***პროექტი***

**საქართველოს ეროვნული ბანკის პრეზიდენტის**

**ბრძანება**

**ფინანსური ორგანიზაციების მიერ ღრუბლოვანი აუთსორსინგული მომსახურების გამოყენების სახელმძღვანელოს დამტკიცების თაობაზე**

„საქართველოს ეროვნული ბანკის შესახებ“ საქართველოს ორგანული კანონის მე-15 მუხლის პირველი პუნქტის „ზ“ ქვეპუნქტისა და 48-ე მუხლის მე–3 პუნქტის შესაბამისად, **ვბრძანებ:**

**მუხლი 1.** დამტკიცდეს ფინანსური ორგანიზაციების მიერ ღრუბლოვანი აუთსორსინგული მომსახურების გამოყენების სახელმძღვანელო თანდართული რედაქციით.

**მუხლი 2.** მიკრობანკებზე ამ სახელმძღვანელოს მოქმედება გავრცელდეს 2023 წლის 1 ივლისიდან.

**მუხლი 3.** ეს ბრძანება ამოქმედდეს გამოქვეყნებისთანავე.

**საქართველოს ეროვნული ბანკის პრეზიდენტის**

**მოვალეობის შემსრულებელი *არჩილ მესტვირიშვილი***

**ფინანსური ორგანიზაციების მიერ ღრუბლოვანი აუთსორსინგული მომსახურების გამოყენების სახელმძღვანელო**

**მუხლი 1. დოკუმენტის მიზანი და გავრცელების სფერო**

1. ამ სახელმძღვანელოს მიზანია ხელი შეუწყოს ფინანსურ ორგანიზაციებს ღრუბლოვან აუთსორსინგულ მომსახურებასთან დაკავშირებული რისკებისა და გამოწვევების იდენტიფიცირებაში, გამკლავებასა და მონიტორინგში, რაც მოიცავს აუთსორსინგის შესახებ გადაწყვეტილების მიღებას, ღრუბლოვანი მომსახურების მომწოდებლის შერჩევას, ღრუბლოვანი აუთსორსინგული საქმიანობის მონიტორინგს, მომსახურებიდან გასვლის სტრატეგიის განხორციელებას.
2. ამ სახელმძღვანელოში განსაზღვრული მოთხოვნები ვრცელდება საქართველოში მოქმედ ყველა კომერციულ ბანკსა და მიკრობანკზე, რომლებსაც სურთ ისარგებლონ ან უკვე სარგებლობენ ღრუბლოვანი აუთსორსინგული მომსახურებით (შემდგომში - „ფინანსური ორგანიზაცია“).

**მუხლი 2. ტერმინთა განმარტებები**

ამ სახელმძღვანელოს მიზნებისთვის მასში გამოყენებულ ტერმინებს აქვს შემდეგი მნიშვნელობა:

ა) ღრუბლოვანი მომსახურება - აუთსორსინგული მომსახურების ერთ-ერთი სახეობა, რომელიც იძლევა დისტანციურ, მოსახერხებელ და მომხმარებლის მოთხოვნის შესაბამის წვდომას კონფიგურირებადი საინფორმაციო სისტემებისა და დაკავშირებული ტექნოლოგიების (IT) რესურსებზე, როგორსაც, მაგალითად, წარმოადგენს, ქსელები, სერვერები, მონაცემთა სანახები, აპლიკაციები და სერვისები;

ბ) კერძო ღრუბლოვანი ინფრასტრუქტურა - ღრუბლოვანი ინფრასტრუქტურა, რომელიც ხელმისაწვდომია მხოლოდ კონკრეტული ფინანსური ორგანიზაციისთვის. ამ შემთხვევაში მფლობელობა, მართვა და ოპერირება შესაძლებელია განხორციელდეს თავად ფინანსური ორგანიზაციის, მესამე მხარის ან მათ მიერ ერთობლივად. კერძო ღრუბლოვანი ინფრასტრუქტურა შესაძლებელია არსებობდეს როგორც ფინანსური ორგანიზაციის გარემოში, ასევე მის გარეთ;

გ) გაერთიანებული ღრუბლოვანი ინფრასტრუქტურა - ღრუბლოვანი ინფრასტრუქტურა, რომელიც ხელმისაწვდომია ექსკლუზიურად კონკრეტული ფინანსური ორგანიზაციების სპეციფიკური მომხმარებლების ჯგუფისთვის, რომელთაც აქვთ საერთო ღირებულებები (მაგალითად, მისია, უსაფრთხოების მოთხოვნები, პოლიტიკები, შესაბამისობის საკითხები). ამ შემთხვევაში მფლობელობა, მართვა და ოპერირება შესაძლებელია განხორციელდეს გაერთიანების ფარგლებში არსებული ერთი ან რამდენიმე ფინანსური ორგანიზაციის, მესამე მხარის მიერ ან მათი ერთობლიობით. გაერთიანებული ღრუბლოვანი ინფრასტრუქტურა შესაძლებელია არსებობდეს როგორც რომელიმე ფინანსური ორგანიზაციის გარემოში, ასევე მის გარეთ;

დ) საჯარო ღრუბლოვანი ინფრასტრუქტურა - ღრუბლოვანი ინფრასტრუქტურა, რომელიც ღიად ხელმისაწვდომი და გამოყენებადია ფართო საზოგადოებისთვის. მისი ფლობა, მართვა და ოპერირება შესაძლებელია განხორციელდეს ბიზნეს, აკადემიური ან სამთავრობო ორგანიზაციების მიერ, ან მათ მიერ ერთობლივად. აღნიშნული მოდელი არსებობს ღრუბლოვანი მომსახურების მომწოდებლის გარემოში;

ე) ჰიბრიდული ღრუბლოვანი ინფრასტრუქტურა - ღრუბლოვანი ინფრასტრუქტურა, რომელიც შედგება ორი ან მეტი ერთმანეთისგან განსხვავებული ღრუბლოვანი ინფრასტუქტურისგან (კერძო, გაერთიანებული ან საჯარო), თითოეული მათგანი ინარჩუნებს უნიკალურობას, თუმცა ერთმანეთთან დაკავშირებული არიან სტანდარტიზებული ან საკუთარი გადაწყვეტილებებით, რაც შესაძლებელს ხდის მონაცემებისა და აპლიკაციების ერთმანეთში მარტივად გადასვლას (მაგ., ღრუბლოვან ინფრასტრუქტურებს შორის დატვირთვის დასაბალანსებლად);

ვ) პროგრამული უზრუნველყოფა როგორც მომსახურება (Software as a Service, SaaS) –ღრუბლოვანი მომსახურების მოდელი, რომელიც საშუალებას აძლევს მომხმარებელს გამოიყენოს მომსახურების მომწოდებლის პროგრამული უზრუნველყოფა, რომლებიც დანერგილია ღრუბლოვან ინფრასტრუქტურაში. პროგრამულ უზრუნველყოფაზე წვდომა შესაძლებელია განხორციელდეს სხვადასხვა მოწყობილობის გამოყენებით, მათ შორის ე.წ. „thin client“ ინტერფეისის, როგორიცაა, ვებ-ბრაუზერი, ან პროგრამული ინტერფეისის მეშვეობით. პროგრამული უზრუნველყოფის, როგორც მომსახურების მოდელის ფარგლებში მომხმარებელი არ მართავს ან არ აკონტროლებს ღრუბლოვან ინფრასტრუქტურას, მათ შორის, ქსელს, სერვერებს, საოპერაციო სისტემებს, საცავებს ან კონკრეტული აპლიკაციის შესაძლებლობებს, გარდა მომხმარებლისთვის სპეციფიკური აპლიკაციების კონფიგურაციის პარამეტრებისა;

