Təşkilati Dayanıqlılıq (Topical Requirement)

Mövzü Əsaslı Tələb İstifadə üzrə Təlimat

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 (Standart 4.1 "Qlobal Daxili Audit Standartlarına Uyğunluq") 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. Daxili Audit Mandatı daxili audit funksiyası tərəfindən həyata keçirilən xidmətlərin həcmini və növlərini, eləcə də Mövzu Əsaslı Tələblərin (Standart 6.1 "Daxili Auditin Mandatı") nəzərə alınması zərurətini aydın şəkildə müəyyən edir. 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. İdarəetmə 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 (Audit planındakı dəyişikliklərlə bağlı Standart 9.4-ə baxın).

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 və yoxlama məqsədlərinə çatmaq üçün zəruri resursları (Standart 13.5 “Audit Tapşırığının İcrası üçün Tələb Olunan Resurslar”) müəyyən edirlər. Əlavə A, “Tətbiq Senariləri”, daxili auditorların Mövzu Əsaslı Tələbdən necə istifadə etməli olduğunu təsvir edir.

Hər bir fərdi tələb hər bir tapşırığa aid olmaya bilər və bəzi tapşırıqlar digər yanaşmalar vasitəsilə yerinə yetirilə bilər. 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.

Standartlara uyğunluq keyfiyyət qiymətləndirmələri zamanı dəyərləndirilməlidir. Mövzu Əsaslı Tələbə riayət edilməsi Standart 14.6 “Audit Tapşırığının Sənədləşdirilməsi”-də təsvir edildiyi kimi auditorların peşəkar mühakiməsindən istifadə etməklə sənədləşdirilməlidir.

Təşkilati Dayanıqlılıq 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 “Səriştə və Bacarıqlar”, 7.2 “Baş Audit İcraçısının İxtisas Tələbləri”, 10.2 “İnsan Resurslarının İdarə Olunması”). Baş audit icraçıları DAİ-nin Daxili Audit Səriştələri Çərçivəsindən ™ istifadə edərək fayda əldə edə bilərlər. 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 Tələblər ardıcıl və yüksək keyfiyyətli daxili audit praktikasını dəstəkləmək üçün nəzərdə tutulmuşdur. Onlar müvafiq yerli qanunvericilik, normativ aktlar, nəzarət orqanlarının tələbləri və digər peşəkar səviyyədə tanınmış çərçivələrlə birlikdə tətbiq edilməlidir; bu çərçivələr əlavə və ya daha konkret tələblər irəli sürə bilər. Daxili auditorlar artıq bu tənzimləmələrə və çərçivələrə əsaslanaraq tapşırıq üzrə iş proqramlarını və test prosedurlarını hazırlamış ola bilərlər. Daxili auditorlar yetərli həcmdə əhatəni təmin etmək üçün nəzərdə tutulan təşkilati dayanıqlılıq nəzarət testlərini və digər daxili və kənar əminlik təminatçıları tərəfindən təqdim olunan istənilən etibarlı testləri (Standart 9.5 "Koordinasiya və Etimad") Mövzu Əsaslı Tələblərə uyğunlaşdırmalıdırlar.

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 D-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", Standart 8.4 "Kənar Keyfiyyət Qiymətləndirməsi", Standart 12.1 "Daxili Keyfiyyət Qiymətləndirməsi"). Nəticələr Şuraya və yüksək rəhbərliyə bildirilməlidir. Təqdimatlar daxili audit funksiyasının Standartlara uyğunluğunu və performans hədəflərinə çatmasını hesabat şəklində əhatə etməlidir.

Mövzu Əsaslı Tələblərə uyğunluq, tapşırıq səviyyəsində aparılan nəzarət fəaliyyətləri zamanı (Standart 12.3: "Audit Tapşırıqlarının İcrasına Nəzarət və Təkmilləşdirilməsi") nəzərə alınmalı və keyfiyyət qiymətləndirmələrində dəyərləndirilməlidir. Keyfiyyət təminatı üzrə yoxlamaya hazırlaşmaq üçün daxili auditorlar Əlavə D-də təqdim olunan alətdən istifadə edə bilərlər.

Təşkilati Dayanıqlılıq

Təşkilati dayanıqlılıq bir təşkilatın dəyişikliklərə, xüsusən də qeyri-sabit dövrlərdə müqavimət göstərmək və onlara uyğunlaşmaq qabiliyyətidir. Beynəlxalq Standartlaşdırma Təşkilatının ISO 22316 çərçivəsində qeyd edildiyi kimi bu, "təşkilatın dəyişən mühitdə təsirləri neytrallaşdırmaq və dəyişikliyə uyğunlaşmaq qabiliyyəti" kimi müəyyən edilir. Bu tərif ideal bir vəziyyət müəyyən etsə də, praktikada müxtəlif təşkilatlar dəyişiklikləri və fəaliyyətin pozulmasını qabaqcadan görməkdə, onlara cavab verməkdə, uyğunlaşmaqda və öz mövqelərini bərpa etməkdə kifayət qədər fərqli davranırlar. Təşkilati dayanıqlılıq strateji, əməliyyat, texnoloji, insan, sosial və maliyyə aspektlərini əhatə etdiyindən, bəzi təşkilatlar dəyişiklikləri effektiv şəkildə mənimsəyə bilir, digərləri isə buna uyğunlaşmaqda çətinlik çəkir və ya qeyri-müəyyənlik şəraitində fərqli yanaşmalar seçə bilərlər.

Praktiki baxımdan, dayanıqlı təşkilatlar gözlənilməz çağırışlardan sağ çıxmaq və belə çağırışlarla üzləşdikdə inkişaf edib uğur qazanmaq üçün daha əlverişli vəziyyətdə olurlar.

Aşağıda qeyd edilmiş, lakin bunlarla məhdudlaşmayan bir çox fəaliyyətin pozulması halları təşkilatın strateji məqsəd və vəzifələrinə çatmasını əngəlləyə bilər:

- Zəlzələlər, yanğınlar, daşqınlar, qasırğalar, sunamilər, tropik fırtınaları və digər ekstremal hava hadisələri kimi təbii fəlakətlər.
- Rəqəmsal məlumatların girov götürülməsi (ransomware), zərərli proqram, xidmətdən imtina hücumları, məlumat sızmaları, daxili təhdidlər kimi kiberhücumlar və təşkilata zərər vermək və ya onun əməliyyatlarını əngəlləmək məqsədilə həyata keçirilən digər bəd niyyətli hərəkətlər.
- Geosiyasi münaqişələr, məsələn iqtisadi sanksiyalar, tariflər, terrorizm, müharibə və dövlətlər arasındakı digər münaqişələr.
- Ətraf mühitin formalaşdırdığı təzyiqlər, məsələn, resurs çatışmazlığı, ictimai səhiyyə böhranları, davamlılıq amilləri və ya iqlim dəyişikliyi.
- Dəyişən xarici amillər, məsələn, inkişaf edən texnologiyaya (o cümlədən süni intellekt), uyğunluq tələblərindəki dəyişikliklər (hüquqi, tənzimləyici və maliyyə hesabatlılığı), məşğulluq səviyyələri, istehlakçı tələbatı və işgüzar nüfuz.
- İnflyasiya və ya deflyasiya, faiz dərəcələri, valyuta məzənnələri və tənəzzül və ya iqtisadi böyümə kimi mövcud bazar şəraiti də daxil olmaqla, maliyyə çağırışları.
- Əməliyyatlarla bağlı çağırışlar, məsələn, mürəkkəb proseslər, üçüncü tərəflərdən yüksək dərəcədə asılılıq, coğrafi mövqe, mədəni çağırışlar, işçi qüvvəsinin məhdudluğu və səmərəsiz rəhbərlik və ya risk idarəçiliyi.
- Təchizat zənciri problemləri, məsələn, xammal əldə etməkdə çətinlik, çeşidli təchizatçıların azlığı və əmtəə qiymətlərinin dəyişkənliyi.
- Daxili hadisələr, məsələn, əsas əməkdaşların işdən ayrılması və əməliyyat xətaları.

Fəaliyyətin pozulmasına səbəb olan hadisənin mahiyyəti dəyişə bilər, lakin təşkilatda davamlı olaraq dəyişiklikləri qabaqcadan görmək, onlara hazırlaşmaq, cavab vermək və uyğunlaşmaq üçün yaxşı müəyyən edilmiş dayanıqlılıq strategiyası və rəsmi proses və prosedurlar olmalıdır. Təşkilati dayanıqlılıq kompleks anlayışdır və strategiya təşkilatdan asılı olaraq biznesin davamlılığı, fəlakətdən bərpa, kritik funksiya matrisləri, varislik planları və bərpa testləri kimi müxtəlif komponentləri əhatə edə bilər.

Təşkilati Dayanıqlılıq üzrə Mövzu Əsaslı Tələbə aşağıdakılar daxildir:

- **İdarəetmə** – təşkilatın missiya və vizyonunun reallaşdırılmasına dəstək verən, aydın şəkildə müəyyən edilmiş əsas dayanıqlılıq məqsədləri və strategiyaları.
- **Risklərin idarə edilməsi** – dayanıqlılığa təhdidləri müəyyən etmək, təhlil etmək, idarə etmək və izləmək, eləcə də dayanıqlılıq hadisələrini dərhal yüksək səviyyəyə çatdırmaq üçün proseslər.
- **Nəzarət** – idarə heyəti tərəfindən müəyyən edilmiş, dayanıqlılıq risklərini həll etmək üçün dövri olaraq qiymətləndirilən nəzarət prosesləri.

