Կիբեռանվտանգության

Թեմատիկ պահանջ

Topical Requirement

The Institute of Internal Auditors

Թարգմանված՝

The Institute of Internal Auditors Armenia

Կիբերանվտանգության թեմատիկ պահանջ

Մասնագիտական գործունեության միջազգային հայեցակարգը *(International Professional Practices Framework®)* ներառում է **Ներքին աուդիտի միջազգային ստանդարտները** *(Global Internal Audit Standards™)*, **Թեմատիկ պահանջներն** ու **Միջազգային ուղեցույցները**: Թեմատիկ պահանջները **պարտադիր** են և պետք է կիրառվեն Ստանդարտների հետ համատեղ, որոնք **հեղինակավոր հիմք** են հանդիսանում պահանջվող պրակտիկաների համար:

Թեմատիկ պահանջները ներքին աուդիտորների համար սահմանում են հստակ ակնկալիքներ՝ որոշակի ռիսկային թեմաների աուդիտ իրականացնելու համար սահմանելով նվազագույն շեմ: Կազմակերպության ռիսկերի պրոֆիլը կարող է պահանջել, որ ներքին աուդիտորները դիտարկեն տվյալ թեմայի լրացուցիչ կողմեր:

Համապատասխանությունը Թեմատիկ պահանջներին կբարձրացնի ներքին աուդիտի ծառայությունների հետևողական իրականացումը, և կբարելավի ներքին աուդիտի ծառայությունների ու արդյունքների **որակն ու վստահելիությունը**: Արդյունքում, Թեմատիկ պահանջները բարձրացնում են ներքին աուդիտի մասնագիտության մակարդակը:

Ներքին աուդիտորները պարտավոր են կիրառել Թեմատիկ պահանջները՝ համապատասխանելով ներքին աուդիտի միջազգային ստանդարտներին: Թեմատիկ պահանջներին համապատասխանելը **պարտադիր է հավաստիացման ծառայությունների**, և **ցանկալի է խորհրդատվական ծառայությունների համար**:

Թեմատիկ պահանջը կիրառելի է, երբ թեման վերաբերում է հետևյալ դեպքերից մեկին.

Ա. Ներքին աուդիտի ծրագրում ներառված հանձնառության թեմա է:

Բ. Թեման ի հայտ է գալիս հանձնառության կատարման ընթացքում:

Գ. Ներքին աուդիտի սկզբնական ծրագրում որպես պահանջ չընդգրկված հանձնառության թեմա է:

Թեմատիկ պահանջի յուրաքանչյուր պահանջի կիրառելիության գնահատման ապացույցներն անհրաժեշտ է փաստաթղթավորել և պահպանել: Ոչ բոլոր առանձին պահանջներն են պարտադիր կիրառելի յուրաքանչյուր հանձնառության դեպքում. եթե որոշ պահանջներ չեն ներառվում, ապա դրա **հիմնավորումը պետք է փաստաթղթավորվի և պահպանվի**: Թեմատիկ պահանջին համապատասխանությունը պարտադիր է և ենթակա է գնահատման՝ որակի գնահատումների ընթացքում:

> *Լրացուցիչ տեղեկատվության համար տես՝ **Կիբերանվտանգության թեմատիկ պահանջների օգտագործողի ուղեցույց**:*

Կիբերանվտանգություն

Ստանդարտների և տեխնոլոգիաների ազգային ինստիտուտը *(NIST)* Կիբերանվտանգությունը[1] պարզապես սահմանում է որպես «**կիբերհարձակումներից կիբերտարածության օգտագործումը պաշտպանելու կարողություն**»:

Կիբերանվտանգությունը տեղեկատվական անվտանգության ավելի ընդհանուր ոլորտի ենթաբաժին է, որը NIST-ն սահմանում է որպես՝ «չարտոնված մուտքից, օգտագործումից, բացահայտումից, խափանումից, փոփոխումից կամ ոչնչացումից **տեղեկատվության և տեղեկատվական համակարգերի պաշտպանություն՝ գաղտնիությունը, ամբողջականությունը և հասանելիությունը** ապահովելու համար»:

Կիբերանվտանգությունը նվազեցնում է ռիսկը՝ ամրապնդելով ընդհանուր հսկողական միջավայրը և պաշտպանելով կազմակերպության տեղեկատվական ակտիվները չարտոնված մուտքից, խափանումից, փոփոխումից կամ ոչնչացումից: Կիբերհարձակումները կարող են հանգեցնել ուղղակի և անուղղակի հետևանքների, որոնք հաճախ էական են, քանի որ համակարգիչները, ցանցերը, ծրագրերը, տվյալներն ու զգայուն տեղեկատվությունը կազմակերպությունների մեծ մասի համար կրիտիկական կարևորություն ունեցող բաղադրիչներ են:

Կիբերանվտանգության ղեկավարման, ռիսկերի կառավարման և հսկողական գործընթացների գնահատում

Այս Թեմատիկ պահանջը տրամադրում է հետևողական, համապարփակ մոտեցում՝ գնահատելու **Կիբերանվտանգության ղեկավարման** *(governance)*, **ռիսկերի կառավարման** *(risk management)* և **հսկողական գործընթացների** *(control processes)* նախագծումն ու ներդրման մակարդակը: Այս պահանջները հանդիսանում են նվազագույն շեմ՝ կազմակերպության Կիբերանվտանգությունը գնահատելու համար:

ՂԵԿԱՎԱՐՈՒՄ. Կիբերանվտանգության ղեկավարման գնահատում

Պահանջներ.

Ներքին աուդիտորները կազմակերպության Կիբերանվտանգության ղեկավարման համատեքստում պետք է գնահատեն հետևյալը.

Ա. Կիբերանվտանգության ռազմավարությունն ու նպատակները ֆորմալ սահմանված են և պարբերաբար թարմացվում են: Կիբերանվտանգության նպատակների կատարման վերաբերյալ թարմացումները պարբերաբար հաղորդակցվում և դիտարկվում են կազմակերպության բարձրագույն ղեկավարության կողմից, ներառյալ՝ Կիբերանվտանգության ռազմավարությանն աջակցելու համար անհրաժեշտ ռեսուրսներին և բյուջեին վերաբերվող հարցերը:

[1] https://csrc.nist.gov/glossary/term/cybersecurity

Բ. Կիբերանվտանգությանը վերաբերվող քաղաքականություններն ու ընթացակարգերը սահմանված են և պարբերաբար թարմացվում են՝ հսկողական միջավայրը ամրապնդելու նպատակով:

Գ. Կիբերանվտանգության նպատակներին աջակցող դերերն ու պատասխանատվությունները սահմանված են: Առկա է այդ դերերը զբաղեցնող անձանց գիտելիքները, հմտություններն ու կարողությունները պարբերաբար գնահատելու գործընթաց:

Դ. Համապատասխան շահառուները ներգրավվում են՝ առկա խոցելիություններն ու Կիբերանվտանգության միջավայրում առաջացող սպառնալիքները քննարկելու և դրանց ուղղված գործողություններ ձեռնարկելու համար: Շահառուները ներառում են ավագ ղեկավարությունը, գործառնական ստորաբաժանումները, ռիսկերի կառավարումը, մարդկային ռեսուրսները, իրավաբանական ծառայությունը, համապատասխանության գործառույթը, մատակարարները և այլոք:

ՌԻՍԿԵՐԻ ԿԱՌԱՎԱՐՈՒՄ: Կիբերանվտանգության ռիսկերի կառավարման գնահատում

Պահանջներ.

Ներքին աուդիտորները կազմակերպության Կիբերանվտանգության ռիսկերի կառավարման համատեքստում պետք է գնահատեն հետևյալը.

