप्शन कुंजी और हार्डवेयर सुरक्षा मॉड्यूल विनियमित संस्था के नियंत्रण में हों। संरचना को कंटेनरों, छवियों और रिलीज को प्रबंधित करने के लिए उपकरणों और प्रक्रियाओं का एक मानक सेट प्रदान करना चाहिए। बहु-उपयोगकर्ता परिवेशों को डेटा अखंडता और गोपनीयता जोखिमों एवं डेटा के सह-मिलन के विरुद्ध संरक्षित किया जाना चाहिए। आर्किटेक्चर लचीला होना चाहिए और डेटा / सूचना सुरक्षा पर न्यूनतम प्रभाव के साथ क्लाउड आर्किटेक्चर में किसी एक या घटकों के संयोजन की विफलता की स्थिति में सुचारू रूप से पुनर्प्राप्ति को सक्षम करना चाहिए।

बी) पहचान और अभिगम प्रबंधन (आईएएम): आईएएम को सीएसपी के साथ सहमति दी जाएगी और उपयोगकर्ता-पहुँच और विशेषाधिकार-पहुँच के संबंध में क्लाउड होस्टेड एप्लीकेशनों के लिए भूमिका-आधारित पहुंच प्रदान करना सुनिश्चित किया जाएगा। क्लाउड-आधारित एप्लीकेशनों की पहचान और पहुँच प्रबंधन के लिए दृढ़ पहुंच नियंत्रण, जैसा कि ऑन-प्रिमाइसेस एप्लिकेशन के लिए लागू है, स्थापित किए जा सकते हैं। क्लाउड सेवा मॉडल को ध्यान में रखे बिना क्लाउड-होस्टेड एप्लिकेशन में सभी प्रकार की उपयोगकर्ता-पहुँच और विशेषाधिकार-पहुँच भूमिकाओं के लिए कर्तव्यों और भूमिका संघर्ष मैट्रिक्स का पृथक्करण लागू किया जाना चाहिए। पहुँच-प्रावधानों को 'जानने की जरूरत' और 'न्यूनतम विशेषाधिकार' के सिद्धांतों द्वारा नियंत्रित किया जाना चाहिए। इसके अलावा, क्लाउड एप्लिकेशन तक पहुंच के लिए बहु-कारक प्रमाणीकरण लागू किया जाना चाहिए।

सी) सुरक्षा नियंत्रण: विनियमित संस्थान यह सुनिश्चित करेंगे कि क्लाउड-आधारित एप्लिकेशन में सुरक्षा नियंत्रणों के कार्यान्वयन से ऑन-प्रिमाइसेस एप्लिकेशन में/ द्वारा प्राप्त नियंत्रण उद्देश्यों की तुलना में समान

या उच्च स्तर के नियंत्रण उद्देश्य प्राप्त हों। इसमें - नेटवर्क सुरक्षा संसाधनों और उनके कॉन्फ़िगरेशन के उचित परिनियोजन के माध्यम से सुरक्षित कनेक्शन; उचित और सुरक्षित कॉन्फ़िगरेशन, विनियमित संस्थान द्वारा उपयोग की जाने वाली क्लाउड आस्तियों की निगरानी; क्लाउड एप्लिकेशन और संबंधित संसाधनों में परिवर्तन को अधिकृत करने के लिए आवश्यक प्रक्रियाएं सुनिश्चित करना शामिल है।

डी) सुदृढ़ नियंत्रण और निगरानी: विनयमित संस्थान क्लाउड वातावरण में न्यूनतम निगरानी आवश्यकताओं को सटीक रूप से परिभाषित करेंगे। विनयमित संस्थानों को क्लाउड सेवा प्रदाता की सूचना/साइबर सुरक्षा क्षमता का आकलन करना सुनिश्चित करना चाहिए, जैसे कि,

i) सीएसपी भेद्यता और खतरों के प्रति अपने जोखिम के अनुरूप सूचना सुरक्षा नीति ढांचे को बनाए रखता है;
ii) सीएसपी भेद्यता और खतरों में परिवर्तन के संबंध में अपनी सूचना/साइबर सुरक्षा क्षमता को बनाए रखने में सक्षम है, जिसमें सूचना आस्तियों या इसके व्यावसायिक परिवेश में परिवर्तन के परिणाम भी शामिल हैं;
iii) आउटसोर्स सेवाओं के संबंध में सीएसपी द्वारा नियंत्रणों के परीक्षण की प्रकृति और आवृत्ति विनयमित संस्था द्वारा आउटसोर्स की जा रही सेवाओं की भौतिकता और खतरे के माहौल के अनुरूप है; और
iv) जहां लागू हो, उप-ठेकेदारों के साथ साझा किए जा रहे डेटा की गोपनीयता, अखंडता और उपलब्धता के संबंध में उप-ठेकेदारों का आकलन करने के लिए सीएसपी के पास तंत्र हो।

ई) घटना की रिपोर्टिंग और क्लाउड पर परिनियोजित सेवाओं से संबंधित घटनाओं से निपटने के लिए लॉग्स का उचित एकीकरण, सीएसपी से घटनाओं को विनियमित संस्था के एसओसी में, जहां कहीं भी लागू हो, और/या क्लाउड में संबंधित लॉग्स का प्रतिधारण सुनिश्चित किया जाएगा।

