საქართველოს ეროვნული ბანკის პრეზიდენტის

ბრძანება №165/04
2023 წლის 30 ივნისი

ქ. თბილისი

მიკრობანკების კიბერუსაფრთხოების მართვის ჩარჩოს დამტკიცების შესახებ

„საქართველოს ეროვნული ბანკის შესახებ“ საქართველოს ორგანული კანონის მე-15 მუხლის პირველი პუნქტის „ზ“ ქვეპუნქტის, 48-ე მუხლის მე-3 პუნქტისა და 49-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტის საფუძველზე, **ვბრძანებ:**

მუხლი 1

დამტკიცდეს მიკრობანკების კიბერუსაფრთხოების მართვის ჩარჩო თანდართულ „მიკრობანკებში საინფორმაციო სისტემებისა და კიბერუსაფრთხოების მართვის ჩარჩოს აუდიტის სახელმძღვანელოსთან“ (დანართთან) ერთად.

მუხლი 2

ეს ბრძანება ამოქმედდეს გამოქვეყნებისთანავე.

საქართველოს ეროვნული ბანკის
პირველი ვიცე-პრეზიდენტი/
საქართველოს ეროვნული ბანკის პრეზიდენტის მოვალეობის შემსრულებელი — ნათელა თურნავა

მიკრობანკების კიბერუსაფრთხოების მართვის ჩარჩო

მუხლი 1. ზოგადი დებულებები

1. საქართველოში მოქმედ ყველა მიკრობანკს უნდა გააჩნდეს კიბერუსაფრთხოების მართვის ჩარჩო.
2. კიბერუსაფრთხოების მართვის ჩარჩო უნდა იყოს მიკრობანკის ზომისა და სირთულის შესაფერისი და შესაბამისობაში უნდა იყოს მიკრობანკის მიერ გაწეულ საქმიანობასთან.

3. კიბერუსაფრთხოების მართვის ჩარჩო სრულიად ინტეგრირებული უნდა იყოს მიკრობანკის მთლიანი რისკების მართვის პროცესში.

მუხლი 2. კიბერუსაფრთხოების მართვის ჩარჩოს კომპონენტები

კიბერუსაფრთხოების მართვის ჩარჩო უნდა მოიცავდეს შემდეგ ძირითად მიმართულებებს:
ა) რისკის იდენტიფიცირება – კიბერუსაფრთხოების რისკის გათვითცნობიერება მიკრობანკის მასშტაბით, რომელიც გულისხმობს კიბერუსაფრთხოების რისკის მართვას. აღნიშნული, თავის მხრივ, მოიცავს მიკრობანკის სისტემებთან, აქტივებთან, მონაცემებთან და პროცესებთან დაკავშირებულ კიბერუსაფრთხოების რისკის მართვას;

ბ) დაცვა – მიკრობანკის მიერ ადეკვატური კონტროლის გარემოს უზრუნველყოფას, დაინტერესებული მხარეებისთვის გასაწევი მომსახურების მიზნით;

გ) აღმოჩენა – კიბერუსაფრთხოების მოვლენებთან დაკავშირებული აღმოჩენითი მექანიზმების შემუშავება და დანერგვა;

დ) რეაგირება – კიბერუსაფრთხოების მოვლენასთან დაკავშირებული რეაგირების ფორმალიზებული მექანიზმების შემუშავება და ჩამოყალიბება;

ე) აღდგენა – კიბერუსაფრთხოების მოვლენებთან დაკავშირებული ფორმალიზებული აღდგენის გეგმის შემუშავება და ჩამოყალიბება.

მუხლი 3. კიბერუსაფრთხოების რისკის იდენტიფიცირება

მიკრობანკის მიერ კიბერუსაფრთხოების რისკის იდენტიფიცირების პროცესი უნდა შედგებოდეს შემდეგი საკითხებისგან/კომპონენტებისგან:

ა) აქტივების მართვა, რომელიც მოიცავს:

ა.ა) მიკრობანკის ფიზიკური მოწყობილობების, აპარატურისა და საინფორმაციო სისტემების სრულფასოვან აღრიცხვას;

ა.ბ) პროგრამული უზრუნველყოფისა და აპლიკაციების სრულფასოვან აღრიცხვას;

ა.გ) მიკრობანკში არსებული კომუნიკაციის არხებისა და ინფორმაციული ნაკადების დადგენას, შესწავლასა და ფორმალურ იდენტიფიცირებას;

ა.დ) მიკრობანკის მიერ გამოყენებული გარე (მესამე მხარის მიერ წარმოებული) საინფორმაციო სისტემების კატალოგს;

ა.ე) ფორმალიზებულ სისტემას, რომელიც მოიცავს მიკრობანკში არსებული რესურსების კლასიფიკაციას კრიტიკულობისა და ბიზნესპრიორიტეტულობის მიხედვით;

ა.ვ) მიკრობანკის ყველა თანამშრომლის როლისა და პასუხისმგებლობების ნათლად და გასაგებად განსაზღვრას კიბერუსაფრთხოების რისკის მართვის ჭრილში;

ა.ზ) მესამე მხარეებთან ურთიერთობებში, მათ შორის, მიკრობანკის მიმწოდებლებთან და კლიენტებთან, კიბერუსაფრთხოების როლებისა და პასუხისმგებლობების ნათლად და გასაგებად განსაზღვრას.

ბ) ბიზნესგარემოს, რომელიც მოიცავს:

ბ.ა) მიკრობანკის მისიის, მიზნებისა და საქმიანობის ფარგლებში კიბერუსაფრთხოების როლის განსაზღვრას;

ბ.ბ) კრიტიკული მომსახურების/პროცესების მიწოდების ფარგლებში დამოკიდებულებებისა და ფუნქციების განსაზღვრას;

ბ.გ) ბიზნესუწყვეტობის მაღალი დონის უზრუნველყოფას კრიტიკული მომსახურების მიწოდების ფარგლებში.

გ) მართვა:

გ.ა) მიკრობანკს უნდა გააჩნდეს ინფორმაციული უსაფრთხოების პოლიტიკა;

გ.ბ) ინფორმაციული უსაფრთხოების ფარგლებში, ყველა როლი და პასუხისმგებლობა შესაბამისობაში უნდა მოვიდეს მიკრობანკში არსებულ თანამშრომელთა შიდა როლებთან და ასევე გარე პარტნიორებთან;

გ.გ) მიკრობანკის მიერ სამართლებრივ ჭრილში ნაკისრი ვალდებულებები კიბერუსაფრთხოების სფეროში, მათ შორის, სამოქალაქო თავისუფლების და პირადობის დაცვის თვალსაზრისით, კარგად უნდა იყოს გათვითცნობიერებული მიკრობანკის მიერ;

გ.დ) მიკრობანკის აღმასრულებელი მმართველობისა და რისკების მართვის პროცესები უნდა მოიცავდეს კიბერუსაფრთხოების რისკს;

გ.ე) მიკრობანკის მიერ ახალი ან ინოვაციური პროდუქტების დანერგვის პროცესი უნდა ითვალისწინებდეს კიბერუსაფრთხოების რისკს;

