সাইবার নিরাপত্তা

Topical Requirement

প্রাসঙ্গিক প্রয়োজনীয়তা

The Institute of
Internal Auditors

সাইবার নিরাপত্তার প্রাসঙ্গিক প্রয়োজনীয়তা

আন্তর্জাতিক পেশাগত অনুশীলন কাঠামো (International Professional Practices Framework®)-এর মধ্যে অন্তর্ভুক্ত রয়েছে বৈশ্বিক অভ্যন্তরীণ নিরীক্ষা মান (Global Internal Audit Standards™), প্রাসঙ্গিক প্রয়োজনীয়তা এবং বৈশ্বিক নির্দেশিকা। প্রাসঙ্গিক প্রয়োজনীয়তাগুলো বাধ্যতামূলক এবং বৈশ্বিক অভ্যন্তরীণ নিরীক্ষা মান-এর সাথে সংযুক্তভাবে ব্যবহার করতে হবে, যা প্রয়োজনীয় অনুশীলনের জন্য অনুমোদিত ভিত্তি প্রদান করে।

প্রাসঙ্গিক প্রয়োজনীয়তার সাথে সামঞ্জস্য রেখে কাজ করা অভ্যন্তরীণ নিরীক্ষা সেবাগুলোর কার্যক্রমে সামঞ্জস্য বৃদ্ধি করবে এবং নিরীক্ষা সেবা ও ফলাফলের গুণগতমান এবং নির্ভরযোগ্যতা উন্নত করবে। শেষ পর্যন্ত, প্রাসঙ্গিক প্রয়োজনীয়তাগুলো অভ্যন্তরীণ নিরীক্ষা পেশার মান বৃদ্ধি করে।

অভ্যন্তরীণ নিরীক্ষকদের অবশ্যই গ্লোবাল ইন্টারনাল অডিট স্ট্যান্ডার্ডের সাথে সামঞ্জস্য রেখে প্রাসঙ্গিক প্রয়োজনীয়তাগুলো প্রয়োগ করতে হবে। প্রাসঙ্গিক প্রয়োজনীয়তার সাথে সামঞ্জস্য রাখা নিশ্চয়তা সেবার জন্য বাধ্যতামূলক এবং পরামর্শমূলক সেবার জন্য সুপারিশকৃত।

প্রাসঙ্গিক প্রয়োজনীয়তা প্রযোজ্য হয় যখন বিষয়টি নিম্নলিখিতগুলোর একটি হয়:

ক. নিরীক্ষা পরিকল্পনার অন্তর্ভুক্ত একটি নিরীক্ষা কার্যক্রমের বিষয়বস্তু।

খ. নিরীক্ষা কার্যক্রম পরিচালনার সময় চিহ্নিত একটি বিষয়।

গ. মূল নিরীক্ষা পরিকল্পনার বাইরে একটি নিরীক্ষা কার্যক্র   অনুরোধের বিষয়বস্তু।

প্রাসঙ্গিক প্রয়োজনীয়তার প্রতিটি শর্ত প্রযোজ্য কিনা তা মূল্যায়নের প্রমাণ ডকুমেন্ট আকারে সংরক্ষণ করতে হবে। সব শর্ত প্রতিটি নিরীক্ষা কার্যক্রমে প্রযোজ্য নাও হতে পারে। যদি কোনো শর্ত বাদ দেওয়া হয়, তবে তার যৌক্তিক ব্যাখ্যা ডকুমেন্ট আকারে সংরক্ষণ করতে হবে। প্রাসঙ্গিক প্রয়োজনীয়তার সাথে সামঞ্জস্য রাখা বাধ্যতামূলক এবং এটি গুণগত মূল্যায়নের সময় মূল্যায়িত হবে।

িবিস্তানরি র‍্যারি র‍্যি "সাইবার নিরাপত্তার পর্াসনিক পর্মোর্য়ীাটো বেবহার নিমদজনশকা" পদেু।

