# ტექნიკური დავალება

## ISO 27001:2013 აუდიტის მომსახურება

I. ზოგადი დებულებები

1. **დავალების მიზანი:**
საქართველოს ეროვნული ბანკის გადაწყვეტილებით საერთაშორისო სტანდარტის ISO 27001:2013 მოთხოვნები დაინერგა ბანკის ყველა პროცესსა და სტრუქტურულ ერთეულზე.

შესაბამისად, ბანკს ესაჭიროება სერტიფიცირების არეალის გაფართოება, რაც გულისხმობს ყველა პროცესისა და სტრუქტურული ერთეულის დაფარვას.

2. **სერტიფიცირების არეალი**
2.1. საქართველოს ეროვნული ბანკის სტრუქტურა
2.1.1. ბანკის ყველა (22) სტრუქტურული ერთეული. დეტალებისთვის იხილეთ ჩვენი ვებ-გვერდი www.nbg.gov.ge
2.1.2. საქართველოს ეროვნულ ბანკში ამჟამად დასაქმებულია 520 თანამშრომელი.
2.2. ბანკის ადგილმდებარეობა
2.2.1. საქართველოს ეროვნული ბანკის თანამშრომლები საქმიანობას ახორციელებენ ხუთ (5) ლოკაციაზე.
2.3. ბანკის ძირითადი ბიზნეს-პროცესები და/ან სერვისები:
2.3.1. მონეტარული პოლიტიკის წარმოება;
2.3.2. ფინანსური სტაბილურობის უზრუნველყოფა;
2.3.3. საგადახდო სისტემების ფუნქციონირება;
2.3.4. საბანკო ზედამხედველობას განხორციელება;
2.3.5. ფულის გათეთრების ინსპექტირებისა და ზედამხედველობა;
2.3.6. როგორც ადგილობრივ, ასევე საერთაშორისო ბაზარზე ფინანსური ოპერაციების წარმოება;
2.3.7. სპეციალიზებული რისკების მართვა;
2.3.8. საზედამხედველო პოლიტიკის წარმოებდა და რეალიზება;
2.3.9. ფინანსური და საზედამხედველო ტექნოლოგიების ფუნქციონირება;
2.3.10. არასაბანკო დაწესებულების ზედამხედველობა;
2.3.11. ფასიანი ქაღალდების ბაზრის ზედამხედველობა;
2.3.12. საკასო ოპერაციებისა და ნაღდი ფულის მიმოქცევის უზრუნველყოფა;
2.3.13. რისკების ცენტრალიზებული მართვა;
2.3.14. მაკროეკონომიკა და სტატისტიკის წარმოება;
2.3.15. მომხმარებელთა უფლებების დაცვა და ფინანსური განათლების ხელმისაწვდომობა;

2.4. ძირითადი ბიზნეს-პროცესების დამხმარე პროცესები და/ან სერვისები:
2.4. 1.იურიდიული კონსულტაცია და სამართლებრივი მხარდაჭერა;
2.4.2.საინფორმაციო ტექნოლოგიების ფუნქციონირება და კიბერუსაფრთხოების უზრუნველყოფა;
2.4.3. ფინანსებისა და ბუღალტრული აღრიცხვა;
2.4.4.შესყიდვებისა და ლოჯისტიკის უზრუნველყოფა;
2.4.5.შიდა აუდიტის უზრუნველყოფა;
2.4.6.უსაფრთხოების უზრუნველყოფა;
2.4.7.პროექტების მართვა;
2.4.8.ადამიანური რესურსების მართვა და განვითარება;
2.4.9.საზოგადოებასთან ურთიერთობა და საერთაშორისო თანამშრომლობა;
2.4.10. საქმისწარმოების უზრუნველყოფა.

ბანკის ინფორმაციული ნაკადების მართვა მისი ყველა სტრუქტურული ერთეულისათვის ხორციელდება ცენტრალიზებულად.

3. **სასერტიფიკაციო აუდიტისთვის შესასრულებელი სამუშაოების ჩამონათვალი:**
3.1. სასერტიფიკაციო აუდიტის ჩატარება:
ა) დაიწყოს ხელშეკრულების ხელმოწერისთანავე;
ბ) დასრულდეს ხელშეკრულების ხელმოწერიდან 98 დღის ვადაში.
3.2. პირველი საკონტროლო აუდიტი:
ა) დაიწყოს არაუადრეს მე-9 თვისა სასერტიფიკაციო აუდიტის დასრულებიდან;
ბ) დასრულდეს არაუგვიანეს 12 (თორმეტი) თვისა სასერტიფიკაციო აუდიტის დასრულებიდან; 3.3. მეორე საკონტროლო აუდიტი:
ა) დაიწყოს არაუადრეს მე-9 თვისა პირველი საკონტროლო აუდიტის დასრულებიდან;
ბ) დასრულდეს არაუგვიანეს 12 (თორმეტი) თვისა პირველი საკონტროლო აუდიტის დასრულებიდან.

