

**İmtiyazlı girişlərin idarə edilməsi sistemi (PAM)**

**Mündəricat**

[**1.** **Məqsəd** 3](#_Toc121230934)

[**2.** **Dəstəklənən Platformalar** 3](#_Toc121230935)

[**3.** **Ümumi Platforma Tələbləri** 3](#_Toc121230936)

[**4.** **Tətbiqin interfeysi** 4](#_Toc121230937)

[**5.** **Sistem Arxitekturası** 4](#_Toc121230938)

[**6.** **Məhsulun Təhlükəsizliyi** 4](#_Toc121230939)

[**7.** **İnteqrasiya** 5](#_Toc121230940)

[**8.** **Hesabat - Audit - Qiymətləndirmə** 5](#_Toc121230941)

[**9.** **İş axınına (work flow) dəstək** 5](#_Toc121230942)

[**11.** **İmtiyazlı Fəaliyyətin Monitorinqi / Video Qeydiyyat** 6](#_Toc121230943)

[**12.** **Təhdid Anzlizi** 7](#_Toc121230944)

1. **Məqsəd**

IT infrastrukturda istifadə olunan serverləri idarə edən 30 sistem administratorunun və 120 kənar istifadəçinin limitsiz sayda şifrələrini idarə edə bilmək üçün İmtiyazlı Şifrə İdarəetmə proqram təminatı və İmtiyazlı Sessiya İdarəetmə / Fəaliyyət Monitorinqini həyata keçirəcək proqram təminatı satın alınacaq.

Tenderdə iştirak edən şirkətlər öz təkliflərinə Fəlakətdən Bərpa (DR-HA) modulu və proqram təminatının bir sınaq mühiti üçün lisenziyaları əlavə etməlidirlər.

Təklif bir və üç illik lisenziya ilə təqdim edilməlidir. Lisenziyalar abunə (subscription) və daimi (perpetual) kimi təklif oluna bilər. Lisenziya yuxarıda qeyd edilən istifadəçinin sayına və ya bu saya uyğun olaraq vendor tərəfindən tövsiyə edilən sessiya sayına əsasən təklif oluna bilinər.

1. **Dəstəklənən Platformalar**
* Əməliyyat sistemləri

- Microsoft Windows

- Unix və Linux əsaslı sistemlər

* Virtual Serverlər (VMWare ESX/ESXi)
* Verilənlər bazası serverləri (Oracle, Microsoft SQL Server, PostgreSQL, DB2, MySQL,)
* Şəbəkə avadanlıqları (Cisco, HP, Palo Alto)
* Təhlükəsizlik avadanlıqları (Check Point, Cisco, Fortinet, Palo Alto)
* SaaS / Vebsaytlar
1. **Ümumi Platforma Tələbləri**
2. Server və müştəri maşınlarında lokal administrator hesablarını idarə edə bilməlidir.
3. İdarə olunacaq hesabların sayı ilə bağlı heç bir limit və/ya məhdudiyyət olmamalıdır.
4. Şifrəsi idarə olunacaq sistemlərdə heç bir komponentin quraşdırılmasına ehtiyac olmamalıdır (Agentsiz arxitektura).
5. İdarə olunacaq hesablar sistemə kollektiv şəkildə daxil edilə bilməlidir.
6. İstifadə olunacaq həll VMware, Microsoft Active Directory, Unix/Linux əsaslı sistemləri müəyyən edilmiş vaxtda və ya avtomatik skan edərək onların üzərində olan imtiyazlı hesabları sistemə daxil etməli və vasitəçi hesab ilə avtomatik idarə etməyə başlamalıdır.
7. Avtomatik aşkarlama prosesi zamanı tapılan hesablar, Servis, vaxta görə planlaşdırılmış tapşırıq və s. içərisində istifadə olunursa, o zaman bu məlumatlar da avtomatik olaraq müəyyən edilə bilməlidir. Yeni əlavə edilmiş və ya çıxarılan sistemlər aşkar edilməlidir. Yeni əlavə edilmiş və ya çıxarılmış sistemlərin hesablarını idarə etməyə başlamaq üçün avtomatik qaydalar tətbiq edilməlidir.
8. Fərqli hesablara fərqli siyasətlər tətbiq edilməlidir.
9. Hesabların şifrələrinin doğruluğu mütəmadi olaraq yoxlanılmalı və hesabat verilməlidir.
10. Məhsulun hesab məlumatlarından (istifadəçi adı və şifrə) başqa həssas məlumatların saxlanması üçün də istifadə oluna bilməsi xüsusiyyətinə üstünlük verilir.
11. Windows Server/Desktop/Laptop Platformalarında servis hesabları yeniləndikdə onların istifadə olunduğu xidmət, vaxta görə planlaşdırılmış tapşırıqlar və s. içərisindəki şifrələrin avtomatik olaraq yenilənməsi təmin olunmalıdır.
12. Təklif olunan məhsulun şifrələri və həssas məlumatları necə saxladığı və görülən təhlükəsizlik tədbirləri ətraflı izah edilməlidir.

