সাইবার নিরাপত্তা

Topical Requirement

প্রাসঙ্গিক প্রয়োজনীয়তা

ব্যবহারকারী নির্দেশিকা

The Institute of
Internal Auditors

Contents

বিষয়ভিত্তিক প্রয়োজনীয়তার সংক্ষিপ্ত বিবরণ

বিষয়ভিত্তিক প্রয়োজনীয়তা আন্তর্জাতিক পেশাদার অনুশীলন কাঠামো (International Professional Practices Framework®)-এর একটি গুরুত্বপূর্ণ উপাদান, যা গ্লোবাল ইন্টারনাল অডিট স্ট্যান্ডার্ডস (Global Internal Audit Standards)™ এবং গ্লোবাল গাইডেন্স এর সাথে অন্তর্ভুক্ত। অভ্যন্তরীণ নিরীক্ষকদের ইনস্টিটিউট (IIA) গ্লোবাল ইন্টারনাল অডিট স্ট্যান্ডার্ডসের সাথে সমন্বয় করে বিষয়ভিত্তিক প্রয়োজনীয়তাগুলো ব্যবহারের নির্দেশ দিয়েছে, যা প্রয়োজনীয় অনুশীলনের জন্য কর্তৃত্বপূর্ণ ভিত্তি প্রদান করে। স্ট্যান্ডার্ডসের তথ্যসূত্র এই নির্দেশিকায় বারবার উপস্থিত হয়েছে, যা আরও বিস্তারিত তথ্যের উৎস হিসেবে কাজ করে।

বিষয়ভিত্তিক প্রয়োজনীয়তাগুলো অভ্যন্তরীণ নিরীক্ষকদের সাধারণ ঝুঁকি ক্ষেত্রগুলো মোকাবিলায় একটি আনুষ্ঠানিক পদ্ধতি প্রবর্তন করে, যা পেশার মধ্যে গুণমান এবং সামঞ্জস্যতা বৃদ্ধি করে। বিষয়ভিত্তিক প্রয়োজনীয়তাগুলো একটি ভিত্তি স্থাপন করে এবং বিষয়ভিত্তিক প্রয়োজনীয়তার সাথে সম্পর্কিত নিশ্চয়তা পরিষেবার জন্য প্রাসঙ্গিক মানদণ্ড প্রদান করে (**স্ট্যান্ডার্ড ১৩.৪ মূল্যায়ন মানদণ্ড**)। নিশ্চয়তা পরিষেবার জন্য বিষয়ভিত্তিক প্রয়োজনীয়তাগুলোর সাথে সামঞ্জস্য বাধ্যতামূলক এবং পরামর্শ পরিষেবার সময় মূল্যায়নের জন্য সুপারিশকৃত। বিষয়ভিত্তিক প্রয়োজনীয়তাগুলো নিশ্চয়তা কার্য সম্পাদনের সময় বিবেচনা করার মতো সমস্ত সম্ভাব্য দিককে অন্তর্ভুক্ত করার উদ্দেশ্যে নয়; বরং, এগুলো ন্যূনতম প্রয়োজনীয়তার একটি সেট সরবরাহ করার উদ্দেশ্যে তৈরি হয়েছে, যা বিষয়টির একটি সামঞ্জস্যপূর্ণ, নির্ভরযোগ্য মূল্যায়ন সক্ষম করে।

বিষয়ভিত্তিক প্রয়োজনীয়তাগুলো **IIA-এর থ্রি লাইনস মডেল** এবং **গ্লোবাল ইন্টারনাল অডিট স্ট্যান্ডার্ডস** এর সাথে সুস্পষ্টভাবে সংযুক্ত। **শাসন, ঝুঁকি ব্যবস্থাপনা, এবং নিয়ন্ত্রণ প্রক্রিয়াগুলো** বিষয়ভিত্তিক প্রয়োজনীয়তার প্রধান উপাদান, যা **স্ট্যান্ডার্ড ৯.১ শাসন, ঝুঁকি ব্যবস্থাপনা এবং নিয়ন্ত্রণ প্রক্রিয়াগুলোর বোঝা**র সাথে সামঞ্জস্যপূর্ণ। থ্রি লাইনস মডেলের ক্ষেত্রে, শাসন বোর্ড/পরিচালনা পর্ষদ সাথে সংযুক্ত, ঝুঁকি ব্যবস্থাপনা দ্বিতীয় লাইনের সাথে এবং নিয়ন্ত্রণ বা নিয়ন্ত্রণ প্রক্রিয়াগুলো প্রথম লাইনের সাথে সংযুক্ত। যদিও ব্যবস্থাপনা প্রথম এবং দ্বিতী উভয় লাইনে প্রতিনিধিত্ব করে, অভ্যন্তরীণ নিরীক্ষা কার্যক্রম তৃতীয় লাইনে একটি স্বাধীন ও

নিরপেক্ষ নিশ্চয়তা প্রদানকারী হিসেবে প্রদর্শিত হয়, যা বোর্ড/পরিচালনা পর্ষদের কাছে প্রতিবেদন প্রদান করে (**নীতিমালা ৮: বোর্ড দ্বারা তত্ত্বাবধান**)।

প্রয়োগযোগ্যতা, ঝুঁকি, এবং পেশাদার বিচার

যেসব বিষয়ে বিষয়ভিত্তিক প্রয়োজনীয়তা বিদ্যমান, সেসব বিষয়ে নিশ্চয়তা কার্য সম্পাদনের সম বা অন্য নিশ্চয়তা কার্যের মধ্যে বিষয়ভিত্তিক প্রয়োজনীয়তার দিকগুলো শনাক্ত হলে, বিষয়ভিত্তিক প্রয়োজনীয়তাগুলো অবশ্যই অনুসরণ করতে হবে।

স্ট্যান্ডার্ডসমূহের মতে, ঝুঁকি মূল্যায়ন প্রধান নিরীক্ষা নির্বাহীর পরিকল্পনার একটি গুরুত্বপূর্ণ অংশ। কোন নিশ্চয়তা কার্যগুলো অভ্যন্তরীণ নিরীক্ষা পরিকল্পনায় অন্তর্ভুক্ত করা হবে তা নির্ধারণের জন্য সংস্থার কৌশল, লক্ষ্য, এবং ঝুঁকিগুলো অন্তত বার্ষিক ভিত্তিতে মূল্যায়ন করা প্রয়োজন (**স্ট্যান্ডার্ড ৯.৪ অভ্যন্তরীণ নিরীক্ষা পরিকল্পনা**)। একক নিশ্চয়তা কার্য পরিকল্পনার সময়, সংশ্লিষ্ট ঝুঁকিগুলো মূল্যায়ন করতে অভ্যন্তরীণ নিরীক্ষকদের অবশ্যই ঝুঁকিগুলো বিবেচনা করতে হবে (**স্ট্যান্ডার্ড ১৩.২ কার্য ঝুঁকি মূল্যায়ন**)।

খন ঝুঁকি-ভিত্তিক অভ্যন্তরীণ নিরীক্ষা পরিকল্পনার প্রক্রিয়ায় একটি বিষয়ভিত্তিক প্রয়োজনীয়তার বিষয় শনাক্ত হয় এবং এটি নিরীক্ষা পরিকল্পনায় অন্তর্ভুক্ত হয়, তখন সংশ্লিষ্ট কার্যক্রমে বিষয়টি মূল্যায়নের জন্য বিষয়ভিত্তিক প্রয়োজনীয়তায় উল্লিখিত প্রয়োজনীয়তাগুলো অবশ্যই ব্যবহার করতে হবে। এছাড়া, যখন অভ্যন্তরীণ নিরীক্ষকরা কোনো কার্য সম্পাদন করেন (পরিকল্পনা অন্তর্ভুক্ত বা অন্তর্ভুক্ত নয়) এবং একটি বিষয়ভিত্তিক প্রয়োজনীয়তার উপাদানগুলো উদ্ভাসিত হয়, তখন কার্যক্রমের অংশ হিসেবে বিষয়ভিত্তিক প্রয়োজনীয়তার প্রাসঙ্গিকতা মূল্যায়ন করতে হবে। পরিশেষে, যদি এমন একটি কার্যক্রমের অনুরোধ করা হয় যা পরিকল্পনায় প্রাথমিকভাবে অন্তর্ভুক্ত ছিল না এবং তাতে বিষয়টি অন্তর্ভুক্ত থাকে, তবে বিষয়ভিত্তিক প্রয়োজনীয়তার প্রাসঙ্গিকতা অবশ্যই মূল্যায়ন করতে হবে।

পেশাদার বিচার বিষয়ভিত্তিক প্রয়োজনীয়তা প্রয়োগে একটি গুরুত্বপূর্ণ ভূমিকা পালন করে। ঝুঁকি মূল্যায়ন প্রধান নিরীক্ষা নির্বাহীদের সিদ্ধান্ত নিতে সহায়তা করে যে কোন কার্যক্রমগুলো অভ্যন্তরীণ নিরীক্ষা পরিকল্পনায় অন্তর্ভুক্ত করা হবে (**স্ট্যান্ডার্ড ৯.৪ অভ্যন্তরীণ নিরীক্ষা পরিকল্পনা**)। এছাড়া, অভ্যন্তরীণ নিরীক্ষকরা পেশাদার বিচার ব্যবহার করে নির্ধারণ করেন যে প্রতিটি কার্যক্রমে কোন দিকগুলি অন্তর্ভুক্ত হবে (**স্ট্যান্ডার্ড ১৩.৩ কার্যক্রমের উদ্দেশ্য এবং পরিসর, ১৩.৪ মূল্যায়ন মানদণ্ড, এবং ১৩.৬ কাজের প্রোগ্রাম**)। এপেনডিক্স এ "ব্যাবহারিক প্রয়োগের উদাহরণসমূহ" বর্ণনা করে কিভাবে অভ্যন্তরীণ নিরীক্ষকরা নির্ধারণ করেন যে বিষয়ভিত্তিক প্রয়োজনীয়তা প্রযোজ্য কিনা।