Nəzərə alınmalı məqamlar

Daxili auditorlar Təşkilati Dayanıqlılıq 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.

Qanunvericilik, dövlət quruluşu və ya siyasi mühit səbəbindən dövlət sektorunda daxili audit fəaliyyətlərindəki məhdudiyyətlər bu işin müəyyən aspektlərinin həllinə potensial maneələr kimi tanınır. Dövlət sektorunda daxili auditorlar risk qiymətləndirmə prosesinin bir hissəsi olaraq əhatə dairəsi üzrə belə məhdudiyyətləri sənədləşdirməli və audit tapşırığının fərdiləşdirilmiş əhatəsini aydın şəkildə müəyyən etmək və çatdırmaq üçün peşəkar mühakiməni tətbiq etməlidirlər.

İdarəetmə üzrə nəzərə alınmalı məqamlar

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

A. İdarə heyəti tərəfindən hazırlanmış, Şura tərəfindən təsdiqlənmiş və icrasına nəzarət edilən sənədləşdirilmiş dayanıqlılıq strategiyası. Bu strategiya bütün işçi heyətinə rəsmi qaydada çatdırılmalı və təşkilatın missiyası, vizyonu, mədəniyyəti və risk idarəetmə yanaşması ilə sıx bağlı olmalı və bu məsələləri dəstəkləməlidir. Dayanıqlılıq strateji planının məqsədləri idarə heyəti tərəfindən təsdiqlənməli, təşkilatın ümumi risklərin idarə edilməsinə yanaşması ilə uyğunlaşdırılmalı və mütəmadi olaraq yoxlanılmalı və nəzərdən keçirilməlidir. Plan aşağıda qeyd olunmuş əməliyyat, texnoloji və maliyyə elementlərini əhatə edə bilər:

   - Əməliyyat – təşkilat daxilində dayanıqlılığın koordinasiyası; dayanıqlılıq risklərinin qiymətləndirilməsi prosesləri; dövri testlər və hesabatları əhatə edən biznesin davamlılığı planlaşdırılması; böhran idarəçiliyi; işçi qüvvəsinin uyğunlaşa bilməsi (məsələn, uzaqdan işləmə qabiliyyəti, ərazidə minimum işçi sayı və kritik rollar üçün çarpaz təlimlərin əhatə dairəsi); vacib kadrlar üçün varislik planlaşdırılması; təchizat zəncirinin dayanıqlılığı; əsas fəaliyyət göstəricilərinin (ƏFG/KPI) müəyyən edilməsi; və Şura üzvlərinin məlumatlılığını təmin etmək üçün təlimlər.
   - Texnoloji – İT infrastrukturuna dair tələblər; kritik məlumatların müəyyən edilməsi (məlumatların təsnifatı); məlumatların ehtiyat nüsxələrinin yaradılması; kibertəhlükəsizliyin möhkəmləndirilməsi və təhdidlərin monitorinqi; kritik texnoloji aktivlərin texniki qulluq edilməsi; və kritik məlumatlar üçün müəyyən edilmiş (bərpa testləri ilə təsdiqlənmiş) bərpa nöqtəsi hədəfi (BNH/RPO) və bərpa vaxtı hədəfi (BVH/RTO).

- Maliyyə – dayanıqlılığa ayrılmış büdcə vəsaitləri; fəaliyyətin pozulması zamanı əməliyyatları davam etdirmək üçün nağd vəsaitlərin ehtiyatları; fəaliyyətin pozulması ilə bağlı əməliyyatları dəqiq əks etdirmək üçün maliyyə hesabatlılığı prosesləri; fəaliyyətin pozulması risklərini azaltmaq üçün sığorta siyasətləri; və fövqəladə hallarda borc götürmək üçün kredit xətlərinin mövcudluğu.

B. Dayanıqlılıqla bağlı dövri (məsələn, aylıq və ya rüblük) yeniləmələr təşkilati dayanıqlılığı idarə edən şəxs və ya komanda tərəfindən idarə heyətinə təqdim edilir; bu yeniləmələr müəyyən edilmiş risk dözümlülüyünü tətikləyən amilləri, ƏFG-lər və ya müşahidə və tendensiyaları göstərən digər məlumatları əhatə edə bilər. Yeniləmələr təşkilati dayanıqlılıq strategiyasının məqsədlərinin vəziyyətini, o cümlədən strateji nəzarəti, monitorinqi və uzunmüddətli planlaşdırmanı əks etdirir. Hesabatlar aşağıdakılar üzrə monitorinq nəticələrini əhatə edə bilər:

- Strateji dayanıqlılıq məqsədlərinə çatılması ilə bağlı vəziyyət və bu məqsədə çatmağı əngəlləyə biləcək çətinliklər.
- Dayanıqlılıq məqsəd və vəzifələrinə çatmaq üçün büdcə dəstəyi, məsələn texnoloji aktivlərə olan tələbləri dəstəkləmək üçün vəsaitlər.
- Dayanıqlılıq risklərinin vəziyyəti, o cümlədən müəyyən edilmiş risk dözümlülük səviyyələrinə təsir edə biləcək dayanıqlılıq risk mühitindəki hər hansı əhəmiyyətli dəyişikliklər.
- Dayanıqlılıqla bağlı daxili nəzarət mexanizmlərinin effektivliyi, o cümlədən düzəliş işlərinin gedişatı.
- Dayanıqlılığın uğurunu ölçmək üçün ƏFG-lər.
- Dayanıqlılıqla bağlı vəzifə öhdəliklərinə malik olan kadrları işə götürmək, təlim keçmək və inkişaf etdirmək üçün tələb olunan insan resursları.

C. Əməliyyat, texnoloji və maliyyə dayanıqlılığı proseslərini idarə etmək üçün istifadə olunan siyasətlər, prosedurlar və digər müvafiq sənədlər, o cümlədən:

- Təhlükəsizlik baxımından kritik olan dayanıqlılıq proseslərinin necə müəyyən edilməsi və onların ən vacib prosesləri düzgün əks etdirib-etdirmədiyini müəyyən etmək üçün mütəmadi olaraq necə təhlil olunmasının vəziyyəti.
- Siyasətlər ən azı ildə bir dəfə (və ya daha yüksək risk səviyyəsinə əsasən daha tez-tez) nəzərdən keçirilir və yenilənir, həmçinin ortaya çıxan dayanıqlılıq riskləri üçün və ya testlərdən və ya real fəaliyyətin pozulması hallarından götürülən dərslərə əsasən daha tez-tez yenilənir.
- Dayanıqlılıq əməliyyatlarını dəstəkləmək üçün siyasət və prosedurların kifayətliliyinə dair yoxlama və təhlil prosesi.
- Risklərin idarə edilməsi, informasiya texnologiyaları və ya idarəetmə kimi əlaqəli proseslər üçün geniş qəbul edilmiş çərçivələrdən istifadə etməklə dayanıqlılıq prosesləri və daxili nəzarət mexanizmlərinin gücləndirilməsinə dair rəyin formalaşması. Nəzərə alınması faydalı ola biləcək nümunələrə NIST, COSO və ya ISO kimi təşkilatlar, xüsusən ISO 22300 seriyası (22316 və ya 22336) aiddir.

D. Dayanıqlılıq məqsədlərinə çatmaqla bağlı rəhbərlik rollarını və məsuliyyətlərini təsvir edən, formalaşdırılmış və sənədləşdirilmiş insident idarəetmə strukturu. Fəaliyyətin pozulması zamanı

dayanıqlılığa dair qərarlar üçün məsul kadrlar kimi mövcud qərarvermə iyerarxiyalarının formalaşmasına dair sübutlar və əməliyyat qərarları üçün tələb olunan təsdiqlər, məsələn, vəsaitlərin ayrılması və ya təşkilata fəaliyyətin pozulması zamanı kömək etmək üçün üçüncü tərəflə rəsmi müqavilə bağlamaq imkanı. Digər nəzərə alınmalı məqamlara fəaliyyətin pozulması zamanı sənədləşdirilmiş eskalasiya yolları və müvəqqəti qərarvermə səlahiyyətləri, o cümlədən maliyyə səlahiyyətlərinin təhvil verilməsi və üçüncü tərəflərlə müqavilə bağlamaq üçün təyin edilmiş hədlər daxildir.

E. Təşkilati dayanıqlılıq proseslərini işlətmək və idarə etmək məsuliyyətini daşıyan şəxslərin bilik, bacarıq və qabiliyyətlərini dövri olaraq (məsələn, illik və ya yarımillik) qiymətləndirmək üçün müəyyən edilmiş proses. Prosesə canlı və ya virtual təlim, konfranslar, tələb üzrə kurslar və ya peşəkar sertifikatlar kimi təlim proqramlarının təşkil edilməsi daxil edilə bilər. Kritik dayanıqlılıq rollarını müəyyən etmək üçün varislik planlaşdırmasının, o cümlədən yalnız bir şəxs və ya məhdud sayda fərd tərəfindən yerinə yetirilə bilən fəaliyyətləri müəyyən etmək məqsədilə ssenari testlərinin mövcudluğuna dair sübutlar. Əvəzetmələr üçün zəruri olan tələblərin müəyyən edilməsinin yoxlanılması.

