



ՀԵՏԱՔՐՔՐՈՒԹՅԱՆ ՀԱՐՑՈՒՄ

ՓԼ/ԱՖ և պատժամիջոցների համապատասխանության ռիսկերի գնահատման և մոնիթորինգի ավտոմատացման համակարգի գնման ընթացակարգի կազմակերպման

1. Հարցման նպատակը

Հայաստանի Հանրապետության Կենտրոնական բանկը (ՀՀ ԿԲ) կազմակերպում է սույն հարցումը՝ առաջիկայում նախատեսվող մրցույթի շրջանակներում «ՓԼ/ԱՖ և պատժամիջոցների համապատասխանության ռիսկերի գնահատման և մոնիթորինգի ավտոմատացման համակարգի» գնման ընթացակարգի վերաբերյալ հնարավոր մատակարարների հետաքրքրությունը և կառուցողական արձագանքը ստանալու նպատակով:

Կից Տեխնիկական Առաջադրանքի (ToR) նախնական տարբերակում սահմանված են ակնկալվող տեխնիկական, ֆունկցիոնալ և ներդրման պահանջները: Պաշտոնական մրցույթային ընթացակարգ նախաձեռնելուց առաջ այս հետաքրքրության հարցումը (REol) կազմակերպվում է հետևյալ նպատակով.

- առաջիկա մրցույթի հնարավոր մասնակիցներին բացահայտելու, և
- Տեխնիկական Առաջադրանքի նախնական տարբերակի վերաբերյալ կարծիքներ հավաքելու, ներառյալ իրագործելիությունը, հստակությունը, իրատեսականությունն ու ամբողջականությունը, ինչպես նաև և իրականացման ընթացքում հնարավոր սահմանափակումներն ու ռիսկերը:

Այս գործընթացը ՀՀ ԿԲ-ին հնարավորություն կտա լավարկել Տեխնիկական Առաջադրանքը և մրցույթային ընթացակարգի կազմակերպումը՝ ապահովելով մրցակցային և արդյունավետ գործընթացի իրականացում:

***Սույն հետաքրքրության հարցումը մրցույթի հրավեր չէ, այն իրականացվում է նմանադրիպ համակարգերի մատակարարների հետաքրքրությունը գնահատելու համար:**



Հետաքրքրություն հայտնաբերող մասնակիցները կարող են մասնակցել առաջիկա բաց մրցույթին և հայտեր ներկայացնել:

2. Նախագծի ամփոփ նկարագրությունը.

Կից ներկայացված տեխնիկական առաջադրանքը ներառում է հետևյալ հիմնական պահանջները՝

- Ֆինանսական հաստատություններից տվյալների հավաքագրման ավտոմատացում հարցումների կամ համակարգային ինտեգրացիաների միջոցով,
 - անհատականացվող ռիսկի մոդելներ (հատուկ, վերահսկողության/ որակի կառավարման, մնացորդային ռիսկի),
 - ինտեգրացիա արտաքին համակարգերի/տվյալների բազաներին (ETL, API-ներ),
 - տեղեկատվական վահանակ, շեղումների հայտնաբերում, միտումների վերլուծություն, մեքենայական ուսուցման հնարավորություններ,
 - մուտքի վերահսկողություն ըստ դերի, գործողությունների գրանցում և բազմագործոն նույնականացում,
 - ամբողջությամբ տեղային (on-premise) տեղակայում (առանց ամպային լուծումների),
 - համապատասխանություն միջազգային ստանդարտներին (օրինակ՝ ISO 27001, FATF ուղեցույցներ),
 - բազմափուլ տվյալների հավաքագրման աջակցություն բազմաթիվ վերահսկվող ոլորտներում:
-

3. Մասնակիցներին ուղղված հարցում.

ՀՀ ԿԲ-ն հրավիրում է բոլոր հետաքրքրված կազմակերպություններին.

- հայտնել մրցույթի մասնակցության հետաքրքրության մասին,
- ուսումնասիրել նախնական Տեխնիկական Առաջադրանքը և
- ներկայացնել մեկնաբանություններ, առաջարկություններ կամ դիտողություններ՝
 - պահանջների տեխնիկական իրագործելիության,
 - իրականացման կամ ներդրման ընթացքում հնարավոր ռիսկերի,
 - բացակայող դրույթների կամ չափազանցված պահանջների,



- լիցենզավորման, տեղայնացման կամ ինտեգրման հետ կապված հնարավոր խնդիրների, ինչպես նաև առաջարկվող գնահատման չափանիշների (դրանց սահմանափակող կամ ոչ հստակ լինելու դեպքում) վերաբերյալ:

Ձեր դիտարկումները կարևոր են արդար, ընդգրկուն և իրագործելի մրցույթ կազմակերպելու համար:

4. Մրցույթին մասնակցության պահանջները և որակավորումը

Գնումների մասին ՀՀ օրենքի համաձայն՝ առաջիկա մրցույթին մասնակցության համար կարող են կիրառվել հետևյալ որակավորման պայմանները.

Մրցույթին չեն կարող մասնակցել հետևյալ անձինք/կազմակերպությունները.

- դատական կարգով ճանաչվել են սնանկ,
 - Վերջին 5 տարիների ընթացքում դատապարտված են եղել ահաբեկչության ֆինանսավորման, երեխայի շահագործման կամ մարդկային թրաֆիքինգ ներառող հանցագործության, հանցավոր համագործակցություն ստեղծելու կամ դրան մասնակցելու, կաշառք ստանալու, կաշառք տալու կամ կաշառքի միջնորդության և օրենքով նախատեսված տնտեսական գործունեության դեմ ուղղված հանցագործությունների համար, բացառությամբ այն դեպքերի, երբ դատվածությունը օրենքով սահմանված կարգով մարված կամ վերացված է,
 - որոնց վերաբերյալ գնումների ոլորտում հակամրցակցային համաձայնության, գերիշխող դիրքի չարաշահման կամ անբարեխիղճ մրցակցության համար պատասխանատվություն սահմանող վարչական ակտը վերջին երեք տարվա ընթացքում դարձել է անբողոքարկելի, իսկ բողոքարկված լինելու դեպքում թողնվել է անփոփոխ,
 - Ներառված են Եվրասիական տնտեսական միությանն անդամակցող երկրների գնումների մասին օրենսդրության համաձայն հրապարակված գնումների գործընթացին մասնակցելու իրավունք չունեցող մասնակիցների ցուցակում,
 - գնումների գործընթացին մասնակցելու իրավունք չունեցող մասնակիցների ցուցակում:
- Փոխկապակցված անձինք կամ կազմակերպությունները, այդ թվում՝ հիմնադրված նույն անձանց կողմից կամ որոնցում վերջիններս ունեն 50%-ից ավելի բաժնեմաս, չեն կարող մասնակցել միաժամանակ, բացառությամբ համատեղ ձեռնարկության (կոնսորցիումի) ձևաչափով:

Մրցույթի պայմաններում նախատեսվում է.



- Հայտի ապահովում՝ գնային առաջարկի մոտ 5%-ի չափով, ներկայացվում է կանխիկ կամ բանկային երաշխիքի տեսքով,
 - Պայմանագրի ապահովում՝ պայմանագրի գնի մոտ 10%-ի չափով՝ կանխիկ կամ բանկային երաշխիքի տեսքով:
-

5. Ներկայացման պահանջները

Խնդրում ենք ներկայացնել.

1. Հետաքրքրության հայտ-նամակ՝ հաստատելու Ձեր պատրաստակամությունը մասնակցելու մրցույթին:
2. Տեխնիկական առաջադրանքի վերաբերյալ ցանկացած կարծիք, դիտարկում կամ առաջարկ:
3. Աշխատանքների կատարման համար կանխատեսվող ժամկետները:
4. Կոնտակտային տվյալներ (կազմակերպության անվանում, պատասխանատու անձ, էլեկտրոնային փոստ, հեռախոսահամար) սույն հարցման հետ կապված պարզաբանումների, ինչպես նաև հետագայում մրցույթի հրավերը ստանալու համար:

****Այս փուլում անհրաժեշտ է ներկայացնել հիմնավորող փաստաթղթեր, ֆինանսական առաջարկներ կամ ընկերության վկայականներ:***

6. Ներկայացման կարգը

- ✉ Խնդրում ենք ուղարկել պատասխան հայտը մինչև 2025թ. սեպտեմբերի 05-ը,
 - ✉ Էլ. փոստ՝ procurement@cba.am, CC՝ edgar.begrakyan@cba.am
 - Թեմա՝ Expression of Interest – AML/CFT System
-

7. Գաղտնիություն և չպարտավորեցնող բնույթ.

Սույն հետաքրքրության հարցմանը մասնակցությունը պարտավորեցնող չէ և չի ենթադրում հայտի պարտադիր ներկայացում ապագա մրցույթում: Բոլոր արձագանքները կդիտարկվեն



գաղտնի և կօգտագործվեն միայն ներքին պլանավորման ու մրցույթի փաստաթղթերի
բարելավման նպատակով:

8. Պարզաբանումների վերաբերյալ Կոնտակտային տեղեկատվություն

Տեխնիկական առաջադրանքի նախնական տարբերակի վերաբերյալ հարցերի դեպքում
դիմել՝

Էդգար Բեգրակյանին

Ֆինանսական վերահսկողության և լիցենզավորման դեպարտամենտի կոորդինատոր

Հայաստանի Հանրապետության Կենտրոնական բանկ

✉ edgar.begrakyan@cba.am

☎ +374 10 592 592

**Հրապարակվել է՝
2025թ.-ի օգոստոսի 20-ին**

Սիրան Եգանյան

Գնումների համակարգման ծառայության ղեկավար
Հայաստանի Հանրապետության Կենտրոնական բանկ

✉ siran.yeganyan@cba.am

☎ +374 10 592 592



Հավելված

«ՓԼ/ԱՖ և ՊԱՏԺԱՄԻՋՈՑՆԵՐԻ ՀԱՄԱՊԱՏԱՍԽԱՆՈՒԹՅԱՆ ՌԻՍԿԵՐԻ ԳՆԱՀԱՏՄԱՆ և ՄՈՆԻԹՈՐԻՆԳԻ ԻՐԱԿԱՆԱՑՄԱՆ ԱՎՏՈՄԱՏԱՑՈՒՄ» ՆԱԽԱԳԾԻ ՇՐՋԱՆԱԿՆԵՐՈՒՄ ՀԱՄԱԿԱՐԳԻ ՁԵՌՔԲԵՐՄԱՆ ՏԵԽՆԻԿԱԿԱՆ ԱՌԱՋԱԴՐԱՆՔ

ՏԵԽՆԻԿԱԿԱՆ և ՖՈՒՆԿՑԻՈՆԱԼ ԲՆՈՒԹԱԳՐԵՐԸ

ՆԵՐԱԾՈՒԹՅՈՒՆ

Հայաստանի Հանրապետության կենտրոնական բանկը (այսուհետ՝ նաև Բանկ կամ ՀՀ ԿԲ) պետական գործառնություններով լիազորված իրավաբանական անձ է: Բանկի առաջնային նպատակներն են՝ ապահովել գների կայունությունը և ֆինանսական կայունությունը՝ համաձայն Հայաստանի Հանրապետության Սահմանադրության և «ՀՀ Կենտրոնական բանկի մասին» ՀՀ օրենքի: ՀՀ ԿԲ-ն հաստատում և իրականացնում է դրամավարկային քաղաքականության ծրագիրը, կարգավորում և վերահսկում է ֆինանսական համակարգը, վերահսկողություն է իրականացնում վճարային համակարգի նկատմամբ, ապահովում է ազգային արժույթի թողարկումը և դրա շրջանառությունը, պայքարում փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ, կառավարում է Հայաստանի Հանրապետության միջազգային պահուստները և այլն:

Այս նախագիծը նպատակ ունի զգալիորեն բարձրացնել Բանկի կարողությունները փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարում և միջազգային պատժամիջոցների համապատասխանության ապահովման հարցերում՝ կիրառելով վերահսկողական տեխնոլոգիաներ (SupTech):



ՆՊԱՏԱԿԸ

Սույն հրավերի նպատակն է գտնել մատակարար, որը կկարողանա տրամադրել համալիր ծրագրային լուծում (այսուհետ՝ «Համակարգ»), ներառյալ դրա տեղակայումը, կարգաբերումը, ուսուցումը և ներդրումից հետո շարունակական ուղեկցումն ու տեխնիկական սպասարկումը:

Համակարգը պետք է հնարավորություն ընձեռի արդյունավետորեն հայտնաբերել, գնահատել և կառավարել փողերի լվացման և ահաբեկչության ֆինանսավորման (ՓԼ/ԱՖ), ինչպես նաև՝ միջազգային պատժամիջոցների համապատասխանության ռիսկերը՝ կիրառելով առաջադեմ տեխնոլոգիական գործիքներ:

Նախագծի իրականացման արդյունքում նախատեսվում է բավարարել ՓԼ/ԱՖ և պատժամիջոցների համապատասխանության ռիսկերի գնահատման և մոնիթորինգի իրականացման գործընթացներում հետևյալ պահանջները.

- Անհրաժեշտ տվյալների (այդ թվում՝ հարցումների միջոցով) ստացման, արտահանման և որակի ստուգման ավտոմատացում,
- Այլ համակարգերին և տվյալների բազաներին ինտեգրման հնարավորություն,
- Տվյալների հիման վրա, ըստ ֆինանսական կազմակերպությունների (այսուհետ՝ ՖԿ), ըստ ոլորտների և ըստ ֆին. համակարգի ՓԼ/ԱՖ և պատժամիջոցների համապատասխանության ներհատուկ և մնացորդային ռիսկերի գնահատման ավտոմատացում,
- Վաղ ահազանգման կամ կարմիր դրոշակների մեխանիզմների կիրառման ավտոմատացում,
- ՖԿ-ի և տարբեր ֆինանսական ոլորտների միտումների շարունակական մոնիթորինգի իրականացման հնարավորության ներդրում (ցանկալի է նաև, ՖԿ, ֆինանսական ոլորտի և/կամ համակարգի անոմալ երևույթների բացահայտման և ապագային միտված ռիսկերի կանխատեսման հնարավորություն),
- Համեմատական վերլուծության իրականացման հնարավորություն, ինչպես՝ ՖԿ-ի, այնպես էլ՝ տարբեր ոլորտների միջև,
- Ազգային մակարդակով ՓԼ/ԱՖ և պատժամիջոցների համապատասխանության ռիսկերի գնահատման օժանդակում,



- Վերահսկողական խորաթափանցության նշանակալի բարձրացման համար անհրաժեշտ տարբեր հաշվետվությունների, դինամիկ վահանակների և UI/UX հարմարավետ հարթակի ներդրում:

ԻՐԱԿԱՆԱՑՄԱՆ ՎԱՅՐԸ

Նախագծի իրականացման վայրը Հայաստանի Հանրապետության Կենտրոնական բանկն է՝ Վազգեն Սարգսյան փ. 6, Երևան, 0010 Հայաստանի Հանրապետություն:

ԻՐԱԿԱՆԱՑՄԱՆ ՏԱՐԱԾՔԸ

Համակարգը պետք է տեղադրվի Կենտրոնական բանկի ներքին ենթակառուցվածքներում (ամպային լուծումներն ընդունելի չեն):

ԱՇԽԱՏԱՆՔՆԵՐԻ/ՊԱՅԱՆՁՆԵՐԻ ԾՐՋԱՆԱԿԸ

Այս բաժնում ներկայացված են Համակարգի նկատմամբ նվազագույն պահանջները: Աշխատանքների շրջանակը կարելի է բաժանել հետևյալ բաժինների.

5.1. Ընդհանուր պահանջներ

Համակարգը պետք է լինի նախապես մշակված (ստանդարտացված) լուծում՝ հասանելի շուկայում առկա ծրագրային արտադրանքի ձևաչափով (off-the-shelf)՝ առանց էական մշակման անհրաժեշտության: Համակարգը նախագծված պետք է լինի արագ տեղակայման համար, պարունակի բոլոր անհրաժեշտ ֆայլերը և հրահանգները՝ նպատակային միջավայրում տեղադրման համար, և լինի կարգաբերելի (customizable):

5.2. Տվյալների կառավարում

ՓԼ/ԱՖ և պատժամիջոցների համապատասխանության ռիսկերի գնահատման համար անհրաժեշտ տեղեկատվությունը Համակարգ կարող է մուտքագրվել ավտոմատացված հարցումներ գեներացնող հարթակի, MS Excel և այլ ստանդարտացված տեսակի ֆայլերի ստացման, այլ թույլատրելի տվյալների բազաներին և արտաքին համակարգերին հարցման միջոցով:



Հարցումների կառավարում: Համակարգը պետք է ունենա ապահով և օգտագործողների համար հարմար հարցաթերթիկների օգտագործման հարթակ, որը նախատեսված է հաշվետու ՖԿ-ից տեղեկատվության ստացման համար: ՖԿ-ը, ստանալով հրավերի հղում, կարող են մուտք գործել հարթակ՝ մուտքագրելու անհրաժեշտ տեղեկատվությունը, պահպանելով և ուղարկելով իրենց պատասխանները: Հարթակը պետք է առաջարկի բազմալեզու աջակցություն, իրական ժամանակում տվյալների վավերացում և ավտոմատացված էլ. նամակներ, ներառյալ՝ հրավերներ, վերջնաժամկետի թարմացումներ և հաստատումներ՝ հարցաթերթիկների հաջող ավարտի մասին: Բացի այդ, այն պետք է ապահովի ամենօրյա վիճակագրական տվյալներ հարցաթերթիկների ակտիվության վերաբերյալ: Այն կարող է կառավարել մի քանի վերահսկվող ոլորտներ և բազմաթիվ հարցաթերթիկներ տարբեր հաշվետու ՖԿ-ից: Անվտանգության նպատակներից ելնելով ծրագրային լուծումը պետք է տեղակայված լինի օգտագործողի համապատասխան ենթակառուցվածքներում աջակցելով երկփուլ նույնականացմանը՝ առանց ամպային ծառայությունների օգտագործման: Այն ներառում է մուտքերի մոնիթորինգ, կողպման (lock out) հսկում(control), ինչպես նաև ծանուցումներ ՖԿ-ի և վերահսկողների համար կողպման դեպքերում, և կարող է գաղտնագրել զգայուն տվյալները: Բացի այդ, պետք է ենթարկված լինի անվտանգության թեստավորման երրորդ կողմի անվտանգության մասնագետների կողմից:

Հարթակը պետք նվազեցնի հաշվետու ՖԿ-ի բեռը՝ Excel-ից զանգվածային պատճենման և պայմանական հարցերի միջոցով, որոնք ցուցադրում են միայն անհրաժեշտ հարցերը, ինչը նվազեցնում է հարցերի ընդհանուր քանակը, որոնց պետք է պատասխանի ՖԿ-ը: Տվյալները պետք է վավերացվեն իրական ժամանակում՝ նախազգուշացումները նշելով հարցաթերթիկում: Տվյալների վավերացման և ձևի ամբողջականության պահանջները պետք է նվազագույնի հասցնեն ՓԼ/ԱՖ հաշվետվությունների հետ կապված հիմնական խնդիրներից մեկը՝ տվյալների որակը: Այն պետք է նվազեցնի կամ նույնիսկ վերացնի որակի խնդիրները, ինչպիսիք են՝ անավարտ հաշվետվությունները, սխալ տվյալները, մարդկային սխալները, բացակա տվյալների վավերացումները, տվյալների օգտագործելի ձևափոխման խնդիրները և այդ պատճառով ծախսված աշխատանքը, որոնք հանդիսանում են ռիսկերի գնահատման գործընթացում ամենամեծ ռեսուրսային կորուստներից մեկը:



Հարթակը պետք է հեշտացնի հարցումների հավաքման գործընթացը: Հարցման արդյունքում ստացված պատասխանների ներմուծումը ռիսկի մոդելներ տվյալների լրացուցիչ մանիպուլյացիա, ագրեգացիա կամ փոխակերպում չի պահանջում (վերահսկողի կողմից ձեռքով միջամտության ձևով): Այսինքն՝ հարցման տվյալները ուղղակիորեն պետք է ավտոմատ ներմուծվեն ռիսկի մոդելի մեջ և ռիսկային միավորները հաշվարկվվեն վայրկյանների ընթացքում՝ ընդամենը մեկ կոճակի սեղմումով, ինչը կխնայի զգալի ժամանակ և ռեսուրսներ:

MS Excel և այլ ստանդարտացված ֆայլերի աջակցություն: Համակարգը պետք է ընդունի MS Excel, ինչպես նաև այլ ստանդարտացված ֆայլերից տեղեկատվություն, ՓԼ/ԱՖ ռիսկերի և դրանց կառավարման որակի ամբողջական գնահատման համար: Այս ֆայլերը պետք է ունենան նախապես սահմանված ձևանմուշ՝ բոլոր ներկայացումների ստանդարտացումն ապահովելու համար: Համակարգը պետք է աջակցի Excel-ի, այդ թվում՝ այլ ստանդարտացված ֆայլերից տվյալների ավտոմատ ներմուծումը, ինչը վերացնում է տվյալների մուտքագրման անհրաժեշտությունը ձեռքով: Ֆայլի վերբեռնումից հետո համակարգը պետք է ավտոմատ կերպով քարտեզագրի և վավերացնի տվյալները՝ ըստ նախապես սահմանված կանոնների, ինչպես նաև պետք է աջակցի տվյալների վերլուծական գործիքների ինտեգրմանը՝ վերահսկողին թույլ տալով վերլուծել ներկայացված տվյալները ռիսկերի գնահատման և համապատասխանության համար:

Տարբեր տվյալների բազաներին և համակարգերին ինտեգրում/համակցում: Համակարգը պետք է աջակցի API-ի միջոցով կապ հաստատել արտաքին համակարգերի հետ և իրականացնի անվտանգ վավերացման մեխանիզմներ API կապեր հաստատելու համար: Համակարգը նաև պետք է կարողանա ավտոմատ կերպով հարցումներ իրականացնել տարբեր տվյալների բազաներից՝ ներբեռնել, փոխակերպել և բեռնել տվյալները (ETL), ինչը վերացնում է ձեռքով տվյալների մուտքագրման կամ փոխակերպման անհրաժեշտությունը, նվազեցնում է սխալների հավանականությունը և բարձրացնում է արդյունավետությունը: Հարցումների արդյունքները անմիջապես պետք է կապվեն ռիսկային մոդելներին՝ թույլ տալով ռիսկային գնահատականների արագ թարմացում:

5.3. Դերեր և իրավասություններ



Համակարգը կիրառում է բազմագործոնային վավերացում (MFA)՝ պահանջելով մուտքի համար տրամադրել երկու կամ ավելի միջոցներ (օրինակ՝ գաղտնաբառ + մեկանգամյա կոդ SMS-ով կամ էլ. փոստով): Բոլոր զգայուն տվյալները կոդավորված են ուժեղ (strong) ալգորիթմներով՝ փոխանցման և պահպանման ժամանակ, կանխելով չարտոնված հասանելիությունը նույնիսկ տվյալների որսման դեպքում: Կիրառվում է դերահիմնավորված մուտքի կառավարում, որպեսզի օգտվողներն ունենան միայն իրենց դերին համապատասխան տվյալների և ֆունկցիաների մուտք՝ նվազեցնելով չարաշահման ռիսկը: Բացի այդ, իրականացվում է օգտվողների գործողությունների լոգագրում և մոնիտորինգ՝ հետևելով մուտքագրման փորձերին, տվյալների փոփոխություններին և այլ կարևոր գործողություններին՝ կասկածելի վարքագծեր հայտնաբերելու համար:

5.4. Ռիսկերի մոդելավորում և վերլուծություն

Համակարգում օգտատերը կարող է ստեղծել հատուկ մոդելներ ներհատուկ ռիսկի և կառավարման որակի/հսկողությունների համար՝ համաձայն ոլորտային ՓԼ/ԱՖ ռիսկի գործոնների, ինչպես նաև կարող է կառավարել հարցաթերթերը և տվյալների ներմուծումը տվյալների կառավարման ֆունկցիոնալությամբ: Լուծումը պետք է ապահովի կարգաբերում՝ ներհատուկ ռիսկի և կառավարման որակի/հսկողությունների մոդելների համար, որոնք հնարավորություն են տալիս խմբագրել մոդելները և տեղեկացնում են հաշվարկների ընթացիկ կարգավիճակի մասին: Համակարգում վերահսկողը կարող է հաշվարկել ներհատուկ ռիսկը, կառավարման որակը/հսկողությունները և մնացորդային ռիսկը՝ ՖԿ-ի և ոլորտի մակարդակներում: Վերջնական արդյունքը մնացորդային ռիսկի ջերմաստիճանային քարտեզն է (heatmap), որը վերահսկողներին տրամադրում է համեմատական ոլորտային տեսլական՝ հնարավորություն տալով ռիսկահեն առաջնահերթությունների սահմանմանը վերահսկողական գործողություններում՝ բարձր ռիսկային ՖԿ-ի և բարձր ռիսկային ոլորտների/գործոնների թիրախավորմանը: Վերահսկողները պետք է հնարավորություն ունենան նաև որակական գնահատումներ իրականացնել, մասնավորապես՝ կարողանան մուտքագրել հեռակա/տեղերում վերահսկողության ժամանակ ի հայտ եկած նոր տեղեկատվությունը, որը կարող է վերաբերել ինչպես համակարգի կողմից ավտոմատ գնահատված ներհատուկ ռիսկի ճշգրտմանը (inherent risk adjustment), այնպես էլ՝ հսկողություններին/կառավարման որակին (controls): Համակարգը պետք է աջակցի ժամանակի ընթացքում մոդելի փոփոխված



տարբերակների պահպանման հնարավորությունը, այսինքն պետք է պահպանվեն մոդելի հին տարբերակները որպեսզի վերահսկողները կարողանան ցանկացած ժամանակ համեմատեն նոր մոդելների գնահատականների հետ:

Հարցաթերթերից ստացված տվյալների ամբողջությունը կօգնի վերահսկողության գործողություններին նույնիսկ հաշվետվական ցիկլի ավարտից հետո՝ տրամադրելով տարբեր մակարդակներում վերլուծություններ իրականացնելու և վիճակագրական տվյալներ ստանալու հնարավորություն, ներառյալ՝ ռիսկի գործոնների մակարդակներում, ՖԿ-ի մակարդակում (նմանատիպ չափի ՖԿ-ի կամ ամբողջ ոլորտի ՖԿ-ի համեմատական վերլուծություն), առանձին իրավասության մակարդակում, երկրի խմբի մակարդակում (օրինակ՝ FATF-ի ցուցակներ), կամ ոլորտային մակարդակներում: Համակարգը հնարավորություն է տրամադրում նաև շեմի ընտրության օժանդակություն, որը հանդիսանում է ռիսկի գնահատման գործառնություն ամենակարևոր դերերից մեկը: Երբ համակարգում հասանելի են մի քանի հաշվետվական ցիկլեր, այն տրամադրում է միտումների վերլուծություն առանձին ՖԿ-ի և ֆինանսական համակարգի/ոլորտի համար: Համակարգը կարող է ինտեգրել մեքենայական ուսուցում և արհեստական ինտելեկտ (ԱԻ)՝ ինքնուրույն սովորելու անցյալի տվյալներից և բարելավելու ռիսկերի կանխատեսման ճշգրտությունը: Արդյունքում՝ համակարգը կարող է ներառել կանխատեսող վերլուծություն՝ ոչ միայն ներկայիս ռիսկերը հասկանալու, այլև ապագա ռիսկերը կանխատեսելու համար՝ հիմնված անցյալի տվյալների և միտումների վրա:

Համակարգը կիրառում է նաև դինամիկ վահանակներ, որոնք ապահովում են տվյալ ոլորտի ընդհանուր ռիսկերի գործոնների և միտումների համապարփակ դիտումը: Ամփոփ վահանակները թույլ են տալիս օգտվողներին համեմատել ռիսկերը տարբեր ՖԿ-ների կամ ոլորտների միջև, բացահայտելով օրինաչափություններ կամ շեղումներ: Օգտվողները հաճախ կարող են հարմարեցնել վահանակները՝ կենտրոնանալու համար հատուկ չափանիշների, ժամանակահատվածների կամ հետաքրքրության ոլորտների վրա:

5.5. Հաշվետվությունների ստեղծում

Համակարգը պետք է աջակցի հարմարեցված հաշվետվությունների ստեղծմանը, հնարավորություն տալով վերահսկողներին կազմել հաշվետվություններ վերլուծության և



կառավարման համար՝ տարբեր ռիսկի գործոնների, հաստատությունների և ոլորտների համար, ինչպես նաև տարբեր հաճախականությամբ (օրինակ՝ օրական, ամսական, եռամսյակային): Օգտվողները պետք է կարողանան ընտրել պարամետրեր և կիրառել ֆիլտրեր (օրինակ՝ ժամանակահատվածի, ոլորտի կամ իրավասության հիման վրա)՝ հաշվետվությունները հարմարեցնելու համար: Համակարգը պետք է գեներացնի և՛ վիզուալ հաշվետվություններ (օրինակ՝ գրաֆիկներ), և՛ աղյուսակային հաշվետվություններ, որոնք ցուցադրում են տվյալների արժեքները ժամանակի ընթացքում: Համակարգը պետք է աջակցի ինչպես պլանավորված, այնպես էլ անմիջապես ստեղծվող հաշվետվություններին և ապահովի նախապես պատրաստված ձևանմուշներ՝ հնարավորություն տալով ստեղծել և պահպանել անհատական ձևանմուշներ պարբերական օգտագործման համար: Հաշվետվությունները պետք է հնարավոր լինի արտահանել MS Excel, PDF, CSV կամ MS Word օգտագործողի համար նախընտրելի ձևաչափերով: Համակարգը պետք է վավերացնի տվյալները, ապահովելով տվյալների հետևողականություն (consistency) և թարմացնի հաշվետվությունները նոր տվյալների ներմուծման հետ: Դերահիմնավորված մուտքի վերահսկողությունը պետք է սահմանափակի, թե ով կարող է ստեղծել, խմբագրել կամ դիտել հաշվետվությունները՝ պահպանելով անվտանգությունը և համապատասխանությունը: Այս ամենը կտրամադրի վերահսկողներին գործիքներ՝ արդյունավետորեն կազմելու ճշգրիտ և նպատակային հաշվետվություններ՝ տվյալափոխ որոշումներ կայացնելու համար:

5.6. Աշխատանքային էկրան

Համակարգը պետք է ունենա օգտագործողակենտրոն դիզայն, որը կապահովի ինտուիտիվ և անխափան փորձառություն աշխատակիցների համար: Միջերեսը պետք է լինի տեսողականորեն պարզ, հեշտ նավարկելի և կարգավորելի, թույլ տալով օգտվողներին հարմարեցնել վահանակները, ահազանգերն ու հաշվետվությունները՝ իրենց նախասիրություններին համապատասխան: Դիզայնը պետք է ապահովի, որ բոլոր հիմնական ֆունկցիաները հասանելի լինեն նույն պատուհանում, նվազեցնելով խափանումները և մտավոր բեռը: Արդյունավետությունը առավելագույնի հասցնելու համար համակարգը պետք է ապահովի հարթ ինտեգրում արտաքին պլատֆորմների և տվյալների բազաների հետ:



Համակարգը ներառում է վերահսկողների կողմից փոփոխությունների կառավարման հուսալի գործընթաց, որը կապահովի հաստատման աշխատանքային հոսքեր ցանկացած փոփոխության համար: Այս պահանջը երաշխավորում է, որ բոլոր կարևոր փոփոխությունները՝ լինի դա ռիսկի շեմերի, ահազանգերի, հաշվետվությունների կամ օգտվողների դերերի փոփոխություն, վերահսկվեն, հաստատվեն և գրանցվեն:



ՖՈՒԼԿՑԻՈՆԱԼ ՊԱՅԱՆՁՆԵՐԻ ՆԿԱՐԱԳԻՐ

N	Պահանջ	Նկարագրություն	Օրինակ
1	<u>Հարցումների և տվյալների կառավարում</u>		

1.1	Կարող է հեշտությամբ ստեղծել և հարմարեցնել հատուկ հարցումներ	- Համակարգը թույլ է տալիս օգտվողներին ստեղծել ՓԼ/ԱՖ և պատժամիջոցների համապատասխանության ռիսկերի գնահատման համար նոր հարցումներ՝ հարմարեցնելով հարցերը, պատասխանի ձևաչափերը և կառուցվածքը՝ հիմնված հատուկ նպատակների կամ տվյալների կարիքների վրա: - Համակարգը տրամադրում է հասկանալի և պարզ ինտերֆեյս, որը թույլ է տալիս նաև ոչ տեխնիկական օգտվողներին նախագծել, հարմարեցնել և կիրառել հարցումները՝ առանց մեծ տեխնիկական գիտելիքների: - Հարցումներում հնարավոր է ներառել պայմանական տրամաբանություն, ընտրության ճյուղավորում և բազմալեզու աջակցություն, ինչը դարձնում է դրանք ճկուն տարբեր իրավիճակների համար: <i>Ավելացնել, խմբագրել կամ հեռացնել հարցեր:</i> Օգտվողները կարող են արագորեն ավելացնել նոր հարցեր, փոփոխել արդեն առկա հարցերը կամ	
-----	---	--	--



		հեռացնել դրանք, եթե դրանք այլևս չեն համապատասխանում պահանջներին: Սա թույլ է տալիս դինամիկ թարմացնել հարցումները՝ առանց զրոյից սկսելու անհրաժեշտության: • <i>Միացնել կամ անջատել հարցերը:</i> Օգտվողները կարող են միացնել կամ անջատել առանձին հարցերը՝ առանց դրանք հեռացնելու: Սա հնարավորություն է տալիս հարմարեցնել հարցումները՝ տարբեր սցենարների համար: Օրինակ, որոշ հարցեր կարող են անջատվել որոշակի ՖԿ-ի համար՝ տվյալների հավաքագրման ճկունությունը պահպանելու համար: • <i>Փոխել հարցերի կարգի հիերարխիան:</i> Համակարգը թույլ է տալիս փոփոխել հարցերի հիերարխիայի կարգը, ինչը հնարավորություն է տալիս ավելի լավ կազմակերպել հարցումները: Օրինակ, հնարավոր է հարցերը խմբավորել ըստ թեմայի կամ բարդության՝ ապահովելով տրամաբանական հաջորդականություն: • <i>Փոփոխել հարցերի հերթականությունը:</i> Օգտվողները կարող են փոփոխել հարցերի հերթականությունը հարցման ներսում, ինչը հեշտացնում է հարցումների հոսքի հարմարեցումը՝ հիմնված հետադարձ կապի կամ առաջնահերթությունների փոփոխության վրա:	
--	--	--	--



1.2	Կարող է հեշտությամբ տարածել և հավաքել հարցումներ, և ավտոմատ կերպով համախմբել արդյունքները	• Համակարգը թույլ է տալիս օգտվողներին հեշտությամբ տարածել հարցումները տարբեր ճանապարհներով (էլ.փոստ, վեբ պորտալներ և այլն), որպեսզի դրանք արդյունավետ կերպով հասնեն թիրախային ֆինանսական հաստատությանը: • Հարցումների տարածումից հետո, համակարգը ավտոմատ կերպով հավաքում է պատասխանները, առանց պահանջելու ձեռքով գործողություն: Այն կարող է հետևել, թե ովքեր են արդեն լրացրել հարցումը և հիշեցումներ ուղարկել նրանց, ովքեր չեն լրացրել: • Համակարգը ավտոմատ կերպով համախմբում է արդյունքները իրական ժամանակում, թույլ տալով օգտվողներին դիտել և վերլուծել տվյալները, հենց որ պատասխանները ստացվեն: Սա օգնում է խնայել ժամանակը և ստանալ ակնթարթային պատկերացումներ: • Համախմբված տվյալները կարող են օգտագործվել հատուկ հաշվետվություններ և վահանակներ ստեղծելու համար՝ ապահովելով հարցումների արդյունքների հստակ վիզուալ ներկայացում: • Համակարգը ապահովում է հավաքագրված տվյալների անվտանգ պահպանում՝ օգտագործելով հասանելիության վերահսկողություն, որպեսզի	
-----	---	--	--



		պաշտպանվի հարցումների պատասխանների ամբողջականությունն ու գաղտնիությունը:	
1.3	Հարցադաշտի հատկություններ	• <i>Հարցի տեքստ:</i> Սա այն հիմնական տեքստն է, որը ցուցադրվում է հարցվողին: • <i>Լրացուցիչ նկարագրություն կամ հղման տեքստ:</i> Այս դաշտը տրամադրում է լրացուցիչ տեղեկատվություն կամ հրահանգներ՝ ուղղորդելու համար հարցվողին: Այն կարող է պարզաբանել հարցի համատեքստը կամ տրամադրել հատուկ հրահանգներ, օրինակ՝ «Ընտրեք բոլոր ճիշտ պատասխանները» կամ «Տրամադրեք թվային պատասխան»: • <i>Հարուստ տեքստի խմբագիր:</i> Համակարգը թույլ է տալիս հարցի տեքստի և հրահանգների ձևաչափման տարբերակներ, ինչպիսիք են թվատառ, թեք տառեր, գծում և այլն: Սա հեշտացնում է հարցի կամ հրահանգի կարևոր մասերը շեշտադրելը՝ ավելի լավ ընկալման համար: • <i>Հղումներ դեպի ռեսուրսներ:</i> Հարցի դաշտը կարող է ներառել հիպերհղումներ դեպի արտաքին ռեսուրսներ կամ փաստաթղթեր, տրամադրելով հարցվողին լրացուցիչ նյութեր կամ համատեքստային տեղեկատվություն, որը վերաբերում է հարցին:	



1.4	Ստացված պատասխանի տվյալների տեսակները	• <i>Թիվ:</i> Թույլ է տալիս հավաքել պարզ թվային տվյալներ (օրինակ՝ քանակներ, միավորներ): • <i>Արժույթ:</i> Աջակցում է մուտքագրել ֆինանսական արժեքներ, ձևավորված որպես արժույթ: • <i>Տոկոսային:</i> Օգտագործվում է տոկոսի արժեքների հավաքագրման համար: • <i>Թվային՝ ըստ բաժանումների:</i> Թվային տվյալներ, որոնք դասակարգվում են ըստ իրավասության, տարածաշրջանի, կամ ցանկացած հատուկ բաժանման (օրինակ՝ վաճառքների դասակարգում ըստ երկրի կամ եկամուտների ըստ բաժնի): • <i>Հաշվարկված տվյալներ:</i> Հարաբերություն երկու թվային տվյալների միջև: Ավտոմատ հաշվարկում է և ցույց տալիս երկու թվային արժեքների հարաբերությունը: • <i>Այլ թվային տվյալների գումար:</i> Ավտոմատ հաշվարկում է սահմանված թվային արժեքների գումարը: • <i>Բինար:</i> Հավաքում է այո/ոչ կամ ճիշտ/սխալ տիպի պատասխաններ: • <i>Տարբերակ:</i> Թույլ է տալիս հարցվողներին ընտրել մեկ կամ ավելի տարբերակներ ցուցակից (օրինակ՝ ռադիո կոճակներ մեկ տարբերակի համար կամ նշման տուփեր բազմակի ընտրությունների համար/radio buttons for single selections or checkboxes for multiple selections/):	
-----	---------------------------------------	---	--



		• <i>Ամսաթիվ:</i> Հավաքում է կոնկրետ ամսաթվեր ստանդարտ ձևաչափով (օրինակ՝ օր/ամիս/տարի): • <i>Ազատ տեքստ:</i> Բաց տեքստի դաշտ, որը թույլ է տալիս հարցվողներին մուտքագրել անհամակարգ տեքստային պատասխաններ: • <i>Երկրի ընտրություն:</i> Ընտրացանկ, որը թույլ է տալիս հարցվողներին ընտրել երկիր նախապես սահմանված ցուցակից: • <i>Հատուկ ընտրացանկ:</i> Հարմարեցվող ընտրացանկ՝ նախապես սահմանված տարբերակների ընտրության համար, ինչպիսիք են արդյունաբերական ոլորտները, ապրանքների տեսակները կամ հատուկ կատեգորիաները: • <i>Փաստաթղթերի ներբեռնում:</i> Թույլ է տալիս հարցվողներին ներբեռնել ֆայլեր կամ փաստաթղթեր որպես պատասխան (օրինակ՝ PDF, Word փաստաթղթեր):	
1.5	Հարցերի պատասխանից կախված՝ հարցաթերթիկի լրացման հարմարավետություններ	• Հարցաթերթիկի լրացման գործընթացում որոշ հարցեր ցուցադրվում են կամ թաքցվում՝ ելնելով հարցվողի նախորդ պատասխաններից: Սա հարցման ընթացքը դարձնում է ավելի հարմարավետ՝ ցուցադրելով միայն համապատասխան հարցերը: Սա ապահովում է, որ հարցվողը տեսնի միայն իր իրավիճակին	



		համապատասխան հարցերը՝ հարմարեցնելով և հեշտացնելով լրացման գործընթացը: • Հարցը կարող է կախված լինել մեկ այլ հարցի «Այո» պատասխանից: Եթե հարցվողը ընտրում է «Այո», կախված հարցը կցուցադրվի: • Նույն կերպ, հարցը կարող է ցուցադրվել միայն այն դեպքում, եթե մեկ այլ հարցին պատասխանել են «Ոչ»: Սա թույլ է տալիս հետևողական հարցերի կիրառումը՝ հիմնված բացասական պատասխանների վրա: • Հարցը կարող է կախված լինել մի քանի հարցերից, և այն կցուցադրվի, եթե որոշակի հարցերի պատասխանները լինեն «Այո» և/կամ «Ոչ»: Սա թույլ է տալիս կառուցել բարդ լոգիկա և հարցումների անհատականացում՝ հիմնված բազմաթիվ պայմանների վրա: • Հարցը կարող է կախված լինել մեկ այլ հարցից, որը ինքնին կախված է մեկ այլ հարցից, և այսպես շարունակ: Սա հնարավորություն է տալիս ստեղծել բազմաշերտ պայմանական տրամաբանություն, ինչը թույլ է տալիս կառուցել խիստ անհատականացված հարցումների հոսք՝ ելնելով պատասխանների շարքից: • Անավարտ հարցերի անցում (հաջորդ/նախորդ): Հարցաթերթիկը թույլ է տալիս օգտվողներին արագ	
--	--	---	--



		անցնել հաջորդ կամ նախորդ անավարտ հարցին: Սա օգնում է ապահովել, որ օգտվողը չբացառի պարտադիր հարցերը և ավելի հարթ դարձնի լրացման փորձը, հատկապես երկար հարցումների դեպքում: • Մեծածավալ տվյալների մուտքագրում: Օգտվողները կարող են մեծ ծավալի տվյալներ մուտքագրել միանգամից՝ դյուրին դարձնելով տվյալների մուտքագրումը, հատկապես այն դեպքերում, երբ պետք է մուտքագրվել բազմակի կամ կրկնվող տվյալներ: • Հարցաթերթիկի պահպանում .xlsx կամ .pdf ֆորմատներով: Հարցաթերթիկի լրացումից հետո օգտվողները կարող են այն պահպանել .xlsx (Excel) կամ .pdf ձևաչափերով: Սա թույլ է տալիս հարցվողներին պահել իրենց պատասխանների ձևաչափված տարբերակը, կիսվել արդյունքներով այլ անձանց հետ կամ օգտագործել տվյալները հետագա վերլուծության համար:	
1.6	Հարցման տվյալների որակի և ամբողջականության ստուգում	• Համակարգը կարող է իրականացնել ավտոմատ ստուգումներ՝ ապահովելու համար, որ բոլոր պարտադիր դաշտերը լրացված են: Սա ապահովում է տվյալների ամբողջականությունը, ստուգելով, որ հարցվողը մուտքագրել է տվյալներ բոլոր պարտադիր հարցերի կամ բաժինների համար՝ նախքան հարցման	Օրինակ՝ եթե մեկ հարցում նշվում է մեկնարկի ամսաթիվ, իսկ մյուսում ավարտի ամսաթիվ, համակարգը կարող է վավերացնել, որ ավարտի



