Kibertəhlükəsizlik

Mövzü Əsaslı Tələb İstifadə üzrə Təlimat

Topical Requirement

The Institute of Internal Auditors

Tərəfindən tərcümə olunmuşdur

The Institute of Internal Auditors Azerbaijan

Mündəricat

Mövzu Əsaslı Tələblərin İcmalı

Mövzu Əsaslı Tələblər Qlobal Daxili Audit Standartları™ (Global Internal Audit Standards™) və Qlobal Təlimatlarla birgə Beynəlxalq Peşəkar Təcrübələr üzrə Çərçivənin® (International Professional Practices Framework®) ayrılmaz hissəsi sayılır. Daxili Auditorlar İnstitutu ("DAİ") Mövzu Əsaslı Tələblərin müvafiq praktikanın tətbiqi zamanı etibarlı istinad mənbəyi olan Qlobal Daxili Audit Standartları ilə birlikdə tətbiq edilməsini tələb edir. Standartlara istinadlar bu təlimatın müxtəlif hissələrində daha ətraflı məlumat mənbəyi kimi yer alır.

Mövzu Əsaslı Tələblər daxili auditorların mövcud risk istiqamətlərinə necə yanaşdıqlarını daxili audit peşəsi kontekstində keyfiyyət və ardıcıllığı təşviq etmək məqsədilə rəsmi çərçivəyə salır. Mövzu Əsaslı Tələblər baza xəttini müəyyən edir və Mövzu Əsaslı Tələblərə dair əminlik xidmətlərinin həyata keçirilməsi üçün müvafiq meyarlar formalaşdırır (Standart 13.4 "Qiymətləndirmə Meyarları"). Mövzu Əsaslı Tələblərə uyğunluq əminlik xidmətləri üçün məcburi, məsləhət xidmətləri zamanı isə nəzərə alınması tövsiyə olunandır. Mövzu Əsaslı Tələblər əminlik fəaliyyətlərinin icra edilməsi zamanı nəzərə alınmalı olan bütün mümkün aspektləri əhatə etmək üçün nəzərdə tutulmayıb və sadəcə olaraq mövzunun ardıcıl və etibarlı qiymətləndirilməsini təmin etmək üçün minimum tələblər toplusunu təqdim etmək məqsədi daşıyır.

Mövzu Əsaslı Tələblər aydın şəkildə DAİ-nin Üç Xətt Modeli və Qlobal Daxili Audit Standartları ("Standartlar") ilə əlaqələndirilmişdir. İdarəetmə, risklərin idarə edilməsi və nəzarət prosesləri Mövzu Əsaslı Tələblərin əsas komponentləridir və Standart 9.1 "İdarəetmə, Risklərin İdarə Edilməsi və Daxili Nəzarət Proseslərinin Başa Düşülməsi" ilə uzlaşdırılmışdır. Üç Xətt Modelinə görə, idarəetmə Şura/idarəedici orqanla, risklərin idarə edilməsi ikinci xəttlə, nəzarət və ya nəzarət prosesləri isə birinci xəttlə əlaqələndirilir. Rəhbərliyin birinci və ikinci səviyyələrdə təmsil olunmasına baxmayaraq, daxili audit funksiyası üçüncü səviyyədə müstəqil və obyektiv əminlik təminatı verən tərəf qismində təsvir edilir və Şuraya/idarəedici orqana hesabat verir (Prinsip 8: "Şura Tərəfindən Nəzarətin Həyata Keçirilməsi").

Uyğunluq, Risk və Peşəkar Mühakimə

Mövzu Əsaslı Tələblər mövcud olduqda daxili audit funksiyaları həmin mövzularla bağlı əminlik təminatı üzrə tapşırıqları yerinə yetirərkən və ya digər təminat tapşırıqları çərçivəsində Mövzu Əsaslı Tələblərin aspektləri müəyyən ediləndə göstərilən bu tələblərə riayət etməlidirlər.

Standartlarda təsvir edildiyi kimi, riskləri qiymətləndirmək baş audit icraçısının planlaşdırma fəaliyyətinin vacib hissəsidir. Daxili audit planına daxil ediləcək əminlik təminatı tapşırıqlarını müəyyən etmək üçün təşkilatın strategiyalarını, məqsədlərini və risklərini ən azı illik qiymətləndirmək tələb olunur (Standart 9.4 "Daxili Audit Planı"). Fərdi təminat tapşırıqlarını

planlaşdırarkən daxili auditorlar tapşırıqla əlaqəli riskləri qiymətləndirməlidirlər (Standart 13.2 “Audit Tapşırığı Çərçivəsində Risklərin Qiymətləndirilməsi).

Risk əsaslı daxili audit planının hazırlanması zamanı Mövzu Əsaslı Tələbin mövzusu müəyyən edilərək audit planına daxil edildikdə, aid olduğu müvafiq yoxlamalarda həmin mövzunun qiymətləndirilməsi üçün Mövzu Əsaslı Tələbdə göstərilən tələblərdən istifadə olunmalıdır. Bundan əlavə, daxili auditorlar (plana daxil edilib-edilmədiyindən asılı olmayaraq) hər hansı bir audit yoxlamasını icra edərkən Mövzu Əsaslı Tələbin elementləri ortaya çıxdıqda, həmin Mövzu Əsaslı Tələb yoxlamanın bir hissəsi kimi tətbiq olunma baxımından qiymətləndirilməlidir. Nəhayət, əgər planlaşdırılmamış, lakin tematik mövzunu əhatə edən hər hansı bir audit tapşırığının icrası tələb olunarsa, Mövzu Əsaslı Tələbin tətbiq olunma baxımından qiymətləndirilməsi təmin olunmalıdır.

Mövzu Əsaslı Tələbi tətbiq edərkən peşəkar mühakimə əsas rol oynayır. Risk qiymətləndirmələri daxili audit planına hansı tapşırıqların daxil edilməsi barədə baş audit icraçılarının qərarlarını müəyyən edir (Standart 9.4). Bundan əlavə, daxili auditorlar peşəkar mühakimədən istifadə edərək hər bir yoxlama çərçivəsində hansı aspektlərin əhatə olunacağını (Standartlar 13.3 “Audit Tapşırığının Məqsədləri və Əhatə Dairəsi”, 13.4 “Qiymətləndirmə Meyarları” və 13.6 “İş Proqramı”) müəyyən edir. Əlavə A, “Praktiki Tətbiq Nümunələri”, daxili auditorların Mövzu Əsaslı Tələbdən necə istifadə etməli olduğunu təsvir edir.