F. Mövcud zəifliklər və ortaya çıxan təhdidləri müəyyən etmək və onlara cavab vermək, eləcə də təşkilati dayanıqlılıq məqsədlərinin reallaşdırılmasına təsir göstərə biləcək informasiya və hesabat strukturlarının yaradılmasında müvafiq daxili və kənar maraqlı tərəfləri müəyyən etmək, prioritetləşdirmək və cəlb etmək üçün təsis edilmiş proses. Dayanıqlılıqla bağlı zəifliklər barədə aparılan müzakirələrdə maraqlı tərəflərin iştirakına dair sübutlar. Bu sübutlar, dayanıqlılığın effektivliyini ölçmək və izləmək üçün müəssisə səviyyəsində ölçü vahidlərindən istifadə edildiyinə dair göstəriciləri ehtiva edən elektron poçtla göndərilən yazışmalar, iclas protokolları və ya hesabatlar şəklində ola bilər.

Risklərin idarə edilməsi üzrə nəzərə alınmalı məqamlar

Risklərin idarə edilməsi proseslərinin təşkilati dayanıqlılıq məqsədlərinə necə tətbiq olunduğunu qiymətləndirmək üçün daxili auditorlar aşağıdakı sübutları nəzərdən keçirə bilərlər:

A. Təşkilatın risk qiymətləndirilməsi və risk idarəetmə prosesləri təşkilati dayanıqlılıq risklərinin müəyyən edilməsini əhatə edir, davamlı şəkildə həyata keçirilir və sənədləşdirilir, nəticələri isə təşkilat daxilində kommunikasiyası təmin olunmaqla paylaşılır. Dayanıqlılıq risklərinin idarə edilməsi prosesi əməliyyatlar, müəssisə risklərinin idarə edilməsi, İT, təchizat zənciri/satınalma, infrastruktur, insan resursları, maliyyə, hüquqi, komplayens (uyğunluq), tənzimləyici, ictimaiyyətlə əlaqələr, kritik təchizatçılar, nüfuz, yeni yaranan risklər və digər əsas proseslərin qiymətləndirilməsini əhatə edir. Dayanıqlılıq risklərinin müəyyən edilməsi ilə yanaşı, proseslərə biznes əməliyyatlarını poza biləcək təhdidlərin və zəifliklərin aşağıdakı aspektlər üzrə qiymətləndirilməsi də daxil edilir:

- İlkin olaraq necə müəyyən edilməsi və təqdim olunması.
- Təşkilati məqsədlərə çatmaq riskini qiymətləndirmək məqsədilə necə təhlil edilməsi.
- Riski qəbul edilə bilən səviyyəyə endirmək üçün tədbirlər planları da daxil olmaqla necə azaldılması.
- Təhdidlər tam aradan qalxana qədər davamlı hesabatlılıq planı da daxil olmaqla necə monitorinq edilməsi.

Əlavə sübutlar bunlardan ibarət ola bilər:

- Təqdimatlar, elektron poçt vasitəsilə göndərilən məktublar və ya iclas protokolları vasitəsilə təşkilatın prosesə cəlb edilmiş sahələrini göstərən sənədlər. Təsir, ehtimal, sürət və digər aspektləri nəzərə almaqla risk amilləri bu sənədlərə daxil edilə bilər.
- Çoxsaylı risk təsirlərinin məcmu təsirini müəyyən etmək məqsədilə təhlil edilən yüksək dərəcədə korrelyasiyalı və ya qarşılıqlı asılı olan risk amilləri
- Risk qiymətləndirilməsi vahid asılılıq nöqtəsinin qarşısını almaq üçün mövcud olan resursların və kritik aktivlərin qorunması mərhələlərinin təhlil edilməsini əhatə edir.
- Risk qiymətləndirilməsi real böhranlardan, fəaliyyətin pozulması hallarından əldə edilən dərslər və aparılan sınaq testlərinin nəticələri nəzərə alınmaqla yenilənir.
- Təşkilat biznesə təsir təhlili üzrə hesabata əsaslanaraq potensial təsir və ehtimal dərəcələrinə əsasən ən yüksək risk yaradan sahələrə üstünlük verir.

B. Təşkilat dayanıqlılıq risklərini izləmək və hesabat formalaşdırmaq məqsədilə fərdi şəxsə və ya komandaya hesabatlılıq və məsuliyyət təyin edir və bu öhdəlikləri mütəmadi olaraq nəzərdən keçirir. Fərdi şəxs və ya komanda dayanıqlılığın idarə edilməsi sahəsində, ideal vəziyyətdə isə təşkilatın fəaliyyət göstərdiyi sahədə (məsələn, səhiyyə, maliyyə xidmətləri və ya dövlət sektoru) təcrübəsi olan ixtisaslı şəxslərdən ibarət olmalıdır. Fərd və ya komanda dayanıqlılıq risklərində yaranan yeni meyllərdən xəbərdar olmaq üçün dövri təlimlərdə iştirak etməlidir.

C. Təşkilat, təşkilati dayanıqlılıq risklərini (yeni yaranan və ya əvvəllər müəyyən edilmiş) izləmək və təşkilatın müəyyən etdiyi risk idarəetmə qaydaları və risk dözümlülüyü, yaxud müvafiq hüquqi və tənzimləyici tələblərlə qəbulolunmaz hesab edilən səviyyəyə çatdıqda onları tez bir zamanda müvafiq orqanlara çatdırmaq üçün proses yaratmalıdır. Maliyyə və qeyri-maliyyə göstəricilərindən irəli gələn təsirlər də daxil olmaqla təşkilati dayanıqlılıq riski üzərində olan təsirlər nəzərdən keçirilməlidir. Maliyyə göstəricilərinə nümunə kimi gəlirlər, xərclər, rentabellik, nağd pul vəsaitlərinin axını, borc, səhm qiyməti və ümumi dəyər kimi anlayışlar göstərilə bilər. Qeyri-maliyyə göstəricilərinə nümunə kimi brendin nüfuzu, müştəri məmnunluğu, ətraf mühitə təsirlər və kadr dövriyyəsi kimi anlayışlar göstərilə bilər. Prosesə aşağıdakılar daxildir:

- Riskin ilkin müəyyən edilməsi və vaxtında yüksək səviyyəyə eskalasiya edilməsi.
- Riskin qiymətləndirilməsi və onun təşkilati məqsədlərin reallaşmasının qarşısını necə ala biləcəyini müəyyən edən təhlilin aparılması.
- Riski vaxtında qəbul edilə bilən səviyyəyə endirmək üsulları da daxil olmaqla təklif olunan və razılaşdırılmış riskin azaldılması üzrə tədbirlər planının hazırlanması. Tədbirlər planı təşkilatın ümumi risk idarəetmə strategiyasına əsaslanmalıdır. Təklifdə zəruri risk azaldılması resursları, məsələn maliyyə resursları, işçi saatları və imkanları artırmaq üçün lazım olan əlavə texnologiya və proqram təminatı üzrə məlumatlar daxil edilməlidir.
- Təhdidlər tam aradan qaldırılanadək əsas risk göstəricilərinə görə davamlı risk monitorinqi və hesabatlılığı təmin olunmalıdır.

D. Təşkilat böhranlara, fəaliyyətin pozulması hallarına, fövqəladə hallara və ya digər hadisələrə cavab vermək və onların təsirlərindən bərpa olunmaq üçün proses həyata keçirməlidir. Proses tam şəkildə dövri olaraq, məsələn, rübdə bir dəfə və ya ildə bir dəfə sınaq yoxlamasından keçirilməli və daha tez-tez, məsələn, aylıq natamam sınaq yoxlamalarını da özündə ehtiva edə bilər. Kritik xidmətlər daha tez-tez sınaq yoxlamasının keçirilməsini tələb edə bilər. İnsidentə reaksiya və bərpa prosesi aşağıdakıları əhatə edə bilər:

- Aşkar etmə – kibertəhdidlərin qarşısının alınması üçün fasiləsiz monitorinqin keçirilməsi. Bu, müdaxilənin aşkarlanması sistemi, təhdid kəşfiyyatı və ya təhlükəsizlik məlumatları və hadisələrinin idarə edilməsi (TMHİE/SIEM) kimi alətlərin istifadəsini əhatə edə bilər. TMHİE/SIEM prosesin gücləndirilməsi üçün süni intellektdən istifadə oluna bilər. Təbii fəlakətlər və ya obyektdə nasazlıqlar baş verdikdə, təşkilat vaxtında maarifləndirmə və məlumat mübadiləsi üçün rabitə şəbəkəsi (xəbərdarlıq protokolları və ya bildirişlər kimi) yaratmalıdır. Bütün hallarda təşkilat müvafiq təcili yardım xidmətlərini və hüquq-mühafizə orqanlarını məlumatlandırmaq üçün bir proses müəyyən etməlidir. Hadisələr kritiklik səviyyəsinə görə prioritetləşdirilməlidir.
- Cavab və Məhdudlaşdırma – hadisəyə reaksiya yanaşması ssenari təhlillərini və müxtəlif fəaliyyətin pozulmasına səbəb olan hadisələrə qarşı dövri stress testlərini əhatə edir. Məsələn, kiber hadisələr zamanı əlavə zərərin qarşısını almaq üçün təşkilat zərərçəkmiş aktivləri izolyasiya etmək üçün proseslər məsələn, şəbəkə trafikini yönləndirmək və ya hadisə zamanı istifadəçi girişini məhdudlaşdırmaq kimi tədbirlər tətbiq etməlidir. Fiziki hadisələr üçün təşkilat təsiri məhdudlaşdırmaq məqsədilə fəaliyyətin pozulmasına səbəb olan hadisələri fiziki cəhətdən izolyasiya edən, o cümlədən işçiləri alternativ yerə köçürən bir prosesi həyata keçirməlidir.
- Bərpa – kibertəhdidlər və ya İT ilə bağlı hadisələr üçün təşkilat əməliyyatları bərpa etmək məqsədilə zəruri olan kritik aktivlərin (məsələn, ehtiyat nüsxələrdən məlumatların bərpası və ya serverlərin yenidən onlayn vəziyyətə gətirilməsi) bərpasına üstünlük verən prosedurlar müəyyən etməlidir. Əməliyyatları bərpa etmək üçün tələb olunan digər qeyri-İT resurslarının da bərpa prosesində üstünlük dərəcəsinə görə prioritetləşdirmə aparılmalıdır. Bu, aparıcı kadrların və ya əsas funksiyaların tədricən geri dönməsini planlaşdırmaqla bağlı tədbirləri əhatə edə bilər.
- İnsidentdən sonrakı təhlil – təşkilat hadisələri təhlil edərək aşağıdakıları müəyyən edir:
  - Fəaliyyətin pozulmasına səbəb olan hadisələrin kök səbəbləri.
  - Görülmüş tədbirlərin effektivliyi.
  - Dayanıqlılıq proseslərini gücləndirmək üçün tələb olunan təkmilləşdirmələr, məsələn siyasətlərin, prosedurların, risklərin və ya strategiyanın yenilənməsi və sair analoji tədbirlər.

