ტექნიკური დავალება

ISO 27001:2013 სასერტიფიკაციო აუდიტის მომსახურება

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. <u>საქართველოს ეროვნული ბანკის სტრუქტურა</u>

2.1.1. ბანკის ყველა (22) სტრუქტურული ერთეული. დეტალებისთვის იხილეთ ჩვენი ვებ-გვერდი www.nbg.gov.ge

2.1.2. საქართველოს ეროვნულ ბანკში ამაჟამად დასაქმებულია 520 თანამშრომელი.

2.2. <u>ბანკის ადგილმდებარეობა</u>

2.2.1. საქართველოს ეროვნული ბანკის თანამშრომლები საქმიანობას ახორციელებენ ხუთ (5) ლოკაციაზე.

2.3. <u>ბანკის ძირითადი ბიზნეს-პროცესები და/ან სერვისები:</u>

2.3.1. მონეტარული პოლიტიკის წარმოება;
2.3.2. ფინანსური სტაბილურობის უზრუნველყოფა;
2.3.3. საგადახდო სისტემების ფუნქციონირება;
2.3.4. საბანკო ზედამხედველობას განხორციელება;ფულის გათეთრების ინსპექტირებისა და ზედამხედველობა;
2.3.5. როგორც ადგილობრივ, ასევე საერთაშორისო ბაზარზე ფინასური ოპერაციების წარმოება;
2.3.6. სპეციალიზებული რისკების მართვა;
2.3.7. საზედამხედველო პოლიტიკის წარმოებდა და რეალიზება;
2.3.8. ფინანსური და საზედამხედველო ტექნოლოგიების ფუნქციონირება;
2.3.9. არასაბანკო დაწესებულების ზედამხედველობა;
2.3.10. ფასიანი ქაღალდების ბაზრის ზედამხედველობა;
2.3.11. საკასო ოპერაციებისა და ნაღდი ფულის მიმოქცევის უზრუნველყოფა;
2.3.12. რისკების ცენტრალიზებული მართვა;
2.3.13. მაკროეკონომიკა და სტატისტიკის წარმოება;
2.3.14. მომხმარებელთა უფლებების დაცვა და ფინანსური განათლების ხელმისაწვდომობა;

2.4. <u>ძირითადი ბიზნეს-პროცესების დამხმარე პროცესები და/ან სერვისები:</u>

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.

2.5. *ბანკის ინფორმაციული ნაკადების მართვა მისი ყველა სტრუქტურული ერთეულისათვის ხორციელდება ცენტრალიზებულად.*

3. სასერტიფიკაციო აუდიტისთვის შესასრულებელი სამუშაოების ჩამონათვალი:

3.1. <u>სასერტიფიკაციო აუდიტის ჩატარება</u>:

ა) პირველი ეტაპის აუდიტი ხელშეკრულების ხელმოწერისთანავე;

3.2. <u>პირველი საკონტროლო აუდიტი</u>:

ა) დაიწყოს არაუადრეს მე-9 თვისა სასერტიფიკაციო აუდიტის დასრულებიდან;

ბ) დასრულდეს არაუგვიანეს 12 (თორმეტი) თვისა სასერტიფიკაციო აუდიტის დასრულებიდან;

3.3. <u>მეორე საკონტროლო აუდიტი:</u>

ა) დაიწყოს არაუადრეს მე-9 თვისა პირველი საკონტროლო აუდიტის დასრულებიდან;

ბ) დასრულდეს არაუგვიანეს 12 (თორმეტი) თვისა პირველი საკონტროლი აუდირის დასრულებიდან.

მოთხოვნები მომსახურების გამწევი პრეტენდენტი ორგანიზაციისადმი:

1. <u>პრეტენდენტი ორგანიზაცია შესაძლებელია თავად იყოს მასერტიფიცირებელი ორგანო.</u> ამ შემთხვევაში იგი უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

1.1. აკრედიტებული უნდა იყოს:

- ან საერთაშორისო სააკრედიტაციო ფორუმის (IAF) და ევროპის სააკრედიტაციო თანამშრომლობის (EA) მიერ
- ან UKAS-ის "ინფორმაციის უსაფრხოების მართვის სისტემების" აუდიტსა და სერტიფიკაციაში ISO/IEC 27001-ის მიხედვით
- ან DAkks-ის მიერ "ინფორმაციის უსაფრხოების მართვის სისტემების" აუდიტსა და სერტიფიკაციაში ISO/IEC 27001-ის მიხედვით
- ან მონაწილეობდეს სტანდარტიზაციის ბრიტანული ინსტიტუტის (BSI) საპარტნიორო პროგრამაში (ACP).