Əgər Mövzu Əsaslı Tələb digər bir tənzimləyici tələb və ya müqavilə şərtləri ilə istisna və ya əvəz edilirsə, eləcə də Standartlara uyğunluq təşkil edən digər prosedurların tətbiqi ilə həll olunursa, bunun əsaslandırılması sənədləşdirilməli və saxlanılmalıdır. Mövzu Əsaslı Tələbə riayət edilməsi Standart 14.6 “Audit Tapşırığının Sənədləşdirilməsi”-də təsvir edildiyi kimi auditorların peşəkar mühakiməsindən istifadə etməklə sənədləşdirilməlidir.

Kibertəhlükəsizlik üzrə Mövzu Əsaslı Tələb nəzərə alınmalı olan nəzarət proseslərinin minimal səviyyəsini təsvir etsə də, müvafiq sahədə riski çox yüksək qiymətləndirən təşkilatlar əlavə aspektləri də qiymətləndirməli ola bilərlər.

Əgər baş audit icraçısı daxili audit funksiyasının Mövzu Əsaslı Tələb çərçivəsində vacib olan audit işlərini yerinə yetirmək üçün zəruri biliyə malik olmadığını müəyyən edərsə, bu işlər kənar xidmət təminatçısına həvalə edilə bilər (Standartlar 3.1 “Sərişte və Bacarıqlar”, 7.2 “Baş Audit İcraçısının İxtisas Tələbləri”, 10.2 “İnsan Resurslarının İdarə Olunması”). Standartlar təşkilatın daxili auditorları birbaşa işə götürməsindən, kənar xidmət təminatçısı vasitəsilə müqavilə bağlamasından və ya hər ikisindən asılı olmayaraq, daxili audit xidmətləri göstərən istənilən şəxsə və ya funksiyaya tətbiq edilir. Baş audit icraçısı standartlara uyğunluğun təmin olunması üzrə son məsuliyyəti öz üzərinə götürür. Bundan əlavə, baş audit icraçısı daxili audit resurslarının kifayət etmədiyini müəyyən etdikdə, resurs çatışmazlığının təsirləri və hər hansı resurs kəsirlərinin necə aradan qaldırılacağı barədə Şuranı məlumatlandırmalıdır (Standart 8.2 “Resurslar”).

İcra, Sənədləşdirmə və Hesabatlılıq

Mövzu Əsaslı Tələbləri tətbiq edərkən daxili auditorlar da Standartlara riayət etməli və işlərini V Fəsil: Daxili Audit Xidmətlərinin Göstərilməsi bölməsinə uyğun şəkildə aparmalıdırlar. V

Fəsildəki standartlar tapşırıqların planlaşdırılmasını (Prinsip 13: “Audit Tapşırıqlarının Səmərəli Planlaşdırılması”), icrasını (Prinsip 14: “Audit Tapşırıqlarının İcra Olunması”) və nəticələrinin təqdim olunmasını (Prinsip 15 “Audit Tapşırığının Nəticələri barədə Məlumatlandırma və Tədbirlər Planının Təqibi”) təsvir edir.

Mövzu Əsaslı Tələbin əhatəsi auditorların peşəkar mühakiməsinə əsasən daxili audit planında və ya tapşırıq üzrə iş proqramında sənədləşdirilə bilər. Bir və ya bir neçə daxili audit tapşırığı bu tələbləri əhatə edə bilər. Bundan əlavə, bütün tələblərin tətbiq oluna bilmədiyi hallar da mövcud ola bilər. Mövzu Əsaslı Tələbin tətbiqolunma imkanına görə qiymətləndirildiyinə dair sübutlar, eləcə də istənilən istisnaların əsaslandırmasını izah edən dəlillər saxlanmalıdır.

Əlavə C-dəki istifadəsi məcburi olmayan alət istinad mənbəyi kimi və daxili auditorların işini sənədləşdirmək üçün istifadə oluna bilər.

Keyfiyyət Təminatı

Standartlar baş audit icraçısından daxili audit funksiyasının bütün aspektlərini əhatə edən keyfiyyət təminatı və təkmilləşdirmə proqramı hazırlamağı, tətbiq etməyi və saxlamağı tələb edir (Standart 8.3 “Keyfiyyət”). Nəticələr Şuraya və yüksək rəhbərliyə bildirilməlidir. Təqdimatlar daxili audit funksiyasının Standartlara uyğunluğunu və performans hədəflərinə çatmasını hesabat şəklində əhatə etməlidir.

Keyfiyyət təminatı üzrə yoxlamaya hazırlaşmaq üçün daxili auditorlar Əlavə C-də təqdim olunan alətdən istifadə edə bilərlər.

Kibertəhlükəsizlik

Kibertəhlükəsizlik hər hansı bir təşkilatın əksər texnoloji aspektləri ilə bağlı olan geniş bir mövzudur. İnformasiya texnologiyalarına əlavə olaraq, kibertəhlükəsizlik adətən biznes proseslərinin bir hissəsi sayılır və bu, daxili auditorların əminlik təminatı tapşırıqlarını planlaşdırarkən, tapşırıqların əhatə dairəsini müəyyən edərkən və həyata keçirərkən kibertəhlükəsizliklə bağlı riskləri qiymətləndirmələrini tələb edir.

ABŞ Ticarət Departamentinin bir hissəsi olan Standartlar və Texnologiya üzrə Milli İnstitut (STMİ/NIST), kibertəhlükəsizliyin tərifini sadə formada “kiberməkanı kiberhücumlardan qorumaq və ya müdafiə etmək qabiliyyəti” kimi təsvir edir. Kibertəhlükəsizlik üzrə Mövzu əsaslı Tələb təşkilatların icazəsiz istifadəçilərdən və zərərli kiber təhdidlərdən yaranan riskləri azaltmaq üçün təmin etdikləri kənar perimetri əhatə 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 üzrə Mövzu Əsaslı Tələbə aşağıdakılar daxildir:

- **İdarəetmə** – təşkilatın missiya və vizyonunun reallaşdırılmasına dəstək verən, aydın şəkildə müəyyən edilmiş əsas kibertəhlükəsizlik məqsədləri və strategiyaları.

- **Risklərin idarə edilməsi** – kibertəhlükəsizliyə təhdidləri müəyyən etmək, təhlil etmək, idarə etmək və izləmək, eləcə də kibertəhlükəsizlik risklərini dərhal eskalasiya etmək üçün proseslər.
- **Nəzarət** – rəhbərlik tərəfindən müəyyən edilmiş, kibertəhlükəsizlik risklərinin təsirlərinin azaldılması üçün dövri olaraq qiymətləndirilən nəzarət prosesləri.