გ.ვ) მიკრობანკის მიერ მესამე მხარეების შერჩევის/ურთიერთობის წარმართვის პროცესში

კიბერუსაფრთხოების რისკი უნდა იყოს გათვალისწინებული;

დ) კიბერუსაფრთხოების რისკების შეფასება:

დ.ა) მიკრობანკის ინფორმაციული აქტივები ფორმალიზებულად უნდა იყოს იდენტიფიცირებული;

დ.ბ) მიკრობანკმა, საფრთხეების და სისუსტეების შესახებ ინფორმაცია უნდა მიიღოს სხვადასხვა ინფორმაციის გაცვლის წყაროებიდან;

დ.გ) შიდა და გარე საფრთხეები ფორმალურად უნდა იყოს იდენტიფიცირებული;

დ.დ) კიბერუსაფრთხოების მოვლენების პოტენციური ზეგავლენა მიკრობანკზე იდენტიფიცირებული უნდა იყოს;

დ.ე) მიკრობანკი უნდა იყენებდეს მეთოდოლოგიას, რომლის მეშვეობითაც ის გამოავლენს საფრთხეებს, სისუსტეებს, ალბათობებსა და ზეგავლენას კიბერუსაფრთხოების რისკის დასადგენად.

მუხლი 4. დაცვა

მიკრობანკის მიერ შემუშავებული დაცვის პროცესი უნდა შედგებოდეს შემდეგი საკითხებისგან/კომპონენტებისგან:

ა) წვდომის კონტროლი:

ა.ა) მიკრობანკი უნდა ახორციელებდეს ავტორიზებული მომხმარებლებისა და მოწყობილობების სრულფასოვან მართვას;

ა.ბ) მიკრობანკის მიერ უნდა ხორციელდებოდეს კუთვნილი ინფორმაციული აქტივების წვდომის მართვა და დაცვა;

ა.გ) მიკრობანკი უნდა ახორციელებდეს ფიზიკური წვდომის მართვას, ხელმისაწვდომობასა და კონტროლს;

ა.დ) დისტანციური წვდომა ინფორმაციულ აქტივებზე სრულფასოვნად უნდა იყოს მართული მიკრობანკის მიერ;

ა.ე) მიკრობანკის მიერ წვდომის უფლებების განსაზღვრა უნდა ხორციელდებოდეს მინიმალური პრივილეგიის პრინციპის დაცვით და მოვალეობების გამიჯვნის პრინციპის შესაბამისად;

ა.ვ) უნდა ხორციელდებოდეს ქსელის მთლიანობის დაცვა, ქსელის გამიჯვნა/დანაწევრების პრინციპის გათვალისწინებით, სადაც ეს შესაძლებელია.

ბ) ცნობიერება და ტრენინგი:

ბ.ა) მიკრობანკის მიერ უნდა ხდებოდეს მიკრობანკის ყველა რგოლის თანამშრომლის, მათ შორის, აღმასრულებელი, საშუალო მენეჯერული და საოპერაციო რგოლების კიბერუსაფრთხოების ტრენინგი, არანაკლებ წელიწადში ერთხელ;

ბ.ბ) მიკრობანკის საინფორმაციო სისტემების ყველა მომხმარებელი ინფორმირებული უნდა იყოს კიბერრისკების შესახებ;

ბ.გ) მიკრობანკის პრივილეგირებულ მომხმარებლებს გათვითცნობიერებული უნდა ჰქონდეთ საკუთარი როლი და მიკრობანკის წინაშე ნაკისრი ვალდებულებები;

ბ.დ) მიკრობანკის მესამე მხარეებს გათვითცნობიერებული უნდა ჰქონდეთ კიბერუსაფრთხოების როლები და პასუხისმგებლობები;

ბ.ე) კიბერუსაფრთხოების ფარგლებში, მიკრობანკის დირექტორატს გათვითცნობიერებული უნდა ჰქონდეს საკუთარი როლი და ნაკისრი პასუხისმგებლობები;

ბ.ვ) მიკრობანკის ფიზიკური და საინფორმაციო უსაფრთხოების თანამშრომლებს კარგად უნდა ჰქონდეთ გათვითცნობიერებული საკუთარი როლები და ნაკისრი პასუხისმგებლობები.

გ) მონაცემთა დაცვა:

გ.ა) მიკრობანკში არსებული სტატიკური მონაცემები უნდა იყოს სათანადოდ დაცული;

გ.ბ) მიკრობანკში არსებული მოძრავი/ტრანზიტული მონაცემები უნდა იყოს სათანადოდ დაცული;

გ.გ) მიკრობანკი სრულფასოვნად უნდა მართავდეს ყველა ინფორმაციულ აქტივს (განადგურება, გაგზავნა, შენახვა/განლაგებისას);

გ.დ) მიკრობანკს უნდა გააჩნდეს მონაცემთა კონტროლისა და ინფორმაციის გაჟონვის პრევენციული მექანიზმი;

გ.ე) მიკრობანკს უნდა გააჩნდეს პროგრამული უზრუნველყოფის, მონაცემების/ინფორმაციის მთლიანობის შემოწმების მექანიზმი;

გ.ვ) პროგრამული უზრუნველყოფის ძირითადი და საცდელი გარემო ერთმანეთისგან უნდა იყოს გამიჯნული.

დ) ინფორმაციის დაცვის პროცესები და პროცედურები:

დ.ა) ინფორმაციული ტექნოლოგიების, მათ შორის, საინფორმაციო სისტემების საბაზისო კონფიგურაცია უნდა ჩამოყალიბდეს მიკრობანკის მიერ;

დ.ბ) უნდა არსებობდეს სისტემების განვითარების სასიცოცხლო ციკლი;

დ.გ) მიკრობანკს უნდა გააჩნდეს სისტემების კონფიგურაციის ცვლილების მართვის ფორმალური მექანიზმი/პროცესი;

დ.დ) მიკრობანკს უნდა გააჩნდეს მონაცემების/ინფორმაციის დაზღვევა/შენახვის ფორმალიზებული მექანიზმები, რომელიც თავის მხრივ მოიცავს ინფორმაციის აღდგენის პროცესის ტესტირებას;

დ.ე) მიკრობანკში მონაცემები უნდა განადგურდეს მიკრობანკის პოლიტიკის შესაბამისად;

დ.ვ) მიკრობანკი უნდა ზრუნავდეს ინფორმაციული აქტივების დაცვის პროცესის მუდმივად გაუმჯობესებაზე;

დ.ზ) დაცვითი ტექნოლოგიების ეფექტიანობა რეგულარულად უნდა გაანალიზდეს;

დ.თ) მიკრობანკს უნდა გააჩნდეს ინციდენტებზე რეაგირების სრულფასოვანი გეგმა;

დ.ი) მიკრობანკი უნდა ახორციელებდეს ინციდენტებზე რეაგირების გეგმის რეგულარულ ტესტირებას;

დ.კ) მიკრობანკს უნდა გააჩნდეს სისუსტეების მართვის გეგმა.