## II. სერტიფიცირების და საზედამხედველო აუდიტის პროცესის ამოცანები და მათი გადაწყვეტის დამადასტურებელი დოკუმენტები

1. ზოგადი ამოცანები - სერტიფიცირების და საზედამხედველო აუდიტის პროცესისთვის მომზადება
1.1. ამოცანა 1 - აუდიტის 3 წლიანი პროექტის წესდების და გეგმის შეთანხმება სებ-ის გუნდთან;

მისაწოდებელი შედეგი:
a. აუდიტის პროექტის წესდება;

b. აუდიტის პროექტის გეგმა.

2. სერთიფიცირების აუდიტი (2021 წელი)

2.1. ამოცანა 1:

2.1.1. ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტაციის შესწავლა;

2.1.2. მე-2 ეტაპის აუდიტისთვის მზაობის განსაზღვრა.

მისაწოდებელი
შედეგები:
a. აუდიტის გეგმა;
b. პირველი ეტაპის აუდიტის ანგარიში.

2.2. ამოცანა 2:
2.2.1.ინფორმაციული უსაფრთხოების მართვის სისტემის ფუნქციონირების ეფექტიანობის შეფასება;
2.2.2.სებ-ის SOA-ში იდენტიფიცირებული მოქმედი კონტროლების შემოწმება მათი საოპერაციო ეფექტურობის დადასტურების მიზნით;
2.2.3.შიდა აუდიტისა და მენეჯერული განხილვების პროცესების შემოწმება.

მისაწოდებელი
შედეგები:
a. აუდიტის გეგმა;
b. მეორე ეტაპის აუდიტის ანგარიში.

2.3. ამოცანა 3:
2.3.1. შეუსაბამობების აღმოფხვრა, მათი არსებობის შემთხვევაში;
2.3.2. გადაწყვეტილება სერტიფიცირების თაობაზე;
2.3.3. სერტიფიკატის მინიჭება და გადაცემა, დადებითი გადაწყვეტილების შემთხვევაში.

<u>მისაწოდებელი შედეგები</u>:
a. ISO 27001:2013-თან შესაბამისობის დამადასტურებელი სერტიფიკატის ელექტრონული და ფიზიკური ასლების მიწოდება სერტიფიცირების აუდიტის წარმატებით გავლის შემთხვევაში (პირველი ფაზის დამთავრებიდან და საბოლოო გაერთიანებული ანგარიშის წარდგენიდან არაუგვიანეს 2 კვირისა გადასცეს შემსყიდველს სასერთიფიკაციო ორგანოს მიერ გაცემული, შესაბამისი ISO/IEC 27001:2013 სერტიფიკატი ელექტრონული ფორმით, ხოლო ერთ თვეში - მატერიალური სახით);
b. სერტიფიცირების აუდიტის ფარგლებში პირველი და მეორე ამოცანების განხორციელების ამსახველი გაერთიანებული ანგარიში

3. საზედამხედველო აუდიტების ჩატარება (2022 – 2023 წლები)

3.1. ამოცანა 1 - პირველი საზედამხედველო აუდიტის ჩატარება (2022 წელი);

3.1.1. სტანდარტთან შესაბამისობის მიმდინარე მდგომარეობის დადგენა.

მისაწოდებელი
შედეგები:

a. აუდიტის გეგმა;
b. საზედამხედველო აუდიტების ანგარიშები.

3.2. ამოცანა 2 - მეორე საზედამხედველო აუდიტის ჩატარება (2023 წელი);

3.2.1. სტანდარტთან შესაბამისობის მიმდინარე მდგომარეობის დადგენა.

მისაწოდებელი
შედეგები:
c. აუდიტის გეგმა;
d. საზედამხედველო აუდიტების ანგარიშები.

4. აუდიტის პროექტის 3 წლიანი გრაფიკი

4.1. აღნიშნული პროცესის შესრულების გრაფიკი წარმოდგენილი უნდა იყოს გამჭვირვალედ, თითოეული ამოცანის შესასრულებლად საჭირო ვადების მითითებით.