Nəzərə alınmalı məqamlar

Daxili auditorlar Kibertəhlükəsizlik üzrə Mövzu Əsaslı Tələbdəki vacib olan tələblərin qiymətləndirilməsində kömək məqsədilə aşağıdakı məqamları nəzərə ala bilərlər. Hər bir nəzərə alınmalı olan məqamın işarələnməsi Mövzu Əsaslı Tələbdəki müvafiq tələb ilə çarpaz istinad təşkil edir. Bu mülahizələr nümunə xarakterlidir, onların tətbiqi məcburi deyil. Daxili auditorlar qiymətləndirmələrinə nəyi daxil edəcəklərini müəyyən edərkən peşəkar mühakimələrinə əsaslanmalıdırlar.

İdarəetmə üzrə nəzərə alınmalı məqamlar

İdarəetmə proseslərinin dayanıqlılıq məqsədlərinə necə tətbiq olunduğunu qiymətləndirmək məqsədilə daxili auditorlar aşağıdakı dəlilləri nəzərdən keçirə bilərlər:

A. Rəsmi formada və sənədləşdirilmiş kibertəhlükəsizlik strateji planı və məqsədləri, o cümlədən informasiya təhlükəsizliyi funksiyasını yerinə yetirən funksional bölmənin rəhbəri, məsələn, baş informasiya təhlükəsizliyi məmuru (BİTM/CISO) tərəfindən təqdim olunan kibertəhlükəsizlik yeniləmələrini direktorlar şurasının dövri olaraq (adətən rübdə bir dəfə) nəzərdən keçirdiyinə dair sübutlar. Sübutlara aşağıdakı hesabatlar daxil edilə bilər:
    - Strateji məqsədlərin yerinə yetirilməsinin monitorinqi.
    - Kibertəhlükəsizlik məqsəd və vəzifələrini dəstəkləmək üçün maliyyə imkanlarının kifayət etməsi.
    - Risklərə və daxili nəzarət mexanizmlərinə, o cümlədən tədbirlər planının icrasının gedişinə diqqət yetirilməsi.
    - Uğuru ölçmək üçün əsas performans göstəriciləri (ƏPG/KPI).
    - Kibertəhlükəsizlik üzrə kadrların işə götürülməsi, təlim keçilməsi və inkişaf etdirilməsi üçün insan resurslarının mövcudluğu.
B. Kibertəhlükəsizlik proseslərini idarə etmək üçün istifadə olunan siyasətlər, prosedurlar və digər müvafiq sənədlər, o cümlədən:
    - İldə ən az bir dəfə nəzərdən keçirilən və yenilənən siyasətlər. Yaranan yeni kibertəhlükəsizlik riskləri təhlillərin və yeniləmələrin daha tez-tez aparılmasını tələb edə bilər.
    - Siyasətlərin və prosedurların kibertəhlükəsizlik əməliyyatlarını dəstəkləmək üçün kifayət edib-etmədiyini müəyyən edən prosesin mövcudluğu.
    - Kibertəhlükəsizlik proseslərini və daxili nəzarəti gücləndirmək üçün geniş şəkildə qəbul edilmiş çərçivələr (NIST, COBIT və digərləri).

C. Kibertəhlükəsizlik məqsədlərinə çatmağı dəstəkləyən rollar və məsuliyyətlər, o cümlədən kibertəhlükəsizlik funksiyasının təşkilat daxilində kifayət qədər görünənliyə malik bir səviyyəyə hesabat verməsini təmin edən təşkilati struktur.
    - Kibertəhlükəsizlik rollarını icra edən heyətin bilik, bacarıq və qabiliyyətlərinin dövri olaraq qiymətləndirilməsi prosesi.

D. Müvafiq maraqlı tərəflərlə (məsələn, yüksək rəhbərlik, əməliyyatlar, risk idarəçiliyi, insan resursları, hüquq, uyğunluq (komplayens), strateji təchizatçılar və digərləri) olan münasibətlərlə bağlı mövcud və yaranmaqda olan kibertəhlükəsizlik riskləri və məlum potensial zəifliklər barədə ünsiyyət də daxil olmaqla, əməkdaşlığın formalaşdığının sübutu. Ünsiyyətin qurulduğuna dair müvafiq sübutlara iclas protokolları, hesabatlar və ya elektron poçtlar daxil ola bilər.

Risklərin idarə edilməsi üzrə nəzərə alınmalı məqamlar

Nəzarət proseslərinin kibertəhlükəsizlik məqsədlərinə necə tətbiq olunduğunu qiymətləndirmək üçün daxili auditorlar aşağıdakı dəlilləri nəzərdən keçirə bilərlər:

A. Təşkilatın kibertəhlükəsizlik riskini necə qiymətləndirdiyini və idarə etdiyini, o cümlədən təhdidlərin və boşluqların hansı formada:
    - İlkin olaraq müəyyən edildiyi və bildirildiyi.
    - Təşkilati məqsədlərə çatmaq riskini qiymətləndirmək üçün təhlil edildiyi.
    - Riski qəbul edilə bilən səviyyəyə endirmək üçün tədbirlər planları da daxil olmaqla azaldıldığı.
    - Təhdidlər tam aradan qalxana qədər davamlı hesabat vermə planı da daxil olmaqla monitorinq edildiyi.

B. Təşkilatın informasiya texnologiyaları, təşkilati risklərin idarə edilməsi, insan resursları, hüquq, uyğunluq (komplayens), əməliyyatlar, mühasibatlıq və maliyyə kimi funksional sahələrdən kibertəhlükəsizlik risklərinin idarə edilməsi ilə bağlı dövri məlumatı necə əldə etməsi. Məlumat əldə etmək üçün funksiyalararası kibertəhlükəsizlik komandası və ya İT idarəetmə komitəsi formalaşdırıla bilər.

C. Təşkilat kibertəhlükəsizlik risklərinin idarə edilməsi üzrə hesabatlılığı və məsuliyyəti bir şəxsə və ya komandaya hansı formada həvalə etməsi.
    - Məsul şəxs(lər) təşkilat daxilində davam edən kibertəhlükəsizlik riskləri barədə yeniləmələri mütəmadi (rüblük, aylıq və ya ehtiyac olduqca) şəkildə çatdırmalı və lazım gəldikdə risklərin azaldılması strategiyaları üçün resurs tələblərini də bu təqdimatlara daxil etməlidir.