ე) შენარჩუნება:

ე.ა) მიკრობანკი უნდა ახორციელებდეს მიკრობანკის აქტივების მართვასთან დაკავშირებული ქმედებების დროულ აღრიცხვას, შესაბამისი, დამტკიცებული და აღიარებული პროცესის/ხელსაწყოების მეშვეობით;

ე.ბ) მიკრობანკის ინფორმაციული აქტივების დისტანციური მართვა უნდა იყოს ფორმალურად დამტკიცებული, აღრიცხული და განხორციელებული ისე, რომ არაავტორიზებული წვდომა იყოს აღკვეთილი;

ვ) დაცვითი ტექნოლოგიები:

ვ.ა) მიკრობანკს უნდა გააჩნდეს აუდიტის კვალის აღრიცხვის ფორმალიზებული მექანიზმი, რომელიც შეესაბამება მიკრობანკის პოლიტიკას;

ვ.ბ) პორტატიული მოწყობილობები დაცული უნდა იყოს და მათი გამოყენება მიკრობანკში უნდა იყოს შეზღუდული მიკრობანკის პოლიტიკის შესაბამისად;

ვ.გ) მიკრობანკის სისტემებზე და აქტივებზე წვდომა უნდა იყოს ფორმალურად გაკონტროლებული, მინიმალური წვდომის პრინციპის უზრუნველყოფით;

ვ.დ) მიკრობანკის კომუნიკაციის და მართვის ქსელი უნდა იყოს დაცული.

მუხლი 5. აღმოჩენა
მიკრობანკის მიერ ჩამოყალიბებული კიბერუსაფრთხოების მოვლენების აღმოჩენის პროცესი უნდა შედგებოდეს შემდეგი საკითხებისგან/კომპონენტებისგან:
ა) ანომალიები და მოვლენები:

ა.ა) მიკრობანკში უნდა არსებობდეს საინფორმაციო სისტემებისა და მომხმარებლებთან დაკავშირებული ქსელური ოპერაციებისა და მოსალოდნელი მონაცემთა ნაკადების საბაზისო გარემო;

ა.ბ) მიკრობანკში უნდა ხდებოდეს აღმოჩენილი მოვლენების ანალიზი იმისათვის, რომ მოხდეს პოტენციური კიბერშეტევის სამიზნეებისა და მეთოდების შესწავლა;

ა.გ) უნდა ხორციელდებოდეს კიბერუსაფრთხოების მოვლენებთან დაკავშირებული მოვლენების შეჯამება და პოტენციური კორელირება სხვადასხვა წყაროებთან;

ა.დ) მიკრობანკს უნდა გააჩნდეს ინციდენტის გაფრთხილების მექანიზმები, შესაბამისი რისკის ინდიკატორებისა და სხვა მეტრიკის სახით:

ბ) აღმოჩენითი პროცესები:

ბ.ა) მიკრობანკს უნდა გააჩნდეს კიბერუსაფრთხოების მოვლენის აღმოჩენასთან დაკავშირებული, მკაფიოდ განსაზღვრული როლები და პასუხისმგებლობები;

ბ.ბ) უნდა ხორციელდებოდეს მოვლენის აღმოჩენის პროცესების (მათ შორის, შესაბამისი კონტროლების) ტესტირება;

ბ.გ) უნდა ხდებოდეს კონკრეტული მოვლენის აღმოჩენასთან დაკავშირებული ინფორმაციის შეტყობინება შესაბამის პირებთან და უწყებებთან;

ბ.დ) მიკრობანკის დირექტორატმა უნდა შეიმუშაოს მსხვილი კიბერუსაფრთხოების მოვლენის შესახებ საქართველოს ეროვნული ბანკისათვის შეტყობინების მექანიზმი;

ბ.ე) მსხვილი კიბერუსაფრთხოების მოვლენის მაღალი ალბათობით მოლოდინის ან დაფიქსირების შემთხვევაში, მიკრობანკი ვალდებულია დაუყოვნებლივ აცნობოს აღნიშნულის შესახებ საქართველოს ეროვნულ ბანკს;

ბ.ვ) უნდა ხდებოდეს მიკრობანკის მოვლენათა აღმოჩენის პროცესების მუდმივი გაუმჯობესება.

მუხლი 6. რეაგირება
კიბერუსაფრთოხების მოვლენებთან დაკავშირებული რეაგირების პროცესი უნდა შედგებოდეს შემდეგი საკითხებისგან/კომპონენტებისგან:
ა) რეაგირების დაგეგმვა:

ა.ა) მიკრობანკს უნდა გააჩნდეს კიბერუსაფრთხოების მოვლენებთან დაკავშირებული ფორმალიზებული რეაგირების გეგმა, რაც, თავის მხრივ, მოიცავს მის მზადყოფნას კიბერუსაფრთხოების შესაძლო/მოსალოდნელ რისკთან მიმართებაში;

ა.ბ) რეაგირების გეგმა უნდა ამოქმედდეს კონკრეტული მოვლენის დაფიქსირების დროს ან მოვლენის დაფიქსირების შემდეგ;

ბ) შეტყობინება:

ბ.ა) მიკრობანკის თანამშრომლებს კარგად უნდა ჰქონდეთ გათვითცნობიერებული საკუთარი როლი/როლები კიბერუსაფრთხოების მოვლენაზე რეაგირებისას;

ბ.ბ) უნდა ხორციელდებოდეს კიბერუსაფრთხოების მოვლენების შეტყობინება დადგენილი მოთხოვნებისა და კრიტერიუმების შესაბამისად;

ბ.გ) კიბერუსაფრთხოების მოვლენებთან დაკავშირებული ინფორმაციის გაცვლა უნდა ხდებოდეს რეაგირების გეგმის შესაბამისად;

ბ.დ) კიბერუსაფრთოხების მოვლენებთან დაკავშირებული ქმედებების კოორდინირება სხვა უწყებებთან უნდა ხდებოდეს რეაგირების გეგმის შესაბამისად;

გ) ანალიზი:

გ.ა) მიკრობანკი უნდა ახორციელებდეს სხვადასხვა სისტემიდან (აღმოჩენითი კონტროლი) მიღებული შეტყობინებების მოკვლევასა და ანალიზს;

გ.ბ) მიკრობანკი სრულად უნდა ათვითცნობიერებდეს კიბერუსაფრთხოების ინციდენტის ზეგავლენას მის საქმიანობაზე;

გ.გ) საჭიროების შემთხვევაში უნდა განხორციელდეს ინციდენტთან დაკავშირებული ექსპერტიზა;

გ.დ) მიკრობანკი უნდა ახდენდეს ინციდენტების კლასიფიკაციას, ინციდენტებზე რეაგირების გეგმის შესაბამისად.

დ) მიტიგაცია/შერბილება:

დ.ა) მიკრობანკის ვალდებულებაა, რომ მოხდეს კიბერუსაფრთხოების ინციდენტის ზეგავლენის სათანადო შერბილება, თუ ინციდენტი მიკრობანკში დაფიქსირდა;

დ.ბ) მიკრობანკი უნდა ახორციელებდეს ახლად აღმოჩენილი სისუსტეების შესწავლას და მოცემული სისუსტეებიდან გამომდინარე საფრთხეების მიტიგაციას ან მიღებას, თუ მოცემული სისუსტე მნიშვნელოვან საფრთხეს არ წარმოადგენს მიკრობანკისთვის;

ე) გაუმჯობესება:

ე.ა) მიკრობანკის ინციდენტებზე რეაგირების გეგმა უნდა ითვალისწინებდეს წარსულ გამოცდილებასა და პრაქტიკას;

ე.ბ) უნდა ხდებოდეს ინციდენტებზე რეაგირების სტრატეგიის რეგულარული განახლება.