ზ) პლატფორმა როგორც მომსახურება (Platform as a Service, PaaS) - ღრუბლოვანი მომსახურების მოდელი, რომლის ფარგლებშიც ღრუბლოვანი მომსახურების მიმწოდებელი მომხმარებლებს საშუალებას აძლევს ღრუბლოვან ინფრასტრუქტურაში განათავსოს მის მიერ შექმნილი/შესყიდული პროგრამული უზრუნველყოფა, რომელიც შემუშავებულია ღრუბლოვანი მომსახურების მომწოდებლის მხარდაჭერილი პროგრამირების ენების, ბიბლიოთეკების, სერვისებისა და სხვა ინფორმაციული ტექნოლოგიების (IT) ხელსაწყოების გამოყენებით. პლატფორმის, როგორც მომსახურების მოდელის ფარგლებში, მომხმარებელი არ მართავს ან არ აკონტროლებს ღრუბლოვან ინფრასტრუქტურას, მათ შორის, ქსელს, სერვერებს, საოპერაციო სისტემებს ან მონაცემთა სანახებს, თუმცა ახორციელებს კონტროლს შემუშავებულ აპლიკაციებზე და მათ ჰოსტინგ-გარემოს კონფიგურაციის პარამეტრებზე;

თ) ინფრასტრუქტურა როგორც მომსახურება (Infrastructure as a Service, IaaS) - ღრუბლოვანი მომსახურების მოდელი, რომელიც მომხმარებლებს უზრუნველყოფს მონაცემთა სანახებით, ქსელითა და სხვა ფუნდამენტური გამოთვლითი და დამუშავების რესურსებით, რომლის ფარგლებშიც მომხმარებელს შესაძლებლობა აქვს განავითაროს და გამართოს სასურველი პროგრამული უზრუნველყოფა, რაც შესაძლოა მოიცავდეს საოპერაციო სისტემებსა და აპლიკაციებს. ინფრასტრუქტურა, როგორც მომსახურების მოდელის ფარგლებში მომხმარებელი არ მართავს ან არ აკონტროლებს ღრუბლოვან ინფრასტრუქტურას, თუმცა აკონტროლებს საოპერაციო სისტემებს, მონაცემთა სანახებს, აპლიკაციებს და ასევე, შესაძლოა გააჩნდეს შეზღუდული კონტროლი ქსელური კომპონენტების შერჩევაზე (მაგალითად, firewall);

ი) ქვეაუთსორსერი - მომწოდებლის მიერ დაქირავებული მესამე მხარე, ორგანიზაცია, რომელიც მონაწილეობს ფინანსური ორგანიზაციისთვის ღრუბლოვანი აუთსორსინგული მომსახურების მიწოდებაში მომწოდებელთან გაფორმებული ხელშეკრულების შესაბამისად.

**მუხლი 3. ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში გასატანი ფუნქციის კრიტიკულობის ან/და მნიშვნელოვნების შეფასება**

ფინანსურმა ორგანიზაციამ საკუთარი ფუნქცი(ებ)ის ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში გატანამდე უნდა შეაფასოს და გაითვალისწინოს კონკრეტული ფუნქციის კრიტიკულობა ან/და მნიშვნელობა შესაბამისად „კომერციული ბანკების მიერ საოპერაციო რისკების მართვის შესახებ დებულების დამტკიცების თაობაზე“ საქართველოს ეროვნული ბანკის პრეზიდენტის 2014 წლის 13 ივნისის №47/04 ბრძანებით დამტკიცებული დებულების მე-8 მუხლის 12 პუნქტის ან საქართველოს ეროვნული ბანკი პრეზიდენტის ბრძანებით დამტკიცებული „მიკრობანკების მიერ საოპერაციო რისკების მართვის შესახებ დებულების“ მე-8 მუხლის მე-4 პუნქტის მიხედვით. შეფასების პროცესში გათვალისწინებული უნდა იქნას შემდეგი საკითხები:

ა) ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში გასატანი ფუნქციის კრიტიკულობა და თანმდევი რისკის პროფილი, კერძოდ, არის თუ არა ეს ფუნქცია ფინანსური ორგანიზაციის ბიზნესის უწყვეტობისთვის/ოპერირებისთვის და ასევე მომხმარებლის წინაშე ნაკისრი ვალდებულებების შესასრულებლად კრიტიკული მნიშვნელობის;

ბ) ფუნქციის პოტენციური შეფერხების საოპერაციო ზეგავლენის დონე, მასთან დაკავშირებული იურიდიული, რეპუტაციული და სხვა რისკები;

გ) მომსახურების ნებისმიერი შეფერხების გავლენა ფინანსური ორგანიზაციის შემოსავლიანობის ან/და მომგებიანობის პერსპექტივაზე;

დ) მონაცემთა კონფიდენციალურობის ან მთლიანობის დარღვევის პოტენციური ზეგავლენის დონე ფინანსურ ორგანიზაციასა და მის მომხმარებლებზე.

**მუხლი 4. საქართველოს ეროვნული ბანკის ინფორმირების ვალდებულება**

1. ფინანსური ორგანიზაცია ვალდებულია გონივრულ ვადაში, მაგრამ არანაკლებ 14 (თოთხმეტი) კალენდარული დღით ადრე აცნობოს საქართველოს ეროვნულ ბანკს (შემდგომში - ეროვნული ბანკი) დაგეგმილი ღრუბლოვანი აუთსორსინგული მომსახურების შესახებ, რომელიც ეხება ფინანსური ორგანიზაციის კრიტიკულ ან/და მნიშვნელოვან ფუნქციას.
2. ეროვნული ბანკისთვის შეტყობინების ვალდებულება ვრცელდება ღრუბლოვანი აუთსორსინგული მომსახურების ისეთ შემთხვევებზეც, რომლებიც მოიცავს ფუნქციას, რომელიც თავდაპირველად შეიძლება არ იყოს კლასიფიცირებული როგორც კრიტიკული ან/და მნიშვნელოვანი და შემდეგ გახდა კრიტიკული ან/და მნიშვნელოვანი.
3. ფინანსური ორგანიზაცია ვალდებულია ეროვნულ ბანკს გაუზიაროს სულ მცირე შემდეგი ინფორმაცია:

ა) ღრუბლოვანი აუთსორსინგული მომსახურების დაწყების თარიღი და, შესაძლებლობის შემთხვევაში, დასრულების, ხელშეკრულების მომდევნო განახლებისა და წინასწარი ინფორმირებისთვის დადგენილი თარიღები;

ბ) ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში გასატანი ფუნქციის მოკლე აღწერა;

გ) დასაბუთება, თუ რატომ მიიჩნევა კონკრეტული აუთსორსინგული ფუნქცია კრიტიკულად ან/და მნიშვნელოვნად;