# **Tətbiqin interfeysi**

1. Vahid İnterfeysli Mərkəzi İdarəetmə olmalıdır.
2. Əgər məhsul arxa planda verilənlər bazasından istifadə edirsə, bu verilənlər bazası məhsul tərəfindən avtomatik idarə olunmalıdır. Əgər standart verilənlər bazası istifadə olunacaqsa, bu verilənlər bazası təhlükəsizlik baxımından ancaq bu məhsul üçün istifadə olunmalıdır və eyni zamanda başqa məhsul üçün istifadə oluna bilməz. İddiaçı şirkət bu verilənlər bazasının Fəlakətdən Bərpa Mərkəzi və lazım olduqda sinxronizasiya (replikasiya) lisenziyaları ilə birlikdə texniki dəstək müddətində lisenziya dəstəyini təmin etməli və quruma lisenziyaları təqdim etməlidir.
3. Təklif olunan məhsul hər bir Sistem Administratoruna yalnız özünün idarə etdiyi sistemlərdə hesabları və şifrələri görməyə imkan verməlidir.
4. Microsoft Active Directory və ya hər hansı LDAP əsaslı kataloq ilə inteqrasiya oluna bilməlidir. Eyni şəkildə, bu kataloqlardakı istifadəçi qrupları sayəsində avtomatik icazələndirmələr mümkün olmalıdır.
5. Tələb olunduqda, hesablarda Toplu Əməliyyatlar həyata keçirmək mümkün olmalıdır.
6. İstifadəçilərə vaxt, IP ünvanı kimi parametrlərə görə giriş məhdudiyyətləri tətbiq oluna bilməlidir.
7. Tələb olunduqda daha məhdud imkanlara malik olan kənar istifadəçilər lisenziyalaşdırıla bilinməlidir. Bu istifadəçilər yalnız seyfdəki hesablara daxil ola bilməli və şifrələri görmədən bu hesablarla hədəf sistemlərə qoşula bilməlidirlər. Bu istifadəçilərin şifrələri görmək və dəyişdirmək icazəsinə malik olmalarına ehtiyac yoxdur.
8. **Sistem Arxitekturası**
9. Virtual Server (VM) dəstəyi olmalıdır. Proqram təminatı virtual serverdə işləyən əməliyyat sistemlərində quraşdırıla bilməlidir. Bu yolla server sistem avadanlığı qurumun ehtiyaclarına uyğun olaraq dəyişdirilə biləcək.
10. Təklif olunan həll, qurumun tələbatının artmasına uyğun olaraq lisenziyanı artırmaqla genişlənə bilməlidir.
11. Məhsulda Fəlakətdən Bərpası (DR) və Redundancy (HA) dəstəyi olmalıdır.
12. Fərqli Seqmentlərdə Səpələnmiş Strukturlar Vahid Mərkəzdən İdarə edilməlidir.