მუხლი 7. აღდგენა

კიბერუსაფრთოხების მოვლენისგან აღდგენის პროცესი უნდა შედგებოდეს შემდეგი საკითხებისგან/კომპონენტებისგან:

ა) მიკრობანკს უნდა გააჩნდეს კიბერუსაფრთხოების მოვლენის შემდეგ ოპერაციების აღდგენის ფორმალური მექანიზმი;

ბ) აღდგენის პროცესი, თავის მხრივ, უნდა ითვალისწინებდეს წარსულში დაფიქსირებული

მოვლენებისგან მიღებულ გამოცდილებას;

გ) მიკრობანკს უნდა გააჩნდეს საზოგადოებასთან ურთიერთობის ფორმალური პროცედურა და მექანიზმი, რომლის ფარგლებშიც მიკრობანკი უზრუნველყოფს საზოგადოების ინფორმირებას კიბერუსაფრთხოების ინციდენტის დაფიქსირებისას, ამის საჭიროების შემთხვევაში და ასევე რეპუტაციული რისკის მართვას;

დ) მიკრობანკი უნდა ახორციელებდეს კონკრეტულ მოვლენასთან დაკავშირებით განხორციელებული ქმედებების შეტყობინებას შიდა დაინტერესებულ მხარეებთან, მათ შორის, მიკრობანკის ხელმძღვანელობასთან.

მუხლი 8. კიბერუსაფრთხოების პროგრამის მართვა

1. მიკრობანკის ხელმძღვანელობა ვალდებულია რეგულარულად გადაამოწმოს მიკრობანკის კიბერუსაფრთხოების/საინფორმაციო უსაფრთხოების პროგრამის ეფექტიანობა.
2. მიკრობანკმა ყოველწლიურად უნდა ჩაატაროს კიბერუსაფრთხოებასთან დაკავშირებული თვითშეფასება.

3. მიკრობანკმა უნდა დაიცვას მსოფლიო ბანკთაშორისი საფინანსო ტელეკომუნიკაციების საზოგადოების (SWIFT) მომხმარებელთა უსაფრთხოების პროგრამის სავალდებულო მოთხოვნები.

4. მიკრობანკმა, არანაკლებ წელიწადში ერთხელ, უნდა ჩაატაროს შეღწევადობის ტესტირება, რომელიც მოიცავს მიკრობანკის ყველა იმ საინფორმაციო სისტემას, რომელიც ქსელში არის ჩართული.

5. მიკრობანკი ვალდებულია ყოველწლიურად ჩაატაროს მიკრობანკის კიბერუსაფრთხოების მართვის ჩარჩოს ყველა კომპონენტის დამოუკიდებელი აუდიტი, ამ ბრძანებით დამტკიცებული „მიკრობანკებში საინფორმაციო სისტემებისა და კიბერუსაფრთხოების მართვის ჩარჩოს აუდიტის სახელმძღვანელოს“ შესაბამისად.

დანართი

მიკრობანკებში საინფორმაციო სისტემებისა და კიბერუსაფრთხოების მართვის ჩარჩოს აუდიტის სახელმძღვანელო

მუხლი 1. ზოგადი დებულება

მიკრობანკებში საინფორმაციო სისტემებისა და კიბერუსაფრთხოების მართვის ჩარჩოს აუდიტის სახელმძღვანელო (შემდგომში – სახელმძღვანელო) განსაზღვრავს მიკრობანკებში საინფორმაციო სისტემებისა და კიბერუსაფრთხოების მართვის ჩარჩოს აუდიტის (შემდგომში – აუდიტი) პროცესის, აუდიტის ანგარიშისა და აუდიტის პროცესში მონაწილე აუდიტორთა გუნდის კომპეტენციის, მიუკერძოებლობისა და ოპერირების მოთხოვნებს.

მუხლი 2. ტერმინთა განმარტება

სახელმძღვანელოში გამოყენებულ ტერმინებს აქვთ შემდეგი მნიშვნელობა:

ა) **საინფორმაციო სისტემების აუდიტი** – ინფორმაციული ტექნოლოგიების (შემდგომში – IT) ინფრასტრუქტურისა და საბანკო სისტემების ფარგლებში არსებული ადმინისტრაციული, ტექნიკური და ფიზიკური კონტროლების გარემოს რისკებზე დაფუძნებული, სისტემატური, დამოუკიდებელი და დოკუმენტირებული შეფასების პროცესი;

ბ) **კიბერუსაფრთხოების აუდიტი** – კიბერუსაფრთხოების მართვის ჩარჩოს ფარგლებში არსებული ადმინისტრაციული, ტექნიკური და ფიზიკური კონტროლების გარემოს რისკებზე დაფუძნებული, სისტემატური, დამოუკიდებელი და დოკუმენტირებული შეფასების პროცესი;

გ) **კომბინირებული აუდიტი** – ერთ მიკრობანკში ერთდროულად ორ ან მეტ მართვის სისტემაზე განხორციელებული აუდიტი;

დ) **აუდიტის გავრცელების სფერო** – აუდიტის მოცულობა და საზღვრები, რაც განსაზღვრავს მიკრობანკის ყველა იმ პროცესსა და დაკავშირებულ ელემენტს, რომლის მიმართაც უნდა განხორციელდეს აუდიტი;

ე) **აუდიტის პროგრამა** – დროის გარკვეულ მონაკვეთში და კონკრეტული მიზნისკენ მიმართული ერთი ან რამდენიმე აუდიტის ფარგლებში დაგეგმილი ღონისძიებების ერთობლიობა, აუდიტის საქმიანობისა და მოქმედებების აღწერა;

ვ) **აუდიტის კრიტერიუმები** – მოთხოვნებისა და მითითებების ჩამონათვალი, რომლის მიმართ ხორციელდება მიკრობანკის შესაბამისობის შეფასება;

ზ) **აუდიტის მტკიცებულება** – აუდიტის კრიტერიუმების შესაბამისი ჩანაწერები, ფაქტები ან სხვა სახის გადამოწმებადი ინფორმაცია;

თ) **აუდიტის დაკვირვება** – შეგროვებული აუდიტის მტკიცებულებების აუდიტის კრიტერიუმებთან შედარების შედეგები;

ი) **აუდიტის ანგარიში** – აუდიტის შედეგი, აუდიტის მიზნების და აუდიტის ყველა დაკვირვების გათვალისწინების შემდეგ;

კ) **აუდიტის გუნდი** – აუდიტის განმახორციელებელი გარე აუდიტორული ფირმის წარმომადგენელი ორი ან რამდენიმე აუდიტორი;

ლ) **აუდიტორი** – აუდიტის განმახორციელებელი პირი;

მ) **ტექნიკური ექსპერტი** – პირი, რომელსაც გააჩნია აუდიტის გავრცელების სფეროში არსებული კონკრეტული საკითხის ექსპერტული ცოდნა/გამოცდილება, რის საფუძველზეც ახორციელებს აუდიტის გუნდის მხარდაჭერას;

ნ) **მართვის სისტემა** – მიკრობანკში არსებული პოლიტიკების, პროცესების, პროცედურებისა და კონტროლების გარემოს ერთობლიობა, რაც უზრუნველყოფს სტრატეგიული მიზნების მიღწევისათვის საჭირო ქმედებების ეფექტურ შესრულებას.