সাইবার নিরাপত্তা

ন্যাশনাল ইনস্টিটিউট অব স্ট্যান্ডার্ডস অ্যান্ড টেকনোলজি (NIST) সাইবার নিরাপত্তাকে সহজভাবে সংজ্ঞায়িত করেছে, "সাইবার আক্রমণ থেকে সাইবারস্পেসের ব্যবহার রক্ষা বা প্রতিরক্ষা করার ক্ষমতা।" সাইবার নিরাপত্তা হলো বৃহত্তর তথ্য সুরক্ষা-এর একটি উপসেট, যা NIST দ্বারা সংজ্ঞায়িত করা হয়েছে, "তথ্য এবং তথ্য সিস্টেমগুলিকে অবৈধ প্রবেশ, ব্যবহার, প্রকাশ, বিঘ্ন, পরিবর্তন, বা ধ্বংস থেকে রক্ষা করার প্রক্রিয়া, যাতে গোপনীয়তা, অখণ্ডতা, এবং প্রাপ্যতা নিশ্চিত করা যায়।"

সাইবার নিরাপত্তা প্রতিষ্ঠানের সামগ্রিক নিয়ন্ত্রণ পরিবেশকে শক্তিশালী করে এবং তথ্য সম্পদগুলোকে অবৈধ অনুপ্রবেশ, বিঘ্ন, পরিবর্তন, বা ধ্বংস থেকে রক্ষা করার মাধ্যমে ঝুঁকি কমায়। সাইবার আক্রমণগুলি সরাসরি এবং পরোক্ষ প্রভাব সৃষ্টি করতে পারে, যা প্রায়ই গুরুতর হয়, কারণ কম্পিউটার, নেটওয়ার্ক, প্রোগ্রাম, তথ্য, এবং সংবেদনশীল তথ্য বেশিরভাগ প্রতিষ্ঠানের জন্য গুরুত্বপূর্ণ উপাদান।

সাইবার নিরাপত্তার শাসন, ঝুঁকি ব্যবস্থাপনা এবং নিয়ন্ত্রণ প্রক্রিয়াগুলো মূল্যায়ন এবং পর্যালোচনা।

এই প্রাসঙ্গিক প্রয়োজনীয়তা সাইবার নিরাপত্তার শাসন, ঝুঁকি ব্যবস্থাপনা এবং নিয়ন্ত্রণ প্রক্রিয়াগুলোর পরিকল্পনা এবং বাস্তবায়ন মূল্যায়নের জন্য একটি সুসংগত এবং বিস্তৃত পদ্ধতি প্রদান করে। এই প্রয়োজনীয়তাগুলো একটি প্রতিষ্ঠানে সাইবার নিরাপত্তা মূল্যায়নের জন্য ন্যূনত ভিত্তি উপস্থাপন করে।

শাসনব্যবস্থা: সাইবার নিরাপত্তার শাসন মূল্যায়ন এবং পর্যালোচনা।

প্রয়োজনীয়তা:

অভ্যন্তরীণ নিরীক্ষকদের অবশ্যই প্রতিষ্ঠানের সাইবার নিরাপত্তার শাসনব্যবস্থা সম্পর্কিত নিম্নলিখিত বিষয়গুলো মূল্যায়ন করতে হবে:

ক. একটি আনুষ্ঠানিক সাইবার নিরাপত্তা কৌশল এবং উদ্দেশ্য প্রতিষ্ঠিত এবং নিয়মিত হালনাগাদ করা হয়েছে। সাইবার নিরাপত্তার লক্ষ্য অর্জনের বিষয়ে হালনাগাদগুলো নিয়মিত বোর্ডে জানানো হয় এবং পর্যালোচনা করা হয়, যার মধ্যে কৌশল বাস্তবায়নের জন্য প্রয়োজনীয় সম্পদ এবং বাজেটের বিষয়গুলো অন্তর্ভুক্ত।

