Kibertəhlükəsizlik

Mövzu Əsaslı Tələb

(Topical Requirement)

The Institute of Internal Auditors

Tərəfindən tərcümə olunmuşdur

The Institute of Internal Auditors Azerbaijan

Kibertəhlükəsizlik üzrə Mövzu əsaslı Tələb

Daxili Auditorlar İnstitutunun (“DAİ”) Peşəkar Təcrübələr üzrə Beynəlxalq Çərçivəsi® (International Professional Practices Framework®) Qlobal Daxili Audit Standartları™ (Global Internal Audit Standards™), Mövzu Əsaslı Tələblər və İstifadə üzrə Qlobal Təlimatdan ibarətdir. Mövzu Əsaslı Tələblər məcburi xarakter daşıyır və nəzərdə tutulan tətbiq zamanı əsas və etibarlı mənbə sayılan Standartlarla birlikdə tətbiq edilməlidir.

Mövzu Əsaslı Tələblər müəyyən edilmiş risk sahələrinin auditi üçün minimum baza xəttini müəyyən etməklə daxili auditorlar üçün aydın şəkildə gözləntilər formalaşdırır. Təşkilatın risk profili daxili auditorlardan mövzunun əlavə aspektlərini, o cümlədən yerli tənzimləməyici tələbləri və qanunvericiliyi nəzərə almalarını tələb edə bilər.

Mövzu Əsaslı Tələblərə uyğunluq daxili audit xidmətlərinin icra edilməsində ardıcıllığı artıracaq və daxili audit xidmətlərinin və nəticələrinin keyfiyyətini və etibarlılığını yaxşılaşdıracaq. Nəticədə, Mövzu Əsaslı Tələblər daxili audit peşəsinin nüfuzunu yüksəldir.

Daxili auditorlar Qlobal Daxili Audit Standartlarına uyğun olaraq Mövzu Əsaslı Tələbləri tətbiq etməlidirlər. Mövzu Əsaslı Tələblərə uyğunluq əminlik təminatı xidmətləri üçün məcburi xarakter daşıyır və məsləhət xidmətləri üçün tövsiyə olunur.

Aşağıdakılardan hər hansı biri müvafiq olduqda Mövzu Əsaslı Tələb tətbiq olunur:

A. Daxili audit planında audit tapşırığının əhatə dairəsinə daxil olduqda.
B. Audit tapşırığı yerinə yetirilərkən müəyyən edildikdə.
C. İlkin daxili audit planında olmayan, lakin sonradan tələb olunan audit tapşırığının əhatə dairəsinə daxil olduqda.

Hər bir fərdi tələb, hər bir tapşırığa aid olmaya bilər və bəzi tələblər digər yanaşmalar vasitəsilə də yerinə yetirilə bilər. Əgər tələb digər tənzimləyici qurumların tələbləri və ya müqavilə öhdəlikləri ilə istisna və ya əvəz edilirsə, yaxud Qlobal Daxili Audit Standartlarına uyğun prosedurların tətbiqi vasitəsilə həll olunursa, bunun əsaslandırılması sənədləşdirilməli və saxlanılmalıdır. Standartlara uyğunluq keyfiyyət qiymətləndirmələri zamanı təhlil olunmalıdır.

Daha ətraflı məlumat üçün Kibertəhlükəsizlik üzrə Mövzu Əsaslı Tələbin İstifadəçi Təlimatına müraciət edin.

Kibertəhlükəsizlik

ABŞ-də yerləşən Standartlar və Texnologiya üzrə Milli İnstitut (STMİ/NIST) kibertəhlükəsizliyin tərifini sadə formada “kibermәkanı kiberhücumlardan qorumaq və ya müdafiə etmək qabiliyyəti” kimi təsvir edir. NIST-in də təsvir etdiyi kimi kibertəhlükəsizlik ümumi informasiya təhlükəsizliyinin bir alt sahəsidir: “Kibertəhlükəsizlik, məlumatların və informasiya sistemlərinin

məxfiliyini, tamlığını və əlçatanlığını təmin etmək məqsədilə onların icazəsiz giriş, istifadə, açıqlanma, pozulma, dəyişdirilmə və ya məhv edilməkdən qorunmasıdır."

Kibertəhlükəsizlik ümumi nəzarət mühitini gücləndirərək və təşkilatın informasiya aktivlərini icazəsiz girişdən, keyfiyyətin pozulmasından, dəyişdirilməkdən və ya məhv olmaqdan qoruyaraq riskləri azaldır. Kompüterlərin, şəbəkələrin, proqram təminatlarının, məlumat bazalarının və həssas məlumatların əksər təşkilatların həyati vacib komponentləri olduğunu nəzərə alaraq kiberhəmlələr çox vaxt əhəmiyyətli sayla biləcək birbaşa və ya dolayı təsirlərə səbəb ola bilər.