4.2. უნდა ჩანდეს წარმოდგენილი აუდიტორების ჩართულობის მოცულობა. კერძოდ, აუდიტის პროექტის მსვლელობისას:

**4.2.1. სახელობითად მთავარი აუდიტორის ჩართულობის მოცულობა:**

a. ამოცანების ჩამონათვალი;
b. დისტანციურად თუ ადგილზე;
c. მისაწოდებელი შედეგები.

**4.2.2. სახელობითად დამხმარე აუდიტორის ჩართულობის მოცულობა:**

a. ამოცანების ჩამონათვალი;
b. დისტანციურად თუ ადგილზე;
c. მისაწოდებელი შედეგები.

## III. საკვალიფიკაციო მოთხოვნები

## 1. მოთხოვნები პრეტენდენტი კომპანიის მიმართ

1. პრეტენდენტი ორგანიზაცია შესაძლებელია თავად იყოს მასერტიფიცირებელი ორგანო. ამ შემთხვევაში ის უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:
1.1. აკრედიტირებული უნდა იყოს აკრედიტაციის გამცემი იმ ორგანოს მიერ, რომელიც არის საერთაშორისო სააკრედიტაციო ფორუმის (IAF) ან ევროპის სააკრედიტაციო თანამშრომლობის (EA) წევრი;
1.2. შესაბამისი აკრედიტაციის გამცემი ორგანოს მიერ მინიჭებული ჰქონდეს აკრედიტაცია ISO 27001:2013-ის "ინფორმაციული უსაფრთხოების მართვის სისტემები" სერტიფიცირებაზე.
1.3. მსოფლიოს მასშტაბით წარმატებით უნდა ჰქონდეს განხორციელებული მინიმუმ სამი (3) ISO 27001:2013-ის "ინფორმაციული უსაფრთხოების მართვის სისტემები" სასერტიფიკაციო და საკონტროლო აუდიტები ბოლო ხუთი 2016-2021 წლის მანძილზე ორგანიზაციებში, რომლებიც განეკუთვნებიან საბანკო და/ან საფინანსო სექტორს.

აღნიშნული მოთხოვნების დასაკმაყოფილებლად პრეტენდენტმა უნდა წარმოადგინოს შემდეგი დოკუმენტები/ინფორმაცია:
ა) პუნქტში 1.1. დასახელებული ორგანიზაციების ოფიციალური ვებ-გვერდების მისამართები, სადაც შესაძლებელი იქნება აკრედიტაციის გამცემი ორგანიზაციების წევრობის მიმდინარე სტატუსის გადამოწმება;
ბ) პუნქტში 1.2. დასახელებული აკრედიტაციის დამადასტურებელი დოკუმენტები;
გ) პუნქტში 1.3. მოთხოვნილი გამოცდილების ამსახველი ინფორმაცია დანართ N3-ში მოცემული ფორმის შესაბამისად.

2. პრეტენდენტი ორგანიზაცია შესაძლებელია არ იყოს მასერტიფიცირებელი ორგანიზაცია. ამ შემთხვევაში:
2.1. იგი უნდა იყოს იმ მასერტიფიცირებელი ორგანიზაციის პარტნიორი ან ფილიალი, რომელიც გაუწევს სერტიფიკაციას შემსყიდველს და აკმაყოფილებს პირველი პუნქტის მოთხოვნებს.
2.2. მას უნდა გააჩნდეს მასერტიფიცირებელ ორგანიზაციასთან ერთად ანალოგიური მომსახურების გაწევის გამოცდილება.

აღნიშნული მოთხოვნების დასაკმაყოფილებლად პრეტენდენტმა უნდა წარმოადგინოს შემდეგი დოკუმენტები/ინფორმაცია:
ა) ოფიციალური დოკუმენტი, რომელიც ადასტურებს, რომ პრეტენდენტი არის მასერტიფიცირებელი ორგანოს პარტნიორი ან ფილიალი;
ბ) დოკუმენ(ებ)ი, რომელიც ადასტურებს, რომ პრეტენდენტის პარტნიორი მასერტიფიცირებელი ორგანო აკმაყოფილებს პირველ პუნქტში მოცემულ მოთხოვნებს, კერძოდ:
ბ.ა) პუნქტში 1.1. დასახელებული ორგანიზაციების ოფიციალური ვებ-გვერდების მისამართები, სადაც შესაძლებელი იქნება აკრედიტაციის გამცემი ორგანიზაციების

წევრობის მიმდინარე სტატუსის გადამოწმება;
ბ.ბ) პუნქტში 1.2 დასახელებული აკრედიტაციის დამადასტურებელი დოკუმენტები;
ბ.გ) პუნქტში 1.3. მოთხოვნილი გამოცდილების ამსახველი ინფორმაცია დანართი N3-ში მოცემული ფორმის შესაბამისად.
გ) პუნქტში 2.2 მოთხოვნილი გამოცდილების ამსახველი ინფორმაცია დანართი N4-ში მოცემული ფორმის შესაბამისად.