বিষয়ভিত্তিক প্রয়োজনীয়তাসমূহের প্রতিটি প্রয়োজনীয়তার প্রযোজ্যতা মূল্যায়ন করা হয়েছে এমন প্রমাণ সংরক্ষণ করতে হবে, যার মধ্যে যেকোনো প্রয়োজনীয়তা বাদ দেওয়ার কারণ ব্যাখ্যা করা হবে। বিষয়ভিত্তিক প্রয়োজনীয়তার সাথে সঙ্গতিপূর্ণতা **স্ট্যান্ডার্ড ১৪.৬ কার্যক্রম নথিপত্র** অনুযায়ী নিরীক্ষককে তার পেশাদার বিচার ব্যবহার করে নথিভুক্ত করতে হবে।

যদিও সাইবারসিকিউরিটি বিষয়ভিত্তিক প্রয়োজনীয়তা একটি নিয়ন্ত্রণ প্রক্রিয়ার মূলভিত্তি প্রদান করে, তবে যেসব সংস্থা সাইবার ঝুঁকিকে খুব বেশি বলে মূল্যায়ন করে, তাদের অতিরিক্ত দিকগুলো মূল্যায়ন করার প্রয়োজন হতে পারে।

যদি প্রধান নিরীক্ষা নির্বাহী মনে করেন যে অভ্যন্তরীণ নিরীক্ষা কার্যক্রম বিষয়ভিত্তিক প্রয়োজনীয়তার বিষয়ে নিরীক্ষা কার্য সম্পাদনের জন্য প্রয়োজনীয় জ্ঞান রাখে না, তবে কার্যক্রমটি আউটসোর্স করা হতে পারে (**স্ট্যান্ডার্ড ৩.১ দক্ষতা, ৭.২ প্রধান নিরীক্ষা নির্বাহীর যোগ্যতা, ১০.২ মানব সম্পদ ব্যবস্থাপনা**)। তারপরও, আউটসোর্সিং অভ্যন্তরীণ নিরীক্ষা কার্যক্রমকে বিষয়ভিত্তিক প্রয়োজনীয়তার সাথে সঙ্গতিপূর্ণতা বজায় রাখার দায়িত্ব থেকে মুক্ত করে না। প্রধান নিরীক্ষা নির্বাহী সঙ্গতিপূর্ণতা নিশ্চিত করার জন্য চূড়ান্ত দায়িত্ব বহন করেন। এছাড়া, যদি প্রধান নিরীক্ষা নির্বাহী মনে করেন যে অভ্যন্তরীণ নিরীক্ষা সম্পদ পর্যাপ্ত নয়, তবে প্রধান নিরীক্ষা নির্বাহী বোর্ডকে সম্পদের অভাবের প্রভাব এবং কিভাবে সম্পদের ঘাটতি মোকাবেলা করা হবে সে সম্পর্কে জানাতে হবে (**স্ট্যান্ডার্ড ৮.২ সম্পদ**)।

কার্যসম্পাদন, নথিপত্র, এবং প্রতিবেদন

বিষয়ভিত্তিক প্রয়োজনীয়তা প্রয়োগ করার সময়, অভ্যন্তরীণ নিরীক্ষকদেরও স্ট্যান্ডার্ডের সাথে সঙ্গতিপূর্ণ থাকতে হবে এবং **ডোমেইন V: অভ্যন্তরীণ নিরীক্ষা পরিষেবা পরিচালনা** এর সাথে সঙ্গতি রেখে তাদের কাজ সম্পাদন করতে হবে। ডোমেইন V-তে বর্ণিত স্ট্যান্ডার্ডগুলো কার্যক্রম পরিকল্পনা করা (**নীতিমালা ১৩: কার্যক্রম কার্যকরভাবে পরিকল্পনা করা**), কার্যক্রম পরিচালনা করা (**নীতিমালা ১৪: কার্যক্রমের কাজ পরিচালনা করা**), এবং কার্যক্রমের ফলাফল জানানো (**নীতিমালা ১৫: কার্যক্রমের ফলাফল জানানো এবং কর্মপরিকল্পনা পর্যবেক্ষণ করা**) সম্পর্কে নির্দেশনা প্রদান

বিষয়ভিত্তিক প্রয়োজনীয়তার পরিধি অভ্যন্তরীণ নিরীক্ষা পরিকল্পনা বা নিরীক্ষার কার্যপত্রে নিরীক্ষকদের পেশাদারী বিচার অনুযায়ী নথিভুক্ত করা যেতে পারে। এক বা একাধিক অভ্যন্তরীণ নিরীক্ষা কার্যক্রম প্রয়োজনীয়তাগুলি অন্তর্ভূক্ত করতে পারে। তদুপরি, সমস্ত প্রয়োজনীয়তা প্রযোজ্য নাও হতে পারে। বিষয়ভিত্তিক প্রয়োজনীয়তা প্রযোজ্য কিনা তা মূল্যায়নের প্রমাণ সংরক্ষণ করতে হবে, যার মধ্যে কোনো কিছু বাদ দেওয়ার যৌক্তিক কারণ ব্যাখ্যা অন্তর্ভুক্ত থাকবে।

অ্যাপেনডিক্স C-তে থাকা ঐচ্ছিক টুলটি রেফারেন্স হিসেবে এবং অভ্যন্তরীণ নিরীক্ষকরা যেসব কাজ সম্পাদন করেন তা নথিভুক্ত করার জন্য ব্যবহার করা যেতে পারে।

গুণগমানের নিশ্চয়তা

স্ট্যান্ডার্ড অনুযায়ী প্রধান নিরীক্ষা কর্মকর্তা (Chief Audit Executive) অভ্যন্তরীণ নিরীক্ষা কার্যক্রমের সমস্ত দিক অন্তর্ভুক্ত করে একটি গুণগত নিশ্চয়তা ও উন্নয়ন কর্মসূচি (Quality Assurance and Improvement Program) প্রণয়ন, প্রয়োগ এবং বজায় রাখতে বাধ্য (স্ট্যান্ডার্ড 8.3 গুণমান)। ফলাফল বোর্ড এবং ঊর্ধ্বতন ব্যবস্থাপনাকে জানাতে হবে। এই যোগাযোগে অভ্যন্তরীণ নিরীক্ষা কার্যক্রমের স্ট্যান্ডার্ডের সাথে সঙ্গতিপূর্ণতা এবং কার্যক্রমের লক্ষ্য অর্জনের বিষয়টি রিপোর্ট করতে হবে।

বিষয়ভিত্তিক প্রয়োজনীয়তার সাথে সঙ্গতিপূর্ণতা গুণমানের মূল্যায়নে পর্যালোচনা করা হবে। একটি গুণমানের পর্যালোচনার জন্য প্রস্তুত হতে অভ্যন্তরীণ নিরীক্ষকরা অ্যাপেনডিক্স C-এ প্রদত্ত টুল ব্যবহার করতে পারেন।

সাইবার নিরাপত্তা

সাইবার নিরাপত্তা একটি বিস্তৃত বিষয়, যা যেকোনো প্রতিষ্ঠানের প্রযুক্তিগত দিকগুলোর সাথে সম্পর্কিত। তথ্য প্রযুক্তির পাশাপাশি সাইবার নিরাপত্তা সাধারণত ব্যবসার প্রক্রিয়ার অংশ, যা অভ্যন্তরীণ নিরীক্ষকদের জন্য সাইবার-সম্পর্কিত ঝুঁকিগুলো মূল্যায়ন করা প্রয়োজনীয় করে তোলে, নিরীক্ষা পরিকল্পনা, পরিধি নির্ধারণ, এবং আশ্বাস প্রদানমূলক কাজ সম্পাদনের সময়।

মার্কিন যুক্তরাষ্ট্রের বাণিজ্য বিভাগের অংশ ন্যাশনাল ইনস্টিটিউট অফ স্ট্যান্ডার্ডস অ্যান্ড টেকনোলজি (NIST) সাইবার নিরাপত্তাকে সহজভাবে সংজ্ঞায়িত করেছে: “সাইবার আক্রমণ থেকে সাইবারস্পেস ব্যবহারের সুরক্ষা বা প্রতিরক্ষা করার সক্ষমতা।”

সাইবারসিকিউরিটি বিষয়ভিত্তিক প্রয়োজনীয়তা মূলত সেই বাইরের সীমানার উপর মনোযোগ দেয়, যা প্রতিষ্ঠানের ঝুঁকি হ্রাস করার জন্য অননুমোদিত ব্যবহারকারী এবং ক্ষতিকারক সাইবার হুমকি থেকে সুরক্ষিত করা হয়।

সাইবার নিরাপত্তা বৃহত্তর তথ্য নিরাপত্তার একটি অংশ, যা NIST এর মতে সংজ্ঞায়িত: “তথ্য এবং তথ্য ব্যবস্থা অননুমোদিত প্রবেশ, ব্যবহার, প্রকাশ, বিঘ্ন, পরিবর্তন বা ধ্বংস থেকে রক্ষা করার জন্য, যাতে গোপনীয়তা, অখণ্ডতা এবং প্রাপ্যতা নিশ্চিত করা যায়।”