Ա. Կազմակերպության ռիսկերի գնահատման և ռիսկերի կառավարման գործընթացները ներառում են Կիբերանվտանգության սպառնալիքների, ինչպես նաև ռազմավարական նպատակների իրականացման վրա դրանց ազդեցության նույնականացումը, վերլուծությունը, մեղմացումը *(mitigation)* և մշտադիտարկումը:

Բ. Կիբերանվտանգության ռիսկերի կառավարումն իրականացվում է ամբողջ կազմակերպության մասշտաբով և կարող է ներառել հետևյալ ոլորտները. Տեղեկատվական տեխնոլոգիաներ, կազմակերպության համապարփակ ռիսկերի կառավարում *(Enterprise Risk Management)*, մարդկային ռեսուրսներ, իրավաբանական ծառայություն, համապատասխանության գործառույթ, գործառնական ստորաբաժանումներ, մատակարարման շղթա, հաշվապահություն, ֆինանսներ և այլն:

Գ. Կիբերանվտանգության ռիսկերի կառավարման համար սահմանված են հաշվետվողականությունն ու պատասխանատվությունը: Նշանակված է անձ կամ թիմ, որը պարբերաբար մշտադիտարկում և զեկուցում է, թե ինչպես են կառավարվում Կիբերանվտանգության ռիսկերը, ներառյալ՝ ռիսկերը մեղմելու և ի հայտ եկող Կիբերանվտանգության սպառնալիքները բացահայտելու համար անհրաժեշտ ռեսուրսները:

Դ. Սահմանված է գործընթաց՝ արագ էսկալացնելու ցանկացած Կիբերանվտանգության ռիսկ *(նոր ի հայտ եկող կամ նախկինում նույնականացված)*, որը հասնում է անընդունելի մակարդակի՝ համաձայն կազմակերպության սահմանված ռիսկերի կառավարման ուղեցույցների կամ կիրառելի իրավական և կարգավորիչ

պահանջների: Պետք է դիտարկվեն Կիբերանվտանգության ռիսկի **ֆինանսական և ոչ ֆինանսական** ազդեցությունները:

Ե. Սահմանված է ղեկավարությանը և աշխատակիցներին Կիբերանվտանգության ռիսկերի վերաբերյալ իրազեկելու գործընթաց: Ղեկավարության համար սահմանված է նաև խնդիրների, բացերի, թերությունների կամ հսկողությունների ձախողումների պարբերաբար վերանայման գործընթաց՝ ժամանակին իրազեկված լինելու և վերականգնողական *(remediation)* գործողություններ նախաձեռնելու հնարավորությամբ:

Զ. Կազմակերպությունը ներդրել է Կիբերանվտանգության միջադեպերի արձագանքման և վերականգնման գործընթաց, որը ներառում է հայտնաբերում, մեկուսացում *(containment)*, վերականգնում և միջադեպից հետո վերլուծություն: Միջադեպերի արձագանքման և վերականգնման գործընթացները պարբերաբար փորձարկվում են:

ՀՍԿՈՂՈՒԹՅՈՒՆՆԵՐ (CONTROLS): Կիբերանվտանգության հսկողական գործընթացների գնահատում

Պահանջներ.

Ներքին աուդիտորները կազմակերպության Կիբերանվտանգության հսկողական գործընթացների համատեքստում պետք է գնահատեն հետևյալը.