एफ) अपनी एप्लिकेशन को सुरक्षित करने में विनियमित संस्था के अपने प्रयासों को सीएसपी के साइबर लचीलेपन नियंत्रणों द्वारा पूरक किया जाएगा। सीएसपी/ विनियमित संस्था एप्लिकेशन को उन्नत खतरों/मैलवेयर से बचाने के लिए अपग्रेड, फिक्स, पैच और सर्विस पैक सहित सुरक्षा से संबंधित सॉफ्टवेयर के निरंतर और नियमित अपडेट सुनिश्चित करेगा।

जी) भेद्यता प्रबंधन: विनियमित संस्था यह सुनिश्चित करेगी कि सीएसपी के पास आवश्यक उद्योग-विशिष्ट खतरे को पहचानने की क्षमताओं द्वारा समर्थित खतरों और भेद्यताओं का प्रबंधन करने के लिए एक अच्छी तरह से शासित और संरचित दृष्टिकोण है।

7. आपदा बहाली और साइबर आघातसहनीयता

ए) विनियमित संस्था का व्यवसाय निरंतरता ढांचा यह सुनिश्चित करेगा कि आपदा की स्थिति में इसकी क्लाउड सेवाओं के प्रभावित या सीएसपी के विफल होने पर, विनियमित संस्था अखंडता और सुरक्षा सुनिश्चित करते हुए सेवाओं में न्यूनतम व्यवधान के साथ अपने महत्वपूर्ण संचालन जारी रख सके।

बी) विनियमित संस्थान यह सुनिश्चित करेंगे कि सीएसपी उनके द्वारा उपयोग में लाई जाने वाली क्लाउड सेवाओं के संबंध में साइबर आघातसहनीयता के लिए तत्परता और तैयारी के लिए प्रदर्शनात्मक क्षमताओं को स्थापित करे। अन्य बातों के साथ-साथ, आवश्यक हितधारकों सहित क्लाउड सेवाओं के विभिन्न स्तरों पर आपदा बहाली (डीआर) अभ्यासों के संचालन सहित सुदृढ़ घटना प्रतिक्रिया और पुनर्प्राप्ति अभ्यासों के माध्यम से इसे व्यवस्थित रूप से सुनिश्चित किया जाना चाहिए।

8. निकास रणनीति विकसित करते समय निम्नलिखित बिंदुओं का मूल्यांकन किया जा सकता है:

ए) एसएलए में निकास रणनीति और सेवा स्तर की शर्तें, *अन्य बातों के साथ-साथ*, कारक होंगी,

i) विनियमित संस्था के सेवा संपार्श्विक और सीएसपी द्वारा रखे गए डेटा को वापस करने के लिए सहमत प्रक्रियाएं और परिवर्तन समय;

ii) डेटा पूर्णता और सुवाह्यता;

iii) सीएसपी के वातावरण से विनियमित संस्थान की जानकारी को सुरक्षित करना;

iv) सेवाओं का सुचारु पारगमन; और

v) देनदारियों, हर्जाने, दंड और क्षतिपूर्ति की स्पष्ट परिभाषा।

बी) अनुप्रयोग और सेवा वितरण प्रौद्योगिकी स्टैक के जारी डिजाइन की निगरानी करना जिससे निकास योजना को संरेखित किया जाए।

सी) संविदात्मक रूप से सहमत निकास/समाप्ति योजनाओं में यह निर्दिष्ट होना चाहिए कि अखंडता और सुरक्षा को बनाए रखते हुए क्लाउड-होस्ट की गई सेवा (ओं) और डेटा को विनियमित संस्था के व्यवसाय की निरंतरता पर न्यूनतम प्रभाव के साथ क्लाउड से कैसे बाहर ले जाया जाएगा।

डी) लेन-देन के सभी रिकॉर्ड, ग्राहक और परिचालन संबंधी जानकारी, कॉन्फ़िगरेशन डेटा को तुरंत सीएसपी से एक व्यवस्थित तरीके से लिए जाने चाहिए और सीएसपी-एंड पर परिशोधन किया जाना चाहिए तथा सीएसपी से अलग करने से पहले स्वतंत्र आश्वासन मांगा जाना चाहिए।

9. **लेखापरीक्षा और आश्वासन:** अन्य बातों के साथ-साथ, क्लाउड उपयोग के अनुसार लेखापरीक्षा/आवधिक समीक्षा/तीसरे पक्ष के प्रमाणीकरण में, क्लाउड अभिशासन में विनियमित संस्थान और सीएसपी दोनों की भूमिकाएं और जिम्मेदारियां, पहुंच और नेटवर्क नियंत्रण, कॉन्फ़िगरेशन, निगरानी तंत्र, डेटा एन्क्रिप्शन, लॉग समीक्षा, परिवर्तन प्रबंधन, घटना प्रतिक्रिया, और आघातसहनीयता तत्परता तथा परीक्षण इत्यादि जैसे पहलू शामिल होने चाहिए।