Dövlət qurumlarının informasiya təhlükəsizliyi mühitinin diaqnostikasının həyata keçirilməsi

QAYDALARI

1. Ümumi müddəalar

1.1. Bu Qaydalar mərkəzi və yerli icra hakimiyyəti orqanlarının, dövlət mülkiyyətində olan və paylarının (səhmlərinin) nəzarət zərfi dövlətə məxsus olan hüquqi şəxslərin, dövlət adından yaradılan publik hüquqi şəxslərin, digər büdcə təşkilatlarının və yerli özünüidarəetmə orqanlarının (bundan sonra – qurumlar) informasiya təhlükəsizliyinə aid əsas parametrlər siyahısını və məqbul hədlərini, habelə informasiya təhlükəsizliyi mühitinin diaqnostikasının həyata keçirilməsini müəyyən edir.

1.2. Bu Qaydalar kritik informasiya infrastrukturu obyektlərinə həmin sahəni tənzimləyən normativ hüquqi aktlara uyğun olaraq tətbiq edilir.

1.3. Bu Qaydalar kəşfiyyat və əks-kəşfiyyat fəaliyyətinin subyektlərinə şamil edilmir.

1.4. İnformasiya təhlükəsizliyi mühitinin diaqnostikasının (bundan sonra - diaqnostika) həyata keçirilməsinin məqsədləri aşağıdakılardır:

1.4.1. qurumların informasiya təhlükəsizliyi arxitekturasının müasir tələblərə uyğunluq dərəcələrinin müəyyən edilməsi;

1.4.2. informasiya təhlükəsizliyi üzrə təşkilati alətlərin mükəmməllik, texniki alətlərin etimadlılıq və kompetensiyalar təminatının adekvatlıq səviyyəsinin müəyyən edilməsi;

1.4.3. informasiya təhlükəsizliyinin davamlı təkmilləşdirilməsi üçün tələbatın müəyyən edilməsi.

2. Əsas anlayışlar

2.1. Bu Qaydaların məqsədləri üçün istifadə olunmuş anlayışlar aşağıdakı mənaları ifadə edir:

2.1.1. **informasiya təhlükəsizliyinin mühiti** – qurumlarda informasiya təhlükəsizliyinin təmin edilməsi ilə bağlı arxitekturanın, təşkilati və texniki alətlərin, işçilərin səriştəliliyinin, proseslərin və idarəetmə mexanizmlərinin aktual vəziyyətini və onların təkmilləşdirilməsi (inkişaf etdirilməsi) imkanlarını xarakterizə edən məcmu;

2.1.2. **informasiya təhlükəsizliyi mühitinin diaqnostikası** (bundan sonra - diaqnostika) – qurumların informasiya təhlükəsizliyi vəziyyətinin müəyyən edilməsi və informasiya təhlükəsizliyinin idarə edilməsi səviyyəsinin ölçülməsi məqsədilə həyata keçirilən qiymətləndirmə;

2.1.3. **diaqnostika meyarları** – diaqnostika altmeyarlarını əhatə edən göstəricilər toplusu;

2.1.4. **diaqnostika altmeyarları** – diaqnostikanın həyata keçirilməsi üçün istifadə edilən və müvafiq faizlə ölçülən göstəricilər;

2.1.5. **informasiya təhlükəsizliyinə aid əsas parametrlər siyahısı** – diaqnostika meyarlarının məcmusu;

2.1.6. **məqbul hədlər** – diaqnostika meyarları üzrə müəyyən edilmiş minimum icra olunmalı göstəricilər.

2.2. Bu Qaydalarda istifadə olunan digər anlayışlar "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununda, Azərbaycan Respublikası Prezidentinin 2018-ci il 12 sentyabr tarixli 263 nömrəli Fərmanı ilə təsdiq edilmiş "Dövlət informasiya ehtiyatları və sistemlərinin formalaşdırılması, aparılması, inteqrasiyası və arxivləşdirilməsi Qaydaları"nda və Azərbaycan Respublikasının digər normativ hüquqi aktlarında müəyyən edilmiş mənaları ifadə edir.

3. Diaqnostikanın mərhələləri

3.1. Diaqnostika aşağıdakı mərhələlərdə həyata keçirilir:

3.1.1. qurumlara diaqnostika meyarlarına, o cümlədən altmeyarlarına uyğun qiymətləndirmə aparılması və cavablandırılması barədə məktubla müraciət edilməsi;

3.1.2. qurumlardan daxil olan müvafiq sənədlərin və məlumatların toplanılması;

3.1.3. toplanılmış sənədlərin, məlumatların yoxlanılması və təhlili;

3.1.4. yerində baxış keçirilməsi və müvafiq qeydlərin aparılması;

3.1.5. təhlil edilmiş sənədlərin və məlumatların, habelə yerində baxışın nəticəsinə dair arayışın və hesabatların hazırlanması.

4. Qurumlarda diaqnostikanın həyata keçirilməsi qaydaları

4.1. Qurumlarda diaqnostika Azərbaycan Respublikasının Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti (bundan sonra – Xidmət) tərəfindən təsdiq edilən fəaliyyət planına uyğun olaraq ildə bir dəfə olmaqla həyata keçirilir.

4.2. Diaqnostikanın keçiriləcəyi tarix və müddət barədə məlumatlar diaqnostikanın başlamasına ən azı 30 (otuz) gün qalmış rəsmi qaydada prosesin keçiriləcəyi quruma təqdim edilir.

4.3. Diaqnostikanın həyata keçirilməsi üçün ilkin olaraq informasiya təhlükəsizliyinə aid əsas parametrlərin siyahısı üzrə bu Qaydaların 1 nömrəli əlavəsi ilə müəyyən edilmiş meyarlara və altmeyarlara uyğun qiymətləndirmə sualları diaqnostikanın keçiriləcəyi quruma məktubla göndərilir.

4.4. Qurumda bu Qaydaların 4.3-cü bəndində nəzərdə tutulmuş məktuba daxil olduğu tarixdən 15 (on beş) iş günü müddətində baxılır, qiymətləndirmə sualları cavablandırılır və zəruri sənədlər məxfi kargüzarlıq qaydalarına uyğun hazırlanmış cavab məktubu ilə Xidmətə təqdim edilir.

4.5. Bu Qaydaların 4.4-cü bəndinə əsasən təqdim edilmiş məlumatlar və sənədlər üzrə dəqiqləşdirmə aparılması məqsədilə Xidmət tərəfindən qurumda yerində baxış keçirilə bilər. Yerində baxış diaqnostika keçirilən quruma ən geci 3 (üç) iş günü əvvəldən xəbər verilməklə keçirilir. Yerində müəyyən olunmuş tarixdə hər hansı səbəbdən baxış keçirilməsi mümkün olmadıqda yeni tarix təyin olunur.

4.6. Təqdim olunmuş sənədlər və məlumatlar yerində baxış zamanı tam və ya qismən təsdiqini tapmadıqda, yaxud qiymətləndirmə sualları natamam cavablandırıldıqda qiymətləndirmə zamanı belə hallar nəzərə alınır və bu Qaydaların 2 nömrəli əlavəsi ilə müəyyən edilmiş formada yerində baxış aktı tərtib edilir.

4.7. Təqdim olunmuş sənədlərin və məlumatların təhlili, habelə tərtib edilmiş yerində baxış aktı nəzərə alınmaqla Xidmət tərəfindən arayış hazırlanır. Həmin arayışda meyarlar, o cümlədən altmeyarlar və qiymətləndirmə sualları üzrə cari vəziyyət, çatışmazlıqlar, diaqnostikanın müəyyən edilən nəticəsi (yekun qiymətləndirmə faizlə göstərilməklə) qeyd olunur.

4.8. Hazırlanmış arayışın layihəsi 10 (on) iş günü müddətində diaqnostikanın nəticələrinə münasibət bildirilməsi üçün diaqnostika aparılan quruma təqdim edilir. Qurum diaqnostikanın nəticəsi ilə razılaşmadıqda bu barədə rəyi diaqnostikanın nəticəsinə dair arayışa əlavə olunur. Qurumun diaqnostika nəticələri ilə bağlı rəyinə bu Qaydaların 4.10-cu bəndində nəzərdə tutulmuş hesabatın hazırlanması zamanı baxılır.

4.9. Xidmət tərəfindən aşkar olunmuş çatışmazlıqların aradan qaldırılması ilə bağlı təkliflər verilir, zərurət yarandıqda quruma əməli və metodiki kömək göstərilir.

4.10. Qurumlarda aparılmış diaqnostikanın nəticələri barədə hesabat “İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında” Azərbaycan Respublikası Prezidentinin 2012-ci il 26 sentyabr tarixli 708 nömrəli Fərmanına uyğun olaraq Xidmət tərəfindən Azərbaycan Respublikasının Prezidentinə mütəmadi təqdim olunan məlumata daxil edilir.

4.11. Xidmət mühafizə olunan şəxslərin, qorunan və strateji obyektlərin, həmçinin onların təhlükəsizliyini təmin edən dövlət orqanlarının və dövlət sirrinə aid edilən fərdi məlumatların informasiya ehtiyatları və sistemləri istisna olmaqla, diaqnostika nəticəsində çatışmazlıqlar aşkar edilən fərdi məlumatların, Elektron Hökumət İnformasiya Sisteminə və “Hökumət buludu”na inteqrasiya və miqrasiya olunan dövlət informasiya ehtiyatlarının və sistemlərinin siyahısını Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyinə təqdim edir.

5. Qurumların informasiya təhlükəsizliyi mühitinin qiymətləndirilməsi

5.1. Qurumların informasiya təhlükəsizliyi mühitinin qiymətləndirilməsi informasiya təhlükəsizliyinə aid əsas parametrlər siyahısı üzrə həyata keçirilir.

5.2. Hər bir meyarın altmeyarları, altmeyarların isə vəzifə və hədəfləri, habelə qiymətləndirmə sualları vardır.

5.3. Qiymətləndirmə sualları əsasında informasiya təhlükəsizliyindəki əhəmiyyəti və roluna görə hər bir meyara və altmeyara münasibətdə ayrıca diaqnostika yükü (qiyməti) müəyyənləşdirilir.

5.4. Altmeyarların diaqnostika yükü (qiyməti) hər bir qiymətləndirmə sualı üzrə tələb nəzərə alınmadıqda 0 balla, nisbətən nəzərə alındıqda 0,25 balla, nəzərə alınıb, lakin nisbi çatışmazlıqlar olduqda 0,75 balla, tam nəzərə alındıqda isə 1 balla qiymətləndirilir.

5.5. Ballar toplandıqda hər bir altmeyarın ümumi diaqnostika yükünə (qiymətinə) münasibətdə əldə olunmuş müvafiq faiz göstəriciləri ilə altmeyarların aid olduğu meyarın qurumun informasiya təhlükəsizliyi vəziyyətinə ümumi təsiri müəyyənləşdirilir.

5.6. Meyarların qurumun ümumi informasiya təhlükəsizliyi mühitinə təsiri "Təşkilati idarəetmə" meyarı üzrə 25 faiz, "Əməkdaşlar və təchizatçılar" meyarı üzrə 25 faiz, "Fiziki təhlükəsizlik" meyarı üzrə 15 faiz və "Avadanlığa, proqram təminatı və məlumatların təhlükəsizliyi" meyarı üzrə isə 35 faiz olaraq hesablanır.

5.7. Qurumun yekun informasiya təhlükəsizliyi vəziyyətinin nəticəsi 0-100 faiz arası nisbətində qiymətləndirilir. Qiymətləndirmə sualları üzrə əldə olunan cavablara görə müvafiq göstərici "Təhlükəsizlik idarəetməsi qeyri-kafi, ciddi risklər mövcuddur" nəticəsi üzrə "0-55" faiz, "Əsas nəzarətlər var, lakin bəzi proseslərdə boşluqlar mövcuddur" nəticəsi üzrə "56-75" faiz və "Sistem bütövlükdə idarə olunur, risklər nəzarət altındadır" nəticəsi üzrə "76-100" faiz arasında qiymətləndirilir.

6. Diaqnostikanın həyata keçirilməsi ilə bağlı vəzifələr

6.1. Diaqnostikanın həyata keçirilməsi ilə bağlı qurum:

6.1.1. diaqnostikanın aparılması ilə bağlı məsul şəxs (şəxslər) təyin edir və Xidmətə həmin şəxs (şəxslər) barədə məlumat verir;

6.1.2. Xidmətin məktubunu cavablandırır, qiymətləndirilmənin keçirilməsi üçün tələb edilən sənədləri və məlumatları bu Qaydalarla müəyyən olunmuş müddətdə Xidmətə təqdim edir;

6.1.3. ilkin diaqnostikanın (özünüqiymətləndirmənin) həyata keçirilməsini təmin edir;

6.1.4. diaqnostikanın aparılması, o cümlədən yerində baxış və rəy sorğularının keçirilməsi üçün Xidmətə lazımi şərait yaradılması ilə bağlı tədbirlər görür, habelə diaqnostikanın aparılmasına maneçilik törədilməməsini təmin edir;

6.1.5. diaqnostikanın nəticəsi ilə bağlı təqdim edilən arayışa uyğun olaraq aşkar olunmuş boşluq və çatışmazlıqların aradan qaldırılması, o cümlədən qurumda informasiya təhlükəsizliyi səviyyəsinin artırılması ilə əlaqədar mümkün qısa müddətdə tədbirlər görür və bu barədə Xidmətə məlumat verir.

6.2. Diaqnostika aparılan qurumun məsul əməkdaşı (əməkdaşları) aktın məzmunu barədə öz mülahizələrini təqdim edə, habelə aktı imzalamaqdan imtina etməsinin səbəblərini göstərə bilər.

7. Qurumların informasiya təhlükəsizliyinə məqbul hədlər

Diaqnostikanın hər bir meyarı üzrə məqbul hədlər aşağıdakı cədvəldə qeyd olunan göstəricilər üzrə hesablanır:

Sıra № -si	Meyarın adı	Ümumi yükü (qiyməti) faizlə	Məqbul həddi (minimum toplanmalı faiz)	Əsaslandırma
1.	Təşkilati idarəetmə	25%	≥ 65%	Siyasət, məsuliyyət və idarəetmə sahə üzrə ümumi fəaliyyətin əsasını təşkil etdiyindən, bu sahədə zəiflik digər sahələrin effektivliyini azaldır. Bu səbəbdən göstərilən istiqamət nisbətən yüksək nəticə tələb edir
2.	Əməkdaşlar və təchizatçılar	25%	≥ 60%	İnsan amili risklərinin yüksək olmasına baxmayaraq, risklərin texnoloji nəzarətlərlə qismən kompensasiya oluna bilinməsi ilə nisbətən aşağı nəticə tələb olunur
3.	Fiziki təhlükəsizlik	15%	≥ 55%	Əsasən infrastruktur səviyyəsindədir, bəzi çatışmazlıqlar texniki tədbirlərlə əvəz oluna biləcəyindən minimal nəticə tələb olunur
4.	Avadanlıq, proqram təminatı və məlumatların təhlükəsizliyi	35%	≥ 70%	Ən kritik texniki sahə olduğu üçün burada kompromis riski birbaşa xidmət dayanmalarına səbəb ola biləcəyindən digərləri ilə müqayisədə daha yüksək nəticə tələb olunur

“Dövlət qurumlarının informasiya təhlükəsizliyi mühitinin
diaqnostikasının həyata keçirilməsi Qaydaları”na

1 nömrəli Əlavə

MEYARLAR VƏ ALTMEYARLAR			QİYMƏTLƏNDİRMƏ SUALI	Hər bir sualın informasiya təhlükəsizliyi diaqnostika-sındakı yükü (qiyməti)	Qiymətləndirmə suallarına cavablar: Tələb nəzərə alınmayıb - 0 bal, Nisbətən nəzərə alınıb - 0,25 bal, Nəzərə alınıb, nisbi çatışmazlıqlar var - 0,75 bal, Tam nəzərə alınıb - 1 bal	ALT MEYAR-LAR ÜZRƏ NƏTİCƏ	MEYAR-LAR ÜZRƏ NƏTİCƏ	ÜMUMİ NƏTICƏ
1.	**Təşkilati idarəetmə**			**2500**				
1.1.	**İnformasiya təhlükəsizliyi siyasəti və əlaqəli sənədlər**			**90**				
	Vəzifə	Hədəf						
	İnformasiya təhlükəsizliyi siyasəti və bu sahədə spesifik predmetlər üzrə alt-siyasətlər müəyyən edilməli, rəhbərlik tərəfindən təsdiq edilməli, dərc edilməli, aidiyyəti işçilərə və müvafiq maraqlı tərəflərə çatdırılmalı və təsdiq edilməli, planlaşdırılmış fasilələrlə və əhəmiyyətli dəyişikliklər baş verdikdə yenidən baxılmalıdır	Biznes, hüquqi, qanunvericilik, tənzimləyici və müqavilə tələblərinə uyğun olaraq idarəetmə istiqamətinin davamlı uyğunluğunu, adekvatlığını, effektivliyini və informasiya təhlükəsizliyinə dəstəyi təmin etmək	1) İnformasiya təhlükəsizliyi siyasəti mövcuddurmu, təsdiq olunubmu?	22	0	**0%**		
			2) İnformasiya təhlükəsizliyi siyasəti qurumun müəyyən edilmiş tələblərinə və məqsədlərinə uyğundurmu?	22	0			
			3) İnformasiya təhlükəsizliyi sahəsində spesifik predmetlər üzrə alt-siyasətlər, qaydalar, təlimatlar mövcuddurmu?	18	0			
			4) İnformasiya təhlükəsizliyi ilə əlaqədar müvafiq sənədlər (alt-siyasətlər, qaydalar, təlimatlar) rəsmi təsdiq olunubmu?	14	0			
			5) İnformasiya təhlükəsizliyi ilə əlaqəli müvafiq sənədlər əməkdaşlara və digər üçüncü tərəf təmsilçilərinə aidiyyəti üzrə əlçatandırmı?	14	0			

1.2.	**İnformasiya təhlükəsizliyi üzrə rollar və vəzifə bölgüsü**			**50**				
	Vəzifə	Hədəf						
	İnformasiya təhlükəsizliyi üzrə rollar və məsuliyyətlər qurumun ehtiyaclarına uyğun olaraq müəyyən edilməli və rollar arasında məsuliyyətlərin bölgüsü aparılmalıdır	Qurum daxilində informasiya təhlükəsizliyinin idarə edilməsi üçün təsdiq edilmiş struktur yaratmaq	1) Mühafizə olunmalı informasiya və onunla bağlı digər aktivlər (proseslər, məlumatlar, proqram, proqram-texniki, texniki və mühəndis təminatı vasitələri, rollar) müəyyən olunubmu?	12	0	**0%**		
			2) İnformasiya təhlükəsizliyi üzrə vəzifələrin (məsuliyyətlərin) rollar üzrə bölgüsü aparılıbmı?	12	0			
			3) Bu bölgü informasiya təhlükəsizliyi siyasətinə və müvafiq sənədlərə (alt-siyasətlərə, qaydalara, təlimatlara) uyğundurmu?	10	0			
			4) İnformasiya təhlükəsizliyinin təşkilinə, nəzarət vəzifələrinin müəyyən olunmasına və onların icrasına nəzarətə ümumi cavabdeh struktur bölmə və ya ştat vahidi müəyyən olunubmu?	8	0			
			5) İnformasiya təhlükəsizliyi üzrə rolların icrası üçün kompetensiya (bilik və bacarıq) tələbatları müəyyən olunubmu? İcraçıların bu tələbatlara uyğunluğu təmin olunurmu? Bunun üçün mütəmadi qiymətləndirmə və təkmilləşdirmə təmin olunurmu?	8	0			
1.3.	**Məsuliyyətlər və səlahiyyət bölgüsü**			**50**				
	Vəzifə	Hədəf						
	Ziddiyyət təşkil edən səlahiyyətlər və məsuliyyət sahələri bir-birindən ayrılmalıdır	Aldatma, səhv və informasiya təhlükəsizliyi nəzarətindən yan keçmə riskini azaltmaq	1) Qurum rəhbərliyi işçilərin informasiya təhlükəsizliyi ilə bağlı rol və məsuliyyətlərini rəsmi formada təyin edibmi?	14	0	**0%**		
			2) Fəaliyyət prosesləri üzrə zəruri olan informasiyaya giriş səlahiyyətlərinin rollar üzrə bölgüsü aparılıbmı, həmçinin proseslərdə rollar üzrə məsuliyyət bölgüsü nəzərə alınıbmı?	12	0			
			3) Fəaliyyət proseslərini dəstəkləyən proqram təminatlarına, onların funksional imkanlarına rollar üzrə səlahiyyətlər bölgüsü, eləcə də bu təminatlar üçün lazım olan texniki və mühəndis aktivlərinə, onların seqmentlərinə, modullarına rollar üzrə səlahiyyətlər bölgüsü aparılıbmı?	10	0			
			4) Qurumda icraçı, təsdiqedici, nəzarətçi kimi bir-biri arasında ziddiyyətli olan fəaliyyət sahələrinə aid vəzifələr, funksiyaların eyni bir şəxsə həvalə olunmasının qarşısı alınıbmı, fəaliyyət sahələri müəyyən olunubmu?	8	0			

			5) Məsuliyyət və səlahiyyət bölgülərinə əməl olunmasına monitorinq, audit və rəhbərliyin nəzarəti kimi digər idarəetmə vasitələri nəzərdə tutulubmu, tətbiq olunurmu?	6	0			
1.4.	**Rəhbərliyin məsuliyyəti**			**80**				
	Vəzifə	Hədəf						
	Rəhbərlik bütün müvafiq işçilər və maraqlı tərəflərdən qurumun təsdiq olunmuş siyasət və proseduralarına uyğun şəkildə informasiya təhlükəsizliyinə yanaşmalarını tələb etməlidir	Rəhbərliyin informasiya təhlükəsizliyində öz rolunu və bütün personalın bu sahədə öhdəliklərini bilməsini və yerinə yetirməsini təmin etmək üçün tədbirlər görmək	1) İnformasiya təhlükəsizliyi ilə əlaqəli siyasətlərin hazırlanmasında, nəzərdən keçirilməsində və analiz edilməsində cavabdeh şəxs təyin edilibmi?	26	0	**0%**		
			2) Rəhbərlik bütün işçilərdən informasiya təhlükəsizliyi siyasətinə və qurumun müvafiq siyasət və prosedurlarına uyğun şəkildə davranmalarını və informasiya təhlükəsizliyi tələblərini tətbiq etmələrini tələb edirmi?	22	0			
			3) İnformasiya təhlükəsizliyi siyasətlərinin, tələblərinin, şərtlərinin, prosedurlarının pozulmasını vaxtında və obyektiv aşkarlama üçün müvafiq mexanizm və ya digər müstəqil vasitələr rəhbərlik tərəfindən tətbiq olunurmu?	18	0			
			4) Qurumun informasiya təhlükəsizliyi siyasətini, tələb və şərtlərini müvafiq işçilərin və podratçıların yerinə yetirməsi üçün həvəsləndirmə mexanizmi rəhbərlik tərəfindən tətbiq olunurmu?	14	0			
1.5.	**Səlahiyyətli orqanlarla əlaqə**			**50**				
	Vəzifə	Hədəf						
	Müvafiq dövlət orqanları ilə lazımi əlaqələr yaradılmalı və saxlanılmalıdır	Qurum və müvafiq hüquqi, tənzimləyici və nəzarət orqanları arasında informasiya təhlükəsizliyi ilə bağlı müvafiq məlumat axınını təmin etmək	1) Qurumda informasiya təhlükəsizliyi insidentləri, fövqəladə hallar zamanı əlaqə saxlanılmalı olunan müvafiq dövlət orqanları müəyyən olunubmu?	20	0	**0%**		
			2) Hər bir hal üçün səlahiyyətli orqanlar ilə əlaqəyə keçəcək şəxs təyin edilibmi?	17	0			
			3) Qurumda informasiya təhlükəsizliyi üzrə fövqəladə hallara qarşı əks-tədbirlər görmək üçün dövlət orqanlarından dəstək istənilməsinin şərtləri müəyyən olunubmu?	13	0			
1.6.	**Təhdid kəşfiyyatı**			**60**				
	Vəzifə	Hədəf						
	İnformasiya təhlükəsizliyi təhdidləri ilə bağlı məlumatlar toplanmalı və təhdidləri öyrənmək üçün təhlil edilməlidir	Təhdidlərin təsir imkanlarının azaldılma tədbirlərinin görülməsi üçün məlumatlılığı təmin etmək	1) Qurum təhdid kəşfiyyatı məlumatlarını toplamaq, təhlil etmək və istifadə etmək üçün rəsmi bir prosesə malikdirmi?	17	0			
			2) Təhdid kəşfiyyatı məlumatlarının idarə olunması ilə bağlı məsul şəxslər və ya komandalar müəyyən edilibmi?	14	0			