მუხლი 3. აუდიტის მიზანი და გავრცელების სფერო

1. აუდიტის მიზანია მიკრობანკის საინფორმაციო სისტემებისა და კიბერუსაფრთხოების მართვის ჩარჩოს საქართველოს ეროვნული ბანკის (შემდგომში – ეროვნული ბანკი) მიერ დადგენილ მინიმალურ მოთხოვნებთან შესაბამისობის შეფასება, რის საფუძველზეც დგება აუდიტის ანგარიში, რომლის მოთხოვნების შესრულება სავალდებულოა.
2. მიკრობანკს შეუძლია ერთმანეთისგან დამოუკიდებლად ჩაატაროს საინფორმაციო სისტემებისა და კიბერუსაფრთხოების მართვის ჩარჩოს აუდიტი ან ჩაატაროს კომბინირებული აუდიტი, რომლის ფარგლებში შეაფასებს აუდიტის გავრცელების სფეროში განსაზღვრულ თითოეულ სტანდარტთან და საზედამხედველო მოთხოვნებთან შესაბამისობას.

3. კიბერუსაფრთხოების მართვის ჩარჩოს აუდიტი უნდა განხორციელდეს ამ ბრძანების შესაბამისად.

4. საინფორმაციო სისტემების აუდიტი უნდა განხორციელდეს ეროვნული ბანკის პრეზიდენტის ბრძანებით დამტკიცებული „მიკრობანკების მიერ საოპერაციო რისკების მართვის შესახებ“ დებულების შესაბამისად, COBIT ან სხვა საერთაშორისოდ აღიარებული სტანდარტის/ჩარჩოს მიმართ ეროვნულ ბანკთან შეთანხმებით.

მუხლი 4. აუდიტის განხორციელების უფლებამოსილების მქონე პირები

1. მიკრობანკი ვალდებულია, უზრუნველყოს აუდიტის განხორციელება ისეთი აუდიტის გუნდის მიერ, რომელიც ოპერაციულად დამოუკიდებელია მიკრობანკისგან და აკმაყოფილებს ამ სახელმძღვანელოს მე-5 მუხლით განსაზღვრულ მინიმალურ მოთხოვნებს.
2. მიკრობანკს უფლება აქვს, განახორციელოს აუდიტი შიდა აუდიტის ერთეულის მიერ, რაც წინასწარ უნდა იქნეს შეთანხმებული ეროვნულ ბანკთან.

3. მიკრობანკის აუდიტის გარე აუდიტორული ფირმის მიერ განხორციელების შემთხვევაში:

ა) მიკრობანკი ვალდებულია შერჩეულ აუდიტორულ ფირმასთან ხელშეკრულების გაფორმებამდე,

უზრუნველყოს ეროვნული ბანკის ინფორმირება. შეტყობინება უნდა მოიცავდეს ინფორმაციას აუდიტორული ფირმის, აუდიტის გუნდის წევრების, მათი კვალიფიკაციის, აუდიტის პროცესის სავარაუდო დაწყებისა და დასრულების შესახებ;

ბ) მიკრობანკმა აუდიტორულ ფირმასთან დადებული ხელშეკრულებით უნდა უზრუნველყოს მიკრობანკის ინფორმაციის კონფიდენციალურობისა და გაუთქმელობის დაცვა.

4. მიკრობანკი ვალდებულია, კიბერუსაფრთხოების მართვის ჩარჩოს აუდიტის ფარგლებში უზრუნველყოს აუდიტის მთლიანი გუნდის/შიდა აუდიტის ერთეულის ცვლილება ყოველი უწყვეტი 2-წლიანი პერიოდის გასვლის შემდეგ, შემდეგი პირობების გათვალისწინებით:

ა) შიდა აუდიტის ერთეულის მიერ უწყვეტად 2 წლის განმავლობაში განხორციელებული აუდიტის შემთხვევაში, მიკრობანკმა მომდევნო წლიდან უნდა უზრუნველყოს აუდიტის ჩატარება გარე აუდიტორული ფირმის მიერ;

ბ) იმავე აუდიტის გუნდის ან შიდა აუდიტის ერთეულის მიერ აუდიტის პროცესის წარმართვა დასაშვებია, სულ მცირე, 2-წლიანი პერიოდის გასვლის შემდეგ, რომელიც აითვლება ამ პუნქტით განსაზღვრული ვადის ამოწურვის მომენტიდან.

მუხლი 5. აუდიტის გუნდის კომპეტენცია და მოთხოვნები

1. აუდიტის გუნდის შერჩევის პროცესში მიკრობანკი უნდა დარწმუნდეს, რომ აუდიტორულ ფირმას/აუდიტის გუნდს გააჩნია:

ა) აუდიტის ჩატარების მეთოდოლოგია, რომელიც შეესაბამება აუდიტის საერთაშორისო სტანდარტებს;

ბ) ხარისხის მართვის სისტემა, რომელიც საშუალებას მისცემს:

ბ.ა) განსაზღვროს აუდიტის გუნდის შემადგენლობა აუდიტორების კომპეტენციაზე, კვალიფიკაციასა და გამოცდილებაზე დაყრდნობით; საჭიროების შემთხვევაში, აუდიტის გუნდს შესაძლებელია დაემატოს ტექნიკური ექსპერტი/ექსპერტები, რომელსაც (რომლებსაც) გააჩნია(თ) სპეციფიკური კომპეტენცია აუდიტის გავრცელების სფეროში არსებული საკითხების/ტექნოლოგიების/სისტემების ფარგლებში;

ბ.ბ) შეაფასოს და აკონტროლოს აუდიტორების და ტექნიკური ექსპერტების საქმიანობა აუდიტის პროცესში.

2. აუდიტის გუნდის წევრების კომპეტენცია უნდა აკმაყოფილებდეს არანაკლებ შემდეგ მოთხოვნებს:

ა) აუდიტის პრინციპების, პროცესებისა და მეთოდების, მათ შორის, სხვადასხვა რისკის ტიპების და რისკებზე დაფუძნებული აუდიტის მიდგომების ცოდნა;

ბ) მართვის სისტემების საერთაშორისო სტანდარტების (მაგ.: ISO 27001, NIST, COBIT და სხვა) ცოდნა და პრაქტიკაში გამოყენების გამოცდილება;

გ) აუდიტის გავრცელების სფეროს შესაბამისი ტექნიკური ცოდნა, გამოცდილება და უნარები;

დ) აუდიტორების კომპეტენციებისა და გამოცდილების დამადასტურებელი საერთაშორისოდ აღიარებული მოქმედი სერტიფიკატ(ებ)ი (მაგ.: CISA, ISO 27001 LA და სხვა);

ე) საზედამხედველო ორგანოების მიერ აუდირებული მიკრობანკის მიმართ არსებული რეგულაციების/მოთხოვნების სრულფასოვანი ცოდნა;

ვ) აუდიტირებული მიკრობანკის საქმიანობის ანალიზის უნარი, რათა მის აქტივობებზე, პროდუქტებსა და მომსახურებებზე დაყრდნობით შეძლოს სრულფასოვანი და ეფექტური აუდიტის განხორციელება.