დ) ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის და მისი მშობელი კომპანიის (ასეთის არსებობის შემთხვევაში) სახელწოდება, რეგისტრაციის ქვეყანა და რელევანტური საკონტაქტო ინფორმაცია;

ე) ღრუბლოვანი აუთსორსინგული მომსახურების შერჩეული ინფრასტრუქტურა და მოდელი;

ვ) ღრუბლოვანი აუთსორსინგული მომსახურების რისკების შეფასება;

ზ) ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლი ორგანიზაციის მიერ დარგობრივ და უსაფრთხოების სფეროში ფართოდ აღიარებულ ჩარჩოსთან და/ან სტანდარტთან შესაბამისობის დამადასტურებელი სერტიფიცირების დოკუმენტები;

თ) ღრუბლოვანი აუთსორსინგული მომსახურების შესახებ ფინანსური ორგანიზაციის შესაბამისი უფლებამოსილი პირ(ებ)ის, დირექტორატის ან სტრუქტურული ერთეულის მიერ მიღებული გადაწყვეტილება სათანადო დასაბუთებით;

ი) ქვეაუთსორსერების ჩამონათვალი, ასეთის არსებობის შემთხვევაში, მათ შორის, რეგისტრაციის ქვეყნები და ლოკაციები, სადაც შეინახება და დამუშავდება ფინანსური ორგანიზაციის მონაცემები. ასევე, ქვეაუთსორსერის დარგობრივ და უსაფრთხოების სფეროში ფართოდ აღიარებულ ჩარჩოსთან ან/და სტანდარტთან შესაბამისობის სერტიფიცირების დამადასტურებელი დოკუმენტები, ასეთის არსებობის შემთხვევაში.

**მუხლი 5. ღრუბლოვანი აუთსორსინგული მომსახურების მმართველობა**

1. ფინანსური ორგანიზაციის ღრუბლოვანი აუთსორსინგული მომსახურების სტრატეგია თანხვედრაში უნდა იყოს ფინანსური ორგანიზაციის ბიზნეს სტრატეგიასთან, შიდა პოლიტიკებთან, პროცედურებთან და პროცესებთან, მათ შორის, ინფორმაციული ტექნოლოგიების, ინფორმაციული უსაფრთხოებისა და საოპერაციო რისკების მიმართულებით.
2. ღრუბლოვანი აუთსორსინგული მომსახურების სტრატეგიის და სამოქმედო გეგმის ჩამოყალიბებისას ფინანსურმა ორგანიზაციამ უნდა გაითვალისწინოს და განსაზღვროს:

ა) ინფორმაციული სისტემებისა და ინფორმაციული აქტივების ტიპები, რომლებსაც განიხილავს ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში გასატანად;

ბ) გავლენა ფინანსური ორგანიზაციის ინფორმაციული ტექნოლოგიების (IT) არქიტექტურასა და საოპერაციო მოდელზე;

გ) ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებელზე დამოკიდებულების მზაობა და მისი არანაკლებ ყოველწლიური მონიტორინგის უნარი.

1. ფინანსურმა ორგანიზაციამ მკაფიოდ უნდა განსაზღვროს ღრუბლოვანი აუთსორსინგული მომსახურების სათანადოდ დოკუმენტირების, მართვისა და კონტროლის პასუხისმგებლობები ფინანსური ორგანიზაციის შიგნით.
2. ფინანსურმა ორგანიზაციამ უნდა ჩამოაყალიბოს ღრუბლოვანი აუთსორსინგული მომსახურების ზედამხედველობის ფუნქცია და განსაზღვროს შესაბამისი თანამშრომელ(ებ)ი, რომლ(ებ)იც ანგარიშვალდებული იქნებიან მმართველი ორგანოს წინაშე და პასუხისმგებელი იქნებიან აუთსორსინგის რისკების მართვასა და ზედამხედველობაზე.
3. რისკების მართვის ფარგლებში ფინანსურმა ორგანიზაციამ უნდა გაითვალისწინოს მისი სიდიდე, კომპლექსურობა, მათ შორის, საფინანსო სისტემისა და აუთსორსინგული ფუნქციების თანმდევი რისკების პროფილი.
4. ფინანსურმა ორგანიზაციებმა უნდა უზრუნველყონ როლებისა და პასუხისმგებლობების მკაფიო განსაზღვრა ღრუბლოვანი აუთსორსინგული მომსახურების მართვისა და ზედამხედველობისთვის.
5. ფინანსურმა ორგანიზაციამ, კრიტიკული ან/და მნიშვნელოვანი ფუნქციის ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში გატანის შემთხვევაში, არანაკლებ წელიწადში ერთხელ უნდა განახორციელოს ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის მიერ განხორციელებული საქმიანობის, უსაფრთხოების ზომებისა და ხელშეკრულებით ნაკისრი ვალდებულებების დაცვის მონიტორინგი.
6. ფინანსურმა ორგანიზაციამ ყოველწლიურად უნდა გადააფასოს თუ რა სახის კრიტიკულ ან/და მნიშვნელოვან ფუნქციებს მოიცავს მისი ღრუბლოვანი აუთსორსინგული მომსახურება და არსებითად ხომ არ შეცვლილა მისი აუთსორსინგული ფუნქციის რისკები, ბუნება და მასშტაბი.
7. ფინანსურმა ორგანიზაციამ უნდა აწარმოოს ყველა ღრუბლოვანი აუთსორსინგული მომსახურების შესახებ მიმდინარე რეესტრი, სადაც კრიტიკული ან/და მნიშვნელოვანი ფუნქციების ღრუბლოვან ინფრასტრუქტურაში აუთსორსინგს გამიჯნავს სხვა დანარჩენი აუთსორსინგული ფუნქციებისგან. გამიჯვნის პროცესში ფინანსურმა ორგანიზაციამ ასევე უნდა მიუთითოს შესაბამისი მიზეზების მოკლე აღწერა, თუ რატომ მიიჩნევა ან არ მიიჩნევა კონკრეტული აუთსორსინგული ფუნქცია კრიტიკულად ან/და მნიშვნელოვნად.
8. ღრუბლოვანი აუთსორსინგული მომსახურების რეესტრი თითოეული მომსახურებისთვის უნდა მოიცავდეს სულ მცირე შემდეგ ინფორმაციას:

ა) უნიკალურ მაიდენტიფიცირებელ ნომერს;

ბ) ღრუბლოვანი აუთსორსინგული მომსახურების დაწყების თარიღს და, შესაძლებლობის შემთხვევაში, დასრულების, ხელშეკრულების მომდევნო განახლებისა და წინასწარი ინფორმირებისთვის დადგენილ თარიღებს;

გ) ფუნქციის მოკლე აღწერას, მათ შორის, თუ რა სახის მონაცემები გადის ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში და, ასევე, შეიცავს თუ არა პერსონალურ მონაცემებს (დიახ/არა მითითებით ცალკე ველში);

დ) მხარეებს (ბიზნეს ერთეულებს), რომლებიც იღებენ ღრუბლოვან აუთსორსინგულ მომსახურებას შესაბამისი ხელშეკრულების ფარგლებში;

ე) მოიცავს თუ არა ღრუბლოვანი აუთსორსინგული მომსახურება ფინანსური ორგანიზაციის კრიტიკულ ან/და მნიშვნელოვან ფუნქციას (დიახ/არა);