Ciddi xidmətləri/funksiyaları və onların asılılıqlarını əhatə edən masaüstü məşqlər, simulyasiyalar və təlimlər vasitəsilə cavab və bərpa prosesinin ciddiliyinin və effektivliyinin yoxlanılması təşkilati risk dözümlülüyü səviyyələri ilə uyğunlaşdırıla bilər. Bu hadisələrin daxili və ya kənar hadisələrdən qaynaqlanması mümkündür. Bu məşqlərin nəticələri Şura və yüksək rəhbərlik tərəfindən təhlil edilə, təkmilləşdirmə tədbirləri isə mütəmadi olaraq izlənilə və müvafiq olaraq hesabat formasında təqdim edilə

bilər. Tövsiyələr icra oluna biləcək şəkildə olmalı, eləcə də vaxt cədvəlinə uyğun olaraq icra üzrə konkret məsuliyyət daşıyan tərəflərə təhkim edilməlidir.

Nəzarət prosesinin təşkili üzrə nəzərə alınmalı məqamlar

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

A. Vacib əməliyyatların davam etdirilməsi üçün kritik üçüncü tərəf təminatçılarını (təchizatçılar və satıcılar) və minimum mal-material səviyyələrini müəyyənləşdirmək və qiymətləndirmək üçün prosesin mövcud olması dəyərləndirilməlidir. Dəyərləndirmə üçüncü tərəflərin dayanıqlılığını və biznesin davamlılığını nəzərə alaraq hər bir təchizatçı üçün risk reytinqlərini əhatə edə bilər. Rəsmi müqavilə bağlamazdan əvvəl təchizatçıları nəzərdən keçirməklə yanaşı, təşkilat risk reytinqlərini davamlı qiymətləndirmək üçün təchizatçıları mütəmadi olaraq da nəzərdən keçirə bilər. Təşkilatın təchizatçı ilə münasibətləri sona çatdıqda potensial olaraq əvəz edəcək təchizatçıların siyahısını saxlaması təhlil oluna bilər.

B. İdarə heyəti məlumatlarının təsnifatlaşdırılması üzrə işin aparılması, xüsusilə fəaliyyətin pozulmasına səbəb olan hadisələrdən bərpa olunmaq və əməliyyatları davam etdirmək üçün zəruri kritik məlumatların müəyyən edilməsi təhlil oluna bilər. Təşkilatın kritik məlumatları qorumaq üçün səmərəli daxili nəzarət mexanizmləri tətbiq etməsi, o cümlədən çıxışın yalnız səlahiyyətli şəxslərlə məhdudlaşdırılması və kritik məlumatların vaxtında ehtiyat nüsxəsinin yaradılmasını və bərpa edilə bilməsini təmin etməklə bağlı prosesləri yoxlanıla bilər.

C. Rəhbərliyin informasiya təhlükəsizliyi risklərini (o cümlədən kiber riskləri) azaltmaq və fəaliyyətin pozulmasına səbəb olan hadisələr zamanı həssas məlumatların qorunmasını təmin etmək üçün kritik İT nəzarətləri və davamlı monitorinq prosesləri yaratması nəzərdən keçirilə bilər. Şifrələmə həssas məlumatları qoruyur. Davamlı monitorinq və real vaxt rejimində təhdid kəşfiyyatı, rəhbərliyə xəbərdarlıqlar formasında məlumat təqdim etməsi və problemlərin vaxtında həll olunması təhlil oluna bilər. Bu zaman NIST, COSO, ISO və digər təşkilatların geniş qəbul olunmuş nəzarət çərçivələrindən istifadə oluna bilər.

D. Təşkilatın böhranlar, fəaliyyətin pozulması halları və fövqəladə hallar zamanı əməliyyatları dəstəkləmək üçün tələb olunan kritik İT aktivlərini, o cümlədən avadanlıq, proqram təminatı və xidmətləri inventarlaşdırması yoxlanıla bilər. Tez bir zamanda əldə edilməsi daha çətin olan İT aktivləri yüksək prioritet kimi müəyyən edilməldir.

E. Biznesin davamlılığı planı və fəlakətdən bərpa planı hazırlanmalı və biznesə təsir təhlilinə əsaslanan bərpa komandaları üçün kadrlar müəyyən edilməlidir. Planlar rüblük və ya illik əsasda masaüstü məşqlər və ya stress testləri vasitəsilə yoxlanılır; bu zaman baş verən fəaliyyətin pozulması halları real fövqəladə halları simulyasiya edir və həm daxili, həm də kənar tərəfdaşlarla kommunikasiya protokollarının testini əhatə edir. Sınaq yoxlamalarının nəticələri, o cümlədən təkmilləşdirmə imkanları, Şuraya və yüksək rəhbərliyə təqdim olunur.

F. Fəaliyyətin pozulmasına səbəb olan hadisələr zamanı iş mühitini dəyişdirmək üçün proses müəyyən edilməlidir. Dəyişikliklərə alternativ iş yerlərindən qoşulma, məsələn evdən işləmək və ya müvəqqəti ofisi vaxtında və səmərəli şəkildə qurmaq kimi tədbirlər daxil edilə bilər. Təşkilat iş yerindən fəaliyyəti əvəz etmək üçün hibrid və ya uzaqdan işləmə variantlarından da istifadə edə

bilər. Digər məqamlara İT və insan resursları da daxil olmaqla, resursların vaxtında və səmərəli şəkildə mobilizasiyası və yenidən bölüşdürülməsi üçün müvafiq protokollar daxil edilə bilər.

G. Təşkilati dayanıqlılıqla bağlı yaranan təhdidləri və zəifliklər davamlı şəkildə izləmək və hesabat vermək, eləcə də təşkilati dayanıqlılıq əməliyyatlarını yaxşılaşdırmaq üçün imkanları müəyyən etmək, prioritetləşdirmək və həyata keçirmək məqsədilə prosesin mövcudluğu yoxlanıla bilər. Monitorinq fəaliyyətlərinə əsas risk göstəriciləri (ƏRG/KRIs), risk idarəetmə panelləri və risk üfüqlərinin araşdırılması məşqləri daxil edilə bilər. Təşkilat yeni yaranan təhdidlər, o cümlədən yumşaldıcı tədbirlər və ya nəzarət mexanizmləri barədə bütün işçilərə məlumat verə bilər. Bütün məlumat verənlərin fəaliyyəti qeydə alınmalı, təhlil olunmalı, vaxtında həll edilməli və yüksək rəhbərliyə çatdırılmalıdır. Məsələləri həll etmək üçün davamlı monitorinq zəruri ola bilər ki, bu da öz növbəsində əlavə hesabatın təqdim olunmasını ehtiva edir.

H. Böhran, fəaliyyətin pozulması və fövqəladə hallar baş verdikdə əməkdaşların riayət etməli olduğu təşkilati dayanıqlılıq siyasətləri və prosedurları barədə təhsil almaq və təlim keçmək üçün prosesin mövcud olması yoxlanıla bilər. Proses pozucu ssenariləri simulyasiya edən təlim məşqlərini əhatə edir. Təlim müntəzəm olaraq, məsələn, rübdə bir dəfə və ya ildə bir dəfə keçirilir. Kritik xidmətlərin daha tez-tez sınaqdan keçirilməsinə zərurət yarana bilər.

I. Böhran, fəaliyyətin pozulması və fövqəladə hallar zamanı zəruri əməliyyat, insan, texnoloji və maliyyə resurslarının büdcəyə salınmasını və mövcud olmasını təmin etmək üçün prosesin mövcud olması yoxlanıla bilər. Rəhbərlik müntəzəm olaraq, məsələn rübdə bir dəfə və ya ildə bir dəfə, qəbul edilmiş risk səviyyələrinə əsasən resursların kifayət edib-etmədiyini nəzərdən keçirməli və ehtiyacları Şuraya təqdim etməlidir. Kritik xidmətlərin daha tez-tez sınaqdan keçirilməsinə zərurət yarana bilər. Təhlil likvidlik səviyyəsini, sığorta təminatını və fövqəladə hallar üçün maliyyələşdirmə tədbirlərini qiymətləndirməyi əhatə edir. Maliyyə resurslarına olan tələblər təşkilatın ölçüsü, mürəkkəbliyi, fəaliyyət sahəsi və risk profili kimi amillərə əsasən planlaşdırılır. Proses maliyyələşmənin əvvəlcədən təsdiqini əhatə edə bilər.