খ. সাইবার নিরাপত্তার সাথে সম্পর্কিত নীতিমালা এবং পদ্ধতিগুলো প্রতিষ্ঠিত এবং নিয়মিত হালনাগাদ করা হয় যাতে নিয়ন্ত্রণ পরিবেশকে শক্তিশালী করা যায়।

গ. সাইবার নিরাপত্তার লক্ষ্যগুলোকে সহায়তা করার জন্য দায়িত্ব এবং ভূমিকা নির্ধারণ করা হয়েছে এবং এই ভূমিকা পালনকারী ব্যক্তিদের জ্ঞান, দক্ষতা এবং সামর্থ্য নিয়মিতভাবে মূল্যায়নের একটি প্রক্রিয়া বিদ্যমান রয়েছে।

ঘ. সংশ্লিষ্ট অংশীজনদের সাইবার নিরাপত্তা পরিবেশে বিদ্যমান দুর্বলতা এবং উদীয়মান হুমকি নিয়ে আলোচনা এবং কার্যকর ব্যবস্থা নিতে যুক্ত করা হয়। এই অংশীজনদের মধ্যে জেষ্ঠ্য ব্যবস্থাপনা, অপারেশন বিভাগ, ঝুঁকি ব্যবস্থাপনা, মানব সম্পদ, আইন, সম্মতি, সরবরাহকারী এবং অন্যান্যরা অন্তর্ভুক্ত।

ঝুঁকি ব্যবস্থাপনা: সাইবার নিরাপত্তার ঝুঁকি ব্যবস্থাপনা মূল্যায়ন এবং পর্যালোচনা।

প্রয়োজনীয়তাসমূহ:

অভ্যন্তরীণ নিরীক্ষকদের অবশ্যই প্রতিষ্ঠানের সাইবার নিরাপত্তার ঝুঁকি ব্যবস্থাপনা সম্পর্কিত নিম্নলিখিত বিষয়গুলো মূল্যায়ন করতে হবে:

ক. প্রতিষ্ঠানের ঝুঁকি মূল্যায়ন এবং ঝুঁকি ব্যবস্থাপনার প্রক্রিয়াগুলোর মধ্যে সাইবার নিরাপত্তার হুমকি সনাক্তকরণ, বিশ্লেষণ, প্রশমন এবং পর্যবেক্ষণ, এবং এগুলোর কৌশলগত লক্ষ্য অর্জনের প্রভাব অন্তর্ভুক্ত।

খ. সাইবার নিরাপত্তার ঝুঁকি ব্যবস্থাপনা সমগ্র প্রতিষ্ঠানের মধ্যে পরিচালিত হয় এবং এর মধ্যে নিম্নলিখিত ক্ষেত্রগুলো অন্তর্ভুক্ত হতে পারে: তথ্য প্রযুক্তি, প্রতিষ্ঠানের ঝুঁকি ব্যবস্থাপনা, মানব সম্পদ, আইন, সম্মতি, কার্যক্রম, সরবরাহ চেইন, হিসাবরক্ষণ, অর্থনীতি এবং অন্যান্য।

গ. সাইবার নিরাপত্তার ঝুঁকি ব্যবস্থাপনার জন্য দায়িত্ব এবং কর্তব্য নির্ধারণ করা হয়েছে। একজন ব্যক্তি বা একটি দলকে চিহ্নিত করা হয়েছে যারা নিয়মিতভাবে পর্যবেক্ষণ এবং প্রতিবেদন প্রদান করে যে কীভাবে সাইবার নিরাপত্তার ঝুঁকি ব্যবস্থাপনা করা হচ্ছে, যার মধ্যে ঝুঁকি প্রশমনের জন্য প্রয়োজনীয় সম্পদ এবং উদীয়মান সাইবার নিরাপত্তার হুমকি সনাক্ত করা অন্তর্ভুক্ত।