მუხლი 6. აუდიტის პროგრამა

მიკრობანკმა უნდა უზრუნველყოს, რომ აუდიტის პროგრამის/გეგმის შემუშავების დროს აუდიტის გუნდის მიერ დაკმაყოფილდეს შემდეგი მოთხოვნები:

ა) აუდიტის გუნდმა უნდა განსაზღვროს აუდიტის პროგრამა/გეგმა აუდიტის მიზნებისა და გავრცელების სფეროს შესაბამისად. პროგრამაში გათვალისწინებული უნდა იყოს შიდა თუ გარე რისკები და შესაძლებლობები, რამაც შესაძლოა გავლენა იქონიოს აუდიტის პროგრამის განხორციელებაზე. აუდიტის გუნდის მიერ გამოყენებული აუდიტის პროგრამა წინასწარ უნდა იქნეს შეთანხმებული მიკრობანკთან;

ბ) აუდიტის გუნდმა უნდა შეარჩიოს და განსაზღვროს აუდიტის ჩატარების ეფექტური მეთოდები. აუდიტის ჩატარება შესაძლებელია ადგილზე, დისტანციურად ან მათი კომბინაციით. აღნიშნული მეთოდების გამოყენება უნდა იყოს დაბალანსებული დაკავშირებული რისკებისა და შესაძლებლობების გათვალისწინებით;

გ) აუდიტის გუნდს შეუძლია გამოიყენოს ანგარიშგების საკუთარი პროცედურები, თუმცა უზრუნველყოფილი უნდა იქნეს სულ მცირე შემდეგი:

გ.ა) აუდიტის გუნდმა მიკრობანკს უნდა წარუდგინოს წერილობითი აუდიტის ანგარიში მიკრობანკის შესაბამისობის შესახებ იმ კრიტერიუმებთან და მოთხოვნებთან, რომელთა მიმართაც განხორციელდა აღნიშნული აუდიტი;

გ.ბ) აუდიტის დასრულებამდე უნდა განხორციელდეს შეხვედრა აუდიტის გუნდსა და მიკრობანკის ხელმძღვანელობას შორის, რომლის ფარგლებშიც:

გ.ბ.ა) აუდიტის გუნდის ლიდერმა უნდა განახორციელოს მიკრობანკის შესაბამისობის შეფასების შეჯამება იმ კრიტერიუმებთან და მოთხოვნებთან, რომლის მიმართაც განხორციელდა აღნიშნული აუდიტი;

გ.ბ.ბ) მიკრობანკის ხელმძღვანელობას უნდა ჰქონდეს შესაძლებლობა, დასვას კითხვები და მოიკვლიოს აუდიტის ფარგლებში იდენტიფიცირებული დაკვირვებების/ხარვეზების მიზეზები და მათი საფუძველი;

დ) აუდიტის განსახორციელებლად აუდიტის გუნდმა სათანადოდ უნდა განსაზღვროს აუდიტის ხანგრძლივობა, რათა სრულყოფილად განახორციელოს მიკრობანკის შეფასება აუდიტის გავრცელების სფეროს ფარგლებში. აუდიტის ხანგრძლივობის განსასაზღვრად გათვალისწინებული უნდა იქნას სულ მცირე შემდეგი ფაქტორები:

დ.ა) მიკრობანკის ზომა (საინფორმაციო სისტემების რაოდენობა, ფილიალების/ოფისების რაოდენობა, თანამშრომელთა რაოდენობა და სხვ.);

დ.ბ) მიკრობანკის კომპლექსურობა;

დ.გ) მიკრობანკის სხვადასხვა მომსახურებების განსახორციელებლად გამოყენებული ტექნოლოგიების მრავალფეროვნება და მოცულობა;

დ.დ) აუდიტის გავრცელების სფეროში განსაზღვრული სხვადასხვა სტანდარტებისა და საზედამხედველო მოთხოვნების მოცულობა;

დ.ე) ძირითადი საბანკო საქმიანობისა და მასთან დაკავშირებული საინფორმაციო სისტემების ფარგლებში გამოყენებული აუთსორსინგისა და მესამე მხარეების მომსახურების მოცულობა.

მუხლი 7. აუდიტის პროცესი

1. აუდიტისთვის მზადების/დაგეგმვის პროცესში, მიკრობანკმა უნდა უზრუნველყოს, რომ:
ა) აუდიტის პროცესის დაწყებამდე აუდიტის გუნდმა განახორციელოს მოსამზადებელი სამუშაოები, რომლის ჭრილში სრულყოფილად მოახდენს აუდიტირებული მიკრობანკის, მისი ფუნქციების/მომსახურებებისა და რისკების პროფილის შესწავლას. მოსამზადებელ ეტაპზე აუდიტის გუნდს შეუძლია მიკრობანკიდან, საჭიროებისამებრ, გამოითხოვოს მინიმუმ შემდეგი ინფორმაცია:

ა.ა) ზოგადი ინფორმაცია მიკრობანკისა და მისი მომსახურებების შესახებ (მდებარეობის, ზომის, ფუნქციების, მესამე მხარეების შესახებ, რომლებიც უზრუნველყოფენ მიკრობანკისთვის ძირითადი

საბანკო მომსახურების მიწოდებას);

ა.ბ) IT და ინფორმაციული უსაფრთხოების სრული დოკუმენტაცია (პოლიტიკები, პროცედურები, პროცესები და სახელმძღვანელოები) აუდიტის გავრცელების სფეროს ფარგლებში;

ა.გ) სხვადასხვა სახის რეპორტები და ჩანაწერები, მათ შორის, შიდა და გარე აუდიტის ანგარიშები, ინფორმაციული უსაფრთხოების დამოუკიდებელი შეფასებისა და თვითშეფასების ანგარიშები.

ბ) აუდიტის დაწყებამდე განიხილოს, თუ რა სახის დოკუმენტაციისა და ჩანაწერების მიწოდება იქნება შესაძლებელი აუდიტის გუნდისთვის მათი კონფიდენციალურობიდან და სენსიტიურობიდან გამომდინარე;

გ) აუდიტის გუნდმა შეაფასოს, რამდენად ეფექტური იქნება აუდიტი მისთვის მიწოდებულ დოკუმენტებზე/ინფორმაციაზე დაყრდნობით და რამდენად იქნება მიღწეული აუდიტის მიზანი. თუ აუდიტის გუნდი გადაწყვეტს, რომ ეფექტური აუდიტი არ იქნება უზრუნველყოფილი მხოლოდ აღნიშნულ ინფორმაციაზე დაყრდნობით, აუდიტირებული მიკრობანკისთვის უნდა იქნეს შეთავაზებული და შეთანხმებული ალტერნატიული მეთოდები/გადაწყვეტილებები, რათა მიღწეულ იქნეს აუდიტის მიზანი.