		նույնարկումը: • Պլատֆորմը թույլ է տալիս սահմանել կանոններ առանձին տվյալների կետի համար: Օրինակ, կարելի է սահմանել ընդունելի սահմաններ թվային դաշտերի համար, սահմանել ամսաթվի դաշտերի ձևաչափերը, կամ սահմանափակել որոշ մուտքեր՝ նախապես սահմանված արժեքներով (օրինակ՝ տոկոսներ 0-100 միջակայքում): Սա ապահովում է, որ յուրաքանչյուր տվյալ համապատասխանի որոշակի որակական չափանիշներին: • Համակարգը նաև աջակցում է հարմարեցվող տվյալների վավերացման կանոններին, որոնք ներառում են հարաբերություններ երկու կամ ավելի տվյալների կետերի միջև:	ամսաթիվը ավելի ուշ լինի, քան մեկնարկի ամսաթիվը:
1.7	Հակավիրուսային ստուգում	• Երբ ֆայլ բեռնվում է, համակարգը ավտոմատ կերպով սկանավորում է ֆայլը հայտնի վիրուսների, վնասակար ծրագրերի և այլ վտանգավոր սպառնալիքների համար՝ օգտագործելով հակավիրուսային ծրագիր: • Ստուգումը պետք է իրականացվի գործարկման (execute) միջոցով: • Եթե վնասակար ֆայլ հայտնաբերվի, համակարգը կարող է տեղեկացնել ադմինիստրատորներին կամ օգտվողներին իրական ժամանակում՝ թույլ տալով	



		նրանց անհապաղ միջոցներ ձեռնարկել, օրինակ՝ ֆայլը մերժել կամ օգտվողին նախազգուշացնել: - Աջակցվող ֆայլի տեսակներ: Հակավիրուսային ստուգումը պետք է ընդգրկի տարբեր ֆայլերի տեսակներ (օրինակ՝ PDF, պատկերներ, Word փաստաթղթեր, աղյուսակներ)՝ ապահովելու համար ամբողջական պաշտպանություն: - Կանոնավոր թարմացումներ: Հակավիրուսային ծրագիրը պետք է կանոնավոր կերպով թարմացվի վերջին վիրուսների սահմանումներով՝ նոր սպառնալիքները հայտնաբերելու համար:	
1.8	Հարցաթերթիկի մերժման հնարավորություն և մերժման պատճառի հաղորդում	- Համակարգը տրամադրում է հնարավորություն վերահսկողին մերժել ներկայացված հարցաթերթիկները, որոնք չեն համապատասխանում պահանջներին կամ պարունակում են սխալներ: Այս հատկությունը ապահովում է, որ միայն ճիշտ, ճշգրիտ և ամբողջական տվյալներն են մշակվում: - Հարցաթերթիկը մերժելուց հետո համակարգը թույլ է տալիս հաղորդել մերժման կոնկրետ պատճառը հարցվողին: Սա կարող է կատարվել ավտոմատ ծանուցումների կամ հաղորդագրությունների միջոցով, որոնց մեջ նշվում է, թե հարցաթերթիկի որ մասը պետք է ուղղել (օրինակ՝ թերի տվյալներ, անվավեր մուտքեր	



		կամ անհամապատասխան պատասխաններ):	
1.9	Մերժված հարցումների նորից մուտք գործելու հնարավորություն:	- Համակարգը թույլ է տալիս օգտվողներին նորից մուտք գործել մերժված հարցումը ցանկացած պահին՝ այն ուղղումների համար վերադարձնելուց հետո: Այս հատկությունը հնարավորություն է տալիս օգտվողին շարունակել հարցումը հենց այն կետից, որտեղից այն մերժվել է՝ կատարելով անհրաժեշտ ուղղումները: - Նախապես մուտքագրված տվյալները մնում են պահպանված, այնպես որ օգտվողները կարիք չեն ունենա կրկին մուտքագրել ամբողջ տեղեկատվությունը: Նրանք կարող են ուղղակի ուղղել այն մասերը, որոնք պատճառ են դարձել մերժման համար, ինչն արագացնում և հեշտացնում է գործընթացը: - Համակարգը նշում է այն հատվածները, որոնք կարիք ունեն ուղղման՝ հիմնվելով մերժման պատճառի վրա, ուղղորդելով օգտվողին դեպի խնդրահարույց բաժինները: Սա նվազեցնում է շփոթությունը և ապահովում է, որ օգտվողները կենտրոնանան միայն անհրաժեշտ դաշտերի ուղղման վրա: - Ուղղումներ կատարելուց հետո օգտվողները կարող են նորից ներկայացնել հարցաթերթիկը՝ առանց գրոյից սկսելու: Սա ապահովում է հարթ և անխափան	



		գործընթաց թե՛ հարցվողի, թե՛ ադմինիստրատորների/վերահսկողի համար:	
1.10	Բազմակի փուլերով հարցումների իրականացում	- Համակարգը թույլ է տալիս իրականացնել հարցումների մի քանի փուլ, ինչը հնարավորություն է տալիս տարբեր փուլերում կամ ժամանակի ընթացքում հավաքել տվյալներ: Այս հատկությունը աջակցում է կրկնվող տվյալների հավաքագրմանը և հնարավորություն է տալիս կատարելագործել կամ լրացնել նախորդ պատասխանները: - Հարցվողների նախորդ փուլերի պատասխանները կարող են փոխանցվել հաջորդ հարցումներին, ինչը հեշտացնում է տվյալների հավաքման գործընթացը: Սա նվազեցնում է հարցվողների բեռը, քանի որ նրանք կարիք չեն ունենա նորից մուտքագրել նույն տեղեկությունները, եթե դրանք չեն փոփոխվել: - Համակարգը հետևում է փոփոխություններին տարբեր հարցումների փուլերում, ինչը հնարավորություն է տալիս համեմատել և վերլուծել, թե ինչպես են պատասխանները փոփոխվում ժամանակի ընթացքում: Սա հատկապես օգտակար է երկարաժամկետ ծրագրերի կամ հետազոտությունների համար, որոնք պահանջում են պարբերական տվյալների հավաքագրում:	



		• Յուրաքանչյուր հարցման փուլ կարող է հարմարեցվել, թույլ տալով ավելացնել նոր հարցեր, փոփոխել առկա հարցերը կամ կարգավորել ձևաչափը՝ ելնելով նախորդ փուլերից ստացված պատկերացումներից: Այս կրկնվող մոտեցումը բարելավում է հավաքագրվող տվյալների որակը և համապատասխանությունը: • Համակարգը հնարավորություն է տալիս ընդգրկուն վերլուծություն կատարել մի քանի փուլերի տվյալների հիման վրա՝ ապահովելով միտումների, օրինաչափությունների և փոփոխությունների մասին պատկերացումներ ժամանակի ընթացքում:	
1.11	Կազմակերպությունների ցանկի թարմացման և հարցաթերթիկների կրկին ուղարկման հնարավորություն (կազմակերպության տվյալների փոփոխության դեպքում):	• Համակարգը թույլ է տալիս վերահսկողներին հեշտությամբ թարմացնել կազմակերպությունների ցանկը, երբ փոփոխություններ են կատարվում կազմակերպության տվյալներում (օրինակ՝ անվան, կոնտակտային տվյալների կամ կարգավիճակի փոփոխություն): Սա ապահովում է, որ բոլոր կազմակերպությունները, որոնք ներառված են հարցման ցանկում, լինեն արդի և համապատասխան: • Կարող եք ավելացնել նոր կազմակերպություններ, թարմացնել առկա կազմակերպությունների տվյալները կամ հեռացնել հին կազմակերպությունները՝	



		պահպանելով ճշգրիտ ցանկ հարցաթերթիկների տարածման համար: - Կազմակերպությունների ցանկի թարմացումից հետո, համակարգը տրամադրում է հարցաթերթիկները կրկին ուղարկելու հնարավորություն այն կազմակերպություններին, որոնց տվյալները փոխվել են: Սա ապահովում է, որ թարմացված կազմակերպությունները ստանան հարցումը կամ հետագա հաղորդակցությունները: Համակարգը կարող է նաև ակտիվացնել ծանուցումներ կամ հիշեցումներ նոր թարմացված կամ ավելացված կազմակերպություններին՝ ապահովելով, որ նրանք ավարտեն հարցումը նշված ժամկետներում: - Կազմակերպության տվյալներում կատարված բոլոր փոփոխությունները համաժամացվում (synchronized) են արդեն ուղարկված հարցումների հետ՝ ապահովելով, որ հավաքագրված տվյալները կապվեն թարմացված կազմակերպությունների գրառումներին:	
1.12	Ավտոմատացված ծանուցումներ	<i>Հրավերներ:</i> Ավտոմատացված էլ. նամակներ կամ ծանուցումներ, որոնք հրավիրում են մասնակցին մասնակցելու հարցման, առաջադրանքի կամ գործընթացի: Դրանք ներառում են անհատականացված	



		հաղորդագրություն՝ հղումով դեպի այն ձևը կամ համակարգը, որը նրանք պետք է մուտք գործեն: • Հիշեցումներ: Ավտոմատ հիշեցումներ են ուղարկվում, եթե օգտվողը չի ավարտել պահանջվող գործողությունը, օրինակ՝ հարցման լրացումը: Համակարգը կարող է ուղարկել մի քանի հիշեցումներ որոշակի ժամանակահատվածում՝ գործողություն կատարելու համար: • Ժամկետի երկարաձգումներ: Ծանուցումներ, որոնք տեղեկացնում են մասնակիցներին ժամկետի երկարաձգման մասին, եթե լրացնելու կամ ձևը հանձնելու համար լրացուցիչ ժամանակ է տրամադրվում: Սա ապահովում է, որ բոլոր կողմերը տեղյակ են ժամանակացույցի փոփոխությունների մասին: • Գաղտնաբառի փոփոխություն: Ավտոմատացված նամակներ ուղարկվում են, երբ օգտվողը խնդրում է փոխել գաղտնաբառը: Այս նամակներն ընդգրկում են հրահանգներ և հղում՝ գաղտնաբառը անվտանգ վերականգնելու համար: • Հանձնված: Օգտվողները ստանում են հաստատման ծանուցումներ, երբ առաջադրանքը, հարցումը կամ ձևը հաջողությամբ հանձնվում է (submit): Սա վստահություն	
--	--	--	--



		է տալիս, որ նրանց հանձնումը հաջողությամբ ստացվել է: • <i>Արգելափակված:</i> Ծանուցումներ են ուղարկվում, երբ օգտվողը արգելափակվում է համակարգից՝ բազմակի սխալ մուտքագրումների կամ անվտանգության պատճառներով: Նամակն առաջարկում է հրահանգներ՝ ինչպես վերականգնել մուտքը:	
1.13	Էլ. նամակների և հարցումների արտաքին տեսքի ձևավորում:	• <i>Հոգոներ և գույներ:</i> Հնարավոր է անհատականացնել էլ. նամակները կազմակերպության լոգոյով, գույներով և վիզուալ ինքնությամբ: Սա հաղորդակցությունը դարձնում է անմիջապես ճանաչելի և ամրապնդում է Կենտրոնական բանկի բրենդի ներկայությունը: • <i>Էլ. նամակի գլխամաս/ոտնամաս:</i> Հնարավոր է ներառել գլխամաս և ոտնամաս յուրաքանչյուր նամակի մեջ՝ Կենտրոնական բանկի անունով, կոնտակտային տվյալներով և կայքի (այդ թվում՝ գաղտնիության քաղաքականության) հղումներով: • <i>Տառադրասակներ և ոճեր:</i> Հնարավոր է օգտագործել համապատասխան տառատեսակներ և տեքստի ոճեր՝ ապահովելով բոլոր հաղորդակցությունների համահունչությունը Կենտրոնական բանկի	



		ինքնությանը:	
1.14	Էլ. նամակի միջոցով հարցումների վիճակագրության տրամադրում:	• <i>Անգործունակ ՖԿ-ներ:</i> Էլ. նամակում նշվում են այն ՖԿ-ները, որոնք դեռ չեն սկսել հարցումը կամ անգործուն են մնացել հրավեր ստանալուց հետո: Սա ադմինիստրատորներին թույլ է տալիս հետևել չարձագանքող ՖԿ-ներին և քայլեր ձեռնարկել՝ հիշեցումներ ուղարկելու կամ լրացուցիչ հաղորդակցություններ իրականացնելու համար: • <i>Ակտիվ ՖԿ-ներ:</i> Համակարգը առանձնացնում է նաև այն ՖԿ-ները, որոնք ներկայումս ակտիվորեն աշխատում են հարցման վրա, բայց դեռ չեն ներկայացրել իրենց պատասխանները: Այս տեղեկատվությունը կարևոր է՝ դիտարկելու համար առաջընթացը և համոզվելու, որ ՖԿ-ները ներգրավված են հարցման գործընթացում: • <i>Հանձնած ՖԿ-ներ:</i> Էլ. նամակը ներառում է այն ՖԿ-ների ցանկը, որոնք հաջողությամբ լրացրել և ներկայացրել են իրենց հարցումները: Սա օգնում է ադմինիստրատորներին/վերահսկողին հետևել, թե որ ՖԿ-ներն են արդեն կատարել իրենց պարտավորությունները:	



1.15	Վերահսկողի մուտքի հասանելիություն ընթացքի մեջ գտնվող հարցաթերթիկներին	• <i>Մոնիթորինգի իրականացում:</i> Վերահսկողները կարող են դիտել մասնակի լրացված հարցաթերթիկների ընթացքը, տեսնել, թե որ բաժիններն են արդեն լրացված, և որոնք են դեռ չլրացված: Սա թույլ է տալիս նրանց իմանալ ընթացիկ աշխատանքների մասին և միջամտել անհրաժեշտության դեպքում: • <i>Ուղղորդում ապահովել:</i> Վերահսկողները կարող են դիտարկել մինչ այժմ (ընթացքում գտնվող) մուտքագրված պատասխանները և տրամադրել հետադարձ կապ կամ ուղղորդում, որպեսզի տվյալների մուտքագրումը համապատասխանի որակի և ամբողջականության պահանջներին մինչև վերջնական ներկայացումը: • <i>Ժամկետների հետևում:</i> Վերահսկողները կարող են հետևել ժամկետներին և ընթացքի կատարելությանը՝ հիշեցնելով տվյալները մուտքագրողներին, եթե հարցաթերթիկի ավարտի վերջնաժամկետը մոտենում է, իսկ այն դեռ չի ավարտվել:	
1.16	ՓԼ/ԱՖ հարցումների համար MS Excel-ի և այլ ստանդարտացված ֆայլերի օգտագործում	• <i>Ֆայլերի ընդունում:</i> Համակարգը կարող է ընդունել MS Excel և այլ ստանդարտացված ֆայլերը ՓԼ/ԱՖ ռիսկերի և դրանց կառավարման որակի գնահատման համար: Այս ֆայլերը պետք է ունենան նախապես	Ձևանմուշը պետք է ներառի պահանջվող դաշտեր, օրինակ ինչպիսիք են՝ կանխիկ



		սահմանված ձևանմուշ՝ բոլոր ներկայացումների ստանդարտացումն ապահովելու համար: • Տվյալների վավերացում: Վերբեռնումից հետո համակարգը պետք է իրականացնի տվյալների վավերացում՝ ստուգելու, որ բոլոր պարտադիր դաշտերը լրացված են և ,որ տվյալները համապատասխանում են պահանջվող կառուցվածքին (օրինակ՝ արժույթների արժեքները ճիշտ ձևաչափով են, ամսաթվերը համապատասխանում են պահանջվող ձևաչափին): • Վավերացման կանոնները կարող են ներառել բացակայող տվյալների, կրկնվող գրառումների կամ սխալ ձևաչափերի ստուգում: • Մշակում և քարտեզագրում: Վավերացումից հետո յուրաքանչյուր տվյալ (օրինակ՝ գումարներ, անուններ, ռիսկային մակարդակներ) պետք է ճիշտ քարտեզագրվի համակարգի ներքին դաշտերին՝ պահպանման և վերլուծության համար: • Ավտոմատացում և ինտեգրում: Համակարգը պետք է աջակցի Excel-ի և այլ ստանդարտացված ֆայլերից տվյալների ավտոմատ ներմուծումը, ինչը վերացնում է տվյալների մուտքագրման անհրաժեշտությունը ձեռքով: Ֆայլի վերբեռնումից հետո համակարգը պետք է	գործարքների ծավալ, կասկածելի գործարքների քանակ, ոչ ռեզիդենտ և ռեզիդենտ հաճախորդների քանակ և այլ համապատասխան տվյալներ:
--	--	--	---



		ավտոմատ կերպով քարտեզագրի և վավերացնի տվյալները՝ ըստ նախապես սահմանված կանոնների: • Պետք է աջակցի տվյալների վերլուծական գործիքների ինտեգրմանը՝ վերահսկողին թույլ տալով վերլուծել ներկայացված տվյալները ռիսկերի գնահատման և համապատասխանության համար: • <i>Սխալների մշակում:</i> Եթե ներկայացված Excel և/կամ այլ ստանդարտացված ֆայլում սխալներ են (օրինակ՝ բացակայող տվյալներ, սխալ ձևաչափեր), համակարգը պետք է օգտվողին տեղյակ պահի սխալների հաղորդագրություններով, նշելով՝ ինչ պետք է ուղղել: • Պետք է լինի վերանայման գործընթաց, որը թույլ կտա օգտվողներին վերբեռնել ուղղված ֆայլերը: • <i>Տվյալների թարմացումներ և վարկածների վերահսկում:</i> Համակարգը պետք է ապահովի վարկածների հսկում, թույլ տալով թարմացնել Excel և այլ ստանդարտացված ֆայլերի ձևանմուշները, երբ կարգավորումները փոխվում են: Սա ապահովում է, որ հարցման ձևաչափերի կամ տվյալների պահանջների փոփոխությունները արտացոլվեն նոր ձևանմուշներում:	
1.17	API-ի միջոցով այլ համակարգերի հետ կապ հաստատել	• Համակարգը պետք է աջակցի API-ի միջոցով կապ հաստատել այլ համակարգերի հետ (տվյալներ ստանալու և տալու հնարավորություն):	



		• Համակարգը պետք է իրականացնի անվտանգ վավերացման մեխանիզմներ API կապեր հաստատելու համար: Համակարգը պետք է ունենա հնարավորություն անվտանգ ֆայլային տվյալների փոխանցման (Secure File Transfer), մասնավորապես՝ SFTP (Secure File Transfer Protocol) օգտագործմամբ: • Համակարգը պետք է ունենա սխալների մշակման հնարավորություն և կրկնության մեխանիզմներ API հարցումների համար: • Համակարգը պետք է տվյալները API միջոցով ստանալուց հետո քարտեզագրի իր ներքին տվյալների կառուցվածքին: • Համակարգը պետք է աջակցի ավտոմատացված, ժամանակացուցված API հարցումների կատարմանը: • Համակարգը պետք է պահպանի API հարցումների ամբողջական գրանցում, որը կներառի հարցումների մանրամասները, պատասխանների կարգավիճակը և սխալները:	
1.18	Ավտոմատ կերպով կատարում է ETL տարբեր տվյալների բազաներից և ներմուծում հարցումների արդյունքները ռիսկային մոդելներ	• <i>Ներբեռնում (Extract):</i> Համակարգը ավտոմատ կերպով հանում է հավաքված հարցումների տվյալները ըստ օգտագործողի սահմանած ժամանակացույցի (օրինակ՝ ամեն օր, ամեն շաբաթ): Սրանք կարող են ներառել պատասխանները, մեթատվյալները և այլ	



		համապատասխան մանրամասներ տարբեր ֆորմատներից կամ հարթակներից: • Փոխակերպում (Transform): Տվյալների ներբեռնումից հետո համակարգը փոխակերպում է տվյալները՝ դարձնելով դրանք հարմար վերլուծության և ռիսկային մոդելների հետ ինտեգրման համար: Սա կարող է ներառել տվյալների մաքրում, նորմալացում և կառուցում, որպեսզի ապահովվի դրանց համահունչությունը և ճշգրտությունը: • Բեռնում (Load): Փոխակերպված տվյալները բեռնվում են ռիսկային մոդելների մեջ, որտեղ դրանք օգտագործվում են ռիսկային գնահատականների, պրոֆիլների կամ չափանիշների թարմացման համար: • Իրական ժամանակում թարմացումներ: Համակարգը թարմացնում է ռիսկային մոդելները անմիջապես ETL գործընթացի ավարտից հետո՝ ապահովելով, որ ռիսկային գնահատականները լինեն արդի և արտացոլեն հարցումների արդյունքների վերջին տվյալները:	
2.	<u>Ռիսկերի մոդելավորում</u>		
2.1	Ռիսկերիի գնահատում (ներհատուկ ռիսկ,	• Ներհատուկ ռիսկի տվյալների հավաքագրում և գնահատում: Համակարգը պետք է տրամադրի	Օրինակ՝ ՓԼ/ԱՖ համատեքստում,