সাইবারসিকিউরিটি বিষয়ভিত্তিক প্রয়োজনীয়তাগুলোতে অন্তর্ভুক্ত:

- শাসন (Governance): সুস্পষ্টভাবে সংজ্ঞায়িত মৌলিক সাইবারসিকিউরিটির উদ্দেশ্য এবং কৌশল, যা প্রতিষ্ঠানের লক্ষ্য, নীতিমালা, এবং পদ্ধতিগুলোকে সমর্থন করে।
- ঝুঁকি ব্যবস্থাপনা (Risk Management): সাইবার হুমকি চিহ্নিত, বিশ্লেষণ, পরিচালনা এবং পর্যবেক্ষণ করার জন্য প্রক্রিয়া, যার মধ্যে সাইবার ঝুঁকি দ্রুত উত্থাপন করার একটি পদ্ধতিও অন্তর্ভুক্ত।
- নিয়ন্ত্রণ (Controls): সাইবার ঝুঁকি কমানোর জন্য ব্যবস্থাপনা কর্তৃক প্রতিষ্ঠিত এবং পর্যায়ক্রমে মূল্যায়নকৃত নিয়ন্ত্রণ প্রক্রিয়াগুলো।

বিবেচ্য বিষয়সমূহ

অভ্যন্তরীন নিরীক্ষকরা সাইবারসিকিউরিটির বিষয়ভিত্তিক প্রয়োজনীয়তাগুলোর মূল্যায়নে সাহায্য করার জন্য নিম্নলিখিত বিবেচ্য বিষয়গুলো ব্যবহার করতে পারেন। এই বিবেচ্য বিষয়গুলো উদাহরণস্বরূপ উপস্থাপিত হলেও তা বাধ্যতামূলক নয়। মূল্যায়নের ক্ষেত্রে কী অন্তর্ভুক্ত করা হবে তা নির্ধারণ করতে ইন্টারনাল অডিটরদের পেশাদার বিচারের ওপর নির্ভর করা উচিত।

সুশাসনের বিবেচনা

সাইবারসিকিউরিটির উদ্দেশ্যগুলির জন্য শাসন প্রক্রিয়া কীভাবে প্রয়োগ হচ্ছে তা মূল্যায়ন করতে, অভ্যন্তরীন নিরীক্ষকরা নিম্নলিখিত বিষয়গুলো পর্যালোচনা করতে পারেনঃ

ক. সাইবারসিকিউরিটির কৌশলগত পরিকল্পনা এবং উদ্দেশ্যসমূহের আনুষ্ঠানিক, নথিভুক্ত রূপ, ার মধ্যে পর্ষদ কর্তৃক (সাধারণত ত্রৈমাসিক ভিত্তিতে) সাইবারসিকিউরিটি হালনাগাদ পর্যালোচনার প্রমাণ থাকতে পারে, যা তথ্য নিরাপত্তা বিভাগের প্রধান, যেমন প্রধান তথ্য নিরাপত্তা কর্মকর্তা (CISO) দ্বারা সরবরাহ করা হয়। প্রমাণের মধ্যে অন্তর্ভুক্ত থাকতে পারেঃ

- কৌশলগত উদ্দেশ্যগুলির অর্জন এর পর্যবেক্ষণ।
- সাইবারসিকিউরিটির লক্ষ্য এবং উদ্দেশ্য সমর্থনে বাজেটের প্রয়োজনীয়তা।
- ঝুঁকি এবং অভ্যন্তরীণ নিয়ন্ত্রণে মনোযোগ, যা প্রতিকারের অগ্রগতি অন্তর্ভুক্ত করে।
- সফলতা পরিমাপ করতে মূল কার্যক্ষমতা সূচক (KPI)।
- সাইবারসিকিউরিটি কর্মীদের নিয়োগ, প্রশিক্ষণ এবং মান উন্নয়ন করার জন্য প্রয়োজনী মানব সম্পদ।

খ. সাইবারসিকিউরিটি প্রক্রিয়া পরিচালনা করতে ব্যবহৃত নীতিমালা, প্রক্রিয়া এবং অন্যান্য প্রাসঙ্গিক নথিভুক্তিকরন, যার মধ্যে অন্তর্ভুক্ত থাকতে পারেঃ

- নীতিমালা যা অন্তত বার্ষিক ভিত্তিতে পর্যালোচনা এবং আপডেট করা হয়। উদীয়মান সাইবার ঝুঁকি এই পর্যালোচনা এবং হালনাগাদগুলি আরও প্রায়ই করার প্রয়োজন হতে পারে।
- একটি প্রক্রিয়া যা নির্ধারণ করে (নীতিমালা এবং প্রক্রিয়া সাইবারসিকিউরিটি কার্যক্রমগুলিকে সমর্থন করতে যথেষ্ট কিনা।
- সাইবারসিকিউরিটি প্রক্রিয়া এবং অভ্যন্তরীণ নিয়ন্ত্রণ শক্তিশালী করতে ব্যাপকভাবে গৃহীত কাঠামো (NIST, COBIT, এবং অন্যান্য)।

গ. সাইবারসিকিউরিটি উদ্দেশ্যগুলির অর্জনকে সমর্থনকারী ভূমিকা এবং দায়িত্বসমূহ, যার মধ্যে একটি কাঠামো অন্তর্ভুক্ত থাকে যা নিশ্চিত করে যে সাইবারসিকিউরিটি ফাংশন একটি স্তরে রিপোর্ট করছে যা সংগঠনের সমর্থন অর্জন করার জন্য যথেষ্ট দৃশ্যমানতা রয়েছে।

- সাইবারসিকিউরিটির ভূমিকা পালনকারী কর্মীদের জ্ঞান, দক্ষতা এবং ক্ষমতা পর্যালোচনা করার একটি প্রক্রিয়া।

ঘ. প্রাসঙ্গিক অংশীজনদের সাথে সম্পৃক্ততার প্রমাণ (যেমন, সিনিয়র ম্যানেজমেন্ট, অপারেশন, ঝুঁকি ব্যবস্থাপনা, মানব সম্পদ, আইন, অনুবর্তিতা, কৌশলগত ভেন্ডর, এবং অন্যান্য), যার মধ্যে বিদ্যমান এবং উদীয়মান সাইবার ঝুঁকি এবং পরিচিত সম্ভাব্য দুর্বলতা সম্পর্কে যোগাযোগ অন্তর্ভুক্ত রয়েছে। যোগাযোগের প্রমাণের মধ্যে থাকতে পারে সভার কার্যবিবরনী, প্রতিবেদন, বা ইমেল।

ঝুঁকি ব্যবস্থাপনা বিবেচনা

ঝুঁকি ব্যবস্থাপনা প্রক্রিয়া কিভাবে সাইবার নিরাপত্তার উদ্দেশ্যে প্রয়োগ করা হচ্ছে তা মূল্যায়ন করতে, অভ্যন্তরীণ নিরীক্ষকরা পর্যালোচনা করতে পারেনঃ

ক. কিভাবে সংস্থা সাইবার নিরাপত্তা ঝুঁকি মূল্যায়ন এবং পরিচালনা করে, যার মধ্যে রয়েছে কিভাবে হুমকি এবং দুর্বলতাগুলিঃ

- প্রথমে চিহ্নিত এবং রিপোর্ট করা হয়।
- সংগঠনের উদ্দেশ্য পূরণের ঝুঁকি মূল্যায়ন করতে বিশ্লেষণ করা হয়।
- ঝুঁকি কমাতে পরিকল্পনা সহ অগ্রগতি গ্রহণ করা হয়।
- ঝুঁকি পর্যবেক্ষণ করা হয়, যার মধ্যে একটি পরিকল্পনা রয়েছে যা হুমকি পুরোপুরি সমাধান না হওয়া পর্যন্ত প্রতিবেদন করা হয়।

খ. কিভাবে সংস্থা সাইবার নিরাপত্তা ঝুঁকি ব্যবস্থাপনা বিষয়ে বিভিন্ন কার্যকরী বিভাগের কাছ থেকে সময়সূচী অনুযায়ী ইনপুট নেয়, যেমন তথ্য প্রযুক্তি, এন্টারপ্রাইজ ঝুঁকি ব্যবস্থাপনা, মানবসম্পদ, আইন, সম্মতি, অপারেশন, হিসাবরক্ষণ এবং অর্থনীতি। একটি আন্তঃবিভাগীয় সাইবার নিরাপত্তা দল বা আইটি স্টিয়ারিং কমিটি তথ্য সংগ্রহের জন্য ব্যবহার হতে পারে।

গ. কিভাবে সংস্থা সাইবার নিরাপত্তা ঝুঁকি ব্যবস্থাপনার জন্য একটি ব্যক্তি বা দলের কাছে দায়বদ্ধতা এবং দায়িত্ব নির্ধারণ করেছে।

- যে ব্যক্তি(রা) দায়ী, তাদের উচিত সাইবার নিরাপত্তা ঝুঁকির হালনাগাদ নিয়মিত (ত্রৈমাসিক, মাসিক বা প্রয়োজন অনুসারে) প্রতিষ্ঠানের মধ্যে যোগাযোগ করা এবং ঝুঁকি প্রশমন কৌশলগুলির জন্য প্রয়োজনীয় সম্পদ নির্ধারণ করা।

ঘ. সাইবার নিরাপত্তা ঝুঁকির জন্য উত্তরণের প্রক্রিয়াগুলি, যার মধ্যে কীভাবে ঝুঁকি বা হুমকির স্তর মূল্যায়ন, নির্ধারণ এবং অগ্রাধিকার দেওয়া হয় তা অন্তর্ভুক্ত থাকবে। পর্যালোচনার মধ্যে থাকতে পারেঃ