J. Hadisələr baş verdikdən sonra böhranları, fəaliyyətin pozulması və fövqəladə halları nəzərdən keçirmək və hadisədən sonrakı icmalları “öyrənilmiş dərslər” əsasında təhlil etmək üçün prosesin mövcudluğu təhlil oluna bilər. Təhlillər rəsmi hesabatlar formasında sənədləşdirilməli və əldə olunan dərslər gələcək dayanıqlılıq planlaşdırmasına inteqrasiya edilməlidir.

Əlavə A. Tətbiq Ssenariləri

Aşağıdakı ssenarilər Təşkilati Dayanıqlılıq üzrə Mövzu Əsaslı Tələbin hansı vəziyyətlərdə tətbiq olunacağını təsvir edir. Əlavə olaraq, DAİ-nin "Mövzu Əsaslı Tələblərin Tətbiqi üzrə Təlimat"-ı (Topical Requirements Application Guidance), məcburi tələbləri yerinə yetirmək, məhdudiyyətləri aradan qaldırmaq və kritik risk səviyyələrini müəyyən etmək üçün praktik məsləhətlər təqdim edir.

Ssenari 1: Təşkilati dayanıqlılıqla bağlı məsələ daxili audit planına daxil edilmiş daxili audit tapşırığının icrası üçün müəyyən edilmişdir.

Daxili audit funksiyası risk əsaslı planlaşdırma prosesini tamamlayıb daxili audit planına təşkilati dayanıqlılıq üzrə bir və ya bir neçə yoxlamanı daxil etdikdə, bu tapşırıqları icra edərkən Mövzu Əsaslı Tələb mütləq tətbiq edilməlidir. Standartlara uyğunluq daxili audit planına bir və ya bir neçə tapşırıq üzrə tələbləri daxil etməklə əldə edilə bilər.

Təşkilati dayanıqlılıq geniş mövzudur və Mövzu Əsaslı Tələbdəki göstərilmiş hər bir məqam bütün tapşırıqların icrası zamanı tətbiq olunmaya bilər. Daxili auditorlar peşəkar mühakiməni tətbiq edərək Təşkilati Dayanıqlılıq 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 təşkilati dayanıqlılıq fəaliyyətlərini növbəlilik əsasında yoxlaması və ya bu bu tapşırıq üzrə dayanıqlılıq riskinin əhəmiyyətinin aşağı olduğunu müəyyən edildiyi halları göstərmək olar.

Ssenari 2: Təşkilati dayanıqlılıq riskləri təşkilati dayanıqlılığı əhatə etməyən audit yoxlaması zamanı müəyyən edilmişdir.

Daxili auditorlar birbaşa dayanıqlılığa aid olmayan prosesi qiymətləndirərkən dayanıqlılıq risklərini müəyyən edə bilərlər. Məsələn, daxili auditorlar təşkilati dayanıqlılığı əhatə etməyən yoxlama çərçivəsində kadr proseslərini (məsələn, işçilərin işə qəbulu və təşkilatda saxlanması) qiymətləndirə və yoxlamanı planlaşdırarkən dayanıqlılıq 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, təşkilatın kadrları necə saxlaması ilə bağlı varislik planlaşdırma riskləri aşkar oluna bilər (Standart 13.2 "Audit Tapşırığı Çərçivəsində Risklərin Qiymətləndirilməsi").

Müvafiq risklər müəyyən edildikdən sonra daxili auditorlar Təşkilati Dayanıqlılıq üzrə Mövzu Əsaslı Tələbi nəzərdən keçirməli və hansı tələblərin tətbiq olunmasının zəruri olduğunu müəyyən etməlidirlər. Bu halda onlar yalnız İdarəetmə bölümündə göstərilmiş E bölümünün tələbinə diqqət yetirə və digər risk idarəetmə və nəzarət tələblərini istisna edə bilərlər. Onlar yoxlama tapşırığı üzrə iş sənədlərində Təşkilati Dayanıqlılıq üzrə Mövzu Əsaslı Tələbin digər müddəalarının istisna edilməsinin əsaslandırmasını sənədləşdirməli və həmin sənədləri müvafiq qaydada saxlamalıdırlar.

Ssenari 3: Əvvəldən daxili audit planına daxil edilməmiş təşkilati dayanıqlılıqla bağlı bir fəaliyyətin həyata keçirilməsi tələb olunmuşdur.

Maraqlı tərəflər, məsələn, Şura, rəhbərlik və ya tənzimləyici orqan daxili auditorlardan ilkin audit planından kənar dayanıqlılıq qiymətləndirmələri aparmağı xahiş edə bilərlər. Məsələn, təşkilatlar kiberhücumun hədəfi olduqda, Şura təşkilatın kiberhücumun fəsadlarını aradan qaldırmağa nə dərəcədə hazır olduğunu qiymətləndirmək üçün dayanıqlılıq nəzarət mexanizmlərini yoxlamaq məqsədilə daxili audit tapşırığının icra edilməsini tələb edə bilər. Mövzu Əsaslı Tələb tətbiq olunmalı, tələblər qiymətləndirilməli və istisnalar sənədləşdirilməlidir (Standart 9.4 “Daxili Audit Planı”).

Əlavə B. Tətbiq Ssenarilərinə Əsaslanan Nümunəvi Audit Tapşırıqları

Ssenari 1: Mövzu daxili audit planına daxil edilmiş tapşırıqla bağlıdır.

Mərkəzi topdansatış bazarı üçün məsuliyyət daşıyan dövlət sektoru subyekti

İllik riskə əsaslanan planlaşdırma prosesi zamanı daxili audit funksiyası əsas bazar əməliyyatlarının fasiləsizliyini logistika pozuntularına, ictimai sağlamlıq hadisələrinə və kritik infrastruktur asılılıqlarına məruz qalma səbəbindən yüksək riskli sahə kimi müəyyən etmişdir. Bu qiymətləndirməyə əsasən daxili auditorlar müəyyən edirlər ki, Təşkilati Dayanıqlılıq üzrə Mövzu Əsaslı Tələb planlaşdırılan bu audit tapşırığına aid edilə bilər.

İdarəetməni qiymətləndirmək üçün daxili auditorlar idarə heyətinin protokollarını, strateji planları və büdcə sənədlərini nəzərdən keçirərək dayanıqlılığa dair məqsədlərin rəsmi olaraq müəyyən edilib-edilmədiyini və onlara nəzarət olunub-olunmadığını müəyyən edirlər. Auditorlar rəhbərliyin nəqliyyatdan asılılıqlar, infrastruktur məhdudiyyətləri və sağlamlıqla bağlı risklər kimi kritik zəifliklər barədə idarəedici orqana dövri olaraq hesabat təqdim edib-etmədiyini qiymətləndirirlər. Tək bir dayanıqlılıq strategiyası sənədi mövcud olmadıqda, daxili auditorlar dayanıqlılıq elementlərinin əməliyyat və strateji sənədlərdə ardıcıl şəkildə əks olunub-olunmadığını qiymətləndirirlər.

Risk idarəetməsi baxımından daxili auditorlar təşkilatın risk reyestrini nəzərdən keçirir və əməliyyatların idarə olunmasından məsul heyət ilə müsahibə apararaq təchizatın davamlılığına təsir edə biləcək risklərin müəyyən edilib-edilmədiyini, qiymətləndirilib-qiymətləndirilmədiyini və məsul şəxslərə təhkim olunub-olunmadığını təsdiqləyirlər. Onlar əvvəlki hadisələrdə, məsələn müvəqqəti bağlanmalar və ya giriş məhdudiyyətləri zamanı eskalasiya mexanizmlərinin işə salınıb-salınmadığını yoxlayır və cavab tədbirlərinin müəyyən edilmiş risk dözümlülüyü parametrləri ilə uyğun olub-olmadığını müəyyən edirlər.

Nəzarət prosedurlarına əməliyyat fasiləsizliyinin təminatı tədbirlərinin nəzərdən keçirilməsi, müntəzəm sınaq məşqlərinə dair sübutların yoxlanılması və fəaliyyətin pozulmasına səbəb olan hadisələr zamanı dövlət orqanları ilə əlaqələndirməyə dair sənədlərin araşdırılması daxildir. Daxili auditorlar həmçinin hadisədən sonrakı hesabatları nəzərdən keçirərək öyrənilmiş təcrübələrin yenilənmiş proseslərə daxil edilib-edilmədiyini müəyyən edirlər. Mövzu Əsaslı Tələbin müəyyən müddəaları qanunvericilik və ya struktur məhdudiyyətləri səbəbindən tətbiq edilmədikdə, daxili auditorlar Standartlara uyğun olaraq istisna edilmək üçün əsaslandırmanı sənədləşdirirlər.

Ssenari 2: Mövzu audit tapşırığı yerinə yetirilərkən müəyyən edilir.

Bir neçə müxtəlif ölkədə yerləşən peşəkar xidmətlər şirkəti

İdarəetmə və müəssisə risklərinin idarə edilməsinə yönəlmiş yoxlama çərçivəsində daxili auditorlar mərkəzdənkənar qərar qəbuletmə, yerli rəhbərliyin aparıcı nümayəndələrinə güvənmə və müxtəlif

yurisdiksiyalarda tənzimləyici risklərlə bağlı zəifliklər müəyyən edirlər. Bu müşahidələrə əsaslanaraq daxili auditorlar, Təşkilati Dayanıqlılıq üzrə Mövzu Əsaslı Tələbin bəzi elementlərinin bu audit tapşırığına aid olduğunu müəyyən edirlər.