1.2. მსოფლიოს მასშტაბით წარმატებით უნდა ჰქონდეს განხორციელებული მინიმუმ ხუთი (5) სასერტიფიკაციო აუდიტი ISO 27001:2013-ზე ბოლო 4 წლის მანძილზე ორგანიზაციებში, რომლებიც:

ა) განეკუთვნებიან საბანკო და/ან საფინანსო სექტორს;

ბ) ოპერირებენ როგორც აზიის, ასევე ევროპის ქვეყნებში;

2. პრეტენდენტი ორგანიზაცია შესაძლებელია არ იყოს მასერტიფიცირებელი ორგანიზაცი, მაგრამ უნდა იყოს რომელიმე მასერტიფიცირებელი ორგანიზაციის პარტნიორი ან ფილიალი. ამ შემთხვევაში:

2.1. მას უნდა გააჩნდეს მასერტიფიცირებელ ორგანიზაციასთან ერთად ანალოგიური მომსახურების გაწევის არანაკლებ 3 წლიანი გამოცდილება. მასერტიფიცირებელი ორგანიზაცია უნდა აკმაყოფილებდეს პუნქტებში 1.1. და 1.2. დასახელებულ მოთხოვნებს.

მოთხოვნები აუდიტორებისადმი:

1. **პრეტენდენტის მიერ წარმოდგენილი აუდიტორები უნდა აკმაყოფილებდნენ შემდეგ მოთხოვნებს:**

1.1. პრეტენდენტმა უნდა წარმოადგინოს მინიმუმ სამი (3), შესაბამისად სერთიფიცირებული წამყვანი ISO 27001: 2013 აუდიტორი, მოქმედი სერტიფიკატებით, რომელთაგანაც ორ (2) აუდიტორს ასევე დამატებით უნდა გააჩნდეს:

ა) ISO 27001:2013 წამყვანი დამნერგავის დამადასტურებელი მოქმედი სერტიფიკატი;

ბ) ISACA-ს მიერ მინიჭებული მოქმედი CISM სერტიფიკატი;

გ) ISACA-ს მიერ მინიჭებული მოქმედი CISA სერტიფიკატი.

2. თითოეულ აუდიტორს უნდა გააჩნდეს მასერტიფიცირებელი ორგანოს ავტორიზაცია აუდიტის ჩატარებაზე;
3. თითოეულ აუდიტორს უნდა გააჩნდეს ISO 27001:2013 სტანდარტზე სერტიფიცირების აუდიტის ჩატარების გამოცდილება მინიმუმ 2018-2020 წლების მანძილზე საჯარო ან საბანკო სექტორში, რაც დადასტურებული უნდა იყოს სერტიფიცირებული ორგანიზაციების მიერ გაცემული დადებითი რეკომენდაციით;

სასერტიფიკაციო აუდიტის 3 წლიანი გეგმა და ღირებულება

მომსახურების გამწევმა პრეტენდენტმა ორგანიზაციამ უნდა წარმოადგინოს სასერტიფიკატიო აუდიტის ჩატარების გრაფიკის, რესურსებისა და ღირებულების შესახებ ინფორმაცია ქვემოთ ცხრილში:

ISO 27001:2013 სასერტიფიკაციო აუდიტი	კაც-საათი	კაც-საათის ღირებულება ლარებში (დღგ-ს გარეშე)	ადგილზე და/ან დისტანციურად	ღირებულება ლარებში (დღგ-ს გარეშე)
პირველი ეტაპის ხანგრძლივობა				
პირველი საკონტროლო აუდიტი				
მეორე საკონტროლო აუდიტი				