ვ) ახორციელებს თუ არა აუთსორსინგული ფუნქცია დროში კრიტიკული ბიზნეს ოპერაციების მხარდაჭერას (დიახ/არა);

ზ) მომწოდებლის და მისი მშობელი კომპანიის (ასეთის არსებობის შემთხვევაში) სახელწოდებას, რეგისტრაციის ქვეყანასა და რელევანტურ საკონტაქტო ინფორმაციას;

თ) ქვეაუთსორსერების ჩამონათვალს, ასეთის არსებობის შემთხვევაში, მათ შორის, რეგისტრაციის ქვეყნებსა და ლოკაციებს, სადაც ინახება და მუშავდება ფინანსური ორგანიზაციის მონაცემები;

ი) ღრუბლოვანი აუთსორსინგული მომსახურების ინფრასტრუქტურასა და მოდელებს;

კ) ქვეყანას ან ქვეყნებს, სადაც შეინახება და დამუშავდება მონაცემები კონკრეტული ღრუბლოვანი მომსახურების ფარგლებში;

ლ) ფინანსური ორგანიზაციის მიერ ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში გატანილი ფუნქციის კრიტიკულობის ან/და მნიშვნელოვნების შეფასების ბოლო თარიღს;

მ) მომწოდებლის აუდიტის/რისკების შეფასების ბოლო თარიღს ძირითადი შედეგების მოკლე აღწერილობით, ასეთის არსებობის შემთხვევაში;

ნ) ფინანსური ორგანიზაციის შესაბამისი უფლებამოსილი პირ(ებ)ის, დირექტორატის ან სტრუქტურული ერთეულის მიერ მიღებულ გადაწყვეტილებას კონკრეტული ღრუბლოვანი აუთსორსინგული მომსახურების თაობაზე;

ო) მომწოდებლის ჩანაცვლების შეფასებას (მარტივად ჩანაცვლებადი, რთულად ჩანაცვლებადი ან შეუძლებელი);

პ) ალტერნატიული მომსახურების მომწოდებელს/მომწოდებლებს, მისი/მათი იდენტიფიცირების შემთხვევაში;

ჟ) ღრუბლოვანი აუთსორსინგული მომსახურების სავარაუდო წლიურ ხარჯს.

1. ფინანსურმა ორგანიზაციამ დაგეგმვის ეტაპზე უნდა განსაზღვროს ღრუბლოვანი აუთსორსინგული მომსახურებიდან გამოსვლის სტრატეგია, რაც, თავის მხრივ, უკავშირდება უწყვეტობის მოთხოვნებს. სტრატეგია უნდა მოიცავდეს ისეთ შემთხვევებს, როგორებიცაა:

ა) მომსახურების დაგეგმილი შეწყვეტის შემთხვევები, როგორიცაა, მაგალითად, ხელშეკრულებით გათვალისწინებული ვადის ამოწურვა;

ბ) მომსახურების გაუთვალისწინებელი შეწყვეტის შემთხვევები, როგორიცაა, მაგალითად, ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის მხარეს არსებული შეფერხებები, მისი გაკოტრება ან მომსახურების არაჯეროვნად შესრულება.

**მუხლი 6. ღრუბლოვანი აუთსორსინგული მომსახურების და მისი მომწოდებლის წინასწარი შეფასება**

1. ღრუბლოვანი აუთსორსინგული მომსახურების შესახებ ხელშეკრულების დადებამდე, ფინანსურმა ორგანიზაციამ უნდა:

ა) განსაზღვროს, მოიცავს თუ არა ღრუბლოვანი აუთსორსინგული მომსახურება კრიტიკულ ან/და მნიშვნელოვან ფუნქციას;

ბ) გამოავლინოს და შეაფასოს ღრუბლოვან აუთსორსინგულ მომსახურებასთან დაკავშირებული შესაძლო რისკები;

გ) განახორციელოს ღრუბლოვანი აუთსორსინგული მომსახურების პოტენციური მომწოდებლის წინასწარი მოკვლევა, სათანადო შესწავლა და ანალიზი, რათა ხელთ ჰქონდეს სათანადო რწმუნება მომწოდებლის სანდოობიის, ფინანსური მდგომარეობის მდგრადობის, კვალიფიკაციისა და რეპუტაციის შესახებ;

დ) გამოავლინოს და შეაფასოს პოტენციური ინტერესთა კონფლიქტი, რაც შეიძლება გამოიწვიოს კონკრეტულმა ღრუბლოვანმა აუთსორსინგულმა მომსახურებამ.

1. ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის წინასწარი მოკვლევა, შესწავლა და ანალიზი უნდა შეესაბამებოდეს აუთსორსინგული ფუნქციის მასშტაბსა და კომპლექსურობას, ასევე, კონკრეტული ფუნქციის თანმდევ რისკებს.
2. წინასწარი შეფასების პროცესი უნდა მოიცავდეს სულ მცირე ღრუბლოვანი აუთსორსინგული მომსახურების პოტენციური ზეგავლენის შეფასებას ფინანსური ორგანიზაციის საოპერაციო, იურიდიულ, შესაბამისობისა და რეპუტაციულ რისკებზე.
3. თუ ღრუბლოვანი აუთსორსინგული მომსახურება მოიცავს კრიტიკულ ან/და მნიშვნელოვან ფუნქციას, ფინანსურმა ორგანიზაციამ ასევე უნდა შეაფასოს საინფორმაციო ტექნოლოგიებთან, ინფორმაციულ უსაფრთხოებასთან, მომწოდებლის ფინანსურ მდგომარეობასთან, საოპერაციო რისკებთან, ბიზნეს უწყვეტობასთან, შეზღუდულ ზედამხედველობასთან დაკავშირებული, ასევე, სამართლებრივი და შესაბამისობის რისკები, რაც გამომდინარეობს:

ა) შერჩეული ღრუბლოვანი აუთსორსინგული მომსახურებისა და ინფრასტრუქტურის მოდელებიდან;

ბ) მიგრაციისა ან/და დანერგვის პროცესებიდან;

გ) ფინანსური ორგანიზაციის ფუნქციისა და მასთან დაკავშირებული მონაცემების სენსიტიურობიდან, რომელიც განიხილება ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში გასატანად;

დ) უსაფრთხოების ზომებიდან;

ე) მომწოდებლისა და ფინანსური ორგანიზაციის სისტემებისა და პროგრამული უზრუნველყოფის თავსებადობიდან;

ვ) ფინანსური ორგანიზაციის მონაცემების გადატანასთან დაკავშირებული რისკებიდან, კერძოდ, ფინანსური ორგანიზაციის მონაცემების ერთი ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლიდან მეორე მომწოდებელთან ან უშუალოდ ფინანსურ ორგანიზაციაში უკან მარტივად გადმოტანის უნარით;

ზ) იმ ქვეყნ(ებ)ის პოლიტიკური სტაბილურობიდან, უსაფრთხოების ვითარებიდან და სამართლებრივი სისტემიდან, სადაც განიხილება ღრუბლოვანი აუთსორსინგული მომსახურების გატანა და სადაც შეინახება ფინანსური ორგანიზაციის მონაცემები; ქვეაუთსორსერების შემთხვევაში, იმ დამატებითი რისკებიდან, რომლებიც შესაძლოა წარმოიშვას, თუ ქვეაუთსორსერი მდებარეობს მესამე ქვეყანაში და თუ ფინანსურ ორგანიზაციასა და ქვეაუთსორსერს შორის არ არის დადებული ხელშეკრულება ან არ არის რაიმე სახით ფორმალიზებული თანამშრომლობა;

თ) კონცენტრაციის რისკიდან, როგორც ფინანსური ორგანიზაციის შიგნით ერთი და იგივე ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის, მათ შორის, ერთი და იგივე ქვეაუთსორსინგული ორგანიზაციის, მომსახურების გამოყენებით, ასევე მთლიანი სექტორის მასშტაბით.