D. Kibertəhlükəsizlik risklərinin eskalasiya prosesləri, o cümlədən təhdid və ya risk səviyyəsinin necə qiymətləndirildiyi, təyin olunduğu və prioritetləşdirildiyi təhlilin aparılması. Təhlilə aşağıdakıların müəyyən edilməsi daxil edilə bilər:

- Təşkilatın müəyyən etdiyi risk səviyyələri – məsələn, yüksək, orta və aşağı – hər bir risk səviyyəsinin ətraflı izahı və hər bir risk kateqoriyası üçün eskalasiya prosedurları.
- Müəyyən edilmiş cari kibertəhlükəsizlik risklərinin siyahısı və hər bir risk hadisəsinin aradan qaldırılması üzrə vəziyyət.
- Müvafiq hüquqi, tənzimləyici və uyğunluq (komplayens) tələbləri.
- Riskin həm maliyyə, həm də qeyri-maliyyə (məsələn, nüfuz) təsirləri.

E. Rəhbərliyə və işçilərə kibertəhlükəsizlik risklərinin çatdırılması prosesi aşağıdakıları əhatə edir:

- Dövri olaraq (ən azı ildə bir dəfə) işçilər üçün kibertəhlükəsizlik təlimi, məsələn, təşkilati şüurun yoxlanılması və izlənməsi üçün əvvəlcədən xəbər verilməmiş, simulyasiya olunmuş fişinq kampaniyalarının keçirilməsi.
- Mövcud kibertəhlükəsizlik problemlərinin aradan qaldırılması üzrə yeniləmələr və gözlənilən tamamlanma tarixləri.
- Qeyri-uyğunluqların monitorinqi ilə bağlı direktorlar şurasına və yüksək rəhbərliyə təqdimatların keçirilməsi.
- Təşkilatın risk iştahası və risk dözümlülüyü dəyişdikdə təhdidlərin yenidən qiymətləndirilməsi.

F. Təşkilatın hadisələrə reaksiyası və onun nəticələrindən bərpa ilə bağlı həyata keçirdiyi proseslər bunlardır:

- Təşkilatın əməliyyatları zamanla dəyişdikcə nəzərdən keçirilən və yenilənən sənədləşdirilmiş plan. Plan aşağıdakıları əhatə etməlidir:
  - İnsidentlərin necə aşkarlandığı və bildirildiyi.
  - Daha çox zərərin qarşısını almaq üçün insidentlərin təsirinin necə məhdudlaşdırıldığı.
  - Təşkilatın əməliyyatları bərpa edib yenidən fəaliyyətə başlamaq üçün necə reaksiya verəcəyi və hansı tədbirləri görəcəyi.
  - Müvafiq insidentin, əldə olunan dərslərin müəyyən edilməsi və gələcəkdə bənzər hadisələrin qarşısın alınması məqsədilə necə təhlil ediləcəyi.
- Dövri olaraq (ən azı ildə bir dəfə) sınaq yoxlamalarının (masaüstü məşq) keçirilməsi və nəticələrin yüksək rəhbərliyə və müvafiq maraqlı tərəflərə hesabat şəklində təqdim edilməsi. Sınaq yoxlamaları nəticəsində tədbirlər planları yarana bilər.

Nəzarət prosesinin təşkili üzrə nəzərə alınmalı məqamlar

Nəzarət proseslərinin kibertəhlükəsizlik məqsədlərinə necə tətbiq olunduğunu qiymətləndirmək üçün daxili auditorlar aşağıdakı dəlilləri nəzərdən keçirə bilərlər:

A. Rəhbərliyin kibertəhlükəsizlik üzrə effektiv daxili nəzarət mühiti qurmaq üçün formalaşdırdığı yanaşma, o cümlədən:
   - Təşkilati risk qiymətləndirilməsi prosesinə əsaslanaraq yüksək risklərin azaldılması və həssas, kritik, şəxsi və ya məxfi məlumatları qorumaq məqsədilə tələb olunan daxili nəzarət mexanizmlərinin qiymətləndirilməsi və tətbiq edilməsi.
   - Kibertəhlükəsizlik üzrə əsas nəzarət mexanizmlərinin saxlanılması üçün resurs tələblərinin müəyyən edilməsi.
   - Təchizatçı əsaslı nəzarət mezanizmlərini nəzarət mühiti kimi nəzərə alaraq, bu çərçivədə işgüzar əlaqəyə başlamazdan əvvəl və əlaqənin müddəti boyunca təchizatçılardan xidmət təşkilatı üzrə nəzarət mexanizmləri (XTNM/SOC) hesabatlarını nəzərdən keçirmək.
   - Kibertəhlükəsizlik nəzarət mexanizmlərinin risklərin təsirlərini azaldan və kibertəhlükəsizlik məqsədlərinə çatmağı dəstəkləyən şəkildə işlədiyini təsdiq edən dövri sınaq yoxlamaları.
   - Daxili nəzarət çatışmazlıqlarının aradan qaldırılması və ya daxili audit funksiyası və ya digər əminlik təminatı verənlər tərəfindən aparılan qiymətləndirmələrin (məsələn, müdaxilə (penetrasiya) testi) nəticələrinin həll edilməsi prosesi.

B. Təşkilatın kibertəhlükəsizlik mütəxəssislərini işə qəbul etmək və onlara təlim keçmək üçün istedad idarəetmə prosesi, o cümlədən təşkilatın kiber təhlükəsizlik mütəxəssislərinin texniki biliklərini dəstəkləmək və yeni yaranan məsələlər barədə təşkilati məlumatlılığı artırmaq üçün imkanları necə müəyyən etməsi.
   - Məsələn, təlimlərdə iştirak, bilik mübadiləsi qruplarına cəlb olunma və kibertəhlükəsizlik sahəsinə aid sertifikatların əldə edilməsini əhatə edən davamlı peşə təhsilinin təmin olunması.

C. Rəhbərliyin gündəlik əməliyyatlara yönəlmiş, yaranan yeni kibertəhlükəsizlik təhdidlərini və boşluqlarını fasiləsiz şəkildə müəyyən etmə, prioritetləşdirmə, monitorinq və hesabat vermə prosesi. Təhlillər yeni və ya formalaşmaqda olan texnologiyalar, məsələn təhdidlərin və boşluqların qiymətləndirilməsi üçün süni intellektin istifadəsi ilə bağlı proseslərin formalaşdırılmasını əhatə edə bilər.