հսկողություններ և մնացորդային ռիսկ)	ներհատուկ ռիսկի գնահատում, օգտագործելով նախապես սահմանված չափանիշներ (հաճախորդի ռիսկը, աշխարհագրական ռիսկը և ապրանքի/ծառայության ռիսկը և այլ նախանշված ցուցանիշներ) կամ կարգավորելի (customizable) մոդելներ՝ ավտոմատ ռիսկային գնահատման համար: Կազմակերպության ընդհանուր ներհատուկ ռիսկի գնահատականը կազմված է կազմակերպության ներհատուկ ռիսկի և ոլորտային ներհատուկ ռիսկի մակարդակի գնահատականների համակցությունից: • Կառավարման որակի/Հսկողությունների և ռիսկի նվազեցման միջոցառումների տվյալների հավաքագրում և գնահատում: Կառավարման որակի/Ներքին հսկողության տվյալները (օրինակ՝ ներքին աուդիտ, գործարքների մոնիտորինգի համակարգեր կամ հաճախորդների պատշաճության ստուգման գործընթացներ (KYC)) պետք է գնահատվեն, և համակարգը պետք է տրամադրի կառավարման որակի/հսկողության գնահատում, որը ցույց կտա, թե որքանով է այդ հսկողությունը արդյունավետ ներհատուկ ռիսկը նվազեցնելու համար:	ներհատուկ ռիսկի տվյալները կարող են ներառել հաճախորդի իրավասությունը, գործարքների տեսակը և ծավալը: Համակարգը գնահատում է ներհատուկ ռիսկը՝ հիմնվելով այդ ցուցանիշների վրա: Օրինակ՝ Եթե ֆինանսական հաստատությունը ունի արդյունավետ գործարքների մոնիտորինգի համակարգ և ուժեղ KYC գործընթացներ, համակարգը պետք է տրամադրի բարձր կառավարման որակի/հսկողությունների
--	---	---



		• Մնացորդային ռիսկի հաշվարկ: Համակարգը պետք է կարողանա հաշվարկել մնացորդային ռիսկ՝ վերցնելով ներհատուկ ռիսկի գնահատումը և հաշվի առնելով կառավարման որակի/հսկողությունների և ռիսկի նվազեցման միջոցառումների արդյունավետությունը: Մնացորդային ռիսկ=Ներհատուկ ռիսկ-կառավարման որակ/հսկողության արդյունավետություն	գնահատում, ինչը կցուցադրի, որ ռիսկերը լավ են վերահսկվում: Օրինակ՝ եթե բարձր ներհատուկ ռիսկ կա՝ հիմնված բարձր ծավալի գործարքների վրա բարձր ռիսկային իրավասությունում, սակայն կառավարման որակ/արդյունավետ հսկողություններ են կիրառված, մնացորդային ռիսկը կարող է զգալիորեն կրճատվել:
2.2	Ռիսկի գնահատման մոդել կշռված միջինների հիման վրա	• Տարբեր ռիսկային գործոնների, ինչպիսիք են հաճախորդի տեսակը, իրավական դաշտը, գործարքների բնույթը, ապրանքի/ծառայության ռիսկերը, պետք է տրվեն տարբեր կշիռներ: • Կշռված միջինները պետք է օգնենք հաշվել ընդհանուր ռիսկը՝ հիմնվելով ՓԼ/ԱՖ ռիսկերի ցուցանիշների վրա:	Օրինակ՝ 50% կշիռ տալ իրավական դաշտի ռիսկին, 30%՝ գործարքների ծավալին, և 20%՝ հաճախորդի տեսակի ռիսկին՝ գնահատելու համար ՓԼ/ԱՖ ռիսկը:



2.3	Հատուկ (custom) և հիերարխիաներ ոչսկային խմբավորումներ թեմաներով	• <i>Հատուկ հիերարխիաների սահմանում:</i> Համակարգը պետք է թույլ տա օգտագործողներին ստեղծել հատուկ հիերարխիաներ՝ հիմնված հաճախորդների կամ ծառայությունների ոչսկի մակարդակի վրա: ◦ Օգտագործողները պետք է կարողանան դասակարգել բարձր ոչսկային հաճախորդներին (օրինակ՝ քաղաքական ազդեցություն ունեցող անձ (PEP), հաճախորդներ բարձր ոչսկային իրավական դաշտից) կամ բարձր ոչսկային ծառայություններ/գործարքներ (օրինակ՝ կրիպտոարժույթի գործարքներ): ◦ Այս դասակարգումները պետք է լինեն կարգավորելի՝ վերահսկողներին հնարավորություն տալով հարմարեցնել հիերարխիաները՝ հիմնվելով նոր սպառնալիքների կամ կարգավորումների փոփոխությունների վրա: • <i>Սեգմենտացված ոչսկի գնահատումներ:</i> Համակարգը պետք է ապահովի սեգմենտացված ոչսկի գնահատումներ՝ յուրաքանչյուր խմբի համար՝ հիմնվելով նախապես սահմանված ոչսկային կատեգորիաների վրա:	Օրինակ՝ Օգտագործողները կարող են սահմանել բարձր ոչսկային հաճախորդներ՝ հիմնվելով բարձր ոչսկային իրավական դաշտում գտնվող հաճախորդների կամ որոշակի տնտեսության ճյուղերի (օրինակ՝ խաղային բիզնես) վրա: Օրինակ՝ Համակարգը խմբավորում է գործարքները հաճախորդի տեսակի և իրավասության հիման վրա՝ թույլ տալով սեգմենտացված ոչսկի գնահատումներ՝ բարձր ոչսկային հաճախորդների համար, որոնք ներառված
-----	--	---	--



		- Յուրաքանչյուր սեգմենտ (օրինակ՝ բարձր ռիսկային հաճախորդներ, բարձր ռիսկային ծառայություններ/ապրանքներ) պետք է առանձնացված գնահատվի, և ռիսկի գնահատումները պետք է կարգավորվեն՝ հիմնվելով յուրաքանչյուր ռիսկային գործոնի կշռի վրա: - Համակարգը պետք է աջակցի ճկուն գնահատումներին, թույլ տալով վերահսկողներին հարմարեցնել ռիսկային կշիռները նոր սպառնալիքների կամ կարգավորումների փոփոխությունների դեպքում:	են անդրսահմանային գործարքներում: Օրինակ՝ Համակարգը գնահատում է բարձր ռիսկային հաճախորդների ռիսկը՝ հաշվի առնելով գործարքների հաճախականությունը և ծավալները և տրամադրում է ռիսկային միավորներ՝ հիմնված այդ չափանիշների վրա:
2.4	Ներհատուկ ռիսկի և կառավարման որակի/հսկողողության գնահատականների արտահանում	- Համակարգը պետք է թույլ տա օգտվողներին արտահանել ներհատուկ ռիսկի և կառավարման որակի/հսկողությունների գնահատականները սահմանված ձևաչափերով (Excel, CSV, PDF, Word): - Արտահանված ֆայլերը պետք է ներառեն մանրամասն նկարագրություններ, հաշվարկներ և բոլոր համապատասխան մոդելային պարամետրերը: - Արտահանված ֆայլերը պետք է լինեն հստակ կառուցված և հեշտ փաստաթղթավորման և վերանայման համար:	Օրինակ՝ արտահանել հարցման արդյունքները, ռիսկային գնահատականները և դասակարգումները յուրաքանչյուր ՖԿ-ի համար



		Արտահանումների գործընթացը պետք է լոգավորվի և հասանելի լինի ադմինիստրատորին:	
2.5	Տարածաշրջանային ռիսկի մոդելներ՝ հիմնված առանձին իրավասությունների ռիսկերի կամ իրավասությունների ցուցակների վրա, որտեղ իրավասությունները կամ ցուցակները կարող են ունենալ տարբեր կշիռներ:	<i>Առանձին իրավասությունների ռիսկեր:</i> Յուրաքանչյուր երկիր կամ իրավասություն գնահատվում է առնվազն հետևյալ գործոններով. - Կարգավորող և իրավական շրջանակներ: - ՓԼ/ԱՖ դեմ պայքարին միտված հսկողության արդյունավետություն: - Միջազգային պատժամիջոցների ցուցակներում ներառված լինելը (օրինակ՝ FATF-ի բարձր ռիսկային երկրներ): - Քաղաքական կայունություն, կոռուպցիայի մակարդակ, և տնտեսական թափանցիկություն: <i>Իրավասությունների ցուցակներ:</i> Իրավասությունները կարող են խմբավորվել ռիսկային կատեգորիաներով (օրինակ՝ բարձր ռիսկային, միջին ռիսկային, ցածր ռիսկային)՝ հատուկ չափանիշների հիման վրա: - Այս ցուցակները կարող են փոփոխվել ժամանակի ընթացքում՝ հաշվի առնելով երկրի կարգավորող միջավայրի փոփոխությունները կամ միջազգային կարգավիճակի վերանայումները:	- Օրինակ, բարձր ռիսկային իրավասությունները (օրինակ՝ երկրներ, որոնք հայտնի են ֆինանսական գաղտնիության և թույլ ՓԼ/ԱՖ կառուցակարգերով) կարող են ավելի բարձր կշիռ ունենալ՝ մեծացնելով այդ իրավասությունների հետ կապված գործարքների կարևորության մակարդակը ՓԼ/ԱՖ տեսանկյունից: - Ավելի ցածր ռիսկային իրավասությունները կարող են ունենալ ավելի ցածր կշիռ:



		Տարբեր կշռով իրավասություններ: Յուրաքանչյուր իրավասություն կամ ցուցակ կարող է տարբեր կշիռներ ունենալ՝ հիմնված նրա ռիսկային պրոֆիլի վրա:	
2.6	Հատուկ տարածաշրջաններ (օրինակ՝ նահանգներ կամ մարզեր իրավասության ներսում), որտեղ տարածաշրջանների տարբերակներին կարող են տրվել տարբեր կշիռներ	Յուրաքանչյուր հատուկ տարածաշրջանին կարող է տրվել հատուկ ռիսկային կշիռ, ինչը նշանակում է, որ որոշ տարածաշրջաններ կարող են դիտարկվել ավելի ռիսկային, քան մյուսները: Սա կարևոր է ռիսկի վրա հիմնված գնահատումների համար, երբ նույն երկրի տարբեր նահանգներ կամ մարզեր կարող են ունենալ տարբեր ռիսկային մակարդակներ՝ ելնելով տեղական օրենքներից, կարգավորող միջավայրից կամ տնտեսական կայունությունից:	Օրինակ՝ Միացյալ Նահանգներում, Նևադան (իր լիբերալ բիզնես օրենքների պատճառով) կարող է ունենալ ավելի բարձր ռիսկային կշիռ՝ համեմատած այլ նահանգների հետ:
2.7	Հատուկ ցուցակներ (օրինակ՝ արժույթներ), որտեղ ցուցակի տարբերակներին կարող են տրվել տարբեր կշիռներ	- Օգտվողները կարող են ստեղծել և սահմանել ցուցակներ՝ հիմնվելով կազմակերպության կարիքների վրա (օրինակ՝ արժույթներ, ակտիվներ, գործարքների տեսակներ): - Այս ցուցակները կարող են ներառել բարձր ռիսկային արժույթներ, զգայուն ապրանքներ կամ խոցելի հաճախորդների խմբեր: - Յուրաքանչյուր ցուցակի տարր (օրինակ՝ արժույթներ, ինչպիսիք են USD, EUR կամ Bitcoin) կարող է ունենալ	Օրինակ՝ վերահսկողը կարող է բարձր ռիսկային կշիռ տալ կրիպտոարժույթներին (օրինակ՝ Bitcoin)՝ համեմատած ավանդական արժույթների (օրինակ՝ USD կամ EUR) հետ՝ հաշվի առնելով դրանց



		հատուկ ռիսկային կշիռ, որը սահմանվում է՝ ելնելով նրա ռիսկային մակարդակից:	անանունության մակարդակը:
2.8	Տվյալների կետերի բաժանում ըստ երկրի, տարածաշրջանի կամ հատուկ ցուցակների	- Համակարգը պետք է թույլ տա օգտվողներին բաժանել գործարքների վերաբերյալ տվյալները ըստ երկրի՝ արդյունքները ցուցադրելով ընտրված իրավասության հիման վրա: - Համակարգը պետք է աջակցի տարածաշրջանային ֆիլտրացիային և վերլուծությանը՝ ապահովելով հատուկ աշխարհագրական տարածքների տվյալների վերլուծություն:	
2.9	Կատարում է տրված ոլորտների հաստատությունների ռիսկի գնահատումներ (հարաբերական ռիսկ)	- Համակարգը պետք է նախ ստեղծի ռիսկային պրոֆիլներ՝ հաշվի առնելով ՓԼ/ԱՖ խոցելիությունները, օրինակ՝ բանկային, ապահովագրական ոլորտներում: Այս պրոֆիլները կարևոր են, որպեսզի հասկանանք, թե ինչպես են տարբեր հաստատությունները ենթարկվում փողերի լվացման կամ ահաբեկչության ֆինանսավորման ռիսկերին: - Համակարգը պետք է դասակարգի հաստատությունները ըստ նրանց ռիսկային մակարդակի՝ համեմատելով իրար հետ: Բարձր ռիսկային գնահատականներ (օրինակ՝ հաշվի առնելով հետևյալ գործոնները՝ KYC, անդրսահմանային	



		գործարքներ և այլն) ունեցող հաստատությունները կնշվեն կարմիր դրոշակով՝ հետագա առավել մանրամասն մոնիտորինգ և վերահսկողական միջոցառումներ իրականացնելու համար: Համակարգը համեմատության միջոցով պետք է բացահայտի առաջարկները հիմնված ՓԼ/ԱՖ ռիսկային գործոնների վրա՝ բացահայտելով համեմատական առավել բարձր և ցածր ռիսկային հաստատությունները:	
2.10	ՖԿ մակարդակով ռիսկերի գնահատումներից՝ սեկտորալ և ազգային ռիսկերի գնահատումների անցման հնարավորություն (բացարձակ ռիսկ)	Համակարգը գնահատում է բացարձակ ՓԼ/ԱՖ ռիսկը, ուսումնասիրելով այն խոցելիությունները, որոնք ներհատուկ են ոլորտին, ինչպիսիք են՝ անդրսահմանային գործարքները, բարձր ռիսկային ոլորտների կամ իրավասությունների հետ կապվածությունը, կամ բարդ սեփականության կառուցվածքները: Այն հաշվի է առնում նաև կարգավորումների բացթողումները, ինչպիսիք են՝ KYC (Ճանաչիր հաճախորդիդ) ընթացակարգերի անբավարար կիրառումը: Ռիսկի գնահատումները հիմնվում են ՓԼ/ԱՖ հատուկ ցուցանիշների վրա, օրինակ՝բարձր ռիսկային հաճախորդների կամ բիզնեսների տոկոսը տվյալ ոլորտում,անսովոր կամ մեծ	



		գործարքների ծավալը, որոնք կարող են հուշել փողերի լվացման ռիսկի մասին, կասկածելի գործարքների մասին չհայտարարելը կամ հաշվետվությունների տարբերությունները: • Համակարգը պետք է ավտոմատ կերպով վերամշակի ՖԿ ռիսկերի գնահատումներից ստացված տվյալները՝ որպես հիմնական մուտքային տվյալներ ոլորտային և ազգային ռիսկերի գնահատումների համար: • Վերամշակումը պետք է ապահովի, որ ՖԿ-ի մակարդակում հայտնաբերված ոլորտային միտումները և ռիսկերը ուղղակիորեն փոխանցվեն ավելի բարձր մակարդակի գնահատումներին: • Այս գնահատումները տրամադրում են տվյալներ, որոնք կարող են մուտքային տվյալներ հանդիսանալ ազգային ռիսկի գնահատմանը (NRA): • Այս գնահատումները օգնում են ձևավորել քաղաքական որոշումներ, ռեսուրսների բաշխում և կարգավորող ռազմավարություններ, որոնք ուղղված են հայտնաբերված ռիսկերի նվազեցմանը:	
2.11	Տվյալների միացման/անջատման կետերի	• Օգտվողները պետք է հնարավորություն ունենան միացնել կամ անջատել որոշակի տվյալների կետերը	Օրինակ՝ Վերահսկողը գնահատում է



	հնարավորություն ներհատուկ ռիսկի և ներքին հսկողության գնահատման համար	ներհատուկ ռիսկի և կառավարման որակի/հսկողությունների գնահատման մոդելներում: Համակարգը պետք է թույլ տա օգտվողներին նշել, թե որ տվյալների կետերը պետք է ներառվեն ներհատուկ ռիսկի գնահատման (օրինակ՝ գործարքների ծավալ, իրավասության ռիսկ) մեջ և որոնք՝ ոչ: Նույնը կիրառելի է կառավարման որակի/հսկողությունների գնահատման համար, որտեղ միայն ակտիվ հսկողության չափանիշները պետք է ազդեն վերջնական գնահատման վրա: • Անջատված տվյալների կետերը չեն նպաստի ընդհանուր ռիսկի կամ հսկողության գնահատմանը, սակայն պետք է մնան հասանելի ապագայում հնարավոր ակտիվացման համար: • Միայն լիազորված օգտվողները (օրինակ՝ որոշակի վերահսկողները կամ ադմինիստրատորներ) պետք է ունենան այս տվյալների կետերի միացման/անջատման հասանելիությունը: • Համակարգում պետք է իրականացվի դերով պայմանավորված մուտքի վերահսկողություն, որպեսզի միայն որոշակի օգտվողներ կարողանան փոփոխել տվյալների կետերի կարգավիճակը:	հաճախորդի ներհատուկ ռիսկը և որոշում է, որ գործարքների ծավալը այլևս կարևոր չէ գնահատման համար՝ համաձայն նոր կանոնակարգերի և անջատում է այդ տվյալների կետը:
--	---	---	--



		• Տվյալների կետերի միացման/անջատման կարգավիճակի բոլոր փոփոխությունները պետք է գրանցվեն համակարգում: • Գրանցումը պետք է ներառի, թե ով է կատարել փոփոխությունը, երբ և ինչ պատճառներով: • Տվյալների կետը միացնելիս կամ անջատելիս համակարգը պետք է վերահաշվարկի ներհատուկ ռիսկի և հսկողության գնահատման միավորները՝ անմիջապես արտացոլելով փոփոխված կոնֆիգուրացիան: • Համակարգը պետք է տրամադրի ծանուցումներ կամ հուշումներ տվյալների կետերի միացման/անջատման հաստատման համար, հատկապես, եթե փոփոխությունը զգալիորեն ազդում է ռիսկի կամ հսկողության գնահատման վրա:	
2.12	Ռիսկի մոդելների փոփոխություններին ավտոմատ կերպով հարմարվող գնահատման ալգորիթմ	• Գնահատման ալգորիթմը պետք է ավտոմատ կերպով հարմարեցնի ռիսկի գնահատումները, երբ փոփոխվում են փոփոխականները, հիերարխիաները, կարգավորումները, քաշերը, շեմերը կամ պատասխանների վարկանիշները: • Ռիսկի մոդելի փոփոխությունները պետք է արտացոլվեն իրական ժամանակում՝ առանց ձեռքով վերահաշվարկման անհրաժեշտության:	



		Համակարգը պետք է պահպանի ճշգրտությունը և արդյունավետությունը բոլոր վերահաշվարկներում:	
2.13	ՓԼ/ԱՖ ռիսկերի հայտնաբերման բարելավում մեքենայական ուսուցման միջոցով	Համակարգը կարող է ինտեգրել մեքենայական ուսուցում և արհեստական ինտելեկտ (ԱԻ)՝ ինքնուրույն սովորելու անցյալի տվյալներից և բարելավելու ռիսկերի կանխատեսման ճշգրտությունը: Համակարգի կատարելագործման շնորհիվ այն կարող է ներառել կանխատեսող վերլուծություն՝ ոչ միայն ներկայիս ռիսկերը հասկանալու, այլև ապագա ռիսկերը կանխատեսելու համար՝ հիմնված անցյալի տվյալների և միտումների վրա:	Օրինակ՝ Համակարգը արձանագրում է միտում, երբ միջին չափի առևտրային բանկը զգալիորեն ավելացնում է իր ներգրավվածությունը բարձր ռիսկ ունեցող ոլորտներում (օրինակ՝ անշարժ գույք, խաղատներ, կրիպտոարժույթների փոխանակում)՝ առանց համապատասխանեցված հարմարվողականության իր ՓԼ/ԱՖ ռիսկերի կառավարման մեխանիզմներում կամ ներքին վերահսկողության համակարգում: Բացի այդ, բանկում կասկածելի գործարքների մասին



			հաղորդումների թիվը նվազում է, չնայած գործարքային ծավալների և հաճախորդների ավելացմանը: Համադրելով այս տվյալները նմանատիպ բանկերի հետ և հիմնվելով նախորդ վերահսկողական գնահատումների վրա՝ համակարգը առաջադրում է նախագգուշացում՝ առաջարկելով բանկը ընդգրկել խորացված վերահսկողության շրջանակում՝ հնարավոր թերությունների հայտնաբերման նպատակով ռիսկային մոտեցման և հաղորդման պարտավորությունների կատարման ուղղությամբ:
2.14	Ցանկացած քանակով ֆինանսական ոլորտներ և	Համակարգը նախագծված է աջակցելու բազմաթիվ ոլորտների՝ ինչպիսիք են բանկային ոլորտը,	Օրինակ՝ մոդելներ բանկերի, վարկային և



	ցանկացած քանակով կազմակերպություններ տվյալ ոլորտում	վարկայինը, ապահովագրությունը և հեշտությամբ կարող է ընդլայնվել՝ ընդգրկելու ցանկացած քանակի ոլորտներ: Այն կարող է կառավարել և կազմակերպել ցանկացած քանակի ֆինանսական հաստատություններ յուրաքանչյուր ոլորտի ներսում:	ապահովագրական ընկերությունների համար
2.15	Նոր ռիսկի մոդելներ կառուցում կամ գոյություն ունեցող տարբերակի հարմարեցում	- Համակարգը թույլ է տալիս օգտվողներին ձևավորել նոր ռիսկային մոդելներ՝ հիմնված հատուկ պարամետրերի վրա, ինչպիսիք են աշխարհագրությունը կամ կարգավորող պահանջները: - Համակարգը կարող է ինտեգրել առկա ռիսկային մոդելները, ապահովելով հարթ անցում կամ թարմացում՝ առանց կորցնելու նախապես մշակված շրջանակները կամ մեթոդաբանությունները: - Օգտվողները կարող են հարմարեցնել մոդելները՝ հիմնվելով նոր տվյալների վրա կամ փոփոխվող ռիսկերի գնահատման կարիքների վրա, ապահովելով, որ ռիսկերի կառավարման գործընթացները լինեն ժամանակակից և ընդարձակելի:	
2.16	Սխալ տվյալների (data points) թարմացման հնարավորություն	- Համակարգը պետք է թույլ տա օգտվողներին ճանաչել այն տվյալների կետերը, որոնք կարող են լինել սխալ: - Օգտագործողները պետք է կարողանան ընտրել այդ տվյալների կետերը թարմացնել:	Օրինակ՝ օգտագործողը հայտնաբերում է սխալ տեղեկատվության