1. ფინანსურმა ორგანიზაციამ უნდა შეაფასოს ღრუბლოვანი აუთსორსინგული მომსახურების ხარჯთსარგებლიანობა, მათ შორის, შეადაროს და გაზომოს ის მნიშვნელოვანი რისკები, რომლებიც, ერთი მხრივ, შესაძლოა შემცირდეს ან უკეთ იმართოს ღრუბლოვანი აუთსორსინგული მომსახურების გამოყენებისას და, მეორე მხრივ, შესაძლოა წარმოშვას ღრუბლოვანი აუთსორსინგული მომსახურების გამოყენებამ.
2. კრიტიკული ან/და მნიშვნელოვანი ფუნქციის ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში გატანის შემთხვევაში, ფინანსურმა ორგანიზაციამ უნდა მოიკვლიოს, შეისწავლოს და შეაფასოს ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის სანდოობა. ამ მიზნით ფინანსურმა ორგანიზაციამ უნდა მიიღოს სათანადო ხარისხის რწმუნება, რომ მომწოდებელს გააჩნია კვალიფიციური საქმიანი რეპუტაცია, მდგრადი ფინანსური მდგომარეობა, საჭირო კომპეტენცია (ცოდნა, უნარები და გამოცდილება), რესურსები (მათ შორის, ადამიანური, IT და ფინანსური), ორგანიზაციული სტრუქტურა, რათა საიმედოდ და პროფესიონალურად შეასრულოს ხელშეკრულებით ნაკისრი ვალდებულები და ფინანსურ ორგანიზაციას მიაწოდოს მაღალი ხარისხის ღრუბლოვანი აუთსორსინგული მომსახურება.
3. დამატებითი ფაქტორები, რაც უნდა იყოს გათვალისწინებული მომწოდებლის შეფასების პროცესში, მოიცავს, მათ შორის, შემდეგ საკითხებს:

ა) ინფორმაციული უსაფრთხოების მართვა, კერძოდ, პერსონალური, კონფიდენციალური თუ სხვა სახის სენსიტიური ინფორმაციის დაცვა;

ბ) მომსახურების მხარდაჭერა, მათ შორის, მხარდაჭერის გეგმები, კომუნიკაცია და ინციდენტების მართვის პროცესები;

გ) ბიზნეს უწყვეტობისა და საინფორმაციო ტექნოლოგიების აღდგენის გეგმები ღრუბლოვანი აუთსორსინგული მომსახურების ჭრილში.

1. მოკვლევის პროცესში მეტი რწმუნების მისაღებად, ფინანსურმა ორგანიზაციამ უნდა გამოითხოვოს დარგობრივ და უსაფრთხოების საერთაშორისო სტანდარტთან/სტანდარტებთან შესაბამისობის დამადასტურებელი სერტიფიკატები და გარე ან შიდა აუდიტის ანგარიშები, ასეთის არსებობის შემთხვევაში.
2. ფინანსურმა ორგანიზაციამ უნდა შეაფასოს ამ სახელმძღვანელოთი დადგენილ კრიტერიუმ(ებ)თან ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის შეუსაბამობის რისკი, რომლის გათვალისწინებითაც უნდა მიიღოს საბოლოო გადაწყვეტილება მომწოდებელთან ურთიერთობის დამყარების შესახებ.

**მუხლი 7. ძირითადი სახელშეკრულებო ელემენტები**

1. ფინანსური ორგანიზაცია ვალდებულია ჩამოაყალიბოს ხელშეკრულება, სადაც მკაფიოდ განსაზღვრავს ღრუბლოვანი აუთსორსინგული მომსახურების პირობებს.
2. ხელშეკრულებაში მკაფიოდ უნდა იყოს განსაზღვრული ფინანსური ორგანიზაციისა და ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის უფლებები და მოვალეობები.
3. ხელშეკრულების მიხედვით ფინანსურ ორგანიზაციას უნდა შეეძლოს საჭიროების შემთხვევაში მომსახურების შეწყვეტა.
4. კრიტიკული ან/და მნიშვნელოვანი ფუნქციების აუთსორსინგის შემთხვევაში, ხელშეკრულება უნდა შეიცავდეს სულ მცირე შემდეგ საკითხებს:

ა) ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში გასატანი ფუნქციის მკაფიო აღწერას;

ბ) მომსახურების მიწოდების დაწყებისა და დასრულების თარიღებს, მათ შორის, უვადოდ გაფორმებული ხელშეკრულების შემთხვევაში სათანადო ჩანაწერს, ასევე, საჭიროების შემთხვევაში, მხარეთა მიერ ხელშეკრულების შეწყვეტის წინასწარი ინფორმირებისთვის დადგენილ ვადას;

გ) ფინანსური ორგანიზაციისა და მომწოდებლის ფინანსურ ვალდებულებებს, რაც უკავშირდება ღრუბლოვან აუთსორსინგულ მომსახურებას;

დ) ქვეაუთსორსერ(ებ)ის არსებობის შემთხვევაში, მასთან დაკავშირებულ ვალდებულებებს, პასუხისმგებლობებს;

ე) მდებარეობ(ებ)ას (რეგიონები ან ქვეყნები), სადაც უზრუნველყოფილი იქნება აუთსორსინგული ფუნქცია და სადაც მოხდება მონაცემების დამუშავება და შენახვა. ხელშეკრულება ასევე უნდა მოიცავდეს მოთხოვნებს, რომ ფინანსურ ორგანიზაციას ეცნობოს მომწოდებლის მონაცემთა ცენტრების მდებარეობის ცვლილებები;

ვ) ინფორმაციული უსაფრთხოებისა და პერსონალური, კონფიდენციალური მონაცემების დაცვასთან დაკავშირებულ დებულებებს, ამ სახელმძღვანელოს მე-8 მუხლის გათვალისწინებით;

ზ) ფინანსური ორგანიზაციის უფლებას, რომ ყოველწლიურად შეაფასოს მომწოდებლის საქმიანობა ღრუბლოვანი აუთსორსინგული მომსახურების ხელშეკრულების ფარგლებში, ამ სახელმძღვანელოს მე-10 მუხლის შესაბამისად;

თ) მომსახურების შეთანხმებულ დონეებს, რომელიც უნდა მოიცავდეს შესრულების რაოდენობრივ და ხარისხობრივ ინდიკატორებს, რათა განხორციელდეს ეფექტური მონიტორინგი და შესაბამისი მაკორექტირებელი ქმედებების დროული მიღება ზედმეტი შეფერხების გარეშე, თუ მომსახურების შეთანხმებული დონეები არ იქნა დაკმაყოფილებული;

