საქართველოს ეროვნული ბანკის პრეზიდენტის

ბრძანება №48/04
2022 წლის 2 მაისი

ქ. თბილისი

„კომერციული ბანკების კიბერუსაფრთხოების მართვის ჩარჩოს დამტკიცების შესახებ“ საქართველოს ეროვნული ბანკის პრეზიდენტის 2019 წლის 22 მარტის №56/04 ბრძანებაში ცვლილების შეტანის შესახებ

„ნორმატიული აქტების შესახებ“ საქართველოს ორგანული კანონის მე-20 მუხლის მე-4 პუნქტისა და „საქართველოს ეროვნული ბანკის შესახებ“ საქართველოს ორგანული კანონის მე-15 მუხლის პირველი პუნქტის „ზ“ ქვეპუნქტის საფუძველზე, **ვბრძანებ:**

მუხლი 1

„კომერციული ბანკების კიბერუსაფრთხოების მართვის ჩარჩოს დამტკიცების შესახებ“ საქართველოს ეროვნული ბანკის პრეზიდენტის 2019 წლის 22 მარტის №56/04 ბრძანებაში (www.matsne.gov.ge; 25/03/2019; ს/კ: 220010000.18.011.016379) შეტანილ იქნეს შემდეგი ცვლილება:

1. ბრძანების პრეამბულა ჩამოყალიბდეს შემდეგი რედაქციით:

„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:**“.

2. ბრძანებით დამტკიცებული წესის მე-8 მუხლის მე-5 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„5. კომერციული ბანკი ვალდებულია ყოველწლიურად ჩაატაროს კომერციული ბანკის კიბერუსაფრთხოების მართვის ჩარჩოს ყველა კომპონენტის დამოუკიდებელი აუდიტი ამ ბრძანების დანართ №1-ით დამტკიცებული „კომერციულ ბანკებში საინფორმაციო სისტემებისა და კიბერუსაფრთხოების მართვის ჩარჩოს აუდიტის სახელმძღვანელოს“ შესაბამისად.“.

3. ბრძანებას დაემატოს დანართი №1 თანდართული რედაქციით.

მუხლი 2

ეს ბრძანება ამოქმედდეს გამოქვეყნებისთანავე.

ეროვნული ბანკის პრეზიდენტი **კობა გვენეტაძე**

დანართი №1

კომერციულ ბანკებში საინფორმაციო სისტემებისა და კიბერუსაფრთხოების მართვის ჩარჩოს აუდიტის სახელმძღვანელო

მუხლი 1. ზოგადი დებულება

კომერციულ ბანკებში საინფორმაციო სისტემებისა და კიბერუსაფრთხოების მართვის ჩარჩოს აუდიტის სახელმძღვანელო (შემდგომ – სახელმძღვანელო) განსაზღვრავს კომერციულ ბანკებში 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 კომერციულ ბანკში ერთდროულად ორ ან მეტ მართვის სისტემაზე განხორციელებული აუდიტი;

დ) აუდიტის გავრცელების სფერო – აუდიტის მოცულობა და საზღვრები, რაც განსაზღვრავს კომერციული ბანკის 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 კომერციული ბანკის 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 – კომერციულ ბანკში 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 კომერციული ბანკის საინფორმაციო სისტემებისა და კიბერუსაფრთხოების მართვის ჩარჩოს საქართველოს ეროვნული ბანკის (შემდგომ – ეროვნული ბანკი) მიერ დადგენილ მინიმალურ მოთხოვნებთან შესაბამისობის შეფასება, რის საფუძველზეც დგება აუდიტის ანგარიში, რომლის მოთხოვნების შესრულება სავალდებულოა.

2. კომერციულ ბანკს 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 საქართველოს ეროვნული ბანკის პრეზიდენტის 2019 წლის 22 მარტის №56/04 ბრძანებით დამტკიცებული „კომერციული ბანკების კიბერუსაფრთხოების მართვის ჩარჩოს“ შესაბამისად.

4. საინფორმაციო სისტემების აუდიტი უნდა განხორციელდეს საქართველოს ეროვნული ბანკის პრეზიდენტის 2014 წლის 13 ივნისის №47/04 ბრძანებით დამტკიცებული „კომერციული ბანკების 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. კომერციული ბანკი ვალდებულია, უზრუნველყოს აუდიტის განხორციელება ისეთი აუდიტის გუნდის მიერ, რომელიც ოპერაციულად დამოუკიდებელია კომერციული ბანკისგან და აკმაყოფილებს ამ სახელმძღვანელოს მე-5 მუხლით განსაზღვრულ მინიმალურ მოთხოვნებს.

2. კომერციულ ბანკს უფლება აქვს, განახორციელოს აუდიტი შიდა აუდიტის ერთეულის მიერ, რაც წინასწარ უნდა იქნეს შეთანხმებული საქართველოს ეროვნულ ბანკთან.

3. კომერციული ბანკის აუდიტის გარე აუდიტორული ფირმის მიერ განხორციელების შემთხვევაში:

ა) კომერციული ბანკი 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) კომერციულმა ბანკმა აუდიტორულ ფირმასთან დადებული ხელშეკრულებით უნდა უზრუნველყოს კომერციული ბანკის ინფორმაციის კონფიდენციალურობისა და გაუთქმელობის დაცვა.

4. კომერციული ბანკი 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, კომერციულმა ბანკმა 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 კომერციული ბანკი 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 კომერციული ბანკის მიმართ არსებული რეგულაციების/მოთხოვნების სრულფასოვანი ცოდნა;

ვ) აუდირებული კომერციული ბანკის საქმიანობის ანალიზის უნარი, რათა მის აქტივობებზე, პროდუქტებსა და მომსახურებებზე დაყრდნობით შეძლოს სრულფასოვანი და ეფექტური აუდიტის განხორციელება.