- সংস্থার সংজ্ঞায়িত ঝুঁকির স্তর – যেমন উচ্চ, মাঝারি, এবং কম – প্রতিটি ঝুঁকি স্তরের বিস্তারিত ব্যাখ্যা এবং প্রতিটি ঝুঁকি শ্রেণীর জন্য উত্তরণের পদ্ধতি।
- বর্তমানে চিহ্নিত সাইবার নিরাপত্তা ঝুঁকির তালিকা এবং প্রতিটি ঝুঁকি ঘটনা প্রশমনের অবস্থান।
- প্রযোজ্য আইন, প্রবিধান এবং সম্মতি প্রয়োজনীয়তা।
- আর্থিক এবং অ-আর্থিক ঝুঁকির (যেমন, সুনাম) প্রভাব।

ঙ. কিভাবে সাইবার নিরাপত্তা ঝুঁকির সংক্রান্ত তথ্য ব্যবস্থাপনা এবং কর্মচারীদের কাছে যোগাযোগ করা হয়, যার মধ্যে রয়েছেঃ

- নিয়মিত (কমপক্ষে বার্ষিক) কর্মচারীদের সাইবার নিরাপত্তা প্রশিক্ষণ, যেমন অঘোষিত, সিমুলেটেড ফিশিং ক্যাম্পেইনগুলি যাতে প্রতিষ্ঠানের সচেতনতা পরীক্ষা এবং ট্র্যাক করা হয়।
- বর্তমান সাইবার নিরাপত্তা সমস্যা সমাধানের হালনাগাদ, প্রত্যাশিত সম্পন্নের তারিখ সহ।
- অপ্রতিপাদন মনিটরিং, যার মধ্যে পর্ষদ এবং শীর্ষ ব্যবস্থাপনা বরাবর হালনাগাদ করা হয়।
- ঝুঁকি গ্রহণ ক্ষমতা এবং ঝুঁকি সহ্য ক্ষমতার পরিবর্তনের সাথে হুমকি পুনর্মূল্যায়ন।

চ. প্রতিষ্ঠান যে প্রক্রিয়াগুলি বাস্তবায়ন করেছে, সাইবার নিরাপত্তা ঘটনা প্রতিক্রিয়া এবং পুনরুদ্ধার সম্পর্কিত, যার মধ্যে রয়েছেঃ

- একটি দলিলবদ্ধ পরিকল্পনা যা সংস্থার কার্যক্রম পরিবর্তিত হওয়ার সাথে সাথে পর্যালোচনা এবং আপডেট করা হয়। পরিকল্পনায় অন্তর্ভুক্ত থাকতে হবেঃ • কিভাবে ঘটনা চিহ্নিত এবং রিপোর্ট করা হয়। • কিভাবে ঘটনা নিয়ন্ত্রণ করা হয় যাতে অতিরিক্ত ক্ষতি প্রতিরোধ করা যায়। • কিভাবে সংস্থা পুনরুদ্ধার করবে এবং কার্যক্রম পুনরায় চালু করবে। • কিভাবে ঘটনা বিশ্লেষণ করা হবে যাতে শিক্ষা (learning) চিহ্নিত করা যায় এবং ভবিষ্যতে অনুরূপ ঘটনা প্রতিরোধ করা যায়।
- নিয়মিত (কমপক্ষে বার্ষিক) পরীক্ষা (টেবিলটপ অনুশীলন) এবং শীর্ষ ব্যবস্থাপনা ও প্রাসঙ্গিক অংশীদারদের ফলাফল রিপোর্ট করা। পরীক্ষার ফলস্বরূপ কর্মপরিকল্পনা হতে পারে।

নিয়ন্ত্রণ প্রক্রিয়া বিবেচনা

সাইবার নিরাপত্তা উদ্দেশ্যগুলির উপর নিয়ন্ত্রণ প্রক্রিয়া কিভাবে প্রয়োগ করা হচ্ছে তা মূল্যায়ন করার জন্য, অভ্যন্তরীণ নিরীক্ষকরা পর্যালোচনা করতে পারেনঃ

ক. একটি কার্যকর সাইবার নিরাপত্তা অভ্যন্তরীণ নিয়ন্ত্রণ পরিবেশ তৈরি করার জন্য ব্যবস্থাপনার দৃষ্টিভঙ্গি, যার মধ্যে অন্তর্ভুক্তঃ

- অভ্যন্তরীণ নিয়ন্ত্রণগুলি মূল্যায়ন এবং প্রয়োগ করা যা উচ্চ ঝুঁকি হ্রাস করতে এবং সংবেদনশীল, গুরুত্বপূর্ণ, ব্যক্তিগত বা গোপনীয় তথ্য সুরক্ষিত করতে সহায়ক, যা প্রাতিষ্ঠানিক ঝুঁকি মূল্যায়ন প্রক্রিয়া দ্বারা প্রাপ্ত।
- গুরুত্বপূর্ণ সাইবার নিরাপত্তা নিয়ন্ত্রণগুলি বজায় রাখার জন্য প্রয়োজনীয় সম্পদের চাহিদা নির্ধারণ করা।
- নিয়ন্ত্রণ পরিবেশের অংশ হিসেবে বহিঃসেবা প্রদানকারীর ভিত্তিতে নিয়ন্ত্রণগুলি বিবেচনা করা, যার মধ্যে ব্যবসায়িক সম্পর্ক শুরু করার আগে এবং সম্পর্কের সময়কালের মধ্যে বহিঃসেবা প্রদানকারীর সেবা সংস্থা নিয়ন্ত্রণ (SOC) রিপোর্ট পর্যালোচনা করা অন্তর্ভুক্ত।
- সাইবার নিরাপত্তা নিয়ন্ত্রণগুলি এমনভাবে কাজ করছে কি না তা পরীক্ষা করার জন্য নিয়মিত পরীক্ষণ, যা ঝুঁকি হ্রাস করতে এবং সাইবার নিরাপত্তা উদ্দেশ্যগুলি অর্জনে সহায়ক।
- অভ্যন্তরীণ নিয়ন্ত্রণের ঘাটতি সমাধান বা অভ্যন্তরীণ নিরীক্ষণ কার্যক্রম বা অন্যান্য আশ্বাস প্রদানকারীদের দ্বারা করা মূল্যায়ন থেকে প্রাপ্ত ফলাফলগুলি মোকাবেলা করার প্রক্রিয়া (যেমন, পেনিট্রেশন টেস্টিং) ।

খ. সাইবার নিরাপত্তা পেশাজীবীদের নিয়োগ এবং প্রশিক্ষণের জন্য সংস্থার প্রতিভা ব্যবস্থাপনা প্রক্রিয়া, যার মধ্যে সংস্থা কীভাবে সাইবার নিরাপত্তা পেশাজীবীদের দক্ষতা বৃদ্ধি করার সুযোগ চিহ্নিত করে, যা প্রযুক্তিগত জ্ঞান সমর্থন করে এবং উদীয়মান বিষয়গুলির প্রতি সংস্থার সচেতনতা উন্নত করে।

- উদাহরণস্বরূপ, প্রশিক্ষণে অংশগ্রহণ, জ্ঞান ভাগাভাগি গ্রুপের সাথে সম্পৃক্ততা, এবং অব্যাহত পেশাগত শিক্ষা যা সাইবার সম্পর্কিত সার্টিফিকেশন অর্জন অন্তর্ভুক্ত।

গ. সাইবার নিরাপত্তা সম্পর্কিত উদীয়মান হুমকি এবং দুর্বলতাগুলি সনাক্ত, অগ্রাধিকার প্রদান, পর্যবেক্ষণ এবং প্রতিবেদন করার জন্য ব্যবস্থাপনার প্রক্রিয়া যা দৈনিক কার্যক্রমে মনোযোগ কেন্দ্রীভূত করে। পর্যালোচনায় অন্তর্ভুক্ত থাকতে পারে যে প্রক্রিয়াগুলি কৃত্রিম বুদ্ধিমত্তার ব্যবহারের মতো নতুন বা উদীয়মান প্রযুক্তি সম্পর্কিত হুমকি এবং দুর্বলতাগুলি মূল্যায়ন করার জন্য প্রতিষ্ঠিত হয়েছে।

ঘ. ব্যবস্থাপনার প্রক্রিয়া এবং নিয়ন্ত্রণগুলি যা আইটি সম্পদগুলির জীবনচক্রের মাধ্যমে ব্যবস্থাপনা এবং সুরক্ষা করার জন্য প্রতিষ্ঠিত হয়েছে, যার মধ্যে হার্ডওয়্যার, সফটওয়্যার এবং বহিঃসংস্থার সেবা নির্বাচন, ব্যবহার, রক্ষণাবেক্ষণ এবং ডিকমিশনিং অন্তর্ভুক্ত। হার্ডওয়্যারের মধ্যে সার্ভার, নেটওয়ার্কিং সরঞ্জাম (যেমন রাউটার বা ফায়ারওয়াল), ডেস্কটপ, ল্যাপটপ, সেল ফোন, ট্যাবলেট এবং পেরিফেরাল যন্ত্রগুলো অন্তর্ভুক্ত। সফটওয়্যারের মধ্যে অপারেটিং সিস্টেম (যেমন উইন্ডোজ), এন্টারপ্রাইজ রিসোর্স প্ল্যানিং সফটওয়্যার, অ্যাপ্লিকেশন, অ্যান্টিভাইরাস প্রোগ্রাম এবং অন্যান্যগুলি অন্তর্ভুক্ত। হার্ডওয়্যার এবং সফটওয়্যার সম্পর্কিত বিবেচনায় অন্তর্ভুক্ত থাকতে পারেঃ