			3) Təhdid kəşfiyyatının strateji, taktiki və operativ səviyyələr üzrə hərəkətləri və əhatə sahəsi müəyyən olunubmu?	12	0	**0%**		
			4) Qurum ümumi təhdid kəşfiyyatını təkmilləşdirmək üçün qarşılıqlı əsasda digər qurumlarla təhdid kəşfiyyatı üsulları və məlumatları paylaşılırmı?	10	0			
			5) Təhdid kəşfiyyatının dəqiqliyi, aktuallığı və mənbələrinin etibarlılığı, informasiya təhlükəsizliyi idarəetmə mexanizmlərinin effektivliyinə təsiri müəyyən olunurmu?	7	0			
1.7.	**Layihələrin idarə edilməsində informasiya təhlükəsizliyi**			**50**				
	Vəzifə	Hədəf						
	Layihənin idarə edilməsinə informasiya təhlükəsizliyi inteqrasiya edilməlidir	Layihələr və onların realizasiyası ilə bağlı olan informasiya təhlükəsizliyi risklərinin emalını layihələrin həyat dövrünü idarəetmə müddətindən başlayaraq səmərəli təmin etmək	1) Layihələr çərçivəsində informasiya təhlükəsizliyi risklərinin müəyyən edilməsi və aradan qaldırılmasını təmin etmək üçün informasiya təhlükəsizliyi qurumun layihələrin idarə edilməsinə erkən mərhələdə inteqrasiya olunurmu?	20	0	**0%**		
			2) Layihə ərzində informasiya təhlükəsizliyinin təmin edilməsini izləmək üçün nəzarət mexanizmləri mövcuddurmu ?	17	0			
			3) Layihələr çərçivəsində informasiya təhlükəsizliyi üzrə vəzifələr müəyyən olunurmu və layihənin idarə edilməsi metodologiyalarında təyin edilmiş rollara həvalə olunurmu?	13	0			
1.8.	**İnformasiyanı və onunla əlaqəli olan digər aktivləri inventarlaşdırma**			**60**				
	Vəzifə	Hədəf						
	İnformasiya və informasiya emalı vasitələri ilə bağlı olan aktivlər müəyyən edilməli və bu aktivlərin inventar siyahısı tərtib edilməli və saxlanmalıdır	İnformasiya təhlükəsizliyini qorumaq və müvafiq mülkiyyət hüququnu təyin etmək üçün qurumun məlumatlarını və digər əlaqəli aktivlərini müəyyən etmək	1) Məlumatların və digər əlaqəli aktivlərin inventarlaşdırılması həyata keçirilirmi, informasiya təhlükəsizliyi baxımından onların əhəmiyyəti müəyyən olunubmu? Bu inventarlaşdırılma prosesi risklərin idarə edilməsinin ilkin addımı kimi nəzərdə tutulurmu?	17	0	**0%**		
			2) İnformasiyanın və digər əlaqəli aktivlərin inventar siyahısının tam və mötəbər, aidiyyəti üzrə əlçatan və ya konfidensial olması təmin olunubmu?	14	0			
			3) Məlumat və digər əlaqəli aktivlərdən məqbul istifadə qaydaları, işləmə (saxlanma, istifadə, ötürülmə və silinmə) prosedurları və digər əlaqəli	12	0			

			proseslər müəyyən edilib, sənədləşdirilib və həyata keçirilibmi?					
			4) Müəyyən edilmiş hər bir aktiv üçün sahib və onun məsuliyyət dairəsi təyin olunubmu?	10	0			
			5) Aktivlərin inventarlaşdırılması prosesi mütəmadi olaraq izlənilirmi, bunun üçün müvafiq göstəricilərdən istifadə olunurmu?	7	0			
1.9.	**Aktivlərin geri qaytarılması**			**50**				
	Vəzifə	Hədəf						
	Bütün işçilər və kənar tərəf istifadəçiləri ilə əmək münasibətlərinə xitam veriləndə, müqavilə və ya saziş müddəti qurtaranda qurumun onlarda olan bütün aktivlərini qaytarmalıdırlar.	Əmək münasibətlərinin, müqaviləsinin və ya sazişinin dəyişdirilməsi və ya xitam verilməsi zamanı qurumun aktivlərini qorumaq.	1) İşçilər və digər maraqlı tərəflərlə əmək müqaviləsi və ya razılaşmada dəyişiklik olduğu və ya ləğv edildiyi hallarda aktivlər geri qaytarılırmı?	14	0		**0%**	
			2) Qurumun aktivlərin qaytarılması üçün rəsmi proseduru varmı? Əgər varsa, bu prosedur həyata keçirilirmi?	12	0			
			3) Qaytarılmalı olan aktivlərin siyahısı varmı?	10	0			
			4) İşdən azad edilmə (xitam) barədə xəbərdarlıq dövründə işdən azad edilən işçilər (və kontragentlər) tərəfindən müvafiq informasiyanın surətinin çıxarılmasına qurum nəzarəti təmin edə bilirmi?	8	0			
			5) İşçi və ya digər maraqlı tərəflər cari əməliyyatlar ilə bağlı vacib biliklərə malikdirsə, həmin biliklərin sənədləşdirilərək quruma ötürülməsi təmin olunurmu?	6	0			
1.10.	**İnformasiyanın təsnifatlaşdırılması**			**70**				
	Vəzifə	Hədəf						
	İnformasiya konfidensiallıq, tamlıq, əlçatanlıq, mötəbərlik xassələri, habelə normativ aktların tələbləri və maraqlı tərəflərin müvafiq tələbatları əsasında qurumun informasiya təhlükəsizliyi ehtiyaclarına uyğun olaraq təsnif edilməlidir	Qurum üçün əhəmiyyətinə uyğun olaraq məlumatın qorunması ehtiyaclarının müəyyən edilməsini və başa düşülməsini təmin etmək.	1) Qurumda informasiyanın təsnifatlaşdırılmasına aid alt-siyasət müəyyən olunubmu?	20	0		**0%**	
			2) İnformasiya konfidensiallıq, tamlıq, əlçatanlıq və mötəbərlik xassələrinə uyğun olaraq və maraqlı tərəflərin müvafiq tələbləri nəzərə alınmaqla təsnifləşdirilirmi?	17	0			
			3) İnformasiyanın emalı, saxlanılması və ötürülməsi onların təsnifatlarına uyğun mühitdə həyata keçirilmi?	14	0			
			4) İnformasiyaya, onun təsnifatlaşdırılmasına cavabdeh tərəf müəyyən olunubmu?	11	0			
			5) İnformasiyanın təsnifatı mütəmadi olaraq yenilənirmi?	8	0			
	İnformasiyanın nişanlanması			**50**				
	Vəzifə	Hədəf						

1.11.	Qurum tərəfindən qəbul olunmuş təsnifat sxeminə uyğun olaraq informasiyanın nişanlanması üçün müvafiq prosedurlar hazırlamaq və tətbiq etmək lazımdır.	İnformasiyanın təsnifatına aid məlumat mübadiləsini asanlaşdırmaq və məlumatların emalı və idarə edilməsinin avtomatlaşdırılmasını dəstəkləmək.	1) Qurumun informasiyanın nişanlanması üçün rəsmi prosedurları varmı? İnformasiya reyestri, metaverilənlər kataloqu varmı?	20	0	**0%**		
			2) İnformasiyanın nişanlanması prosesinə tələblər və təhlükəsizlik tədbirləri müəyyən edilirmi? Risklər reyestrinə müvafiq qeydiyyat aparılıbmı?	15	0			
			3) İşçilər və kontragentlər nişanlama prosedurları ilə tanışdırlarmı?	10	0			
			4) Nişanların asanlıqla tanınması təmin olunubmu?	5	0			
1.12.	**İnformasiyanın ötürülməsi**			**50**				
	Vəzifə	Hədəf						
	Bütün növ kommunikasiya vasitələrinin köməyi ilə informasiyanın qurum daxilində və qurumla digər tərəflər arasında ötürülməsini mühafizə etmək üçün prosedurları və idarəetmə vasitələri işlənib hazırlanmalıdır	Qurum daxilində və hər hansı kənar maraqlı tərəflə ötürülən məlumatların təhlükəsizliyini qorumaq	1) Qurumda informasiyanın ötürülməsi ilə bağlı alt-siyasət, üsullar, prosedurlar və razılaşmalar müəyyən olunubmu?	14	0	**0%**		
			2) İnformasiya mübadiləsi üçün istifadə olunan texniki vasitələr müəyyən olunubmu? (məsələn: e-poçt, bulud xidmətləri, fiziki media və s.)	12	0			
			3) İnformasiyanın ötürülməsi zamanı müvafiq şifrələmə və ya digər mühafizə tədbirləri tətbiq olunurmu?	10	0			
			4) Ötürülən informasiyanın təsnifatı nəzərə alınırmı?	8	0			
			5) İnformasiyanın şifahi, fiziki yaddaş daşıyıcıları və şəbəkə vasitəsilə ötürülməsi üçün standart mühafizə tələbləri müəyyən olunubmu?	6	0			
1.13.	**Girişin idarə edilməsi**			**90**				
	Vəzifə	Hədəf						
	Müraciətlərin idarə edilməsi prosedurunu biznes və təhlükəsizlik tələbləri əsasında tərtib etmək, sənədləşdirmək və tətbiq etmək lazımdır	İnformasiyaya və digər əlaqəli aktivlərə icazəli müraciəti (girişi) təmin etmək və icazəsiz girişin qarşısını almaq	1) Qurum müraciətin (girişin) idarə edilməsi üçün alt-siyasət müəyyən edibmi?	25	0	**0%**		
			2) İnformasiyaya fiziki və məntiqi giriş üçün nəzarət qaydaları və s. başqa əlaqəli proseslər, fəaliyyət davamlılığı və informasiya təhlükəsizliyi tələbləri əsasında yaradılır və həyata keçirilirmi?	22	0			
			3) Qurumun müraciətin (girişin) idarə edilməsi üçün müvafiq nəzarət mexanizmləri (məsələn: istifadəçi adı və şifrə, biometrik sistemlər və s.) tətbiq edilirmi?	18	0			
			4) İstifadəçilərin sistemə girişləri mütəmadi olaraq izlənilirmi? Hər hansı bir uyğunsuzluq aşkar edildikdə reaksiya verilirmi? Verilən reaksiyaların qeydiyyatı aparılırmı?	14	0			

			5) Müraciət (giriş) hüquqları ilə informasiyanın təsnifatı və fiziki perimetrin təhlükəsizlik tələbləri arasında uzlaşdırma aparılırmı?	11	0			
1.14.	**İdentifikasiya idarəetməsi**			**70**				
	Vəzifə	Hədəf						
	İdentifikasiya informasiyasının həyat dövrü tam idarə olunmalıdır	İnformasiyaya və digər əlaqəli aktivlərə müraciət (giriş) icazəsi alan şəxslərin və sistemlərin unikal identifikasiyasını, həmçinin icazə hüquqlarının müvafiq təyin olunmasını təmin etmək	1) Yeni istifadəçilərin qeydiyyatı müvafiq prosedura uyğun həyata keçirilirmi?	20	0	**0%**		
			2) ID-lərə (identifikasiya vasitələri) ehtiyac qalmadıqda onların vaxtında dayandırılması və ya ləğv edilməsi təmin olunurmu?	17	0			
			3) Qurumun identifikasiya prosesində istifadə üçün metodlar (məsələn: istifadəçi adı və şifrə, biometrik sistemlər, çox faktorlu identifikasiya) müəyyən olunubmu?	14	0			
			4) İdentifikasiya və autentifikasiyaya aid mühüm hadisələrin qeydiyyatının aparılması və jurnallarda saxlanılması təmin olunurmu?	11	0			
			5) Qurum identifikasiya prosesini mütəmadi olaraq audit edirmi?	8	0			
1.15.	**Autentifikasiya idarəetməsi**			**90**				
	Vəzifə	Hədəf						
	Autentifikasiya informasiyasının (parolların, kriptoqrafik açarların və autentifikasiya kodlarını generasiya etmək üçün aparat tokenlərində saxlanılan digər verilənlərin) paylanması və idarə edilməsi formal idarəetmə prosesi vasitəsilə nəzarətdə saxlanılmalıdır	Subyektlərin düzgün autentifikasiyasını təmin etmək və autentifikasiya proseslərində uğursuzluqların qarşısını almaq	1) Autentifikasiya məlumatlarının ötürülməsi və idarə edilməsinə aid prosedur müəyyən olunubmu?	25	0	**0%**		
			2) Parolu idarəetmə siyasəti və sistemi mövcuddurmu?	22	0			
			3) Autentifikasiya məlumatlarının şifrələnməsi və ya digər mühafizə tədbirləri tətbiq olunurmu?	18	0			
			4) Autentifikasiya məlumatlarının oğurlanması və ya sızdırılması halları olarsa, onların qarşısının alınması üçün müvafiq prosedurlar müəyyən olunubmu?	14	0			
			5) Çoxfaktorlu autentifikasiya (MFA) sisteminin tətbiqi varmı?	11	0			
1.16.	**Müraciət (giriş) hüquqları**			**80**				
	Vəzifə	Hədəf						
	İnformasiyaya və digər əlaqəli aktivlərə müraciət (giriş) hüquqları qurumun predmet ilə bağlı siyasətinə və girişə	İnformasiyaya və digər əlaqəli aktivlərə girişin biznes tələblərinə uyğun olaraq müəyyən edilməsini və icazə verilməsini təmin etmək	1) İstifadəçilərin müraciət (giriş) hüquqlarının müəyyən edilməsi və idarə edilməsi üçün rəsmi prosedurlar varmı?	26	0	**0%**		
			2) İstifadəçilərin sistemə müraciət (giriş) hüquqları müəyyən edilirmi? Hər bir istifadəçi üçün müvafiq meyarlara əsaslanırmı?	22	0			

	nəzarət proseduruna uyğun olaraq təmin edilməli, nəzərdən keçirilməli, dəyişdirilməli və ləğv edilməlidir		3) İstifadəçi hüquqları ilə bağlı hərəkətlərin qeydiyyatı aparılırmı?	18	0			
			4) Giriş təmin edilməli olan informasiya emalı vasitələrinin siyahısı varmı?	14	0			
1.17.	**Təchizatçılar ilə münasibətlərdə informasiya təhlükəsizliyi**			**70**				
	Vəzifə	Hədəf						
	Təchizatçının məhsul və ya xidmətlərindən istifadə ilə bağlı informasiya təhlükəsizliyi risklərini idarə etmək üçün proseslər və prosedurlar müəyyən edilməli və həyata keçirilməlidir	Təchizatçılarla münasibətlərdə razılaşdırılmış informasiya təhlükəsizliyi səviyyəsini saxlamaq	1) Təchizatçılar ilə münasibətlərdə informasiya təhlükəsizliyini idarəetmə proseduru müəyyən olunubmu?	20	0	**0%**		
			2) Təchizatçılar tərəfindən təqdim olunan məhsul və xidmətlərin istifadəsi ilə bağlı təhlükəsizlik riskləri və həllər müəyyən olunubmu?	17	0			
			3) Təchizatçılar tərəfindən təqdim olunan məhsul və xidmətlərin növlərini (məsələn: İKT xidmətləri, logistika, kommunal xidmətlər, maliyyə xidmətləri, İKT infrastrukturu komponentləri), qurumun informasiya təhlükəsizliyinə (konfidensiallığa, tamlığa, əlçatanlığa, mötəbərliyə) mümkün təsirləri müəyyən olunubmu?	14	0			
			4) Məhsul və xidmətlərin təchizatında qurumun informasiya təhlükəsizliyinin monitorinqi təmin olunurmu?	11	0			
			5) Məhsul və xidmətlərin təchizatının dayandırılma və ya xitam verilmə şərtləri müəyyən olunubmu?	8	0			
1.18.	**Təchizatçılar ilə sazişlər çərçivəsində informasiya təhlükəsizliyi məsələlərinə baxılması**			**50**				
	Vəzifə	Hədəf						
	Müvafiq informasiya təhlükəsizliyi tələbləri müəyyən edilməli və onlar təchizatçı ilə işgüzar münasibətlərin tipindən asılı olaraq razılaşdırmalıdır	Təchizatçılarla işgüzar münasibətlərdə razılaşdırılmış informasiya təhlükəsizliyi səviyyəsini saxlamaq	1) Hər bir təchizatçıya təqdim ediləcək və ya ondan əldə ediləcək məlumatların siyahısı və informasiya təminatı üsulları müəyyən olunubmu?	14	0	**0%**		
			2) Təchizatçıya qurumun informasiya təhlükəsizliyi üzrə aidiyyəti tələbləri və təchizatçının bununla əlaqədar öhdəlikləri və sahədə monitorinq mexanizmi müəyyən olunubmu?	12	0			
			3) Təchizatçıya qurumun informasiya təhlükəsizliyi üzrə aidiyyəti tələblərinin yerinə yetirməməsinə görə kompensasiya şərtləri müəyyən olunubmu?	10	0			

			4) Təchizatçı tərəfindən yaranan uyğunsuzluqların həlli və münaqişələrin həlli prosedurları müəyyən olunubmu?	8	0			
			5) Təchizatçı ilə müqavilənin sonunda başqa təchizatçıya və ya qurumun özünə təhvil şərtləri, prosedurları müəyyən olunubmu?	6	0			
1.19.	**İKT sahəsində təchizat zəncirində informasiya təhlükəsizliyinin idarə edilməsi**			**70**			**0%**	
	Vəzifə	Hədəf						
	Təchizatçı ilə sazişlərə İKT (o cümlədən bulud hesablama (cloud computing) xidmətlərinin və məhsullarının təchizat zənciri ilə əlaqəli informasiya təhlükəsizliyi risklərinə dair tələblər daxil edilməlidir	Təchizatçılarla işgüzar münasibətlərdə razılaşdırılmış informasiya təhlükəsizliyi səviyyəsini saxlamaq	1) İKT məhsulunun və ya xidmətinin təqdim edilməsi zamanı tətbiq olunacaq informasiya təhlükəsizliyi tələbləri müəyyən olunubmu?	20	0	**0%**		
			2) İKT məhsulları təchizatçılarından məhsullarda istifadə olunan proqram komponentlərini, həmçinin məhsulların funksiyalarını və konfiqurasiyanı təsvir edən məlumatın təqdim edilməsi tələb olunurmu?	17	0			
			3) Təchizatçıların İKT məhsullarının, komponentlərinin orijinal olmasını və onların spesifikasiyasına uyğun olmasını, dəyişdirilməməsini təmin edən, performansın spesifikasiyaya uyğun olmasını yoxlayan prosedur müəyyən olunubmu?	14	0			
			4) İKT məhsullarının tələb olunan etimad səviyyəsində olması müəyyən olunurmu? Təhdidlərin qarşısının alınmasının və aşkarlanmasının İKT məhsulun sistemin həyat dövrünün layihələndirmə, hazırlama, inteqrasiya, istismar və müşayiət (“design, development, integration, operations & maintenance”) mərhələlərində həyata keçirilirmi?	11	0			
			5) İKT məhsulların, komponentlərin həyat dövrünə olan informasiya təhlükəsizliyi riskləri qiymətləndirilirmi?	8	0			
1.20.	**Təchizatçıların xidmətlərində olan dəyişikliklərin monitorinqi, təhlili və idarə edilməsi**			**50**				
	Vəzifə	Hədəf						
	Qurum təchizatçının informasiya təhlükəsizliyini təminetmə	Təchizatçı ilə müqavilələrə uyğun olaraq, informasiya təhlükəsizliyinin və	1) Təchizatçının göstərdiyi xidmətləri, xüsusilə müqavilədə nəzərdə tutulmuş informasiya təhlükəsizliyi şərtlərinə riayət olunması monitorinq (izlənilməsi) və təhlil olunurmu?	14	0			

	metodlarında təcrübələrində və xidmətlərin göstərilməsində dəyişiklikləri mütəmadi izləməli, nəzərdən keçirməli, qiymətləndirməli və idarə etməlidir	xidmətlərin göstərilməsinin razılaşdırılmış səviyyəsini saxlamaq	2) Təchizatçılar tərəfindən xidmətlərə edilən dəyişikliklər nəzarətdə saxlanılırmı?	12	0	**0%**		
			3) Göstərilən xidmətlərdə informasiya təhlükəsizliyi insidentləri haqqında məlumat vermə şərtləri müəyyən olunubmu?	10	0			
			4) Göstərilən xidmətlərdə informasiya təhlükəsizliyi hadisələrinə, insidentlərinə və fövqəladə hallara cavab vermə, zəifliklər aşkarlama sahəsində məsuliyyət bölgüsü müəyyən olunubmu?	8	0			
			5) Göstərilən xidmətlərin davamlılığını təminetmə proseduru müəyyən olunubmu?	6	0			
1.21	**Bulud xidmətlərindən istifadə üçün informasiya**			**50**				
	Vəzifə	Hədəf						
	Qurumun informasiya təhlükəsizliyi tələblərinə uyğun olaraq bulud xidmətləri üçün müraciət edilməsi, xidmətlərin istifadəsi, idarə edilməsi və dayandırılması prosesləri qurulmalıdır.	Bulud xidmətlərindən istifadə üçün informasiya təhlükəsizliyi vəziyyətini dəqiqləşdirmək və idarə etmək.	1) Qurum bulud xidmətlərindən istifadə ilə bağlı alt-siyasətini müəyyən edibmi?	18	0	**0%**		
			2) Bulud xidmətlərinin əldə edilməsi, onlardan istifadə etmək, idarə etmək və çıxmaq üçün proseslər qurumun informasiya təhlükəsizliyi tələblərinə uyğun olaraq müəyyən edilibmi?	9	0			
			3) Bulud xidməti provayderini seçərkən təhlükəsizlik meyarları nəzərə alınırmı?	6	0			
			4) Xidmət provayderinin təhlükəsizlik sertifikatları (məsələn: ISO 27001, ISO 27017 və ya ISO 27018 üzrə) mövcudluğu yoxlanılırmı?	4	0			
			5) Məlumatların saxlanma yerləri (data residency) ilə bağlı provayderlə razılaşmalar varmı?	4	0			
			6) Bulud xidmətlərinə giriş hüquqlarının idarə olunması həyata keçirilirmi?	3	0			
			7) Bulud xidmətlərində fəaliyyətlər mütəmadi olaraq monitorinq olunurmu?	3	0			
			8) Bulud xidmətlərindən istifadə dayandırıldıqda məlumatların silinməsi və ya köçürülməsi proseduru varmı?	2	0			
			9) Qurum bulud xidmətlərindən istifadə ilə bağlı potensial təhlükəsizlik risklərini qiymətləndirirmi?	1	0			
1.22.	**Süni intellekt**			**50**				
	Vəzifə	Hədəf						
	İnformasiya təhlükəsizliyini idarəetmə üzrə qərarvermə, riskləri,	İnformasiya təhlükəsizliyini idarəetmə üzrə tədbirlərdə operativliyi	1) Süni intellekt həllərindən istifadə ilə bağlı alt-siyasət müəyyən edilibmi?	14	0			
			2) Süni intellekt həllərinin tətbiqi zamanı informasiya təhlükəsizliyi tələbləri	12	0			

	insidentləri müəyyənetmə, o cümlədən funksionallıqda anomaliyaları və konfiqurasiyada sanksiyasız dəyişiklikləri aşkaretmə, qabaqlayıcı və bərpaedici əks-tədbirləri hazırlama işlərində süni intellekt texnologiyalarının imkanlarından istifadə etmək	və optimallığı artırmaq, o cümlədən insan faktorununun minimallaşdırılmasını təmin etmək	nəzərə alınırmı?			**0%**		
			3) Süni intellekt modellərinin öyrədilməsində istifadə olunan məlumatlar müəyyən edilibmi? Bu məlumatlar fərdi və ya konfidensial xarakter daşıyırmı?	10	0			
			4) Fərdi və ya konfidensial xarakter daşıyan məlumatların anonimləşdirilməsi tətbiq edilirmi?	8	0			
			5) Süni intellekt həllərinin risk dəyərləndirilməsi aparılırmı?	6	0			
1.23.	**İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi sahəsində planlaşdırma və hazırlıq işləri**			**70**				
	Vəzifə	Hədəf						
	Təşkilat informasiya təhlükəsizliyi insidentlərinin idarə edilməsi proseslərini, rollarını və məsuliyyətlərini müəyyən etmək, qurmaq və çatdırmaqla informasiya təhlükəsizliyi insidentlərinin idarə edilməsini planlaşdırmalı və hazırlamalıdır	İnformasiya təhlükəsizliyi hadisələri ilə bağlı kommunikasiya da daxil olmaqla, informasiya təhlükəsizliyi insidentlərinə tez, effektiv, ardıcıl və nizamlı cavab vermək	1) Qurumda informasiya təhlükəsizliyi insidentlərinin idarə edilməsi həyata keçirilirmi? İnsidentlərinin idarəetmə prosedurları və rollar üzrə məsuliyyət bölgüsü müəyyən olunubmu?	25	0	**0%**		
			2) Qurum informasiya təhlükəsizliyi insidentlərinin idarə edilməsi proseslərini, rollarını və məsuliyyətlərini təyin edərək, hazırlayaraq və kommunikasiya edərək informasiya təhlükəsizliyi insidentlərini idarə etmək üçün rəsmi plan yaradıb və hazırlıq işləri görübmü?	12	0			
			3) İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi planında müvafiq mərhələlər tətbiq olunurmu? Süni intellekt əsaslı texnologiyalar tətbiq olunurmu?	8	0			
			4) Plan informasiya təhlükəsizliyi insidentlərinin aşkar edilməsi, təsdiqi, təsnifatı və həlli ilə bağlı prosedurları əhatə edirmi? İnformasiya təhlükəsizliyi insidentlərinə, onların kateqoriyalarına uyğun olaraq, qiymətləndirmə və cavabvermə üçün müvafiq ssenarilər və avtomatlaşdırma vasitələri, kompetensiya tələbləri, prioritetlər və reqlamentlər, hədlər müəyyən olunubmu?	6	0			