13. Digital Vault API dəstəyinə malik olmalıdır. API dəstəyi ətraflı izah edilməlidir. API dəstəyi üçün Lisenziya tələb olunursa, bu lisenziya təmin edilməlidir. İstifadəçi icazəsi, hesabların əlavə edilməsi/çıxarılması/yenilənməsi, tətbiq hesablarının əlavə edilməsi/səlahiyyətləndirilməsi/yenilənməsi, şifrələrin dəyişdirilməsi kimi funksiyalar API-larla təmin edilməlidir.
14. **Məhsulun Təhlükəsizliyi**
15. Bütün Sistem komponentlərinin bir-biri ilə əlaqəsi şifrələnmiş olmalıdır.
16. Şifrələrın saxlandığı yer təcrid olunmuş “Təhlükəsiz Zona” olmalıdır.
17. Şifrələrin saxlandığı sistemi idarə edən şəxslərin saxlanılan şifrələrə çıxışı olmamalıdır.
18. Video qeydiyyat, jurnallar, qaydalar və s. şifrələnmiş və təhlükəsiz şəkildə saxlanmalıdır. Lazım gələrsə, video qeydiyyatı xarici yerdə saxlanılması mümkün olmalıdır.
19. Məhsula girişlər iki addımlı autentifikasiya sistemləri ilə inteqrasiya edə bilməlidirlər. (two-factor authentication). Məhsul özündə 2 fərqli autentifikasiya sistemindən (məsələn, Windows Authentication + Radius və/və ya lokal istifadəçi bazası) istifadə etməklə daha təhlükəsiz giriş təmin etməlidir.
20. Fövqəladə hal zamanı şifrələrin cari vəziyyətinin qorunmasının necə təmin olunduğu izah olunmalıdır.
21. Fövqəladə hal zamanı ehtiyat nüsxədən bərpa ssenarisi izah olunmalıdır.
22. **İnteqrasiya**
23. LDAP, Windows SSO, PKI, RADIUS, SAML, RSA kimi Doğrulama Metodları ilə uyğun olmalıdır.
24. Böyük Strukturda LDAP/AD-də çox yönlü sorğu və nəzarət mümkün olmalıdır. (global groups, multiple forests və s.)
25. Log toplama və korrelyasiya (SIEM) məhsulları ilə inteqrasiya imkanı olmalıdır. Məhsul, özünün dəstəklədiyi formatında eyni anda birdən çox və müxtəlif SIEM sistemlərinə log göndərə bilməlidir.
26. Identity Management Sistemi (One Identity) ilə inteqrasiya edə bilməlidir .
27. Qualys Vulnerability Management məhsullu ilə inteqrasiya imkanı.
28. **Hesabat - Audit - Qiymətləndirmə**
29. İstənilən vaxtda və ya müəyyən vaxt aralıqlarında hesabat almaq mümkün olmalıdır.
30. Hesabatlar ən azı aşağıdakı məlumatları ehtiva etməlidir:

• İmtiyazlı istifadəçi hesabatları

• İstifadəçi fəaliyyətləri

• İmtiyazlı Hesab inventarı

• Tətbiq inventarı

• Uyğunluq Hesabatı

1. Hesabat nəticələri ən azı Excel və ya CSV formatlarını dəstəkləməlidir.
2. Sistem Girişlərinin hərəkətləri barədə məlumat verilməlidir.
3. İstifadəçilər tərəfindən Şifrələrin Tələb Olunduğu haqqında hesabat verilməlidir
4. Dəyişdirilə bilməyən şifrələr haqqında hesabat verilməsi mümkün olmalıdır.
5. Dəyişdirilmiş şifrələr haqqında hesabat verilməsi mümkün olmalıdır.
6. Siyasətə əməl etməyən istifadəçilər barədə məlumat verilməlidir
7. Şifrələrin Vəziyyəti haqqında hesabat verilməlidir
8. Hesabatlar fərdiləşdirilə və ya əvvəlcədən şablon kimi yaradıla bilər.
9. Məlumat ixrac edilə bilən (export) olmalıdır. (crystal reports və s.)
10. Hesabatları görəcək şəxslər məhdudlaşdırılmalıdır.
11. **İş axınına (work flow) dəstək**
12. Təsdiq mexanizmi və birdən çox Avtorizasiya Dəstəyi olmalıdır. Şifrə giriş Sorğu/Təsdiqdən sonra mümkün olmalıdır.
13. İstifadəçilər, şifrədən istifadə tələbini gələcək bir tarix ya da zaman aralığı üçün də təsdiqə göndərə / istəyə bilməlidirilər.
14. Müəyyən edilmiş istifadəçilər təsdiq mexanizminə ehtiyac olmadan imtiyazlı hesablara daxil ola bilməlidirlər.
15. Veb interfeysi mobil cihaz dəstəyinə malik olmalıdır. (iPhone, Android və s.)
16. Tələb olunduqda, təsdiqləmə prosesindən sonra istifadəçilərə hədəf sistemdə müvəqqəti Lokal Administrator hüquqları verilməli və istifadəçi birbaşa idarəçi hüquqları ilə hədəf sistemlə uzaqdan və ya lokal əlaqə qura bilməlidir. Lokal idarəetmə hüququ təyin olunan müddətin sonunda avtomatik olaraq silinməlidir.
17. İş axını izlənilə və bu barədə hesabat verilməsi mümkün olmalıdır.
18. **Sistem Şifrə İdarəetmə / Səlahiyyətli Hesab İdarəetmə**
19. Şifrələr müəyyən vaxt intervallarında avtomatik olaraq dəyişdirilə bilməlidir.
20. Şifrələr birdəfəlik istifadə olunmalıdır. O, qrup, platforma və ya sistem əsasında tətbiq edilməlidir.
21. Şifrələr əllə, siyasətdən asılı olaraq və ya təsdiqləmə xətasından sonra avtomatik dəyişdirilə bilməlidir.
22. Hesablara təsadüfi şifrələr təyin etmək mümkün olmalıdır və bu hallarda baş verməlidir:

• Hesab Meneceri tərəfindən tələb olunduqda

• Siyasətdən asılı olaraq, zamanı gəldikdə

• İstifadə müddəti bitdikdə

1. Şifrələr hədəf sistemdə avtomatik yoxlanılmalıdır.
2. Şifrələr vaxtaşırı yoxlanılmalı və təsdiq olunmayan şifrələr avtomatik olaraq xəbərdarlıq verməlidir
3. Şifrələrın yoxlanılması və ya istifadə edilməməsi halında, onlar sinxronizasiya hesabı ilə avtomatik olaraq yenidən təyin oluna bilməlidirlər.
4. Təyin ediləcək Şifrələrin uzunluğu, mürəkkəbliyi və s. xüsusiyyətləri bütün hədəf cihazları üçün müəyyən edilə bilməlidir
5. Şifrələrin geri versiyalarını sistemdə saxlamaq və lazım gəldikdə onlara daxil olmaq mümkün olmalıdır.
6. Avtomatik şifrə dəyişikliyi əməliyyatlarında istifadə olunan şifrə siyasətləri manual dəyişikliklər edərkən də İstifadə edilə bilməlidir
7. Şifrə dəyişdirilərkən əvvəllər istifadə edilmiş şifrələrin yenidən istifadəsinin arşısı alınmalıdır
8. Hər bir hədəf cihaz üçün fərqli şifrə yarada bilməlidir.
9. Hədəf cihaz tipləri eyni olsa belə, fərqli siyasətlər tətbiq edilməlidir
10. Şifrələrin idarə edilməsi və sessiyanın qeydiyyatı üçün vahid siyasət tətbiq etməyi bacarmalıdır.
11. Birdəfəlik Şifrə yaratmaq mümkün olmalıdır.
12. Fəaliyyətlər barədə e-poçt vasitəsilə xəbərdarlıq göndərə bilməlidir
13. Şifrə bloklaması mümkün olmalıdır. Məs. bir istifadəçi şifrədən istifadə etdikdə digər istifadəçilərin həmin şifrədən istifadəsinin qarşısı alınmalıdır.
14. Eyni şifrəni gözləyən istifadəçiyə şifrənin artıq istifadəyə götürülə bilməsi haqqında interfeysdən məlumat verilməlidir.
15. Məhsul, şifrənin müddətinin bitəcəyi barədə məlumatı vaxtından əvvəl istifadəçi qrupuna ötürə bilməlidir (e-mail).
16. Eyni hesabın şifrəsinin eyni anda birdən çox istifadəçi tərəfindən istifadə edilməsinin qarşısını ala bilməlidir.
17. Hədəf sistemə şifrəni görməyə və ya daxil etməyə ehtiyac olmadan qoşulmaq mümkün olmalıdır.
18. Hədəf sistemə giriş və ya hədəf sistem dəyişikliyi, şifrə istifadəsi, şifrədən istifadə sorğusu haqqında e-poçt göndərə bilməlidir.
19. Microsoft servis və planlaşdırılmış tapşırıqların içərisindəki şifrələrin toplanması və yenilənməsi imkanları haqqında məlumat verilməlidir.
20. Faylda mətn əsaslı şifrələrın toplanması və yenilənməsi imkanları haqqında məlumat verilməlidir.
21. Bölünmüş şifrə (split password) saxlamaq imkanı olmalıdır. 2 fərqli şəxs və ya komanda şifrənin özlərinə aid hissəsini görə və idarə edə bilməlidir.
22. Birgə hesablardan eyni vaxtda birdən çox şəxs istifadə edə bilər və ya onların eyni vaxtda birdən çox şəxs tərəfindən istifadəsinin qarşısı alına bilər.
23. Qrup sistem üçün eyni şifrə yaratmaq mümkün olmalıdır.
24. Linux/Unix əməliyyat sistemlərində istifadə edilən SSH (Key) açarları eyni həll üzərində səlahiyyətli hesablarla birlikdə saxlanmalı və idarə edilməlidir.
25. Təklif olunan həllin SSH (key) açarlarının zəiflikləri haqqında məlumatı bildirməsi üstünlük təşkil edir.
26. **İmtiyazlı Fəaliyyətin Monitorinqi / Video Qeydiyyat**

Bu xüsusiyyət ilə hədəf sistemlərə aid tətbiqləri görmədən hədəf qurum daxilində şəbəkə izolyasiyası, hədəf serverlərə təhlükəsiz giriş, sessiya fəaliyyətlərinin qeydi və proqram istifadəçilərinin Şifrə məlumatları işlədilə bilər. Bunu təmin edəcək sistem aşağıdakı xüsusiyyətlərə malik olmalıdır;