Ա. Սահմանված է գործընթաց՝ համոզվելու, որ կազմակերպության համակարգերի և տվյալների գաղտնիությունը, ամբողջականությունը և հասանելիությունը պաշտպանելու համար գործում են ինչպես ներքին, այնպես էլ գործընկերների (*vendor*) մոտ ներդրված հսկողություններ: Պարբերաբար իրականացվում են գնահատումներ՝ որոշելու համար արդյոք հսկողությունները գործում են այնպես, որ նպաստեն կազմակերպության Կիբերանվտանգության նպատակների իրագործմանը և խնդիրների արագ լուծմանը:

Բ. Սահմանված է տաղանդների (կադրերի) կառավարման գործընթաց, որը ներառում է ուսուցում՝ զարգացնելու և պահպանելու Կիբերանվտանգության գործառնական գործունեությանը վերաբերող տեխնիկական կարողությունները: Գործընթացը պարբերաբար վերանայվում է:

Գ. Սահմանված է գործընթաց՝ շարունակաբար մշտադիտարկելու և զեկուցելու ի հայտ եկող կիբերսպառնալիքներն ու խոցելիությունները, ինչպես նաև Կիբերանվտանգության գործողությունները բարելավելու հնարավորությունները բացահայտելու, առաջնահերթություն տալու և իրականացնելու համար:

Դ. Կիբերանվտանգությունը ներառված է SS բոլոր ակտիվների կենսացիկլի կառավարման մեջ *(ընտրություն, օգտագործում, սպասարկում և շահագործումից հանում)*, ներառյալ՝ սարքավորումներ *(hardware)*, ծրագրային ապահովում *(software)* և մատակարարների ծառայություններ *(vendor services)*:

Ե. Սահմանված են գործընթացներ Կիբերանվտանգության ամրապնդման համար, ներառյալ՝ կարգաբերումների (*configuration*) կառավարում, վերջնական օգտագործողի սարքերի ադմինիստրավորում, ծածկագրում, թարմացումների տեղադրում, օգտագործողների հասանելիության կառավարում, ինչպես նաև **հասանելիության ու աշխատանքի մշտադիտարկում**: Կիբերանվտանգության նկատառումները ներառված են նաև ծրագրային ապահովման մշակման մեջ *(DevSecOps)*:

Զ. Սահմանված են ցանցին վերաբերվող հսկողություններ, ինչպիսիք են ցանցային մուտքի վերահսկումն ու սեգմենտավորումը, հրապատերի *(firewall)* կիրառությունը և տեղաբաշխումը, արտաքին ցանցերից դեպի ներս և ներսից դեպի արտաքին ցանցերի միացումների սահմանափակումները, վիրտուալ մասնավոր ցանցի (VPN)/զրոյական վստահության ցանցային մուտքը (ZTNA), իրերի ինտերնետի *(IoT)* ցանցի կառավարումը և ներխուժման հայտնաբերման *(IDS - intrusion detection system)* և կանխարգելման համակարգերը (*IPS - intrusion prevention systems)*:

Է. Սահմանված են վերջնակետերի հաղորդակցման անվտանգության հսկողություններ՝ էլեկտրոնային փոստի, ինտերնետ դիտարկիչների, տեսակոնֆերանսների, հաղորդագրությունների, սոցիալական մեդիայի, ամպային ծառայությունների և ֆայլերի փոխանակման պրոտոկոլների համար:

Ներքին Աուդիտորների Ինստիտուտի մասին

Ներքին Աուդիտորների Ինստիտուտը (ՆԱԻ) միջազգային մասնագիտական ասոցիացիա է, որը սպասարկում է ավելի քան 260,000 անդամների և տրամադրել է ավելի քան 200,000 Որակավորված ներքին աուդիտորի *(Certified Internal Auditor® (CIA®))* հավաստագիր ամբողջ աշխարհում: Հիմնադրված 1941 թվականին՝ ՆԱԻ-ն աշխարհում ճանաչվում է որպես ներքին աուդիտի մասնագիտության ստանդարտների, հավաստագրերի, կրթության, հետազոտությունների և տեխնիկական ուղեցույցների առաջատար:

Լրացուցիչ տեղեկատվության համար այցելեք՝ www.theiia.org:

Փետրվար 2025

Թարգմանությունը՝ **Ներքին Աուդիտորների Ինստիտուտ - Հայաստան:**

Փետրվար 2026

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