			5) İnsidentlərə müdaxilə zamanı istifadə üçün zəruri resurslar mövcuddurmu?	5	0			
			6) Qurum mütəmadi olaraq insident idarəçiliyi üzrə simulyasiya və ya sınaq keçirirmi?	4	0			
			7) İnsident zamanı məlumatlandırılması zəruri olan daxili və xarici maraqlı tərəflər müəyyən edilibmi?	4	0			
			8) Qurumda insidentlərin idarə olunması planı müvafiq qanunvericiliyə və standartlara uyğundurmu?	3	0			
			9) İnsidentlərin idarə edilməsi planı mütəmadi olaraq nəzərdən keçirilir və yenilənirmi?	3	0			
1.24.	**İnformasiya təhlükəsizliyi hadisələrinin qiymətləndirilməsi və qərarların qəbul edilməsi**			**70**		**0%**		
	Vəzifə	Hədəf						
	Təşkilat informasiya təhlükəsizliyi hadisələrini qiymətləndirməli və onların informasiya təhlükəsizliyi insidentləri kimi təsnif edilib-edilməməsinə qərar verməlidir	İnformasiya təhlükəsizliyi hadisələrinin effektiv təsnifatını və prioritetləşdirilməsini təmin etmək	1) İnformasiya təhlükəsizliyi hadisələrini müəyyənetmə üçün meyarlar, təsir dərəcələrini qiymətləndirmə və təsnifatlaşdırma mexanizmi, aləti, texnologiyaları müəyyən olunubmu?	20	0			
			2) İnformasiya təhlükəsizliyi insidentlərini, fövqəladə halları aşkarlama üçün meyarlar müəyyən olunubmu?	17	0			
			3) İnformasiya təhlükəsizliyi hadisələrinin qeydiyyatları (sistem jurnalı), insidentlərin və fövqəladə halların uçotu aparılırmı? Bu qeydiyyatlar və uçot monitorinq, kiber-kriminalistika üçün dəlil-sübut kimi yetərli, yararlı hesab olunurmu, istifadə olunurmu?	14	0			
			4) Bu qeydiyyatlar və uçot insidentlərə, fövqəladə hallara cavabvermə qərarları üçün istinad kimi yetərli, yararlı hesab olunurmu, istifadə olunurmu?	11	0			
			5) Bu qərarların qəbuluna məsuliyyət daşıyan şəxs müəyyən olunubmu?	8	0			
	İnformasiya təhlükəsizliyi insidentlərinə reaksiya (cavabvermə)			**80**				
	Vəzifə	Hədəf						
	İnformasiya təhlükəsizliyi insidentlərinə sənədləşdirilmiş prosedurlara uyğun cavab verilməlidir	İnformasiya təhlükəsizliyi ilə bağlı insidentlərə operativ və effektiv cavab verilməsini təmin etmək	1) Qurumda informasiya təhlükəsizliyi insidentlərinə reaksiya (cavabvermə) prosedurları mövcuddurmu?	18	0			
			2) İnformasiya təhlükəsizliyi insidentlərinə sənədləşdirilmiş prosedurlara uyğun olaraq cavab verilirmi?	14	0			

1.25.			3) Təhlükəsizlik insidentlərinə cavab vermək üçün xüsusi bir qrup (məsələn: Kiber İnsidentlərə Müdaxilə Qrupu - CSIRT) yaradılıbmı?	13	0	**0%**		
			4) Təhlükəsizlik insidentlərini idarə etməkdən məsul olan komandanın rolları və məsuliyyətləri müəyyən edilibmi?	11	0			
			5) Təhlükəsizlik insidentləri araşdırılır və kök səbəbləri müəyyən edilirmi? O cümlədən təhdidləri (təhdid sxemi ilə), təhdidlərin istifadə etdiyi zəifliklər və digər uyğunsuzluqları, fəsadları qiymətləndirmə, həmçinin uyğunsuzluqları və fəsadları aradan qaldırma – "təhlükəsizliyin normal səviyyəsini" bərpaetmə mexanizmləri müəyyən olunubmu?	10	0			
			6) Təhlükəsizlik insidentləri ilə bağlı sənədlər (məsələn: hesabatlar) müvafiq şəkildə hazırlanır və saxlanılırmı?	8	0			
			7) İnformasiya təhlükəsizliyi insidentlərindən əldə edilən biliklər informasiya təhlükəsizliyinə nəzarəti gücləndirmək və təkmilləşdirmək üçün istifadə edilirmi?	6	0			
1.26.	**İnformasiya təhlükəsizliyi insidentlərindən öyrənmə, dərsalma**			**50**		**0%**		
	Vəzifə	Hədəf						
	İnformasiya təhlükəsizliyi ilə bağlı insidentlərdən əldə edilən biliklərdən informasiya təhlükəsizliyinə nəzarəti gücləndirmək və təkmilləşdirmək üçün, o cümlədən insidentlərin baş vermə ehtimalını və ya onların təsirini azaltmaq üçün istifadə edilməlidir	Gələcək hadisələrin ehtimalını və ya nəticələrini azaltmaq	1) Qurumda informasiya təhlükəsizliyi hadisələrinin fasiləsiz monitorinqinə və informasiya təhlükəsizliyi insidentlərinin təsirlərinin qiymətləndirilməsinə aid mexanizmlər müəyyən olunubmu? Bu mexanizmlər həyata keçirilirmi?	14	0			
			2) İnformasiya təhlükəsizliyi insidentlərinin qiymətləndirilməsi nəticəsində əldə edilən biliklər toplanılırmı? Qurumun informasiya təhlükəsizliyi üzrə biliklər, çıxarılan dərslər, həllər bazası varmı?	12	0			
			3) Bu biliklərdən eyni və ya oxşar hallarda istifadə üçün onların tamlığı, əlçatanlığı, konfidensiallığı və mötəbərliyi təmin olunurmu?	10	0			
			4) Bu biliklərdən insidentlərə cavabvermə ssenarilərində və insidentləri, riskləri idarəetmə planlarında istifadə olunurmu?	8	0			
			5) Bu biliklərdən insidentləri idarəetmə sahəsində təlim-tədris proqramlarında və təcrübə mübadiləsində istifadə olunurmu?	6	0			

1.27.	**İnformasiya təhlükəsizliyi hadisələrinə aid sübutların idarə edilməsi**			**50**				
	Vəzifə	Hədəf						
	Qurum informasiya təhlükəsizliyi hadisələri ilə bağlı dəlil, sübut olan informasiyanın müəyyən edilməsi, toplanması, əldə edilməsi və mühafizəsi prosedurlarını müəyyən etməli və tətbiq etməlidir	İnformasiya təhlükəsizliyi insidentləri ilə bağlı dəlil, sübutların intizam və hüquqi tədbirlər məqsədilə ardıcıl və effektiv idarə olunmasını təmin etmək	1) Qurum informasiya təhlükəsizliyi hadisələrinə aid sübutların intizam tədbirləri və kiber-kriminalistika prosesləri üçün müəyyən edilməsi, toplanması, əldə edilməsi, sənədləşdirilməsi və mühafizəsi üçün prosedurlar müəyyən edib və həyata keçiribmi?	10	0	**0%**		
			2) Sübutların toplanması prosesinin addımları müəyyən olunubmu?	9	0			
			3) Sübutların toplanması zamanı onların bütövlüyünü təmin etmək üçün müvafiq tədbirlər görülürmü? Bu sübutları özündə daşıya bilən fiziki daşıyıcıların yığılması üçün prosedur müəyyən olunubmu?	8	0			
			4) Elektron və ya fiziki sübutların toplanmasında müvafiq texnologiya və alətlərdən istifadə olunurmu?	7	0			
			5) Sübutların saxlanması zamanı onların məxfiliyini qorumaq üçün müvafiq mexanizmlər tətbiq olunurmu? Sübutlar olan informasiyanın tamlığının və ilkin vəziyyətinin saxlanılması və qorunması üçün prosedur müəyyən olunubmu?	6	0			
			6) Sübutların saxlanma müddəti və arxivlənmə prosedurları necə tənzimlənir? Sübutlar olan informasiyanın surətinin yaradılması üçün prosedur müəyyən olunubmu?	5	0			
			7) Sübutların analizi zamanı üçüncü tərəflərin cəlb olunması mümkündürmü və bu proses idarə olunurmu?	4	0			
			8) Sübutların mənbəyi, toplanma tarixi və vaxtı barədə məlumatlar detallı şəkildə qeyd olunurmu? Sübut olan informasiyanın nüsxələrinin orijinal ilə eyni olduğu, bu informasiyanın toplanıldığı zaman həmin informasiyanın yazıldığı, qeydə alındığı sistemin düzgün işlədiyi sübut oluna, təmin oluna bilinirmi?	1	0			
	Davamlılığının pozulması halında informasiya təhlükəsizliyi			**70**				
	Vəzifə	Hədəf						

1.28.	Qurum əlverişsiz şəraitdə, məsələn: böhran və ya fəlakət baş verərkən, özünün informasiya təhlükəsizliyi və informasiya təhlükəsizliyinin davamlılığının idarə edilməsi üçün plan və tələblərini müəyyən etməlidir	İnformasiya təhlükəsizliyinin davamlılığının pozulması zamanı informasiyanın və digər əlaqəli aktivlərin mühafizəsini təmin etmək	1) İnformasiya təhlükəsizliyini idarəetmə alətlərinin təhlükəsizlik tələblərinin pozulduğu hallarda təkmilləşdirilməsinə və uyğunlaşdırılmasına aid tələblər müəyyən olunubmu?	20	0	**0%**		
			2) Bu tələblər fəaliyyətin davamlılığını idarəetmə tələbləri ilə uzlaşdırılıbmı?	17	0			
			3) Kritik fəaliyyət proseslərinin informasiya təhlükəsizliyi ilə bağlı pozulma və ya dayanma hallarına bu proseslərin davamlılığına dəstək və ya davamlılığın bərpa planları, o cümlədən məqbul hədlər müəyyən olunubmu, sınaqdan keçirilibmi, tətbiq olunurmu?	14	0			
			4) Qurumda fəaliyyət proseslərinin və İKT xidmətlərinin informasiya təhlükəsizliyi baxımından davamlılığının idarə olunması üçün müvafiq alətlər müəyyən edilmişdirmi? Həmin alətlər tətbiq olunurmu və onların fəaliyyəti üçün zəruri dəstək təmin edilirmi?	11	0			
			5) Qurumda fəaliyyət davamlılığı pozulan hallara aid alternativ imkanlar, kompensasiya və təkmilləşdirmə mexanizmləri müəyyən olunubmu?	8	0			
	Biznesin (fəaliyyətin) davamlılığına İKT-nin hazırlığı			**80**				
	Vəzifə	Hədəf						
1.29.	İKT-nin hazırlığının təminetmə tədbirləri planlaşdırılmalı, həyata keçirilməli, aktual vəziyyətdə saxlanmalı və biznesin davamlılığı hədəfləri və İKT davamlılığı tələbləri baxımından sınaqdan keçirilməlidir	İnformasiya təhlükəsizliyinin davamlılığının pozulması zamanı qurumun informasiyanın və digər əlaqəli aktivlərinin əlçatanlığını təmin etmək	1) Fəaliyyətin davamlılığının təmin edilməsi üçün lazımi sənədlər və resurslar mövcuddurmu? Fəaliyyətə təsirin təhlili (“business impact analysis, BIA”) proseduru, maksimal məqbul dayanma hədləri (“maximum acceptable outage. MAO”), fəaliyyətin davamlılığının minimal hədəfləri (“minimum business continuity objective, MBCO”) müəyyən olunubmu?	18	0			
			2) İKT hazırlığı fəaliyyətin davamlılığı məqsədlərinə və İKT-nin dayanıqlılığı tələblərinə uyğun olaraq planlaşdırılır, həyata keçirilir, saxlanılır və sınaqdan keçirilirmi? Prioritet, kritik fəaliyyət prosesləri müəyyən olunubmu? Fəaliyyət davamlılığını bərpa etmək üçün nəzərdə tutulan bərpa nöqtəsi (“recovery point objective; RPO”) və nəzərdə tutulan bərpa müddəti (“recovery time objective, RTO”), ehtiyac olan resurslar, İKT xidmətləri müəyyən olunubmu?	14	0			

			3) Qurumda BIA nəticələri və İKT xidmətləri üzrə risk qiymətləndirmələri əsasında hazırlanmış, fəaliyyətin davamlılığını pozuntu baş verməzdən əvvəl, pozuntu zamanı və pozuntudan sonra təmin etməyə yönəlmiş rəsmi "İKT Davamlılıq Planı" mövcuddurmu? Əgər mövcuddursa, həmin plan hansı fövqəladə halları və fasilə və ya pozuntu növlərini əhatə edir?	13	0	**0%**		
			4) Qurumun kritik İKT infrastrukturunun dayanıqlılığını təmin etmək üçün müvafiq texnologiyalar tətbiq olunurmu?	11	0			
			5) Kritik sistemlər üçün ehtiyat enerji mənbələri və ya alternativ infrastrukturlar mövcuddurmu?	10	0			
			6) Tərəfdaşlarla bağlanılmış müqavilələrdə fövqəladə hallara dair xüsusi tələblər qeyd olunubmu?	8	0			
			7) Biznesin davamlılığının idarə edilməsi proseduru mövcuddurmu?	6	0			
1.30.	**Qanunvericilik, normativ və müqavilə üzrə tələblər**			**90**				
	Vəzifə	Hədəf						
	Bütün müvafiq qanunvericilik, normativ və müqavilə tələblərini və bu tələblərin yerinə yetirilməsinə qurumun yanaşmasını aydın müəyyən etmək, sənədləşdirmək və hər bir informasiya sistemi və qurum üçün aktuallığını saxlamaq lazımdır	İnformasiya təhlükəsizliyi ilə bağlı qanunvericilik, normativ və müqavilə tələblərinə əməl olunmasını təmin etmək	1) İnformasiya təhlükəsizliyinə aid qanunvericilik, normativ tələblər və müqavilə öhdəlikləri tam müəyyən olunubmu? İnformasiyanın əlçatanlığını, mötəbərliyini, tamlığını və konfidensiallığını təmin edən mexanizm formalaşdırılıb tətbiq olunurmu?	25	0	**0%**		
			2) İnformasiya təhlükəsizliyinin təşkilati və texniki idarəetmə alətlərinin, təchizatçılarla müqavilələrin işlənib hazırlanmasında, tətbiqində, təkmilləşdirilməsində, məsuliyyət bölgülərinin aparılmasında qanunvericilik, normativ tələblər nəzərə alınırmı?	22	0			
			3) Qurumun fəaliyyətinə informasiya təhlükəsizliyi sahəsində olan qanunvericilik, normativ tələblər toplanılıb təsnifatlaşdırılıbmı? Bu tələblər toplusunun aktuallığı mütəmadi təmin olunurmu?	18	0			
			4) Qurumda informasiya təhlükəsizliyi sahəsində hüquqi məsləhət xidməti formalaşdırılıbmı, habelə tətbiq olunurmu?	14	0			
			5) Müştərilərlə, təchizatçılarla, sığorta edənlərlə müqavilələrə informasiya təhlükəsizliyi üzrə müvafiq tələblər daxil edilirmi?	11	0			

1.31.	**Əqli mülkiyyət hüquqları**			**50**				
	Vəzifə	Hədəf						
	Əqli mülkiyyət hüquqları ilə bağlı və patentli proqram təminatı məhsullarının istifadəsi üzrə qanunvericilik, normativ və müqavilə tələblərinə riayət edilməsinin təmin olunması üçün müvafiq prosedurlar müəyyən olunmalı və tətbiq olunmalıdır	Əqli mülkiyyət hüquqları və patentli məhsullarından istifadə ilə bağlı qanunvericilik, normativ və müqavilə tələblərinə əməl olunmasını təmin etmək	1) Əqli mülkiyyət hüquqlarını ehtiva edən materiallara – proqram təminatına və sənədlərə müəlliflik hüquqlarının, modellərə olan hüquqların, ticarət nişanlarının, patentlərin və proqramın mənbə koduna (ilkin mətninə) verilən lisenziyaların uçotu formalaşdırılıbmı? Bu uçotun aktuallığı mütəmadi təmin olunurmu?	14	0	**0%**		
			2) Əqli mülkiyyət hüquqları ilə bağlı qanunvericilik, normativ və müqavilə tələblərinin siyahısı müəyyən olunubmu? Bu siyahının aktuallığı mütəmadi təmin olunurmu?	12	0			
			3) Bu tələblərə riayət edilməsinin təmin olunması üçün müvafiq prosedurlar müəyyən olunubmu?	10	0			
			4) Əqli mülkiyyət hüquqlarına əməl olunmasına aid alt-siyasət müəyyən olunubmu? Tətbiq olunurmu?	8	0			
			5) Əqli mülkiyyət hüquqlarının pozulmasına qarşı məsuliyyət və sanksiyalar müəyyən olunubmu?	6	0			
1.32.	**Qeydiyyat, dəlil yazılarının mühafizəsi**			**50**				
	Vəzifə	Hədəf						
	Qanunla müəyyən olunmuş, qanunvericilik, normativ və müqavilə və biznes tələblərinə müvafiq olaraq, qeydiyyat, dəlil-sübut və digər yazılar itkidən, məhv olmadan, saxtalaşdırmadan, icazəsiz müraciət və icazəsiz nəşrdən qorumaq lazımdır	Qanunvericilik, normativ və müqavilə tələblərinə, habelə qeydiyyat, dəlil-subut və digər yazıların mühafizəsi və mövcudluğu ilə bağlı ictimai gözləntilərə uyğunluğu təmin etmək	1) İnformasiya təhlükəsizliyi ilə bağlı olan hadisələrin qeydiyyatını idarəetmə alt-siyasəti müəyyən olunubmu?	14	0	**0%**		
			2) Qeydiyyata alınacaq hadisələrin seçilməsi mexanizmi müəyyən olunubmu?	12	0			
			3) Bu qeydiyyatların tamlığının və mötəbərliyinin mühafizəsi, qeydlərin saxtalaşdırılmasının qarşısının alınması mexanizmi və qeydlərin həyat dövrü sxemləri müəyyən olunubmu?	10	0			
			4) Qeydiyyatların saxlanılma müddətləri (təsnifat kateqoriyalarına uyğun), formatları və saxlanılma daşıyıcılarından bərpa mexanizmi müəyyən olunubmu? Qeydlərin saxlanması üçün istifadə olunan daşıyıcıların xarab olma ehtimalı nəzərə alınırmı?	8	0			
			5) Saxlanılma müddətləri başa çatan qeydiyyatların məhv edilməsi və arxivləşdirilməsi, arxivlərin şifrələnməsi mexanizmi, şifrələnmiş arxivlər və ya rəqəmsal imzalarla əlaqəli kriptoqrafik açarlar və proqramlar müəyyən olunubmu?	6	0			

1.33.	**Fərdi identifikasiya informasiyasının (Fİİ) konfidensiallığı və mühafizəsi**			**90**				
	Vəzifə	Hədəf						
	Konfidensiallıq və fərdi identifikasiya informasiyasının (Fİİ) mühafizəsi üzrə müvafiq qanunvericilik, normativ və müqavilə və biznes tələbləri dəqiqləşdirilməli və təmin edilməlidir	Fİİ-nin mühafizəsinin informasiya təhlükəsizliyi aspektləri ilə bağlı qanunvericilik, normativ və müqavilə və biznes tələblərinə uyğunluğunu təmin etmək	1) Fərdi identifikasiya informasiyasının – Fİİ (“personally identifiable information, PII”) konfidensiallığına və mühafizəsinə aid alt-siyasət müəyyən olunubmu?	25	0	**0%**		
			2) Konfidensiallığa təsirlərin qiymətləndirilməsi – KTQ (“privacy impact assessment, PIA”) mexanizmi və hesabatı formaları müəyyən olunurmu, standart tövsiyələr nəzərə alınırmı? Bu mexanizm tətbiq olunurmu?	22	0			
			3) Fərdi identifikasiya informasiyasının konfidensiallığına və mühafizəsinə dair risklər qiymətləndirilibmi? Risklərin emal həlləri müəyyən olunubmu? Bu risklər və həllər risklər reyestrinə daxil edilibmi?	18	0			
			4) Fərdi identifikasiya informasiyasının konfidensiallığına və mühafizəsinə aid idarəetmə alətləri, rollar və məsuliyyət bölgüsü müəyyən olunubmu?	14	0			
			5) Fərdi identifikasiya informasiyasının konfidensiallığına və mühafizəsinə kompetensiyalı məsul əməkdaş təyin olunubmu? Təşkilati ştat strukturunda müvafiq ştat vahidi müəyyən olunubmu?	11	0			
1.34.	**İnformasiya təhlükəsizliyinin müstəqil yoxlanılması**			**50**		**0%**		
	Vəzifə	Hədəf						
	İnformasiya təhlükəsizliyinin idarə edilməsi və onun icrasına qurumun yanaşması (yəni, idarəetmə məqsədləri, informasiya təhlükəsizliyinin idarəetmə vasitələri, siyasətlər, prosedurlar) planlaşdırılmış intervallarla və ya	İnformasiya təhlükəsizliyinin idarə edilməsində qurumun yanaşmasının davamlı uyğunluğunu, adekvatlığını və effektivliyini təmin etmək	1) İnformasiya təhlükəsizliyi vəziyyətinin qiymətləndirilməsi üçün rəhbərlik tərəfindən plan müəyyən olunubmu?	14	0			
			2) Bu planda qiymətləndirmə üçün tələb olunan meyarlar və sübutların toplusu, təkmilləşdirilmə tələb edilən sahələrin müəyyən edilməsi nəzərdə tutulurmu?	12	0			
			3) Qiymətləndirmənin həyata keçirilməsi üçün zəruri bilik, bacarıq və təcrübəyə malik əməkdaşlar və ya ixtisaslaşmış kənar təşkilatlar müəyyən edilmişdirmi? Qiymətləndirmənin etibarlılığını, obyektivliyini və qərəzsizliyini təmin etmək	10	0			