		Միայն լիազորված օգտագործողները (օրինակ՝ ադմինիստրատորներ կամ տվյալների կառավարիչներ) պետք է ունենան տվյալների կետերի թարմացման հնարավորություն:	գրառում համակարգում: Նա կարող է հայտ ներկայացնել համապատասխան թույլտվություններ ունեցող անձին թարմացման վերաբերյալ:
2.17	Դերեր և թույլտվություններ	- Համակարգը պետք է ունենա դերերի և իրավասությունների կառավարման գործառույթ, որը կթույլատրի ճշգրտորեն սահմանել, կառավարել և վերահսկել օգտվողների հասանելիությունը տարբեր մոդուլների և գործողությունների նկատմամբ՝ RBAC (Role-Based Access Control), SOD (Segregation of Duties) և Least Privilege սկզբունքների համաձայն: - Համակարգը պետք է ապահովի 4 աչքերի հաստատման գործընթաց բոլոր վերագրանցումների համար՝ կապված ներհատուկ ռիսկի և կառավարման որակի/հսկողությունների փոփոխման հետ: - Բոլոր վերագրանցումները և գործողությունները պետք է փաստագրվեն հաշվետու լոգերում՝ հստակ մանրամասներով այն մասին, թե ով է նախաձեռնել և հաստատել գործողությունները: Ինչպես նաև՝ սխալները	



		և համակարգային իրադարձությունները՝ հետագա աուդիտի և դեբազի աջակցման համար:	
3	<i>Տվյալների վերլուծության հնարավորություններ</i>		
3.1	ՖԿ-ի և ոլորտների ամփոփ վիճակագրական տվյալներ	- Համակարգը պետք է ապահովի ոլորտներում ՓԼ/ԱՖ կարևոր ցուցիչների ավտոմատ հաշվարկ և ամփոփում: Հաշվարկվում են նվազագույնը, միջինը, մոդան, առավելագույն արժեքը, ընդհանուր արժեքներ և հարցմանը պատասխանող ՖԿ-ի քանակը, ինչը թույլ է տալիս գնահատել ոլորտի ռիսկերը: - Համակարգը պետք է ապահովի ամփոփումներ յուրաքանչյուր ՖԿ-ի համար, ինչը թույլ է տալիս հայտնաբերել ՓԼ/ԱՖ դեմ պայքարի համապատասխանության հետ կապված արտառոց գործունեություն: Ամփոփումները պետք է տրամադրվեն յուրաքանչյուր ՖԿ-ի համար՝ գնահատելու նրանց ռիսկային մակարդակը և կառավարման որակի/հսկողությունների արդյունավետությունը:	Օրինակ՝ Տրամադրել որոշակի բանկի կասկածելի գործարքների վերաբերյալ մանրամասն հաշվետվություն և համեմատել դրա արժեքները ոլորտի միջին ցուցանիշների հետ:
3.2	Նախորդ հաշվետու ժամանակահատվածի նկատմամբ փոփոխություններ,	Համակարգը պետք է հայտնաբերի և գրանցի փոփոխությունները ընթացիկ և նախորդ հաշվետու ցիկլերի միջև: Փոփոխությունները կարող են ներառել.	Օրինակ՝ Եթե ֆինանսական հաստատության ռիսկային



	Տվյալների միտումների վերլուծություն	◦ Ցուցանիշների տարբերություններ, այդ թվում և քանակական և որակական (օրինակ՝ գնահատականների աճ կամ նվազում) ◦ Ռիսկային գնահատականների, շեմերի կամ այլ կատարողական ցուցանիշների փոփոխություններ ◦ Մասնավոր հարցերի կամ հարցումների պատասխանների տարբերություններ ◦ ՖԿ-ին ներհատուկ փոփոխություններ, ինչպիսիք են գործարքների ծավալները կամ համապատասխանության մակարդակը • Օգտագործողները պետք է կարողանան տեսնել այդ փոփոխությունները համեմատական հաշվետվության կամ վահանակի տեսքով: • Համակարգը պետք է աջակցի միտումների վերլուծությանը ցանկացած սահմանված տվյալների չափանիշի (օրինակ՝ ռիսկային միավորներ, գործարքների ծավալներ, համապատասխանության խախտումներ) համար՝ որոշակի ժամանակահատվածի ընթացքում: • Համակարգը պետք է գեներացնի տվյալ չափանիշի փոփոխության վիզուալ ներկայացում, ներառյալ գծային	գնահատականը նվազել է նախորդ ցիկլի համեմատ, համակարգը պետք է նշի փոփոխությունը և քանակականացնի տարբերությունը: Օրինակ՝ Օգտագործողը կարող է ցանկանալ համեմատել միայն բարձր ռիսկային գնահատականները հաշվետու ցիկլերի միջև: Օրինակ՝ Բանկը կարող է օգտագործել միտումների վերլուծությունը՝ դիտարկելու վերջին վեց ամիսների ընթացքում բարձր ռիսկային գործարքների աճը՝ ՓԼ/ԱՖ
--	--	---	--



		գրաֆիկներ, սյունակային գծապատկերներ կամ այլ համապատասխան վիզուալիզացիաներ: • <i>Չափանիշի ընտրություն:</i> Օգտվողները պետք է կարողանան ընտրել, թե որ չափանիշերը վերլուծել, և համակարգը պետք է թույլ տա համեմատել տարբեր չափանիշեր: • Համակարգը պետք է ապահովի թե՛ նախապես սահմանված չափանիշեր (օրինակ՝ ռիսկային գնահատականներ, գործարքների ծավալ), և թե՛ օգտագործողի կողմից սահմանված չափանիշեր: • <i>Ժամանակահատվածի հարմարեցում:</i> Օգտվողները պետք է կարողանան ընտրել տվյալների վերլուծության համար ժամանակահատվածը՝ ընտրելով , օրինակ, օրական, շաբաթական, ամսական, եռամսյակային կամ տարեկան համեմատություններ: • <i>Վերլուծության ցուցանիշներ:</i> Համակարգը պետք է հաշվարկի միտումների վերլուծության համար առանցքային ցուցանիշները, ներառյալ՝ ◦ Տոկոսային փոփոխություններ ժամանակի ընթացքում ◦ Շարժվող միջիններ՝ կարճաժամկետ տատանումները հարթելու համար ◦ Աճման կամ նվազման արագություն	ռիսկերը հայտնաբերելու համար: Օրինակ: Ֆինանսական հաստատությունը կարող է դիտարկել խոշոր կանխիկ դեպոզիտների միտումները ամսական/եռամսյակային կամ այլ կտրվածքով կտրվածքով:
--	--	--	---



		○ Տվյալների գազաթների և անցքերի հայտնաբերում • Վիզուալ և աղյուսակային հաշվետվություններ: Համակարգը պետք է գեներացնի և՛ վիզուալ հաշվետվություններ (օրինակ՝ գրաֆիկներ, աղյուսակներ), և՛ աղյուսակային հաշվետվություններ, որոնք ցուցադրում են տվյալների արժեքները ժամանակի ընթացքում: • Օգտվողները պետք է կարողանան արտահանել այս հաշվետվությունները տարբեր ձևաչափերով, ինչպիսիք են Excel, PDF կամ CSV: • Անոմալիաների հայտնաբերում կամ վաղ ահազանգում: Համակարգը պետք է ներառի անոմալիաների հայտնաբերման գործառույթ, որը կտեղեկացնի օգտվողներին, եթե տվյալ չափանիշի շեղումներ կամ անսպասելի փոփոխություններ են նկատվում:	Օրինակ՝ Համակարգը պետք է ցույց տա, որ բարձր արժեք ունեցող գործարքների գազաթնակետը եղել է տարվա առաջին եռամսյակում:
3.4	Շեմերի սահմանում	• Համակարգը պետք է հնարավորություն ունենա շեմերի ընտրության, պահպանման և կիրառման գործում առանցքային ՓԼ/ԱՖ ռիսկային ցուցանիշների համար: • Օգտվողները պետք է կարողանան սահմանել և վերաօգտագործել հարմարեցված ՓԼ/ԱՖ շեմերը: • Շեմերի խախտման դեպքում պետք է ավտոմատ կերպով ահազանգեր ստեղծվեն:	



3.5	Վահանակներ ոլորտի և ոլորտի ամփոփ վիճակագրական տվյալների վերաբերյալ	<i>Ոլորտի ամփոփ(այդ թվում՝ վիճակագրական) վահանակներ:</i> - Այս վահանակները ապահովում են տվյալ ոլորտի ընդհանուր դիսկերի գործոնների և միտումների համապարփակ դիտում: Օգտատերերը կարող են հասանելիություն ունենալ հիմնական տվյալներին: - Ներառում է կանոնակարգերի համապատասխանության, ի հայտ եկող դիսկերի կամ բարելավման հնարավորությունների ընդգծում: - Տրամադրում է ամփոփ վիճակագրական տվյալներ, ինչպիսիք են ոլորտում դիսկերի մակարդակը: - Այս տվյալները ներկայացվում են վիզուալ ձևաչափերով (գծապատկերներ, աղյուսակներ կամ գրաֆիկներ)՝ պարզեցնելու համար տվյալների մեկնաբանումը և դյուրին դարձնելու բարդ տվյալների ըմբռնումը: - Ամփոփ վահանակները թույլ են տալիս օգտվողներին համեմատել կատարողականը տարբեր ՖԿ-ի կամ ոլորտների միջև, բացահայտելով օրինաչափություններ կամ շեղումներ: <i>Անհատականացվող դիտումներ:</i> - Վերահսկողները հաճախ կարող են հարմարեցնել վահանակները՝ կենտրոնանալու համար հատուկ	Օրինակ՝ ֆինանսական ծառայությունների ոլորտում կարգավորող մարմինը կարող է օգտագործել համախմբված վիճակագրությունը՝ բանկերից ստացված տվյալների հիման վրա գնահատելու ոլորտի ընդհանուր դիսկերի մակարդակը, ինչպիսիք են՝ ՓԼ/ԱՖ և պատժամիջոցների համապատասխանության դիսկերը կամ վերջիններիս աճը
-----	--	--	---



		չափանիշների, ժամանակահատվածների կամ հետաքրքրության ոլորտների վրա: <i>Իրական ժամանակում տվյալներ:</i> Այս վահանակները սովորաբար ցուցադրում են իրական ժամանակում կամ գրեթե իրական ժամանակին մոտ տվյալներ, ինչը հնարավորություն է տալիս արագ արձագանքել ոլորտի կատարողականի կամ ռիսկերի մակարդակի փոփոխություններին:	
3.6	Տրամադրում է բազմաթիվ ՖԿ-ի գնահատականների, պատասխանների և դասակարգումների հորիզոնական համեմատություն	- Համակարգը ցուցադրում է մի քանի ՖԿ-ի տվյալները կողք կողքի՝ հեշտացնելով նրանց ռիսկային գնահատականների կամ հարցումների պատասխանների համեմատությունը տարբեր կատեգորիաների կամ չափանիշների հիման վրա: - Համեմատությունը ներառում է գնահատականներ (օրինակ՝ ռիսկային գնահատականներ, համապատասխանության գնահատականներ), պատասխաններ հարցումներից կամ գնահատումներից, և դասակարգումներ, ինչը թույլ է տալիս օգտվողներին տեսնել, թե որ ՖԿ-ն է լավագույնը կամ վատագույնը յուրաքանչյուր կատեգորիայի մեջ: - Օգտվողները կարող են հարմարեցնել համեմատվող չափանիշները կամ ցուցանիշները՝ համեմատելու	Օրինակ՝ Բանկային ոլորտ: Կարգավորող մարմինը կարող է համեմատել տարբեր բանկերի ռիսկային գնահատականները կողք կողքի՝ հասկանալու, թե որ հաստատություններն են ամենաարդյունավետը ռիսկի կառավարման հարցում:



		համար ՖԿ-ը իրենց գործունեությանը կամ կարգավորող պահանջներին համապատասխան: - Համակարգը թույլ է տալիս օգտվողներին ֆիլտրել և դասակարգել արդյունքները՝ կենտրոնանալով հատուկ ոլորտների, ժամանակային շրջանակների կամ պատասխանների տեսակների վրա: - Համեմատությունը հաճախ ներկայացվում է գրաֆիկական ձևաչափով (գրաֆիկներ, աղյուսակներ, գծապատկերներ), ինչը թույլ է տալիս արագորեն հայտնաբերել օրինաչափություններ կամ շեղումներ ՖԿ-ի միջև:	
--	--	---	--

ԾԱՐՏԱՐԱԴԵՏԱԿԱՆ ՊԱՅԱՆՁՆԵՐ

No.	Պահանջներ	Նկարագրություն
1.	Գործառնական համակարգ. ցանկալի է Windows Server 19 կամ ավելի նոր տարբերակ	Ցանկալի է, որ համակարգը սահուն աշխատի Windows Server 19-ում կամ ավելի նոր տարբերակում: Համակարգը չպետք է օգտագործի հնացած կամ խոցելի պրոտոկոլներ՝ արձանագրություններ (օրինակ՝ SMBv1, TLS 1.0/1.1):



2.	Տվյալների բազայի պահանջ. ցանկալի է DBMS, MS SQL SERVER	Համակարգը պետք է կապված լինի հետևյալ տվյալների բազաներից առնվազն մեկի հետ՝ DBMS, MS SQL SERVER, Oracle, PostgreSQL, MySQL-Maria DB (ցանկալի է, որ աջակցի վերջին երկարաժամկետ սպասարկվող տարբերակին (LTS)՝ խուսափելու հնացած և խոցելի թողարկումներից): Վերջիններս համատեղելի են բոլոր հիմնական վեբ դիտարկիչների հետ(Տես գլուխ 9-ի 3-րդ կետ):
3.	Ինտեգրված է մշտադիտարկման ճկուն համակարգ	Մշտադիտարկման ճկուն համակարգ՝ գտման հնարավորությամբ (նաև հատուկ բաղադրիչների մշտադիտարկում, օրինակ՝ աշխատանքային գործընթացի մշտադիտարկում)՝ խափանումների որոնման և ուղղման, խափանումների պատճառները որոշելու և դեպքերի վերաբերյալ հաղորդագրությունները ֆիլտրելու ժամանակի սպառումը նվազագույնի հասցնելու համար:
4.	Համակարգի վերականգնման գործիքներ	Անհրաժեշտ մուտքի դեպքում օգտագործողները կարող են վերականգնել համակարգի ցանկացած տեղեկության կորուստ: Համակարգը պետք է ինտեգրվի Veeam ծրագրային ապահովման հետ:



5.	Համակարգի կառավարման գործիքներ	Համակարգի կառավարման գործիքները լիովին հասանելի են (օգտատիրոջ գրանցում, օգտատիրոջ իրավունքների շնորհում, օգտատիրոջ փոխարինում, կատալոգների սպասարկում)
6.	Համակարգի արդյունավետության ապահովման գործիքներ	Համակարգի արդյունավետության ապահովման գործիքները տրամադրվում են Հայտատուի կողմից
7.	Համակցման հնարավորություններ	Համակցման հնարավորությունները ներառում են Client/Server, N-tier, middleware architecture և service-oriented architecture (SOA) տարբերակներից ցանկացածի կիրառություն:

ՀԱՄԱԿԱՐԳԵՐԻ ՂԵԿԱՎԱՐՄԱՆ, ԻՆՏԵԳՐՄԱՆ և ԿԱՌԱՎԱՐՄԱՆ ՊԱՅԱՆՋՎՈՂ ԳՈՐԾԱՌՈՒՅԹՆԵՐ

No.	Պահանջներ	Նկարագրություն	Օրինակ
1.	Ծրագրային ապահովումը հնարավորություն է տալիս առանձնացնելու օգտատերերի	ա) Օգտատերերի հասանելիության դերերը/իրավունքները մուտքագրվում են համակարգ՝ օգտատերերի և դերերի կառավարման նպատակով:	Օրինակ՝ նոր աշխատակիցը AD-ից ստանում է մուտքի հասանելիություն ընդհանուր և իր պարտականությունների



	հասանելիության իրավունքները/դերերը	բ) Նշված տեղեկատվությունը հնարավոր է համակարգ մուտքագրել ինչպես ձեռքով, այնպես էլ այլ համակարգերից՝ ավտոմատացված հարցումների միջոցով (AD, SSO և այլն): գ) Օգտատերերի հաջող գրանցումը ենթադրում է բոլոր հնարավոր իրավասությունների/դերերի վերաբերյալ կարգավորումներ, ամրացում կառուցվածքի այս կամ այն ճյուղին, ինչպես նաև համակարգում կատարված գործողությունների և փոփոխությունների ժանանակ կատարողի նույնականացում (principle of non-repudiation)	շրջանակներին համապատասխան ֆունկցիոնալ գործընթացներին:
2.	Օգտատերերի գործողությունները լոգավորվում են	բոլոր համակարգում Գործընթացում գործողությունների հնարավորություն: Մասնավորապես՝ 1. Համակարգը պետք է պահպանի օգտագործողների մուտքերի և գրանցման բոլոր գործողությունների լոգերը՝ ապահովելով անվտանգության մոնիտորինգ և անոմալիաների հայտնաբերում:	



		2. Համակարգը պետք է կիրառի Գաղտնաբառերի անվտանգության քաղաքականություն (Password Policy)՝ ապահովելու ուժեղ և հաճախակի փոխվող գաղտնաբառեր:	
3.	Համակարգում վարվում է բոլոր ֆայլային արտահանումների աուդիտային մատյան	ա) Աուդիտային մատյանը պարունակում է արտահանումներ, այդ թվում՝ արտահանումը կատարած օգտատերը, արտահանման ժամը և ամսաթիվը, բ) Համակարգից արտահանված ֆայլը պետք է բավականաչափ տեղեկատվություն պարունակի այն արտահանած օգտատիրոջը նույնականացնելու համար, այդպիսի տեղեկատվության ցանկացած փոփոխության դեպքում ֆայլը պետք է դառնա անգործածելի/փչացած: գ) Պետք է աջակցի անվտանգության տեղեկատվության և իրադարձությունների կառավարման Trellix- SIEM լուծումն հետ ինտեգրմանը որպեսզի հնարավոր լինի	Եթե օգտատերը ֆայլ է ներբեռնում համակարգից, ֆայլին կցվում է օգտատիրոջ եզակի ստորագրությունը կամ անուն ազգանունը:



		վերահսկել ֆայլային արտահանումները, հայտնաբերել անոմալիաները և կանխել չարտոնված փոփոխությունները:	
4.	Համակարգը տալիս է իրադարձությունների մատյանների վարման ֆունկցիոնալ հնարավորություն	ա) Համակարգում սահմանված իրադարձությունների (այդ թվում՝ աշխատանքի ընթացքում ի հայտ եկած սխալների և սահմանափակումների) վարման և մշտադիտարկման ֆունկցիոնալ հնարավորություն: բ) Սխալների խմբավորում և տարբեր ադմինիստրատորների խմբերի հասցեագրում:	Սերվիսների հետ համակցումների սխալների տարանջատում տվյալների բազայի հասանելիության սխալից և տարբեր ադմինիստրատորների հասցեագրում:
5.	Համակարգում առկա է համակարգի կառավարման և մշտադիտարկման պատուհան	Համակարգի աշխատունակության վերաբերյալ տեղեկատվության արտացոլում ժամանակի իրական ռեժիմում:	Արտադրողականության և սխալների գրաֆիկական արտապատկերում ժամանակի իրական ռեժիմում:
6.	Համակարգը պետք է ունենա արտաքին համակարգերի հետ	Համակարգը պետք է ապահովի տվյալների փոխանցման և ինտեգրման բազմազան մեխանիզմներ, ինչը կարևոր է տարբեր	



	ինտեգրման հետևյալ տեխնոլոգիաները/պրոտոկոլները	համակարգերի միջև հուսալի, անվտանգ և արդյունավետ փոխգործակցության համար: Ստորև ներկայացված են հիմնական տեխնոլոգիական պահանջները՝ տվյալների փոխանակման համար. ա) API պրոտոկոլներ (REST, SOAP, RPC) բ) FTP/SFTP, գ) Ցանկացած տեխնոլոգիայի տվյալների բազայի ուղիղ հասանելիություն, դ) MQ տեխնոլոգիաներ:	
7.	Համակարգը պետք է աջակցի տվյալների փոխանցման հետևյալ ձևաչափերը	XLSX, CSV, JSON, XML կամ այլ ընդունված ստանդարտ	