ი) მომწოდებლის მხრიდან ანგარიშგების ვალდებულებებს ფინანსური ორგანიზაციის წინაშე და საჭიროების შემთხვევაში, უსაფრთხოების და სხვა ძირითადი ფუნქციების შესაბამისი ანგარიშების წარდგენის ვალდებულებებს, როგორიცაა, მათ შორის, მომწოდებლის დამოუკიდებელი აუდიტის მიერ მომზადებული ანგარიშები;

კ) ინციდენტების მართვასთან დაკავშირებულ მოთხოვნებს, მათ შორის, მომწოდებლის ვალდებულებას, დაუყონებლივ შეატყობინოს ფინანსურ ორგანიზაციას იმ ინციდენტების შესახებ, რომლებმაც ზეგავლენა იქონია ფინანსური ორგანიზაციის სახელშეკრულებო მომსახურების ოპერირებაზე;

ლ) მომწოდებლის მიერ გარკვეული რისკების სავალდებულო დაზღვევის საჭიროებას და შესაძლებლობის შემთხვევაში, მოთხოვნილი სადაზღვევო დაფარვის დონეს;

მ) მომწოდებლის მიმართ ბიზნესის უწყვეტობისა და საინფორმაციო ტექნოლოგიების აღდგენის გეგმების დანერგვისა და ტესტირების მოთხოვნებს;

ნ) მომწოდებლის მიმართ აუდიტისა და ზედამხედველობის უფლებებს, რაც შესაძლოა განხორციელდეს უშუალოდ ფინანსური ორგანიზაციის ან მის მიერ განსაზღვრული დამოუკიდებელი მესამე მხარის მიერ, ამ სახელმძღვანელოს მე-10 მუხლის გათვალისწინებით;

ო) ფინანსური ორგანიზაციის მომწოდებლის მიერ დამუშავებული და შენახული მონაცემების ხელმისაწვდომობის და, საჭიროების შემთხვევაში, აღდგენისა და ფინანსური ორგანიზაციისთვის დაბრუნების მოთხოვნებს, ამ სახელმძღვანელოს მე-9 მუხლის შესაბამისად.

**მუხლი 8. ღრუბლოვანი ინფრასტრუქტურის უსაფრთხოების მართვა**

1. ფინანსურმა ორგანიზაციამ უნდა განსაზღვროს ღრუბლოვანი აუთსორსინგული მომსახურებისადმი ინფორმაციული უსაფრთხოების მოთხოვნები, როგორც თავის შიდა პოლიტიკებსა და პროცედურებში, ისე ღრუბლოვანი აუთსორსინგული მომსახურების ხელშეკრულებებში და ყოველწლიურად შეაფასოს დადგენილ მოთხოვნებთან შესაბამისობა. აღნიშნული მოთხოვნები უნდა იყოს აუთსორსინგული ფუნქციის მასშტაბისა და კომპლექსურობის, ასევე ფუნქციის თანმდევი რისკების შესაბამისი.
2. ინფორმაციული უსაფრთხოების მოთხოვნების განსაზღვრისას ფინანსურმა ორგანიზაციამ რისკზე დაფუძნებული მიდგომის გამოყენებით უნდა განსაზღვროს სულ მცირე შემდეგი საკითხები:

ა) *ინფორმაციული უსაფრთხოების ორგანიზება:* უზრუნველყოს ინფორმაციული უსაფრთხოების როლებისა და პასუხისმგებლობების მკაფიო გადანაწილება ფინანსურ ორგანიზაციასა და ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებელს შორის, მათ შორის, საფრთხეების აღმოჩენასთან, ინციდენტების მართვასა და სისტემის განახლებების („პატჩი“) მართვასთან დაკავშირებით. ფინანსური ორგანიზაცია ასევე უნდა დარწმუნდეს, რომ მომწოდებელს შეუძლია ეფექტურად შეასრულოს თავისი როლები და პასუხისმგებლობები;

ბ) *უსაფრთხოების რისკების შეფასება:* უზრუნველყოს უსაფრთხოების რისკების შეფასება და მართვა ყველა იდენტიფიცირებული სისტემისა და ინფორმაციული აქტივის ჭრილში, რომლებიც განთავსებულია ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში;

გ) *იდენტობისა და წვდომების მართვა (IAM):* უზრუნველყოს, რომ დანერგილი იყოს ძლიერი ავთენტიფიკაციის მექანიზმი და წვდომის კონტროლები, რათა თავიდან იქნას აცილებული არაავტორიზებული წვდომა ფინანსური ორგანიზაციის მონაცემებსა და ღრუბლოვან რესურსებზე;

დ) *მონაცემთა შიფრაცია:* ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში სხვადასხვა დონის სენსიტიური ინფორმაციის დასაცავად, საჭიროების შემთხვევაში, გამოყენებული უნდა იყოს შესაბამისი შიფრაციის მექანიზმები მონაცემთა შენახვის, მიმოცვლის, დამუშავებისა და მონაცემთა სარეზერვო ასლებისთვის;

ე) *შიფრაციის გასაღებების მართვა:* მონაცემთა შიფრაციის მექანიზმების გამოყენებისას, ფინანსურმა ორგანიზაციამ უნდა უზრუნველყოს ისეთი გასაღებების მართვის თანამედროვე გადაწყვეტილებების გამოყენება, რომელიც გამორიცხავს შიფრაციის გასაღებებზე არაავტორიზებულ წვდომას. აღნიშნული პროცესის ფარგლებში, ფინანსურმა ორგანიზაციამ:

ე.ა) უნდა ჩამოაყალიბოს შიფრაციის გასაღებების მართვის პროცესი და მკაფიოდ განსაზღვროს და გადაანაწილოს პასუხისმგებლობები ფინანსურ ორგანიზაციასა და ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებელს შორის;

ე.ბ) უნდა გამოიყენოს გასაღებების მართვის ისეთი მექანიზმები, რომლებიც უზრუნველყოფენ კრიტიკული ან/და მნიშვნელოვანი ფუნქციის ან კონფიდენციალური, პერსონალური და სხვა სახის სენსიტიური მონაცემების დაცულობას არაავტორიზებული წვდომისგან და კომპრომეტირებისგან;

ვ) *მონაცემთა მთლიანობა:* ფინანსურმა ორგანიზაციამ უნდა გამოიყენოს ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში განთავსებული მონაცემების მთლიანობის შემოწმების მექანიზმი, რათა მონაცემები დაცული იყოს არაავტორიზებული ცვლილებისაგან;

ზ) *საოპერაციო და ქსელური უსაფრთხოება:* ფინანსურმა ორგანიზაციამ უნდა განიხილოს ქსელის ხელმისაწვდომობის დონეები, ქსელის სეგმენტაცია, კერძოდ, ღრუბლოვანი აუთსორსინგული მომსახურების მომხმარებლის იზოლირება ღრუბლოვანი ინფრასტრუქტურის საზიარო გარემოში და გამიჯვნა საოპერაციო დონეზე, რაც მოიცავს აპლიკაციის, ოპერაციული სისტემის, ქსელის, მონაცემთა ბაზის მართვის სისტემის (DBMS) და მონაცემთა სანახების დონეებს და დამუშავების გარემოებს (კერძოდ, დეველოპმენტის, ტესტირების, რეალური გარემოები);