- সংস্থার এনক্রিপশন, অ্যান্টিভাইরাস সফটওয়্যার, মোবাইল ডিভাইস ম্যানেজমেন্ট, জটিল পাসওয়ার্ডের প্রয়োজনীয়তা, ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN)/জিরো ট্রাস্ট নেটওয়ার্কিং (ZTN) প্রমাণীকরণের জন্য এবং ফার্মওয়্যারের নিয়মিত আপডেট ব্যবহারের কৌশল।
- একটি সম্পদ ব্যবস্থাপনা প্রক্রিয়া যা নিশ্চিত করে যে কোম্পানির-প্রদত্ত হার্ডওয়্যার ইস্যু করার সময় উপযুক্ত সিকিউরিটি কনফিগারেশন রয়েছে এবং সম্পদ অবসরপ্রাপ্ত হলে সঠিকভাবে নিষ্পত্তি করা হয়।
- ডাটাবেস-সম্পর্কিত নিয়ন্ত্রণ যা ব্যবহারকারী এবং প্রশাসকের প্রবেশাধিকার সীমিত করা, এনক্রিপশনের ব্যবহার নিশ্চিত করা, ডাটাবেস ব্যাকআপ এবং পরীক্ষণ, এবং শক্তিশালী নেটওয়ার্ক সিকিউরিটি নিয়ন্ত্রণের উপস্থিতি অন্তর্ভুক্ত।

- সিস্টেম ডেভেলপমেন্ট লাইফ সাইকেল (SDLC) এ সাইবার নিরাপত্তা হুমকি বা দুর্বলতাগুলি কিভাবে বিবেচিত হয়।
- ডেভেলপমেন্ট, সিকিউরিটি এবং অপারেশন (DevSecOps) দ্বারা ব্যবহৃত কৌশল যা নিশ্চিত করে যে সফটওয়্যার ডেভেলপমেন্ট প্রক্রিয়া সাইবার নিরাপত্তাকে অন্তর্ভুক্ত করে এবং দুর্বলতাগুলি পূর্বাভাসে চিহ্নিত করে।

ঙ. সাইবার নিরাপত্তা শক্তিশালী করতে ব্যবহৃত প্রক্রিয়া, যার মধ্যে অন্তর্ভুক্তঃ

- সাইবার নিরাপত্তা ঝুঁকি কমাতে সিকিউরিটি সেটিংস কনফিগারেশন।
- মোবাইল ডিভাইস প্রশাসন (ইমেইল এবং অ্যাপ্লিকেশন ব্যবহারের সহিত) কনফিগার করা াতে সাইবার নিরাপত্তা ঝুঁকি কমানো যায় এবং যদি একটি ব্যবহারকারীর ডিভাইস ক্ষতিগ্রস্ত হয় তবে এটি দূর থেকে পরিচালনা করা যায়।
- তথ্যের এর জন্য এনক্রিপশন ব্যবহার "অবস্থিত", যেমন হার্ড ড্রাইভে সংরক্ষিত তথ্য, অথবা ডেটা "পরিবহনরত" এর জন্য, যেমন ইমেইল এনক্রিপ্ট করা।
- সর্বশেষ সিকিউরিটি রিলিজের সাথে সার্ভার বা সফটওয়্যার (যেমন অপারেটিং সিস্টেম) প্যাচ করা।
- ব্যবহারকারী প্রবেশ ব্যবস্থাপনা, যেমন মাল্টিফ্যাক্টর প্রমাণীকরণ (MFA) এবং জটিল পাসওয়ার্ড সহ অনন্য ইউজার আইডি ব্যবহার যা সময়ে সময়ে মেয়াদ উত্তীর্ণ হয়।
- পর্যবেক্ষণ নিয়ন্ত্রণ ব্যবস্থা যা নির্ধারণ করে যে প্রপ্যতা এবং সম্পদ ব্যবহারের কার্যকারিতা থাযথভাবে কাজ করছে কিনা, যা সাইবার নিরাপত্তা সমস্যাগুলির পর্যালোচনা এবং বিশ্লেষণ করার সুযোগ দেয় । কর্মক্ষমতাকে বিপদে ফেলতে পারে।
- সাইবার নিরাপত্তা SDLC তে একীভূত করা যাতে সফটওয়্যার উৎপাদনে স্থানান্তরের আগে সাইবার নিরাপত্তার দুর্বলতাগুলি চিহ্নিত এবং সমাধান করা যায়।

চ. নেটওয়ার্ক-সম্পর্কিত নিয়ন্ত্রণগুলি যা সংস্থার পরিধি সুরক্ষিত করে, যার মধ্যে সংস্থা কীভাবে ব্যবহার করেঃ

- নেটওয়ার্ক বিভাজন।
- ফায়ারওয়াল।
- ব্যবহারকারী-প্রবেশ নিয়ন্ত্রণ।

- বাহ্যিক এবং অভ্যন্তরীণ সংযোগের উপর সীমাবদ্ধতা।
- ইন্টারনেট অব থিংস (IoT) সম্পর্কিত নিয়ন্ত্রণ যা আন্তঃসংযুক্ত নেটওয়ার্কের জন্য ব্যবহৃত হয়।
- অনুপ্রবেশ সনাক্তকরণ/প্রতিরোধ ব্যবস্থা যা সাইবার নিরাপত্তা আক্রমণ প্রতিরোধ, সনাক্ত এবং পুনরুদ্ধার করতে সহায়ক।

ছ. এন্ড-পয়েন্ট যোগাযোগ সুরক্ষা নিয়ন্ত্রণগুলি যা পরিষেবাগুলির জন্য প্রযোজ্য, যেমন ইমেইল, ইন্টারনেট ব্রাউজার, ভিডিও কনফারেন্সিং, মেসেজিং (Zoom, MS Teams এবং অন্যান্য), সোশ্যাল মিডিয়া, ক্লাউড এবং ফাইল শেয়ারিং প্রোটোকল। নিয়ন্ত্রণগুলির মধ্যে অন্তর্ভুক্ত থাকতে পারে কিছু ফাইল এক্সটেনশনের ব্যবহার সীমাবদ্ধ করা (যেমন .exe ফাইলগুলি) এবং ফাইল শেয়ারিংয়ের জন্য মাল্টিফ্যাক্টর প্রমাণীকরণ।

অ্যাপেন্ডিক্স A ব্যবহারিক প্রয়োগের উদাহরণসমূহ

নিম্নলিখিত উদাহরণগুলি সাইবার নিরাপত্তা বিষয়ভিত্তিক প্রয়োজনীয়তা প্রযোজ্য এমন পরিস্থিতি বর্ণনা করেঃ

উদাহরণ ১: সাইবার নিরাপত্তা একটি অভ্যন্তরীণ নিরীক্ষা পরিকল্পনায় অন্তর্ভুক্ত অভ্যন্তরীণ নিরীক্ষা কার্যক্রমের জন্য চিহ্নিত করা হয়েছে।

যখন অভ্যন্তরীণ নিরীক্ষা কার্যক্রম তার ঝুঁকি ভিত্তিক পরিকল্পনা প্রক্রিয়া সম্পন্ন করে এবং অভ্যন্তরীণ নিরীক্ষা পরিকল্পনায় সাইবার নিরাপত্তার উপর একটি বা একাধিক কার্যক্রম অন্তর্ভুক্ত করে, তখন এই ধরনের নিয়োগ পরিচালনা করার সময় বিষয়ভিত্তিক প্রয়োজনীয়তা প্রযোজ্য। এক বা একাধিক নিয়োগে প্রয়োজনীয়তা অন্তর্ভুক্ত করার মাধ্যমে সম্মতি অর্জন করা যেতে পারে।

সাইবার নিরাপত্তা একটি বিস্তৃত বিষয়, এবং টপিক্যাল রিকোয়ারমেন্টের সব প্রয়োজনীয়তা প্রতিটি কার্যক্রমের প্রযোজ্য নাও হতে পারে। যখন অভ্যন্তরীণ নিরীক্ষকরা পেশাদার সিদ্ধান্ত প্রয়োগ করেন এবং নির্ধারণ করেন যে সাইবার নিরাপত্তা টপিক্যাল রিকোয়ারমেন্টের এক বা একাধিক প্রয়োজনীয়তা প্রযোজ্য নয় এবং নিয়োগ থেকে বাদ দেওয়া উচিত, তখন অভ্যন্তরীণ নিরীক্ষকদের সেই প্রয়োজনীয়তাগুলি বাদ দেওয়ার যুক্তি ডকুমেন্ট করে সংরক্ষণ করতে হবে। উদাহরণস্বরূপ, কিছু প্রয়োজনীয়তা বাদ দেওয়ার যুক্তি হতে পারে যে অভ্যন্তরীণ নিরীক্ষা কার্যক্রম পর্যায়ক্রমিক ভিত্তিতে বিভিন্ন সাইবার নিরাপত্তা কার্যক্রম পরিচালনা করে বা তারা নির্ধারণ করেছে যে কার্যক্রমের ঝুঁকির গুরুত্ব কম।

উদাহরণ ২: একটি নিরীক্ষা কার্যক্রমের সময় সাইবার নিরাপত্তার ঝুঁকি চিহ্নিত করা হয়েছে I সাইবার নিরাপত্তার উপর আলোকপাত করে না।