İdarəetməni qiymətləndirmək üçün daxili auditorlar təşkilatın tənzimləyici dəyişikliklər, kritik kadrların əhəmiyyətli dəyişməsi və ya bir yurisdiksiyada daha geniş təsirə malik reputasiya hadisələri zamanı əməliyyatların necə davam etdiriləcəyini müəyyən edib-etmədiyini təhlil etmək məqsədilə qlobal siyasətləri, Şuraya təqdim olunan hesabat materiallarını və böhran idarəetmə protokollarını nəzərdən keçirirlər. Auditorlar, idarəetmə orqanının müxtəlif yurisdiksiyalar üzrə kritik risklər barədə konsolidasiya olunmuş hesabat alıb-almadığını və dayanıqlılığın nəzarəti üzrə məsuliyyətlərin aydın şəkildə müəyyən edilib-edilmədiyini qiymətləndirirlər.

Risk idarəetməsi baxımından daxili auditorlar müəssisənin risk çərçivəsini yoxlayaraq əsas şəxsdən asılılığı, sərhədlərarası prudensial uyğunluq və işgüzar nüfuz risklərinin təşkilatın strateji məqsədləri ilə əlaqələndirilib-əlaqələndirilmədiyini təsdiqləyirlər. Onlar yerli hadisələrin qlobal rəhbərliyə düzgün səviyyədə çatdırılıb-çatdırılmadığını və cavab qərarlarının müəyyən edilmiş səlahiyyət səviyyələri daxilində qəbul edilib-edilmədiyini müəyyən etmək məqsədilə seçilmiş hadisələrin nümunəvi yoxlamasını aparırlar.

Nəzarətlə bağlı prosedurlar müxtəlif yurisdiksiyalarda biznesin davamlılığı tədbirlərini nəzərdən keçirməyi, kritik rolların kifayət qədər əhatə olunub-olunmadığını və fövqəladə hallar üçün ehtiyat heyətin və ya düzgün qurulmuş varislik proseslərinin mövcudluğunu yoxlamağı, həmçinin koordinasiyalı uzaqdan idarə olunan əməliyyatları dəstəkləyən texnoloji infrastrukturun kifayətliliyini qiymətləndirməyi əhatə etməlidir. Daxili auditorlar hadisədən sonrakı təhlillərin sənədlərini də nəzərdən keçirərək düzəldici tədbirlərin həyata keçirildiyini də təsdiqləməlidirlər. Mövzu Əsaslı Tələbin yalnız müəyyən müddəaları tətbiq olunduqda, daxili auditorlar daxil etmə və ya istisna etmə əsaslarını sənədləşdirməlidirlər.

Ssenari 3: Mövzu tələb olunan audit tapşırığının predmetidir.

Kritik milli infrastruktur üçün məsul olan təşkilat

Qonşu yurisdiksiyada baş verən dağıdıcı qasırğa idarə heyətinin üzvünü daxili audit funksiyasından audit planına təşkilati dayanıqlılığın yoxlamasını əlavə etməyi xahiş etməyə sövq edir ki, qurumun əməliyyat fasilələrinə məruz qalmasını, ixtisaslaşmış təchizatçılardan asılılığını, tənzimləyici öhdəliklərini və ciddi ekoloji hadisələrlə bağlı risklərə məruz qaldığını təsdiqləsin. Bu halda Təşkilati Dayanıqlılıq üzrə Mövzu Əsaslı Tələb hərtərəfli şəkildə tətbiq edilməlidir.

İdarəetməni qiymətləndirmək üçün daxili auditorlar idarə heyəti tərəfindən təsdiqlənmiş strateji planı və əlaqəli sənədləri nəzərdən keçirərək kritik xidmətlərin davamlılığının uzunmüddətli planlaşdırmaya rəsmi olaraq daxil edilməsini təsdiqləyirlər. Onlar idarə heyətinə təqdim olunan hesabatları əməliyyat əlçatanlığı, kritik aktivlərin texniki qulluq işləri və müxtəlif maliyyə ssenarilərinin planlaşdırılması, o cümlədən sığorta təminatı və ehtiyat ayırmaları ilə bağlı əsas göstəricilərin mütəmadi olaraq nəzərdən keçirilib-keçirilmədiyini müəyyən etmək məqsədilə yoxlayırlar.

Risk idarəçiliyi baxımından daxili auditorlar infrastruktur pozuntuları, təchizatçıların təmərküzləşməsi, tənzimləmə sahəsində uyğunluq (komplayens) və ətraf mühitə məruz qalma ilə bağlı risklərin müəssisə risk idarəçiliyi çərçivəsində necə müəyyən edilməsi, qiymətləndirilməsi və monitorinq edilməsini dəyərləndirirlər. Onlar bu risklərin monitorinqi üçün məsuliyyətin aydın şəkildə müəyyən edilib-edilmədiyini və əvvəlki xidmət kəsintiləri zamanı, o cümlədən tənzimləyicilər və fövqəladə hallar üzrə

məsul orqanlar ilə əlaqələndirmə də daxil olmaqla, eskalasiya protokollarının yerinə yetirilib-yetirilmədiyini nəzərdən keçirirlər.

Nəzarət mexanizmlərinin yoxlanılmasına düzəldici tədbirlərin izlənilməsi və icra edilməsinin vəziyyətinin müəyyən edilməsi məqsədilə biznesin davamlılığı və fəlakətdən bərpa planlarının mövcudluğunun və onların müntəzəm olaraq yoxlanılmasının təsdiqlənməsi, kritik aktivlərin siyahısının nəzərdən keçirilməsi, alternativ təminatçılarla bağlanmış müqavilə şərtlərinin araşdırılması və hadisədən sonrakı təhlil sənədlərinin qiymətləndirilməsi də daxildir. Prudensial tənzimləmələrin tələblərinə görə müəyyən tələblər tətbiq edilmədikdə, daxili auditorlar Standartlara uyğun olaraq müvafiq əsaslandırmanı sənədləşdirirlər.

Əlavə C. Çərçivələrlə Əlaqələndirmə

Təşkilat öz təşkilati tədbirlərini ISO 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 təşkilati dayanıqlılıq üzrə mövcud olan nəzarət mexanizmlərinin sınaq testlərini Mövzu Əsaslı Tələb ilə uzlaşdırmalıdırlar (Standart 13.4 "Qiymətləndirmə Meyarları"). Aşağıdakı cədvəl Təşkilati Dayanıqlılıq üzrə Mövzu Əsaslı Tələbi ISO 22336 Çərçivəsinə uyğunlaşdırır. Çərçivə üzrə əlavə istinadlar Əlavə E bölümündə sadalanmışdır.

İdarəetmə tələbləri	ISO 22336 Çərçivəsi
A. Dayanıqlılığı nəzərə alan rəsmi təşkilati strategiya idarə heyəti tərəfindən müəyyən edilməli, direktorlar şurası tərəfindən ona nəzarət olunmalı və dəyişiklikləri idarə etmək və əməliyyatları davam etdirmək üçün tələb olunan əməliyyat, texnologiya və maliyyə elementlərini əhatə etməlidir. Dayanıqlılıq məqsədləri təşkilatın ümumi risk idarəetmə yanaşması ilə uyğunlaşdırılmalıdır.	4.1; 6.1; 6.2; 7.1; 8.4; 8.5; 9.1; 9.5
B. Dayanıqlılıq məqsədlərinin yerinə yetirilməsi ilə bağlı yeniləmələr mütəmadi olaraq təhlil edilmək məqsədilə idarə heyətinə təqdim olunmalıdır. Bu, dayanıqlılığın strateji nəzarət, uzunmüddətli planlaşdırma prosesləri, varislik planlaşdırılması və təşkilatın mədəniyyətinə, o cümlədən kritik biznes fəaliyyətlərini dəstəkləmək üçün tələb olunan resurs və büdcə baxışlarına daxil edilməsini təmin etməlidir.	6.4; 8.6; 10.2
C. Kritik əməliyyat, texnoloji və maliyyə prosesləri üçün siyasət və prosedurlar müəyyən edilməli və nəzarət mühitini gücləndirmək məqsədilə mütəmadi olaraq nəzərdən keçirilməli, sınaq testləri tətbiq olunmalı və zərurət olduqda yenilənməlidir.	4.2; 6.3; 8.3; 8.4; 9.4
D. Hadisə idarəçiliyi strukturu yaradılmalı və təşkilati dayanıqlılıq məqsədlərinə nəzarət etmək və onları dəstəkləmək üçün istifadə olunmalıdır. Bu, qərar qəbuletmə iyerarxiyalarını, kommunikasiya və eskalasiya protokollarını, eləcə də rəhbərlik və əməliyyat rolları və məsuliyyətlərini əhatə etməlidir.	5.4
E. Dayanıqlılıq uğuru üçün tələb olunan səriştələri dövri olaraq təsdiqləmək və dayanıqlılıq proseslərində kritik rolları icra edən şəxslərin səriştələrini yenidən qiymətləndirmək üçün proses müəyyən edilməlidir.	9.6
F. Təşkilati dayanıqlılıq məqsədlərinə çatmaq üçün məlumat və hesabat strukturlarının yaradılmasında bütün müvafiq daxili və kənar maraqlı tərəflərin müəyyən edilməsi və cəlb olunmasını, prioritetlərin müəyyən edilməsini təmin edən proses müəyyən olunmalıdır. Maraqlı tərəflərə yüksək rəhbərlik, əməliyyatlar, risk idarəçiliyi, İT, təchizat zənciri/satınalmaların keçirilməsi, infrastruktur, insan resursları, maliyyə, hüquq, əminlik təminatçıları (daxili audit də daxil olmaqla), uyğunluq (komplayens), ictimaiyyətlə əlaqələr, kritik təchizatçılar, müştərilər, tənzimləyicilər və digərləri daxil edilə bilər.	9.2; 9.5

Risk idarəetməsi tələbləri	ISO 22336 Çərçivəsi
A. Təşkilati dayanıqlılıqla bağlı risklər təşkilat üzrə mütəmadi olaraq müəyyən edilməli, qiymətləndirilməli və idarə olunmalıdır. Dayanıqlılıq riskləri təşkilatın strateji məqsədlərinə uyğunlaşdırılmalıdır. Dayanıqlılıq risklərinin idarə edilməsi prosesi əsas proseslərin qiymətləndirilməsini əhatə etməlidir.	4.4; 5; 7.3; 7.4; 7.5, 7.6, 9.2, 9.3
B. Məsul şəxs və ya komanda təşkilati dayanıqlılıq risklərinin idarə edilməsini, o cümlədən riskin azaldılması üçün zəruri resursları və təşkilati dayanıqlılığa yönələn yeni təhdidlərin müəyyən edilməsini müntəzəm olaraq izləmək və hesabat vermək üçün təyin olunmalıdır.	4.3; 8.2; 9.6
C. Təşkilatın mövcud risk idarəetmə qaydaları və risk dözümlülüyü və ya müvafiq qanun və tənzimləyici tələblər əsasında qəbuledilməz hesab olunan səviyyəyə çatmış təşkilati dayanıqlılıq risk (yeni yaranan və ya əvvəllər müəyyən edilmiş) səviyyələrini izləmək və onları tez bir zamanda müvafiq qurumlara çatdırmaq üçün proses müəyyənləşdirilməlidir. Təşkilati dayanıqlılıq riskinin təsirləri nəzərdən keçirilməlidir.	7.2; 7.6; 10.1
D. Rəhbərlik böhran, fəaliyyətin pozulması və fövqəladə hallar baş verdikdə onlara cavab vermək və onların təsirlərindən bərpa olunmaq üçün müəyyən bir proses tətbiq etməli və mütəmadi olaraq sınaq yoxlamalarından keçirməlidir. Hadisəyə reaksiya və bərpa prosesi aşkarlanma, prioritetləşdirmə, məhdudlaşdırma, bərpa və hadisədən sonrakı təhlili əhatə etməlidir. Hadisəyə reaksiya yanaşması mümkün fəaliyyətin pozulmasına səbəb olan hadisələrin müxtəlif spektri üzrə ssenari təhlillərini və dövri stress testlərini əhatə etməlidir.	7.2; 7.6; 7.8

Nəzarət prosesi tələbləri	ISO 22336 Çərçivəsi
A. Kritik üçüncü tərəf təminatçılarını (təchizatçılar və satıcılar) müəyyən etmək və əsas əməliyyatların davam etdirilməsi üçün tələb olunan minimum mal-material səviyyələrini müəyyən etmək üçün proses həyata keçirilməlidir. Bu proses həmçinin alternativ təchizatçıların cari siyahısının aparılmasını da əhatə etməlidir.	7.7
B. Əməliyyatlar üçün kritik məlumatlar müəyyən edilməli və təsnifləşdirilməlidir. Məlumat təsnifatı məlumatların harada saxlanıldığını, kimlərin ona çıxış tələb etdiyini, necə çıxış edildiyini və fövqəladə hallarda ehtiyat nüsxəsinin olub-olmadığını və bərpa edilə bilib-bilməyəcəyini müəyyən etməyi əhatə edir.	6.1
C. Məlumat təhlükəsizliyi risklərini (o cümlədən kibertəhlükə risklərini) azaltmaq və böhran, fəaliyyətin pozulması və fövqəladə hallar zamanı həssas məlumatların qorunmasını təmin etmək üçün kritik İT nəzarətləri və davamlı monitorinq tətbiq edilməlidir. Nəzarət tədbirləri və davamlı monitorinq real vaxt rejimində təhdid kəşfiyyatı və çıxışın yalnız səlahiyyətli istifadəçilərlə məhdudlaşdırılmasını əhatə edir.	7.5
D. Kritik İT aktivlərinin siyahısı tərtib olunmalıdır. Aktivlərə böhranlar, fəaliyyətin pozulması və fövqəladə hallar zamanı əməliyyatları dəstəkləmək üçün tələb olunan avadanlıqlar, proqram təminatları və xidmətlər daxildir.	9.2

E.	Biznesin davamlılığı və fəlakətdən bərpa planları hazırlanmalı və təyin olunmuş heyət və bərpa komandaları üçün müəyyən edilmiş rol və vəzifələri əhatə etməlidir. Planlar mütəmadi olaraq sınaqdan keçirilməli (məsələn, "masaüstü məşq" şəklində) və sınaq yoxlamalarının nəticələri, o cümlədən təkmilləşdirmə imkanları direktorlar şurasına və yüksək rəhbərliyə təqdim olunmalıdır.	8.6; 9.6; 10.3
F.	Böhranlar, fəaliyyətin pozulması və fövqəladə hallar zamanı iş mühitini dəyişdirmək üçün proses müəyyən edilməlidir.	9.3
G.	Təşkilati dayanıqlılığa təsir göstərə biləcək yeni təhdidləri və zəifilikləri davamlı şəkildə izləmək və hesabat vermək üçün müəyyən bir proses yaradılmalıdır. Bu proses təşkilati dayanıqlılıq əməliyyatlarını, o cümlədən məlumat vermə sistemi və ya risk kəşfiyyatı və məlumat toplama sistemləri də daxil olmaqla, təkmilləşdirmə üçün imkanları müəyyən etmək, prioritetləşdirmək və həyata keçirmək üçün istifadə olunur.	7.6
H.	Təşkilati dayanıqlılıqla bağlı heyətin təhsili və təlimi üçün proses müəyyən edilməli, bu proses onların riayət etməli olduqları siyasət və prosedurlardan və böhran, fəaliyyətin pozulması və fövqəladə hallar baş verdikdə atılmalı olan addımlardan xəbərdar olmalarını təmin etməlidir. Proses fəlakət ssenarilərinin simulyasiya olunduğu təlim məşqlərini əhatə etməlidir.	10.2; 10.3
I.	Zəruri əməliyyat, insan, texnologiya və maliyyə resurslarının böhranlar, fəaliyyətin pozulması və fövqəladə hallar zamanı büdcələndirilməsini və mövcud olmasını təmin etmək üçün proses müəyyən edilməlidir. Təşkilati dayanıqlılığı dəstəkləmək üçün zəruri maliyyə resursları mütəmadi olaraq təhlil edilməli və idarə heyətinə çatdırılmalıdır.	6.4; 7.6; 9.6
J.	Hadisələr baş verdikdən sonra böhranları, fəaliyyətin pozulması və fövqəladə halları nəzərdən keçirmək və hadisədən sonrakı icmalları "öyrənilmiş dərslər" prosesi çərçivəsində təhlil etmək, o cümlədən bu dərsləri gələcək təşkilati dayanıqlılıq planlaşdırılmasına daxil etmək üçün proses müəyyən edilməlidir.	10.2, 10.3

Əlavə D. 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 Təşkilati Dayanıqlılıq üzrə Mövzu Əsaslı Tələbə uyğunluğu sənədləşdirmək üçün bir seçim təqdim edir, lakin onun istifadəsi məcburi deyil.

Təşkilati dayanıqlılıq – İdarəetmə

Tələb	İcra edilən elementlərin əhatəsi və ya istisna üçün əsaslandırma	Sənədləşdirməyə istinad
A. Dayanıqlılığı nəzərə alan rəsmi təşkilati strategiya idarə heyəti tərəfindən müəyyən edilməli, direktorlar şurası tərəfindən ona nəzarət olunmalı və dəyişiklikləri idarə etmək və əməliyyatları davam etdirmək üçün tələb olunan əməliyyat, texnologiya və maliyyə elementlərini əhatə etməlidir. Dayanıqlılıq məqsədləri təşkilatın ümumi risk idarəetmə yanaşması ilə uyğunlaşdırılmalıdır.		
B. Dayanıqlılıq məqsədlərinin yerinə yetirilməsi ilə bağlı yeniləmələr mütəmadi olaraq nəzərdən keçirilməsi üçün direktorlar şurasına təqdim olunur. Bu, dayanıqlılığın strateji nəzarət, uzunmüddətli planlaşdırma prosesləri, varislik planlaşdırılması və təşkilatın mədəniyyətinə, o cümlədən kritik biznes fəaliyyətlərini dəstəkləmək üçün tələb olunan resurs və büdcə hazırlanması proseslərinə daxil edilməsini təmin edir.		
C. Kritik əməliyyatlar, texnoloji və maliyyə prosesləri üçün siyasət və prosedurlar müəyyən edilməli və nəzarət mühitini gücləndirmək məqsədilə mütəmadi olaraq nəzərdən keçirilməli, sınaq yoxlamaları aparılmalı və zərurət olduqda yenilənməlidir.		