D. Rəhbərliyin İT aktivlərini həyat dövrü boyunca idarə etmək və qorumaq üçün müəyyən etdiyi proseslər və nəzarət mexanizmləri, o cümlədən avadanlıq, proqram təminatı və təchizatçı xidmətlərinin seçilməsi, istifadəsi, texniki qulluq və istismardan çıxarılması. Avadanlıqlar serverləri, şəbəkə avadanlıqlarını (məsələn, marşrutlaşdırıcılar (ruter) və ya şəbəkələrarası ekranlar (firewall)), masaüstü kompüterlər, noutbuklar, mobil telefonlar, planşetlər və periferik qurğuları əhatə edir. Proqram təminatları əməliyyat sistemlərini (məsələn, Windows), müəssisə resurslarının planlaşdırılması proqramını, tətbiqləri, antivirus proqramlarını və digər proqramları əhatə edir. Avadanlıqlar və proqram təminatları ilə bağlı nəzərə alınmalı məqamlar bunlardır:
   - Təşkilatın şifrələmə, antivirus proqram təminatı, mobil cihazların idarə edilməsi, mürəkkəb şifrə tələbləri, autentifikasiya üçün virtual özəl şəbəkə (VÖŞ/VPN)/sıfır etibar şəbəkələşməsi (SEŞ/ZTN) və mikroproqram təminatının (firmware) dövri yenilənməsindən istifadə etməsi.

- Təşkilat tərəfindən verilən cihazların təqdim edilməsi zamanı müvafiq təhlükəsizlik konfiqurasiyasına malik olmasını və aktivlərin istifadədən çıxarılması və silinməsi zamanı düzgün utilizasiya olunmasını təmin edən aktivlərin idarə edilməsi prosesinin mövcudluğu.
- Verilənlər bazası ilə bağlı nəzarət tədbirləri: istifadəçi və administrator girişinin məhdudlaşdırılması, şifrələmədən istifadənin təmin edilməsi, verilənlər bazalarının ehtiyat nüsxəsinin yaradılması və sınaq yoxlamalarından keçirilməsi, eləcə də şəbəkə təhlükəsizliyi üzrə güclü nəzarət mexanizmlərinin mövcudluğu.
- Sistem qurulmasının həyat dövründə (SQHD/SDLC) kibertəhlükə və boşluqların necə nəzərə alınması.
- Proqram Təminatının Təhlükəsizlik Əməliyyatları (DevSecOps) çərçivəsində proqram təminatının hazırlanması prosesinə kibertəhlükəsizliyi proaktiv şəkildə boşluqları müəyyən etmək üçün daxil edən yanaşmanın formalaşması.

E. Kibertəhlükəsizliyi gücləndirmək üçün istifadə olunan proseslər, o cümlədən:
- Kibertəhlükəsizlik risklərini minimuma endirmək üçün təhlükəsizlik parametrlərinin konfiqurasiyası.
- Mobil cihaz inzibatçılığının (o cümlədən elektron poçt və tətbiqlərin istifadəsi) kibertəhlükəsizlik risklərini azaltmaq və istifadəçinin cihazları ələ keçirildikdə uzaqdan idarə etmək üçün tənzimlənilməsi.
- Məlumatın “saxlanarkən” (məsələn, sərt diskdə yadda saxlanılan məlumat) və ya “daşıma zamanı” (məsələn elektron poçtların göndərilməsi) şifrələnməsi.
- Serverləri və ya proqram təminatlarını (məsələn, əməliyyat sistemini) ən son təhlükəsizlik yeniləmələri ilə təmin etmək.
- Çoxfaktorlu autentifikasiya (ÇFA/MFA) və unikal istifadəçi adları kimi texnikaları əhatə edən, eləcə də mütəmadi olaraq müddəti bitən və mürəkkəb şifrələrin istifadəsini ehtiva edən istifadəçi girişinin idarə edilməsi prosesi.
- Əlçatanlığın və resurslardan istifadə səviyyəsinin kifayət qədər adekvat işlədiyini müəyyən etmək üçün tətbiq edilmiş nəzarət mexanizmləri, fəaliyyət göstəriciləri üçün təhlükə yarada biləcək potensial kibertəhlükəsizlik problemlərinin nəzərdən keçirilməsinə və təhlilinə imkan verir.
- Proqram təminatı istehsal prosesinə köçürülməzdən əvvəl kibertəhlükəsizlik boşluqlarını müəyyən etmək və aradan qaldırmaq üçün kibertəhlükəsizlik proseslərinin “SQHD/SDLC”-yə inteqrasiyası.

F. Təşkilatın perimetrini təmin edən şəbəkə ilə əlaqəli nəzarət mexanizmlərinin, o cümlədən aşağıdakıların istifadə edilmə tərzi:
- Şəbəkə seqmentasiyası.
- Şəbəkələrarası ekranlar (firewall).
- İstifadəçi səlahiyyətlərinə nəzarətlər.
- Həm kənar, həm də daxili bağlantılarda məhdudiyyətlər.

- Bir-biri ilə əlaqəli şəbəkələr üçün Əşyaların İnterneti (Əİ/IoT) ətrafındakı nəzarət mexanizmləri.
- Kiberhücumların qarşısını almaq, onları aşkarlamaq və onların təsirlərindən bərpa olmaq üçün müdaxilənin aşkarlanması/qarşısının alınması sistemləri.

G. Elektron poçt, internet brauzerləri, video konfrans, mesajlaşma (Zoom, MS Teams və digərləri), sosial media, bulud və fayl paylaşma protokolları kimi xidmətlərə aid son nöqtə kommunikasiyalarının təhlükəsizliyinə nəzarət mexanizmləri. Nəzarət tədbirləri müəyyən fayl uzantılarının (məsələn, ".exe" faylları) istifadəsinin məhdudlaşdırılmasını və fayl paylaşımı üçün çoxfaktorlu autentifikasiyanın istifadəsini əhatə edə bilər.

Əlavə A. Praktiki Tətbiq Nümunələri

Aşağıdakı nümunələr Kibertəhlükəsizlik Mövzu əsaslı Tələbin tətbiq oluna biləcəyi ssenariləri təsvir edir:

Nümunə 1: Kibertəhlükəsizlik daxili audit planına daxil edilmiş daxili audit yoxlaması çərçivəsində nəzərdə tutulmuşdur.

Daxili audit funksiyası risk əsaslı planlaşdırma prosesini tamamlayıb daxili audit planına kibertəhlükəsizlik üzrə bir və ya bir neçə yoxlama tapşırığını daxil etdikdə, bu yoxlama tapşırıqlarını icra edərkən Mövzu əsaslı Tələb mütləq nəzərə alınmalıdır. Uyğunluq daxili audit planına bir və ya bir neçə tapşırıq üzrə tələbləri daxil etməklə əldə edilə bilər.

