

# ISO 27001 თქვენი ბიზნესისთვის



# ISO 27001 - ინფორმაციული უსაფრთხოების სტანდარტი

## რა არის ISO 27001?

ISO 27001 არის საერთაშორისოდ აღიარებული სტანდარტი ინფორმაციის უსაფრთხოების მართვის სისტემებისთვის (ISMS). ის საშუალებას აძლევს ორგანიზაციებს - დაამყარონ, დანერგონ, შეინარჩუნონ და მუდმივად გააუმჯობესონ თავიანთი ინფორმაციული უსაფრთხოების პროცესები.



## რატომ არის ISO 27001 მნიშვნელოვანი?

თანამედროვე ორგანიზაციებისთვის ყველაზე ღირებული აქტივი ინფორმაციაა.

ISO 27001 ის უზრუნველყოფს ორგანიზაციების სისტემურ მიდგომას ინფორმაციის უსაფრთხოების მართვისადმი. სტანდარტი მოიცავს უსაფრთხოების კონტროლის ფართო სპექტრს, მათ შორის ფიზიკურ უსაფრთხოებას, წვდომის კონტროლს, მონაცემთა უსაფრთხოებას და ინციდენტზე რეაგირებას.

ISO 27001-ის დანერგვით, ბიზნესებს შეუძლიათ აჩვენონ პასუხისმგებლობა, ძლიერი ინფორმაციული უსაფრთხოების პრაქტიკის შეინარჩუნონ მძლავრი ინფორმაციული უსაფრთხოების პრაქტიკა. ის ეხმარება ორგანიზაციებს ნდობის ჩამოყალიბებაში დაინტერესებულ მხარეებთან, კლიენტებთან და პარტნიორებთან და აძლიერებს მათ რეპუტაციას ბაზარზე.

## რა სარგებელი აქვს ISO 27001-ის დანერგვას?



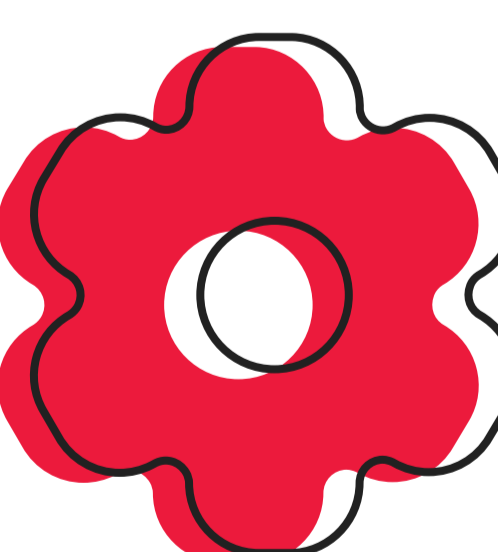
**გაძლიერებული უსაფრთხოება:** ISO 27001 ეხმარება ორგანიზაციებს დანერგონ სისტემატური მიდგომა ინფორმაციის უსაფრთხოებასთან დაკავშირებით, რაც ამცირებს მონაცემთა გაჟონვის და მათზე არაავტორიზებული წვდომის რისკს.



**რეგულაციებთან შესაბამისობა:** ISO 27001 უზრუნველყოფს ორგანიზაციებს დააკმაყოფილონ საკანონმდებლო / მარეგულირებელი ან საკონტრაქტო მოთხოვნები, რომლებიც დაკავშირებულია ინფორმაციის უსაფრთხოებასთან, ჯარიმებისა და სამართლებრივი შედეგების თავიდან აცილების მიზნით.



**მომხმარებელთა/კლიენტების ნდობა:** ISO 27001 სერთიფიკატი აჩვენებს კლიენტების ინფორმაციის დაცვისადმი მაღალ პასუხისმგებლობას, აძლიერებს მათ ნდობას თქვენი ორგანიზაციის მიმართ.



**კონკურენტული უპირატესობა:** ISO 27001 სერთიფიკატი განასხვავებს თქვენს ბიზნესს კონკურენტებისგან და არწმუნებს მომხმარებელს, რომ პრიორიტეტს ანიჭებთ მათ ინფორმაციულ უსაფრთხოებას.



**გაუმჯობესებული შიდა პროცესები:** ISO 27001-ის დანერგვა ხელს უწყობს უსაფრთხოების ცნობიერების კულტურას და ორგანიზაციის შიგნით ინფორმაციის უსაფრთხოების პრაქტიკის მუდმივ გაუმჯობესებას.