მუხლი 6. აუდიტის პროგრამა

კომერციულმა ბანკმა 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 კომერციულ ბანკთან;

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 კომერციულ ბანკს უნდა წარუდგინოს წერილობითი აუდიტის ანგარიში კომერციული ბანკის შესაბამისობის შესახებ იმ კრიტერიუმებთან და მოთხოვნებთან, რომელთა მიმართაც განხორციელდა აღნიშნული აუდიტი;

გ.ბ) აუდიტის დასრულებამდე უნდა განხორციელდეს შეხვედრა აუდიტის გუნდსა და კომერციული ბანკის მენეჯმენტს შორის, რომლის ფარგლებშიც:

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

გ.ბ.ბ) კომერციული ბანკის მენეჯმენტს 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 კომერციული ბანკის შეფასება აუდიტის

გავრცელების სფეროს ფარგლებში. აუდიტის ხანგრძლივობის განსასაზღვრად გათვალისწინებული უნდა იქნას სულ მცირე შემდეგი ფაქტორები:

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

დ.ბ) კომერციული ბანკის კომპლექსურობა;

დ.გ) კომერციული ბანკის 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, კომერციულმა ბანკმა უნდა უზრუნველყოს, რომ:

ა) აუდიტის პროცესის დაწყებამდე აუდიტის გუნდმა განახორციელოს მოსამზადებელი სამუშაოები, რომლის ჭრილში სრულყოფილად მოახდენს აუდირებული კომერციული ბანკის, მისი ფუნქციების/მომსახურებებისა და რისკების პროფილის შესწავლას. მოსამზადებელ ეტაპზე აუდიტის გუნდს შეუძლია კომერციული ბანკიდან საჭიროებისამებრ გამოითხოვოს მინიმუმ შემდეგი ინფორმაცია:

ა.ა) ზოგადი ინფორმაცია კომერციული ბანკისა და მისი მომსახურებების შესახებ (მდებარეობის, ზომის, ფუნქციების, მესამე მხარეების შესახებ, რომლებიც უზრუნველყოფენ კომერციული ბანკისთვის 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, აუდირებული კომერციული ბანკისთვის 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 აუდირებული კომერციული ბანკის 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 კომერციული ბანკის შესაბამის წარმომადგენლებთან, რათა:

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

ბ.ბ) შეფასდეს, რამდენად შესაბამისობაშია ბანკში არსებული პროცესები კომერციული ბანკის მიზნებთან, შემუშავებულ პოლიტიკასა და პროცედურებთან;

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

3. აუდირებულმა კომერციულმა ბანკმა 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 კომერციული ბანკის მხრიდან ინტერვიუებში მონაწილე პირების იდენტიფიცირებასა და დროისა და ადგილის დადასტურებაში;

ბ) აუდიტორებისთვის კომერციული ბანკის დაცულ ადგილებში დაშვების უფლების მოპოვებას;

გ) აუდიტის გუნდის წევრების გაცნობას აუდირებული კომერციული ბანკის 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. კომერციული ბანკისთვის მიწოდებული აუდიტის ანგარიში უნდა შედგებოდეს შემოწმების/აუდიტის სრული, ზუსტი, ლაკონური და მკაფიო ჩანაწერებისგან და უნდა მოიცავდეს, სულ მცირე, შემდეგ ინფორმაციას:

ა) კომერციული ბანკის 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 კომერციული ბანკის პროცესების, დოკუმენტების სია, რომლის შეფასება მოხდა აუდიტის პროცესში, ასევე, იმ სტანდარტებისა თუ საზედამხედველო მოთხოვნების ჩამონათვალი, რომელთა მიმართაც განხორციელდა კომერციული ბანკის პროცესების შესაბამისობის შეფასება;

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

ზ) კომერციული ბანკის 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) კომერციული ბანკის 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 კომერციული ბანკი შესაბამისობაში მოვა კონკრეტულ მოთხოვნასთან/კრიტერიუმთან.

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

მუხლი 9. შეფასების სისტემა

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

ა) **დონე 0:** კომერციული ბანკში არ არის დანერგილი აუდიტის კრიტერიუმის შესაბამისი პროცესები და კონტროლების გარემო.

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

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

დ) **დონე 3:** კომერციული ბანკში დანერგილია ფორმალიზებული პროცესები და სრულყოფილი/ორგანიზებული კონტროლების გარემო. შეინიშნება მცირე რაოდენობით

კონტროლების ოპერაციული ეფექტურობის ხარვეზები.

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

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

2. აუდირებული კომერციული ბანკის 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 კომერციული ბანკის 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 იქნას შეთანხმებული კომერციულ ბანკთან, რათა სწორად იქნას აღქმული თითოეული ხარვეზის/შეუსაბამობის კრიტიკულობა.

მუხლი 10. ეროვნული ბანკის უფლებამოსილებები

1. ეროვნული ბანკი უფლებამოსილია:

ა) ამ სახელმძღვანელოს მე-4 მუხლის მე-3 პუნქტის „ა“ ქვეპუნქტის შესაბამისად, კომერციული ბანკის 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 კომერციულ ბანკს 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 კომერციული ბანკისგან ან/და აუდიტის გუნდისგან კომერციული ბანკის შუამდგომლობით;

გ) კომერციული ბანკისაგან მოითხოვოს ინფორმაცია აუდიტის გუნდის მიერ ბანკისათვის გაწეული ყველა მომსახურების შესახებ, აუდიტის გუნდის დამოუკიდებლობისა და მიუკერძოებლობის შეფასების მიზნით;

დ) ბანკს 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 კომერციულ ბანკს აუდიტის ანგარიშის მიღებიდან 10 სამუშაო დღის ვადაში.