ঘ. প্রতিষ্ঠানের নির্ধারিত ঝুঁকি ব্যবস্থাপনার নির্দেশিকা বা প্রযোজ্য আইনগত এবং নিয়ন্ত্রক সংস্থার নির্দেশনা অনুযায়ী অগ্রহণযোগ্য স্তরে পৌঁছানো যে কোনো সাইবার নিরাপত্তার ঝুঁকি (নতুন বা পূর্বে সনাক্ত) দ্রুত উন্নীত করার একটি প্রক্রিয়া প্রতিষ্ঠিত করা হয়। সাইবার নিরাপত্তার ঝুঁকির আর্থিক এবং অ-আর্থিক প্রভাব বিবেচনা করা উচিত।

ঙ. ব্যবস্থাপনা এবং কর্মচারীদের মধ্যে সাইবার নিরাপত্তার ঝুঁকি সচেতনতা যোগাযোগের জন্য একটি প্রক্রিয়া প্রতিষ্ঠিত করা হয় যেন ব্যবস্থাপনা নিয়মিতভাবে সমস্যাগুলো, ঘাটতি, ত্রুটি বা নিয়ন্ত্রণ ব্যর্থতার বিষয়গুলো সময়মতো প্রতিবেদন এবং সমাধানের সাথে পর্যালোচনা করতে পারে।

চ. প্রতিষ্ঠানটি একটি সাইবার নিরাপত্তার সংঘটন প্রতিক্রিয়া এবং পুনরুদ্ধার প্রক্রিয়া বাস্তবায়ন করেছে, যার মধ্যে সনাক্তকরণ, নিয়ন্ত্রন, পুনরুদ্ধার এবং পরবর্তী ঘটনার বিশ্লেষণ অন্তর্ভুক্ত। এই সংঘটন প্রতিক্রিয়া এবং পুনরুদ্ধার প্রক্রিয়া নিয়মিতভাবে পরীক্ষা করা হয়।

নিয়ন্ত্রণ: সাইবার নিরাপত্তার নিয়ন্ত্রণ প্রক্রিয়া মূল্যায়ন এবং পর্যালোচনা

প্রয়োজনীয়তাসমূহ:

অভ্যন্তরীণ নিরীক্ষকদের অবশ্যই প্রতিষ্ঠানের সাইবার নিরাপত্তার নিয়ন্ত্রণ প্রক্রিয়াগুলোর সাথে সম্পর্কিত নিম্নলিখিত বিষয়গুলো মূল্যায়ন করতে হবে:

ক. একটি প্রক্রিয়া প্রতিষ্ঠিত হয়েছে যা নিশ্চিত করে যে প্রতিষ্ঠানের সিস্টেম এবং তথ্যের গোপনীয়তা, অখণ্ডতা এবং প্রাপ্যতা সুরক্ষার জন্য অভ্যন্তরীণ নিয়ন্ত্রণ এবং বিক্রেতা-ভিত্তিক নিয়ন্ত্রণ উভয়ই কার্যকর রয়েছে। নিয়ন্ত্রণগুলো প্রতিষ্ঠানের সাইবার নিরাপত্তার লক্ষ্য অর্জন এবং সমস্যা দ্রুত সমাধানে কার্যকর কিনা তা নির্ধারণে নিয়মিত মূল্যায়ন হয়।

খ. একটি ট্যালেন্ট ম্যানেজমেন্ট প্রক্রিয়া প্রতিষ্ঠিত হয়েছে, যার মধ্যে সাইবার নিরাপত্তা কার্যক্র সম্পর্কিত প্রযুক্তিগত দক্ষতা উন্নয়ন এবং বজায় রাখার জন্য প্রশিক্ষণ অন্তর্ভুক্ত। এই প্রক্রিয়া নিয়মিত পর্যালোচনা করা হয়।