1. Məhsul Hədəf Sistemində agent quraşdırılmadan işləməlidir.
2. Sessiyanın Video qeydiyyatı, Hədəf Kompüterində Performansın azalmasına səbəb olmamalıdır.
3. Məhsul, Hədəf mənbəyində seanslara nəzarət etmək üçün mövcud şəbəkə strukturunun dəyişilməsinə ehtiyac yaratmamalıdır.
4. Qeydlər Şifrələnmiş Təhlükəsiz yerdə Saxlanılmalıdır.
5. Hesabların idarə edilməsi, sessiyalara nəzarət və monitorinq vahid interfeysdən mümkün olmalıdır.
6. Video qeydiyyatla yanaşı, müəyyən protokollar üçün mətn əsaslı yazılar da olmalı, bu yazılarda axtarış edilməsi və müvafiq video qeydiyyatın müvafiq hissəsinin izlənilməsi mümkün olmalıdır.
7. Video qeydiyyatlarda, istifadə edilən əmrlər arasında mətn əsaslı axtarış mümkün olmalıdır. (RDP, Unix, Database və s. kimi Əmr və sorğular)
8. Məhsul şəbəkə izolyasiyasını təmin etmək məqsədilə təhlükəsiz proksi kimi işləməyi bacarmalıdır.
9. Sessiyaları qeydiyyat zamanı real vaxt rejimində izləmək mümkün olmalıdır.
10. Sessiyaların Qeydiyyatının administrator tərəfindən sonlandırılması mümkün olmalıdır.
11. Sessiya qeydinə baxarkən, qeyri-fəaliyyət hissələri avtomatik olaraq atlanmalıdır (Skip idle).
12. Məhsul istənilən proqramı avtomatik işə sala və hədəf sistemə daxil ola bilməlidir. Həll ilə birlikdə gələn tətbiq dəstəyi siyahıya alınmalıdır. Əlavə avtomatlaşdırma komponenti ilə hər hansı bir xüsusi müştəri proqramı və ya veb tətbiqi avtomatlaşdırma interfeysi ilə avtomatik olaraq daxil edilməlidir. Bunun üçün çevik API və s. təmin edilməlidir. Beləliklə, qurum istehsalçının yeni versiyanın inkişaf prosesini gözləmədən daxili tətbiqləri sistemə inteqrasiya edə bilməlidir.
13. Təklif olunan həll yüksək əlçatanlılığı dəstəkləməlidir. Yüksək əlçatanlıq (HA) həlli haqqında ətraflı məlumat verilməlidir.
14. Təklif olunan həllin agentlər olmadan (hədəf sistemdə agentlər quraşdırmadan) əmr qadağası xüsusiyyətlərinə malik olması üstünlük təşkil edir.
15. Təklif olunan həllin agentlər olmadan (hədəf sistemdə agent quraşdırmadan) Active Directory istifadəçiləri ilə Linux sistemlərə lokal istifadəçi kimi (AD bridge) qoşulma imkanına üstünlük verilir.
16. Təklif olunan həll CLI əmrlərində daxil edilmiş bütün simvolları enter düyməsini basmadan qeydiyyata ala bilməlidir.
17. Sessiyanın idarə edilməsi və qeydiyyatı bütün protokolları əhatə etməlidir.
18. İstifadəçilər HTML5 dəstəkləyən bələdçı vasitəsilə sessiya aça bilməlidirlər.
19. Uzaq sistemlərə SSH bağlantılarında müştəri və ya server tərəfində agent quraşdırmadan əmrləri blok etmək imkanı olmalıdır.
20. SSH sessiya log-ları backspaces, arrows, tabs, command history kimi yan keçid üsullarının qarşısının alınmasını dəstəkləməlidir.
21. **Təhdid Anzlizi**

Həll sistemlə inteqrasiya olunmuş imtiyazlı hesablar üçün təhdid analizi apara bilməlidir. Təhdidlərin analizi modulu aşağıdakı imkanlara malik olmalıdır:

* Qabaqcıl istehsalçıların SIEM sistemləri ilə inteqrasiya edərək imtiyazlı hesabların sistemlər üzərindəki istifadəsini izləməyi bacarmalıdır.
* İmtiyazlı hesabların idarə edilməsi zamanı istifadə vərdişlərini müəyyənləşdirə bilməlidir.
* Sistem tərəfindən idarə olunmayan hesablar aşkar edilməli və həyəcan siqnalı yaradılmalıdır.
* Riskli seansların qeydə alınması riskə görə prioritetləşdirilməli və ya sıralanmalıdır.
* Riskli fəaliyyətlər tələb olunduqda qurum üçün xüsusi olaraq müəyyən edilə bilməli və risk balı və fəaliyyət müəyyən edilməlidir. Qaydalar maşın (hostname), İmtiyazlı Hesab və İstifadəçi üçün fərdiləşdirilə bilməlidir.
* Şübhəli fəaliyyət aşkar edildikdə həyəcan siqnalı yarada bilməli və imtiyazlı hesabı qorumaq üçün Şifrə rotasiyası təmin edilməlidir.
1. **Çox faktorlu İstifadəçi Doğrulaması (MFA)**
2. Active Directory istifadəçiləri, Integrated Windows Authentication ilə həll interfeysinə və inteqrasiya olunmuş proqramlara daxil ola bilməlidirlər.
3. İstifadəçilərə öz iş təsvirlərinə uyğun olaraq rol əsaslı icazələr təyin oluna bilməlidir.
4. Rol (qrup) üzvlükləri statik və dinamik olaraq təyin edilə bilməlidir.
5. Həll interfeysinə daxil olarkən, OATH əsaslı metodlarla (Google Authenticator, RSA/Gemalto/SafeNet və s. kimi fiziki tokenlər) çox addımlı doğrulama mümkün olmalıdır.
6. İstifadəçilər, rollar kimi digər resurslarda REST API vasitəsilə CRUD əməliyyatlarını yerinə yetirə bilməlidirlər.
7. Həll tərəfindən təmin edilən SSO portalına masaüstü brauzerlər, smartfonlar və ya planşetlər vasitəsilə daxil olmaq mümkün olmalıdır.
8. iOS və Android əməliyyat sistemləri üçün mobil proqram təmin edilməlidir.
9. İki addımlı doğrulama üçün E-Mail ilə OTP dəstəklənməlidir.
10. İki addımlı doğrulama dəstəklənən inteqrasiyalar üçün (məsələn, SAML, Web portal) QR kodu ilə doğrulama dəstəklənməlidir. Tələb olunduqda, QR kodu ilə şifrəsiz (passwordless) doğrulama üçün istifadə oluna bilməlidir.
11. **Texniki dəstək**

Aşağıdakı dəstək xidmətləri və xidmət səviyyəsi müqavilələri (SLA) minimum olaraq tələb olunur:

* 24X7 standart dəstək əhatəsi
* Əhəmiyyətlik dərəcəsi 1 olan biznesə kritik təsiri olan problemlər üçün 2 saat ərzində cavablandırma
* Əhəmiyyətlik dərəcəsi 2 olan biznesə əhmiyətli təsiri olan problemlər üçün 4 saat ərzində cavablandırma
* Əhəmiyyətlik dərəcəsi 3 olan minimal biznes təsirləri olan problem üçün növbəti iş gününün sonuna gədər cavablandırmaq
1. **Planlanma, Quraşdırılma, İşci heyəti, təlim.**

Bank PAM həllinin həyata keçirilməsinə kömək etmək üçün konsaltinq resurslarını tələb edir və tenderdə iştirak edən şirkətlərdən quraşdırılma xidmətləri ilə bağlı aşağıdakılara cavab verməsini istəyir:

• Yol Xəritəsi– Bank üçün təklif olunan PAM həllinin tətbiqi yol xəritəsini və mərhələlərini təsvir edən illüstrasiya. Tenderdə iştirak edən şirkət hər bir mərhələni bölməli və həyata keçirilən icranın təsvirini təqdim etməlidir

• Təxmini vaxt qrafiki –bütün mərhələlər üçün təxmini vaxt qrafiklərinin icmalını təqdim edən cədvəl və ya qrafik təsvir

• Təxmini iş həcmi (Level of Effort/ Staffing Plan) – Tenderdə iştirak edən şirkət və Bankın resursları üçün tələb olunan iş həcmini təqdim edin – tələb olunan Bank resursunun növünü göstərin (Sistem Administratoru, Şəbəkə Administratoru və sairə) və hər bir resurs və hər bir tapşırıq üçün nəzərdə tutulan vaxtın miqdarı

• Təfərrüatlı təlim planı – layihədə bank tərəfindən iştirak edəcək və sistemin inzibatçılığını həyata keçirdəcək əməkdaşlar üçün

• Sistem administratorları və son istifadəçilər üçün metodologiya sənədləri/istifadəçi təlimatlarını hazırlamaq