# ISO 27001-ის დანერგვასთან დაკავშირებული გამოწვევები

სტანდარტის დანერგვა შესაბამისი თანმიმდევრული ნაბიჯებით უნდა განხორციელდეს. ISO 27001-ის დანერგვასთან დაკავშირებული გამოწვევები განსხვავდება ორგანიზაციის ზომისა და სირთულის მიხედვით. თუმცა, ქვემოთ ჩამოთვლილი ყველასთვის საერთო:

## რესურსების განაწილება:

ორგანიზაციამ უნდა გამოყოფოს/მოიძიოს შესაბამისი რესურსები, მათ შორის დრო, ბიუჯეტი და გამოცდილი პერსონალი სტანდარტის ეფექტურად დანერგვისა და შენარჩუნებისთვის.

## ორგანიზაციული ვალდებულება:

ISO 27001 სერტიფიკატის მიღება მოითხოვს მაღალი რგოლის მენეჯმენტის მაღალ პასუხისმგებლობას პროაქტიულ მიდგომას მთელი ორგანიზაციის მასშტაბით.

## კომპლექსური დოკუმენტაცია:

ISO 27001-ის დოკუმენტაციის მოთხოვნები შეიძლება იყოს ვრცელი და მოითხოვს ფრთხილად დაგეგმვას, პოლიტიკის, პროცედურების და სახელმძღვანელოების შექმნას.

## პერსონალის ინფორმირებულობა და ტრენინგები:

იმის უზრუნველყოფა, რომ ყველა თანამშრომელმა გააცნობიეროს თავისი როლები და პასუხისმგებლობები ინფორმაციული უსაფრთხოების შენარჩუნებაში, გადამწყვეტია, რაც შეუძლებელია სათანადო ტრენინგებისა და ინფორმირებულობის პროგრამების გარეშე.

# ISO 27001 - ის მნიშვნელობა მესამე მხარის ურთიერთობებში

B2B კომპანიებისთვის ISO 27001 უმნიშვნელოვანესია მესამე მხარის ურთიერთობებში ნდობისა და უსაფრთხოების დამყარებისთვის. ISO 27001 სერტიფიკატის აღებით, B2B კომპანიებს შეუძლიათ დაარწმუნონ თავიანთი პარტნიორები და კლიენტები, რომ მათ განახორციელეს ინფორმაციული უსაფრთხოების ეფექტური კონტროლი. იმის დემონსტრირებით, რომ ორგანიზაციას აქვს ეფექტური ISMS, B2B კომპანიებს შეუძლიათ აჩვენონ, რომ ისინი მზად არიან დაიცვან თავიანთი მომხმარებლებისა და პარტნიორების ინფორმაციის კონფიდენციალურობა, მთლიანობა და ხელმისაწვდომობა. ეს შეიძლება განსაკუთრებით მნიშვნელოვანი იმ კომპანიებისთვის, რომლებიც მუშაობენ სენსიტიურ მონაცემებთან, როგორცაა ფინანსური ან ჯანდაცვის ინფორმაცია. ISO 27001 სერტიფიკატს, როგორც ძლიერ დიფერენციატორს, შეუძლია მიანიჭოს B2B კომპანიებს კონკურენტული უპირატესობა კონტრაქტებზე, პარტნიორობაზე და ტენდერში მონაწილეობის მიღებისას.

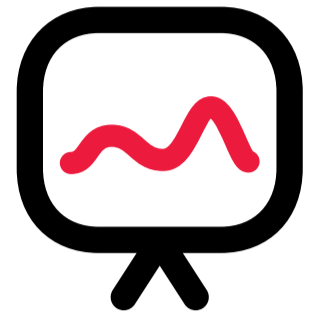


# ISO 27001 - ის დანერგვის პროცესი



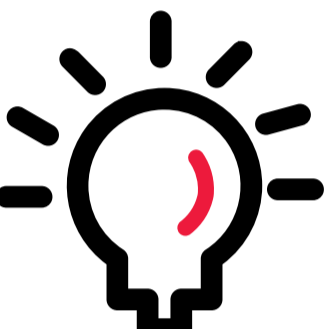
## ჩამოაყალიბეთ ISMS

განსაზღვრეთ თქვენი ინფორმაციული უსაფრთხოების მართვის სისტემის ფარგლები, მიზნები და პოლიტიკა.



## ჩაატარეთ რისკების შეფასება

განსაზღვრეთ და შეაფასეთ რისკები თქვენი საინფორმაციო აქტივებისთვის, როგორც შიდა, ასევე გარე საფრთხეების გათვალისწინებით.