2. აუდიტის პროცესი უნდა განხორციელდეს არანაკლებ 2 ეტაპად:

ა) პირველი ეტაპის დროს აუდიტის გუნდმა უნდა განიხილოს და შეაფასოს ყველა ის დოკუმენტაცია და ინფორმაცია, რაც გამოთხოვილი იყო მათ მიერ აუდიტის მოსამზადებელ ეტაპზე. აღნიშნულ ეტაპზე აუდიტის გუნდმა უნდა:

ა.ა) შეისწავლოს აუდიტირებული მიკრობანკის პროცესები, ოპერაციები და ფუნქციები, რათა განსაზღვროს მომდევნო ეტაპზე შესასრულებელი აუდიტის აქტივობები;

ა.ბ) განიხილოს დოკუმენტირებული პროცესები და კონტროლები, რათა დადგინდეს აუდიტის კრიტერიუმებთან შესაძლო შესაბამისობა და გამოავლინოს შესაძლო ხარვეზები, ნაკლოვანებები და კონფლიქტები.

ბ) მეორე ეტაპი მოიაზრებს ინტერვიუების და შეხვედრების ჩანიშვნას მიკრობანკის შესაბამის წარმომადგენლებთან, რათა:

ბ.ა) განხორციელდეს პირველი ეტაპის დროს იდენტიფიცირებული ხარვეზების/კონფლიქტების ვალიდაცია;

ბ.ბ) შეფასდეს, რამდენად შესაბამისობაშია მიკრობანკში არსებული პროცესები მიკრობანკის მიზნებთან, შემუშავებულ პოლიტიკასა და პროცედურებთან;

ბ.გ) შეფასდეს მიკრობანკში დანერგილი IT და ინფორმაციული უსაფრთხოების კონტროლების ოპერაციული ეფექტურობა.

3. აუდიტირებულმა მიკრობანკმა აუდიტის პროცესში უნდა გამოყოს ერთი ან რამდენიმე წარმომადგენელი, რომელიც უნდა დაეხმაროს აუდიტის გუნდს და იმოქმედოს აუდიტის გუნდის ლიდერის ან აუდიტორის მოთხოვნის შესაბამისად. მისი პასუხისმგებლობები უნდა მოიცავდეს:

ა) აუდიტორების დახმარებას მიკრობანკის მხრიდან ინტერვიუებში მონაწილე პირების იდენტიფიცირებასა და დროისა და ადგილის დადასტურებაში;

ბ) აუდიტორებისთვის მიკრობანკის დაცულ ადგილებში დაშვების უფლების მოპოვებას;

გ) აუდიტის გუნდის წევრების გაცნობას აუდიტირებული მიკრობანკის დაშვების, უსაფრთხოების, კონფიდენციალურობისა და სხვა წესებთან;

დ) აუდიტის პროცესისა და აუდიტის ფარგლებში დაგეგმილი სხვადასხვა აქტივობების

მეთვალყურეობას, საჭიროების შემთხვევაში;

ე) აუდიტის პროცესში აუდიტორებისთვის საჭირო განმარტებებისა და ინფორმაციის შეკრებასა და მიწოდებას.

მუხლი 8. აუდიტის ანგარიში

1. მიკრობანკისთვის მიწოდებული აუდიტის ანგარიში უნდა შედგებოდეს შემოწმების/აუდიტის სრული, ზუსტი, ლაკონური და მკაფიო ჩანაწერებისგან და უნდა მოიცავდეს, სულ მცირე, შემდეგ ინფორმაციას:

ა) მიკრობანკის რისკების პროფილისა და კონტროლების გარემოს შემაჯამებელ შეფასებას, მათ შორის, განხილული დოკუმენტების შემაჯამებელ შეფასებას;

ბ) აუდიტის შედეგების შემაჯამებელ სტატისტიკას გრაფიკულად ან სიტყვიერი სახით, რომელიც მოიცავს შემდეგს:

ბ.ა) იდენტიფიცირებული ხარვეზები/რისკები კრიტიკულობის მიხედვით;

ბ.ბ) კონკრეტულ სტანდარტთან თუ მარეგულირებელ მოთხოვნებთან შესაბამისობის დადგენა პროცენტული ან/და რაოდენობრივი მაჩვენებლით;

გ) აუდიტის სრული ხანგრძლივობა და აუდიტის თითოეული ეტაპის ფარგლებში დახარჯული დრო, მათ შორის, დოკუმენტაციის განხილვის, დისტანციურად ან ადგილზე შემოწმებისა და აუდიტის ანგარიშის მოსამზადებლად გამოყენებული დრო;

დ) აუდიტის მეთოდოლოგია, რომელიც გამოყენებულ იქნა კონკრეტულ სტანდარტებთან და საზედამხედველო მოთხოვნებთან შესაბამისობის დასადგენად. მეთოდოლოგია ასევე უნდა მოიცავდეს ტესტირების პროცედურებსა და გამოყენებულ შერჩევის მეთოდოლოგიას;

ე) აუდიტის გავრცელების სფერო, სადაც განსაზღვრული იქნება მიკრობანკის პროცესების, დოკუმენტების სია, რომლის შეფასება მოხდა აუდიტის პროცესში, ასევე, იმ სტანდარტებისა თუ საზედამხედველო მოთხოვნების ჩამონათვალი, რომელთა მიმართაც განხორციელდა მიკრობანკის პროცესების შესაბამისობის შეფასება;

ვ) აუდიტის პროცესში ჩართული აუდიტის გუნდის/შიდა აუდიტის ერთეულის წევრების სია;

ზ) მიკრობანკის თანამშრომელთა სია (სახელი, გვარი, პოზიცია), რომლებიც ჩართულნი იყვნენ აუდიტის პროცესში და რომლებთანაც განხორციელდა ინტერვიუები აუდიტის მსვლელობის დროს სხვადასხვა პროცესების თუ საკითხების განსახილველად;

თ) შეფასების სისტემა, რომლის მიხედვითაც აუდიტის გუნდმა/შიდა აუდიტის ერთეულმა მოახდინა იდენტიფიცირებული შეუსაბამობების/რისკების კრიტიკულობის შეფასება;

ი) აუდიტის შედეგებისა და შესაბამისობის შეფასება, რომელიც უნდა მოიცავდეს, სულ მცირე, შემდეგ ინფორმაციას:

ი.ა) პოზიტიური და ნეგატიური დაკვირვებები აუდიტის გავრცელების სფეროში განსაზღვრული სტანდარტების/საზედამხედველო ჩარჩოს თითოეული კრიტერიუმის ჭრილში;

ი.ბ) თითოეული მოთხოვნის ფარგლებში იდენტიფიცირებული ნებისმიერი შეუსაბამობის დეტალური აღწერა. აუდიტის ანგარიშის დანართის სახით წარმოდგენილ უნდა იქნეს აღნიშნული შეუსაბამობების დამადასტურებელი ობიექტური მტკიცებულებები (მსგავსის არსებობის შემთხვევაში) და უნიკალური კავშირი შესაბამის მოთხოვნაზე;

ი.გ) მიკრობანკის შესაბამისობის შეფასება თითოეული მოთხოვნის/კრიტერიუმის ჭრილში ამ სახელმძღვანელოს მე-9 მუხლის მე-2 პუნქტის შესაბამისად;

ი.დ) აუდიტის ანგარიშში წარმოდგენილი ხარვეზების/რისკების კრიტიკულობის შეფასება ამ სახელმძღვანელოს მე-9 მუხლის მე-3 პუნქტის შესაბამისად;

ი.ე) რეკომენდაციები თითოეული ხარვეზის ჭრილში, რომლის გათვალისწინების შემთხვევაში მიკრობანკი შესაბამისობაში მოვა კონკრეტულ მოთხოვნასთან/კრიტერიუმთან.