গ. উদীয়মান সাইবার নিরাপত্তার হুমকি এবং দুর্বলতাগুলো নিয়মিত পর্যবেক্ষণ এবং প্রতিবেদন প্রদান করার জন্য এবং সাইবার নিরাপত্তা কার্যক্র উন্নত করার সুযোগগুলো চিহ্নিত, অগ্রাধিকার প্রদান এবং বাস্তবায়নের জন্য একটি প্রক্রিয়া প্রতিষ্ঠিত হয়েছে।

ঘ. সাইবার নিরাপত্তাকে সমস্ত আইটি সম্পদের জীবনচক্র ব্যবস্থাপনায় (নির্বাচন, ব্যবহার, রক্ষণাবেক্ষণ এবং অবলোপন) অন্তর্ভুক্ত করা হয়েছে, যার মধ্যে হার্ডওয়্যার, সফটওয়্যার এবং বিক্রেতার পরিষেবা অন্তর্ভুক্ত।

ঙ. সাইবার নিরাপত্তাকে শক্তিশালী করার জন্য প্রক্রিয়াগুলো প্রতিষ্ঠিত হয়েছে, যার মধ্যে রয়েছে কনফিগারেশন, এন্ড-ইউজার ডিভাইস প্রশাসন, এনক্রিপশন, প্যাচিং, ব্যবহারকারীর অনুপ্রবেশ ব্যবস্থাপনা, এবং প্রাপ্যতা ও কর্মক্ষমতা পর্যবেক্ষণ। সফটওয়্যার উন্নয়নে (DevSecOps) সাইবার নিরাপত্তার বিষয়গুলো অন্তর্ভুক্ত করা হয়েছে।

চ. নেটওয়ার্ক সম্পর্কিত নিয়ন্ত্রণগুলো প্রতিষ্ঠিত হয়েছে, যেমন নেটওয়ার্ক-প্রবেশাধিকার নিয়ন্ত্রণ এবং বিভাজন; ফায়ারওয়ালের ব্যবহার এবং অবস্থান; বাহ্যিক নেটওয়ার্ক থেকে এবং বাহ্যিক নেটওয়ার্কে সংযোগ সীমিত করা; ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN)/জিরো ট্রাস্ট নেটওয়ার্ক অ্যাক্সেস (ZTNA); ইন্টারনেট অব থিংস (IoT) নেটওয়ার্ক নিয়ন্ত্রণ; এবং অনুপ্রবেশ সনাক্তকরণ/প্রতিরোধ ব্যবস্থা (IDS এবং IPS)।

ছ. এন্ডপয়েন্ট-যোগাযোগ নিরাপত্তা নিয়ন্ত্রণগুলো ইমেইল, ইন্টারনেট ব্রাউজার, ভিডিও কনফারেন্সিং, মেসেজিং, সামাজিক যোগাযোগ মাধ্যম, ক্লাউড এবং ফাইল-শেয়ারিং প্রোটোকলের তো পরিষেবাগুলোর জন্য প্রতিষ্ঠিত হয়েছে।

অভ্যন্তরীণ নিরীক্ষকদের ইনস্টিটিউট সম্পর্কে

অভ্যন্তরীণ নিরীক্ষকদের ইনস্টিটিউট (The IIA) একটি আন্তর্জাতিক পেশাদার সংস্থা, যা সারা বিশ্বে ২,৫৫,০০০-এরও বেশি সদস্যকে সেবা প্রদান করে এবং ২,০০,০০০-এর বেশি সার্টিফায়েড ইন্টারনাল অডিটর® (CIA®) সনদ প্রদান করেছে। ১৯৪১ সালে প্রতিষ্ঠিত এই সংস্থা সারা বিশ্বে অভ্যন্তরীণ নিরীক্ষা পেশার মান, শংসাপত্র, শিক্ষা, গবেষণা, এবং কারিগরি নির্দেশনার ক্ষেত্রে নেতা হিসেবে স্বীকৃত। আরও তথ্যের জন্য, ভিজিট করুন www.theiia.org.

February 2025

The Institute of Internal Auditors

Global Headquarters
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101