D.	Hadisə idarəçiliyi strukturu yaradılmalı və təşkilati dayanıqlılıq məqsədlərinə nəzarət etmək və dəstəkləmək üçün istifadə olunmalıdır. Bu, qərar qəbuletmə iyerarxiyalarını, kommunikasiya və eskalasiya protokollarını, eləcə də rəhbərlik və əməliyyat rolları və məsuliyyətlərini əhatə edir.		
E.	Dayanıqlılıq üzrə uğur əldə etmək məqsədilə tələb olunan bilik və bacarıqları dövri olaraq təsdiqləmək və dayanıqlılıq proseslərində kritik rolları icra edən şəxslərin bilik və bacarıqlarını yenidən qiymətləndirmək üçün proses müəyyən edilməlidir.		
F.	Təşkilati dayanıqlılıq məqsədlərinə çatmaq üçün məlumat və hesabat strukturlarının yaradılmasında bütün müvafiq daxili və kənar maraqlı tərəflərin müəyyən edilməsi, prioritetlərin təyin edilməsi və cəlb edilməsini təmin edən proses müəyyən edilməlidir. Maraqlı tərəflərə yüksək rəhbərlik, əməliyyatlar, risk idarəçiliyi, İT, təchizat zənciri/satınalma, infrastruktur, insan resursları, maliyyə, hüquq, əminlik təminatçıları (daxili audit də daxil olmaqla), uyğunluq, ictimaiyyətlə əlaqələr, kritik təchizatçılar, müştərilər, tənzimləyicilər və digərləri daxil ola bilər.		

Təşkilati Dayanıqlılıq – Risklərin İdarə Edilməsi

Tələb	İcra edilən elementlərin əhatəsi və ya istisna üçün əsaslandırma	Sənədləşdirməyə istinad
A. Təşkilati dayanıqlılıqla bağlı risklər təşkilat üzrə mütəmadi olaraq müəyyən edilməli, qiymətləndirilməli və idarə olunmalıdır. Dayanıqlılıq riskləri təşkilatın strateji məqsədlərinə uyğunlaşdırılmalıdır. Dayanıqlılıq risklərinin idarə edilməsi prosesi əsas proseslərin qiymətləndirilməsini əhatə edir.		
B. Təşkilati dayanıqlılıq üzrə risklərin idarə olunmasına görə hesabatlılıq və məsuliyyət aydın şəkildə müəyyən edilməlidir. Təşkilati dayanıqlılıq üzrə risklərin idarə edilməsini, o cümlədən riskin azaldılması üçün zəruri resursları və təşkilati dayanıqlılığa yönələn yeni təhdidlərin müəyyən edilməsini müntəzəm olaraq izləmək		

	və hesabat vermək üçün məsul şəxs və ya komanda təyin edilməlidir.		
C.	Təşkilatın mövcud risk idarəetmə qaydaları və risk dözümlülüyü və ya müvafiq qanun və tənzimləyici tələblər əsasında qəbuledilməz hesab olunan səviyyəyə çatmış təşkilati dayanıqlılıq üzrə risk (yeni yaranan və ya əvvəllər müəyyən edilmiş) səviyyələrini izləmək və onları qısa bir zamanda müvafiq qurumlara çatdırmaq üçün proses müəyyən edilməlidir. Təşkilati dayanıqlılıq riskinin təsirləri nəzərdən keçirilməlidir.		
D.	Rəhbərlik böhran, fəaliyyətin pozulması və fövqəladə hallar baş verdikdə onlara cavab vermək və təsirlərindən bərpa olunmaq üçün proses tətbiq etməli və mütəmadi olaraq bu prosesləri sınaq yoxlamasından keçirməlidir. Hadisəyə reaksiya və bərpa prosesi aşkarlanma, prioritetləşdirmə, məhdudlaşdırma, bərpa və hadisədən sonrakı təhlili əhatə etməlidir. Hadisəyə reaksiya yanaşması ssenari təhlillərini və müxtəlif fəaliyyətin pozulmasına səbəb olan hadisələrə qarşı dövri stress testləri əhatə etməlidir.		

Təşkilati Dayanıqlılıq – Nəzarət Mexanizmləri

Tələb	İcra edilən elementlərin əhatəsi və ya istisna üçün əsaslandırma	Sənədləşdirməyə istinad
A. Vacib əməliyyatların davam etdirilməsi üçün tələb olunan minimum mal-material səviyyələrini müəyyən etmək və kritik üçüncü tərəf təminatçıları (təchizatçılar və satıcılar) müəyyən etmək üçün proses mövcud olmalıdır. Bu proses həmçinin alternativ təchizatçıların cari siyahısının saxlanılmasını da əhatə edir.		
B. Əməliyyatlar üçün kritik məlumatlar müəyyən edilir və təsnifləşdirilir. Məlumatların təsnifatı onların harada saxlanıldığını, kimlərin bu məlumatlara çıxış tələb etdiyini, onların hansı formada çıxışla təmin olunduğunu və fövqəladə hallarda ehtiyat nüsxəsinin olub-olmadığını və bərpa edilə bilib-bilməyəcəyini müəyyən etməyi əhatə edir.		

C.	Məlumat təhlükəsizliyi risklərini (o cümlədən kibertəhlükə risklərini) azaltmaq və böhran, fəaliyyətin pozulması və fövqəladə hallar zamanı həssas məlumatların qorunmasını təmin etmək üçün kritik İT nəzarətləri və davamlı monitorinq tətbiq edilməlidir. Nəzarət tədbirləri və davamlı monitorinq real vaxt rejimində təhdid kəşfiyyatı və çıxış imkanının yalnız səlahiyyətli istifadəçilərlə məhdudlaşdırılmasını əhatə edir.		
D.	Kritik İT aktivlərinin siyahısı tərtib edilməlidir. Aktivlərə böhranlar, fəaliyyətin pozulması və fövqəladə hallar zamanı əməliyyatları dəstəkləmək üçün tələb olunan avadanlıq, proqram təminatları və xidmətlər daxildir.		
E.	Biznesin davamlılığı və fəlakətdən bərpa planları hazırlanmalı və təyin olunmuş heyət və bərpa komandaları üçün müəyyən edilmiş rol və vəzifələri əhatə etməlidir. Planlar mütəmadi olaraq sınaq yoxlamalarından keçirilməli (məsələn, "masaüstü məşq" şəklində) və sınaq yoxlamalarının nəticələri, o cümlədən təkmilləşdirmə imkanları direktorlar şurasına və yüksək rəhbərliyə təqdim olunmalıdır.		
F.	Böhranlar, fəaliyyətin pozulması və fövqəladə hallar zamanı iş mühitini dəyişdirmək üçün proses müəyyən edilməlidir.		
G.	Təşkilati dayanıqlılığa təsir göstərə biləcək yeni təhdidləri və zəifikləri davamlı şəkildə izləmək və hesabat vermək üçün müəyyən bir proses yaradılmalıdır. Bu proses təşkilati dayanıqlılığın əməliyyatlarını, o cümlədən məlumat vermə sistemi və ya risk kəşfiyyatı və məlumat toplama sistemləri də daxil olmaqla, təkmilləşdirmək üçün imkanları müəyyən etmək, prioritetləşdirmək və həyata keçirmək üçün istifadə olunur.		
H.	Təşkilati dayanıqlılıqla bağlı heyətin təhsili və təlimi üçün bir proses yaradılmalı, bu proses onların riayət etməli olduqları siyasət və prosedurlardan və böhran, fəaliyyətin pozulması və fövqəladə hallar baş verdikdə atılmalı olan addımlardan xəbərdar olmalarını təmin etməlidir. Proses pozucu ssenarilərin simulyasiya olunduğu təlim məşqlərini də əhatə etməlidir.		
I.	Zəruri əməliyyat, insan, texnologiya və maliyyə resurslarının böhranlar,		

	fəaliyyətin pozulması və fövqəladə hallar zamanı büdcələndirilməsini və əlçatan olmasını təmin etmək üçün proses müəyyən edilməlidir. Təşkilati dayanıqlılığı dəstəkləmək üçün zəruri maliyyə resursları mütəmadi olaraq təhlil edilməli və direktorlar şurasına təqdim olunmalıdır.		
J.	Hadisələr baş verdikdən sonra böhranları, fəaliyyətin pozulması və fövqəladə halları nəzərdən keçirmək və hadisədən sonrakı icmalları "öyrənilmiş dərslər" prosesi vasitəsilə təhlil etmək, o cümlədən bu dərsləri gələcək təşkilati dayanıqlılıq planlaşdırılmasına daxil etmək üçün proses müəyyən edilməlidir.		

Əlavə E. Çərçivəyə Əlavə İstinadlar

Sahə	ISO-ya İstinad	Mövzu/Bənd başlıqları
İdarəetmə	ISO 22316:2017	Siyasət və strategiya; rəhbərliyin öhdəlikləri; ortaq baxışlar; mədəniyyət; kommunikasiya; davamlı təkmilləşdirmə.
Risklərin idarə edilməsi	ISO 31000:2018	Çərçivə/kontekst/meyarlar; riskin qiymətləndirilməsi; praktik tətbiq; monitorinq; ünsiyyət və məlumatlandırma.
Biznesin davamlılığı/fəlakətdən bərpanın əsasları	ISO 22301: 2019; ISO/TS 22317:2021	Biznesin Davamlılığının İdarə Edilməsi Sisteminin (BDİES/BCMS) konteksti, idarəçiliyi, planlaşdırılması və əməliyyatlar; Biznesə Təsirin Qiymətləndirilməsi Təhlili (BTQ/BIA) fəaliyyətləri və nəticələr.
Təchizat zəncirinin dayanıqlılığı	ISO/TS 22318:2021	Təchizatçılardan asılılığın təhlili; davamlılıq strategiyaları; alternativlər; əminlik təminatı üzrə tələblər.
İnformasiya və Kommunikasiya Texnologiyaları üzrə hazırlıq səviyyəsi	ISO/IEC 27031	İKT davamlılığı; bərpa hədəfləri; sınaq testləri və təkmilləşdirmələr; BDİES/ BCMS ilə əlaqələndirmə.

Daxili Auditorlar İnstitutu haqqında

Daxili Auditorlar İnstitutu (“IIA”), qeyri-kommersiya təşkilatı olaraq dünyanın müxtəlif ölkələrində 270,000-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

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