2. მიკრობანკი ვალდებულია ეროვნულ ბანკს წარუდგინოს აუდიტის ანგარიში და სამოქმედო გეგმა აუდიტის დასრულებიდან არაუმეტეს 1 თვის ვადაში.

მუხლი 9. შეფასების სისტემა

1. მიკრობანკის აუდიტის ფარგლებში აუდიტის თითოეული კრიტერიუმის შეფასება უნდა განხორციელდეს შემდეგი სიმწიფის შკალის შესაბამისად:

ა) **დონე 0:** მიკრობანკში არ არის დანერგილი აუდიტის კრიტერიუმის შესაბამისი პროცესები და კონტროლების გარემო;

ბ) **დონე 1:** მიკრობანკში დანერგილია არაფორმალიზებული პროცესები და ინტუიციური/არაორგანიზებული კონტროლები/პრაქტიკები. შეინიშნება დიდი რაოდენობით კონტროლების დიზაინისა და ოპერაციული ეფექტურობის ხარვეზები;

გ) **დონე 2:** მიკრობანკში დანერგილია არაფორმალიზებული პროცესები და მეტად ორგანიზებული კონტროლები/პრაქტიკები. შეინიშნება მცირე რაოდენობით კონტროლების დიზაინისა და ოპერაციული ეფექტურობის ხარვეზები;

დ) **დონე 3:** მიკრობანკში დანერგილია ფორმალიზებული პროცესები და სრულყოფილი/ორგანიზებული კონტროლების გარემო. შეინიშნება მცირე რაოდენობით კონტროლების ოპერაციული ეფექტურობის ხარვეზები;

ე) **დონე 4:** მიკრობანკში დანერგილია ფორმალიზებული პროცესები და სრულყოფილი/ორგანიზებული კონტროლების გარემო, რომლის ეფექტურობა არის გაზომვადი წინასწარ განსაზღვრული მეტრიკების გამოყენებით;

ვ) **დონე 5:** მიკრობანკში დანერგილია ფორმალიზებული პროცესები და სრულყოფილი/ორგანიზებული კონტროლების გარემო, რომლის ეფექტურობა არის გაზომვადი წინასწარ განსაზღვრული მეტრიკების გამოყენებით და ხორციელდება მისი მუდმივი გაუმჯობესება.

2. აუდიტირებული მიკრობანკის შესაბამისობა აუდიტის გავრცელების სფეროში განსაზღვრული სტანდარტების/საზედამხედველო მოთხოვნების თითოეულ კრიტერიუმთან უნდა შეფასდეს შემდეგნაირად:

ა) **არ შეესაბამება:** როდესაც კონკრეტული მოთხოვნის ფარგლებში განხილული პროცესები აკმაყოფილებს „დონე 0“-ს ან „დონე 1“-ს ამ მუხლის პირველ პუნქტში განსაზღვრული პროცესის სიმწიფის შკალის შესაბამისად;

ბ) **ნაწილობრივ შეესაბამება:** როდესაც კონკრეტული მოთხოვნის ფარგლებში განხილული პროცესები აკმაყოფილებს „დონე 2“-ს ან „დონე 3“-ს ამ მუხლის პირველ პუნქტში განსაზღვრული პროცესის სიმწიფის შკალის შესაბამისად;

გ) **შეესაბამება:** როდესაც კონკრეტული მოთხოვნის ფარგლებში განხილული პროცესები აკმაყოფილებს „დონე 4“-ს ან „დონე 5“-ს ამ მუხლის პირველ პუნქტში განსაზღვრული პროცესის სიმწიფის შკალის შესაბამისად.

3. აუდიტის პროცესში იდენტიფიცირებული თითოეული ხარვეზი/შეუსაბამობა უნდა შეფასდეს მიკრობანკის კონტექსტისა და მისი რისკებიდან გამომდინარე; შეფასების სისტემა შესაძლოა იყოს რაოდენობრივი (მაგ., 1-დან 5-მდე) ან ხარისხობრივი (მაგ., „მცირე შეუსაბამობა“, „არსებითი შეუსაბამობა“) აუდიტის მეთოდოლოგიის შესაბამისად და წინასწარ უნდა იქნეს შეთანხმებული მიკრობანკთან, რათა სწორად იქნეს აღქმული თითოეული ხარვეზის/შეუსაბამობის კრიტიკულობა.

მუხლი 10. ეროვნული ბანკის უფლებამოსილებები

ეროვნული ბანკი უფლებამოსილია:

ა) ამ სახელმძღვანელოს მე-4 მუხლის მე-3 პუნქტის „ა“ ქვეპუნქტის შესაბამისად, მიკრობანკის მიერ აუდიტორული ფირმის შერჩევასთან დაკავშირებით შეტყობინებიდან 5 სამუშაო დღის ვადაში, მოითხოვოს დამატებითი ინფორმაცია აუდიტის გუნდის ამ სახელმძღვანელოთი განსაზღვრულ მოთხოვნებთან შესაბამისობის შემოწმების მიზნით ან/და მოსთხოვოს მიკრობანკს აუდიტორული ფირმის ცვლილება, თუ საეჭვოა აუდიტორული ფირმის/აუდიტის გუნდის დამოუკიდებლობა ან/და კომპეტენტურობა;

ბ) აუდიტის გუნდის/შიდა აუდიტის ერთეულის მიერ აუდიტის ანგარიშის გამოცემიდან ნებისმიერ დროს წერილობითი სახით მოითხოვოს დამატებითი ინფორმაცია აუდიტის ანგარიშთან მიმართებით მიკრობანკისგან ან/და აუდიტის გუნდისგან მიკრობანკის შუამდგომლობით;

გ) მიკრობანკისაგან მოითხოვოს ინფორმაცია აუდიტის გუნდის მიერ მიკრობანკისთვის გაწეული ყველა მომსახურების შესახებ, აუდიტის გუნდის დამოუკიდებლობისა და მიუკერძოებლობის შეფასების მიზნით;

დ) მიკრობანკს მოსთხოვოს სხვა აუდიტის გუნდის შერჩევა, თუ დაადგენს, რომ აუდიტი არ არის განხორციელებული სტანდარტების შესაბამისად ან აუდიტის გუნდი/შიდა აუდიტის ერთეული არღვევს ამ სახელმძღვანელოს მოთხოვნებს, რის შესახებაც ეროვნულმა ბანკმა წერილობით უნდა აცნობოს მიკრობანკს აუდიტის ანგარიშის მიღებიდან 10 სამუშაო დღის ვადაში.