অভ্যন্তরীণ নিরীক্ষকরা এমন একটি প্রক্রিয়া মূল্যায়ন করার সময় সাইবার নিরাপত্তার ঝুঁকি চিহ্নিত করতে পারেন যা সরাসরি সাইবার নিরাপত্তার সাথে সম্পর্কিত নয়। উদাহরণস্বরূপ, অভ্যন্তরীণ নিরীক্ষকরা একটি নিরীক্ষা কার্যক্রমের পাওনাদারের হিসাব প্রক্রিয়া মূল্যায়ন করতে পারেন যা সাইবার নিরাপত্তার উপর আলোকপাত করে না এবং তারা কার্যক্রম পরিকল্পনা করার সময় সাইবার নিরাপত্তার ঝুঁকি সীমানার মধ্যে চিহ্নিত করেন না। তবে, প্রথমিক কার্যক্রম সম্পন্ন করার পরে, অভ্যন্তরীণ নিরীক্ষকরা সিদ্ধান্ত নেন যে এমন ঝুঁকিগুলি কর্যক্রমের পরিধিতে থাকা উচিত;

উদাহরণস্বরূপ, তারা ওয়েব-ভিত্তিক প্রাথমিক ক্রয় অর্ডার অনুরোধ জমাদানের সাথে সম্পর্কিত সাইবার নিরাপত্তা ঝুঁকি চিহ্নিত করেন (স্ট্যান্ডার্ড ১৩.২ কার্যক্রম ঝুঁকি মূল্যায়ন)।

যখন প্রাসঙ্গিক ঝুঁকিগুলি চিহ্নিত হয়ে ায়, অভ্যন্তরীণ নিরীক্ষকদের সাইবার নিরাপত্তা বিষয়ভিত্তিক প্রয়োজনীয়তা পর্যালোচনা করতে হবে এবং কোন প্রয়োজনীয়তাগুলি প্রযোজ্য তা নির্ধারণ করতে হবে। এই উদাহরণে, তারা সাইবার নিরাপত্তা শাসন প্রক্রিয়া বা সাইবার নিরাপত্তা ঝুঁকি ব্যবস্থাপনা প্রক্রিয়া বাদ দিতে পারেন। তারা কার্যপত্রে অন্যান্য সাইবার নিরাপত্তা বিষয়ভিত্তিক প্রয়োজনীয়তার প্রযোজ্যতা বাদ দেওয়ার যুক্তি ডকুমেন্ট করে সংরক্ষণ করবেন।

উদাহরণ ৩: একটি সাইবার নিরাপত্তা কার্যক্রম যা মূলত অভ্যন্তরীণ নিরীক্ষা পরিকল্পনায় অন্তর্ভুক্ত ছিল না, অনুরোধ করা হয়েছে।

শেয়ারহোল্ডাররা যেমন পর্ষদ, ব্যবস্থাপনা বা একটি নিয়ন্ত্রক সংস্থা অভ্যন্তরীণ নিরীক্ষকদের মূল নিরীক্ষা পরিকল্পনার বাইরে সাইবার নিরাপত্তা মূল্যায়ন করতে অনুরোধ করতে পারে। উদাহরণস্বরূপ, যখন সংস্থাগুলি সাইবার আক্রমণের লক্ষ্য হয়, পর্ষদ সাইবার নিরাপত্তা নিয়ন্ত্রণ মূল্যায়ন করার জন্য একটি অভ্যন্তরীণ নিরীক্ষা নিয়োগের অনুরোধ করতে পারে। এই ক্ষেত্রে বিষয়ভিত্তিক প্রয়োজনীয়তার প্রযোজ্য প্রয়োজনীয়তাগুলি মূল্যায়ন করতে হবে এবং কোনও বাদ দেওয়া প্রয়োজনীয়তা ডকুমেন্ট করতে হবে।

অ্যাপেন্ডিক্স B ফ্রেমওয়ার্কের সাথে ম্যাপিং

সংস্থার তার নিজস্ব সাইবার নিরাপত্তার প্রয়াস থাকতে পারে, যা ঝুঁকি ব্যবস্থাপনা এবং শাসন কাঠামো ব্যবহার করে যেমন COBIT বা NIST। অভ্যন্তরীণ নিরীক্ষকরা হয়তো ইতিমধ্যেই এই কাঠামোগুলির ভিত্তিতে নিরীক্ষা কার্যক্রম এবং পরীক্ষণ প্রক্রিয়া তৈরি করেছেন। অভ্যন্তরীণ নিরীক্ষকদের তাদের উদ্দেশ্যপ্রণোদিত সাইবার নিরাপত্তা নিয়ন্ত্রণ পরীক্ষণকে বিষয়ভিত্তিক প্রয়োজনীয়তার সাথে সঙ্গতিপূর্ণ করতে হবে যাতে পর্যাপ্ত পরিধি নিশ্চিত করা যায়। নিচের চিত্রে সাইবার নিরাপত্তা বিষয়ভিত্তিক প্রয়োজনীয়তাকে তিনটি প্রচলিত কাঠামোর সাথে ম্যাপ করা হয়েছেঃ NIST সাইবার নিরাপত্তা ফ্রেমওয়ার্ক ২.০, COBIT ২০১৯, এবং NIST ৮০০-৫৩। এই কাঠামোগুলিকে ম্যাপ করা হয়েছে কারণ এগুলি সহজে এবং বিনামূল্যে পাওয়া যায়।

	কাঠামোর তথ্যসূত্র		
শাসন প্রয়োজনীয়তা	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
ক. একটি আনুষ্ঠানিক সাইবার নিরাপত্তা কৌশল এবং লক্ষ্য স্থাপন করা হয় এবং সময়ে সময়ে আপডেট করা হয়। সাইবার নিরাপত্তা লক্ষ্য অর্জনের আপডেটগুলি সময়ে সময়ে বোর্ড দ্বারা যোগাযোগ এবং পর্যালোচনা করা হয়, যার মধ্যে সাইবার নিরাপত্তা কৌশলকে সমর্থন করার জন্য সম্পদ এবং বাজেট সম্পর্কিত বিবেচনাও অন্তর্ভুক্ত থাকে।	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12

খ. সাইবার নিরাপত্তা সম্পর্কিত নীতি এবং প্রক্রিয়া স্থাপন করা হয়, সময়ে সময়ে আপডেট করা হয়, এবং নিয়ন্ত্রণ পরিবেশকে শক্তিশালী করা হয়।	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
গ. সাইবার নিরাপত্তা লক্ষ্যসমূহকে সমর্থনকারী ভূমিকা এবং দায়িত্বসমূহ স্থাপন করা হয়, এবং যারা এসব ভূমিকা পালন করছেন তাদের জ্ঞান, দক্ষতা এবং সক্ষমতা সময়ে সময়ে মূল্যায়ন করার জন্য একটি প্রক্রিয়া বিদ্যমান থাকে।	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07
ঘ. প্রাসঙ্গিক অংশীজনদের সাইবার নিরাপত্তা পরিবেশে বিদ্যমান দুর্বলতা এবং উদীয়মান হুমকির উপর আলোচনা এবং কার্যক্রমে সম্পৃক্ত করা হয়। অংশীজনদের মধ্যে জেষ্ঠ্য ব্যবস্থাপনা, অপারেশনস, ঝুঁকি ব্যবস্থাপনা, মানবসম্পদ, আইনি, কমপ্লায়েন্স, ভেন্ডর এবং অন্যান্যরা অন্তর্ভুক্ত থাকে।	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
ঝুঁকি ব্যবস্থাপনা প্রয়োজনীয়তা	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
ক. সংস্থার ঝুঁকি মূল্যায়ন এবং ঝুঁকি ব্যবস্থাপনা প্রক্রিয়াগুলির মধ্যে সাইবার নিরাপত্তা হুমকি এবং তাদের কৌশলগত লক্ষ্য অর্জনে প্রভাব সনাক্তকরণ, বিশ্লেষণ, প্রশমণ এবং পর্যবেক্ষণ অন্তর্ভুক্ত থাকে।	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12

খ. সাইবার নিরাপত্তা ঝুঁকি ব্যবস্থাপনা সংস্থাজুড়ে পরিচালিত হয়, যা নিম্নলিখিত ক্ষেত্রগুলো অন্তর্ভুক্ত করতে পারে: তথ্য প্রযুক্তি, এন্টারপ্রাইজ ঝুঁকি ব্যবস্থাপনা, মানবসম্পদ, আইনি, কমপ্লায়েন্স, অপারেশনস, সরবরাহ শৃঙ্খলা, হিসাবরক্ষণ, অর্থনীতি, এবং অন্যান্য।	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
গ. সাইবার নিরাপত্তা ঝুঁকি ব্যবস্থাপনার জন্য দায়বদ্ধতা এবং দায়িত্ব প্রতিষ্ঠিত হয় এবং একটি ব্যক্তি বা দল সনাক্ত করা হয় যারা সময়ে সময়ে সাইবার নিরাপত্তা ঝুঁকি ব্যবস্থাপনার পর্যবেক্ষণ এবং রিপোর্ট করে, যার মধ্যে ঝুঁকি প্রশমনের জন্য প্রয়োজনীয় সম্পদ এবং উদীয়মান সাইবার নিরাপত্তা ঝুঁকি সনাক্তকরণ অন্তর্ভুক্ত থাকে।	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12
ঘ. সংস্থার প্রতিষ্ঠিত ঝুঁকি ব্যবস্থাপনা নির্দেশিকা বা প্রযোজ্য আইনি ও নিয়ন্ত্রক প্রয়োজনীয়তা মেনে চলার ভিত্তিতে যেকোন সাইবার নিরাপত্তা ঝুঁকি (উদীয়মান বা পূর্বে চিহ্নিত) দ্রুত উন্নত করার জন্য একটি প্রক্রিয়া প্রতিষ্ঠিত হয় যা একটি অগ্রহণযোগ্য স্তরে বৃদ্ধি পায়। সাইবার নিরাপত্তা ঝুঁকির আর্থিক এবং অ-আর্থিক প্রভাব উভয়ই বিবেচনা করা উচিত।	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12