Kibertəhlükəsizlik geniş mövzudur və Mövzu Əsaslı Tələbdəki göstərilmiş hər bir məqam bütün tapşırıqların icrası zamanı tətbiq olunmaya bilər. Daxili auditorlar peşəkar mühakiməni tətbiq edərək Kibertəhlükəsizlik üzrə Mövzu Əsaslı Tələbin bir və ya bir neçə tələbinin aktual olmadığını və buna görə də tapşırığın əhatə dairəsindən çıxarılmalı olduğunu müəyyən etdikdə, həmin tələblərin kənarlaşdırılması üçün əsaslandırmanı sənədləşdirib saxlamalıdırlar. Məsələn, bəzi tələblərin istisna edilməsinin əsaslandırılması üçün əsas olaraq, daxili audit funksiyasının müxtəlif kibertəhlükəsizlik fəaliyyətlərini növbəlilik əsasında yoxlaması və ya bu tapşırıq üzrə kibertəhlükəsizlik riskinin əhəmiyyətinin aşağı olduğunu müəyyən edildiyi halları göstərmək olar.

Nümunə 2: Kibertəhlükəsizlik riskləri kibertəhlükəsizlik proseslərini əhatə etməyən audit yoxlaması zamanı müəyyən edilmişdir.

Daxili auditorlar birbaşa kibertəhlükəsizliyə aid olmayan prosesi qiymətləndirərkən kibertəhlükəsizliklə bağlı riskləri müəyyən edə bilərlər. Məsələn, daxili auditorlar kibertəhlükəsizlik proseslərini əhatə etməyən yoxlama çərçivəsində kreditor borcları üzrə prosesləri qiymətləndirə və yoxlamanı planlaşdırarkən kibertəhlükəsizlik risklərini əhatə dairəsinə daxil etməyə bilərlər. Buna baxmayaraq, ilkin yoxlama prosesini həyata keçirdikdən sonra daxili auditorlar bu risklərin yoxlama çərçivəsinə daxil olduğunu müəyyən etdikdə, məsələn, internet üzərindən ilkin satınalma sorğusunun verilməsi prosesi ilə bağlı kibertəhlükəsizlik riskləri aşkar oluna bilər (Standart 13.2 “Audit Tapşırığı Çərçivəsində Risklərin Qiymətləndirilməsi”).

Müvafiq risklər müəyyən edildikdən sonra daxili auditorlar Kibertəhlükəsizlik üzrə Mövzu Əsaslı Tələbi nəzərdən keçirməli və hansı tələblərin tətbiq olunmasının zəruri olduğunu müəyyən etməlidirlər. Bu halda onlar kibertəhlükəsizlik üzrə risk idarəetmə və nəzarət tələblərini istisna edə bilərlər. Onlar yoxlama tapşırığı üzrə iş sənədlərində Kibertəhlükəsizlik üzrə Mövzu Əsaslı Tələbin digər müddəalarının istisna edilməsinin əsaslandırmasını sənədləşdirməli və həmin sənədləri müvafiq qaydada saxlamalıdırlar.

Nümunə 3: Əvvəldən daxili audit planına daxil edilməmiş kibertəhlükəsizliklə bağlı bir fəaliyyətin həyata keçirilməsi tələb olunmuşdur.

Maraqlı tərəflər, məsələn, Şura, rəhbərlik və ya tənzimləyici orqan daxili auditorlardan ilkin audit planından kənar kibertəhlükəsizlik qiymətləndirmələri aparmağı xahiş edə bilərlər. Məsələn, təşkilatlar kiberhücumun hədəfi olduqda, Şura kibertəhlükəsizlik nəzarət mexanizmlərini yoxlamaq məqsədilə daxili audit tapşırığının icra edilməsini tələb edə bilər. Bu zaman Mövzu Əsaslı Tələb tətbiq olunmalı, tələblər qiymətləndirilməli və istisnalar sənədləşdirilməlidir.

Əlavə B. Çərçivələrlə Əlaqələndirmə

Təşkilat kibertəhlükəsizliklə bağlı öz tədbirlərini “COBIT” və ya “NIST” kimi müvafiq çərçivələrdən istifadə etməklə həyata keçirə bilər. Daxili auditorlar artıq bu çərçivələrə əsaslanaraq audit proqramları və test prosedurları hazırlamış ola bilərlər. Daxili auditorlar kifayət qədər əhatəni təmin etmək üçün nəzərdə tutulan kibertəhlükəsizlik üzrə mövcud olan nəzarət mexanizmlərinin sınaq testlərini Mövzu Əsaslı Tələb ilə uzlaşdırmalıdırlar. Aşağıdakı cədvəl Kibertəhlükəsizlik üzrə Mövzu Əsaslı Tələbi ən çox istifadə olunan üç çərçivəyə uyğunlaşdırır: NIST Kibertəhlükəsizlik Çərçivəsi 2.0, COBIT 2019 və NIST 800-53. Bu çərçivələrin geniş istifadəçi auditoriyası üçün əlçatanlığını nəzərə alaraq əlavə istinadlar aşağıdakı şəkildə təqdim olunmuşdur.

İdarəetmə tələbləri	Çərçivələrə istinadlar		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Rəsmi şəkildə kibertəhlükəsizlik strategiyası və məqsədləri müəyyən edilir və mütəmadi olaraq yenilənir. Kibertəhlükəsizlik məqsədlərinin yerinə yetirilməsi ilə bağlı yeniləmələr, kibertəhlükəsizlik strategiyasını dəstəkləmək üçün resurslar və büdcə məsələləri daxil olmaqla, mütəmadi olaraq direktorlar şurasına çatdırılır və müvafiq təhlillər aparılır.	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
B. Kiber təhlükəsizliklə bağlı siyasətlər və prosedurlar müəyyən edilir, mütəmadi yenilənir və nəzarət mühiti gücləndirilir.	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
C. Kibertəhlükəsizlik məqsədlərini dəstəkləyən rollar və məsuliyyətlər müəyyən edilir, bu rolları icra edənlərin bilik, bacarıq və qabiliyyətlərini mütəmadi qiymətləndirmək üçün proses mövcuddur.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. Kibertəhlükəsizlik mühitində mövcud boşluqları 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.	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
Risk idarəetməsi tələbləri	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Təşkilatın risk qiymətləndirilməsi və risk idarəetmə proseslərinə kibertəhlükəsizlik təhdidlərinin müəyyən edilməsi, təhlili, azaldılması və monitorinqi, eləcə də onların strateji məqsədlərə çatmaqda olan təsirinin qiymətləndirilməsi daxildir.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. Kibertəhlükəsizlik risklərinin idarə edilməsi təşkilat üzrə həyata keçirilir və aşağıdakı sahələri əhatə edə bilər: informasiya texnologiyaları, müəssisə risklərinin idarə edilməsi, insan resursları, hüquq, uyğunluq (komplayens), əməliyyatlar, təchizat zənciri, mühasibatlıq, maliyyə və digərləri.	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
C. Kibertəhlükəsizlik risklərinin idarə edilməsinə görə hesabatlılıq və məsuliyyət müəyyən edilir və kibertəhlükəsizlik risklərinin necə idarə olunduğunu, risklərin təsirlərini azaltmaq üçün tələb olunan resursları və ortaya çıxan kibertəhlükələri müəyyən etmək, mütəmadi olaraq izləmək və hesabat vermək üçün bir fərd və ya komanda təyin olunur.	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