	əhəmiyyətli dəyişiklik baş verdikdə, müstəqil şəkildə yoxlanılmalıdır		məqsədilə həmin tərəflərin müstəqilliyi təmin olunubmu?					
			4) Bu qiymətləndirmənin nəticələrinin, o cümlədən tövsiyələrin qeydiyyatları və onların toplanıb saxlanılması, rəhbərliyə hesabatların təqdimatı mexanizmləri müəyyən olunubmu? Bu mexanizmlər tətbiq olunurmu?	8	0			
			5) Bu qiymətləndirmənin nəticələrinin analizi və tövsiyələrin sintezi mexanizmi müəyyən olunubmu?	6	0			
1.35.	**İnformasiya təhlükəsizliyi üzrə siyasətlərə, prosedurlara və standartlara uyğunluq**			**50**				
	Vəzifə	Hədəf						
	Rəhbərlər öz səlahiyyətləri daxilində informasiya emalı və prosedurlarının müvafiq təhlükəsizlik siyasətləri, standartları və hər hansı digər təhlükəsizlik tələblərinə uyğunluğunu müntəzəm şəkildə nəzərdən keçirməlidir.	İnformasiya təhlükəsizliyinin qurumun informasiya təhlükəsizliyi siyasətinə, predmetlər üzrə alt-siyasətlərinə, prosedurlarına və standartlarına uyğun olaraq həyata keçirilməsini və idarə olunmasını təmin etmək.	1) İnformasiya təhlükəsizliyi üzrə təyin olunmuş tələblərin yerinə yetirilməsinin rəhbərlik, məhsul və xidmətlərə cavabdehlər, informasiya sahibləri tərəfindən qiymətləndirilməsinə aid prosedur müəyyən olunubmu?	14	0	**0%**		
			2) Bu qiymətləndirilmənin müntəzəm və səmərəli olması üçün avtomatik ölçmə və hesabat alətləri nəzərdə tutulubmu?	12	0			
			3) Bu qiymətləndirilmə nəticəsində aşkar olunan uyğunsuzluqların aradan qaldırılmasına aid prosedurlar müəyyən olunubmu?	10	0			
			4) Bu qiymətləndirmənin nəticələrinin, o cümlədən tövsiyələrin qeydiyyatları və onların toplanıb saxlanılması, müstəqil qiymətləndirmə subyektlərinə və cavabdeh tərəflərə verilməsi mexanizmləri müəyyən olunubmu?	8	0			
			5) Bu qiymətləndirilmə nəticəsində aşkar olunan uyğunsuzluqların aradan qaldırılmasının nəticələrini qeydiyyata alma, risklərin emalı səmərəliliyini təyinetmə mexanizmləri müəyyən olunubmu?	6	0			
1.36.	**Əməliyyat prosedurlarının sənədləşdirilməsi**			**50**				
	Vəzifə	Hədəf						
	İnformasiya emalı vasitələri üçün işgüzar (əməliyyat) və istismar prosedurları sənədləşdirilməli və əlçatan olmalıdır	İnformasiya emalı vasitələrinin düzgün və təhlükəsiz işləməsini təmin etmək	1) İnformasiya emalı vasitələri üçün fəaliyyət və informasiya təhlükəsizliyini idarəetmə üzrə əməliyyat prosedurları müəyyən olunub sənədləşdirilibmi və onlara ehtiyacı olan işçilərin istifadəsinə verilirmi? Bu prosedurlar aşağıdakı halları da əhatə edirmi?	14	0			

			- fəaliyyətin bir çox insan tərəfindən eyni şəkildə yerinə yetirilməsinə ehtiyac olması; fəaliyyət nadir hallarda həyata keçirildikdə və həmin fəaliyyət növbəti dəfə icra edildikdə prosedurun unudulma ehtimalının olması; - fəaliyyətin yeni olması və düzgün yerinə yetirilməzsə risk yaratması; - fəaliyyətin yeni kadrlara həvalə edilməsi.			**0%**		
			2) Sənədlərdə əməliyyat mərhələləri, məsuliyyətlər və istifadə olunan vasitələr müvafiq dərəcədə detallı şəkildə əks etdirilirmi?	12	0			
			3) Sənədlər qurumun hər bir bölməsinə uyğun olaraq fərdiləşdirilibmi?	10	0			
			4) Sənədlər rəhbərlik tərəfindən təsdiqlənirmi və vaxtaşırı nəzərdən keçirilirmi?	8	0			
			5) Əməliyyat prosesləri ilə əlaqəli mümkün risklər sənədlərdə nəzərə alınıbmı?	6	0			
1.37.	**Nüfuzetmə sınaqları**			**50**				
	Vəzifə	Hədəf						
	İnformasiya mühafizəsinin obyekti olan aktivlərdə (o cümlədən informasiya resurslarında və həllər bazasında, proqram, texniki və mühəndis təminatı vasitələrində) boşluqları, çatışmazlıqları, zəifliklər, nəzarətsizlikləri və digər uyğunsuzluqları müəyyənetmə üçün nüfuzetmə sınaqları aparılmalıdır	İnformasiya mühafizəsinin obyekti olan aktivlərdə risk amillərinin, o cümlədən təhdidlərin reallaşma imkanlarının müəyyən olunmasını təmin etmək	1) Qurumda nüfuzetmə sınaqlarının keçirilməsi ilə bağlı rəsmi siyasət və prosedur mövcuddurmu?	16	0	**0%**		
			2) Nüfuzetmə sınaqları qurumun bütün informasiya sistemlərini və şəbəkələrini əhatə edirmi?	14	0			
			3) Yeni istifadəyə verilən sistemlər nüfuzetmə sınaqlarından keçirilirmi?	11	0			
			4) Mövcud sistemlərin nüfuzetmə sınaqları ən azı ildə bir dəfə həyata keçirilirmi?	9	0			
	Zəifliklərin idarə edilməsi			**70**				
	Vəzifə	Hədəf						
	İstifadədə olan informasiya sistemlərinin texniki zəiflikləri haqqında	Texniki zəifliklərin istifadəsinin (istismarının) və əlaqəli risklərin qarşısını almaq	1) Zəifliklərin idarə olunması üçün sənədləşdirilmiş siyasət və prosedurlar mövcuddurmu?	17	0			
			2) Zəifliklərin idarə edilməsi üçün hansı alətlərdən istifadə edilir?	14	0			

1.38.	məlumat vaxtında əldə edilməli, qurumun belə zəifliklərə məruz qalma faktı, ehtimalı aşkarlanmalı, qiymətləndirilməli, əlaqəli riskləri qarşı müvafiq tədbirlər görülməlidir		3) Hansı tezliklə zəifliklərə dair skanlar aparılır? (həftəlik, aylıq və s.)	13	0	**0%**		
			4) Hər zəiflik üçün tədbirlərin icra müddəti müəyyən olunubmu? (məsələn: kritik zəiflik 72 saat içində?)	11	0			
			5) Tətbiq və əməliyyat sistemləri üçün yamaqlama (patching) siyasəti varmı?	8	0			
			6) Təhlükəsizlik yamaqları (patch) test olunaraq tətbiq edilir, yoxsa avtomatik?	7	0			
	İnformasiya təhlükəsizliyi risklərinin idarə edilməsi			**100**				
	Vəzifə	Hədəf						
1.39.	Qurumda informasiya mühafizəsinin obyekti olan aktivlərə informasiya təhlükəsizliyi üzrə tələblər və həllər müəyyən olunmalı, bu həllərin tətbiqi təşkil olunmalı, nəticələr təhlil olunmalı və mühafizə davamlı təkmilləşdirilməlidir	Qurumun işgüzar fəaliyyət proseslərinin davamlılığını, o cümlədən bu proseslərin informasiya, kompetensiya və texnologiya tələbatlarını əvvəlcədən təyin olunmuş məqbul hədlərdə (səviyyədə) təmin etmək	1) Qurumun informasiya təhlükəsizliyi üzrə risk idarəetmə siyasəti varmı?	30	0	**0%**		
			2) Risklər reyestri aparılırmı, habelə risklərin müəyyənləşdirilməsi, qiymətləndirilməsi və cavab verilməsi üçün prosedurlar sənədləşdirilibmi?	35	0			
			3) Bu siyasətlər mütəmadi olaraq nəzərdən keçirilirmi?	15	0			
			4) Qurumun risklərin qiymətləndirilməsi üçün risk matrisi varmı?	10	0			
			5) Risklərin qəbul edilə bilən səviyyəsi təyin olunubmu?	10	0			
2.	**Əməkdaşlar və təchizatçılar**			**2500**				
	İşə qəbul olunmaq üçün namizədlərin və əməkdaşların təhlükəsizlik yoxlamaları			**300**				
	Vəzifə	Hədəf						
2.1.	İşə götürülmə üçün bütün namizədlərin tərcümeyi-hal məlumatlarının yoxlanılması qanunvericiliyə, qaydalara və etikaya müvafiq şəkildə yerinə yetirilməli və biznesin tələblərinə, istifadəyə verilən informasiyanın	İşçilər və kontragentlərin öz vəzifələrini başa düşmələrini və təyin olunduqları rollara müvafiq olmalarını təmin etmək.	1) İşə qəbul olunmaq üçün bütün namizədlər yoxlamadan keçirilirmi?	80	0	**0%**		
			2) Bütün namizədlər haqqında toplanılan və emal olunan məlumatların siyahısı, buna aid qanunvericilik tələblərinin siyahısı müəyyən olunubmu və tətbiq olunurmu? Bu barədə namizədlərlə bu yoxlama haqqında əvvəlcədən məlumatlandırma aparılırmı?	50	0			
			3) İşə qəbul üçün müraciət edən namizədlər tərəfindən açıqlanan akademik məlumatların və sertifikatların etibarlılığı yoxlanılırmı?	40	0			

	təsnifatına, həmçinin qəbul olunan risklərə proporsional olmalıdır		4) Namizədlərin anket məlumatları, keçmiş iş təcrübəsi, əvvəllər məhkum olunub-olunmaması üzrə yoxlamalar aparılırmı?	90	0			
			5) Yoxlamaların qiymətləndirmə nəticələri saxlanılırmı?	40	0			
2.2.	**Əməkdaşlar və təchizatçılarla bağlanılan müqavilələrdə informasiya təhlükəsizliyi öhdəlikləri**			**350**				
	Vəzifə	Hədəf						
	İşçilər və təchizatçılarla bağlanılan müqavilələrdə onların və qurumun informasiya təhlükəsizliyi üzrə məsuliyyətləri göstərilməlidir	İşçilərin və kontragentlərin onlara həvalə olunan rollar üçün informasiya təhlükəsizliyi məsuliyyətlərini bilmələrini təmin etmək	1) İşçilər və ya podratçılar ilə bağlı müqavilələrdə informasiya təhlükəsizliyinə dair öhdəliklər müəyyən edilmişdirmi?	80	0	**0%**		
			2) Müqavilənin məzmunu çərçivəsində informasiya təhlükəsizliyi ilə bağlı tələblərin adekvat şəkildə təmin edilib-edilməməsi müntəzəm olaraq yoxlanılırmı?	60	0			
			3)Müvafiq işçilər/podratçılar işə xitam verildikdən və ya iş şəraitinin dəyişdirilməsindən sonra riayət etməli olduqları informasiya təhlükəsizliyi öhdəlikləri müəyyən edilibmi?	60	0			
			4) İnformasiya təhlükəsizliyi pozuntusuna yol vermiş kadr/podratçı üçün müvafiq qanunlar, əmək müqavilələri və s. amilləri nəzərə alan intizam prosesi varmı?	50	0			
			5)Əməkdaşların və təchizatçıların əməl etməli olduğu informasiya təhlükəsizliyi siyasətləri, prosedurları və təlimatları müəyyən edilibmi?	50	0			
			6)Müvafiq sənədlər qurumun informasiya təhlükəsizliyi tələblərinə cavab verirmi?	30	0			
			7) İnformasiya təhlükəsizliyi tələblərində hər hansı dəyişiklik olduqda sənədlər yenilənirmi?	20	0			
2.3.	**Aktivlərin məqbul istifadəsi**			**150**				
	Vəzifə	Hədəf						
	İnformasiya və informasiya emalı vasitələri ilə bağlı olan aktivlərdən və informasiyadan yolverilən istifadə qaydalarını müəyyən etmək, sənədləşdirmək və tətbiq etmək lazımdır	İnformasiyanın və digər əlaqəli aktivlərin əvvəlcədən təyin olunmuş qaydada mühafizəsini, istifadəsini və emalını təmin etmək	1) Aktivlər üçün məqbul istifadə siyasəti müəyyən edilibmi?	50	0	**0%**		
			2) Aktivlərdən məqbul istifadə siyasəti qurum işçilərinə və podratçılara elan edilibmi?	30	0			
			3) Qurumun işçi heyətinin və podratçılarının aktivlərdən məqbul istifadə siyasətinə əməl etməsi təmin olunur və nəzarətdə saxlanılırmı?	70	0			

2.4.	**Sosial media təhlükəsizliyi**			**100**				
	Vəzifə	Hədəf						
	Sosial media mühitində qurumun fəaliyyətinə aid yayılması nəzərdə tutulan informasiyanın təsnifatı və məzmunları müəyyən olunmalıdır, vaxtında təqdim olunmalıdır, başqa tərəflərdən yanlış informasiya yayma halları və cəhdləri müvafiq texnologiyalarla vaxtında aşkar olunmalıdır	Sosial media mühitində qurumun işgüzar nüfuzuna ola bilən təhdidlərə qarşı tədbirlər görmək, qabaqlayıcı tədbirlərə üstünlük vermək	1) Sosial mediadan istifadə üzrə siyasət müəyyən edilibmi?	30	0	**0%**		
			2) Sosial mediadan istifadə siyasətinə əməl olunurmu və pozuntular barədə qeydiyyat aparılırmı?	30	0			
			3) Məxfi məlumatların işçilər tərəfindən sosial media vasitəsilə paylaşılmamasına nəzarət olunurmu?	40	0			
2.5.	**İnformasiya təhlükəsizliyi üzrə maarifləndirmə, təhsil və təlim**			**400**				
	Vəzifə	Hədəf						
	Qurumun bütün işçiləri və zərurət olduqda, aidiyyəti müvafiq maraqlı tərəflər müvafiq maarifləndirmə təlimləri keçməli və tədris edilməli, həmçinin onların iş funksiyalarına aid olan, qurumun siyasət və prosedurları üzrə olan yeniliklərlə müntəzəm olaraq təmin olunmalıdırlar	İşçilər və müvafiq maraqlı tərəflər, qurumun informasiya təhlükəsizliyi üzrə öz vəzifələrindən xəbərdar olmasını və onları yerinə yetirməsini təmin etmək	1) Qurumun işçi heyəti və müvafiq maraqlı tərəflər informasiya təhlükəsizliyi üzrə maarifləndirmə təlimi və təhsili alırmı? Bunun üçün qurumun informasiya təhlükəsizliyi siyasətinə, alt-siyasətlərə və müvafiq prosedurlara uyğun məlumatlandırma, təhsil və təlim proqramı müəyyən olunubmu? Plan üzrə dövrü olaraq tətbiq olunurmu?	90	0	**0%**	**0%**	
			2) Maarifləndirmə proqramları mütəmadi olaraq təşkil olunurmu və bütün işçiləri əhatə edirmi?	70	0			
			3) Təlimlər üçün əsas mövzular (məsələn: şifrə təhlükəsizliyi, fişinq hücumları və s.) müəyyən edilib təsdiq olunubmu? Qurumun informasiya təhlükəsizliyi üzrə məlumatlandırma, təhsil və təlim proqramının və planın səmərəliliyi nəticə yönümlü qiymətləndirilirmi? Qurumun informasiya təhlükəsizliyi üzrə “biliklər bazası”, o cümlədən baş vermiş insidentlərdən çıxarılan nəticələr bu proqramlarda nəzərə alınırmı?	90	0			
			4)Məlumatlandırma, təhsil və təlim proqramında iştirak edən işçilər üçün qeydiyyat aparılır və davamiyyət izlənilirmi?	40	0			

			5) Kritik məlumatlara və sistemlərə giriş icazəsi olan işçilər üçün xüsusi təhlükəsizlik təlimləri təşkil edilirmi? Onların ixtisaslaşma, ixtisasartırma planları müəyyən olunubmu?	70	0			
			6) İnformasiya təhlükəsizliyi və Kiber İnsidentlərə Cavabvermə Qrupu əməkdaşlarına, kiber və ya informasiya təhlükəsizliyinin pozulması hadisələrini aşkar etmək və necə hesabat verilməsi ilə bağlı təlim verilirmi?	40	0			
2.6.	**İntizam tədbirləri**			**100**				
	Vəzifə	Hədəf						
	İnformasiya təhlükəsizliyi qaydalarını pozmuş işçilərə qarşı rəsmi və əvvəlcədən bildirilmiş intizam tədbirləri müəyyən olunmalıdır	Şəxsi heyətin və digər aidiyyəti maraqlı tərəflərin qurumun informasiya təhlükəsizliyi siyasətinin pozulmasının nəticələrini başa düşmələrini, pozuntuların qarşısının alınmasını, pozuntuya yol vermiş şəxsi heyət və digər aidiyyəti maraqlı tərəflər üçün müvafiq tədbirlərin görülməsini təmin etmək	1)İnformasiya təhlükəsizliyi siyasətinin pozulması hadisələrini aşkaretmə (məsələn: müəyyən edilmiş meyarlarla faktiki vəziyyətin müqayisəsi) mexanizmi müəyyən olunubmu?	25	0	**0%**		
			2) İnformasiya təhlükəsizliyi siyasətinin mühafizəsi və pozulması ilə əlaqədar intizam (təqdir və tənbeh) tədbirləri və onların tətbiq mexanizmləri müəyyən olunubmu?	20	0			
			3) İnformasiya təhlükəsizliyi siyasətinin pozulmasına səbəb ola bilən amillər (təhdidlər), həmçinin risklər əvvəlcədən müəyyən olunubmu?	15	0			
			4) İnformasiya təhlükəsizliyi siyasətinin pozulması hadisəsinin qəsdən və ya təsadüfi olmasını, əvvəlcədən hazırlanıb-hazırlanmamasını təyin edə bilən mexanizm müəyyən olunubmu?	20	0			
			5) Qəsdən, hazırlıqlı törədilmiş pozuntular barədə dərhal atılmalı olan addımlar müəyyən olunubmu?	20	0			
2.7.	**İşə xitam verildikdə və ya iş yeri dəyişdirildikdə informasiya təhlükəsizliyi**			**300**				
	Vəzifə	Hədəf						
	İnformasiya təhlükəsizliyinə aid olan, işdən çıxandan və ya iş yerini dəyişəndən sonra qalan məsuliyyət və vəzifələr müəyyən edilməli, işçiyə və ya kontragentə çatdırılmalı	İşdən azad edilmə və ya işin dəyişdirilməsi prosesinin tərkib hissəsi kimi qurumun maraqlarını qorumaq	1) İşə, müqaviləyə xitam verildikdə və ya iş yeri dəyişdirildikdə informasiya təhlükəsizliyi üzrə proseslər təsbit edilib və tətbiq edilirmi?	140	0			
			2) Vəzifə ilə bağlı xitam və ya dəyişikliklərdən sonra da qüvvədə qalan informasiya təhlükəsizliyi öhdəlikləri və məsuliyyətləri müəyyən edilir, həyata keçirilir və müvafiq işçilərə və digər maraqlı tərəflərə bildirilirmi?	90	0	**0%**		

	və hüquqi formada sənədləşdirilməlidir		3) İşdən çıxan və ya vəzifəsini dəyişən işçilər haqqında daxili komandalar (məsələn: İT şöbəsi, insan resursları) məlumatlandırılırmı?	70	0			
2.8.	**Konfidensiallıq və ya yaymamaq haqqında razılaşmalar**			**300**				
	Vəzifə	Hədəf						
	İnformasiyanın qorunması ilə bağlı qurumun ehtiyaclarını əks etdirən konfidensiallıq və ya yayılmama haqqında sazişlər, öhdəliklər üçün tələblər müəyyən edilməli və onlara müntəzəm şəkildə təkrar baxılmalı və sənədləşdirilməlidir	Qurumun aktivlərini müəyyən etmək, işçilər və ya kənar şəxslər tərəfindən əldə edilən məlumatların mühafizəsini təmin etmək	1) Konfidensiallıq və ya yaymamaq haqqında razılaşmalar müəyyən edilibmi?	60	0	**0%**		
			2) Konfidensiallıq və ya yaymamaq haqqında razılaşmalar mütəmadi olaraq nəzərdən keçirilib işçilər və digər maraqlı tərəflər tərəfindən imzalanıbmı?	70	0			
			3) Bu razılaşmalarda onların qüvvədə olma müddətləri müəyyən olunubmu, mühafizə olunan informasiyanın təsnifatı, o cümlədən istifadə üçün icazə verilən istifadə məqsədləri, səlahiyyətlər bölgüsü nəzərə alınıbmı?	70	0			
			4) Bu razılaşmalarda tərəflər üçün öhdəliklər qeyd edilibmi? Bu razılaşmalara xitam verildikdə tələb olunan hərəkətlər, o cümlədən geri qaytarılmalı və ya məhv edilməli olan aktivlərin siyahısı müəyyən olunubmu?	60	0			
			5)Məxfilik müqaviləsi pozulduğu halda görüləcək tədbirlər müəyyən edilibmi?	40	0			
2.9.	**Məsafədən iş zamanı informasiya təhlükəsizliyi**			**200**				
	Vəzifə	Hədəf						
	Məsafədən iş yerlərində (məntəqələrdə, binalarnda) müraciət olunan, emal edilən və ya saxlanılan informasiyanı mühafizə etmək üçün prosedur və onu dəstəkləyən təhlükəsizlik tədbirləri tətbiq olunmalıdır	İşçilər və ya kontragentlər uzaqdan işləyərkən informasiya təhlükəsizliyini təmin etmək	1) Məsafədən işləmək üçün siyasət mövcuddurmu?	20	0	**0%**		
			2) Məsafədən iş siyasəti işçilərin hüquq və öhdəliklərini dəqiq şəkildə təsvir edirmi?	20	0			
			3) Məsafədən işləyən işçilər qurumun məlumat sistemlərinə yalnız təhlükəsiz şəbəkə vasitəsilə qoşulurlarmı (məsələn: VPN istifadə olunurmu)?	40	0			
			4) Məsafədən işləmə zamanı qurumun hüquqi rejiminə görə istifadəsi məhdudlaşdırılan məlumatlarının təhlükəsiz şəkildə ötürülməsi təmin edilirmi? Məsafədən iş mühitində istifadə oluna bilinən informasiyanın təsnifatı müəyyən olunubmu? Qurumda “uzaqdan iş”, “çevik iş yeri”, “virtual iş mühitləri”, “uzaqdan texniki xidmət” və bu kimi digər belə formalar qanunvericiliyə uyğun tənzimlənirmi?	40	0			