თ) *ბიზნეს უწყვეტობისა და საინფორმაციო ტექნოლოგიების აღდგენის გეგმები:* ფინანსურმა ორგანიზაციამ უნდა უზრუნველყოს ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში გატანილი მომსახურების ბიზნეს უწყვეტობა შემდეგი ფაქტორების გათვალისწინებით:

თ.ა) დარწმუნდეს და შეაფასოს, რომ ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებელს გააჩნია ეფექტური ბიზნეს უწყვეტობისა და საინფორმაციო ტექნოლოგიების აღდგენის გეგმები, კერძოდ, დარწმუნდეს, აქვს თუ არა მომწოდებელს განსაზღვრული წარმადობის მინიმალური მოთხოვნები; გააჩნია თუ არა გეოგრაფიულად დაშორებული მონაცემთა ცენტრები, საჭიროების შემთხვევაში, ერთიდან მეორეზე გადართვის შესაძლებლობით; განიხილოს მონაცემთა ნაკადები, რომლის მიხედვითაც ფინანსური ორგანიზაციის მონაცემები მიმოიცვლება ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის სისტემებში; ხორციელდება თუ არა ვირტუალური მანქანებისა თუ მონაცემების სარეზერვო ასლების წარმოება დამოუკიდებელ სანახ ლოკაციაზე, რომელიც სათანადოდ არის გამიჯნული ქსელურ დონეზე და სხვა);

თ.ბ) გააჩნია თუ არა შიდა ბიზნეს უწყვეტობისა და საინფორმაციო ტექნოლოგიების აღდგენის განახლებული გეგმები, რომლებიც მოიცავს ღრუბლოვანი აუთსორსინგული მომსახურების უწყვეტობის სცენარებსაც და ხორციელდება თუ არა მათი პერიოდული ტესტირება;

თ.გ) კრიტიკული ან/და მნიშვნელოვანი ფუნქციების აუთსორსინგის შემთხვევაში, ადგილობრივ დონეზე უზრუნველყოს ღრუბლოვანი სისტემისა და მონაცემების სარეზერვო ასლების წარმოება იმგვარად, რომ სხვადასხვა რისკების დადგომის შემთხვევაში (როგორიცაა, კავშირის დაკარგვა და ხელმიუწვდომლობა ღრუბლოვან მომსახურებასთან) მაქსიმალური დასაშვები შეფერხების (MTO) მაჩვენებლის ფარგლებში შეძლოს ღრუბლოვანი მომსახურების აღდგენა;

ი) *მონაცემთა ადგილმდებარეობა:* უნდა გამოიყენოს რისკზე დაფუძნებული მიდგომა მონაცემთა შენახვისა და დამუშავების ადგილმდებარეობის (რეგიონის ან ქვეყნ(ებ)ის) შერჩევის პროცესში პერსონალურ მონაცემთა დაცვის სამსახურის მიერ შემუშავებული პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხიდან;

კ) *შესაბამისობა და მონიტორინგი:* დარწმუნდეს, რომ ღრუბლოვანი აუთსორსინგული მომსახურებების მომწოდებელი შეესაბამება ინფორმაციული უსაფრთხოების საერთაშორისოდ აღიარებულ სტანდარტებს და გააჩნია ინფორმაციული უსაფრთხოების შესაბამისი კონტროლების გარემო;

ლ) *ცვლილებების მართვა:* უნდა შეიმუშაოს ახალი პოლიტიკა, პროცედურები, სტანდარტები ან განავრცოს სისტემების/პროგრამული უზრუნველყოფის შემუშავების სასიცოცხლო ციკლის არსებული პრაქტიკა ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში დანერგილ სერვისებსა და პროგრამულ უზრუნველყოფაზეც. ასევე, უნდა უზრუნველყოს ორგანიზაციული პრაქტიკის დაცვა ღრუბლოვან აუთსორსინგულ ინფრასტრუქტურაში დანერგილი სისტემების მთლიანი სასიცოცხლო ციკლის მანძილზე.

**მუხლი 9. კრიტიკული ან/და მნიშვნელოვანი ფუნქციების ღრუბლოვანი აუთსორსინგული მომსახურებიდან გასვლის სტრატეგია**

1. კრიტიკული ან/და მნიშვნელოვანი ფუნქციების აუთსორსინგის შემთხევაში, ფინანსურმა ორგანიზაციამ უნდა შეიმუშაოს მომსახურებიდან გასვლის სტრატეგია, რათა უზრუნველყოფილი იქნას ფინანსური ორგანიზაციის შეუფერხებელი ოპერირება და შესაბამისობა რელევანტურ მარეგულირებელ და საკანონმდებლო მოთხოვნებთან, მათ შორის, ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დაცვა.
2. მომსახურებიდან გასვლის მიზნით ფინანსური ორგანიზაცია ვალდებულია იქონიოს და გამოიყენოს დოკუმენტირებული, სრულყოფილი და გატესტილი გეგმები, რომელთა განახლებაც უნდა განახორციელოს დადგენილი პერიოდულობით ან/და მომსახურების ცვლილების შემთხვევაში.
3. ფინანსურმა ორგანიზაციამ უნდა გამოავლინოს ალტერნატიული საშუალებები და შეიმუშავოს მიგრაციის გეგმა, რომლის მიხედვითაც განახორციელებს ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის და, არსებობის შემთხვევაში, ქვეაუთსორსერის ინფრასტრუქტურიდან აუთსორსინგული ფუნქციისა და მონაცემების წაშლას და ალტერნატიულ მომწოდებელთან გადატანას ან საკუთარ ინფრასტრუქტურაში უსაფრთხო და დროულ დაბრუნებას. ასევე, ფინანსურმა ორგანიზაციამ უნდა მიიღოს შესაბამისი ზომები გარდამავალი ფაზის განმავლობაში ბიზნესის უწყვეტობის უზრუნველსაყოფად.
4. ფინანსურმა ორგანიზაციამ უნდა უზრუნველყოს, რომ ხელშეკრულება მოიცავდეს ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის ვალდებულებას, მხარი დაუჭიროს აუთსორსინგული ფუნქციისა და ფინანსური ორგანიზაციის მონაცემების მიგრაციას საკუთარი ინფრასტრუქტურიდან, მათ შორის, ქვეაუთსორსერებიდან, ფინანსური ორგანიზაციის მიერ შერჩეულ სხვა მომწოდებელთან ან უშუალოდ ფინანსურ ორგანიზაციაში, თუ ფინანსური ორგანიზაცია გაააქტიურებს გასვლის სტრატეგიას. ვალდებულებები ასევე უნდა მოიცავდეს მონაცემების უსაფრთხო წაშლას ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის და, არსებობის შემთხვევაში, ქვეაუთსორსერის სისტემებიდან.
5. მომსახურებიდან გასვლის გეგმების და ალტერნატიული საშუალებების განსაზღვრისას ამ მუხლის მე-2 და მე-3 პუნქტების მიხედვით, ფინანსურმა ორგანიზაციამ უნდა:

ა) განსაზღვროს გასვლის სტრატეგიის მიზნები და ამოცანები;