D. Təşkilatın müəyyən etdiyi risklərin idarə edilməsi qaydalarına əsasən qəbuledilməz səviyyəyə çatmış (yeni yaranan və ya əvvəlcədən müəyyən edilmiş) istənilən kibertəhlükəsizlik riskini dərhal eskalasiya etmək üçün bir proses müəyyən edilir və ya tətbiq olunan hüquqi və tənzimləyici tələblərə əməl etmək üçün müəyyən edilmiş proses icra olunur. Kibertəhlükəsizlik riskinin həm maliyyə, həm də qeyri-maliyyə təsirləri nəzərə alınmalıdır.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Rəhbərliyə və işçilərə kibertəhlükəsizlik riskləri barədə məlumat vermək, habelə rəhbərlik tərəfindən problemlər, boşluqlar, çatışmazlıqlar və ya nəzarət uğursuzluqları üzrə hesabat hazırlamaq və onları aradan qaldırmaq üçün dövri olaraq təhlil prosesini təmin etmək üçün prosedur müəyyən edilir.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. Təşkilat aşkarlanma, məhdudlaşdırma, bərpa və insidentdən sonrakı təhlili əhatə edən kibertəhlükəsizlik hadisələrinə reaksiya və bərpa prosesini tətbiq edir. İnsidentlərə reaksiya və bərpa prosesi mütəmadi olaraq yoxlanılır.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Nəzarət prosesi tələbləri	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Təşkilatın sistemlərinin və məlumat bazalarının məxfiliyinin, tamlığının və əlçatanlığının qorunmasını təmin etmək üçün həm daxili nəzarət mexanizmlərinin, həm də təchizatçı əsaslı nəzarət mexanizmlərinin mövcudluğunu təmin edən proses müəyyən edilir. Nəzarət mexanizmləri təşkilati kibertəhlükəsizlik məqsədlərinin reallaşdırılmasını və problemlərin vaxtında həllini təşviq edəcək şəkildə işlədiklərini müəyyən etmək üçün mütəmadi olaraq dəyərləndirilir.	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

B. Kibertəhlükəsizlik əməliyyatları üçün texniki səriştələri inkişaf etdirmək və saxlamaq məqsədilə təlim imkanları da daxil olmaqla, istedad idarəetmə prosesi yaradılır və mütəmadi olaraq nəzərdən keçirilir.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Yaranan kibertəhlükəsizlik təhdidlərini və zəifliklərini davamlı şəkildə izləmək və hesabat vermək, eləcə də kibertəhlükəsizlik əməliyyatlarını təkmilləşdirmək üçün imkanları müəyyən etmək, prioritetləşdirmək və həyata keçirmək məqsədilə proses yaradılır.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Kibertəhlükəsizlik bütün İT aktivlərinin (avadanlıq, proqram təminatı və təchizatçı xidmətləri də daxil olmaqla) həyat dövrü idarəçiliyinə (seçim, istifadə, texniki qulluq və istismardan çıxarılma) daxil edilir.	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
E. Kibertəhlükəsizliyi təşviq etmək üçün konfiqurasiya, son istifadəçi cihazlarının idarə edilməsi, şifrələmə, yamaqlama, istifadəçi səlahiyyətlərinin idarə edilməsi və əlçatanlıq və faəliyyətin monitorinqi də daxil olmaqla müvafiq proseslər müəyyən edilmişdir. Proqram təminatının hazırlanmasında kibertəhlükəsizlik məsələləri (DevSecOps) nəzərə alınır.	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
F. Şəbəkə ilə bağlı idarəetmə tədbirləri müəyyən edilmişdir, 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).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02

G. 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.	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

Əlavə C. Könüllü sənədləşdirmə aləti

Daxili auditorlardan, tələblərin tətbiqolunma imkanını risk qiymətləndirməsinə əsaslanaraq müəyyən etdikdə peşəkar mühakimə yürütmələri və bəzi tələblərin istisnalarını müvafiq şəkildə sənədləşdirmələri gözlənilir. Mövzu Əsaslı Tələb auditorun peşəkar mühakiməsinə əsasən daxili audit planında və ya yoxlama tapşırığı üzrə iş sənədlərində rəsmiləşdirilə bilər. Bir və ya bir neçə daxili audit tapşırığı bu tələbləri əhatə edə bilər. Bundan əlavə, bütün tələblərin tətbiq olunması mümkün olmayan tapşırıqlar da ola bilər. Bu çap edilə bilən forma Kibertəhlükəsizlik üzrə Mövzu Əsaslı Tələbə uyğunluğu sənədləşdirmək üçün bir seçim təqdim edir, lakin onun istifadəsi məcburi deyil.

Kibertəhlükəsizlik – İdarəetmə

Tələb	İcra edilən elementlərin əhatəsi və ya istisna üçün əsaslandırma	Sənədləşdirməyə istinad
A. Rəsmi şəkildə kibertəhlükəsizlik strategiyası və məqsədləri müəyyən edilir və mütəmadi olaraq yenilənir. Kibertəhlükəsizlik məqsədlərinin yerinə yetirilməsi ilə bağlı yeniləmələr, kibertəhlükəsizlik strategiyasını dəstəkləmək üçün resurslar və büdcə məsələləri daxil olmaqla, mütəmadi olaraq direktorlar şurasına çatdırılır və müvafiq təhlillər aparılır.		
B. Kibertəhlükəsizliklə bağlı siyasətlər və prosedurlar müəyyən edilir, mütəmadi yenilənir və nəzarət mühiti gücləndirilir.		
C. Kibertəhlükəsizlik məqsədlərini dəstəkləyən rollar və məsuliyyətlər müəyyən edilir, bu rolları icra edənlərin bilik, bacarıq və qabiliyyətlərini mütəmadi qiymətləndirmək üçün proses mövcuddur.		
D. Kibertəhlükəsizlik mühitində mövcud boşluqları və yeni 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.		