ঙ. একটি প্রক্রিয়া স্থাপন করা হ যাতে সাইবার নিরাপত্তা ঝুঁকি সচেতনতা ব্যবস্থাপনা এবং কর্মীদের কাছে যোগাযোগ করা য়, এবং ব্যবস্থাপনার দ্বারা সময়ে সময়ে বিষয়গুলো, গ্যাপ, ঘাটতি, বা নিয়ন্ত্রণ ব্যর্থতার পর্যালোচনা করা হয়, যার মধ্যে প্রতিবেদন এবং মেরামত অন্তর্ভুক্ত থাকে।	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
চ. সংস্থা একটি সাইবার নিরাপত্তা ঘটনার প্রতিক্রিয়া এবং পুনরুদ্ধার প্রক্রিয়া বাস্তবায়ন করেছে যার মধ্যে সনাক্তকরণ, নিয়ন্ত্রণ, পুনরুদ্ধার এবং ঘটনার পরবর্তী বিশ্লেষণ অন্তর্ভুক্ত রয়েছে। ঘটনার প্রতিক্রিয়া এবং পুনরুদ্ধারের প্রক্রিয়া পর্যায়ক্রমে পরীক্ষা করা হয়।	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
নিয়ন্ত্রণ প্রক্রিয়া প্রয়োজনীয়তা	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
ক. একটি প্রক্রিয়া স্থাপন করা হ যা নিশ্চিত করে যে সংস্থার সিস্টেম এবং ডেটার গোপনীয়তা, অখণ্ডতা এবং প্রাপ্যতা রক্ষায় অভ্যন্তরীণ নিয়ন্ত্রণ এবং ভেন্ডর-ভিত্তিক নিয়ন্ত্রণ উভয়ই কার্যকর রয়েছে। নিয়ন্ত্রণগুলি সময়ে সমে মূল্যায়ন করা হয় যাতে নিশ্চিত করা যায় যে সেগুলি এমনভাবে কাজ করছে যা সংস্থার সাইবার নিরাপত্তা লক্ষ্য অর্জনে সহায়ক এবং সমস্যা সমাধানের জন্য থাসময়ে ব্যবস্থা নিচ্ছে।	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01

খ. একটি ট্যালেন্ট ম্যানেজমেন্ট প্রক্রিয়া স্থাপন করা হয় এবং সাইবার নিরাপত্তা অপারেশনসের জন্য সময়ে সময়ে পর্যালোচনা করা হয়, যা প্রযুক্তিগত দক্ষতা উন্নয়ন এবং রক্ষণাবেক্ষণের জন্য প্রশিক্ষণের সুযোগ অন্তর্ভুক্ত করে।	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
গ. একটি প্রক্রিয়া স্থাপন করা হ যা সাইবার নিরাপত্তা উদীয়মান হুমকি এবং দুর্বলতাগুলির ক্রমাগত মনিটরিং এবং প্রতিবেদন প্রদান করে এবং সাইবার নিরাপত্তা অপারেশন উন্নত করার জন্য সুযোগ চিহ্নিত, অগ্রাধিকার দেওয়া এবং বাস্তবায়ন করে।	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
ঘ. সাইবার নিরাপত্তা সমস্ত আইটি সম্পদের জীবনচক্র ব্যবস্থাপনায় (নির্বাচন, ব্যবহার, রক্ষণাবেক্ষণ এবং অবসর গ্রহণ) অন্তর্ভুক্ত করা হয়, যার মধ্যে হার্ডওয়্যার, সফটওয়্যার এবং ভেন্ডর সেবা অন্তর্ভুক্ত রয়েছে।	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06
ঙ. সাইবার নিরাপত্তা প্রচারের জন্য প্রক্রিয়া স্থাপন করা হয়, যার মধ্যে কনফিগারেশন, এন্ড-ইউজার ডিভাইস প্রশাসন, এনক্রিপশন, প্যাচিং, ব্যবহারকারী-প্রবেশাধিকার ব্যবস্থাপনা এবং উপলব্ধতা ও কর্মক্ষমতা পর্যবেক্ষণ অন্তর্ভুক্ত রয়েছে। সফটওয়্যার উন্নয়নে সাইবার নিরাপত্তা বিষয়গুলি (DevSecOps) অন্তর্ভুক্ত করা হয়।	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01

চ. নেটওয়ার্ক সম্পর্কিত নিয়ন্ত্রণগুলি স্থাপন করা হয়, যেমন নেটওয়ার্ক প্রবেশাধিকার নিয়ন্ত্রণ এবং সেগমেন্টেশন; ফায়ারওয়াল ব্যবহার এবং স্থাপন; বাহ্যিক নেটওয়ার্ক থেকে এবং বাহিরে সংযোগের সীমাবদ্ধতা; ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN)/জিরো ট্রাস্ট নেটওয়ার্ক অ্যাক্সেস (ZTNA), ইন্টারনেট অব থিংস (IoT) নেটওয়ার্ক নিয়ন্ত্রণের অন্তর্ভুক্তি, এবং অনুপ্রবেশ সনাক্তকরণ/প্রতিরোধ সিস্টেম (IDS এবং IPS)।	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
ছ. এন্ডপয়েন্ট যোগাযোগ সুরক্ষা নিয়ন্ত্রণগুলি প্রতিষ্ঠিত হয়, যেমন ইমেইল, ইন্টারনেট ব্রাউজার, ভিডিও কনফারেন্সিং, মেসেজিং, সোশ্যাল মিডিয়া, ক্লাউড এবং ফাইল শেয়ারিং প্রোটোকল সম্পর্কিত সেবাসমূহে।	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

অ্যাপেনডিক্স C ঐচ্ছিক ডকুমেন্টেশন টুল

অভ্যন্তরীণ নিরীক্ষকদের কাছ থেকে প্রত্যাশা করা হয় যে তারা ঝুঁকি মূল্যায়ন ভিত্তিক প্রয়োজনীয়তার প্রযোজ্যতা নির্ধারণে পেশাদার সিদ্ধান্ত গ্রহণ করবে এবং কিছু প্রয়োজনীয়তার ব্যতিক্রমগুলি সঠিকভাবে ডকুমেন্ট করবে। বিষয়ভিত্তিক প্রয়োজনীয়তা অভ্যন্তরীণ নিরীক্ষা পরিকল্পনায় বা নিরীক্ষকের পেশাদার সিদ্ধান্তের ভিত্তিতে কার্যক্রমের কার্যপত্রে নথিভুক্ত করা যেতে পারে। এক বা একাধিক অভ্যন্তরীণ নিরীক্ষা কার্যক্রমের প্রয়োজনীয়তাগুলি অন্তর্ভক্ত করতে পারে। এছাড়াও, সব প্রয়োজনীয়তা প্রযোজ্য নাও হতে পারে। নিচে প্রিন্টযোগ্য ফর্মটি সাইবার নিরাপত্তা বিষয়ভিত্তিক প্রয়োজনীয়তার সাথে সামঞ্জস্যতা নথিভুক্ত করার একটি বিকল্প প্রদান করে, তবে এর ব্যবহার বাধ্যতামূলক নয়।

সাইবার নিরাপত্তা – শাসন

প্রয়োজনীয়তা	সম্পাদিত কাভারেজ বা ব্যতিক্রমের যৌক্তিকতা	নথিভুক্তিকরন তথ্যসূত্র
ক. একটি আনুষ্ঠানিক সাইবার নিরাপত্তা কৌশল এবং লক্ষ্য স্থাপন করা হয় এবং সময়ে সময়ে হালনাগাদ করা হয়। সাইবার নিরাপত্তা লক্ষ্যগুলির অর্জনের হালনাগাদগুলি সময়ে সময়ে পর্ষদের মাধ্যমে যোগাযোগ এবং পর্যালোচনা করা হয়, যার মধ্যে সাইবার নিরাপত্তা কৌশল সমর্থন করার জন্য সম্পদ এবং বাজেটের বিষয়গুলি অন্তর্ভুক্ত থাকে।		
খ. সাইবার নিরাপত্তা সম্পর্কিত নীতিমালা এবং প্রক্রিয়া স্থাপন করা হয়, সময়ে সময়ে আপডেট করা হ এবং নিয়ন্ত্রণ পরিবেশকে শক্তিশালী করে।		

প্রয়োজনীয়তা	সম্পাদিত কাভারেজ বা ব্যতিক্রমের যৌক্তিকতা	নথিভুক্তিকরন তথ্যসূত্র
গ. সাইবার নিরাপত্তা লক্ষ্য সমর্থনকারী ভূমিকা এবং দায়িত্বগুলি স্থাপন করা হয়, এবং যারা এই ভূমিকা পালন করছে তাদের জ্ঞান, দক্ষতা এবং সক্ষমতা সময়ে সময়ে মূল্যায়ন করার জন্য একটি প্রক্রিয়া রয়েছে।		
ঘ. সংশ্লিষ্ট অংশীজনদের সাইবার নিরাপত্তা পরিবেশে বিদ্যমান দুর্বলতা এবং উদীয়মান হুমকি নিয়ে আলোচনা এবং পদক্ষেপ গ্রহণের জন্য সম্পৃক্ত করা হয়। অংশীজনদের মধ্যে জেষ্ঠ্য ব্যবস্থাপনা, অপারেশন, ঝুঁকি ব্যবস্থাপনা, মানবসম্পদ, আইন, সম্মতি, ভেন্ডর এবং অন্যান্যরা অন্তর্ভুক্ত থাকে।		