ბ) დაადგინოს ის გარემოებები/კრიტერიუმები, რაც განაპირობებს მომსახურებიდან გასვლის სტრატეგიის ამოქმედებას, მათ შორის, როგორც მომწოდებლის, ასევე, თავად ფინანსური ორგანიზაციის ინიციატივით გააქტიურების შემთხვევები;

გ) ჩაატაროს ღრუბლოვანი აუთსორსინგული ფუნქციების ბიზნესზე გავლენის ანალიზი, რათა განისაზღვროს გასვლის სტრატეგიის განხორციელებისთვის აუცილებელი ადამიანური, ტექნიკური და სხვა სახის რესურსები;

დ) განსაზღვროს და შესაბამის პირებს თუ ბიზნეს ერთეულებს მიანიჭოს მომსახურებიდან გასვლის სტრატეგიის მართვისთვის საჭირო როლები და პასუხისმგებლობები;

ე) წელიწადში ერთხელ შეაფასოს სტრატეგიის ქმედუნარიანობა რისკზე დაფუძნებული მიდგომის გამოყენებით, რაც უნდა მოიცავდეს აუთსორსირებული ფუნქცი(ებ)ის ალტერნატიულ მომწოდებელთან გადატანისთვის საჭირო ხარჯებს, გავლენას, რესურსებს და დროში შეზღუდვებს;

ვ) განსაზღვროს მომსახურებიდან გასვლის სტრატეგიისა და ალტერნატიულ მომწოდებელთან გადასვლის ან საკუთარ ინფრასტრუქტურაში დაბრუნების წარმატების კრიტერიუმები.

**მუხლი 10. მომწოდებლის შეფასებისა და აუდიტის უფლებები**

1. ფინანსურმა ორგანიზაციამ უნდა უზრუნველყოს, რომ ღრუბლოვანი აუთსორსგინგული მომსახურების ხელშეკრულებით არ შეიზღუდოს ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის აუდიტისა და ზედამხედველობის უფლებები, რაც შესაძლოა განხორციელდეს უშუალოდ ფინანსური ორგანიზაციის ან მის მიერ განსაზღვრული დამოუკიდებელი მესამე მხარის მიერ.
2. თუ ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის აუდიტი ან კონკრეტული აუდიტის ინსტრუმენტები/მეთოდები მომწოდებელს ან/და მის სხვა მომხმარებლებს უქმნის დამატებით რისკებს (ზეგავლენა აქვს მომსახურების ხარისხზე ან მონაცემების კონფიდენციალურობაზე, მთლიანობასა და ხელმისაწვდომობაზე), ფინანსურმა ორგანიზაციამ, მომწოდებლისგან მიღებული შესაბამისი დასაბუთების საფუძველზე, მასთან უნდა შეათანხმოს სხვა ალტერნატიული გზები, რათა მიიღოს მსგავსი შედეგები და იმავე ხარისხის რწმუნება.
3. ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის აუდიტის მიზნით ან მისი კონტროლების გარემოს ეფექტურობისა და უსაფრთხოების შესაფასებლად, ფინანსურ ორგანიზაციას შეუძლია მიიღოს მსგავსი ხარისხის რწმუნება და გარანტიები, მათ შორის, შემდეგი მეთოდების გამოყენებით:

ა) ერთიანი აუდიტი, რომელიც ორგანიზებულია იმავე ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის სხვა კლიენტებთან ერთად და შესრულებულია უშუალოდ ამ კლიენტების ან მათ მიერ დანიშნული დამოუკიდებელი მესამე მხარის მიერ. ფინანსურმა ორგანიზაციამ შესაძლებელია გამოიყენოს უკვე ჩატარებული, უახლესი აუდიტის დასკვნა;

ბ) დამოუკიდებელი მესამე მხარის დარგობრივი სერტიფიცირება და გარე აუდიტის ანგარიშები, რაც ხელმისაწვდომი იქნება ღრუბლოვანი აუთსორსინგული მომსახურების მომწოდებლის მხრიდან, მხოლოდ იმ შემთხვევაში, თუ დაკმაყოფილებულია ყველა შემდეგი პირობა:

ბ.ა) სერტიფიცირება და აუდიტის ანაგრიშების გავრცელების სფერო მოიცავს ყველა იმ სისტემას (მაგალითად, აპლიკაციებს, ინფრასტრუქტურას, მონაცემთა ცენტრებს და სხვა) და კონტროლებს, რაც ფინანსური ორგანიზაციის მიერ კრიტიკულად ან/და მნიშვნელოვნად იქნება იდენტიფიცირებული;

ბ.ბ) ფინანსური ორგანიზაცია სიღრმისეულად შეისწავლის და შეაფასებს სერტიფიცირებისა და აუდიტის ანგარიშების შინაარსსა და შედეგებს და დარწმუნდება, რომ სერტიფიცირება ან/და აუდიტის ანგარიშები არის აქტუალური და არ არის მოძველებული;

ბ.გ) სერტიფიცირების ან აუდიტის განმახორციელებელი მხარის კომპეტენცია და უნარები (მაგალითად, კვალიფიკაცია, ექსპერტიზა, შესრულებული სამუშაოს ხარისხი, როტაცია და სხვა) დამაკმაყოფილებელი იქნება ფინანსური ორგანიზაციისთვის;

ბ.დ) სერტიფიცირება ან აუდიტი განხორციელებულია მსოფლიოში აღიარებული სტანდარტების მიმართ და მოიცავს, მათ შორის, ძირითადი კონტროლების ოპერაციული ეფექტურობის შეფასებასაც;

ბ.ე) ფინანსური ორგანიზაცია ინარჩუნებს სახელშეკრულებო უფლებას თავისი შეხედულებისამებრ განახორციელოს ინდივიდუალური აუდიტი აუთსორსინგული ფუნქციის ფარგლებში.

**მუხლი 11. ქვეაუთსორსინგი**

1. ფინანსურ ორგანიზაციასთან გაფორმებული ღრუბლოვანი აუთსორსინგული მომსახურების შესახებ ხელშეკრულების ფარგლებში მომწოდებელმა შესაძლებელია დაიქირავოს მესამე მხარე, ორგანიზაცია, რომელიც ამ სახელმძღვანელოს მიზნებისთვის განიხილება როგორც ქვეაუთსორსერი.
2. ფინანსური ორგანიზაცია ვალდებულია მოსთხოვოს მომწოდებელს იმავე მოთხოვნების დაკმაყოფილება ქვეაუთსორსერის მიერ, რასაც თავად ითხოვს მომწოდებლისგან კონკრეტული ღრუბლოვანი აუთსორსინგული მომსახურების მიღების ფარგლებში ხელშეკრულებით გათვალისწინებული პირობების შესაბამისად.

**მუხლი 12. ეროვნული ბანკის უფლებამოსილება**

ეროვნული ბანკი უფლებამოსილია, თავისი საზედამხედველო მანდატისა და ფუნქციების გათვალისწინებით, ფინანსურ ორგანიზაციას მითითება მისცეს ამ სახელმძღვანელოთი განსაზღვრულ მოთხოვნებთან დაკავშირებით, მათ შორის, ფინანსური მომსახურების ან პროცესის კრიტიკული ან/და მნიშვნელოვანი ფუნქციების აუთსორსინგად მიჩნევის თაობაზე.