Kibertəhlükəsizlik – Risklərin İdarə Edilməsi

Tələb	İcra edilən elementlərin əhatəsi və ya istisna üçün əsaslandırma	Sənədləşdirməyə istinad
A. Təşkilatın risk qiymətləndirilməsi və risk idarəetmə proseslərinə kibertəhlükəsizlik təhdidlərinin müəyyən edilməsi, təhlili, azaldılması və monitorinqi, eləcə də onların strateji məqsədlərə çatmaqda olan təsirinin qiymətləndirilməsi daxildir.		
B. Kibertəhlükəsizlik risklərinin idarə edilməsi təşkilat üzrə həyata keçirilir və aşağıdakı sahələri əhatə edə bilər: informasiya texnologiyaları, müəssisə risklərinin idarə edilməsi, insan resursları, hüquq, uyğunluq (komplayens), əməliyyatlar, təchizat zənciri, mühasibatlıq, maliyyə və digərləri.		
C. Kibertəhlükəsizlik risklərinin idarə edilməsinə görə hesabatlılıq və məsuliyyət müəyyən edilir və kiber təhlükəsizlik risklərinin necə idarə olunduğunu, riskləri azaltmaq üçün tələb olunan resursları və ortaya çıxan kibertəhlükələri müəyyən etmək, mütəmadi olaraq izləmək və hesabat vermək üçün bir fərd və ya komanda təyin olunur.		

Tələb	İcra edilən elementlərin əhatəsi və ya istisna üçün əsaslandırma	Sənədləşdirməyə istinad
D. Təşkilatın müəyyən etdiyi risklərin idarə edilməsi qaydalarına əsasən qəbuledilməz səviyyəyə çatmış (yeni yaranan və ya əvvəlcədən müəyyən edilmiş) istənilən kibertəhlükəsizlik riskini dərhal eskalasiya etmək üçün bir proses müəyyən edilir və ya tətbiq olunan hüquqi və tənzimləyici tələblərə əməl etmək üçün müəyyən edilmiş proses icra olunur. Kibertəhlükəsizlik riskinin həm maliyyə, həm də qeyri-maliyyə təsirləri nəzərə alınmalıdır.		
E. Rəhbərliyə və işçilərə kibertəhlükəsizlik riskləri barədə məlumat vermək, habelə rəhbərlik tərəfindən problemlər, boşluqlar, çatışmazlıqlar və ya nəzarət uğursuzluqları üzrə hesabat hazırlamaq və onları aradan qaldırmaq üçün dövri olaraq təhlil prosesini təmin etmək üçün prosedur müəyyən edilir.		
F. Təşkilat aşkarlanma, məhdudlaşdırma, bərpa və insidentdən sonrakı təhlili əhatə edən kibertəhlükəsizlik hadisələrinə reaksiya və bərpa prosesini tətbiq edir. İnsidentlərə reaksiya və bərpa prosesi mütəmadi olaraq yoxlanılır.		

Kibertəhlükəsizlik – Nəzarət Mexanizmləri

Tələb	İcra edilən elementlərin əhatəsi və ya istisna üçün əsaslandırma	Sənədləşdirməyə istinad
A. Təşkilatın sistemlərinin və məlumat bazalarının məxfiliyinin, tamlığının və əlçatanlığının qorunmasını təmin etmək üçün həm daxili nəzarət mexanizmlərinin, həm də təchizatçı əsaslı nəzarət mexanizmlərinin mövcudluğunu təmin edən proses müəyyən edilir. Nəzarət mexanizmləri təşkilati kibertəhlükəsizlik məqsədlərinin reallaşdırılmasını və problemlərin vaxtında həllini təşviq edəcək şəkildə işlədiklərini müəyyən etmək üçün mütəmadi olaraq dəyərləndirilir.		
B. Kibertəhlükəsizlik əməliyyatları üçün texniki səriştələri inkişaf etdirmək və saxlamaq məqsədilə təlim imkanları da daxil olmaqla, istedad idarəetmə prosesi yaradılır və mütəmadi olaraq nəzərdən keçirilir.		
C. Yeni yaranan kibertəhlükəsizlik təhdidlərini və zəifliklərini davamlı şəkildə izləmək və hesabat vermək, eləcə də kibertəhlükəsizlik əməliyyatlarını təkmilləşdirmək üçün imkanları müəyyən etmək, prioritetləşdirmək və həyata keçirmək məqsədilə proses yaradılır.		
D. Kibertəhlükəsizlik bütün İT aktivlərinin (avadanlıq, proqram təminatı və təchizatçı xidmətləri də daxil olmaqla) həyat dövrü idarəçiliyinə (seçim, istifadə, texniki qulluq və istismardan çıxarılma) daxil edilir.		

Tələb	İcra edilən elementlərin əhatəsi və ya istisna üçün əsaslandırma	Sənədləşdirməyə istinad
E. Kibertəhlükəsizliyi təşviq etmək üçün konfiqurasiya, son istifadəçi cihazlarının idarə edilməsi, şifrələmə, yamaqlama, istifadəçi girişlərinin idarə edilməsi və əlçatanlıq və faəliyyətin monitorinqi də daxil olmaqla müvafiq proseslər müəyyən edilir. Proqram təminatının hazırlanmasında kibertəhlükəsizlik məsələləri (DevSecOps) nəzərə alınır.		
F. Şəbəkə ilə bağlı idarəetmə tədbirləri müəyyən edilmişdir, 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).		
G. 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.

Məsuliyyətdən imtina

Daxili Auditorlar İnstitutu (“IIA”) bu sənədi məlumat və tədris məqsədləri ilə dərc etmişdir. Bu material müəyyən fərdi hallara dair qəti cavablar vermək üçün nəzərdə tutulmayıb və buna görə də yalnız təlimat kimi istifadə olunmaq məqsədi daşıyır. Daxili Auditorlar İnstitutu (“IIA”) hər bir konkret vəziyyətlə bağlı birbaşa olaraq müstəqil ekspertdən məsləhət almağı tövsiyə edir. Daxili Auditorlar İnstitutu (“IIA”) yalnız bu materiala əsaslanaraq və güvənərək qərar vermiş hər hansı bir şəxsə görə heç bir məsuliyyət daşımır.

Müəllif hüquqları

© 2026 Daxili Auditorlar İnstitutu (“IIA”). Bütün hüquqlar qorunur. Bu sənədi istənilən formada çoxaltmaq üçün icazənin əldə edilməsi ilə bağlı copyright@theiia.org elektron poçt ünvanı vasitəsilə əlaqə saxlamanız xahiş olunur.

Fevral 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