			5) Məsafədən işləyən işçilərin qurum sistemlərinə girişləri izlənilir və qeydə alınırmı, audit və monitorinq alətləri müəyyən olunubmu? Məsafədən iş mühiti üçün istifadəçilər, istifadə olunan avadanlıqlar üçün xüsusi autentifikasiya tələbləri, təhlükəsizlik divarları, zərərli proqramlardan qorunma kimi tələblər müəyyən olunubmu?	40	0			
			6) İT şöbəsi məsafədən işləyən işçilərə texniki dəstək və təhlükəsizlik məsələləri ilə bağlı dərhal reaksiya göstərə bilirmi?	20	0			
			7) İşdən çıxan işçilərin məsafədən giriş icazələri vaxtında ləğv edilir və məlumatların qaytarılması təmin edilirmi?	20	0			
2.10.	**İnformasiya təhlükəsizliyi hadisələrinin hesabatı**			**300**				
	Vəzifə	Hədəf						
	İnformasiya təhlükəsizliyi hadisələri, uyğunsuzluqları haqqında hesabat idarəetmənin müvafiq kanalları ilə mümkün olduğu qədər tez verilməlidir	Personalın və ya maraqlı tərəflərin müəyyən olunan informasiya təhlükəsizliyi hadisələrinin, uyğunsuzluqların vaxtında, ardıcıl və effektiv hesabatını təmin etmək	1) Əməkdaşlar tərəfindən informasiya təhlükəsizliyi insidentləri barədə dərhal məlumat verilirmi?	70	0	**0%**		
			2) Qurum işçilərin müşahidə etdiyi və ya şübhələndiyi informasiya təhlükəsizliyi insidentləri barədə müvafiq kanallar vasitəsilə vaxtında məlumat verməsi üçün bildiriş mexanizmini təmin edibmi?	60	0			
			3) İnformasiya təhlükəsizliyi hadisələrinə aid verilən məlumatlarda göstərilməli olan halların siyahısı müəyyən olunubmu?	40	0			
			4) İnformasiya təhlükəsizliyi insidentlərinin vaxtında bildirilməsi üçün vaxt məhdudiyyətləri müəyyən edilibmi?	50	0			
			5) Qurumda informasiya təhlükəsizliyi hadisələrinə səbəb ola bilən təhdidlərin (məsələn: məsuliyyət və səlahiyyət bölgülərinin pozulması, insan səhvləri), təhdidlərin istifadə edə biləcəyi zəifliklərin, boşluqların və digər uyğunsuzluqların (məsələn: qeyri-effektiv nəzarət tədbirləri, nəzarətsiz aparılan sistem dəyişiklikləri, proqram və ya aparat təminatının nasazlıqları) təhdidlərin yarada biləcəyi fəsadların siyahısı və onların ölçüləri müəyyən olunubmu?	80	0			
3.	**Fiziki təhlükəsizlik**			**1500**				
	Fiziki təhlükəsizlik perimetrləri			**110**				
	Vəzifə	Hədəf						

3.1	İnformasiyanı və informasiya emalı vasitələri olan digər əlaqəli aktivləri ehtiva edən zonaları (əraziləri) qorumaq üçün təhlükəsizlik perimetrləri müəyyən edilməlidir	Təşkilatın informasiyasına və informasiya emalı vasitələri olan digər əlaqəli aktivlərinə icazəsiz fiziki girişin, zərərin və digər müdaxilənin qarşısını almaq	1) Qurumun fiziki təhlükəsizlik perimetrləri, xüsusi zonalar və müvafiq mühafizə rejimləri dəqiq müəyyən edilibmi? Bu perimetrlər qurumun informasiya təhlükəsizliyi siyasətində təsvir edilibmi?	22	0	**0%**		
			2) Fiziki təhlükəsizlik perimetrlərində olan, informasiya ilə əlaqəli olan və mühafizə obyekti olan aktivlər müəyyən olunubmu, bu aktivlərə olan təhlükəsizlik tələbləri və risklər qiymətləndirilibmi, o cümlədən ola bilən təhdidlər, mövcud zəifliklər, ola bilən fəsadlar müəyyən olunubmu?	19	0			
			3) Fiziki təhlükəsizlik perimetrlərinə aid qeydə alınmış məlumatların konfidensiallığı və bütövlüyü təmin olunurmu?	16	0			
			4) Fiziki təhlükəsizlik perimetrlərini qorumaq üçün hasarlar, divarlar və digər baryerlər mövcuddurmu?	14	0			
			5) Fiziki təhlükəsizlik perimetrlərində fövqəladə hallar üçün təxliyə yolları mövcuddurmu?	13	0			
			6) Fiziki təhlükəsizlik perimetrinə daxil olan şəxslərin mənsubiyyətləri yoxlanılırmı?	11	0			
			7) Fiziki təhlükəsizlik perimetrlərinin təhlükəsizlik tədbirləri mütəmadi olaraq yoxlanılırmı?	9	0			
			8)Fiziki təhlükəsizlik perimetrində elektrik enerjisinin kəsilməsi halları üçün ehtiyat güc mənbələri mövcuddurmu?	6	0			
3.2.	**Fiziki girişlərə nəzarət**			**145**				
	Vəzifə	Hədəf						
	Təhlükəsiz ərazilər müvafiq girişi idarəetmə vasitələri ilə qorunmalı və giriş nöqtələri ilə təmin olunmalıdır	Qurumun informasiyasına və digər əlaqəli aktivlərinə yalnız avtorizasiya olunan fiziki girişin olmasını təmin etmək	1) Qurumda yalnız icazə verilmiş şəxslərin fiziki olaraq obyektə daxil olmasını təmin edən prosedurlar mövcuddurmu?	29	0	**0%**		
			2) Xüsusi mühafizə olunmalı ərazilərə yalnız icazə verilmiş heyətin girişini təmin etmək üçün müvafiq girişə nəzarət vasitələri ilə təmin edilib?	25	0			
			3) Fiziki giriş icazələri işçi mövqeyinə, vəzifəsinə və ya roluna uyğun olaraq müəyyənləşdirilirmi?	22	0			
			4) Binaların və ya təhlükəsizlik zonalarının girişində fiziki nəzarət tədbirləri (məsələn: təhlükəsizlik personalı, turniketlər) tətbiq olunurmu?	19	0			
			5) Giriş-çıxışlar müvafiq şəkildə qeydə alınır və izlənilirmi?	17	0			
			6) Hər hansı icazəsiz giriş cəhdləri qeydə alınırmı və dərhal araşdırılırmı?	15	0			

			7) İstifadə olunmuş giriş kartları və ya digər vasitələr müntəzəm olaraq yenilənir və ya deaktivasiya edilir?	12	0			
			8) Ofis və obyektlərin icazəsiz girişlərdən qorunmasını təmin etmək üçün əlavə baryerlər və ya kilid sistemləri mövcuddurmu?	6	0			
3.3.	**Bina, ofis, otaq və obyektlərin mühafizəsi**			**110**				**0%**
	Vəzifə	Hədəf						
	Ofislər, otaqlar və obyektlər üçün fiziki təhlükəsizlik layihələndirilməli və həyata keçirilməlidir	Ofislərdə, otaqlarda və obyektlərdə qurumun informasiyasına və digər əlaqəli aktivlərinə icazəsiz fiziki girişin, zədələnmənin və digər müdaxilənin qarşısını almaq	1) Fiziki təhlükəsizlik perimetrlərində olan ərazi, bina, otaq və digər yerlərin mühafizəsini müəyyən edən prosedur müəyyən olunubmu?	31	0	**0%**		
			2) Fiziki təhlükəsizlik perimetrlərində olan ərazi, bina, otaq və digər yerlərə kritik obyektlər yerləşdirilərndə həmin yerlərə kənar şəxslərin girişinin qarşısını almaq tələbi təmin olunurmu?	26	0			
			3) Fiziki təhlükəsizlik perimetrlərində olan ərazi, bina, otaq və digər yerlərin görüntülərinin kənardan diqqəti cəlb etməməsi, bu yerlərdə informasiya proseslərinin aparılmasını bildirən, bu yerlərin təyinatını açıqlaya bilən əlamət və işarələrin kənardan və daxildən diqqəti cəlb etməməsi tələbləri hansı dərəcədə təmin olunur?	22	0			
			4) Konfidensial informasiyanın və kənara açıqlanmayan proseslərin kənardan görünən və eşidilən olmasının qarşısı alına bilinirmi? Bunun üçün qurğuların konfiqurasiyası həmin tələbi təmin edirmi? Müvafiq elektromaqnit qoruyuculardan istifadə olunurmu?	18	0			
			5) Konfidensial informasiyanın emal olunduğu yerləri müəyyən edə bilən məlumat kitabçalarını, daxili telefon kitabçalarını kənar şəxslərdən gizli saxlama mexanizmi müəyyən olubmu? Bu gizlilik təmin olunurmu?	13	0			
3.4.	**Fiziki təhlükəsizliyin monitorinqi**			**90**				
	Vəzifə	Hədəf						
	Bina və digər mühafizə perimetrləri icazəsiz girişə qarşı daimi nəzarət altında olmalıdır	İcazəsiz fiziki girişi aşkar etmək və qarşısını almaq	1) Fiziki təhlükəsizliyi izləmək üçün müvafiq monitorinq sistemləri (videomüşahidə kameraları (CCTV), siqnalizasiya, hərəkət sensorları) quraşdırılıbmı?	25	0	**0%**		
			2) Fiziki təhlükəsizlik sistemləri 24/7 rejimində işləyirmi?	22	0			

			3) Monitorinq sistemləri vasitəsilə qeydə alınan məlumatlar avtomatik olaraq saxlanılır və arxivləşdirilirmi?	18	0			
			4) Monitorinq sistemlərinin layihələndirilməsi, texniki layihə və istifadə sənədlərinin, habelə bu sahədə zəiflik, boşluq və digər uyğunsuzluqlar barədə informasiyanın konfidensial saxlanılması təmin olunurmu?	14	0			
			5) Mühafizə sisteminin idarəetmə panelinin mühafizəsini təminetmə mexanizmi müəyyən olunubmu? Tətbiq olunurmu?	11	0			
3.5.	**Fiziki və ekoloji təhdidlərdən qorunma**			**120**				
	Vəzifə	Hədəf						
	Mühafizə perimertlərini təbii fəlakətlərdən və qəsdlə olan və ya qəsdlə olmayan digər fiziki və ekoloji təhdidlərdən qorunma tədbirləri layihələndirilməli və həyata keçirilməlidir	Fiziki və ekoloji təhdidlərdən yaranan hadisələrin qarşısını almaq və ya nəticələrini azaltmaq	1) Ətraf mühit risklərinə (yanğın, sel, zəlzələ və s.) qarşı qoruma tədbirləri mövcuddurmu?	29	0	**0%**		
			2) Fiziki və ekoloji təhlükələrə (məsələn fəlakətlərə qarşı və digər qəsdən və ya təsadüfi fiziki təhdidlərə) qarşı qorunma üçün infrastruktur layihələndirilir və həyata keçirilirmi?	24	0			
			3) Ətraf mühit təhdidlərinə qarşı tədbirlər üçün xüsusi avadanlıqlar (yanğınsöndürmə sistemi, su nasosları və s.) quraşdırılıbmı?	22	0			
			4) Fiziki və ətraf mühit təhlükələrinə qarşı müdafiə tədbirlərini əhatə edən fövqəladə hallar planı hazırlanıbmı? Əgər varsa, qurumun işçiləri bu planlardan xəbərdardırlarmı və fövqəladə hallarda necə hərəkət edəcəklərini bilirlərmi?	19	0			
			5) Yanğın təlimləri mütəmadi olaraq keçirilir və işçilər məlumatlandırılırmı?	14	0			
			6) Məlumatların saxlanıldığı server otaqları və digər avadanlıqlar fiziki təhlükələrə qarşı qorunubmu?	12	0			
3.6.	**Mühafizəli zonalarda iş**			**80**				
	Vəzifə	Hədəf						
	Mühafizə perimetrlərində işləmək üçün təhlükəsizlik tədbirləri layihələndirilməli və həyata keçirilməlidir	Mühafizə perimetrlərində olan informasiyanı və digər əlaqəli aktivləri bu ərazilərdə işləyən personal tərəfindən zədələnmədən və	1)Mühafizə perimetrlərində işləmək üçün təhlükəsizlik tədbirləri müəyyən olunubmu? Bu tədbirlər təhlükəsiz ərazilərdə işləmək üçün bütün aidiyyəti personala şamil edilirmi və təhlükəsiz ərazidə baş verən bütün aidiyyəti prosesləri əhatə edirmi?	22	0			
			2) Mühafizə olunan sahələr və ya onların daxilindəki fəaliyyət haqqında personalın yalnız	19	0			

		icazəsiz müdaxilədən qorumaq	lazımi məlumatlılıq prinsipi əsasında məlumatlandırılması təmin olunurmu?			**0%**		
			3) Mühafizə olunan sahələrdə işlərin yalnız nəzarət altında aparılma mexanizmi müəyyən olunubmu? Tətbiq olunurmu?	16	0			
			4) Müəyyən səbəblərdən istifadə olunmayan, boş qalan mühafizə olunan sahələrin fiziki bağlanması, qıfıllanması və vaxtaşırı yoxlanılması təmin olunurmu?	13	0			
			5) Mühafizə olunan sahələrdə birbaşa icazə verilmədiyi hallarda, foto, video, audio və digər yazan qurğuların istifadəsinin qadağan edilməsi təmin olunurmu? Qadağa və nəzarət mexanizmləri müəyyən olunubmu?	10	0			
3.7.	**“Təmiz masa” və “təmiz ekran”**			**70**				
	Vəzifə	Hədəf						
	Kağızlar və çıxarıla bilən yaddaş daşıyıcıları üçün “təmiz masa” proseduru və informasiya emalı vasitələri üçün “təmiz ekran” proseduru müəyyən edilməli və müvafiq formada tətbiq edilməlidir	Mövcud iş saatları ərzində və onlardan kənarda masalar, ekranlar və digər əlçatan yerlərdə icazəsiz giriş, informasiyanın itirilməsi və zədələnməsi risklərini azaltmaq	1) Qurumda yaddaş daşıyıcıları üçün “təmiz masa” və informasiyanın əks olunduğu vasitələr üçün “təmiz ekran” prosedurlar mövcuddurmu və işçilər onunla tanışdırmı? Bu prosedurlarda qurmun informasiya təsnifatı, informasiya təhlükəsizliyi mədəniyyəti nəzərə alınıbmı?	20	0			
			2) İşçilərin iş yerlərini tərk edərkən masalarındakı məxfi, konfidensial sənədləri və məlumatları yığışdırması tələb olunurmu? Lazım olmadıqda konfidensial və kritik xidməti informasiyanın yazı lövhələrindən,ekranlardan vaxtında silinməsi təmin olunurmu?	17	0			
			3) Məlumat daşıyıcıları (USB, xarici sabit disk) və digər məxfi materiallar təhlükəsiz yerlərdə saxlanılırmı? İstifadə olunmayan, tələb olunmayan konfidensial və ya kritik informasiya daşıyıcılarının mühafizə olunan yerdə qapadılması, dövriyyədən çıxarılanda təhlükəsiz utilizasiyası/məhv edilməsi həyata keçirilirmi?	14	0		**0%**	
			4) Kompüter ekranlarının iş yeri tərk edildikdə avtomatik olaraq kilidlənməsi üçün siyasətdə tələb qeyd edilibmi? Müəyyən vaxtda istifadə edilməyən və ya nəzarətdən kənar qalan hallarda istifadəçi cihazlarının fiziki açarla, autentifikasiya mexanizmi ilə, cihazı, ekranı və klaviaturanı kilidləmə	11	0			

			mexanizmi və ya digər təhlükəsizlik vasitələri ilə təmin olunurmu?					
			5) Məxfi sənədlər printerlərdə, skanerlərdə və ya açıq yerlərdə uzun müddət nəzarətsiz qalırmı? Printerlərdən və ya çoxfunksiyalı cihazlardan çıxan kağız və ya digər daşıyıcıların autentifikasiya vasitələri ilə və həmin cihazların yanında fiziki olub təsdiqləməklə əldə edə bilməsi və dərhal götürməsi təmin olunurmu? Buna nəzarət olunurmu?	8	0		**0%**	
3.8.	**Avadanlıqların yerləşdirilməsi və mühafizəsi**			**90**				
	Vəzifə	Hədəf						
	Mühafizə perimetrlərində avadanlıq etibarlı şəkildə yerləşdirilməlidir və qorunmalıdır	Mühafizə perimetrlərində fiziki və ekoloji təhdidlərdən, icazəsiz giriş və zədələrdən yaranan riskləri azaltmaq	1) Avadanlıqlar etibarlı şəkildə yerləşdirilir və qorunurmu? Avadanlıqlar iş sahələrində yerləşdiriləndə həmin sahələrə girişlərin minimuma endirilməsi, icazəsiz girişin qarşısının alınması, bu avadanlıqlarda emal olunan konfidensial informasiyanı kənar şəxslərin görmə riskinin azaldılması, fiziki və ekoloji təhdidlərdən (məsələn: oğurluq, yanğın, partlayıcı maddələr, tüstü, subasma və ya su borularının qəzası, toz, titrəyiş, kimyəvi təsirlər, elektrik enerjisi ilə təchizatda əngəllər, rabitədə ilişiklik (interference), elektromaqnit şüası, vandallıq/qəsdən zədələmə kimi amillərdən) qorunma mexanizmləri müəyyən olubmu? Bu mexanizmlər tətbiq olunurmu?	25	0		**0%**	
			2) Avadanlıqların yerləşdirildiyi yerlər texniki xidmətlər üçün asanlıqla əlçatandırmı?	22	0			
			3) Avadanlıqlar yerləşdirilən iş sahələrində temperatur və rütubət kimi ətraf mühit şəraitinin informasiya emalı vasitələrinin işinə mənfi təsir göstərə biləcək şərait, təbiət hadisələri (məsələn: zəlzələ, torpaq sürüşməsi, subasma və s.) və bu təsirlərə nəzarət mexanizmi müəyyən olunubmu? Bu mexanizm tətbiq olunurmu?	18	0			
			4) Avadanlıqlar yerləşdirilən iş sahələrində elektrik və rabitə xətlərinə ildırımdan mühafizə filtrlərinin quraşdırılması, konfidensial informasiyanın elektromaqnit şüalanma ilə və ya digər üsullarla sızma təhdidinin qarşısının alınması təmin olunubmu?	14	0			
			5) Qurum tərəfindən idarə olunan və kənar tərəflər tərəfindən idarə olunan informasiya emal	11	0			

			vasitələrinin bir-birindən fiziki olaraq ayrılması təmin olunurmu?					
3.9.	**Sistem otağının (məlumat mərkəzinin) təhlükəsizliyi**			**145**				
	Vəzifə	Hədəf						
	İnformasiya mühafizəsinin obyekti olan ilkin kateqoriyalı aktivlərin (proqram təminatı vasitələrinin və informasiya resurslarının) toplanıb saxlanılma daşıyıcılarının, bu daşıyıcıların funksionallığını təmin edən texniki təminat vasitələrinin, onların yerləşdiyi mühəndis təminatı vasitələrinin təhlükəsizliyi təmin olunmalıdır	İnformasiya mühafizəsinin obyekti olan ilkin kateqoriyalı aktivlərin toplanıb saxlanılma daşıyıcılarının konfiqurasiyasına və funksionallığına təhdidlərin qarşısını almaq	1) Sistem otağının (məlumat mərkəzinin) təhlükəsizliyi siyasəti hazırlanıbmı?	48	0	**0%**		
			2) Sistem otağının (məlumat mərkəzinin) təhlükəsizliyi siyasəti ilə bağlı prosedurlar varmı, onların pozulmasının qeydiyyatı aparılırmı?	24	0			
			3) Sistem otağına (məlumat mərkəzinə) daxil olmaq icazəsi olan işçilərin icazələri vaxtaşırı yoxlanılırmı?	16	0			
			4) Dəstək və texniki xidmətlər üçün gələn üçüncü tərəf işçiləri müşayiət olunurmu?	12	0			
			5) Üçüncü tərəf işçiləri tərəfindən edilən əməliyyatlar qeydə alınırmı?	10	0			
			6) Sistem otağında (məlumat mərkəzində) rütubət, temperatur və tüstü sensorları varmı?	8	0			
			7) Sistem otağında (məlumat mərkəzində) kamera müşahidə sistemi varmı?	7	0			
			8) Sistem otağının (məlumat mərkəzinin) divarları nəmə və alova davamlı materialla örtülmüşdürmü?	6	0			
			9) Sistem otağına (məlumat mərkəzinə) giriş və çıxışın təhlükəsizliyini təmin etmək üçün nəzarət vasitələri mövcuddurmu?	5	0			
			10) Sistem otağından (məlumat mərkəzindən) giriş və çıxış qeydləri saxlanılırmı?	5	0			
			11) Sistem otağında (məlumat mərkəzində) istifadə olunan kondisionerlərin ehtiyatı varmı?	4	0			
	Qurumun mühafizə perimetrlərindən kənarda olan aktivlərin təhlükəsizliyi			**90**				
	Vəzifə	Hədəf						
	Mühafizə perimetrlərindən kənarda olan aktivlər də qorunmalıdır	Mühafizə perimetrlərindən kənarda olan cihazların itirilməsinin, zədələnməsinin, oğurlanmasının və ya sındırılmasının və qurumun fəaliyyətinin	1) Qurum ərazisindən kənarda istifadə olunan aktivlər qorunurmu? Qurumun ərazisindən kənarda istifadə edilən informasiyanı saxlayan və ya emal edən hər hansı cihaz, o cümlədən quruma məxsus cihazlar və şəxsi mülkiyyətdə olan və qurum adından istifadə edilən cihazların qorunması, “BYOD” (“bring your own device”) prinsipi təmin olunurmu? Buna rəhbərlik tərəfindən münasibət bildirilibmi?	25	0			

3.10.		dayandırılmasının qarşısını almaq	2) Qurum ərazisindən kənarda istifadə olunan informasiyanı saxlayan və ya emal edən hər hansı cihazın ictimai və qorunmayan yerlərdə fasiləsiz nəzarət mexanizmi və bu mühafizə üzrə istehsalçının göstərişləri müəyyən olunub tətbiq edilirmi?	22	0	**0%**		
			3) Qurumun ərazisindən kənarda məlumatların istifadəsi ilə bağlı qaydaları müəyyən edilibmi? 1-ci və 2-ci suallarda qeyd olunan cihazların yerinin izlənilməsi və cihazda saxlanılan informasiyanın uzaqdan silinməsi şərtləri və imkanları müəyyən olunub tətbiq edilirmi?	18	0			
			4) Avadanlığın qurumun ərazisindən kənara çıxarılma, ərazidən kənarda avadanlığın müxtəlif şəxslər və ya maraqlı tərəflərdə saxlanılma və onlar arasında ötürülmə zəncirinin qeydiyyatı (audit üçün izlərin yazılması) təmin olunurmu?	14	0			
			5) Qurumun ərazisindən kənarda daimi quraşdırılan avadanlığın zədələnmə, oğurlanma, dinlənilmə və digər riskləri qiymətləndirlibmi? Adekvat mühafizə tədbirləri müəyyən olunubmu?	11	0			
3.11.	**Son istifadəçi cihazı və media təhlükəsizliyi**			**120**				
	Vəzifə	Hədəf						
	Saxlanc qurğuları, daşıyıcılar, qurum tərəfindən qəbul olunmuş təsnifat sxeminə və istifadə tələblərinə uyğun olaraq, onların həyat dövrü boyunca, o cümlədən əldə edilməsi, istifadəsi, daşınması və utilizasiyası müddətlərində idarə edilməlidir	Saxlanc qurğularında, daşıyıcılarında məlumatın yalnız icazə əsasında açıqlanmasını, dəyişdirilməsini, silinməsini və ya məhv edilməsini təmin etmək	1) Son istifadəçi cihazı və media təhlükəsizliyi ilə bağlı prosedur qaydaları mövcuddurmu?	40	0	**0%**		
			2) Korporativ məlumatlara daxil olan şəxsi cihazlar üçün müəyyən edilmiş mobil cihazdan istifadə siyasəti varmı?	20	0			
			3) İstifadəçilərə mobil cihaz təhlükəsizliyi üzrə təlim verilirmi?	13	0			
			4) Qurumun mülkiyyətində olan cihazların İKT inventarları saxlanılırmı?	10	0			
			5) Qurum kritik məlumatlara daxil olan cihazları mərkəzləşdirilmiş şəkildə idarə edə bilirmi?	8	0			
			6) Yaddaş daşıyıcılarının istifadəsi, daşınması və utilizasiyası/məhv edilməsi proseslərinin hər mərhələsində qurumun təsnifat sxemi və prosedur tələblərinə uyğunluq təmin olunurmu?	7	0			
			7) Təkrar istifadə edilməzdən əvvəl yaddaş daşıyıcılarından bütün məxfi məlumatlar silinirmi?	6	0			