## 2. მოთხოვნები აუდიტორთა გუნდის მიმართ

1. პრეტენდენტმა უნდა წარმოადგინოს შესაბამისი კომპეტენციის მქონე აუდიტორების გუნდი.
1.1. გუნდი დაკომპლექტებული უნდა იყოს მინიმუმ 2 აუდიტორით და თითოეულს უნდა გააჩნდეს ISO 27001: 2013 "ინფორმაციული უსაფრთხოების მართვის სისტემები" წამყვანი აუდიტორის მოქმედი სერტიფიკატი.
1.2. აუდიტორებს უნდა გააჩნდეთ მასერტიფიცირებელი ორგანოს, რომლის პარტნიორიც არის პრეტენდენტი, ავტორიზაცია ISO 27001:2013 სტანდარტზე სერტიფიცირების და საკონტროლო აუდიტების ჩატარებაზე;
1.3. აუდიტორები წარმოდგენილი უნდა იყვნენ შემდეგი როლებით:
1.3.1. მთავარი აუდიტორი, რომელსაც უნდა გააჩნდეს ISO 27001:2013 სტანდარტზე სერტიფიცირების და/ან საკონტროლო აუდიტის ჩატარების გამოცდილება მინიმუმ 2016-2021 წლების განმავლობაში საბანკო და/ან საფინანსო სექტორში;
1.3.2. დამხმარე აუდიტორი, რომელსაც სასურველია გააჩნდეს სერტიფიცირებისა და/ან საკონტროლო აუდიტების ჩატარების გამოცდილება.

აღნიშნული მოთხოვნების დასაკმაყოფილებლად პრეტენდენტმა უნდა წარმოადგინოს შემდეგი დოკუმენტები/ინფორმაცია:

ა) შემოთავაზებულ აუდიტორთა გუნდის შემადგენლობა, რომელშიც სახელობითად არის მითითებული მთავარი და დამხმარე აუდიტორების პასუხისმგებლობები სათანადო ამოცანების მითითებით.
ბ) გუნდის თითოეული წევრის რეზიუმე (CV), სადაც დადასტურებული იქნება 1.3. პუნქტში მითითებული მოთხოვნების დაკმაყოფილება.
გ) გუნდის წევრების 1.1 პუნქტში მითითებული სერტიფიკატების ასლები.
დ) მასერთიფიცირებელი ორგანოს ოფიციალური წერილ(ებ)ის ასლ(ებ)ი, სადაც მითითებული იქნება, რომ ჯგუფის წევრები (სახელობითად) უფლებამოსილნი არიან ISO 27001:2013 სტანდარტზე აუდიტის განხორციელებისათვის.

ფასების ცხრილი

| ISO 27001:2013<br>სასერტიფიკაციო აუდიტი | ღირებულება<br>(ლარი) |
|---|---|
| სასერტიფიკაციო აუდიტის ჩატარება - ფაზა N1 | |
| პირველი საკონტროლო აუდიტი - ფაზა N2 | |
| მეორე საკონტროლო აუდიტი - ფაზა N3 | |
| | ჯამი: |

შენიშვნები:

1.ზემოაღნიშნული ფასები მოიცავს მომსახურების გაწევისათვის აუცილებელ ყველა ხარჯს და საქართველოს კანონმდებლობით გათვალისწინებულ ყველა გადასახადს.
2.ფასები მითითებულ უნდა იქნას ფასების ცხრილის ყველა პოზიციისათვის, წინააღმდეგ შემთხვევაში მოხდება პრეტენდენტის დისკვალიფიკაცია დაზუსტების მოთხოვნის გარეშე.

_____
(პრეტენდენტის დასახელება)

_____
(უფლებამოსილი პირის სახელი და გვარი)

_____
(უფლებამოსილი პირის თანამდებობა)

_____
(უფლებამოსილი პირის ხელმოწერა)