## კონტროლის დანერგვა

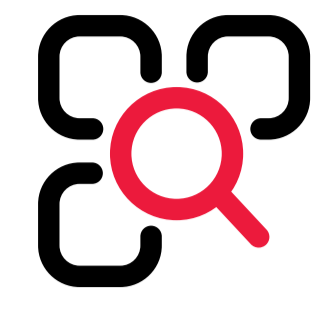
შეარჩიეთ და განახორციელეთ უსაფრთხოების შესაბამისი კონტროლი გამოვლენილი რისკების შესამცირებლად.

=

## შეიმუშავეთ დოკუმენტაცია



შექმენით საჭირო დოკუმენტაცია, როგორცაა პოლიტიკა, პროცედურები და სახელმძღვანელო მითითებები ISMS-ის მხარდასაჭერად.



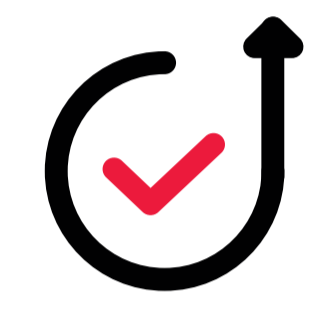
## ტრენინგი და ინფორმირებულობა

იზრუნეთ ტრენინგებსა და ცნობიერების ამაღლების პროგრამებზე, რათა ყველა თანამშრომელმა გაიაზროს თავისი როლი ინფორმაციული უსაფრთხოების მართვის სისტემაში.



## მონიტორინგი და გაზომვა

რეგულარულად აკონტროლეთ და გაზომეთ თქვენი ინფორმაციული უსაფრთხოების კონტროლის ეფექტურობა, განსაზღვრეთ გაუმჯობესების სფეროები.



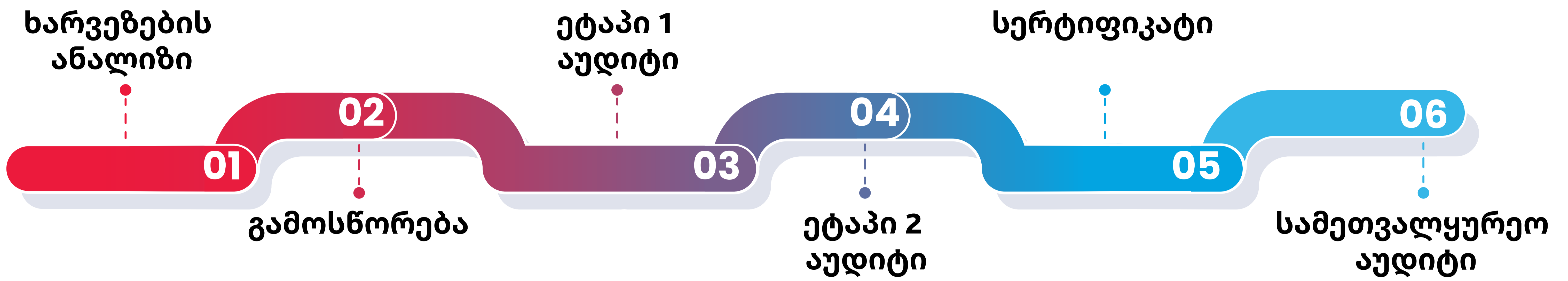
## მუდმივი გაუმჯობესება

მუდმივად შეაფასეთ და გააუმჯობესეთ თქვენი ISMS აუდიტის, მიმოხილვისა და მაკორექტირებელი ქმედებების მეშვეობით.



# სერტიფიცირების პროცესი

ISO 27001-ის სერტიფიცირების პროცესი მოიცავს შემდეგ ნაბიჯებს:



**01** ჩაატარეთ შიდა აუდიტი თქვენს არსებულ პრაქტიკასა და ISO 27001 მოთხოვნებს შორის არსებული ხარვეზების გამოსავლენად.

**02** ჩაატარეთ შიდა აუდიტი თქვენს არსებულ პრაქტიკასა და ISO 27001 მოთხოვნებს შორის არსებული ხარვეზების გამოსავლენად.

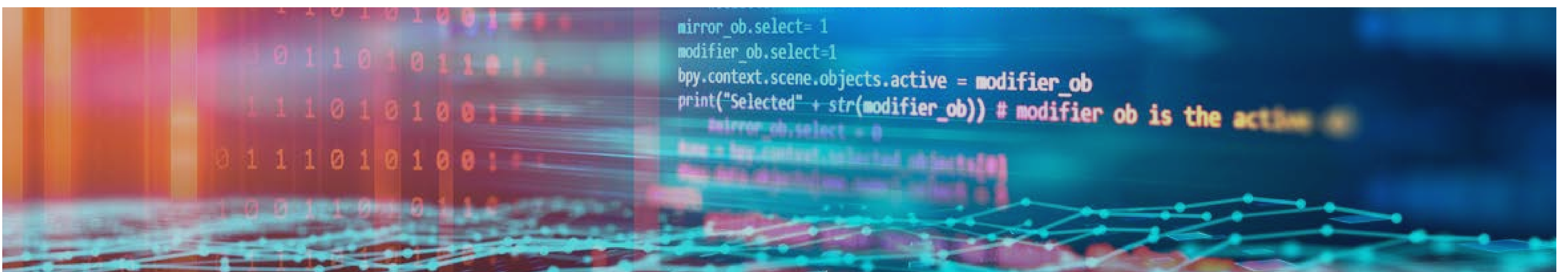
**03** სერტიფიცირების ორგანო ახორციელებს პირველად აუდიტს, რათა შეაფასოს თქვენი მზადყოფნა სერტიფიცირებისთვის.

**04** სერტიფიცირების ორგანო ატარებს სიღრმისეულ აუდიტს თქვენი ISMS-ის ეფექტურობისა და შესაბამისობის შესაფასებლად.

**05** ორი ეტაპის აუდიტის წარმატებით დასრულების შემდეგ, სერტიფიკაციის ორგანო გასცემს ISO 27001 სერტიფიკატს, რომელიც მოქმედებს გარკვეული ხანგრძლივობით.

**06** ყოველწლიურად სამეთვალყურეო აუდიტს ატარებს სერტიფიცირების ორგანო, რათა უზრუნველყოს მუდმივი შესაბამისობა და გაუმჯობესება.

ISO 27001 არის მნიშვნელოვანი სტანდარტი ყველა ზომის და სირთულის ორგანიზაციისთვის, რომელსაც სურს დაიცვას თავისი ინფორმაციული აქტივები. სტანდარტი უზრუნველყოფს ინფორმაციული უსაფრთხოების მართვისადმი სისტემატურ მიდგომას და ეხმარება ორგანიზაციებს გააუმჯობესონ უსაფრთხოების კოზიცი, შეამცირონ მონაცემთა დარღვევის რისკი და გააძლიერონ ბრენდის რეპუტაცია.



## როგორ დაგეხმარებათ BDO Digital

BDO Digital-ის კიბერ და ინფორმაციული უსაფრთხოების გუნდის გამორჩეული მომსახურების ერთ-ერთი მნიშვნელოვანი შემადგენელი ნაწილი სწორედ ინფორმაციის უსაფრთხოების უზრუნველყოფაა, უსაფრთხოების საერთაშორისო სტანდარტების მიხედვით. ჩვენი პარტნიორები დარწმუნებული არიან, რომ მათი კომპანიის მონაცემები დაცულია მსოფლიოს საუკეთესო პრაქტიკის შესაბამისად.

ჩვენს კომპეტენტურ გუნდს აქვს ბაზარზე 5 წლიანი გამოცდილება კიბერ და ინფორმაციული უსაფრთხოების მიმართულებით. ამ დროის განმავლობაში წარმატებით განვახორციელეთ პროექტები სხვადასხვა ინდუსტრიაში, როგორცაა საბანკო და საფინანსო სექტორი, სადაზღვევო ბიზნესი, ჯანდაცვა, წარმოება, რითეილი და სხვა.

ანზორ მეხრიშვილი - დირექტორი,  
ციფრული კონსულტაციების მიმართულება.  
ISO 27001 Senior Lead Implementer, Senior  
Lead Asuditor

ნიკა სოფრომაძე - საინფორმაციო  
ტექნოლოგიების აუდიტის მენეჯერი.  
ISO 27001 Lead Auditor

## როგორ მოვიქცე?

თუ თქვენ დაინტერესებული ხართ გაიგოთ მეტი ISO 27001-ის შესახებ, ან თუ გსურთ მიიღოთ თქვენი ორგანიზაციის სერტიფიცირება, გადადით ჩვენს ვებ-გვერდზე და გაეცანით ინფორმაციას [ISO 27001-ის](#) და [ISMS - ინფორმაციული უსაფრთხოების მართვის სისტემის](#) შესახებ.

ან დაგვიკავშირდით პირდაპირ ნომერზე: **+995 591 155 326**