			8) Son istifadəçi kompüterlərdə təhlükəsizlik proqramı quraşdırılıbmı?	5	0			
			9) Qurumun mobil cihazları təmirə göndərilənə qədər təhlükəsizlik tədbirləri görülürmü?	4	0			
			10) Son istifadəçi kompüterlərin oğurlanması və itirilməsi riskinə qarşı tədbirlər görülürmü?	4	0			
			11) Son istifadəçi yaddaş daşıyıcılarında yerləşdirilən məlumatların təhlükəsizliyi təmin edilirmi?	3	0			
3.12.	**Dəstəkləyici xidmətlər və elektrik kəsintilərindən mühafizə**			**100**				
	Vəzifə	Hədəf						
	İnformasiya emalı avadanlıqları elektrik enerjisinin kəsilməsindən və kommunal xidmətlərdə pozuntular nəticəsində yaranan digər nasazlıqlardan qorunmalıdır	İnformasiyanın və digər əlaqəli aktivlərin itirilməsinin, zədələnməsinin və ya nüfuzdan düşməsinin və ya dəstəkləyici kommunal xidmətlərin pozulması səbəbindən qurumun fəaliyyətinin dayandırılmasının qarşısını almaq	1) Elektrik nasazlıqlarına qarşı qoruma tədbirləri (məsələn: UPS, generatorlar) mövcuddurmu? Qurumun informasiya emalı avadanlıqlarında ola biləcək nasazlıqlar və digər uyğunsuzlar müəyyən olunubmu?	28	0	**0%**		
			2) Bu sistemlərin gücü və işləmə müddəti qurumun kritik avadanlığının fasiləsiz işini təmin etmək üçün uyğundurmu? Qurumun informasiya emalı avadanlıqlarını dəstəkləmək üçün asılı olduğu kommunal xidmətlər (məsələn: elektrik enerjisi, telekommunikasiya, su təchizatı, qaz, kanalizasiya, ventilyasiya və kondisioner), onların xüsusiyyətləri, xidmətlər kataloqu, xidmət səviyyələri müəyyən olunubmu? sənədləşdirilibmi?	24	0			
			3) Bu sistemlərin saz vəziyyətdə olması mütəmadi olaraq yoxlanılırmı? Quruma göstərilən kommunal xidmətləri dəstəkləyən avadanlıqlar, onların konfiqurasiyaları müəyyən olunubmu? Bu avadanlıqlara texniki qulluqların idarə edilməsi (inzibatçılıq), o cümlədən mütəmadi olaraq yoxlanılması və sınaqdan keçirilməsi təmin olunurmu? Kommunal xidmətlərdə müxtəlif fiziki marşrutlara malik birdən çox marşrut və kanaldan, kommunal provayderdən istifadə edilməsi təmin olunurmu?	20	0			
			4) Kommunal xidmətləri dəstəkləyən avadanlıqların və informasiya emalı qurğularının bir-birindən ayrı olan şəbəkələrə qoşulması təmin olunurmu? Kommunal xidmətləri dəstəkləyən avadanlığın	16	0			

			internetə yalnız lazım olduqda və yalnız təhlükəsiz şəkildə qoşulması təmin olunurmu?.					
			5) Elektrik təchizatı kəsildikdə qəza işıqlandırma və kommunikasiya vasitələri işə düşürmü? Kommunal xidmətləri kritik hallarda kəsmək üçün qəza açarları və klapanlar müəyyən olunubmu? Onların qəza çıxışlarının və ya avadanlıq otaqlarının yaxınlığında yerləşdirilməsi təmin olunubmu?	12	0			
3.13.	**Kabellərin təhlükəsizliyi**			**70**				
	Vəzifə	Hədəf						
	Məlumatları ötürən və ya informasiya xidmətlərini dəstəkləyən və ya təchiz edən elektrik enerjisi və telekommunikasiya xətləri dinləmədən (“interception”), müdaxilədən və zədələnmədən qorunmalıdır	İnformasiyanın və digər əlaqəli aktivlərin itirilməsinin, zədələnməsinin, oğurlanmasının və ya nüfuzdan düşməsinin və qurumun enerji və rabitə kabelləri ilə bağlı olan əməliyyatlarının kəsilməsinin qarşısını almaq	1) Qurumun daxili və xarici kabel infrastrukturları təhlükəsizlik baxımından qorunurmu?	20	0	**0%**		
			2) Kabel marşrutları təsadüfi zədələnmələrə və kənar müdaxilələrə qarşı qorunurmu? Rabitə kabellərinə elektromaqnit təsirlərin qarşısının alınması, o cümlədən bunun üçün həmin kabellərin və elektrik kabellərinin bir-birindən ayrılması təmin olunubmu?	17	0			
			3) Kabellərin yerləşdirilməsi təhlükəsiz yerlərdə və gizli marşrutlarla təmin olunurmu? İnformasiya proseslərini təmin edən yerlərə, avadanlıqlara çəkilən elektrik və telekommunikasiya xətləri üçün alternativ mühafizə üsulları müəyyən olunubmu? Tətbiq olunurmu?	14	0			
			4) Kabel təhlükəsizliyi ilə bağlı mütəmadi yoxlamalar və auditlər aparılırmı? Kabelləri yoxlama və qoşulma nöqtələri siqnalizasiya ilə təmin olunubmu?	11	0			
			5) Kabel təhlükəsizliyi üçün xüsusi fiziki qoruma avadanlıqları (məsələn: kabel kanalları və ya qoruyucu borular) mövcuddurmu? Kabellər üçün zirehli boruların və kilidli otaqların və ya qutuların quraşdırılması təmin olunubmu?	8	0			
3.14.	**Avadanlıqlara texniki qulluq**			**70**				
	Vəzifə	Hədəf						
	İnformasiyanın tamlığını, əlçatanlığını, konfidensiallığını və mötəbərliyini təmin etmək üçün avadanlığa müvafiq qaydada qulluq göstərilməlidir	İnformasiyanın tamlığını, əlçatanlığını, konfidensiallığını və mötəbərliyini təmin etmək üçün avadanlığa müvafiq qaydada qulluq göstərilməlidir.	1) İnformasiyanın tamlığını, əlçatanlığını, konfidensiallığını və mötəbərliyini təmin etmək üçün tətbiq olunan avadanlığın (informasiya emalı qurğularının texniki komponentləri, fasiləsiz enerji təchizatı və batareyalar, enerji generatorları, güc alternatorları və çeviricilər, fiziki müdaxilənin aşkarlanması sistemləri və siqnalizasiyaları, tüstü	17	0			

		İnformasiyanın və digər əlaqəli aktivlərin itirilməsinin, zədələnməsinin, oğurlanmasının və ya nüfuzdan düşməsinin və qurumun texniki xidmətlərdə pozulma səbəblərindən əməliyyatlarının kəsilməsinin qarşısını almaq	detektorları, yanğınsöndürənlər, kondisioner və liftlərin) uçotu müəyyən olunubmu? Bu uçotun aktuallığı təmin olunurmu?			**0%**		
			2) Qurumun avadanlıqları üçün mütəmadi texniki xidmət planı mövcuddurmu? Bu avadanlığa göstərilmək üçün texniki qulluğa tələblər, o cümlədən texniki qulluq xidmətinin tezliyi və spesifikasiyalar/şərtlər müəyyən olunubmu?	14	0			
			3) Texniki xidmət göstərilən avadanlıqların (misal: serverlər, iş stansiyaları, printerlər və s.) siyahısı mövcuddurmu?	13	0			
			4) Texniki xidmət zamanı məlumatların itirilməməsi üçün ehtiyat nüsxələr çıxarılırmı?	11	0			
			5) Texniki xidmət iş təminatçıları (daxili və üçüncü tərəf) müəyyən olunubmu?	8	0			
			6) Texniki xidmət işləri ilə bağlı aparılmış fəaliyyətlər sənədləşdirilirmi? Qurumun avadanlıqlarında bütün şübhəli və ya faktiki nasazlıqların və bütün qabaqlayıcı və düzəldici texniki xidmətin uçotunun aparılması təmin olunurmu? Bu avadanlığa göstərilən texniki qulluğun tələblərə uyğunluğunun monitorinqi təmin olunurmu?	7	0			
3.15.	**Avadanlığın təhlükəsiz utilizasiyası və ya təkrar istifadə edilməsi**			**90**				
	Vəzifə	Hədəf						
	Tərkibində yaddaş daşıyıcıları olan avadanlığın elementləri ləğv edilməzdən, atılmadan, təkrar istifadədən əvvəl yoxlanılmalıdır. Bu daşıyıcılarda saxlanılan kritik olan, mühafizə olunan informasiyanın və lisenziyalı proqram təminatının silinməsinə və ya təhlükəsiz şəkildə başqa yerə köçürülməsinə (təzədən	Ləğv edilməsi və ya təkrar istifadəsi (utilizasiyası) nəzərdə tutulan avadanlıqdan informasiya sızmasının qarşısını almaq	1) Avadanlıqların utilizasiyası/məhv edilməsi və ya yenidən istifadəsi üçün müəyyən edilmiş siyasət və prosedurlar varmı?	25	0			
			2) Avadanlıqların utilizasiyası/məhv edilməsi zamanı məlumatların təhlükəsiz silinməsi təmin edilirmi? Konfidensial və ya müəllif hüquqları ilə qorunan məlumatları ehtiva edən yaddaş daşıyıcılarının fiziki olaraq məhv edilməsi, daşıyıcılarda olan orijinal məlumatı geri qaytarmaq mümkün olmayan üsullardan istifadə etməklə məlumatın məhv edilməsi, silinməsi və ya üzərinə yazılması aləti müəyyən olunubmu?	22	0			
			3) Utilizasiya/məhv edilmə üçün seçilən təminatçıların təhlükəsizlik və məxfiliklə bağlı müqavilələri varmı?	18	0	**0%**		

	yazılmasına) əminlik yaranmalıdır		4) Yenidən istifadə ediləcək avadanlıqların tamamilə təmizlənməsi (məlumatların silinməsi) təmin olunurmu?	14	0			
			5) Utilizasiya olunan (məhv edilən) və ya yenidən istifadə edilən avadanlıqların qeydiyyatı aparılırmı? Tərkibində yaddaş daşıyıcıları olan nasaz avadanlıqların təmirə göndərilməsi və ya atılmasının, və ya bunun əvəzinə fiziki məhv edilməsinin lazım olduğu müəyyən olunurmu? Bunun üçün risk qiymətləndirilməsi təmin olunurmu?	11	0			
4.	**Avadanlığa, proqram təminatına və məlumatların təhlükəsizliyinə dair meyarlar**			**3500**				
4.1.	**Son istifadəçi cihazlarının təhlükəsizliyi**			**129**				
	Vəzifə	Hədəf						
	İstifadəçinin son nöqtə cihazlarında saxlanılan, emal edilən və ya onlar vasitəsilə əldə edilən informasiya qorunmalıdır	İstifadəçinin son nöqtə cihazlarından istifadə edəndə informasiyanı risklərdən qorumaq	1) Son istifadəçi cihazlarında saxlanılan, emal olunan və ya onlar vasitəsilə əldə oluna bilən informasiyalar qorunurmu?	40	0	**0%**		
			2) Son istifadəçi cihazlarına quraşdırılan proqram təminatının təhlükəsizliyi yoxlanılırmı?	30	0			
			3) İstifadəçilərin cihazlarında quraşdırılan proqram təminatı mütəmadi olaraq yenilənirmi?	25	0			
			4) Simsiz bağlantılara aid prosedurlar müəyyən olunubmu? İstifadəçilərə ictimai Wi-Fi şəbəkələrində cihazların təhlükəsizliyini təmin etmək üçün təlimatlar verilirmi?	20	0			
			5) Son nöqtə cihazlarının istifadəçiləri üçün təhlükəsizlik tələbləri, məsuliyyətlər müəyyən olunubmu?	14	0			
4.2.	**İmtiyazlı müraciət (giriş) hüquqları**			**180**				
	Vəzifə	Hədəf						
	İmtiyazlı müraciət, giriş hüquqlarının verilməsi və istifadə edilməsi məhdudlaşdırılmalı və idarə olunmalıdır	İmtiyazlı giriş hüquqlarının yalnız səlahiyyətli istifadəçilərə, proqram komponentlərinə və xidmətlərə verilməsinə əminlik yaratmaq	1) İmtiyazlı giriş hüquqlarının verilməsi və dəyişdirilməsi üçün təsdiq prosesləri mövcuddurmu?	45	0			
			2) İmtiyazlı giriş hüquqlarının verilməsi üçün meyarlar müəyyən edilibmi?	35	0			
			3) İmtiyazlı giriş hüquqlarına dair qeyri-qanuni fəaliyyətlər aşkarlandıqda görülən tədbirlər müəyyən olunubmu?	40	0	**0%**		

			4) İmtiyazlı istifadəçilərin müvəqqəti giriş hüquqlarının müddətləri müəyyən olunubmu?	30	0			
			5) İmtiyazlı giriş hüquqları ilə bağlı mütəmadi auditlər keçirilirmi?	30	0			
4.3.	**Məlumatlara müraciət (giriş) məhdudiyyəti**			**158**				
	Vəzifə	Hədəf						
	İnformasiyaya və digər əlaqəli aktivlərə müraciət, giriş bu sahəyə aid tələblərə uyğun olaraq məhdudlaşdırılmalıdır	İnformasiyaya və digər əlaqəli aktivlərə yalnız icazəli müraciət, giriş imkanı verilməsini təmin etmək və icazəsiz müraciətlərin, girişlərin qarşısını almaq	1) Məlumatlara giriş hüquqları verilən tərəflər və meyarlar müəyyən olunubmu?	30	0	**0%**		
			2) Hər bir istifadəçi üçün giriş icazələrinin müəyyən edilməsi ilə bağlı təsdiq prosedurları mövcuddurmu?	28	0			
			3) Məlumatlara girişin məhdudlaşdırılması üzrə nəzarət tədbirləri həyata keçirilirmi? Girişə nəzarət siyahıları (“ACL, access control list”) tərtib olunurmu?	40	0			
			4) Giriş icazələrinin pozulması halında müvafiq tədbirlər görülürmü?	25	0			
			5) Məlumatlara giriş məhdudiyyətləri ilə bağlı qeyri-qanuni fəaliyyətlərin aşkar edilməsi üçün monitorinq alətləri mövcuddurmu?	20	0			
			6) Məlumatlara giriş məhdudiyyətləri ilə bağlı mütəmadi auditlər keçirilirmi?	15	0			
4.4.	**Proqram təminatlarının inventarı**			**65**				
	Vəzifə	Hədəf						
	Qurumun proqram təminatı vasitələrinin inventar uçotu tərtib edilməli və saxlanmalıdır	Qurumda identifikasiya, autentifikasiya və avtorizasiya olunmayan proqram təminatı vasitələrindən istifadə ilə əlaqədar olan təhdidlərin qarşısını əvvəlcədən almaq	1) Qurum daxilində detallı və güncəllənmiş proqram təminatı inventarı saxlanılırmı?	25	0	**0%**		
			2) İnventar idarəetmə prosesi müəyyən edilibmi?	15	0			
			3) Proqram təminatı inventarında proqram təminatlarının quraşdırıldıqları avadanlıq və ya virtual mühitin qeydiyyatı aparılırmı?	15	0			
			4) İnventarda olmayan proqram təminatlarının istifadəsi ilə bağlı prosedur mövcuddurmu?	10	0			
4.5.	**Proqramın mənbə, ilkin koduna əlçatanlıq**			**50**				
	Vəzifə	Hədəf						
	Proqramın ilkin/ mənbə koduna/ mətninə (“source code”), proqramlaşdırma, hazırlama alətlərinə və proqram	Razılaşdırılmamış, bəyan olunmamış funksionallığın daxil edilməsinin, pis niyyətlə və ya bilmədən dəyişiklilər edilməsinin	1) Mənbə koduna girişin məhdudlaşdırılması ilə bağlı meyarlar müəyyən edilibmi?	12	0			
			2) Mənbə koduna giriş hüququ olan şəxslərin siyahısı müəyyən edilibmi?	8	0			
			3) Mənbə koduna giriş hüquqları necə monitorinq edilir?	10	0			

	kitabxanalarına oxumaq və yazmaq imkanları mütləq müvafiq qaydada nəzarətdə saxlanılmalı, idarə edilməlidir	əvvəlcədən qarşısını almaq və dəyərli əqli mülkiyyətin konfidensiallığını qorumaq	4) Mənbə kodunun mərkəzləşdirilmiş saxlanma kitabxanası (mənbə kodu repozitoriyası) formalaşdırılıbmı?	8	0	**0%**		
			5) Mənbə kodu kitabxanasına (repozitoriyasına) bütün girişlərin və mənbə koduna edilən bütün dəyişikliklərin audit jurnalı aparılması təmin olunurmu?	12	0			
4.6.	**Təhlükəsiz autentifikasiya**			**158**				
	Vəzifə	Hədəf						
	İnformasiyaya müraciətlər, girişlər bu sahəyə aid prosedura uyğun idarə olunmalı, məhdudlaşdırılmalıdır və bunun üçün etibarlı, təhlükəsiz autentifikasiya texnologiyaları, prosedurları tətbiq olunmalıdır	Sistemlərə, tətbiqi proqram vasitələrinə və xidmətlərə müraciət, giriş icazəsi vermək üçün istifadəçinin və ya digər varlıqların təhlükəsiz autentifkasiyasını təmin etmək	1) İstifadəçinin, proqram vasitələrinın və digər varlıqların iddia olunan identikliyini sübut etmək üçün uyğun autentifikasiya metodu müəyyən olunubmu?	30	0	**0%**		
			2) Autentifikasiyanın etibarlılıq səviyyəsi giriş nəzərdə tutulan informasiyanın təsnifat kateqoriyasına uyğun olması təmin olunurmu? Bunun üçün alternativ metodların (məsələn: rəqəmsal sertifikatların, smart kartların, aparat açarlarının, tokenlərin, kriptoqrafik vasitələrin, biometrik vasitələrin) istifadəsi nəzərdə tutulurmu?	32	0			
			3) Kritik informasiya sistemlərinə daxil olmaq üçün çox faktorlu autentifikasiyanın tətbiqi təmin olunurmu?	45	0			
			4) Biometrik autentifikasiya məlumatlarının aktuallığı, müəyyən səbəblərdən dəyişəndən sonra (məsələn: insanın qocalması, cərrahi əməliyyat, qəza hadisəsi səbəbindən) yenilənmə mexanizmi müəyyən olunubmu?	18	0			
			5) Sistemə, tətbiqi proqram vasitəsinə və xidmətə icazəsiz giriş riskini minimallaşdıra bilən müraciət, giriş proseduru, texnologiyası müəyyən olunubmu?	33	0			
4.7.	**Potensialın, imkanların idarə edilməsi**			**43**				
	Vəzifə	Hədəf						
	Resursların istifadə vəziyyətinin cari və gözlənilən potensiala, imkanlara aid tələblərə uyğun olması nəzarətdə saxlanılmalı və tənzimlənməlidir	İnformasiya emalı vasitələrinin, insan resurslarının, ofislərin və digər obyektlərin tələb olunan potensiala, imkanlara (“capacity requirements”) uyğun olmasını təmin etmək	1) Müvafiq sistemlərin və proseslərin fəaliyyətin kritikliyi nəzərə alınmaqla, informasiya emalı vasitələrinin, insan kapitalının, ofislərin və digər obyektlərin potensialına, imkanlarına tələblər (“capacity requirements”) müəyyən olunubmu?	10	0			
			2) Sistemlərin, xidmətlərin əlçatanlığını və səmərəliliyini təmin etmək və zəruri hallarda təkmilləşdirmək üçün tənzimləmə və monitorinq təmin olunurmu? Real göstəricilərin (performansın)	13	0			

			potensial, imkan tələblərinə uyğunluğu müəyyən olunurmu? Stress-testlər həyata keçirilirmi? Problemlərin vaxtında aşkarlanması mümkün olurmu?			**0%**		
			3) Davamlı təkmilləşdirmə üçün potensial tələblərin proqnozlaşdırılması təmin olunurmu? Fəaliyyətin tələbatları, tendensiyalar, satınalma müddətlərinin uzun olması, xərclərin yüksək olması vaxtında nəzərə alınırmı?	8	0			
			4) Resurs məhdudiyyətləri, korporativ kompetensiya səviyyəsi və əsas işçilərdən asılılıq müəyyən olunubmu? Müvafiq tədbirlər planlaşdırılırmı?	6	0			
			5) Tələb olunan potensialın, imkanların təmin olunması üçün mövcud potensialdan, imkanlardan istifadənin optimallaşdırılması planı müəyyən olunubmu?	6	0			
4.8.	**Zərərli proqramlardan qorunma**			**158**				
	Vəzifə	Hədəf						
	Zərərverici proqram təminatından mühafizə istifadəçi məlumatlılığının müvafiq səviyyədə olmasını təmin etməklə həyata keçirilməli və dəstəklənməlidir	İnformasiyanın və informasiya ilə əlaqəli aktivlərin zərərverici proqramlardan mühafizəsini təmin etmək	1) Zərərli proqramların aşkar edilməsi üçün antivirus proqramları və alətlər istifadə olunurmu?	30	0	**0%**		
			2) Antivirus proqramları və alətləri XRİTDX-nin mərkəzləşdirilmiş sisteminə inteqrasiya edilibmi?	28	0			
			3) Son istifadəçi kompüterində zərərverici aşkar edildikdə insidentə cavab proseduru varmı? Zərərverici proqram tərəfindən istifadə edilə bilən zəifliklər müəyyən olunubmu?	40	0			
			4) Əməkdaşlara elektron poçt və media vasitələri ilə gələn zərərvericilər barədə təlimlər keçirilibmi? İstifadəsinə icazə verilən proqram təminatının, vebsaytların siyahısı, onların tətbiq sahələri müəyyən olunubmu?	30	0			
			5) Sistemlərin, xüsusən də kritik fəaliyyət proseslərini dəstəkləyən sistemlər üçün proqram təminatının və verilənlərin məzmununun müntəzəm avtomatlaşdırılmış yoxlanması, icazəsiz faylların, dəyişikliklərin mövcudluğunun araşdırılması təmin olunurmu?	30	0			
	Konfiqurasiyaların təhlükəsizliyi			**129**				
	Vəzifə	Hədəf						
	Proqram, texniki və mühəndis təminatı	Proqram, texniki və mühəndis təminatı	1) Avadanlıq, proqram təminatı, servis və şəbəkələrin konfiqurasiyalarının, o cümlədən	40	0			

4.9.	vasitələrinin, xidmətlərin və şəbəkələrin konfiqurasiyaları, o cümlədən təhlükəsizlik konfiqurasiyaları müəyyənləşdirilməli, sənədləşdirilməli, tətbiq olunmalı, fasiləsiz monitorinq edilməli və mütəmadi yoxlanılmalıdır	vasitələrinin, xidmətlərin və şəbəkələrin funksionallıqlarının təhlükəsizlik üzrə tələb olunan parametrlərə uyğun olmasını, konfiqurasiyalarında sanksiyasız və ya yanlış dəyişikliklərin qarşısının alınmasını təmin etmək	təhlükəsizlik konfiqurasiyalarının idarə edilməsi həyata keçirilirmi? Bu konfiqurasiyalar, onların baza vəziyyəti (təsdiqlənmiş ilkin konfiqurasiya) müəyyən olunubmu?			**0%**		
			2) Standart konfiqurasiya şablonları müəyyən edilibmi?	20	0			
			3) Konfiqurasiyalara edilən dəyişikliklər nəzarət altında edilirmi? Konfiqurasiyada dəyişikliklərin qeydiyyatı aparılırmı?	30	0			
			4) İcazəsiz və ya təhlükəli dəyişikliklərin qarşısını almaq üçün yoxlama və təsdiq prosedurları varmı?	25	0			
			5) Mütəmadi olaraq konfiqurasiyaların ehtiyat nüsxələri çıxarılıb təhlükəsiz yerdə saxlanılırmı?	14	0			
4.10.	**Məlumatların silinməsi**			**65**				
	Vəzifə	Hədəf						
	İnformasiya sistemlərində, qurğularda və ya hər hansı digər yaddaş daşıyıcılarında saxlanılan məlumatlar, lazım olmayandan sonra, silinməlidir	Konfidensial informasiyanın lazım olmayan hallarda açıqlanmasının qarşısını almaq və informasiyanın silinməsi lazım olan hallarda qanunvericilik, normativ və müqavilə tələblərini təmin etmək	1) İnformasiya sistemlərində, cihazlarında və ya hər hansı başqa yerdə saxlanılan məlumatlar ehtiyac qalmadıqda silinirmi?	20	0	**0%**		
			2) Silinməsi planlaşdırılan məlumatlar təsnifatlaşdırılmı?	10	0			
			3) Məlumatların silinməsi üçün istifadə edilən metod və alətlərə tələblər müəyyən olunubmu? Bulud xidmətlərindən istifadə edildikdə, bulud xidməti provayderi tərəfindən təqdim edilən silmə metodunun məqbul olub-olmadığının yoxlanılmasına tələblər müəyyən olunurmu?	15	0			
			4) Silinmə prosesinin təsdiqi üçün prosedurlar müəyyən olunubmu?	10	0			
			5) Bu silinmə və onun nəticələrinin sübut kimi qeydiyyatı təmin olunurmu?	10	0			
4.11	**Məlumatların maskalanması**			**65**				
	Vəzifə	Hədəf						
	Məlumatların maskalanması mexanizmindən qurumun müraciətə, girişə nəzarət üzrə və digər əlaqəli sahələr üzrə prosedurlarına və müvafiq qanunvericiliyə və işgüzar (biznes)	Fİİ (“PII”) daxil olmaqla həssas məlumatların açıqlanmasını məhdudlaşdırmaq və qanunvericilik, normativ və müqavilə tələblərini təmin etmək	1) Məlumatların maskalanması həyata keçirilirmi?	15	0	**0%**		
			2)Konfidensial informasiyanın xüsusi mühafizəsinə, bunun üçün psevdonimləşdirməyə, anonimləşdirməyə qurumda ehtiyac olan hallar müəyyən olunubmu?	15	0			
			3) Fİİ (fərdi identifikasiya informasiyasının) və digər konfidensial, o cümlədən həssas məlumatların gizlədilməsinə (Fİİ ilə onun subyekti arasında heç bir əlaqənin göstərilməməsinə), o cümlədən	25	0			

	fəaliyyətin tələblərinə uyğun olaraq istifadə edilməlidir		maskalanmasına (Fİİ-nin konfidensial elementlərinin əvəzlənməsi), psevdonimləşdirilməsinə (Fİİ-nin təxəllüslə, ləqəblə əvəzlənməsinə) və ya anonimləşdirilməsinə (Fİİ-nin geri dönə bilinməz formada dəyişdirilməsinə) aid müvafiq metodlar və texnologiyalar tətbiq edilirmi?					
			4) Maskalanmış məlumatların istifadəsi ilə bağlı qeydlər aparılırmı?	10	0			
4.12.	**Data baza təhlükəsizliyi**			**129**				
	Vəzifə	Hədəf						
	Qurumda verilənlərin toplanılıb saxlanılma strukturları (relyasion, çoxölçülü, faktəsaslı, obyekt-yönümlü, xronologiya əsaslı (“relational, dimensional, fact-based, object-oriented, time-based” və NoSQL modelləri üzrə), verilənlərin tipləri (təsnifatlaşdırma kateqoriyaları haqqında, aktivlər, resurslar haqqında, fəaliyyət prosesləri haqqında, tranzaksiyalar haqqında verilənlər üzrə), verilənlər arasında əlaqə mexanizmləri, verilənlərə rollar üzrə səlahiyyətlər bölgüsü müəyyən olunmalıdır	İnformasiya mühafizəsinin obyekti olan verilənlərin keyfiyyətini, o cümlədən tamlığını, mötəbərliyini onların həyat dövrü (yazma, oxuma, təzələmə, pozma/ "create, read, update, delete") proseslərində təmin etmək	1) Data baza məlumatlarının təhlükəsizliyi təmin edilirmi?	35	0	**0%**		
			2) Data bazaya girişlərin idarə edilməsi həyata keçirilirmi?	30	0			
			3) Data bazaya girişlərin qeydiyyatı aparılırmı?	29	0			
			4) Mühafizə olunan şəxslərin fərdi məlumatlarına girişlərə nəzarət tətbiq edilibmi?	25	0			
			5) Proqram təminatının hazırlanması zamanı yalnız test məlumatlarından istifadə təmin olunurmu?	10	0			
4.13.	**Məlumatların sızmasının qarşısı necə alınır?**			**180**				
	Vəzifə	Hədəf						
	İnformasiya sızmasının qarşısının alınması tədbirləri həssas məlumatları emal edən, saxlayan və ya ötürən	Fərdlər və ya sistemlər tərəfindən informasiyanın icazəsiz açıqlanmasının və çıxarılmasının	1) Sızmadan mühafizə olunmalı olan informasiya, icazəsiz açıqlanma riski olan həssas informasiya müəyyən olunubmu, təsnifatlaşdırılıbmı?	40	0			
			2) Məlumatların sızma cəhdlərinin qeydiyyatı və analizi aparılırmı?	35	0			

	sistemlərə, şəbəkələrə və avadanlıqlara tətbiq edilməlidir	aşkarlanmasını və qarşısının alınmasını təmin etmək	3) Məlumatların sızmasının qarşısının alınması üçün müvafiq alətlər və texnologiyalar istifadə edilirmi?	50	0	**0%**		
			4) Sızma halında qurumun reaksiyası üçün müvafiq prosedurlar mövcuddurmu?	30	0			
			5) Məlumat sızmasının qarşısının alınması tədbirləri həssas məlumatları emal edən, saxlayan və ya ötürən sistemlərə, şəbəkələrə və bütün digər cihazlara tətbiq edilirmi?	25	0			
4.14.	**Məlumatların ehtiyat nüsxələnməsi**			**122**				
	Vəzifə	Hədəf						
	İnformasiyanın, proqram təminatının və sistemlərin ehtiyat nüsxələri saxlanılmalı və bu sahəyə aid prosedura uyğun olaraq müntəzəm sınaqdan keçirilməlidir	İnformasiyanın və ya sistemlərin itki, nasazlıq baş verən hallarda bərpa olunma imkanını təmin etmək	1) Qurumda məlumatların ehtiyat nüsxələnməsi üçün müvafiq siyasət və ya prosedurlar mövcuddurmu?	18	0	**0%**		
			2) Məlumatların ehtiyat nüsxələnməsi üçün müvafiq metodlar (məsələn: tam, diferensial, artan) istifadə olunurmu?	16	0			
			3) Ehtiyat nüsxələnmə prosesi müvafiq tezliklə (gündəlik, həftəlik, aylıq) həyata keçirilirmi?	24	0			
			4) Ehtiyat nüsxələnməsi həyata keçirilən məlumatların saxlandığı müvafiq mühit (lokal, bulud, xarici disk) müəyyən edilibmi?	14	0			
			5) Ehtiyat nüsxələrin mühafizəsi üçün təhlükəsizlik tədbirləri görülürmü?	18	0			
			6) Kritik məlumatların ehtiyat nüsxələri kriptoqrafik vasitələrlə qorunurmu?	20	0			
			7) Qurum bulud xidmətindən istifadə etdikdə, bulud xidməti mühitində qurumun məlumat, proqram və sistemlərinin ehtiyat nüsxələrinə aid tələblər təchizatçı ilə razılaşdırma sənədində müəyyən olunubmu? Monitorinq olunurmu?	12	0			
4.15.	**Məlumat emalı qurğularının yetərli və ehtiyat imkanlı (məqbul izafi) olması**			**57**				
	Vəzifə	Hədəf						
	İnformasiya emalı vasitələri, əlçatanlıq və yararlılıq (“availability”) tələblərinə əməl olunması üçün, yetərli qədər (məqbul izafiliklə) ehtiyat imkanlara malik olmalıdır	İnformasiya emalı vasitələrinin fasiləsiz fəaliyyətini təmin etmək	1) Qurumda fəaliyyətə lazım olan xidmətlərə və informasiya sistemlərinə, onların əlçatanlığına aid tələblər müəyyən olunubmu? Bu tələblər fəaliyyətin davamlılığını və riskləri idarəetmə tələbləri ilə uzlaşdırılırmı?	12	0			
			2) Bu tələblərə uyğun xidmətlərin spesifikasiyasının və informasiya sistemlərinin arxitekturasının ehtiyat imkanlar nəzərdə tutmaqla (məqbul izafi olmaqla),	15	0			

			layihələndirilməsi təmin olunurmu? Məlumat emalı sistemləri üçün ehtiyat avadanlıqlar və ya şəbəkələr mövcuddurmu?			**0%**		
			3) Ehtiyat sistemləri qurumun əsas məlumat emalı sistemləri ilə eyni performans səviyyəsini təmin edirmi?	10	0			
			4) Ehtiyat sistemlərinin aktivləşdirilməsi halları müəyyən edilibmi?	8	0			
			5) Ehtiyat sistemlərinin iş qabiliyyəti mütəmadi olaraq test edilirmi?	12	0			
4.16.	**Hadisələrin qeydiyyatı (loqlar)**			**115**				
	Vəzifə	Hədəf						
	Fəaliyyətləri, istisnaları, nasazlıqları və digər müvafiq hadisələri qeyd edən jurnallar formalaşdırılmalı, saxlanmalı, mühafizə olunmalı və müntəzəm təhlil edilməlidir	Hadisələrin qeydiyyatını, dəlil-sübutların yazılmasını, jurnal məlumatlarının tamlığını təmin etmək, icazəsiz müraciətin, girişin qarşısını almaq, informasiya təhlükəsizliyi insidentinə səbəb ola biləcək informasiya təhlükəsizliyi hadisələrini müəyyən etmək və araşdırmaları dəstəkləmək	1) Hadisələrin qeydiyyatı (loqlar) aparılırmı? İnformasiya təhlükəsizliyi hadisələrinin qeydiyyat jurnallarında (lokal və mərkəzləşdirilmiş sistem jurnallarında) toplanılmalı olan məlumatların siyahısı müəyyən olunubmu?	25	0	**0%**		
			2) Hadisə qeydiyyatı aparılan sistemlər və tətbiqlər müəyyən edilibmi? Təhlükəsizlik məlumatlarını və hadisələri idarəetmə sistemi (SIEM) tətbiq olunurmu?	25	0			
			3) Qeydlərin konfidensiallığının və dəyişdirilməyə qarşı qorunmasının təmin edilmə tədbirləri həyata keçirilirmi? Sistem jurnallarına aid informasiya təhlükəsizliyi tələbləri və təhdidlər müəyyən olunubmu?	20	0			
			4) Qeydlər mütəmadi olaraq nəzərdən keçirilirmi və analiz edilirmi? İnformasiya təhlükəsizliyi hadisələrini, o cümlədən informasiya məkanının konfiqurasiyasının komponentlərində və parametrlərində icazəsiz dəyişiklikləri, buna cəhdləri, bu məkanda funksional anomaliyalarını aşkarlama üçün tələb olunan məlumatların siyahısı müəyyən olunubmu?	25	0			
			5) Məlumatın emalı və ya göndərilməsinə təsir edə biləcək istifadəçi və ya sistem xətaları qeydə alınırmı? Informasiya təhlükəsizliyi hadisələrinin qeydiyyat jurnallarını idarəetmə prosesləri, rollar və vəzifələr (məsuliyyətlər) müəyyən olunubmu? Jurnalların informasiya mənbələri ilə uzlaşdırılma mexanizmi müəyyən olunubmu?	15	0			

			6) Qeydlərin saxlanma müddətləri müəyyən edilibmi?	5	0		**0%**	
4.17.	**Monitorinq fəaliyyəti**			**115**				
	Vəzifə	Hədəf						
	Funksionallıqda anomaliyalar (normal funksionallqdan sapmalar) müəyyən olunmalıdır, bunun üçün, şəbəkələr, sistemlər və proqramlar monitorinq edilməli və ola bilən informasiya təhlükəsizliyi insidentlərini qiymətləndirmək üçün müvafiq tədbirlər görülməlidir	Davranışda, funksionallqda anomaliyaları və potensial informasiya təhlükəsizliyi insidentlərini aşkar etmək (baş verən riskləri müəyyən etmək)	1) Monitorinq fəaliyyəti ilə bağlı siyasət və yaxud prosedur mövcuddurmu?	15	0			
			2) Şəbəkə, sistem və tətbiqlərin monitorinqi üçün texnologiyalar və alətlər müəyyən olunubmu?	25	0			
			3) Şəbəkə və sistemlərdə icazəsiz dəyişiklikləri, buna cəhdləri, anomaliyaları aşkarlamaq üçün alqoritmlər və ya metodlar müəyyən olunubmu?	35	0			
			4) Monitorinq nəticələrinə dair hesabatlar mütəmadi olaraq hazırlanırmı?	20	0	**0%**		
			5) Hazırlanan hesabatlar rəhbərlik və müvafiq komandalarla paylaşılırmı?	20	0			
4.18.	**Saat sinxronizasiyası**			**29**				
	Vəzifə	Hədəf						
	Qurum tərəfindən istifadə olunan informasiya emalı sistemlərinin saatları təsdiq edilmiş vaxt mənbələri ilə sinxronlaşdırılmalıdır	Təhlükəsizliklə bağlı hadisələrin və digər qeydə alınmış informasiyanın korrelyasiyasını və təhlilini təmin etmək, informasiya təhlükəsizliyi insidentləri ilə bağlı araşdırmaları dəstəkləmək	1) Saat sinxronizasiyası tətbiq edilirmi?	6	0			
			2) Saat sinxronizasiyası tətbiq olunan sistemlər və avadanlıqlar müəyyən olunubmu?	5	0			
			3) Saat sinxronizasiyası tam avtomatlaşdırılıbmı?	6	0			
			4) Saat sinxronizasiyası tətbiq olunan bütün informasiya sistemlərinin saatları dəqiq bir mənbə ilə sinxronlaşdırılıbmı?	8	0	**0%**		
			5) Saat sinxronizasiyasına aid hadisələrin qeydiyyatı təmin olunurmu?	4	0			
4.19.	**İmtiyazlı proqram təminatlarının istifadəsi**			**65**				
	Vəzifə	Hədəf						
	Sistem və tətbiqi idarəetmə vasitələrindən yan keçə (aşa), onları əvəzləyə və ya üstələyə bilən utilit (köməkçi) proqram təminatı vasitələrinin istifadəsi məhdudlaşdırılmalı və	İnformasiya təhlükəsizliyinə, onun sistem və proqram idarəetmə alətlərinə utilit (köməkçi) proqram təminatı vasitələrindən zərər vurulmamasını təmin etmək	1) İmtiyazlı proqram təminatlarının istifadəsi idarə edilirmi?	15	0			
			2) İmtiyazlı proqramların istifadəsi zamanı fəaliyyətlər monitorinq olunurmu?	15	0			
			3) İmtiyazlı proqramların istifadəçilərinə giriş məhdudiyyətləri tətbiq olunurmu?	15	0			
			4) İmtiyazlı utilit (köməkçi) proqramların qurumun sistemlərində və tətbiqi vasitələrində qoyulmuş nəzarət tədbirlərini yan keçə (aşa), onları əvəzləyə və ya üstələyə bilən imkanları, həmin sistem və	10	0	**0%**		

	ciddi nəzarətdə saxlanılmalıdır		vasitələrdə bu utilitlərin təhdid üçün istifadə edə biləcəyi zəifliklər (boşluqlar, çatışmazlıqlar, nəzarətsizliklər və digər uyğunsuzluqlar) müəyyən olunubmu?					
			5) İmtiyazlı proqramların istifadəsinə dair audit qeydləri saxlanılırmı? Bu qeydlər mütəmadi olaraq nəzərdən keçirilirmi?	10	0			
4.20.	**Əməliyyat sistemlərində proqram təminatlarının quraşdırılması**			**57**				
	Vəzifə	Hədəf						
	Əməliyyat sistemlərində proqram təminatı vasitələrinin quraşdırılmasını təhlükəsiz idarə etmək üçün tənzimləyici prosedurlar və tədbirlər işlənilib hazırlanmalı, tətbiq olunmalıdır	Əməliyyat sistemlərinin bütövlüyünü təmin etmək və texniki zəifliklərdən istifadənin qarşısını almaq	1) Əməliyyat sistemlərində proqram təminatlarının quraşdırılması prosedurları varmı?	12	0	**0%**		
			2) Quraşdırılan proqram təminatları etibarlı mənbələrdən götürülürmü?	15	0			
			3) Lisenziyasız (crack) proqram təminatlarından istifadə halları olurmu? Lisenziyasız (crack) proqram təminatından istifadə aşkarlandıqda qarşısı alınırmı?	10	0			
			4) Quraşdırma yalnız imtiyazlı şəxslər tərəfindən həyata keçirilirmi?	12	0			
			5) Quraşdırılmasına icazə verilən və qadağan edilən proqram təminatının növləri müəyyən olunubmu?	8	0			
4.21.	**Şəbəkələrin təhlükəsizliyi**			**180**				
	Vəzifə	Hədəf						
	Şəbəkələr və şəbəkə avadanlıqları (onlarla əlaqəsi olan sistemlərdə və tətbiqi proqram təminatı vasitələrində olan informasiyanın təhlükəsizliyi üçün) mühafizə olunmalı, onlara inzibatçılıq olunmalı və onlar nəzarətdə saxlanılmalıdır	Şəbəkələrdə və onları dəstəkləyən informasiya emalı vasitələrində olan informasiyanı şəbəkədən istifadə etməklə nüfuzdan salma təhdidlərindən qorunmasını təmin etmək	1) Qurumun şəbəkə təhlükəsizliyi üçün siyasət və ya proseduru mövcuddurmu?	20	0	**0%**		
			2) Mövcud şəbəkələrin güncəl və təsdiqlənmiş topologiyası mövcuddurmu?	20	0			
			3) Şəbəkə təhlükəsizliyi üçün konkret məsuliyyətlər müəyyən edilibmi?	15	0			
			4) Şəbəkənin təhlükəsizlik arxitekturası mütəmadi olaraq nəzərdən keçirilir və yenilənirmi?	25	0			
			5) Şəbəkəyə daxil olmaq üçün autentifikasiya və səlahiyyət yoxlanışı tətbiq edilirmi?	35	0			
			6) Şəbəkə avadanlıqlarına və resurslarına girişi məhdudlaşdırmaq üçün mexanizmlər mövcuddurmu?	30	0			
			7) Şəbəkədə baş verən hadisələrin monitorinqi aparılırmı? Şəbəkələrin konfiqurasiyası, qurumun informasiya təhlükəsizliyinə təsir edə bilən və ya	35	0			

			ona aidiyyəti olan hadisələrin qeydiyyatı təmin olunurmu?					
4.22.	**İnternet və qurumlararası əlaqələrin təhlükəsizliyi**			**300**				
	Vəzifə	Hədəf						
	Qurumun qlobal internet şəbəkəsinə qoşulmasında və digər dövlət qurumları ilə olan şəbəkə əlaqələrində AzStateNet şəbəkəsindən istifadə edilməlidir. Rəsmi veb-sayt GOV.AZ domen zonasında yerləşməli və rəsmi mail yazışmaları XRİTDX mail şlüzündən keçməlidir	İnternet şəbəkəsindən gələ biləcək təhdidlərin qarşısını almaq və digər dövlət qurumları ilə əlaqə zamanı ötürülən məlumatların təhlükəsizliyini təmin etmək. Rəsmi veb-saytın və mail xidmətinin təhlükəsizliyini təmin etmək	1) Qurum internet bağlantısı üçün yalnız AzStateNet şəbəkəsindən istifadə edirmi?	60	0	**0%**		
			2) Qurum digər dövlət qurumları ilə əlaqə üçün yalnız AzStateNet şəbəkəsindən istifadə edirmi?	50	0			
			3) 3-cü tərəflərlə əlaqə üçün istifadə edilən hər hansı digər monitorinq olunmayan şəbəkə mövcuddurmu?	50	0			
			4) Qurumun mail serveri XRİTDX-nin mail şlüzündən istifadə edirmi?	80	0			
			5) Qurumun rəsmi internet ünvanları GOV.AZ zonasındadırmı?	60	0			
4.23.	**Şəbəkə xidmətlərinin təhlükəsizliyi**			**65**				
	Vəzifə	Hədəf						
	Şəbəkə xidmətlərinin təhlükəsizlik mexanizmləri, xidmət səviyyələri və xidmət tələbləri müəyyən edilməli, tətbiq edilməli və monitorinq edilməlidir	Şəbəkə xidmətlərindən istifadə zamanı təhlükəsizliyi təmin etmək	1) Qurumda istifadə olunan şəbəkə xidmətlərinin siyahısı və təsviri mövcuddurmu?	10	0	**0%**		
			2) Şəbəkə xidmətlərinin təhlükəsizlik tələbləri müəyyən edilib və sənədləşdirilibmi? Şəbəkə xidmətlərinin təhlükəsizlik tələblərinə uyğunluğu fasiləsiz monitorinq olunurmu?	15	0			
			3) Şəbəkə xidmətlərinə giriş səlahiyyətləri idarə olunurmu?	15	0			
			4) Şəbəkə xidmətlərinə giriş qeydləri (loglar) saxlanılır və analiz olunurmu?	10	0			
			5) Şəbəkə xidmətləri ilə təhlükəsiz əlaqə qurmaq üçün müvafiq protokollar (məsələn: HTTPS, VPN) müəyyən olunubmu?	10	0			
			6) Şəbəkə xidmətləri ilə əlaqəli şifrələmə açarlarının idarə edilməsi proseduru mövcuddurmu?	5	0			
	Şəbəkənin seqmentasiyası			**122**				
	Vəzifə	Hədəf						
	İnformasiya xidmətləri, istifadəçilər və informasiya sistemləri müvafiq şəbəkələrdə	Şəbəkələrin təhlükəsizlik hüdudlarında	1) Qurumun şəbəkələri informasiya xidmətləri, istifadəçilər və informasiya sistemləri qrupları üzrə ayrılıbmı?	30	0			
			2) Şəbəkə seqmentləri arasında əlaqəni idarə					

4.24	qruplalaşdırılmalıdır (seqmentləşdirilməlidir)	(sərhədlərində), biznes tələbatlarına uyğun olaraq, bir-birindən ayrılmasını və onlar arasında trafikin nəzarətdə saxlanılmasını təmin etmək	etmək üçün müvafiq texnologiyalar (məsələn: firewall, VLAN) müəyyən olunubmu? Şəbəkə seqmentləri arasında giriş üçün şlüzlər ("gateways"), məsələn: təhlükəsizlik divarları, filtrləmə marşrutlaşdırıcıları müəyyən olunubmu?	30	0	**0%**		
			3) Hər bir şəbəkə seqmentinə giriş səlahiyyətləri müəyyənləşdirilib və sənədləşdirilibmi?	22	0			
			4) Giriş hüquqları şəbəkə seqmentlərinin təhlükəsizlik səviyyəsinə uyğun olaraq məhdudlaşdırılıbmı?	25	0			
			5) Simsiz şəbəkələrin ayrılması zamanı radio siqnalın əhatə dairəsinin qeyri-dəqiq olması nəzərə alınıbmı? Bütün simsiz girişin xarici əlaqə kimi nəzərdən keçirilməsi və daxili şəbəkələrdən müvafiq şlüzlə ayrılması təmin olunubmu?	15	0			
4.25.	**Veb filtrləmə**			**36**				
	Vəzifə	Hədəf						
	Zərərverici (bədniyyətli) məzmuna (kontentə) məruzqalma riskini azaltmaq üçün xarici veb-saytlara müraciətlər, girişlər idarə edilməlidir	Sistemləri zərərverici proqram vasitələri ilə nüfuzdan salınmadan qorumaq və icazəsiz veb-resurslara müraciətin, girişin qarşısını almaq	1) Qurumun iş fəaliyyəti üçün hansı veb-saytların və ya xidmətlərin istifadəsinə icazə verildiyi müəyyən edilibmi?	6	0	**0%**		
			2) Veb filtrləmə texnologiyaları (məsələn: DNS filtrasiya, proxy serverlər) tətbiq edilirmi?	10	0			
			3) Bloklana bilən veb-saytların kateqoriyaları müəyyən edilibmi?	6	0			
			4) Fişinq, zərərli proqram yayan saytlar və ya qeyri-məqsədəuyğun məzmunlar avtomatik bloklanırmı?	10	0			
			5) Kiber gigiyena təlimlərinin keçirilməsi təmin olunurmu?	4	0			
4.26.	**Kriptoqrafiyadan istifadə**			**158**				
	Vəzifə	Hədəf						
	Kriptoqrafiyadan səmərəli istifadə prosedurları, o cümlədən kriptoqrafik açarların idarə edilməsi prosedurları müəyyən edilməli və tətbiq olunmalıdır	İşgüzar (biznes) fəaliyyət və informasiya təhlükəsizliyi tələblərinə uyğun olaraq, kriptoqrafiya ilə bağlı qanunvericilik, normativ və müqavilə tələblərini nəzərə alaraq, informasiyanın konfidensiallığını, tamlığını, mötəbərliyini və əlçatanlığını	1) Qurumda kriptoqrafiyanın istifadəsi ilə bağlı yazılı siyasət və prosedurlar mövcuddurmu?	25	0	**0%**		
			2) Təsnifatına uyğun olaraq saxlanma və ötürülmə zamanı məlumatlara şifrləmə tətbiq edilirmi?	45	0			
			3) Kriptoqrafiyadan səmərəli istifadə qaydaları, o cümlədən kriptoqrafik açarların idarə edilməsi qaydaları müəyyən edilib və həyata keçirilibmi?	40	0			
			4) Əldə edilməsi qanunla məhdudlaşdırılan məlumatların ötürülməsi zamanı şifrləmə avadanlıqlarından istifadə edilirmi?	28	0			
			5) Açarların yaradılması, saxlanması və arxivləşdirilməsi üçün istifadə olunan fiziki	20	0			

		qorumaq üçün kriptoqrafiyadan düzgün və səmərəli istifadəni təmin etmək	daşıyıcıların, funksional proqram, texniki və mühəndis təminatı vasitələrinin fiziki təhlükəsizliyinə tələblər müəyyən olunubmu? Təmin olunurmu?					
4.27.	**Proqram təminatının hazırlanması zamanı informasiya təhlükəsizliyi**			**65**				
	Vəzifə	Hədəf						
	Proqram təminatı və sistemlərin təhlükəsizliyi üzrə prosedurlar müəyyən olunmalı və tətbiq edilməlidir	İnformasiya təhlükəsizliyinin layihələndirilməsini və həyata keçirilməsini proqram təminatının və sistemlərin təhlükəsiz işlənilib hazırlanmasının həyat dövrü çərçivəsində təmin etmək	1) Qurumun proqram təminatlarının həyat dövrü prosesi standart mərhələlərdən ibarətdirmi, bu mərhələlərdə təhlükəsizlik təmin edilirmi?	12	0		**0%**	
			2) Proqram təminatları hazırlanarkən və ya satın alınarkən informasiya təhlükəsizliyi tələbləri müəyyən edilir, dəqiqləşdirilir və təsdiqlənirmi?	12	0			
			3) Kodun versiyalaşdırılması və izlənilməsi sistematik şəkildə aparılırmı?	10	0			
			4) Açıq mənbə kitabxanalardan istifadə zamanı onların zəifliklərinə dair monitorinq aparılırmı?	10	0			
			5) Proqram təminatı istifadəyə verilməzdən əvvəl təhlükəsizlik auditi və ya penetrasiya testi aparılırmı?	15	0			
			6) Kənar şirkətlərə proqram təminatı yazdırarkən proqram təminatının mənbə kodları ilə birgə təhvil alınması nəzərdə tutulurmu?	6	0			
4.28.	**Təhlükəsizlik tələblərinin tətbiqi**			**65**				
	Vəzifə	Hədəf						
	Tətbiqi proqram təminatı vasitələrinin hazırlanması və ya əldə edilməsi zamanı informasiya təhlükəsizliyi tələbləri müəyyən edilməli, dəqiqləşdirilməli və təsdiq edilməlidir	Tətbiqi proqram təminatı vasitələri işlənilib hazırlanarkən və ya əldə edilərkən informasiya təhlükəsizliyi üzrə bütün tələblərinin müəyyən edilməsini və nəzərə alınmasını təmin etmək	1) Tətbiqi proqram təminatı vasitələrinin hazırlanması və ya əldə edilməsi zamanı informasiya təhlükəsizliyi tələbləri müəyyən olunurmu? Tətbiq olunurmu?	15	0		**0%**	
			2) Bunun üçün risklərin qiymətləndirilməsi və proqram təminatı vasitələrinin təyinatının nəzərə alınması təmin olunurmu?	15	0			
			3) Proqram təminatı vasitələri ilə emal ediləcək informasiyanın təsnifatı informasiya təhlükəsizliyi tələblərində nəzərə alınırmı?	15	0			
			4) Proqram təminatı vasitələrinin təyinatına aid sahə üzrə qanunvericilik, normativ, müqavilə tələbləri informasiya təhlükəsizliyi tələblərində nəzərə alınırmı?	10	0			
			5) Qurum və tərəfdaş arasında əməliyyat xidmətləri təmin edən proqramlar üçün informasiya	10	0			

			təhlükəsizliyi üzrə etimadlıq səviyyələri müəyyən olunurmu? Nəzərə alınırmı?					
4.29.	**Təhlükəsiz sistem arxitekturası və mühəndislik prinsipləri**			**72**				
	Vəzifə	Hədəf						
	Təhlükəsiz sistemlərin mühəndislik prinsipləri yaradılmalı, sənədləşdirilməli, saxlanmalı və istənilən informasiya sisteminin inkişafı fəaliyyətlərinə tətbiq edilməlidir	İnformasiya sistemlərinin təhlükəsiz şəkildə layihələndirilməsini, tətbiq olunmasını və istismar olunmasını sistemlərin işlənilib hazırlanmasının həyat dövrü ərzində təmin etmək	1) Təhlükəsizlik sistemlərin mühafizəli qurulmasına dair prinsiplər müəyyən olunubmu? Risklər bütün arxitektura səviyyələrində (fəaliyyət prosesləri, verilənlər, proqramlar və texnologiya) nəzərə alınırmı?	18	0	**0%**		
			2) İstismara və təhlükəsizliyə aid arxitekturaların inteqrasiyanı təmin olunurmu?	25	0			
			3)Təhlükəsiz sistem mühəndisliyi aşağıdakı prinsipləri əhatə edirmi? - “layihələndirmə ilə təhlükəsizlik” (“security by design”); - “dərin mühafizə” (“defence in depth”); - “susma ilə təhlükəsizlik” (“security by default”); - “ susma ilə qadağa” (“default deny”); - “təhlükəsiz imtina” (“fail security”); - “kənar proqram vasitələrindən verilənlərə inamsızlıq” (“distrust input from external applications”; - “yerləşdirmədə təhlükəsizlik” (“security in deployment”); - “pozuntu ehtimalı” (“assume breach”); - “ən az imtiyaz” ("least privilege"); - “istifadə olunmalıq və idarə olunmalıq” (“usability and manageability”); - “ən az funksionallıq” (“least functionality”); - “verilənlərin sanitarizasiyası” (“data sanitisation”); - “sıfır inam” ("zero trust"); “heç vaxt inanma və həmişə yoxla” (“never trust and always verify”)	12	0			
			4) Qurumda təhlükəsizlik sistem mühəndisliyi prinsiplərinin (qurum və təchizatçı arasında müqavilələr vasitəsilə) informasiya sistemlərinin kənar təşkilatlar tərəfindən hazırlanmasına tətbiq edilməsi təmin olunurmu?	10	0			
			5) Qurumda təhlükəsizlik sistem mühəndisliyi prinsiplərinin (aktuallığı təmin etmək üçün)	7	0			

			mütəmadi olaraq nəzərdən keçirilməsi və təkmilləşdirilməsi təmin olunurmu?					
4.30.	**Təhlükəsiz kodlaşdırma**			**65**				
	Vəzifə	Hədəf						
	Proqram təminatının hazırlanması zamanı təhlükəsiz kodlaşdırma (proqram təminatının ilkin mətnini təhlükəsiz tərtib etmə) üzrə prinsiplər tətbiq edilməlidir	Proqram təminatının ilkin mətnini təhlükəsiz yazılmasını (tərtib olunmasını) təmin etmək, bununla da proqram təminatında informasiya təhlükəsizliyi üzrə potensial zəifliklərin (və digər uyğunsuzluqların) sayının azaldılmasını təmin etmək	1) Qurumda təhlükəsiz kodlaşdırma üzrə proseslər müəyyən olunubmu? Bununla əlaqədar, dünyada olan təhdidlər və qabaqcıl təcrübələr nəzərə alınırmı?	15	0	**0%**		
			2) Kodlaşdırmanın planlaşdırılması və hazırlıq mərhələsi aşağıdakı məsələləri əhatə edirmi? - işləyib hazırlama üçün inteqrasiya olunmuş mühitin (“IDE, integrated development environments”) formalaşdırılması; - işləyib hazırlama üçün aktual alətlərin (məsələn: kompilyatorların) seçilməsi və ayarlanması; proqram təminatı vasitəsinin təyinatına uyğun istismarına və təhlükəsizliyinə aid tələblərin müəyyən olunması, həmin vasitənin layihələndirilməsi, o cümlədən təhdidlərin modelləşdirilməsi	15	0			
			3) Kodlaşdırmanın həyata keçirilməsi mərhələsində proqram təminatı vasitəsinin mənbə kodunun tərtib olunması, sənədləşdirilməsi və sınaqlardan keçirilməsi təmin olunurmu? Sınaqların keçirilməsi proqram təminatının işlənilib hazırlanma zamanı və ondan sonra da təmin olunurmu? Proqram təminatında təhlükəsizlik zəifliklərini və digər uyğunsuzluqları aşkarlama üçün “statik proqram təhlükəsizlik testi” (“SAST, static application security testing”) prosesləri tətbiq olunurmu?	20	0			
			4) Proqram təminatı vasitəsinin tətbiq olunması və texniki müşayiət mərhələsi istismar, inzibatçılıq və mühafizə tədbirlərini əhatə edirmi?	10	0			
			5) Proqram təminatı vasitəsində təkmilləşdirmə lazım olduqda bunun üçün planlaşdırma və hazırlıq mərhələsinə keçid olunurmu?	5	0			
4.31.	**İşləyib hazırlama və təhvil təslim mərhələsində təhlükəsizlik sınaqları**			**72**				
	Vəzifə	Hədəf						
	Təhlükəsizliyin sınaqdan keçirilməsi	Proqram təminatı və ya onun ilkin mətni (kodu)	1) Yeni informasiya sistemlərinin, yeniləmələrin işləyib hazırlama prosesləri zamanı hərtərəfli					

	prosesləri işləyib hazırlamanın həyat dövrü ərzində müəyyən edilməli və tətbiq olunmalıdır	istehsal mühitinə yerləşdirildikdə informasiya təhlükəsizliyi tələblərinə əməl olunub-olunmamasını yoxlamaq	sınaqdan keçirilməsi və yoxlanılması təmin olunurmu? Təhlükəsizliyin sınaqlarının sistemlər və ya komponentlər üçün sınaqların tərkib hissəsi olması təmin olunurmu?	18	0	**0%**		
			2) Təhlükəsizlik testində aşağıdakılar əhatə olunurmu? - təhlükəsizlik funksiyaları; - təhlükəsiz kodlaşdırma; təhlükəsiz konfiqurasiyalar	14	0			
			3) Test planları tərtib olunurmu? Bu planlarda aşağıdakılar əhatə olunurmu? - test üzrə sınaqların ətraflı qrafiki; - sınaqlar üçün daxil olunan verilənlər və müəyyən şərtlərə uyğun gözlənilən nəticələr; - test nəticələrini qiymətləndirmə üçün meyarlar; - testdən sonrakı hərəkətlər.	12	0			
			4) Təşkilat kod təhlili alətləri və ya zəiflik skanerləri kimi avtomatlaşdırılmış alətlərdən istifadə edirmi? Bu testlər aşağıdakı məsələləri əhatə edirmi? - təhlükəsizlik zəifliklərinin müəyyən olunması – əvvəldən bildirmədən giriş məlumatları daxil etməklə və şərtlər yaratmaqla; - etibarlı olmayan konfiqurasiyaların və sistem zəifliklərinin müəyyən olunması – zəiflikləri skan etməklə; - etibarlı olmayan kodun və arxitekturanın müəyyən olunması – nüfuzetmə üsul və vasitələri tətbiq etməklə.	18	0			
			5) Sınaqların sınaq olunan obyektin təyinat mühitinə maksimal uyğun gələn mühitdə aparılması təmin olunurmu? Sınaqların dərinliyinin sınaq olunan obyektin əhəmiyyətinə mütənasibliyi təmin olunurmu?	10	0			
4.32.	**Kənar tərəfdə işləyib hazırlama**			**50**				
	Vəzifə	Hədəf						
	Qurum sistemin işlənilib hazırlanmasını kənar tərəflərə həvalə edəndə, bu fəaliyyəti istiqamətləndirməli,	Sistemin işlənilib hazırlanması kənar tərəflərə həvalə olunanda informasiya təhlükəsizliyi	1) Kənar tərəflərə sistemin işlənilib hazırlaması həvalə ediləndə bu fəaliyyəti istiqamətləndirmə, gözləntilərə cavab verib-vermədiyini daim nəzarətdə saxlamaq üçün prosedurlar müəyyən olunubmu?	12	0			

	nəzarətdə saxlamalı, o cümlədən monitorinq etməlidir	tədbirlərinin həyata keçirilməsini təmin etmək	2) Kənar tərəflərə işləyib hazırlama həvalə ediləndə lisenziya müqavilələri, texniki layihə sənədinə, proqram koduna mülkiyyəti və əqli mülkiyyət hüquqları müəyyən olunurmu?	10	0	**0%**		
			3) Kənar tərəflərə işləyib hazırlama həvalə ediləndə təhlükəsiz layihələndirmə, kodlaşdırma və sınaq təcrübələri üçün tələblər müəyyən olunurmu, müqaviləyə daxil edilirmi?	12	0			
			4) Kənar tərəflərə işləyib hazırlama həvalə ediləndə təhdid modelləri müəyyən olunurmu, test planlarında, o cümlədən məhsulların keyfiyyətinin və dəqiqliyinin qəbul sınaqlarında nəzərə alınırmı?	8	0			
			5) Kənar tərəflərə işləyib hazırlama həvalə ediləndə işləyib hazırlama və nəzarət proseslərinin auditi üçün müqavilə hüququ müəyyən olunurmu?	8	0			
4.33.	**İşləyib hazırlama, test və istismar mühitlərinin ayrılması**			**58**				
	Vəzifə	Hədəf						
	İşləyib hazırlama, sınaq və istismar mühitləri bir-birindən ayrılmalı və mühafizə olunmalıdırlar	İstehsal mühitini və informasiyanı işləyib hazırlama, sınaq proseslərində nüfuzdan salınmadan (komprometasiyadan) mühafizə etmək	1) İşləyib hazırlama, sınaq və istismar mühitləri arasında bir-birindən ayrılma səviyyəsi müəyyən olunubmu? Qurum tərəfindən Təmin olunurmu?	18	0	**0%**		
			2) Hər mühit üçün təhlükəsizlik müəyyən edilibmi?	12	0			
			3) İşləyib hazırlama, sınaq və istismar mühitlərinin təhlükəsizliyinin, o cümlədən bu mühitlərdə icazəsiz dəyişiklərin aşkarlanması üçün monitorinqi təmin olunurmu? Belə dəyişiklik imkanının qarşısının alınması təmin olunubmu?	18	0			
			4) Hər bir mühit üçün giriş hüquqları müəyyən edilibmi?	10	0			
4.34.	**Dəyişikliklərin idarə edilməsi**			**65**				
	Vəzifə	Hədəf						
	İnformasiyanın emalı vasitələrində və informasiya sistemlərində edilən dəyişikliklər dəyişiklikləri idarəetmə prosedurları ilə tənzimlənməlidir	Dəyişikliklər həyata keçirilərkən informasiya təhlükəsizliyini təmin etmək	1) İnformasiya emalı vasitələrində və informasiya sistemlərində dəyişikliklərin idarə edilməsi üçün prosedur mövcuddurmu?	18	0	**0%**		
			2) İnformasiya emalı vasitələrində və informasiya sistemlərində dəyişiklikləri təsdiqləyəcək şəxslər müəyyən olunubmu?	12	0			
			3) İnformasiya emalı vasitələrində və informasiya sistemlərində hər hansı bir dəyişiklik zamanı məlumatların itkisi və ya zədələnməsi riskini minimuma endirmək üçün müvafiq tədbirlər görülürmü?	20	0			

			4) İnformasiya emalı vasitələri və informasiya sistemləri dəyişikliklərinin tarixçəsi saxlanılırmı?	15	0			
4.35.	**Sınaq üçün verilənlər**			**29**				
	Vəzifə	Hədəf						
	Sınaq üçün istifadə olunan verilənlər diqqətlə seçilməli, mühafizə və idarə edilməlidir	Testin aktuallığını (relevantlığını) və sınaq üçün istifadə olunan əməliyyat məlumatlarının mühafizəsini təmin etmək	1) Sınaq üçün istifadə olunan verilənləri seçmə, mühafizə və idarəetmə proseduru müəyyən olunubmu?	6	0	**0%**		
			2) Real mühitdə seçilən sınaq məlumatları testlərin nəticələrinin etibarlılığını və istismar məlumatlarının məxfiliyini təmin etmək üçün yararlı olurmu?	6	0			
			3) Konfidensial informasiyanın (o cümlədən Fİİ-nin) işləyib hazırlama və sınaq mühitlərinə köçürülməsinin qarşısının alınması təmin olunurmu?	9	0			
			4) Qurumda və ya bulud xidmətində yaradılmasından asılı olmayaraq, sınaq məqsədlərinə istifadə olunan istismar məlumatlarının surətlərinin qorunması təmin olunurmu?	5	0			
			5) Test barədə məlumatların etibarlı şəkildə saxlanılması təmin olunurmu?	3	0			
4.36.	**Audit zamanı informasiya sistemlərinin qorunması**			**29**				
	Vəzifə	Hədəf						
	Tətbiqi sistemlərin qiymətləndirilməsini ehtiva edən audit testləri və digər etimad yaratma hərəkətləri planlaşdırılılmalı, auditor ilə müvafiq rəhbərlik arasında razılaşdırılmalıdır	Audit və digər etimad yaratma hərəkətlərinin istismarda olan sistemlərin funksionallığına və işgüzar (biznes) fəaliyyət proseslərinə təsirini minimallaşdırmaq	1) Tətbiqi sistemlərin qiymətləndirilməsini əhatə edən audit testlərinin və digər təhlükəsizliyin təsdiqlənmə tədbirlərinin planlaşdırılması və auditor ilə müvafiq rəhbərlik arasında razılaşdırılması təmin olunurmu?	6	0	**0%**		
			2) Texniki audit sınaqlarının həcminin razılaşdırılması və nəzarətdə saxlanılması təmin olunurmu?	5	0			
			3) Proqram və məlumatlara audit testləri üçün girişin “yalnız oxumaq üçün” səviyyəsi ilə məhdudlaşdırılması (belə imkan olmadıqda, testin auditor adından lazımi giriş hüquqlarına malik olan təcrübəli inzibatçı tərəfindən həyata keçirilməsi) təmin olunurmu?	8	0			
			4) Audit üçün lazım olan faylların təcrid olunmuş nüsxələrinə giriş icazəsinin verilməsi, audit başa çatdıqdan sonra bu nüsxələrin silinməsi və ya (audit sənədlərinin tələblərinə uyğun saxlamaq	6	0			

			öhdəliyi olduqda) onlara müvafiq mühafizənin verilməsi təmin olunurmu?					
			5) Audit üçün istifadə olunan bütün girişlərin qeydiyyatı və monitorinqi təmin olunurmu?	4	0			

İnformasiya təhlükəsizliyi vəziyyətinin qiymətləndirilməsi 4 ana istiqamət üzrə həyata keçirilir. 4 Ana istiqamətin ümumi faizi 100% olsa da onların hər birinin informasiya təhlükəsizliyinə təsiri baxımından müəyyən edilmiş təsir meyarı fərqləndirilmiş və təsir indeksi qarşısına yazılmışdır. Bununla yanaşı hər bir istiqamətin alt-meyarları, alt-meyarlarının da hər bir sualı informasiya təhlükəsizliyindəki əhəmiyyəti və roluna görə təsir indeksini aidiyyəti meyar və istiqamətin aldığı ümumi indeksin alt-qiyməti kimi indeksləşdirilmişdir. Belə ki, hər bir sual aid olduğu meyara təsiri baxımından cədvəldə qeyd olunmuş indeksə malikdir. Hər bir meyar üzrə sualların indeksləri toplandıqda həmin meyarın müəyyən olunmuş istiqamət üzrə təsir indeksini formalaşdırır. Hər bir meyarın təsir indeksi toplandıqda isə aidiyyəti istiqamətin informasiya təhlükəsizliyinə təsir indeksini formalaşdırır. Ümumilikdə "Təşkilati idarəetmə" üzrə meyarların toplamının ümumi informasiya təhlükəsizliyi vəziyyətinə təsiri 25%, "Əməkdaşlar və təchizatçılar" istiqaməti 25%, "Fiziki təhlükəsizlik" istiqaməti 15%, "Avadanlığa, proqram təminatına və məlumatların təhlükəsizliyi" istiqamətinə aid meyarların təsiri isə 35% hesablanmışdır. Hesablamanın asan olması üçün 25% - 2500, 25%-2500, 15%-1500, 35% - 3500 indeksi ilə göstərilmişdir.

Verilmiş suallara cavablama diaqnostikadan keyfiyyətli nəticə əldə etmək üçün 4 səviyyədə müəyyən edilmişdir. Bunlar sualda qeyd olunmuş tələb nəzərə alınmamışsa - 0 bal, nisbətən nəzərə alınmışsa 0,25 bal, nəzərə alınmış, lakin nisbi çatışmazlıqlar varsa - 0,75 bal, tam icrası nəzərə alınmışdırsa və ya icra edilirsə - 1 bal qiymətlə qiymətləndirilərək həmin sual üzrə təsir indeksinə vurulacaqdır. Hər bir meyar üzrə suallardan əldə edilmiş nəticələr toplandıqda və meyarın təsir indeksinə bölündükdə həmin meyar üzrə icra faizi əldə edilir. İstiqamət üzrə bütün sualların cavablanmasından əldə edilmiş nəticələr toplanıb istiqamətin təsir indeksinə bölünərsə aidiyyəti istiqamətin icra faizi əldə edilmiş olunur. Bütün sualların cavablanmasından əldə edilmiş nəticələr toplanıb 10000 bölünərsə, bu zaman qurumun ümumi informasiya təhlükəsizliyi səviyyəsinin faizlə göstəricisi müəyyən edilir.

“Dövlət qurumlarının informasiya təhlükəsizliyi mühitinin diaqnostikasının həyata keçirilməsi Qaydaları”na

2 nömrəli əlavə

Yerində baxış aktı

№ _____

“____” _____20____il **Bakı şəhəri**

Biz,

_____
(aktı tərtib edən şəxslərin soyadı, adı, vəzifəsi, aid olduğu dövlət qurumunun adı)

_____

_____
(diaqnostika aparılan qurumun adı)

_____

_____
(diaqnostika zamanı müəyyən edilmiş faktlar)

_____

müəyyən etdik.

Diaqnostika aparılan qurumun məsul əməkdaşı (əməkdaşları)

_____
(soyadı, adı, vəzifəsi)

_____
(soyadı, adı, vəzifəsi)

izah etdi:

_____
(izahatın və ya mülahizənin məzmunu)

Diaqnostika aparılan qurumun məsul əməkdaşı (əməkdaşları):

_____ _____
(soyadı, adı) (imza)

_____ _____
(soyadı, adı) (imza)

Qeyd. _____

Aktı tərtib edən şəxs (şəxslər):

_____ _____
(soyadı, adı) (imza)

_____ _____
(soyadı, adı) (imza)

Diaqnostika aparılan qurumun məsul əməkdaşı (əməkdaşları):

_____ _____
(soyadı, adı) (imza)

_____ _____
(soyadı, adı) (imza)

Qeyd. Diaqnostika aparılan qurumun məsul əməkdaşının aktın məzmunu barədə öz mülahizələrini təqdim etmək, habelə aktı imzalamaqdan imtina etməsinin səbəblərini göstərmək hüquqları vardır. Aktı imzalamaqdan imtina edildikdə, bu barədə müvafiq qeydlər aparılır:

_____
_____

Diaqnostika aparılan qurumun məsul əməkdaşına aktın surəti verilir.
"Aktın surətini aldım" _____
(qurumun məsul əməkdaşının soyadı, adı, vəzifəsi, imzası)

_____