সাইবার নিরাপত্তা – ঝুঁকি ব্যবস্থাপনা

প্রয়োজনীয়তা	সম্পাদিত কাভারেজ বা ব্যতিক্রমের যৌক্তিকতা	নথিভুক্তিকরন তথ্যসূত্র
ক. সংগঠনের ঝুঁকি মূল্যায়ন এবং ঝুঁকি ব্যবস্থাপনা প্রক্রিয়া সাইবার নিরাপত্তা হুমকি চিহ্নিত করা, বিশ্লেষণ করা, কমানো এবং পর্যবেক্ষণ করার পাশাপাশি, তাদের কৌশলগত লক্ষ্য অর্জনে প্রভাব মূল্যায়ন অন্তর্ভুক্ত থাকে।		

প্রয়োজনীয়তা	সম্পাদিত কাভারেজ বা ব্যতিক্রমের যৌক্তিকতা	নথিভুক্তিকরন তথ্যসূত্র
খ. সাইবার নিরাপত্তা ঝুঁকি ব্যবস্থাপনা সংগঠনের মধ্যে পরিচালিত হয় এবং এতে নিম্নলিখিত ক্ষেত্রগুলি অন্তর্ভুক্ত থাকতে পারেঃ তথ্য প্রযুক্তি, এন্টারপ্রাইজ ঝুঁকি ব্যবস্থাপনা, মানবসম্পদ, আইন, সম্মতি, অপারেশন, সরবরাহ চেইন, হিসাবরক্ষণ, অর্থ, এবং অন্যান্য।		
গ. সাইবার নিরাপত্তা ঝুঁকি ব্যবস্থাপনার জন্য জবাবদিহিতা এবং দায়িত্ব নির্ধারণ করা হয়। একটি ব্যক্তি বা দল চিহ্নিত করা হয় যারা নিয়মিতভাবে সাইবার নিরাপত্তা ঝুঁকি কীভাবে ব্যবস্থাপনা করা হচ্ছে তা পর্যবেক্ষণ এবং প্রতিবেদন করবে, যার মধ্যে ঝুঁকি কমাতে প্রয়োজনীয় সম্পদ এবং উদীয়মান সাইবার নিরাপত্তা হুমকি চিহ্নিত করা অন্তর্ভুক্ত থাকে।		
ঘ. একটি প্রক্রিয়া প্রতিষ্ঠিত করা হয় যা দ্রুত সাইবার নিরাপত্তা ঝুঁকি (উদীয়মান বা পূর্বে চিহ্নিত) যেগুলি সংগঠনের প্রতিষ্ঠিত ঝুঁকি ব্যবস্থাপনা নির্দেশিকা বা প্রযোজ্য আইনগত এবং নিয়ন্ত্রক প্রয়োজনীয়তা অনুযায়ী অগ্রহণযোগ্য স্তরে পৌঁছায়, তা দ্রুত উন্নত করবে। সাইবার নিরাপত্তা ঝুঁকির আর্থিক এবং অ-আর্থিক প্রভাবগুলি বিবেচনা করা উচিত।		

প্রয়োজনীয়তা	সম্পাদিত কাভারেজ বা ব্যতিক্রমের যৌক্তিকতা	নথিভুক্তিকরন তথ্যসূত্র
ঙ. একটি প্রক্রিয়া প্রতিষ্ঠিত করা হয় যা সাইবার নিরাপত্তা ঝুঁকির সচেতনতা ব্যবস্থাপনা এবং কর্মচারীদের কাছে যোগাযোগ করবে এবং ব্যবস্থাপনার জন্য সময়মতো প্রতিবেদন এবং প্রতিকারের জন্য সমস্যা, গ্যাপ, ঘাটতি বা নিয়ন্ত্রণ ব্যর্থতা সময়ে সময়ে পর্যালোচনা করবে।		
চ. সংগঠন একটি সাইবার নিরাপত্তা ঘটনা প্রতিক্রিয়া এবং পুনরুদ্ধার প্রক্রিয়া বাস্তবায়ন করেছে, যার মধ্যে সনাক্তকরণ, সীমাবদ্ধকরণ, পুনরুদ্ধার এবং পরবর্তী ঘটনা বিশ্লেষণ অন্তর্ভুক্ত। ঘটনা প্রতিক্রিয়া এবং পুনরুদ্ধার প্রক্রিয়া সময়ে সময়ে পরীক্ষা করা হয়।		

সাইবার নিরাপত্তা – নিয়ন্ত্রণ প্রক্রিয়া

প্রয়োজনীয়তা	সম্পাদিত কাভারেজ বা ব্যতিক্রমের যৌক্তিকতা	নথিভুক্তিকরন তথ্যসূত্র
ক. একটি প্রক্রিয়া প্রতিষ্ঠিত করা হয় যা নিশ্চিত করে যে সংগঠনের সিস্টেম এবং ডেটার গোপনীয়তা, অখণ্ডতা, এবং প্রাপ্যতা সুরক্ষিত রাখতে অভ্যন্তরীণ নিয়ন্ত্রণ এবং বিক্রেতা-ভিত্তিক নিয়ন্ত্রণ উভয়ই বিদ্যমান। নিয়ন্ত্রণগুলি সময়ে সময়ে মূল্যায়ন করা হয় যাতে তা নিশ্চিত করা যায় যে নিয়ন্ত্রণগুলি সংগঠনের সাইবার নিরাপত্তা লক্ষ্য অর্জনে সহায়কভাবে কাজ করছে এবং সমস্যা সমাধানে দ্রুত সমাধান প্রদান করছে।		
খ. একটি প্রতিভা ব্যবস্থাপনা প্রক্রিয়া প্রতিষ্ঠিত করা হয়েছে যা সাইবার নিরাপত্তা কার্যক্রমের সাথে সম্পর্কিত প্রযুক্তিগত দক্ষতা উন্নয়ন এবং রক্ষা করার জন্য প্রশিক্ষণ অন্তর্ভুক্ত করে। এই প্রক্রিয়াটি সময়ে সময়ে পর্যালোচনা করা হয়।		
গ. একটি প্রক্রিয়া প্রতিষ্ঠিত করা হয়েছে যা উদীয়মান সাইবার নিরাপত্তা হুমকি এবং দুর্বলতাগুলি অবিচ্ছিন্নভাবে মনিটর এবং রিপোর্ট করে এবং সাইবার নিরাপত্তা কার্যক্রম উন্নত করার জন্য সুযোগগুলি চিহ্নিত, অগ্রাধিকার এবং বাস্তবায়ন করে।		

প্রয়োজনীয়তা	সম্পাদিত কাভারেজ বা ব্যতিক্রমের যৌক্তিকতা	নথিভুক্তিকরন তথ্যসূত্র
ঘ. সাইবার নিরাপত্তা সমস্ত আইটি সম্পদের জীবনচক্র ব্যবস্থাপনায় (নির্বাচন, ব্যবহার, রক্ষণাবেক্ষণ এবং অবসান) অন্তর্ভুক্ত করা হয়, যার মধ্যে হার্ডওয়্যার, সফটওয়্যার এবং বিক্রেতা সেবা রয়েছে।		
ঙ. সাইবার নিরাপত্তা প্রচারের জন্য প্রক্রিয়া প্রতিষ্ঠিত করা হয়েছে, যার মধ্যে কনফিগারেশন, এনডি ইউজার ডিভাইস প্রশাসন, এনক্রিপশন, প্যাচিং, ইউজার-অ্যাক্সেস ব্যবস্থাপনা, এবং উপলব্ধতা ও কর্মক্ষমতা মনিটরিং অন্তর্ভুক্ত রয়েছে। সফটওয়্যার উন্নয়নে (DevSecOps) সাইবার নিরাপত্তা বিবেচনাগুলি অন্তর্ভুক্ত করা হয়।		
চ. নেটওয়ার্ক সম্পর্কিত নিয়ন্ত্রণগুলি প্রতিষ্ঠিত করা হয়েছে, যেমন নেটওয়ার্ক প্রবেশ নিয়ন্ত্রণ এবং বিভাজন; ফায়ারওয়াল ব্যবহৃত এবং স্থাপন; বাহ্যিক নেটওয়ার্ক থেকে এবং বাহিরে সংযোগের সীমিত করা; ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN)/জিরো ট্রাস্ট নেটওয়ার্ক অ্যাক্সেস (ZTNA), ইন্টারনেট অব থিংস (IoT) নেটওয়ার্ক নিয়ন্ত্রণ, এবং প্রবাহ সনাক্তকরণ/প্রতিরোধ ব্যবস্থা (IDS এবং IPS)।		

প্রয়োজনীয়তা	সম্পাদিত কাভারেজ বা ব্যতিক্রমের যৌক্তিকতা	নথিভুক্তিকরন তথ্যসূত্র
ছ. এন্ডপয়েন্ট যোগাযোগ সুরক্ষা নিয়ন্ত্রণগুলি প্রতিষ্ঠিত করা হয়েছে, যেমন ইমেইল, ইন্টারনেট ব্রাউজার, ভিডিও কনফারেন্সিং, মেসেজিং, সোশ্যাল মিডিয়া, ক্লাউড এবং ফাইল-শেয়ারিং প্রোটোকলসের জন্য।		

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.

ডিসক্লেইমার

কপিরাইট

February 2025

The Institute of Internal Auditors

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