ՀԱՄԱԿԱՐԳԻ ԱՐՏԱԴՐՈՂԱԿԱՆՈՒԹՅԱՆ և ՕԳՏԱԳՈՐԾՈՂԻ ՄԻՋԵՐԵՍԻ ՊԱՅԱՆՁՆԵՐ

No.	Պահանջներ	Նկարագրություն
-----	-----------	----------------



1.	Առնվազն 10 օգտատերերի արագ և առանց խափանումների սպասարկման ապահովում (առավելագույն քանակը՝ 50).	Միաժամանակյա աշխատող օգտատերերի աշխատանքի անխափան ապահովում և համակարգին հասանելիություն:
2.	Համակարգն ունի մեծ ծավալի ֆայլերի հետ գործ ունենալու մասշտաբայնություն՝ առանց արտադրողականության հետ կապված որևէ խնդրի	Համակարգը ունակ է գործ ունենալու տվյալների հարաճուն քանակության հետ՝ առանց ազդեցություն թողնելու համակարգի արագության կամ հուսալիության վրա: Համակարգը պետք է ապահովի դիտարկման մեխանիզմներ (monitoring mechanisms) , օգտագործի caching և սեղմման մեթոդներ, որպեսզի մեծ ֆայլերի հետ գործելը չազդի համակարգի արագության վրա:
3.	Համակարգը չունի կախվածություն դիտարկչից և կարող է օգտատերերին հասանելի լինել տարբեր սարքերից և հարթակներից	Բազմաթիվ դիտարկիչների հետ համատեղելիություն. Համակարգը համատեղելի է բոլոր հիմնական վեբ դիտարկիչների հետ, ինչպիսիք են՝ Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari և այլն:
4.	Համակարգը կարող է ապահովել մեծ թվով ոլորտների և ՖԿ-ի գնահատումը առնվազն ամսական պարբերականությամբ	Համակարգը պետք է ապահովի առնվազն բանկային, վարկային, վճարահաշվարկային, ներդրումային կազմակերպությունների (այդ թվում՝ դեպոզիտարիա) ոլորտների և համապատասխան ֆինանսական կազմակերպությունների (բանկեր-17, վարկային կազմակերպություններ-42, վճարահաշվարկային



		կազմակերպություններ-16, ներդրումային կազմակերպություններ-22, դեպոզիտարիա-1) գնահատումը առնվազն ամսական պարբերականությամբ (հետագայում գնահատման հաճախականությունը մեծացնելու հնարավորությունը իրականին մոտ կամ իրական նախընտրելի է):
5.	Օգտատերերը հեշտությամբ են օգտագործում համակարգը	Օգտագործողի միջերեսի հիմնական պահանջներ • Հեշտ և ինտուիտիվ նավիգացիա – Համակարգի կառուցվածքը պետք է թույլ տա օգտատերերին արագ գտնել իրենց անհրաժեշտ ֆունկցիոնալությունը՝ առանց երկար որոնման: • Գործողությունների հստակ ուղեցույց (User Journey Clarity) – UI/UX դիզայնը պետք է ապահովի, որ օգտատերերը հասկանան իրենց հաջորդ քայլերը և կարողանան հեշտությամբ կատարել անհրաժեշտ գործողությունները: • Հասանելիություն (Accessibility) – Համակարգը պետք է լինի հարմար տարբեր օգտատերերի համար (Ցանկալի է բավարի Web Content Accessibility Guidelines (WCAG) 2.1-ի պահանջներին): UI/UX Գնահատում – Համակարգի օգտագործելիությունը (UI/UX) պետք է գնահատվի հանձնաժողովի կողմից, որը կվերլուծի դիզայնի հարմարավետությունը, հասկանալիությունը և



		արդյունավետությունը՝ վերջնական օգտատերերի փորձը բարելավելու համար:
--	--	--

ՀԱՄԱԿԱՐԳԻ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՊԱՅԱՆՁՆԵՐ

No.	Պահանջներ	Նկարագրություն	Օրինակ
1.	Համակարգն ապահովում է օգտատիրոջ և սերվերի միջև տեղեկատվության փոխանակման անվտանգությունը	Համակարգը պետք է ապահովի օգտատիրոջ և սերվերի միջև տվյալների անվտանգ փոխանցում, կանխելով տվյալների արտահոսքը, չարտոնված մուտքը և կիրքեր սպառնալիքները	
2.	Անվտանգության միջազգային ստանդարտներին համապատասխանություն	Համակարգը նախընտրելի է համապատասխանի միջազգային անվտանգության չափանիշներին, ինչպիսիք են՝ ISO 27001 – Տեղեկատվության անվտանգության կառավարման համակարգ: Մասնավորապես՝ Համակարգը պետք է համապատասխանի առնվազն ISO 27001:2022 ստանդարտի հետևյալ control-ներին՝ • 8.25 - Secure development life cycle • 8.26 - Application security requierments • 8.27 - Secure system architecture and engineering principles • 8.28 - Secure coding	



		• 8.29 - Security testing in development and acceptance • 8.30 - Outsourced development	
3.	Համակարգը տալիս է կցված ֆայլերին վերաբերող չափի, ձևաչափի այլ չափորոշիչների սահմանափակման հնարավորություն	Համակարգը պետք է ապահովի կցված ֆայլերի (attachments) սահմանափակման գործառույթ, ինչը թույլ կտա վերահսկել ֆայլերի չափերը, ձևաչափերը և այլ չափորոշիչները՝ համապատասխան տեղեկատվական անվտանգության և տվյալների կառավարման պահանջներին:	
4.	Համակարգի՝ վթարից վերականգնման պլան (Disaster Recovery Plan)	Համակարգը պետք է ապահովի ավտոմատ կրկնօրինակում, տվյալների վերականգնում, վթարային իրավիճակներում անխափան աշխատանք և արագ վերագործարկման մեխանիզմներ (Failover & Failback), ինչպես նաև համապատասխանի RTO (Recovery Time Objective) և RPO (Recovery Point Objective) սահմանված չափանիշներին:	



5.	Համակարգն ունի ֆայլերը վերծանելու, ծածկագրելու և ապածածկագրելու (encrypt, decrypt) ֆունկցիոնալ հնարավորություն	• Ֆայլերի գաղտնագրման և բանալիների օգնությամբ ֆայլերի վերծանման, ծածկագրման և ապածածկագրման ֆունկցիոնալ հնարավորություն: Անհրաժեշտ է կիրառել ժամանակակից գաղտնագրման ալգորիթմներ (AES), և բանալիների կառավարումն իրականացնել Key Management System-ի (KMS) միջոցով: Համակարգը պետք է ապահովի ծածկագրման և ապածածկագրման գործընթացների ավտոմատ իրականացում: • Համակարգը ապահովում է, որ բոլոր զգայուն տվյալները, ինչպես փոխանցման ընթացքում, այնպես էլ հանգստի վիճակում, գաղտնագրված լինեն առնվազն SHA 256 (Secure Hash Algorithm 256-bit) ալգորիթմով: Սա կանխում է չարտոնված անձանց կողմից տվյալների կարդալը կամ հասանելիությունը, նույնիսկ եթե դրանք որսան:	
6.	Լրացուցիչ անվտանգության միջոցներ (դերեր և իրավասություններ)	• Համակարգը կիրառում է բազմագործոնային վավերացում (MFA): Սա պահանջում է օգտվողներից տրամադրել երկու կամ ավելի վավերացման միջոցներ մուտք գործելու համար	



		(օրինակ՝ գաղտնաբառ + մեկանգամյա կոդ (OTP) էլ. նամակի կամ SMS-ի միջոցով): • Համակարգը պետք է ինտեգրվի այնպիսի MFA լուծումների հետ, որոնք ապահովում են օգտվողի նույնականացումը բջջային հավելվածի միջոցով, մասնավորապես՝ Push notification մեխանիզմի կիրառմամբ, OTP ծածկագրերի միջոցով: Վերոնշյալ տեսակի ծրագրային ապահովումներից են Openspan, Thales կամ համարժեք այլ լուծումներ, որոնք համապատասխանում են ոլորտային անվտանգության չափանիշներին: • Համակարգը կիրառում է դերահիմնավորված մուտքի կառավարում, որպեսզի սահմանափակվի մուտքը տվյալներին և համակարգի գործառույթներին՝ հիմնվելով օգտվողի դերերի վրա: Սա նվազեցնում է չարտոնված տվյալների հասանելիության և չարաշահման վտանգը: • Տրամադրում է օգտվողների գործունեության համապարփակ լոգագրում և մոնիտորինգ: Հետևում է մուտքագրման փորձերին, տվյալների փոփոխություններին և այլ կարևոր	
--	--	--	--



		գործողություններին՝ կասկածելի վարքագծերի և հնարավոր անվտանգային խախտումների հայտնաբերման համար: • Համակարգը պետք է ինտեգրվի Trellix SIEM (Security Information and Event Management) համակարգի հետ՝ ապահովելով բոլոր համապատասխան իրադարձությունների, գործողությունների և անվտանգության հետ կապված տեղեկամատյանների ավտոմատացված և անխափան փոխանցում դեպի SIEM:	
7.	Անընդհատության ապահովում	• <i>Կրկնօրինակություն (Redundancy):</i> Համակարգը պետք է աջակցի կրկնօրինակման բաղադրիչներին (օրինակ՝ սերվերներ, տվյալների բազաներ, պահեստավորումներ), որոնք վերացնում են խափանման մեկ կետը: Եթե մեկ բաղադրիչ խափանվի, մյուսը կարող է անմիջապես փոխարինել այն՝ շարունակական սպասարկում ապահովելու համար: • <i>Մոնիթորինգ և ահազանգեր:</i> Պրոակտիվ մոնիթորինգի և ահազանգման համակարգեր՝ աղմինիստրատորներին օգնելու համար	



		հայտնաբերել և արձագանքել հնարավոր խնդիրներին նախքան դրանք հանգեցնեն խափանումների: Սա օգնում է պահպանել համակարգի շարունակական մատչելիությունը և հուսալիությունը:	
--	--	--	--

ԱՌԴԻՏԻ ԵՆԹԱԿԱ ՊԱՅԱՆՁՆԵՐ

No.	Պահանջներ	Նկարագրություն
1.	Մուտք գործելու անհաջող փորձեր	Համակարգը սահմանափակում է կիրարկում օգտատիրոջ կողմից անվավեր մուտքի հաջորդական փորձերի որոշակի քանակի նկատմամբ: Մուտքի անհաջող փորձերի առավելագույն թվի գերազանցման պարագայում համակարգն ինքնաշխատ հետաձգում է մուտքի հաջորդ հուշումը, համաձայն համակարգի կարգաբերումների, կամ կողպում է հաշիվը, մինչև ադմինիստրատորն այն կարգելաբացի: Անհաջող փորձի առավելագույն թվի գերազանցման դեպքում անհրաժեշտ է նաև ներդրված լինի ծանուցման մեխանիզմ:
2.	Աշխատաշրջանների (սեանսների) դադարեցում	Համակարգն օգտատերերի միացման սեանսը ինքնաշխատ կերպով դադարեցնում է անգործության որոշակի ժամանակահատվածից հետո:



3.	Ինքնաշխատ նշագրումներ	Համակարգը, օգտագործելով անվանումների ստանդարտ պայմանաթղթեր, նշագրում է ելքային տվյալները՝ նույնացնելու համար տարածման, մշակման կամ բաշխման հատուկ հրահանգները:
4.	Աուդիտի իրադարձություններ ենթակա	Համակարգը գեներացնում է աուդիտային գրառումներ հետևյալ իրադարձությունների համար. • Հաշիվների ստեղծում, ակտիվացում, փոփոխում, վերանայում, անջատում և հեռացում: • Պաշտպանված օբյեկտների ստեղծում, փոփոխում և դրանց նկատմամբ հասանելիություն • Մուտքի և ելքի իրադարձություններ • Մուտքի և հասանելիության անհաջող փորձեր
5.	Աուդիտային բովանդակություն գրառումների	Համակարգն ապահովում է աուդիտային գրառումներ, որոնք բավարար տեղեկություններ են տալիս տեղի ունեցած իրադարձությունների, իրադարձությունների աղբյուրների, ինչպես նաև իրադարձությունների արդյունքների մասին: Աուդիտային գրառումների բովանդակությունը ներառում է. • իրադարձության ամսաթիվը և ժամը, • համակարգի բաղադրիչը, • իրադարձության տեսակը, • օգտատիրոջ/սուբյեկտի ինքնությունը,



		• իրադարձության արդյունքը/ելքը (հաջողում կամ ձախողում): • համակարգը հնարավորություն է տալիս, ըստ տեսակի, գտնվելու վայրի կամ սուբյեկտի, բացահայտված աուդիտորական իրադարձությունների մասին լրացուցիչ, ավելի մանրամասն տեղեկատվություն ներառելու աուդիտային գրառումներում: • Համակարգը հնարավորություն է տալիս ողջ համակարգի մասշտաբով կենտրոնացված կառավարելու առանձին բաղադրիչների կողմից գեներացված աուդիտային գրառումների բովանդակությունը:
6.	Արձագանք աուդիտի գործընթացի խափանումներին	Աուդիտի գործընթացի խափանումների դեպքում համակարգը ահազանգում է կազմակերպության համապատասխան պաշտոնատար անձանց: Աուդիտի գործընթացի խափանումներ են, օրինակ, ծրագրային/սարքավորումային սխալները, աուդիտորական գրանցումների մեխանիզմի խափանումները և աուդիտի պահեստային կարողությունների լրացումը կամ գերազանցումը: Համակարգը նախազգուշացում է տալիս, երբ աուդիտի գրառումների պահպանման հատկացված ծավալը հասնում է որոշակի սահմանված չափի:
7.	Աուդիտի ծավալի կրճատում և հաշվետվությունների գեներացում	Համակարգն ապահովում է աուդիտի ծավալի կրճատման և հաշվետվություններ գեներացնելու հնարավորություն: Համակարգը հնարավորություն է տալիս ինքնաշխատ մշակելու հետաքրքրություն ներկայացնող իրադարձությունների աուդիտորական գրառումներ՝ ելնելով իրադարձությունների չափորոշիչների ընտրովիությունից:



8.	Աուդիտային տեղեկությունների պաշտպանություն	Համակարգն ապահովում է աուդիտային տեղեկությունների և աուդիտի գործիքների պաշտպանությունը չարտոնված մուտքից, փոփոխումից և ջնջումից:
9.	Հերքման բացակայություն	Համակարգը հնարավորություն է տալիս որոշելու՝ արդյոք տվյալ անհատը կատարել է որոշակի գործողություն:
10.	Նվազագույն ֆունկցիոնալություն	Համակարգը պետք է ապահովի միայն էական կարողությունները կարգաբերելու հնարավորությունները և հատուկ արգելում և/կամ սահմանափակում է բոլոր ոչ անհրաժեշտ գործառույթների, սարքամուտքերի, պրոտոկոլների և/կամ ծառայությունների օգտագործումը:
11.	Փոխանցման ամբողջականություն	Համակարգը պաշտպանում է փոխանցվող տեղեկությունների ամբողջականությունը: համակարգը փոխանցման ընթացքում տեղեկատվության փոփոխությունները ճանաչելու համար գործադրում է ծածկագրային մեխանիզմներ, եթե տեղեկատվությունը պաշտպանված չէ այլընտրանքային ֆիզիկական միջոցներով:
12.	Փոխանցման գաղտնիություն	Համակարգը պաշտպանում է փոխանցվող տեղեկությունների գաղտնիությունը: Փոխանցման ընթացքում տեղեկատվության չարտոնված բացահայտումը կանխելու նպատակով համակարգը գործադրում է ծածկագրային մեխանիզմներ, եթե տեղեկատվությունը պաշտպանված չէ այլընտրանքային ֆիզիկական միջոցներով:
13.	Տվյալների գաղտնիություն և պաշտպանություն	Մատակարարը պետք է ապահովի Պայմանագրի շրջանակներում տրամադրված կամ մուտք գործած բոլոր տեղեկությունների խիստ գաղտնիությունը, ամբողջականությունը և անվտանգությունը, ներառյալ, բայց ոչ միայն՝ կարգավորող հաշվետվությունները,



վերահսկողական հարցումները, Փողերի լվացման և ահաբեկչության ֆինանսավորման (ՓԼ/ԱՖ) ու պատժամիջոցների համապատասխանության ռիսկերի գնահատումները, ինչպես նաև այլ զգայուն կամ հեղինակային տվյալները:

- Մատակարարին խստիվ արգելվում է որևէ իրական վերահսկողական տվյալների բացահայտումը, մշակումը, փոխանցումը, պատճենումը կամ որևէ այլ կերպ օգտագործումը՝ թեստավորման կամ համակարգի զարգացման նպատակներով:
- Համակարգի թեստավորման նպատակով պետք է օգտագործվեն բացառապես անանուն և արհեստական («կեղծ») տվյալներ, որոնք ստեղծվել կամ հաստատվել են Պատվիրատուի կողմից:
- Եթե անհրաժեշտ է տեղում թեստավորում, ապա Մատակարարի լիազորված ներկայացուցիչը պետք է ֆիզիկապես ներկա լինի Պատվիրատուի տարածքում և գտնվի լիազորված աշխատակիցների անմիջական վերահսկողության ներքո:
- Տվյալների ցանկացած չթույլատրված մուտք, բացահայտում, մշակում կամ չարաշահում կհանդիսանա պայմանագրի էական խախտում, որը կհանգեցնի պայմանագրի անմիջական լուծարմանը և պատասխանատվության՝ համաձայն գործող օրենսդրության:
- Մատակարարը պարտավոր է ստորագրել տվյալների գաղտնիության և չբացահայտման համաձայնագիր (NDA)՝ համակարգի համար նախատեսված միջավայր մուտք գործելուց առաջ:



14.	Անվտանգության թեսթավորում և ռիսկերի գնահատում	Մատակարարը պետք է տարեկան իրականացնի թափանցելիության թեստավորում (penetration testing) և խոցելիությունների գնահատում՝ ապահովելու համար, որ ՓԼ/ԱՖ համակարգը մնում է անվտանգ: Մատակարարը պարտավորվում է պահանջի դեպքում տրամադրել մանրամասն անվտանգության թեստավորման հաշվետվություններ: Ցանկալի է, որ համակարգը պաշտպանված լինի OWASP 10 և SANS/CWE 25 խոցելիություններից:
15.	Տվյալների հեռացում	Պայմանագրի լուծարման կամ օրենսդրությամբ սահմանված տվյալների պահպանման քաղաքականության համաձայն, բոլոր պահված տվյալները պետք է անվտանգ ջնջվեն՝ օգտագործելով ոլորտում ընդունված տվյալների մաքրման տեխնոլոգիաներ: Պետք է կիրառվի տվյալների վերականգնման անհնարինություն ապահովող մեթոդներ (DoD 5220.22-M, NIST 800-88):
16.	Տեղեկատվության ճշգրտություն, ամբողջականություն, վավերություն և իսկություն	Համակարգը ստուգում է տեղեկատվության ճշգրտությունը, ամբողջականությունը, վավերությունը և իսկությունը:
17.	Համակարգի բաղադրիչների գույքացանկ	Գույքագրում և Տեղեկատվություն Սեփականության Մասին: Մասնակիցը պետք է մշակի և տրամադրի համակարգի բոլոր բաղադրիչների ընթացիկ գույքացանկը, ներառյալ դրանց սեփականության կարգավիճակի վերաբերյալ համապատասխան փաստաթղթերը:



		• Բաց Ելքային Կոդով Ծրագրերի Օգտագործում: Ըստ քաղաքականության, բաց ելքային կոդով ծրագրերի (open-source software) օգտագործումը խորհուրդ չի տրվում, եթե դրանք չեն համապատասխանում անվտանգության և աջակցման պահանջներին: • Երրորդ Կողմի Ծրագրային Ապահովման Աջակցություն: Համակարգի բաղադրիչների մաս կազմող երրորդ կողմի ծրագրային ապահովումը (third-party software) պետք է լինի արդի, և դրանց աջակցման (support & maintenance) ժամկետը չպետք է լրացած լինի: Հնացած կամ անպաշտպան ծրագրային ապահովման օգտագործումը անթույլատրելի է:
18.	Համակարգի վերականգնում և վերակազմավորում	Հայտատուն տրամադրում է մեխանիզմներ՝ օժանդակ ընթացակարգերով, որոնք թույլ կտան համակարգը խափանումից կամ անսարքությունից հետո վերականգնել և վերակազմավորել հայտնի անվտանգ վիճակի: Հայտատուն համակարգի ամբողջական վերականգնումը և վերակազմավորումը ներառում է որպես արտակարգ իրավիճակների պլանի փորձարկման մաս:
19.	Համակարգի սպասարկման և քաղաքականություն ընթացակարգեր	Հայտատուն մշակում և տրամադրում է. (i) համակարգի սպասարկման քաղաքականության ֆորմալ, փաստաթղթային հենք, որով սահմանվում են նպատակը, շրջանակները, դերերը, և (ii) համակարգի սպասարկման քաղաքականության և դրա



		հետ կապված համակարգերի սպասարկման հսկողության իրականացումն ապահովող ֆորմալ, փաստաթղթավորված ընթացակարգեր:
20.	Ժամանակին սպասարկում	Հայտատուն սպասարկումն ու աջակցությունն ապահովում է համաձայնեցված ժամանակահատվածի համար:
21.	Համակարգի փաստաթղթեր	Հայտատուն լիազորված անձնակազմին համապատասխան փաստաթղթեր է տրամադրում համակարգի վերաբերյալ: Փաստաթղթերը ներառում են աղմինիստրատորի և օգտագործողի ուղեցույցներ, որոնք տեղեկատվություն են պարունակում՝ (i) համակարգի կարգաբերման, տեղակայման և շահագործման, և (ii) համակարգի անվտանգության առանձնահատկություններից արդյունավետորեն օգտվելու վերաբերյալ:
22.	Կոնֆիգուրացիայի Փոփոխությունների կառավարում	և Մատակարարը պետք է ներկայացնի, որ առաջարկվող պատրաստի համակարգը գտնվում է կոնֆիգուրացիայի և փոփոխությունների կառավարման պաշտոնական գործընթացի ներքո, ներառյալ անվտանգ թարմացումների իրականացումը, փոփոխությունների փաստագրված մատյանները և հիմնական փոփոխությունների կամ ուղղումների վերաբերյալ Պատվիրատուին ծանուցելու մեխանիզմը:
23.	Երրորդ կողմի լիցենզիա	Եթե առաջարկվող լուծման իրականացման համար անհրաժեշտ է երրորդ կողմի լիցենզիայի ձեռքբերում կամ օգտագործում, Կենտրոնական բանկը որևէ պարտավորություն չունի ընդունելու այդ մասով հայտատուի առաջարկը կամ կրելու դրա հետ կապված իրավական, ֆինանսական կամ տեխնիկական պարտավորություններ:



ԸՆԴՀԱՆՈՒՐ ՏԵԽՆԻԿԱԿԱՆ ՊԱՅԱՆՁՆԵՐ

No.	Պահանջներ	Նկարագրություն
1.	Համակարգում օգտագործվող ծրագրավորման կոդերը վերջին հնարավոր տարբերակներն են:	Թարմ ծրագրային ապահովում (Latest Software Versions) • Համակարգի ծրագրային կոդերը, տվյալների բազաները և ծրագրավորման ֆրեյմվորքները պետք է լինեն վերջին հասանելի կայուն տարբերակները: • Պետք է ապահովվի, որ համակարգի բոլոր բաղադրիչները ներկայումս աջակցվում են արտադրողների կողմից: Չպետք է օգտագործվեն դադարեցված կամ հնացած տեխնոլոգիաներ • Արգելվում է օգտագործել ծրագրային ապահովում, որի արտադրողը կամ մշակող խումբը պաշտոնապես հայտարարել է դրա աջակցման դադարեցման մասին (EOL - End of Life, EOS - End of Support): • Անվտանգության թարմացումներ չստացող ծրագրերը պետք է փոխարինվեն կամ թարմացվեն համապատասխան այլընտրանքներով: Համատեղելիություն և աջակցում



		• Օգտագործվող ծրագրերը պետք է ապահովեն ամբողջական համատեղելիություն համակարգի մյուս բաղադրիչների հետ: • Երրորդ կողմի ծրագրերը պետք է ունենան երկարաժամկետ աջակցության երաշխիքներ (Long-Term Support - LTS):
2.	Մատակարարը պետք է ներկայացնի համակարգի ներդրման պլան:	Ներդրման պլանն առնվազն ներառում է հետևյալը. ա) Համակարգի բաղադրիչների միացման և տեղադրության սխեման, բ) Ցանցային միացումների նկարագրությունը, գ) Տվյալների հոսքերի նկարագրությունը, դ) Կոնֆիգուրացիոն ֆայլերը և դրանց նկարագրությունը, ե) Համակարգի սպասարկման և գործունակության ապահովման համար երրորդ անձանց/մատակարարների կողմից մատակարարվող ռեսուրսների բաղադրիչների նկարագրությունը, ցանկը և անհրաժեշտ ծավալները:
3.	Մատակարարը պատվիրատուի մասնագետների մասնակցությամբ ձևավորում է «Փորձարկման» (Testing	



	Environment) և «Արտադրական» միջավայրեր (Production Environment):	
--	--	--

ՈՒՍՈՒՑՈՒՄ ԵՎ ՈՒՍՈՒՄՆԱԿԱՆ ՆՅՈՒԹԵՐ

No.	Պահանջներ	Նկարագրություն
1.	Փաստաթղթավորում (Բոլոր վերաբերելի գործառնություններն ու տեղեկատու ձեռնարկները և մյուս փաստաթղթերը, որոնք անհրաժեշտ են, որպեսզի ապահովեն ծրագրերի յուրաքանչյուր տարրն իր ողջ ներուժով շահագործելու նկարագրությունները, պետք է տրամադրվեն օգտատերերին:)	- Օգտագործողի ձեռնարկ: Պետք է տրամադրվի մանրամասն օգտագործողի ձեռնարկ, որը կբացատրի համակարգի հիմնական ֆունկցիոնալությունը: Այն պետք է ներառի քայլ առ քայլ հրահանգներ, համակարգի նավիգացիայի ուղեցույցներ և խնդիրների լուծման խորհուրդներ: - Ռիսկային մոդելների ուղեցույց: Պետք է տրամադրվի հատուկ ռիսկային մոդելների ուղեցույց, որը կներկայացնի, թե ինչպես է համակարգը հաշվարկում ռիսկերը, ինչպես կազմել ռիսկային պարամետրերը և ինչպես մեկնաբանել ռիսկային գնահատականները: - Ուսումնական ծրագիր: Համակարգի հետ պետք է տրամադրվի ուսումնական ծրագիր, որը կներկայացնի դասընթացների թեմաները և նյութերը՝ ներառելով թե՛ հիմնական օգտագործողի ուսուցում, և թե՛ առաջադեմ ռիսկային մոդելների տեխնիկաներ:



		• Առաջին մակարդակի աջակցման ուղեցույց: Պետք է տրամադրվի առաջին մակարդակի աջակցման ուղեցույց, որը կներկայացնի ընդհանուր խնդիրների լուծման քայլերն ու գործընթացները, ներառյալ՝ ◦ Համակարգային սխալների լուծման հիմունքներ ◦ Հաճախ տրվող հարցեր (FAQ) և օգտվողների ամենատարածված խնդիրների պատասխանները ◦ Հրահանգներ՝ խնդիրը բարձրացնել ավելի բարձր մակարդակի աջակցման համար • Տեխնիկական շահագործման ուղեցույց: Համակարգի օպերատորների և ադմինիստրատորների համար, գումարած՝ ժամանակացույցի պարբերաբար սպասարկում, տվյալների արխիվացում, մեխանիզմների վերականգնում, պահուստային կրկնօրինակում, խնդիրների վերացում և այլն: • API սահմանումներ: Պետք է հասանելի լինի API սահմանումների ամբողջական փաթեթը, որը կօգնի ծրագրավորողներին ինտեգրել ծրագրային լուծումը/հարթակը այլ համակարգերի հետ: Սա պետք է ներառի՝ ◦ API վերջնակետերի ամբողջական ցանկ ◦ Հավաստագրման պրոտոկոլները՝ արձանագրությունները ◦ Տվյալների ձևաչափի սահմանումները մուտք/ելքի համար ◦ Հարցումների և պատասխանների օրինակներ ◦ Rate limit և սխալների մշակման քաղաքականություն
--	--	---



		◦ Տեխնիկական սահմանափակումներ
2.	Համակարգի ադմինիստրատորի ուղեցույց	• Ծրագրի (կամ համակարգի) նշանակությունը և կիրառման շրջանակը, • ծրագրի կազմը, դրա շահագործման հիմնական սկզբունքները, • մատակարարման փաթեթը (եթե նշված չէ առանձին փաստաթղթում), • ծրագրի կամ դրա բաղադրիչների համակարգային պահանջները, • բաղադրիչների տեղակայման նախընտրելի հաջորդականությունը, • ծրագրի կամ դրա յուրաքանչյուր բաղադրիչի տեղակայման գործընթացը, • ծրագրի պարտադիր նախնական կարգաբերումների հերթականությունը, • բաղադրիչի տեղադրված պատճենների միմյանց ինտեգրման ուղիները, • ծրագրի ինտեգրումը, օրինակ՝ ծրագրային ապահովմանը, տվյալների բազայի սերվերին, • ծրագրի շահագործման ճշգրտության վերահսկման եղանակներն ու պարբերականությունը, • գործող ծրագրի պատճենների ընթացիկ պահպանման կարգը, • բոլոր հնարավոր օժանդակ խնդիրների լուծման կարգը, • արտակարգ իրավիճակները և դրանց հաղթահարման եղանակները, • ադմինիստրատիվ վահանակի օգտատիրոջ ինտերֆեյս



		• հրամանի տողի հարմարանքները և դրանց գործարկման շարակարգը, • կոնֆիգուրացիոն ֆայլերը և դրանք գրելու կանոնները, • control script գրելու լեզուն:
3.	Օգտատերերի/տեխնիկական թիմի ուսուցում,	Մատակարարը պարտավորվում է իրականացնել առաջին դասընթացները նախքան համակարգի ներդրումը՝ նախապատրաստելով անձնակազմին համակարգի սահուն շահագործմանը: Մասնավորապես՝ տեխնիկական թիմին առնվազն համակարգի գործարկման, APIs, կրկնօրինակման և պահպանման շրջանակներում, իսկ ՓԼ/ԱՖ թիմին՝ առնվազն ռիսկերի մոդելների, կանխարգելիչ համակարգի, վահանակների և հաշվետվողականության վերաբերյալ: Ցանկալի է նաև իրականացնել դասընթացներ բիզնես վերլուծաբանի և մենեջմենթի համար:
4.	Դասընթացները պետք է իրականացվեն տարեկան կտրվածքով՝ Ծառայություններ մատուցողի կողմից՝ ԿԲ պահանջով:	Մատակարարը (Ծառայություններ մատուցողը) պարտավորվում է իրականացնել տարեկան վերապատրաստման դասընթացներ, որոնք ուղղված են համակարգի արդյունավետ կիրառմանը, անվտանգության ապահովմանը և նոր գործառույթների յուրացմանը՝ Պատվիրատուի պահանջով:



ՓՈՐՁԱՐԿՈՒՄ/ԹԵՍՏԱՎՈՐՈՒՄ

No.	Պահանջներ	Նկարագրություն
1.	Տեղադրման վավերացում (Deployment validation)	Մատակարարը պետք է՝ - Տրամադրի բոլոր համապատասխան փաստաթղթերը (Մանրամասների համար տես Գլուխ 13), ներառյալ՝ տեղադրման ստուգման ցուցակը, կոնֆիգուրացիայի և ինտեգրման ապահովման փաստաթղթերը: Գնորդը պետք է՝ - Մատակարարի կողմից տրամադրված փաստաթղթերի հիման վրա իրականացնի համակարգի կոնֆիգուրացիան՝ վերահսկողական գործառույթների տրամաբանությանը և ռիսկերի մեթոդաբանությանը համապատասխան: - Հաստատի, որ ցանցային և ինտեգրման կետերը գործում են ըստ նախատեսվածի: - Վերանայի և հաստատի տրամադրված փաստաթղթերը: - Պաշտոնապես հաստատի պատրաստակամությունը ընդունման թեստավորման անցնելու համար՝ միայն տեղադրման հաջող վավերացումից հետո:



		Տեղադրման վավերացումը համարվում է հաջողված, եթե՝ • Համակարգի բոլոր բաղադրիչները աշխատում են և հասանելի են: • Տեղեկատվական անվտանգությունն ու ինտեգրացիան հաստատված են: • Կոնֆիգուրացիան համահունչ է վերահսկողական պահանջներին: • Չկան մնացած տեխնիկական խնդիրներ: • Բոլոր անհրաժեշտ փաստաթղթերը ներկայացված և հաստատված են Գնորդի կողմից:
2.	Ընդունման թեստավորում (QA+UAT) համաձայն ISO/IEC 12207, ISO/IEC 90003	Մատակարարը ներկայացնում է թեստավորման պլան, ներառյալ թեստավորման ուղեցույցը և ընդունման չափանիշները, որը հնարավորություն է տալիս գնահատել՝ արդյոք տեղադրված համակարգը համապատասխանում է Գնորդի բիզնես, ֆունկցիոնալ, արտադրողականության, անվտանգության և օգտագործելիության պահանջներին՝ հիմնվելով իրական վերահսկողական սցենարների և թեստային դեպքերի վրա: Մատակարարի պարտականություններ • Աջակցել Գնորդին թեստավորման ընթացքում՝ ◦ Օգնելով թերությունների գրանցման և դասակարգման գործընթացում ◦ Ապահովելով ժամանակին անսարքությունների վերացում և սխալների/թերությունների շտկում



		• Հետևել բոլոր խնդիրներին թերությունների/սխալների գրանցամատյանում՝ ներառյալ կարգավիճակ, լրջություն (severity), լուծման ամսաթիվ և վերաթեստավորման արդյունք: • Թեստավորման ավարտին տրամադրել ամփոփ հաշվետվություն՝ թեստավորման ծածկույթի և հայտնաբերված խնդիրների վերաբերյալ: Գնորդի պարտականություններ • Տրամադրել ամբողջությամբ գործունակ թեստային միջավայր՝ համահունչ արտադրական կոնֆիգուրացիային: • Իրականացնել վերահսկողական իրական դեպքերն արտացոլող թեստային սցենարներ (օր.՝ ռիսկի գնահատման ճշտում): • Վերանայել ստացված արդյունքները՝ վահանակներ (dashboards), ազդանշաններ/կարմիր դրոշակներ և հաշվետվություններ՝ ճշտության և համապատասխանության տեսանկյունից: • Գրանցել բոլոր արդյունքներն ու սխալները/թերությունները՝ համաձայն նախապես համաձայնեցված դասակարգման մեթոդաբանության (օր.՝ Կրիտիկական, Բարձր, Միջին, Ցածր): • Վավերացնել ոչ ֆունկցիոնալ հիմնական ասպեկտները՝ ներառյալ համակարգի արտադրողականություն, իրավասու մուտք, օգտագործելիություն: • Հաստատել, թե արդյոք յուրաքանչյուր պահանջ բավարարված է՝ ելնելով նախապես սահմանված ընդունման չափանիշներից (օր.՝ ակնկալվող
--	--	---



		միավորներ, աշխատանքային հոսքերի ճշգրտություն, հաշվետվությունների համապատասխանություն): <i>Թեստավորումը համարվում է «ընդունված», եթե՝</i> • Բոլոր բիզնես սցենարները լիարժեք աշխատում են՝ առանց սխալների/թերությունների: • Բաց սխալներ/թերություններ չեն մնացել: • Հաստատվել են արժեքային հատկանիշները՝ ֆունկցիոնալություն, արտադրողականություն, օգտագործելիություն, անվտանգություն և ինտեգրում: • Թեստավորման փաստաթղթերը, սխալների/թերությունների վերաբերյալ մատյանները և շտկման հաշվետվությունները վերանայված և հաստատված են Գնորդի կողմից:
3.	Թերությունների/սխալների շտկում	Յուրաքանչյուր խնդիր, որը գրանցվում է ընդունման թեստավորման (QA+UAT) ընթացքում, պետք է դասակարգվի ըստ լրջության մակարդակի. • Կրիտիկական (Critical) – Խոչընդոտում է AML/CFT համակարգի էական ֆունկցիոնալությունը (օր.՝ ռիսկի սխալ գնահատում, տվյալների ներմուծման ձախողում)



	• Բարձր (High) – Ազդում է հիմնական աշխատանքային հոսքերի վրա (օր.՝ ազդանշանի/կարմիր դրոշի սխալ էսկալացում, վահանակի անաշխատունակություն) • Միջին / Ցածր (Medium/Low) – Չխոչընդոտող (non-blocking) միջերեսի սխալներ կամ առաջարկներ <i>Թերությունների/սխալների շտկում: Մատակարարը պարտավոր է՝</i> • Կիրառել տեխնիկական շտկումներ • Օպտիմալացնել կոնֆիգուրացիաներն ու պարամետրերը • Թարմացնել API-ները կամ ինտեգրացիաները՝ անհրաժեշտության դեպքում <i>Վերաթեստավորում և փակման գործընթաց</i> • Շտկումները տեղակայելուց հետո Գնորդը կրկին իրականացնում է ձախողված սցենար(ներ)ի թեստավորում՝ խնդրի լուծումը հաստատելու նպատակով: • Փակումը թույլատրվում է միայն Գնորդի կողմից հաստատման և փաստաթղթավորված վերաթեստավորման հաջող արդյունքի պարագայում:
--	---



		Թերությունների/սխալների շտկման փուլը համարվում է հաջողությամբ ավարտված (ընդունված), եթե՝ • Բոլոր թերությունները/սխալները փակված են և հաստատված Գնորդի կողմից: • Վերաթեստավորման ընթացքում նոր թերություններ չեն ի հայտ եկել: • Բոլոր հարցերը փաստաթղթավորված են: • Թարմացված թերությունների մատյանը հաստատված է Գնորդի կողմից:
4.	Փորձնական շահագործում (Pilot run)	Փորձնական շահագործման փուլը պետք է կենտրոնանա վերահսկողական գործընթացների աշխատանքային հոսքերի վավերացման վրա՝ օգտագործելով իրական տվյալներ: Որպես կանոն, ընդգրկվում են հետևյալ հիմնական բաղադրիչները՝ • Ռիսկի գնահատման տրամաբանություն և ազդանշանային շեմեր • Կարմիր դրոշակների գեներացում և վահանակներ • Վիզուալիզացիա/Հաշվետվությունների ձևավորում Փորձնական շահագործումը նպատակ չունի համակարգի բոլոր ֆունկցիոնալ հնարավորությունների ամբողջական թեստավորում կատարելու, այլ՝ ապահովելու, որ վերահսկողական հիմնական տրամաբանությունը գործում է



		ճշգրտորեն, և օգտվողները կարող են կատարել իրենց կարևոր գործառնությունները: Փորձնական շահագործումը համարվում է հաջողված («ընդունված»), եթե՝ • Վերահսկողները կարողանում են ամբողջությամբ իրականացնել աշխատանքային հոսքերը՝ առանց էական խոչընդոտի կամ ձախողման: • Փորձարկման ընթացքում չեն արձանագրվում ռիսկի գնահատման տրամաբանության կրիտիկական սխալներ կամ համակարգային խափանումներ: • Օգտվողները հաստատում են հիմնական արժեքային չափորոշիչների (օրինակ՝ ֆունկցիոնալություն, օգտագործելիություն, ռիսկի գնահատում, նավիգացիա) բավարար լինելը:
5.	Շահագործման պատրաստականության հաստատումը (Go-Live Readiness Sign-Off)	Նախքան շահագործման պատրաստականության հաստատումը, պետք է ամբողջությամբ ավարտվեն և հաստատվեն հետևյալ փուլերը՝ • Տեղադրման վավերացում (Deployment Validation) ▪ Բոլոր մոդուլները տեղադրված են, կոնֆիգուրացված և հասանելի • Օգտագործողի ընդունման թեստավորում (QA+UAT) ▪ Բոլոր ֆունկցիոնալ և ոչ ֆունկցիոնալ պահանջները վավերացված են • Թերությունների շտկում (Defect Resolution) ▪ Բոլոր խնդիրները փակված են



	• Փորձնական շահագործում (Pilot run) ▪ Կրիտիկական/հիմնական աշխատանքային հոսքերը ցուցադրված են իրական օգտատերերի կողմից • Վերապատրաստման ավարտ (Training Completion) <i>(տե՛ս Գլուխ 13 մանրամասների համար)</i> ▪ Վերջնական օգտվողների վերապատրաստում՝ վերահսկողների, վերլուծաբանների և ադմինիստրատորների համար • Փաստաթղթերի տրամադրում (Documentation Delivered) ▪ Տեխնիկական ճարտարապետություն, կոնֆիգուրացիայի ամփոփումներ, օգտագործողի ձեռնարկներ և ստանդարտ գործողությունների ընթացակարգեր (SOPs) Հաջողության պայման (Pass Condition): Գնորդը ստորագրում է շահագործման պատրաստակամության հաստատման ակտը՝ հաստատելով, որ լուծումը բավարարում է բոլոր գործառնական չափանիշներին և պատրաստ է շահագործման: Ձախողման պայման (Fail Condition): Չշտկված թերությունները, բաց փաստաթղթերը կամ թեստավորման բացթողումները խոչընդոտում են համակարգի գործարկմանը:
--	--



--	--	--

ՏԵԽՆԻԿԱԿԱՆ ԱԶԱԿՑՈՒԹՅԱՆ ՊԱՅԱՆՁՆԵՐ

No.	Պահանջներ	Նկարագրություն
1.	Մատակարարի աջակցության շրջանակներում միջինում 5 տարիների ընթացքում մատակարարը պետք է ապահովի համակարգի սպասարկումը:	- Տեխնիկական աջակցություն և սպասարկում - Համակարգի թարմացումներ և օպտիմալացում - Անվտանգության Աջակցություն - Օգտատերերի աջակցություն և դասընթացներ - Պարբերական հաշվետվություն և SLA (Service Level Agreement) պահպանություն: SLA-ն պետք է ներառի արձագանքման կոնկրետ ժամանակներ (օրինակ՝ սխալների ուղղման հաստատված ժամկետներ երաշխիքային ժամանակահատվածում):
2.	Կիրառական ելքային կոդն իր լրիվ ու ամբողջական կազմով և ուղեկցող մանրամասն փաստաթղթերը Մատակարարի կողմից պետք է տրամադրվեն Գնորդին՝ ծրագրերի մշակման համապատասխան բոլոր	Գնորդը պետք է ստանա ամբողջական և փոփոխելի ելքային կոդը (ներառյալ՝ Dependencies և configurations), որը թույլ կտա նրան ապագայում կատարել ծրագրային փոփոխություններ, տեղակայում և ադապտացիա



	գործիքների և հարմարությունների օրինակի հետ միասին, եթե այդպիսիք կան, որոնք պահանջվում են կիրառական ծրագրերը փոփոխելու, վերակազմելու, տեղակայելու, փորձարկելու և արտադրական միջավայր փոխադրելու համար:	Մատակարարը պետք է տրամադրի բոլոր անհրաժեշտ ուղեկցող փաստաթղթերը, որոնք կօգնեն տեխնիկական թիմին լիարժեքորեն հասկանալ և կառավարել համակարգը:
3.	Տեխնիկական աջակցությունը պետք է հասանելի լինի երեք մակարդակով:	Առաջին մակարդակ (Ներքին աջակցություն, որն ապահովում է Գնորդը). բավարար ծավալի ուսուցումը, ինչպես և համապատասխան բոլոր ելքային կոդերը և փաստաթղթերն անհրաժեշտ են, որպեսզի Գնորդի ՏՏ անձնակազմին հնարավորություն տրվի ապահովելու այս առաջին մակարդակի աջակցությունը համակարգի շահագործման և մասնակիցների ու հաճախորդների կողմից ներկայացված խնդիրներին լուծում տալու համար: Երկրորդ մակարդակ (Հեռակա աջակցություն, որն ապահովում է Մատակարարը). Մատակարարն անհրաժեշտ աջակցությունը և սպասարկումն ապահովում է հեռահար հաղորդակցության միջոցներով, ինչպիսիք են հեռակա մուտքի եղանակը, էլ. փոստը, հեռախոսը և հեռակառավարման ծրագրային միջոցները: Երրորդ մակարդակ (Տեղում տրամադրվող աջակցություն Մատակարարի կողմից). Հայաստանում Մատակարարը պարտավոր է հասանելի լինել