Kibertəhlükəsizlik ilə bağlı idarəetmə, risk idarəçiliyi və nəzarət proseslərinin qiymətləndirilməsi və yoxlanılması

Bu Mövzu əsaslı Tələb kibertəhlükəsizliklə bağlı idarəetmə, risk idarəçiliyi və nəzarət proseslərinin dizaynını və tətbiqini qiymətləndirmək üçün ardıcıl və hərtərəfli bir yanaşma təqdim edir. Bu tələblər təşkilatda kibertəhlükəsizliyin qiymətləndirilməsi üçün minimum baza səviyyəsini təmsil edir.

İDARƏETMƏ: Kibertəhlükəsizliklə bağlı idarəetmənin qiymətləndirilməsi və yoxlanılması

Tələblər:

Daxili auditorlar təşkilatın kibertəhlükəsizliklə bağlı idarəetmə fəaliyyəti üzrə aşağıdakıları qiymətləndirməlidirlər:

A. Rəsmi formada kibertəhlükəsizlik strategiyası və məqsədləri müəyyən edilir və mütəmadi olaraq yenilənir. Kibertəhlükəsizlik məqsədlərinin yerinə yetirilməsi ilə bağlı yeniləmələr, eləcə də kibertəhlükəsizlik strategiyasını dəstəkləmək üçün resurslar və büdcə məsələləri də daxil olmaqla, mütəmadi olaraq direktorlar şurasına məlumat təqdim olunur və şura tərəfindən bu məlumatlar təhlil edilir.

B. Nəzarət mühitini gücləndirmək məqsədilə kibertəhlükəsizliklə bağlı siyasətlər və prosedurlar müəyyən edilir və mütəmadi olaraq yenilənir.

C. Kibertəhlükəsizlik məqsədlərini dəstəkləyən rollar və məsuliyyətlər müəyyən edilir və bu rolları icra edən şəxslərin bilik, bacarıq və qabiliyyətlərini dövri olaraq qiymətləndirmək üçün müəyyən bir proses mövcuddur.

D. Kibertəhlükəsizlik mühitində mövcud zəiflikləri və yaranan təhdidləri müzakirə etmək və onlara qarşı tədbir görmək üçün müvafiq maraqlı tərəflər cəlb edilir. Maraqlı tərəflərə yüksək rəhbərlik, əməliyyatlar, risk idarəçiliyi, insan resursları, hüquq, uyğunluq (komplayens), təchizatçılar və digərləri daxildir.

RİSKLƏRİN İDARƏ EDİLMƏSİ: Kibertəhlükəsizlik risklərinin idarə edilməsinin qiymətləndirilməsi və yoxlanılması

Tələblər:

Daxili auditorlar təşkilatın kibertəhlükəsizlik risklərinin idarə edilməsi ilə bağlı aşağıdakıları qiymətləndirməlidirlər:

A. Təşkilatın risk qiymətləndirilməsi və risklərin idarə edilməsi proseslərinə kibertəhlükəni müəyyən etmək, təhlil etmək, azaltmaq və bu risklərin strateji məqsədlərə çatmaqda təşkilat üçün yaratdıqları təsiri izləmək daxil edilir.

B. Kibertəhlükəsizlik risklərinin idarə edilməsi təşkilat üzrə həyata keçirilir və aşağıdakı sahələri əhatə edə bilər: informasiya texnologiyaları, korporativ risk idarəçiliyi, insan resursları, hüquq, uyğunluq (komplayens), əməliyyatlar, təchizat zənciri, mühasibatlıq, maliyyə və digərləri.

C. Kibertəhlükəsizlik risklərinin idarə edilməsinə görə hesabatlılıq və məsuliyyət müəyyən edilir. Mütəmadi olaraq kibertəhlükəsizlik risklərinin necə idarə olunduğunu, riskləri azaltmaq üçün tələb olunan resursları və ortaya çıxan kibertəhlükəsizlik təhdidlərini müəyyən etmək üçün monitorinq aparmaq və hesabat vermək məqsədilə bir fərd və ya komanda təyin edilir.

D. Təşkilatın müəyyən etdiyi risk idarəetmə qaydalarına və ya müvafiq hüquqi və tənzimləyici tələblərə əsasən qəbuledilməz səviyyəyə çatmış istənilən kibertəhlükəsizlik riskinin (yeni yaranan və ya əvvəlcədən müəyyən edilmiş) tez bir zamanda eskalasiya edilməsi üçün proses müəyyən edilir. Kibertəhlükəsizlik riskinin maliyyə və qeyri-maliyyə təsirləri nəzərə alınmalıdır.

E. Rəhbərlik və işçilərə kibertəhlükəsizlik riskləri barədə məlumat vermək, eləcə də rəhbərliyin bu problemləri, boşluqları, çatışmazlıqları və nəzarət uğursuzluqlarını vaxtında hesabat təqdim etməklə və aradan qaldırmaqla mütəmadi şəkildə nəzərdən keçirməsi üçün bir proses müəyyən edilir.

F. Təşkilat aşkarlanma, məhdudlaşdırma, bərpa və insidentdən sonrakı təhlili əhatə edən kibertəhlükəsizlik hadisələrinə reaksiya və bərpa prosesini tətbiq etmişdir. İnsidentə reaksiya və bərpa prosesi mütəmadi olaraq sınaq yoxlamasından keçirilir.

NƏZARƏT MEXANİZMLƏRİ: Kibertəhlükəsizlik üzrə nəzarət proseslərinin qiymətləndirilməsi və yoxlanılması

Tələblər:

Daxili auditorlar təşkilatın kibertəhlükəsizlik nəzarət prosesləri ilə əlaqədar aşağıdakıları qiymətləndirməlidirlər:

A. Təşkilatın sistemlərinin və məlumatlarının məxfiliyinin, tamlılğının və əlçatanlığının qorunmasını təmin etmək üçün həm daxili nəzarət, həm də təchizatçı əsaslı nəzarət mexanizmlərinin mövcudluğunu təmin edən bir proses müəyyən edilir. Nəzarət mexanizmlərinin təşkilati kibertəhlükəsizlik məqsədlərinin reallaşdırılmasına və

B. problemlərin operativ həllinə xidmət edəcək şəkildə fəaliyyət göstərib-göstərmədiyini müəyyən etmək üçün mütəmadi olaraq dəyərləndirilmələr aparılır.

C. Kibertəhlükəsizlik əməliyyatları ilə bağlı texniki sərişte və bacarıqları inkişaf etdirmək və qorumaq üçün təlimləri əhatə edən istedad idarəetmə prosesi yaradılır. Proses mütəmadi olaraq təhlil edilir və nəzərdən keçirilir.

D. Yaranan kibertəhlükəsizlik təhdidlərini və boşluqlarını davamlı şəkildə izləmək və hesabat vermək, eləcə də kibertəhlükəsizlik əməliyyatlarını təkmilləşdirmək üçün imkanları müəyyənləşdirmək, prioritetləşdirmək və həyata keçirmək məqsədilə bir proses yaradılır.

E. Kibertəhlükəsizlik bütün İT aktivlərinin (avadanlıqlar, proqram təminatı və təchizatçı xidmətləri də daxil olmaqla) həyat dövrü idarəçiliyinə (seçimi, istifadəsi, texniki qulluq və istismardan çıxarılması) daxil edilir.

F. Kibertəhlükəsizliyi gücləndirmək üçün konfiqurasiya, son istifadəçi cihazlarının idarə edilməsi, şifrələmə, yamaqlama, istifadəçi girişlərinin idarə edilməsi, eləcə də əlçatanlıq və fəaliyyət göstəricilərinin monitorinqi də daxil olmaqla proseslər müəyyən edilir. Proqram təminatının hazırlanmasında kibertəhlükəsizlik məsələləri (DevSecOps) nəzərə alınır.

G. Şəbəkə ilə bağlı idarəetmə tədbirləri müəyyən edilir, məsələn, şəbəkəyə girişə nəzarət və seqmentasiya; şəbəkələrarası ekranların (firewall) istifadəsi və yerləşdirilməsi; kənar şəbəkələrlə yaradılan məlumat mübadiləsi əlaqələrinin məhdudlaşdırılması; virtual özəl şəbəkə (VÖŞ/VPN)/sıfır etibar şəbəkə girişi (SEŞG/ZTNA); Əşyaların İnterneti (Əİ/IoT) üzrə şəbəkə idarəetmələri; və sızma aşkarlanması/qarşısının alınması sistemləri (SAS/IDS və SQS/IPS).

H. E-poçt, internet brauzerləri, video konfrans, mesajlaşma, sosial media, bulud və fayl paylaşımı protokolları kimi xidmətlər üçün son nöqtə kommunikasiyalarının təhlükəsizliyinə nəzarət mexanizmləri müəyyən edilir.

Daxili Auditorlar İnstitutu haqqında

Daxili Auditorlar İnstitutu (“IIA”), qeyri-kommersiya təşkilatı olaraq dünyanın müxtəlif ölkələrində 255,000-dən artıq üzvünə xidmət göstərən və 200,000 nəfərdən çox şəxsə “Sertifikatlaşdırılmış Daxili Auditor” (Certified Internal Auditor®) sertifikatı təqdim etmiş, daxili auditorların beynəlxalq peşəkar assosiasiyasıdır. Əsası 1941-ci ildə qoyulmuş Daxili Auditorlar İnstitutu (“IIA”), daxili audit sahəsində standartlaşdırma, sertifikatlaşdırma, təlimlərin keçirilməsi, tədqiqatların aparılması və texniki təlimatların hazırlanması ilə bağlı fəaliyyət göstərən lider təşkilat kimi tanınır. Əlavə məlumat almaq üçün www.theiia.org internet səhifəsinə müraciət edə bilərsiniz.

Müəllif hüquqları

Fevral 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