		ողջամիտ ժամկետներում և ցուցաբերել արագ փորձագիտական աջակցություն, ինչը կարող է հանգեցնել ծախսված ժամանակի և գումարների, որոնք ներառվում են գնառաջարկի մեջ:
4.	Երաշխիքային և օպերատիվ աջակցություն.	Մատակարարը սահմանված երաշխիքային ժամանակահատվածում մատակարարվող բոլոր լուծումային բաղադրիչների համար տրամադրելու է երաշխիք, որը համահունչ է համագործակցող ցանկացած դուստր մատակարարի կողմից տրված առավելագույն երաշխիքային ժամկետներին կամ դրանցից ավելի երկար է: Սահմանված երաշխիքային ժամանակահատվածում Մատակարարը հանդես է գալու որպես Գնորդի գործակալ՝ մատակարարի կողմից մատակարարված և երաշխավորված որևէ բաղադրիչի մասով շտկումներ պահանջելու համար, ընդ որում՝ երաշխիքի ներքո գտնվող բաղադրիչները շտկվելու են առանց Գնորդից որևէ հավելյալ վճար գանձելու: Կիրառական ծրագրերի համար տրվող երաշխիքը գործելու է պաշտոնապես Ընդունման թեստավորման ավարտին արձանագրված պաշտոնական Ընդունման ամսաթվի պահից (տեղադրման ամբողջական հավաստիացումից հետո) մեկ տարվա համար: Երաշխիքային ժամանակահատվածում Մատակարարը, անհրաժեշտության դեպքում, տեղում օպերատիվ աջակցություն է տրամադրելու՝ Գնորդի



		օպերացիոն թիմ գործուղելով առնվազն մեկ մասնագետի (ով ուղղակիորեն մասնակցել է ծրագրային ապահովման գործարկման աշխատանքին):
5.	Տեխնիկական սպասարկում	Գնորդը խորհրդատվություն պետք է ստանա զարգացման միջավայրի հետ կապված նոր առանձնահատկությունների, ապավինման աղբյուրների և հարակից տեխնոլոգիական պահանջների վերաբերյալ՝ ի ապահովումն նրա, որ Գնորդը տնօրինում է Համակարգի հուսալի և անընդհատ շահագործումը երաշխավորելու համար բավարար գործիքների և կարողությունների ամբողջական և համապատասխան լրակազմը: Մատակարարը պարտավորվում է ապահովել Երկրորդ մակարդակի տեխնիկական աջակցության սպասարկում, որը գործելու է երաշխիքային ժամանակահատվածի ավարտին հաջորդող օրվանից առնվազն 5 (հինգ) օրացուցային տարվա համար: Տեխնիկական սպասարկման ժամանակահատվածում Մատակարարը պետք է իր լավագույն ջանքերը գործադրի և օգնի Գնորդին՝ ձեռք բերելու ծրագրային ապահովման լավարկման (թերությունների վերացում, շտկում), խնդիրների վերհանման ու լուծման և, անհրաժեշտության դեպքում, տեխնիկական օգնության բնագավառում համապատասխան գիտելիքներ, կարողություններ և փորձ: Մատակարարը պետք է տեղում ստուգումներ և կանխարգելիչ սպասարկում իրականացնի գնորդի խնդրանքով, որի դիմաց գնորդը կվճարի:



		Սպասարկման ժամանակահատվածում Մատակարարն ընդունում է Երրորդ մակարդակի տեխնիկական աջակցություն տրամադրելու վերաբերյալ Գնորդի խնդրանքը:
6.	Փաստաթղթերի թարմացում	Ամբողջ մանրամասն տեխնիկական բնութագրերը, ներառյալ՝ բոլոր թարմացումները, լրացումները և այլ փոփոխություններ, Գնորդին տրամադրվելու են նախքան թեստային կամ արտադրական միջավայրում որևէ այդպիսի թարմացում, լրացում կամ այլ փոփոխություն իրականացնելը: Ընդունված բոլոր միջազգային և արդյունաբերական ստանդարտները և ընդունված կամ կիրառվող տեղական ստանդարտները պետք է հստակորեն վկայաբերվեն և ուղեկցվեն համանման ստանդարտների մանրամասն բնութագրերի բովանդակ լրակազմով: Մանրամասն և թարմացված փաստաթղթերը կարող են տրամադրվել նաև հայերենով: Մատակարարի տեղական տեխնիկական աջակցության գործակալը, եթե այդպիսին կիրառելի է, պետք է տեղեկացված և քաջածանոթ լինի Գնորդի տնօրինության տակ եղած տեխնիկական փաստաթղթերին և սարքերի ու համակարգի ծրագրային ապահովման միջավայրին:



ՀԱՄԱԿԱՐԳԻ ՇԱՀԻԿԱՍԱՐԻ ՆԵՐԿԱՅԱՑՄԱՆ ՊԱՅԱՆՁՆԵՐ

Հայտատուն պետք է ապահովի նաև համակարգի ամբողջական ներկայացում շահիկասարի միջոցով:

ՆԱԽԱՏԵՍՎՈՂ ԺԱՄԿԵՏՆԵՐԸ

Սույն Նախագծի իրականացման վերջնաժամկետ է համարվում պայմանագիրը կնքելուց հետո վեց ամսյա ժամկետը, որը փոխադարձ փոխադարձ համաձայնությամբ կարող է երակարաձգվել: Մասնակիցը հայտով ներկայացնում է մանրամասն ժամանակացույց՝ առնվազն ներառելով ստորև ներկայացված ակնկալվող արդյունքները.

ԱԿՆԿԱԼՎՈՂ ԱՐԴՅՈՒՆՔՆԵՐԸ

Համակարգի ներդրման ժամանակացույց (ըստ յուրաքանչյուր գործընթացի)

Նախագծի իրականացում

Դասընթացի ժամանակացույց

Վերջնական ընդունում հանձնում

Երաշխիքային սպասարկում

Մատակարարը պետք է տրամադրի Նախագծի կառավարման պլանը և Նախագծի իրականացման ժամանակացույցը:

Մատակարարը, անհրաժեշտության դեպքում, պետք է ֆիզիկապես ներկա գտնվի Համակարգի ներդրման, հանձնման-ընդունման, թեստավորման, ուսուցման փուլերում:

ԳՆԱՀԱՏՄԱՆ և ՈՐԱԿԱՎՈՐՄԱՆ ՉԱՓՈՐՈՇԻՉՆԵՐ

1. ՄԱՍՆԱԿԻՑՆԵՐԻ ՈՐԱԿԱՎՈՐՄԱՆ ՉԱՓԱՆԻՇՆԵՐԸ

Մասնակցության իրավունքից բացի, Մասնակիցը պետք է բավարարի հետևյալ որակավորման նվազագույն չափանիշներին.

1.1. Առնվազն 3 տարվա փորձ ՓԼ/ԱՖ և պատժամիջոցների համապատասխանության ռիսկերի գնահատման ավտոմատացման և առաջադեմ վերահսկողական տեխնոլոգիական (SupTech) լուծումների ներդրման բիզնեսում՝ որպես գրանցված ընկերություն/սուբյեկտ: Նմանատիպ համակարգերի ներդրման հաջող փորձ այլ կարգավորող մարմիններում՝ պահանջվող չափանիշներին (օրինակ՝ FATF 40 առաջարկություններին) համապատասխան:



Որպես ապացույց ներկայացվում է կազմակերպության պորտֆոլիոն, հայտը ներկայացնելուն նախորդող երեք տարիների ընթացքում պարշաճ ձևով ներդրված համակարգերի մասին տեղեկատվություն՝ ներառելով պարզիկապարզ գործունեության ոլորտը, իրականացման ժամկետները և ծավալը:

Մասնակիցը ներկայացնում է նախկին պարզիկապարտությունների կողմից տրամադրված երաշխավորության նամակ այն մասին, որ համակարգը հաջողությամբ ներդրված է, գործում է և համապատասխանում է պահանջվող չափանիշներին:

1.2. Մասնակիցը պետք է հատկացնի համապատասխան անձնակազմ՝ պահանջվող առաջադրանքները կատարելու և Պայմանագրի նպատակներին ժամանակային և որակային առումներով հասնելու համար: Նախագծի իրականացման համար ներգրավված անձնակազմը պետք է ունենա համապատասխան որակավորում , աշխատանքային փորձ (առնվազն 5 տարի), նմանատիպ նախագծեր իրականացնելու հմտություններ և ապահովի աշխատանքների իրականացման բարձր որակ: Մասնակիցը պետք է տրամադրի փորձագետների թիմ, որը տիրապետում է AML/CFT համապատասխանության, կարգավորող հաշվետվությունների, ծրագրային ինտեգրման, կիբերանվտանգության և համակարգի աջակցության ոլորտներին:

Որպես ապացույց՝ ներկայացվում է հիմնական փորձագետների ինքնակենսագրականները (այդ թվում՝ որակավորումները հավաստող փաստաթղթերը), որտեղ հստակ պետք է նշվի համապատասխան աշխատանքային փորձը՝ համապատասխան տարիներով: Թիմի անդամները պետք է առնվազն տիրապետեն անգլերենին (ցանկալի է նաև ռուսերեն):

2. ՀԱՅՏԻ ՆԵՐԿԱՅԱՑՄԱՆ ՊԱՀԱՆՋՆԵՐ

2.1. Գնային առաջարկը

- 1) Գնային առաջարկը պետք է ներառի համակարգի ներդրման ընդհանուր գինը, ինչպես նաև ներդրումից հետո ակնկալվող ծախսերը 5 տարիների կտրվածքով, ներառյալ՝ ներդրման, տեղակայման, գործարկման, ուսուցման, սպասարկման, ուղեկցման, անձնակազմի, անհրաժեշտության դեպքում ՀՀ գործուղման և այլ անհրաժեշտ գները (համաձայն Հավելված 3-ի, որը հավասար է Հավելված 3.1-ի և Հավելված 3.2-ի հանրագումարին):
- 2) Մասնակիցը Հավելված 3.1-ով ներկայացնում է համակարգի ներդրման մանրամասն բացվածք, որում պետք է մանրամասն ներկայացնել առաջարկվող յուրաքանչյուր բաղադրիչի միավորի և ընդամենը գները:



- 3) Մասնակիցը առանձին բացվածքով (Հավելված 3.2-ով) ներկայացնում է համակարգի ներդրումից հետո ակնկալվող ծախսերը (ներառյալ դրանց հետերաշխիքային սպասարկման, ուղեկցման և այլ անհրաժեշտ ծախսերը) 5 տարիների կտրվածքով՝ հաշվի առնելով առնվազն մեկ տարի երաշխիքային սպասարկման պայմանը, ինչպես նաև վճարման պայմանները, ժամանակացույցը և կարգը:
- 4) Մասնակիցը կարող է առանձին ներկայացնել նաև լրացուցիչ առաջարկներ, եթե այդպիսիք կան, որի ընտրությունը կկատարվի պատվիրատուի հայեցողությամբ:

2.2. Տեխնիկական առաջարկը

- 1) Մասնակիցը հայտով տրամադրում է առաջարկվող Համակարգի մանրամասն նկարագիրը, մասնավորապես՝
 - Տեխնիկական առաջադրանքով սահմանված պահանջներին բավարարող Տեխնիկական առաջարկ, ներառյալ անվտանգության համապատասխանություն միջազգային ստանդարտներին, օգտագործելիության առանձնահատկություններ, ինչպիսիք են օգտագործման պարզությունը, կառավարման և զարգացման/կատարելագործման պարզությունը, համատեղելիությունը գոյություն ունեցող ենթակառուցվածքների հետ և այլ անհրաժեշտ տեղեկատվություն,
 - համակարգի երաշխիքային և հետսպասարկման պայմանները,
 - մասնակցի կողմից իրագործման ճանապարհային քարտեզը, մանրամասն ժամանակացույցը,
 - Ուսուցման մեթոդաբանությունը, ժամանակացույցը և անհրաժեշտ այլ պայմանները:
 - Այլ անհրաժեշտ տեղեկատվություն, որը մասնակիցը կգտնի նպատակահարմար՝ իր կողմից ներկայացված առաջարկը լավագույնս ներկայացնելու/բնութագրելու համար:
- 2) ծրագրային ապահովումների համար պետք է ներկայացվի Արտադրող ընկերության կամ նրա պաշտոնական ներկայացուցչության կողմից տրված ՀՀ տարածքում տվյալ մատակարարման իրավունքի վերաբերյալ հեղինակայնացման հավաստագիր (MAF - Manufacturers Authorisation Form):
- 3) Տեղեկատվություն ՀՀ-ում արտադրողի կողմից հավաստագրված սպասարկման մասնագիտացված կենտրոնի առկայության կամ արտադրողի կողմից սպասարկումը միասնական կենտրոնի կողմից իրականացնելու մասին: Սպասարկման մասնագիտացված կենտրոնների տվյալները պետք է նշված լինեն արտադրողի վեբ-կայքում կամ հաստատվի համապատասխան սերտիֆիկատներով:



- 4) Տեղեկատվություն երաշխիքի ժամկետի և աշխատունակության վերականգնման ժամկետի վերաբերյալ,
- 5) Կազմակերպության գրանցման վկայականը,
- 6) Մասնագիտական փորձառության վերաբերյալ համապատասխան տեղեկանք համաձայն սույն հրավերին կից Հավելված 5-ի,
- 7) Անհրաժեշտ աշխատանքային ռեսուրսների առկայության մասին տեղեկանք համաձայն սույն հրավերին կից Հավելված 6-ի,
- 8) Տեղեկատվական և կիբեռանվտանգության միջազգային ստանդարտների պահանջներին համապատասխանության սերտիֆիկատներ (ISO: 27001),

3. Առաջարկների գնահատումը

Հայտերի գնահատման ժամանակ, բացի գնային առաջարկից, հաշվի են առնվում նաև ոչ գնային պայմանները: Այս մեթոդաբանության մեջ **ոչ գնային չափանիշների և Տեխնիկական առաջարկի կշիռը 70% է, իսկ գնային առաջարկի կշիռը՝ 30%:** Պայմանագրի կնքման չափանիշ է ոչ գնային և գնային չափանիշների կշիռների ամենաբարձր համակցված միավորը:

Համեմատվում են բոլոր այն մասնակիցների գնային առաջարկները, որոնք տեխնիկական գնահատման արդյունքում 100 միավորից կհավաքեն նվազագույնը 70 միավոր:

Ընդհանուր տեխնիկական միավորը (SU) գնահատված բոլոր տեխնիկական հատկանիշների համակցված կշռված միավորն է:

Գնահատման չափորոշիչներ	Կշիռ %	Առավելագույն միավոր
Տեխնիկական առաջարկի գնահատում	70	
Առաջարկվող լուծման համարժեքություն, կարգավորման համապատասխանություն և նորարարություն		30
Համակարգի տեխնոլոգիական մոտեցում/լուծում և համապատասխանություն միջազգային ՓԼ/ԱՖ հայեցակարգերի պահանջներին (օրինակ՝ FATF)		20
Օգտագործողի միջերեսի (UI/UX) մատչելիություն, հեշտ նավիգացիա և վահանակների արդյունավետություն (Հայերեն լեզվով հասանելիությունը և/կամ WCAG 2.1-ին համապատասխանությունը կդիտվի առավելություն)		5



• Իրագործման ճանապարհային քարտեզ, մեթոդաբանություն և ոլորտների կառավարման ռազմավարություն		5
Ենթակառուցվածքներ և ծրագրային տեխնոլոգիական ապահովում		20
• Համակարգի անվտանգության համապատասխանություն ISO 27001 պահանջների շրջանակին և աղետի վերականգնման մեխանիզմներ, բարձր հասանելիություն (կրկնօրինակում և վերականգնում)		10
• Գործող ենթակառուցվածքների/էկոհամակարգերի հետ առավելագույն համատեղելիություն		5
• Երաշխիքային, հետերաշխիքային սպասարկման պայմաններ		5
Մատակարարի փորձառություն և արդյունաբերության վարկանիշ		20
• Առնվազն 3 տարվա փորձ ՓԼ/ԱՖ/SupTech կամ ֆինանսական SCS համապատասխանության լուծումներում, ՓԼ/ԱՖ կարգավորող նախագծերի հաջող իրականացում տարբեր իրավասությունների կարգավորող մարմիններում (նախընտրելի է cross-border փորձառություն)		16
• Վստահելի գործընկերոջ հավաստագրեր / երաշխավորագրեր		4
Հիմնական անձնակազմի փորձառություն և լուծման ներդրման թիմի հմտություններ		10
• Անձնակազմի համապատասխանության հավաքական գնահատական		10
Ուսուցում և ուսումնական նյութեր		10
• Ուսուցման հայեցակարգ և ուսումնական նյութեր		10
Համակարգի պրեզենտացիա		10
• Համակարգի ամբողջական պրեզենտացիա		10
Տեխնիկական մասով ընդհանուր միավորներ		100



ՀԱՏՈՒԿ ՊԱՅՄԱՆՆԵՐ

1. Ծրագրային ապահովումների բոլոր բաղադրիչները պետք է ապահովված լինեն բաժանորդագրությամբ՝ տեղադրման օրվանից առնվազն 5 տարի ժամկետով:
2. Արտադրողի կայքում չպետք է լինի տեղեկատվություն արտադրողի կողմից առաջարկվող ծրագրային ապահովումների երաշխիքային սպասարկման (end of support) և շահագործման վերջնաժամկետի ավարտի վերաբերյալ (end of life),
3. Տեխնիկական աջակցում՝ 24x7 ռեժիմում հայտ գրանցելու հնարավորությամբ (անհրաժեշտության դեպքում նաև արտադրողի համակարգում), պատահար (սերվիս-դեպք) գրանցելու հնարավորությամբ և առավելագույնը 4-ժամյա հետադարձ կապով:
4. Համակարգի ներդրման ամսաթիվը համարվում է վերջնական հանձնման-ընդունման ակտի ստորագրման ամսաթիվը: Նույն ամսաթիվը պետք է դիտարկվի սպասարկման և/կամ աջակցման ծառայությունների երկարաձգման համար և այլն, եթե կիրառելի է:
5. Պատվիրատուն գնային համեմատության նպատակով կարող է հաշվի առնել նաև կամընտիր կետերը (եթե պահանջվում է սույն տեխնիկական առաջադրանքով): Պատվիրատուն կարող է որոշել օգտվել կամընտիր կետերից պայմանագրի ընթացքում ըստ անհրաժեշտության՝ նույն արժեքով:

ՊԱՅՄԱՆԱԳՐԱՅԻՆ ՊԱՅՄԱՆՆԵՐ

1. Պայմանագիրն ուժի մեջ է մտնում Կողմերի կողմից ստորագրման պահից և գործում է մինչև կողմերի՝ պայմանագրով ստանձնած պարտավորությունների ողջ ծավալով կատարումը, ընդ որում, Պայմանագրով ստանձնած պարտավորությունների ողջ ծավալով կատարման վերջնաժամկետ սահմանվում է՝ պայմանագիրը կնքելուց հետո վեց ամսյա ժամկետը՝ կողմերի համաձայնությամբ երկարաձգման հնարավորությամբ:
2. Համակարգի ներդրումը համարվում է ավարտված և Պատվիրատուի կողմից ընդունված ավարտական հանձնման-ընդունման ակտը երկկողմանի ստորագրվելուց հետո:
3. Համակարգի ներդրման աշխատանքների ընդունումն իրականացվում է նախապես փոխադարձ համաձայնեցված և հաստատված ժամանակացույցով, հետևյալ կարգով.
 - Պատվիրատուն համակարգը (կամ առանձին ենթահամակարգերը) ներդնելուց հետո նախապես փոխադարձ համաձայնեցված և հաստատված ժամանակացույցով սահմանված ժամանակահատվածում ուսումնասիրում է իրականացված աշխատանքների որակն ու համապատասխանությունը Պայմանագրում նշված պահանջներին և ,թերությունների բացակայության դեպքում, ստորագրում է հանձնման-ընդունման համապատասխան ակտ/երը: Թերությունների հայտնաբերման դեպքում Կատարողը պարտավոր է թերություններն իր հաշվին վերացնել տասն աշխատանքային օրվա ընթացքում, որից հետո նոր միայն ստորագրվում է համապատասխան հանձնման-ընդունման ակտը:



4. Վճարումն իրականացվում է համապատասխան հերթական հանձնման-ընդունման ակտ/երը Կողմերի կողմից ստորագրվելուց և Կատարողի կողմից համապատասխան հարկային հաշվի դուրս գրման պահից՝ 5 աշխատանքային օրվա ընթացքում:
5. Համակարգի ներդրումից հետո ակնկալվող հետերաշխիքային սպասարկման Ծառայությունների մատուցումը, հանձնում-ընդունումը, անձնակազմի ուսուցման հետ կապված վճարումները սահմանվում են Պայմանագրով:
6. Կատարողի կողմից Պայմանագրով նախատեսված ժամկետների խախտման դեպքում Կատարողից Ծառայության մատուցման յուրաքանչյուր ուշացված աշխատանքային օրվա համար գանձվում է տույժ՝ կատարման ենթակա, սակայն չկատարված աշխատանքների (չմատուցված Ծառայության) գնի 0,1 տոկոսի չափով՝ կիրառելով միայն օրենքով նախատեսված տարեկան առավելագույն չափի սահմանափակումները:
7. Պատվիրատուի կողմից Պայմանագրով նախատեսված վճարման ժամկետի խախտման համար Պատվիրատուի նկատմամբ պարտավորությունների կատարման յուրաքանչյուր ուշացված աշխատանքային օրվա համար հաշվարկվում է տույժ՝ վճարման ենթակա, սակայն չվճարված գումարի 0,1 տոկոսի չափով՝ կիրառելով միայն օրենքով նախատեսված տարեկան առավելագույն չափի սահմանափակումները:
8. Կատարողի կողմից Պատվիրատուին վճարման ենթակա տույժերը Պատվիրատուն իրավունք ունի անակցեպտ գանձելու պայմանագրին համապատասխան Կատարողին վճարման ենթակա գումարներից: