საქართველოს იუსტიციის სამინისტრო

მონაცემთა გაცვლის სააგენტო

# მგს 27005:2011

28 ნოემბერი 2011 წელი
Version 1.0

# ინფორმაციული უსაფრთხოების რისკების მართვა

საქართველოს იუსტიციის სამინისტრო
სსიპ. მონაცემთა გაცვლის სააგენტო
წმ. ნიკოლოზის/ ნ. ჩხეიძის 2
0101 თბილისი, საქართველო
ტელ.: (+995 32) 91 51 40
ელ. ფოსტა: info@dea.gov.ge

# Contents

## 1. შესავალი

აღნიშნული სტანდარტი წარმოადგენს ორგანიზაციაში ინფორმაციული უსაფრთხოების რისკების მართვის სახელმძღვანელოს, კერძოდ მხარს უჭერს ინფორმაციული უსაფრთხოების მართვის სისტემების (იუმს) მოთხოვნებს მგს 27001:2011-ის (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები) თანახმად. თუმცაღა აღნიშნული სტანდარტი არ წარმოადგენს რაიმე სპეციფიკურ მეთოდოლოგიას ინფორმაციული უსაფრთხოების რისკების მართვის კუთხით. კონკრეტულმა ორგანიზაციამ თავად უნდა განსაზღვროს თუ როგორი იქნება მისი მიდგომა რისკების მართვისადმი, რაც დამოკიდებულია, მაგალითად, იუმს-ის მიზნებზე, რისკების მართვის გარემოზე, ან დარგობრივ სექტორზე. არსებული მეთოდოლოგიები შეიძლება გამოყენებული იქნას იმ სტრუქტურით, რაც აღწერილია აღნიშნულ სტანდარტში, რათა განხორციელდეს იუმს-ის მოთხოვნები.

# ინფორმაციული ტექნოლოგია - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთხოების რისკის მართვა

## 1. გამოყენების სფერო

აღნიშნული სტანდარტი წარმოადგენს ინფორმაციული უსაფრთხოების რისკების მართვის სახელმძღავნელოს.

აღნიშნული სტანდარტი მხარს უჭერს მგს 27011:2001-ში განსაზღვრულ ძირითად კონცეფციებს და მისი მიზანია ხელი შეუწყოს ინფორმაციული უსაფრთხოების ადექვატურ განხორციელებას, რაც დაფუძნებული იქნება რისკების მართვის მიდგომაზე.

მგს 27001-სა (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები) და 27002-ში (ინფორმაციული ტექნოლოგია - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთხოების მართვის წესები და ნორმები) აღწერილი კონცეფციების, მოდელების, პროცესებისა და ტერმინოლოგიის ცოდნა მნიშვნელოვანია აღნიშნული სტანდარტის სრულყოფილად გაგებისათვის.

მოცემული სტანდარტი მიესადაგება ყველა ტიპის ორგანიზაციას რისკების მართვის განხორციელებისთვის (მაგალითად: კომერციული ორგანიზაციები, სამთავრობო უწყებები, არაკომერციული ორგანიზაციები).

## 2. ნორმატიული საცნობარო ინფორმაცია

შემდეგი საცნობარო დოკუმენტაცია არის აუცილებელი მოცემული დოკუმენტის თანხლებისათვის.

მგს 27001:2011, *ინფორმაციული ტექნოლოგია - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთხოების მართვის სისტემები - მოთხოვნები*
მგს 27002:2011, *ინფორმაციული ტექნოლოგია - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთხოების მართვის წესები და ნორმები*

## 3. ტერმინები და განმარტებები

მოცემული დოკუმენტი გამოიყენებს მგს 27001:2011, მგს 27002:2011-ში განმარტებულ ტერმინებს.

3.1.

**გავლენა**

მიღწეულ შედეგებზე საზიანო ცვლილების მოხდენა

3.2.

**ინფორმაციული უსაფრთხოების რისკი**

შესაძლებლობა იმისა, რომ მოცემული საფრთხე ისარგებლებს ინფორმაციული უსაფრთხოების აქტივის ან აქტივების სისუსტით და ამგვარად გამოიწვევს ორგანიზაციისთვის ზიანის მიყენებას.

3.3

**რისკის თავიდან არიდება**

რისკის შემცველ სიტუაციში არ მონაწილეობის ან მასზე უარის თქმის შესახებ გადაწყვეტილების მიღება

3.4

**რისკების შესახებ ინფორმირება**

რისკის შესახებ ინფორმაციის გაცვლა ან გაზიარება გადაწყვეტილების მიმღებ და სხვა დაინტერესებულ პირებს შორის.

3.5

**რისკის მიახლოებითი შეფასება**

რისკის ალბათობისა და მისი შედეგების ფასეულობის დადგენის პროცესი

3.6

**რისკის აღმოჩენა**

რისკის შემცველი ელემენტების პოვნა, ჩამოთვლა და მახასიათებლების აღწერა

3.7

**რისკის შემცირება**

ქმედება, რომელიც მიმართულია რისკთან დაკავშირებული ალბათობის ან/და უარყოფითი შედეგების შესამცირებლად

3.8

**რისკის დაშვება**

ცალკეული რისკისგან მიღებულ სარგებლზე ან მისი დაკარგვით გამოწვეულ სირთულეებზე თანხმობა

3.9

**რისკის გადაცემა**

მესამე მხარესთან რისკისგან მიღებული სარგებლის ან მისი დაკარგვით გამოწვეულ სირთულეებზე პასუხისმგებლობის განაწილება.

## 4. აღნიშნული სტანდარტის სტრუქტურა

მოცემული სტანდარტი შეიცავს ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის აღწერასა და მასთან დაკავშირებულ ქმედებებს.
დამატებითი ინფორმაცია წარმოდგენილია 5-ე პუნქტში.
ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის ზოგადი მიმოხილვა მოცემულია 6-ე პუნქტში.

ინფორმაციული უსაფრთხოების რისკების მართვასთან დაკავშირებული ყველა ქმედება, რაც წარმოდგენილია 6-ე პუნქტში, მოგვიანებით აღწერილია შემდეგ პუნქტებში:

- ორგანიზაციული გარემოს დადგენა 7-ე პუნქტში;
- რისკების შეფასება 8-ე პუნქტში;
- რისკებთნა მობყრობა 9-ე პუნქტში;
- რისკების მიღება 10-ე პუნქტში;
- რისკების შესახებ ინფორმირება 11-ე პუნქტში;
- რისკების მონიტორინგი და განხილვა 12-ე პუნქტში.

დამატებითი ინფორმაცია ინფორამციული უსაფრთხოების რისკების მართვასთან დაკავშრებულ ქმედებებზე წარმოდგენილია დანართებშიც. **დანართი ა** წარმოადგენს ორგანიზაციული გარემოს შესახებ ინფორმაციას (განსაზღვრულია ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის მასშტაბი და საზღვრები). აქტივების იდენტიფიცირება და ფასეულობის დადგენა და შეფასებების ზეგავლენა განხილულია **დანართში ბ** (აქტივების მაგალითი), **დანართი გ** (ტიპიური საფრთხეების მაგალითი) და **დანართი დ** (ტიპიური სისუსტეების მაგალითი).

ინფორმაციული უსაფრთხოების რისკების მართვის მიდგომების ნიმუშები წარმოდგენილია **დანართში ე.**
რისკების შემცირების შეზღუდვები წარმოდგენილია **დანართში ვ**.

რისკების მართვასთან დაკავშირებული ყველა ქმედება, რომლებიც წარმოდგენილია **7-ე დანართიდან 12-ე დანართამდე** სტრუქტურულად გამოიყურება შემდეგნაირად:

**შემავალი რესურსები:** ქმედების შესასრულებლად საჭირო ყველა ინფორმაციის იდენტიფიცირება.

**ქმედება:** აღწერს ქმედებას.

**სახელმძღვანელო მითითებები:** წარმოადგენს ქმედებების შესრულების სახელმძღვანელოს. თუმცა შესაძლოა ორგანიზაციამ სხვა უფრო ეფექტური გზებიც არჩიოს.

**შედეგები:** ქმედების შესრულების შემდეგ მიღებული ნებისმიერი ინფორმაციის იდენტიფიცირება.

## 5. წინა პირობები

ინფორმაციული უსაფრთხოების რისკების მართვისადმი სისტემური მიდგომა აუცილებელია ორგანიზაციის საჭიროებების იდენტიფიცირებისათვის ინფორმაციული უსაფრთხოების მოთხოვნების თვალსაზრისით და ეფექტური ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) შესაქმნელად. ეს მიდგომა უნდა შეესაბამებოდეს ორგანიზაციულ გარემოს. უსაფრთხოების მიმართულებით გამოსაყენებელმა ძალისხმევებმა ეფექტურად და დროულად უნდა განახორციელონ საპასუხო ქმედებები. ინფორმაციული უსაფრთხოების რისკების მართვა უნდა იყოს ინფორმაციული უსაფრთხოების მართვის განუყოფელი ნაწილი და უნდა გამოიყენებოდეს იუმს-ის როგორც დანერგვის, ასევე მისი ფუნქციონირების ეტაპებზე.

ინფორმაციული უსაფრთხოების რისკების მართვა უნდა იყოს უწყვეტი პროცესი. პროცესმა უნდა დაადგინოს ორგანიზაციული გარემო, შეაფასოს რისკები და გადაჭრას რისკები რისკებთან მობყრობის გეგმის მიხედვით რეკომენდაციების და გადაწყვეტილებების დასანერგად. რისკების დასაშვებ დონეზე დაყვანისათვის რისკების მართვა აანალიზებს რეაგირების არქონის შემთხვევაში შესაძლო უარყოფით მოვლენებს და განსაზღვრავს სამოქმედო გეგმას.

ინფორმაციული უსაფრთხოების რისკების მართვამ ხელი უნდა შეუწყოს:

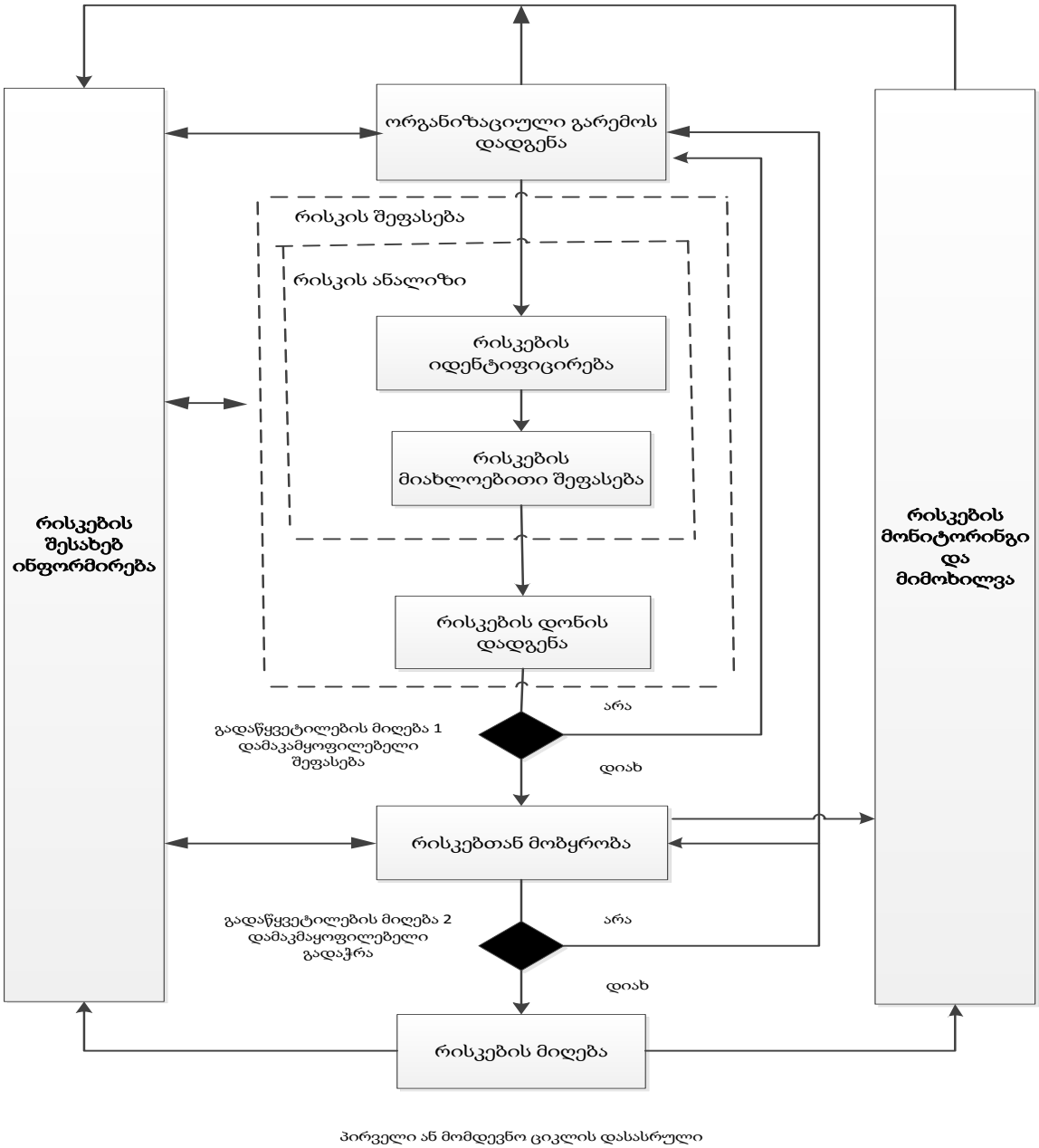
- რისკების იდენტიფიცირებას;
- რისკების შეფასებას იმისდა მიხედვით, თუ რა შედეგები მოყვება მათ ბიზნესთან მიმართებაში და მათი ხდომილების ალბათობა;
- ამ რისკების დადგომის ალბათობას და მათ შესაძლო შედეგებს, მათ შესახებ ინფორმირებულობის არსებობას;
- რისკებთან მობყრობის პრიორიტეტულობის დადგენას;
- რისკების შემცირების შესახებ ქმედებების პრიორიტეტულობას;

- რისკების მართვასთან დაკავშირებული გადაწყვეტილებების მიღებაში ჩართული დაინტერესებული პირები და მათი ინფორმირებულობა რისკების მართვის სტატუსის შესახებ;
- რისკებთან მობყრობის მონიტორინგის ეფექტიანობას;
- რისკებისა და რისკების მართვის პროცესის რეგულარულ მონიტორინგსა და განხილვას;
- რისკების მართვისადმი მიდგომის გაუმჯობესების მიზნით საჭირო ინფორმაციის შეგროვებას;
- მენეჯერებისა და თანამშრომლების ინფორმირებულობას რისკებისა და მათი შემცირების შესახებ.

ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი შესაძლოა მიესადაგოს მთლიან ორგანიზაციას, ან მის ცალკეულ ნაწილს (მაგალითად: დეპარატმენტს, ფიზიკურ მდებარეობას, სერვისს), ნებისმიერ ინფორმაციულ სისტემას, კონტროლის მექანიზმების არსებულ ან დაგეგმილ ან სპეციფიკურ ასპექტებს (მაგალითად: ბიზნესის უწყვეტობის დაგეგმვა).

# 6. ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის მიმოხილვა

ინფორმაციული უსაფრთხოების მართვის პროცესი შედგება შემდეგი პროცესებისგან: ორგანიზაციული გარემოს დადგენა (7), რისკების შეფასება (8), რისკებთან მობყრობა (9), რისკების მიღება (10), რისკების შესახებ ინფორმირება (11) და რისკების მონიტორინგი და განხილვა (12).




ნახაზი 1 - ინფორმაციული უსაფრთხოების რისკის მართვის პროცესი

როგორც ნახაზი 1 გვიჩვენებს, ინფორმაციული უსაფრთხოების მართვის პროცესი შეიძლება იყოს განმეორებადი ხასიათის რისკების შეფასებისა და/ ან რისკებთან მობყრობის ქმედებების თვალსაზრისით. რისკის შეფასების მართვის განმეორებადობამ შესაძლოა გააღრმავოს და უფრო დეტალური გახადოს შეფასება ყოველი შემდგომი ციკლისას. განმეორებადი ხასიათის მიდგომა წარმოადგენს საუკეთესო ბალანსს დროის დაზოგვასა და კონტროლის მექანიზმის იდენტიფიცირებას შორის, ამავდროულად უზრუნველყოფს მაღალი დონის რისკების შესაბამის შეფასებას.

პირველ რიგში უნდა დადგინდეს გარემო. შემდგომ კი უნდა მოხდეს რისკის შეფასება. თუ ამ ქმედებების შემდეგ ხელთ გვექნება საკმარისი ინფორმაცია იმისათვის, რომ რისკები დაყვანილი იქნას დასაშვებ დონემდე, მაშინ შეიძლება ჩაითვალოს, რომ დავალება შესრულებულია და შემდგომი ეტაპი უკვე არის რისკებთან მობყრობა. არასაკმარისი ინფორმაციის არსებობის შემთხვევაში ადგილი ექნება რისკის შეფასების შემდგომ ციკლს (გარემოს გადახედვის ჩათვლით) (მაგალითად: რისკების შეფასების, მნიშვნელოვნების დადგენის კრიტერიუმები, რისკებზე თანხმობის კრიტერიუმები ან ზემოქმედების კრიტერიუმები), რაც სავარაუდოდ ვრცელდება მთლიანი ფარგლების კონკრეტულ ნაწილზე (იხილეთ ნახაზი 1, გადაწყვეტილების მიღება 1).

რისკებთან მობყრობის ეფექტიანობა დამოკიდებულია რისკის შეფასების შედეგებზე. შესაძლებელია რისკებთან მობყრობამ მაშინვე არ უზრუნველყოს მოცემული რისკის დასაშვები დონე. ასეთ შემთხვევაში შესაძლოა საჭირო გახდეს რისკების განმეორებითი შეფასება გარემოს განსაზღვრის შეცვლილი პარამეტრებით (მაგალითად: რისკების შეფასება, რისკების მიღება ან რისკების გავლენის კრიტერიუმები), რომლის თანმხლები პროცესი არის რისკებთან შემდგომი მობყრობა (იხილეთ ნახაზი 1, გადაწყვეტილების მიღება 2).

რისკების მიღებამ უნდა უზრუნველყოს რეაგირების გარეშე დარჩენილ რისკზე ცალსახა თანხმობა ორგანიზაციის მენეჯერების მხრიდან. ეს მომენტი განსაკუთრებით მნიშვნელოვანია ისეთ დროს, როდესაც კონტროლის მექანიზმის დანერგვა უგულვებელყოფილია ან გადადებულია, მაგალითად ხარჯების მიზეზით.

ინფორმაციული უსაფრთხოების რისკების მართვის მთელი პროცესის განმავლობაში მნიშვნელოვანია, რომ არსებობდეს კომუნიკაცია რისკებსა და მათთან მობყრობას შორის, ასევე შესაბამის მენეჯერებსა და საოპერაციო თანამშრომლებს შორის. რისკთან მობყრობამდე კი ძალზე მნიშვნელოვანია ინფორმაცია იდენტიფიცირებული რისკის შესახებ, რათა მოხდეს ინციდენტის მართვა, რამაც შესაძლოა ხელი შეუწყოს პოტენციური ზიანის შემცირებას. მენეჯრებისა და თანამშრომლების ინფორმირებულობა ორგანიზაციის რისკების შესახებ, რისკების და პრობლემური საკითხების შემცირების კონტროლის მექანიზმის შესახებ ხელს უწყობს ინციდენტების და მოულოდნელი შემთხვევების ეფექტურ აღმოფხვრას. ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის თითოეული ქმედების დეტალური შედეგი და ასევე რისკების შესახებ გადაწყვეტილების მიღების შედეგი უნდა იყოს დოკუმენტირებული.

მგს 27001:2011 (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები) განსაზღვრავს, რომ იუმს-ის მიერ დადგენილ ფარგლებსა და წინასწარ განსაზღვრულ გარემოში დანერგილი კონტროლის მექანიზმები უნდა ეფუძნებოდეს რისკებს. ეს მოთხოვნა შესაძლოა დააკმაყოფილოს ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის გამოყენებამ. არსებობს რამდენიმე მიდგომა, რომელთა გამოყენებაც პროცესის წარმატებულ განხორციელებას უზრუნველყოფს ორგანიზაციაში. ორგანიზაციამ უნდა გამოიყენოს ისეთი მიდგომა, რომელიც ყველაზე მეტად მიესადაგება არსებულ პროცესებს.

იუმს-ის მიერ განსაზღვრული გარემო, რისკების შეფასება, რისკებთან მობყრობის გეგმის შემუშავება და რისკების მიღება გახლავთ **„დაგეგმვის“** ფაზის ნაწილი. იუმს-ის მიერ განსაზღვრული **„აღსრულების“** ფაზა გულისხმობს, რომ რისკების დასაშვებ დონეზე დაყვანასთან დაკავშირებული საჭირო ქმედებები და კონტროლის მექანიზმები დანერგილია რისკებთან მობყრობის გეგმის თანახმად. იუმს-ის მიერ განსაზღვრული **„შემოწმების“** ფაზა გულისხმობს, რომ მენეჯერებმა უნდა განსაზღვრონ რისკების შეფასების და მათთან მობყრობის გადასინჯვის საჭიროება ინციდენტებისა და ცვლილებების გათვალისწინებით. **„ქმედების“** ფაზაში სრულდება ნებისმიერი საჭირო ქმედება, მათ შორის ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი.

ქვემოთ მოყვანილი ცხრილი აჯამებს ინფორმაციული უსაფრთხოების რისკების მართვის ყველა საჭირო ქმედებას იუმს-ის მიერ განსაზღვრული ოთხივე ფაზისათვის:

**ცხრილი 1 - იუმს-ის და ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის შესაბამისობა**

| **იუმს-ის პროცესი** | **ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი** |
|---|---|
| დაგეგმვა | გარემოს განსაზღვრა<br>რისკების შეფასება<br>რისკებთან მობყრობის გეგმის შემუშავება<br>რისკების მიღება |
| აღსრულება | რისკებთან მობყრობის გეგმის დანერგვა |
| შემოწმება | რისკების უწყვეტი მონიტორინგი და მიმოხილვა |
| ქმედება | ინფორმაციული უსაფრთხოების მართვის პროცესის მხარდაჭერა და გაუმჯობესება |

# 7. გარემოს განსაზღვრა

## 7.1 ზოგადი მოსაზრებები

**შემავალი რესურსები:** ინფორმაციული უსაფრთხოების რისკების მართვის გარემოს განსაზღვრისთვის აუცილებელი ყველა სახის ორგანიზაციული ინფორმაცია.
**ქმედება:** ინფორმაციული უსაფრთხოების რისკების მართვის გარემო უნდა იქნას განსაზღვრული, რაც თავისთავად მოიცავს საჭირო კრიტერიუმების დადგენას ინფორმაციული უსაფრთხოების რისკების მართვის თვალსაზრისით (7.2), გამოყენების სფეროსა და ჩარჩოების განსაზღვრას (7.3) და შესაბამისი ორგანიზაციული სტრუქტურის შექმნას, რომელიც განახორციელებს ინფორმაციული უსაფრთხოების რისკების მართვას (7.4).

**სახელმძღვანელო მითითებები:** ინფორმაციული უსაფრთხოების რისკების მართვის მიზნის განსაზღვრა არის არსებითი მომენტი, რადგანაც იგი ზეგავლენას ახდენს მთლიან პროცესზე და გარემოს განსაზღვრაზე ნაწილობრივ. მიზანი შესაძლოა იყოს:

- იუმს-ის მხარდაჭერა
- კანონთან შესაბამისობა და საქმის ზედმიწევნით შესრულების მტკიცებულება
- ბიზნეს უწყვეტობის გეგმის მომზადება
- ინციდენტზე რეაგირების გეგმის მომზადება
- ინფორმაციული უსაფრთოების მოთხოვნების აღწერა პროდუქტის ან სერვისის კუთხით

გარემოს განსაზღვრის წესი ასევე განხილულია პუნქტებში: 7.2, 7.3 და 7.4.

**შედეგები:** ძირითადი კრიტერიუმების, მიზნების და ჩარჩოების სპეციფიკაცია და ორგანიზაციული სტრუქტურა ინფორმაციული უსაფრთხოების რისკების მართვის პროცესისათვის.

## 7.2. ძირითადი კრიტერიუმები

რისკების მართვის ფარგლებიდან და მიზნებიდან გამომდინარე, შესაძლოა გამოყენებული იქნას სხვადასხვა მიდგომები. ასევე სხავდასხვა სახის მიდგომა შეიძლება არსებობდეს ყოველი შემდგომი ციკლისთვის.

შერჩეული და შემუშავებული უნდა იქნას რისკების მართვის შესაბამისი მიდგომა, რომელიც მიმართებაშია ისეთ ძირითად კრიტერიუმებთან, როგორებიცაა: რისკების შეფასების კრიტერიუმები, გავლენის კრიტერიუმები, რისკების მიღების კრიტერიუმები.
ასევე, ორგანიზაციამ უნდა შეაფასოს არსებობს თუ არა საჭირო რესურსები:

- რისკების შეფასებისა და რისკებთან მობყრობის გეგმის შემუშავებისთვის;
- პოლიტიკისა და პროცედურების განსაზღვრა და განხორციელება, მათ შორის შერჩეული კონტროლის მექანიზმების დანერგვა;
- კონტროლის მექანიზმების მონიტორინგი
- ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის მონიტორინგი

### რისკების დონის დადგენის კრიტერიუმები

რისკების დონის დადგენის კრიტერიუმები უნდა შემუშავდეს ორგანიზაციის ინფორმაციული უსაფრთხოების რისკების შეფასების მიზნით, რაც ასევე გულისხმობს შემდეგს:

- ბიზნეს ინფორმაციის პროცესის სტრატეგიული მნიშვნელობა;
- ჩართული ინფორმაციული აქტივების კრიტიკულობა;
- იურიდიული და მარეგულირებელი მოთხოვნები, სახელშეკრულებო ვალდებულებები;
- ხელმისაწვდომობის, კონფიდენციალურობისა და მთლიანობის ოპერაციული და ბიზნეს მნიშვნელობა;
- დაინტერესებული პირების მოლოდინები და აღქმა, და რეპუტაციის შელახვის უარყოფითი შედეგები;

დამატებით, ასევე შესაძლოა რისკების დონის დადგენის კრიტერიუმები გამოყენებული იქნას რისკების გადაჭრის პრიორიტეტების განსაზღვრისათვის.

### გავლენის კრიტერიუმები

გავლენის კრიტერიუმები შემუშავებული და განსაზღვრული უნდა იქნას ორგანიზაციისთვის მიყენებული ზიანის ან ხარჯების დონის გათვალისწინებით, რაც შესალოა გამოწვეული იყოს ინფორმაციული უსაფრთხოების შემთხვევის მიერ და მოიცავდეს შემდგომს:

- რისკის გავლენის ქვეშ არსებული ინფორმაციული აქტივის კალსიფიკაციის დონე;
- ინფორმაციული უსაფრთხოების დარღვევა (მაგალითად: კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დაკარგვა);
- გაუარესებული ოპერაციები (შიდა ან მესამე მხარისა);
- ბიზნეს და ფინანსური ღირებულების შემცირება;
- გეგმებისა და მათი შესრულების ვადების დარღვევა;
- რეპუტაციის შელახვა;
- იურიდიული, მარეგულირებელი და სახელშეკრულებო მოთხოვნების დარღვევა.

### რისკის მიღების კრიტერიუმები

შემუშავებული და განსაზღვრული უნდა იქნას რისკის მიღების კრიტერიუმები. რისკის მიღების კრიტერიუმები დამოკიდებულია ორგანიზაციის პოლიტიკაზე, მიზნებზე და დაინტერესებული პირების ინტერესებზე.
ორგანიზაციამ თავად უნდა განსაზღვროს დასაშვები რისკის საკუთარი სქემა. შემუშავების პროცესში გათვალისწინებული უნდა იყოს შემდეგი:

- რისკის მიღების კრიტერიუმებს შესაძლოა ქონდეს შეზღუდვები რისკების სასურველი დონის თვალსაზრისით, მაგრამ აუცილებელია გარკვეულ ვითარებებში ზედა რგოლის მენეჯერების მხრიდან განხორციელდეს რევიზია, რათა მიღებული იქნას თანხმობა ამ კონკრეტული დონის ზემოთ დაფიქსირებულ რისკებზე;
- რისკის მიღების კრიტერიუმები შეიძლება წარმოდგენილი იყოს როგორც გაანგარიშებული მოგების შეფარდება გაანგარიშებულ რისკთან;
- რისკის მიღების სხვადასხვა კრიტერიუმები შეიძლება მიესადაგოს სხვადასხვა კლასის რისკებს, მაგალითად: რისკებმა შესაძლოა თავი იჩინონ მარეგულირებლებთან ან კანონთან შეუსაბამობის შედეგად და, ამდენად, არ მოხდეს ასეთ რისკებზე თანხმობა, მაშინ, როდესაც მაღალი დონის რისკებზე თანხმობა შეიძლება დასაშვები იყოს, თუკი ამის საშუალებას იძლევა სახელშეკრულებო მოთხოვნები;
- რისკის მიღების კრიტერიუმები შეიძლება შეიცავდეს სამომავლოდ მათი გადაჭრის მოთხოვნებს, მაგალითად რისკი შესაძლოა მიღებული იქნას, თუკი არსებობს მტკიცებულება და ვალდებულება იმისა, რომ განხორციელდეს ქმედება რისკის დასაშვებ (მისაღებ) დონემდე შემცირების მიზნით განსაზღვრულ დროის პერიოდში.

რისკის მიღების კრიტერიუმები ერთმანეთისგან რისკის არსებობის მოსალოდნელი ხანგრძლივობით განსხვავდებიან, მაგალითად: რისკი შეიძლება დაკავშირებული იყოს ხანგრძლივ ან ხანმოკლე ქმედებებთან. რისკის მიღების კრიტერიუმები უნდა ითვალისწინებდეს და ეფუძნებოდეს შემდეგს:

- ბიზნეს კრიტერიუმები;
- იურიდიული და მარეგულირებელი ასპექტები;
- ოპერაციები;
- ტექნოლოგია;
- ფინანსები;
  სოციალური და ადამიანური ფაქტორები.

დამატებითი ინფორმაცია იხილეთ **დანართში ა.**

## 7.3. გამოყენების სფერო და საზღვრები

ორგანიზაციამ უნდა განსაზღვროს ინფორმაციული უსაფრთხოების რისკის მართვის გამოყენების სფერო და საზღვრები.

ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის მიზნები აუცილებლად უნდა იქნას განსაზღვრული, რათა გათვალისწინებული იყოს ყველა საჭირო აქტივი რისკების შეფასებისას. დამატებით უნდა ითქვას, რომ საზღვრების დადგენა ასევე აუცილებელია [იხილეთ მგს 27001:2011 (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები) პუნქტი 4.2.1 ა)], რათა რეაგირება მოხდეს ისეთ რისკებზე, რომლებმაც შესაძლოა თავი იჩინონ კონკრეტულ ფარგლებში.

ორგანიზაციის შესახებ ინფორმაციის შეგროვება აუცილებელია იმ გარემოს დასადგენად, რომელშიც იგი ფუნქციონირებს და ასევე მისი გასათვალისწინებელია მისი აუცილებლობა ინფორმაციული უსაფრთხოების რისკების მართვის პროცესისთვის.

გამოყენების სფეროსა და საზღვრების დადგენისას ორგანიზაციამ უნდა გაითვალისწინოს შემდეგი ინფორმაცია:

- ორგანიზაციის სტრატეგიული ბიზნეს მიზნები, სტრატეგია და პოლიტიკა;
- ბიზნეს პროცესები;
- ორგანიზაციის ფუნქციები და სტრუქტურა;
- ორგანიზაციის შესაბამისი იურდიული, მარეგულირებელი და სახელშეკრულებო მოთხოვნები;
- ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკა;
- ორგანიზაციის ზოგადი მიდგომა რისკების მართვისადმი;
- ინფორმაციული აქტივები;
- ორგანიზაციის ადგილმდებარეობა და მისი გეოგრაფიული მახასიათებლები;
- ორგანიზაციაზე გავლენის მომხდენი ფაქტორები;
- დაინტერესებული პირების მოლოდინები;
- სოციალურ-კულტურული გარემო;
- ინტერფეისები (მაგალითად: გარემოსთან გაცვლილი ინფორმაცია).

დამატებით, ორგანიზაციამ უნდა უზრუნველყოს გამონაკლისების გამართლება.
რისკის მართვის მიზნის მაგალითად შესაძლოა ჩაითვალოს ი.ტ. პროგრამული უზრუნველყოფები, ი.ტ. ინფრასტრუქტურა, ბიზნეს-პროცესი ან ორგანიზაციის განსაზღვრული ნაწილი.

**შენიშვნა:** ინფორმაციული უსაფრთხოების რისკების მართვაში ნახსენები ფარგლები და საზღვრები დაკავშირებულია მგს 27001:2011-ის 4.2.1 ა პუნქტში განმარტებულ იუმს-ის ფარგლებსა და საზღვებთან.

დამატებითი ინფორმაცია იხილეთ **დანართში ა**.

## 7.4. ინფორმაციული უსაფრთხოების რისკების მართვის ორგანიზაციული სტრუქტურა

უნდა დადგინდეს და დაცული იქნას ინფორმაციული უსაფრთხოების რისკების მართვის პროცესისთვის საჭირო ორგანიზაციული სტრუქტურა და პასუხისმგებლობები. ძირითადი როლები და პასუხისმგებლობები გახლავთ:

- ორგანიზაციაზე მორგებული ინფორმაციული უსაფრთხოების რისკების მართვის პორცესის შემუშავება;
- დაინტერესებული პირების გამოვლენა და ანალიზი;
- ყველა მხარის (როგორც შიდა ასევე გარე) როლებისა და პასუხისმგებლობების განსაზღვრა ორგანიზაციისათვის;
- ორგანიზაციასა და დაინტერესებულ პირებს შორის საჭირო ურთიერთობის დამტკიცება, ასევე ორგანიზაციის მაღალი დონის რისკების მართვის ფუნქციებისთვის ინტერფეისების დადგენა (მაგალითად: ოპერაციული რისკების მართვა), ასევე სხვა პროექტების და ქმედებებისთვის საჭირო ინტერფეისები;
- გადაწყვეტილების მიღების წესის განსაზღვრა;
- აღრიცხვიანობის (რეგისტრირების, ჩანაწერების) მახასიათებლები.

ამგვარი ორგანიზაციული სტრუქტურა დამტკიცებული უნდა იქნას მენეჯერების მიერ.

# 8 ინფორმაციული უსაფრთხოების რისკების შეფასება

## 8.1 ინფორმაციული უსაფრთხოების რისკების შეფასების ზოგადი აღწერა

**შენიშვნა:** რისკების შეფასების ქმედებები მოხსენიებულია როგორც პროცესი მგს 27001:2011-ში.

**შემავალი რესურსები:** ძირითადი კრიტერიუმები, ფარგლები და საზღვრები და ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის ორგანიზაციული სტრუქტურის ჩამოყალიბება.

**ქმედება:** უნდა მოხდეს რისკების იდენტიფიცირება, მათი რაოდენობრივი და ხარისხობრივი აღწერა, და ორგანიზაციაში არსებული რისკების შეფასების კრიტერიუმების და მიზნების პრიორიტეტების დადგენა.

**სახლემძღვანელო მითითებები:** რისკი, ეს არის არასასურველი მოვლენით ან მისი ხდომილების ალბათობით გამოწვეული უარყოფითი შედეგების კომბინაცია. რისკების რაოდენობრივი და ხარისხობრივი შეფასება აღწერს რისკს და საშუალებას აძლევს მენეჯერებს პრიორიტეტები მიანიჭონ რისკებს სერიოზულობისა ან სხვა დადგენილი კრიტერიუმების მიხედვით.
რისკების შეფასება შედგება შემდეგი ქმედებებისგან:

- რისკის ანალიზი (პუნქტი 8.2), რომელიც შეიცავს:
  - რისკების იდენტიფიცირებას (პუნქტი 8.2.1)
  - რისკების მიახლოებითი შეფასება (პუნქტი 8.2.2)
- რისკის დონის დადგენა (პუნქტი 8.3)

რისკების შეფასება განსაზღვრავს ინფორმაციული აქტივების ფასულობას, ახდენს მოსალოდნელი საფრთხეების და არსებული (ან შესაძლო) სუსტი წერტილების იდენტიფიცირებას, განსაზღვრავს არსებულ კონტროლის მექანიზმს და მის გავლენას აღმოჩენილ რისკებზე, ასევე განსაზღვრავს პოტენციურ უარყოფით შედეგებს და საბოლოოდ ანიჭებს პრიორიტეტებს გამოვლენილ რისკებს და ახდენს მათ კლასიფიცირებას კონკრეტულ გარემოში.

რისკების შეფასება ხშირად წარიმართება ორ (ან მეტ) განმეორებად ციკლად. პირველ რიგში უნდა ჩატარდეს ზედა დონის შეფასება, რათა მოხდეს პოტენციურად მაღალი რისკების გამოვლენა, რაც წარმოადგენს საფუძველს შემდგომი შეფასებისთვის. მომდევნო განმეორებადი ციკლი მოიცავს იმ მაღალი რისკების შემდგომ სიღრმისეულ განხილვას, რომლებიც აღმოჩენილი იქნა საწყისი ციკლის დროს. თუკი გარკვეულ ეტაპზე იგი იძლევა რისკის შეფასების თვალსაზრისით არასაკმარის ინფორმაციას, მაშინ ხორციელდება შემდგომი დეტალური ანალიზი, სავარაუდოდ განსხვავებული მეთოდების გამოყენებით კონკრეტულ ნაწილზე.

მთლიანად ორგანიზაციაზეა დამოკიდებული რისკების მართვისადმი საკუთარი მიდგომის არჩევა, რაც დაფუძნებული იქნება რისკების შეფასების მიზნებსა და ამოცანებზე.

ინფორმაციული უსაფრთხოების რისკების შეფასებისადმი მიდგომების განხილვა მოცემულია **დანართში ე**.

**<u>შედეგები:</u>** შეფასებული რისკების ჩამონათვალი, სადაც თითოეულ მათგანს მინიჭებული აქვს პრიორიტეტები რისკების შეფასების კრიტერიუმების თანახმად.

## 8.2 რისკების ანალიზი

### 8.2.1 რისკების იდენტიფიკაცია

#### *8.2.1.1 შესავალი*

რისკების იდენტიფიკაციის მიზანია განისაზღვროს თუ რა შეიძლება მოხდეს პოტენციური დანაკარგის გამოწვევით, და მოვიპოვოთ ცოდნა იმისა, თუ როგორ, სად და რატომ შეიძლება მოხდეს დანაკარგი. 8.2.1-ის ქვეპუნქტებში აღწერილია შეგროვებული შემავალი რესურსები რისკების მიახლოებითი შეფასებისათვის.

**შენიშვნა:** ქვემოთ პუნქტებში აღწერილი ქმედებები შეიძლება განხორციელდეს სხვადასხვა თანმიმდევრობით გამოყენებული მეთოდოლოგიის თანახმად.

### *8.2.1.2 აქტივების იდენტიფიკაცია*

**<u>შემავალი რესურსები:</u>** განსახორციელებელი რისკების შეფასების მიზნები და ჩარჩოები, შემადგენელი ნაწილების ჩამონათვალი მფლობელების, ადგილმდებარეობის, ფუნქციის შესაბამისად და ასე შემდეგ.

**<u>ქმედება:</u>** უნდა მოხდეს აქტივების იდენტიფიცირება დადგენილ ჩარჩოებში (მგს 27001:2011 (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები) , პუნქტი 4.2.1 დ) 1-ის შესაბამისად).

**<u>სახელმძღვანელო მითითებები:</u>** აქტივი არის ნებისმიერი რამ, რაც ფასეულია ორგანიზაციისთვის და ამდენად მოითხოვს დაცვას. აქტივების იდენტიფიცირებისათვის უნდა გვახსოვდეს, რომ ინფორმაციული სისტემა არ შედგება მხოლოდ აპარატურისა და კომპიუტერული პროგრამებისგან.

აქტივების იდენტიფიკაცია უნდა შესრულდეს დეტალურობის გარკვეულ მისაღებ დონემდე, რაც განაპირობებს რისკების შეფასებისათვის საჭირო ინფორმაციის მოპოვებას. აქტივების იდენტიფიკაციისას გამოყენებული დეტალურობის დონე გავლენას ახდენს რისკების შეფასებისას შეგროვილი ინფორმაციის მოცულობაზე. აღნიშნული დონე შეიძლება გაუმჯობესებული იქნას რისკების შეფასების შემდგომი ციკლის დროს.

ყოველი აქტივის იდენტიფიცირებისას აუცილებლად უნდა მოხდეს კონკრეტული აქტივის მფლობელის გამოვლენა, რათა დადგინდეს აქტივზე პასუხისმგებლობა და ანგარიშვალდებულება. აქტივის მფლობელს შესაძლოა არ გააჩნდეს საკუთრების უფლება კონკრეტულ აქტივზე, მაგრამ მას აქვს პასუხისმგებლობა მის წარმოებაზე, განვითარებაზე, მხარდაჭერაზე, გამოყენებასა და მის უსაფრთხოებაზე საჭიროების შემთხვევაში. აქტივის მფლობელი ხშირად არის სწორედ ის პირი, რომელიც განსაზღვრავს კონკრეტული აქტივის ფასეულობას ორგანიზაციისათვის (იხილეთ 8.2.2.2 აქტივების შეფასება).

ორგანიზაციის აქტივებზე განხორციელებული მეთვალყურეობის ჩარჩოები წარმოადგენს იმ არეალს, რომელიც განსაზღვრულია ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის წარმართვისათვის.

დამატებითი ინფორმაცია აქტივების იდენტიფიკაციისა და ფასეულობის დადგენის შესახებ (ინფორმაციული უსაფრთხოების თვალსაზრისით) შეგიძლიათ იხილოთ **დანართში ბ**.

**შედეგები:** რისკის შემცველი აქტივების ჩამონათვალი, ასევე ამ აქტივებთან დაკავშირებული ბიზნეს-პროცესები და მათი მნიშვნელობა.

### *8.2.1.3 საფრთხეების დადგენა*

**შემავალი რესურსები:** ინფორმაცია საფრთხეების შესახებ მოიპოვება ინციდენტების მიმოხილვის, აქტივების მფლობელების, მომხმარებლების და სხვა წყაროების, მათ შორის გარე საფრთხეების კატალოგის მეშვეობით.

**ქმედება:** უნდა მოხდეს საფრთხეებისა და მათი წარმოშობის წყაროების იდენტიფიცირება (მგს 27001:2011 (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები), პუნქტი 4.2.1 დ) 1)).

**სახელმძღვანელო მითითებები:** საფრთხეს შეუძლია ზიანი მიაყენოს ისეთ აქტივებს, როგორებიცაა ინფორმაცია, პროცესები და სისტემები, და აქედან გამომდინარე თავად ორგანიზაციასაც. საფრთხეები შეიძლება იყოს ბუნებრივი ხასიათის ან ადამიანის მიერ შექმნილი, და ასევე შემთხვევითი ან გამიზნული. აუცილებლად უნდა იქნას იდენტიფიცირებული როგორც შემთხვევითი, ასევე გამიზნული სართხეების წარმოშობის წყაროები. საფრთხე შეიძლება წარმოიშვას როგორც ორგანიზაციის შიგნით, ასევე მის გარეთ. უნდა გაიმიჯნოს ზოგადი და ტიპიური საფრთხეები (მაგალითად: არაავტორიზებული ქმედება, ფიზიკური ზიანი, ტექნიკური ჩავარდნა) და შემდეგ განხორციელდეს ინდივიდუალური საფრთხეების მიკუთვნება გარკვეული სახეობების კლასისადმი. ეს გულისხმობს, რომ არც ერთი სართხე, მათ შორის მოულოდნელიც, არ რჩება გამოვლენისა და ამოცნობის გარეშე, მაგრამ ამასთან დაკავშირებული სამუშაოების მოცულობა შესაძლოა დაკავშრებული იყოს გარკვეულ შეზღუდვებთან.

ზოგიერთმა საფრთხემ შესაძლოა რამდენიმე აქტივზე იქონიოს გავლენა. ასეთ შემთხვევაში, მათი ზეგავლენა სხვადასხვანაირი იქნება აქტივიდან გამომდინარე.

საფრთხის იდენტიფიკაცია და მათი ხდომილების ალბათობის შეფასება (იხილეთ 8.2.2.3) შეიძლება მოვიპოვოთ აქტივების მფლობელების ან მომხმარებლებისაგან, მომსახურე პერსონალისგან, ინფრასტრუქტურის მართვაში ჩართული პერსონალისაგან და ინფორმაციული უსაფთხოების სპეციალისტებისგან, ფიზიკური უსაფრთხოების ექსპერტებისგან, იურიდიული დეპარტამენტისგან და სხვა ორგანიზაციებისგან, მათ შორის სამართალდამცავი ორგანოებისგან, ისევე როგორც ხელისუფლების, სადაზღვევო კომპანიებისა და ქვეყნის მმართველობისგან. საფრთხეზე რეაგირებისას აუცილებლად გათვალისწინებული უნდა იქნას გარემო და კულტურული ასპექტები.

მიმდინარე შეფასებებში აუცილებლად გათვალისწინებული უნდა იყოს შიდა ინციდენტების შესახებ არსებული გამოცდილება და ასევე წარსული საფრთხეების შეფასება. მნიშვნელოვანია

ასევე სხვა სახის საფრთხეების კატალოგების გათვალისწინება (მაგალითად კონკრეტული ორგანიზაციისა ან ბიზნესისთვის სპეციფიკური), რათა ხელთ გვქონდეს ძირითადი საფრთხეების სახეობების (ნომენკლატურის) სრულყოფილი სია საჭიროების შემთხვევაში. საფრთხეების კატალოგების და სტატისტიკის წყაროს შესაძლოა წარმოადგენდნენ დარგობრივი ორგანოები, მთავრობა, სამართალდამცავი ორგანოები, სადაზღევვო კომპანიები.

საფრთხეების კატალოგის ან წინა საფრთხის შეფასების შედეგების გამოყენების დროს აუცილებლად უნდა გავაცნობიეროთ: მნიშვნელოვანი საფრთხეები მუდმივად იცვლებიან, განსაკუთრებით იმ შემთხვევაში, როდესაც იცვლება ბიზნეს გარემო ან ინფორმაციული სისტემა.

დამატებითი ინფორმაცია საფრთხეების ტიპების შესახებ იხილეთ **დანართში გ**.

**შედეგები:** საფრთხეების ჩამონათვალი, მათი ტიპებისა და წარმოშობის წყაროების იდენტიფიცირებით.

### *8.2.1.4 არსებული კონტროლის მექანიზმების იდენტიფიკაცია*

**შემავალი რესურსები:** დოკუმენტაცია კონტროლის მექანიზმების და რისკების გადაჭრის გეგმის შესახებ.

**ქმედება:** უნდა განხორციელდეს არსებული და დაგეგმილი კონტროლის მექანიზმების იდენტიფიკაცია.

**სახელმძღვანელო მითითებები:** არსებული კონტროლის მექანიზმების იდენტიფიკაცია უნდა განხორციელდეს იმ მიზნით, რათა თავიდან იქნას აცილებული ზედმეტი უსარგებლო სამუშაო და ხარჯები, მაგალითად: კონტროლის მექანიზმის დუბლირება. დამატებით უნდა ითქვას, რომ არსებული კონტროლის მექანიზმების იდენტიფიცირებისას, შემოწმებამ უნდა უზრუნველყოს კონტროლის მექანიზმის ზუსტი (უშეცდომო) მუშაობა - არსებულმა იუმს-ის აუდიტის ანგარიშებმა უნდა შეამცირონ ამ დავალების შესრულებზე დახარჯული დრო. თუ კონტროლის მექანიზმი არ სრულდება მოლოდინის შესაბამისად, მაშინ მან შეიძლება გამოიწვიოს სუსტი წერტილები. მხედველობაში უნდა იქნას მიღებული ის სიტუაცია, როდესაც არჩეული კონტროლის მექანიზმი (ან სტრატეგია) განიცდის წარუმატებლობას ოპერაციისას და ამდენად საჭირო ხდება დამატებითი კონტროლის მექანიზმების გამოყენება იდენტიფიცირებულ რისკზე ეფექტური რეაგირებისათვის. იუმს-ში, მგს 27001:2011-ის (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები) თანახმად, იგი ეფუძვნება კონტროლის მექანიზმის ეფექტიანობის საზომს. კონტროლის მექანიზმის ეფექტის შეფასების გზა გახლავთ დავინახოთ თუ როგორ ამცირებს იგი საფრთხის ალბათობას, სუსტი წერტილებით სარგებლობის სიმარტივეს, ან ინციდენტის მიერ მოხდენილ უარყოფით გავლენას. არსებული კონტროლის მექანიზმები ეფექტიანობაზე

ინფორმაციას იძლევა ასევე ხელმძღვანელობის მიერ ჩატარებული განხილვა (ანალიზი, შეფასება) და აუდიტის ანგარიშები.

რისკების გადაჭრის გეგმის მიხედვით დასანერგი კონტროლის მექანიზმების დანერგვისას გათვალისწინებული უნდა იყოს უკვე დანერგილი კონტროლის მექანიზმების დანერგვის გამოცდილება.

არასებული ან დაგეგმილი კონტროლის მექანიზმი შესაძლოა მიჩნეული იყოს როგორც არაეფექტური, ან არასაკმარისი ან უსაფუძვლო. უსაფუძვლობის ან არასაკმარისობის შემთხვევაში უნდა შემოწმდეს კონტროლის მექანიზმი, რათა განისაზღვროს საჭიროა თუ არა მისი გაუქმება, შეცვლა სხვა მეტად შესაბამისი კონტროლის მექანიზმით, თუ უნდა დავტოვოთ არსებული კონტროლის მექანიზმი, მაგალითად ხარჯების თვალსაზრისით.

არსებული ან დაგეგმილი კონტროლის მექანიზმების იდენტიფიკაციის დამხამრე ქმედებებია:

- კონტროლის მექანიზმების შესახებ დოკუმენტაციის გადახედვა (მაგალითად, რისკებთან მობყროობის გეგმა). თუ ინფორმაციული უსაფრთხოების მართვის პროცესები მაღალ დონეზეა დოკუმენტირებული, მაშინ ყველა არსებული და დაგეგმილი კონტროლის მექანიზმი და მათი განხორციელების სტატუსი უნდა იყოს ხელმისაწვდომი;
- ინფორმაციულ უსაფრთხოებაზე პასუხისმგებელ პირებთან (მაგალითად, ინფორმაციული უსაფრთხოების ოფიცერი და ინფორმაციული სისტემის უსაფრთხოების ოფიცერი, შენობის კომენდანტი ან ოპერაციათა მენეჯერი) და მომხმარებლებთან გადამოწება იმისა, თუ რომელი კონტროლის მექანიზმი ხორციელდება რეალურად კონკრეტული ინფორმაციული პროცესებისა და ინფორმაციული სისტემებისთვის;
- ფიზიკური კონტროლის მექანიზმების ადგილზე დაკვირვება, შედარება უკვე განხორციელებული კონტროლის მექანიზმებისა და კონკრეტულად დასანერგი კონტროლის მექანიზმების სიისა, უკვე განხორციელებული კონტროლის მექანიზმების გადამოწმება იმ მიზნით, რამდენად სწორად და ეფექტიანად მუშაობენ, ან
- შიდა აუდიტის შედეგების მიმოხილვა.

**შედეგები:** ყველა არსებული და დაგეგმილი კონტროლის მექანიზმების ჩამონათვალი, მათი დანერგვისა და გამოყენების სტატუსი.

### *8.2.1.5 სუსტი წერტილების იდენტიფიცირება*

**შემავალი რესურსები:** ცნობილი საფრთხეების ჩამონათვალი, აქტივების ჩამონათვალი და არსებული კონტროლის მექანიზმები.

**ქმედება:** აუცილებელია სუსტი წერტილების იდენტიფიკაცია, რომელი სისუსტეებით სარგებლობაც წარმოადგენს საფრთხეს აქტივებისა ან ორგანიზაციასთვის (მგს 27001:2011 (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები), პუნქტი 4.2.1 დ) 3)).

**სახელმძღვანელო მითითებები:** სუსტი წერტილების გამოვლენა შესაძლებელია:

- ორგანიზაციაში;
- პროცესებსა და პროცედურებში;
- ხელმძღვანელობაში;
- პერსონალში;
- ფიზიკურ გარემოში;
- ინფორმაციული სისტემის კონფიგურაციაში;
- აპარატურაში, კომპიუტერულ პროგრამებში ან საკომუნიკაციო აღჭურვილობებში;
- მესამე მხარეებზე დამოკიდებულებაში.

თავისთავად სუსტი წერტილების არსებობა არ გულისხმობს ზიანის გამოწვევას, თუკი არ არსებობს საფრთხე, რომელიც ამ სუსტი წერტილებით ისარგებლებს. სუსტი წერტილი შესაბამისი საფრთხის არ არსებობის შემთხვევაში, არ საჭიროებს მასზე კონტროლის მექანიზმის განხორციელებას, მაგრამ უნდა იქნას გაცნობიერებული და ხდებოდეს მისი ცვლილებების მონიტორინგი. უნდა აღინიშნოს, რომ არაკორექტულად ან შეფერხებებით განხორციელებული კონტროლის მექანიზმი ან არაკორექტულად გამოყენებული კონტროლის მექანიზმი თავად შეიძლება აღმოჩნდეს სუსტი წერტილი. კონტროლის მექანიზმი შეიძლება იყოს ეფექტიანი ან არაეფექიანი, რაც დამოკიდებულია იმ გარემოზე, რომელშიც ის ფუნქციონირებს. მეორეს მხრივ, საფრთხე, რომელსაც არ გააჩნია შესაბამისი სუსტი წერტილი, არ იწვევს რისკს.

აქტივებს შესაძლოა ახასიათებდეს სუსტი წერტილები, რომლებიც გამოიყენება გარკვეულწილად, ან გარკვეული მიზნებისათვის (გარდა იმისა, რომ ვიცოდეთ თუ როდის იქნა შეძენილი და წარმოებული აქტივი). მხედველობაში უნდა იქნას მიღებული სუსტი წერტილების წარმოშობის სხვადასხვა წყარო, მაგალითად თვისობრივი და შემთხვევითი.

სუსტი წერტილების და მათი შეფასების მეთოდების შესახებ ნიმუშები იხილეთ **დანართში დ.**

**შედეგი:** აქტივებთან, საფრთხეებთან და კონტროლის მექანიზმებთან მიმართებაში არსებული სუსტი წერტილების ჩამონათვალი; სუსტი წერტილების ჩამონათვალი, რომლებიც არ არიან დაკავშირებული არცერთ იდენტიფიცირებულ საფრთხესთან და ამდენად, არ ექვემდებარებიან განხილვას.

### *8.2.1.6 უარყოფითი შედეგების იდენტიფიკაცია*

**შემავალი რესურსები:** აქტივების, ბიზნეს-პროცესების, საფრთხეების და სუსტი წერტილების ჩამონათვალი, საჭიროების შემთხვევაში მათი კავშირი აქტივებთან.

**ქმედება:** აუცილებლად უნდა მოხდეს უარყოფითი შედეგების იდენტიფიცირება, რამაც შეიძლება გამოიწვიოს აქტივების კონფიდენციალურიობის, მთლიანობის და ხელმისაწვდომობის დაკარგვა (იხილეთ მგს 27001:20011 (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები), 4.2.1 დ) 4)).

**სახელმძღვანელო მითითებები:** უარყოფითი შედეგი შეიძლება იყოს ეფექტიანობის არარსებობა, მავნე სამუშაო პირობები, ბიზნესის დაკარგვა, რეპუტაციის შელახვა, ზარალი და ასე შემდეგ.

აღნიშნული ქმედება განსაზღვრავს ორგანიზაციის ზიანს ან მისთვის უარყოფით შედეგებს, რაც შესაძლოა გამოწვეული იყოს ინციდენტის სცენარის შესაბამისად. ინციდენტის სცენარი არის საფრთხის მიერ სუსტი წერტილით ან სუსტი წერტილების ნაკრებით სარგებლობის აღწერა ინფორმაციული უსაფრთხოების ინციდენტის დროს (იხილეთ მგს 27002:2011 (ინფორმაციული ტექნოლოგია - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთხოების წესები და ნორმები), პუნქტი 13). გარემოს განსაზღვრის დროს დადგენილი გავლენის კრიტერიუმების გათვალისწინებით უნდა მოხდეს ინციდენტების სცენარების გავლენების განსაზღვრაც. მან შესაძლოა გავლენა იქონიოს ერთ ან მეტ აქტივზე ან მის ნაწილზე. თუმცაღა აქტივებს შესაძლოა დადგენილი ქონდეთ ფასეულობა როგორც ფინანსური თვალსაზრისით, ასევე ბიზნესისთვის უარყოფითი შედეგების კუთხით, თუკი მოხდება მათი დაზიანება ან საფრთხის ქვეშ დაყენება. უარყოფითი შედეგები შესაძლოა იყოს დროებითი ან პერმანენტული, მაგალითად, აქტივის განადგურება.

**შენიშვნა:** მგს 27001:2011 ინციდენტის სცენარის ხდომილებას აღწერს როგორც „უსაფრთხოების დარღვევას“.

ორგანიზაციამ უნდა მოახდინოს ინციდენტების სცენარების უარყოფითი ოპერაციული შედეგების იდენტიფიკაცია შემდეგი მიზნებისთვის:

- გამოძებისა და აღდგენის (გამოსწორების) დრო;
- (სამუშაო) დროის არასწორად გამოყენება;
- სახარბიელო სიტუაციის დაკარგვა;
- ჯანმრთელობა და უსაფრთხოება;
- ზარალის აღდგენისთვის საჭირო სპეციფიკური უნარ-ჩვევების გამოყენებისას ფინანსური დანახარჯები;
- რეპუტაცია.

დეტალები ტექნიკური სუსტი წერტილების შეფასების შესახებ იხილეთ **B.3 შეფასების გავლენა.**

**შედეგი:** ინციდენტების სცენარების ჩამონათვალი, მათი უარყოფითი შედეგებით აქტივებსა და ბიზნეს-პროცესებთან მიმართებაში.

### 8.2.2 რისკების მიახლოებითი შეფასება

#### *8.2.2.1 რისკების შეფასების მეთოდოლოგიები*

რისკის ანალიზი შესაძლოა ჩატარდეს დეტალურობის სხვადასხვა დონეზე, რაც დამოკიდებულია აქტივის კრიტიკულობაზე, ცნობილი სუსტი წერტილების ხარისხზე და ორგანიზაციაში არსებულ წინა ინციდენტებზე. შეფასების მეთოდოლოგია შეიძლება იყოს ხარისხობრივი ან რაოდენობრივი, ან ორივე ერთად გამომდინარე ვითარებიდან. როგორც პრაქტიკაშია მიღებული, თავდაპირველად გამოიყენება ხარისხობრივი შეფასება, რათა მოპოვებული იქნას რისკის დონის ზოგადი მახასიათებელი და გამოვლენილი იქნას ძირითადი რისკები. მოგვიანებით კი შესაძლოა ჩატარდეს უფრო სპეციფიკური ხასიათის ან რაოდენობრივი ანალიზი ძირითადი რისკებისა, რადგანაც რაოდენობრივი ანალიზის პროცესი ხასიათდება ნაკლები კომპლექსურობით და დანახარჯებით, ვიდრე ხარისხობრივისა.

ანალიზის ფორმა შეთავსებადი უნდა იყოს რისკების დონის დადგენის კრიტერიუმებთან, რომლებიც შემუშავებული იქნა როგორც ორგანიზაციული გარემოს ნაწილი.

შეფასების მეთოდოლოგიის შემდგომ დეტალებს განვიხილავთ ქვემოთ:

**(ა) ხარისხობრივი შეფასება:**
ხარისხობრივი შეფასება გამოიყენებს ხარისხობრივი ატრიბუტების შკალას, რათა აღწერილი იქნას პოტენციური უარყოფითი შედეგების მნიშვნელოვნება (მაგალითად, დაბალი, საშუალო და მაღალი) და ასევე ამ უარყოფითი შედეგების დადგომის ალბათობა. ხარისხობრივი შეფასების უპირატესობა არის მისი აღქმის სიმარტივე, მაშინ, როდესაც მისი უარყოფითი მხარე შკალის სუბიექტურ არჩევანში მდგომარეობს.

შეიძლება ამ შკალების ადაპტირება და მორგება გარკვეულ ვითარებებზე, ასევე სხვადასხვა რისკებისთვის სხვადასხვა აღწერილობების გამოყენება. ხარისხობრივი შეფასება შეიძლება გამოყენებული იქნას:

- როგორც საწყისი გადამოწმება რისკების იდენტიფიცირებისათვის, რაც მოითხოვს შემდგომ დეტალურ ანალიზს;
- იქ, სადაც ამგვარი ანალიზი მისაღებია გადაწყვეტილების მისაღებად;
- იქ, სადაც ციფრობრივი მონაცემები ან რესურსები არაადექვატურია რაოდენობრივი შეფასებისათვის.

ხარისხობრივი ანალიზი უნდა ტარდებოდეს ფაქტებზე დაყრდნობით და გამოიყენებდეს მოპოვებულ მონაცემებს.

**(ბ) რაოდენობრივი შეფასება:**

რაოდენობრივი შეფასებისას გამოიყენება ციფრული მნიშვნელობის შკალა სხვადასხვა წყაროების მონაცემებით (შედარებით ხარისხობრივ შეფასებასთან, სადაც გამოიყენება აღწერითი შკალა). ანალიზის ხარისხი დამოკიდებულია ციფრული მნიშვნელობის სიზუსტესა და სრულყოფილებაზე და გამოყენებული მოდელების სანდოობაზე. რაოდენობრივი შეფასება ხშირ შემთხვევაში გამოიყენებს წინა ინციდენტების მონაცემებს, რაც განაპირობებს იმ უპირატესობას, რომ იგი შესალოა დაკავშირებული იყოს პირდაპირ ინფორმაციული უსაფრთხოების მიზნებთან და ორგანიზაციისთვის პრობლემატურ საკითხებთან. უარყოფითი მხარე კი მდგომარეობს ახალი რისკების შესახებ მონაცემების სიმცირეში ან ინფორმაციული უსაფრთხოების სისუსტეში. რაოდენობრივი მიდგომის უარყოფითმა მხარემ შესაძლოა თავი იჩინოს იქ, სადაც ფაქტებით გამყარებული, შემოწმებადი მონაცემები არ არის ხელმისაწვდომი და ამდენად იქმნება რისკების შეფასების მნიშვნელობისა და სიზუსტის შესახებ მცდარი წარმოდგენა.

უარყოფითი შედეგები და ალბათობა, ასევე მათი გაერთიანება რისკის დონის გამოსავლენად შესაძლოა იცვლებოდეს რისკის ტიპის მიხედვით და ასევე იმ მიზნის შესაბამისად, რისთვისაც რისკების შეფასების შედეგი გამოიყენება. უარყოფითი შედეგებისა და ალბათობის ბუნდოვანება და ცვალებადობა გათვალისწინებული უნდა იყოს ანალიზისას და ინფორმაცია უნდა იცვლებოდეს ეფექტურად.

### *8.2.2.2 უარყოფითი შედეგების შეფასება*

**შემავალი რესურსები:** იდენტიფიცირებული მნიშვნელოვანი ინციდენტების სცენარების ჩამონათვალი, მათ შორის საფრთხეების, სუსტი წერტილების, გავლენის ქვეშ მყოფი აქტივების, აქტივებისა და ბიზნეს პროცესებისთვის უარყოფითი შედეგები.

**ქმედება:** ბიზნესის გავლენა ორგანიზაციაზე, რაც შეიძლება იყოს შესაძლო ან აქტუალური ინფორმაციული უსაფრთხოების ინციდენტის შედეგი, უნდა შეფასდეს და ამასთანავე გათვალისწინებული უნდა იყოს ინფორმაციული უსაფრთხოების დარღვევის უარყოფითი შედეგები, როგორებიცაა აქტივების კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის დაკარგვა (მგს 27001:2011 (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები), პუნქტი 4.2.1 ე) 1)).

<u>სახელმძღვანელო მითითებები:</u> დაკვირვების ქვეშ მყოფი აქტივების იდენტიფიკაციის შემდეგ, უარყოფითი შედეგების შეფასებისას გათვალისწინებული უნდა იყოს ამ აქტივების მნიშვნელობა და ფასეულობა. ბიზნესზე გავლენის მნიშვნელობა შეიძლება გამოიხატოს ხარისხობრივად ან რაოდენობრივად, მაგრამ მისთვის ფულადი ფასეულობის მინიჭების ნებისმიერმა მეთოდმა შესაძლოა უზრუნველყოს მეტი ინფორმაცია გადაწყვეტილების მიღებისთვის და ამდენად ხელი შეუწყოს გადაწყვეტილების მიღების კიდევ უფრო ეფექტურ პროცესს.

აქტივების ფასეულობის დადგენა იწყება აქტივების კლასიფიკაციით, გათვალისწინებული უნდა იყოს მათი კრიტიკულობაც, ასევე აქტივების მნიშვნელობა ორგანიზაციის ბიზნეს მიზნების შესრულების თვალსაზრისით. ფასეულობა დგინდება ორი საზომის გამოყენებით:

- აქტივის შეცვლის ღირებულება: ინფორმაციის აღდგენითი სამუშაოების და შეცვლის დანახარჯების დაფარვა (თუ საერთოდ შესაძლებელია), და
- ბიზნესის უარყოფითი შედეგები ან აქტივის საფრთხის ქვეშ დაყენება, როგორიცაა პოტენციური მავნე ბიზნეს და/ან იურიდიული ან მარეგულირებელი ხასიათის უარყოფითი შედეგები ინფორმაციის სააშკარაოზე გამოტანის, შეცვლის, ხელმიუწვდომლობის და/ან განადგურების შედეგად, და სხვა ინფორმაციული აქტივები.

ბიზნესზე გავლენის ანალიზი განსაზღვრავს ამგვარი ფასეულობის დადგენას. ღირებულება, რომელიც განსაზღვრულია ბიზნესისთვის უარყოფითი შედეგებით, ჩვეულებრივ მნიშვნელოვანწილად უფრო მაღალია ვიდრე უბრალოდ შეცვლის ღირებულება, რაც თავის მხრივ დამოკიდებულია ორგანიზაციისათვის აქტივის მნიშვნელობაზე საკუთარი ბიზნეს მიზნების მისაღწევად.

აქტივების ფასეულობის დადგენა წარმოადგენს ინციდენტების სცენარის გავლენის შეფასების ძირითად ფაქტორს, რადგანაც ინციდენტმა შესაძლოა გავლენა მოახდინოს ერთ ან რამდენიმე აქტივზე (მაგალითად, დამოკიდებული აქტივები), ან აქტივის მხოლოდ ნაწილზე. სხვადასხვა საფრთხეები და სუსტი წერტილები სხვადასხვა გავლენას ახდენენ აქტივებზე, მაგალითად: კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის დაკარგვა. უარყოფითი შედეგების შეფასება ამგვარად დაკავშირებულია აქტივების ფასეულობის დადგენასთან, რაც თავის მხრივ ეფუძნება ბიზნესზე გავლენის ანალიზს.

უარყოფითი შედეგები ან ბიზნესზე გავლენა შეიძლება განპირობებული იყოს შემთხვევის ან შემთხვევების შედეგების მოდელირებით, ან ექსპერიმენტული ან წარსული მონაცემების ექსტრაპოლაციის მეშვეობით.

უარყოფითი შედეგები შეიძლება გამოიხატოს ფულადი, ტექნიკური ან ადამიანური (სოციალური) გავლენის კრიტერიუმებით, ან სხვა ორგანიზაციისათვის მნიშვნელოვანი კრიტერიუმებით. ზოგიერთ შემთხვევაში ერთზე მეტი ციფრული საზომია საჭირო შედეგების განსასაზღვრად სხვადასხვა დროის, ადგილის, ჯგუფისა ან სიტუაციისათვის.

დროული და ფინანსური ხასიათის უარყოფითი შედეგები უნდა იზომებოდეს ერთნაირი მიდგომით, რაც გამოიყენება ასევე საფრთხის ალაბთობისა და სუსტი წერტილის შემთხვევაში. თანმიმდევრულობა (ლოგიკურობა) შენარჩუნებული უნდა იყოს რაოდენობრივი ან ხარისხობრივი მიდგომით.

დამატებითი ინფორმაცია აქტივების ფასეულობის დადგენისა და გავლენის შეფასების თაობაზე იხილეთ **დანართში ბ**.

**შედეგი:** ინციდენტების სცენარების შეფასებული უარყოფითი შედეგების ჩამონათვალი, დაკავშირებული აქტივებთან და გავლენის კრიტერიუმებთან.

### *8.2.2.3 ინციდენტის ალბათობის შეფასება*

**შემავალი რესურსები:** იდენტიფიცირებული, მნიშვნელოვანი ინციდენტების სცენარების ჩამონათვალი, მათ შორის საფრთხეების, გავლენის ქვეშ მყოფი აქტივების, გამოყენებული სუსტი წერტილების, აქტივების და ბიზნეს-პროცესებისთვის უარყოფითი შედეგების იდენტიფიკაცია. ასევე, ყველა არსებული ან დაგეგმილი კონტროლის მექანიზმების, მათი ეფექტიანობისა, დანერგვისა და გამოყენების სტატუსების ჩამონათვალი.

**ქმედება:** უნდა შეფასდეს ინციდენტის სცენარების ალბათობა (მგს 27001:2011 (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები), პუნქტი 4.2.1 ე) 2)).

**სახელმძღვანელო მითითებები:** ინციდენტის სცენარის იდენტიფიკაციის შემდეგ, აუცილებელია შეფასდეს ყოველი სცენარის ალაბთობა და გავლენა, რის დროსაც გამოყენებული უნდა იყოს როგორც ხარისხობრივი ასევე რაოდენობრივი შეფასების ტექნიკა. ასევე გათვალისწინებული უნდა იყოს თუ რამდენად ხშირად იჩენს თავს საფრთხე და რამდენად მარტივია სუსტი წერტილებით სარგებლობა, ასევე მხედველობაშია მისაღები:

- საფრთხის სტატისტიკა და ალბათობა;
- განზრახ წარმოშობილი საფრთხის წყაროებისთვის: მოტივაცია და შესაძლებლობა, რაც დროთა განმავლობაში იცვლება და ასევე შესაძლო თავდამსხმელების ხელთ არსებული რესურსები, ისევე როგორც აქტივების მნიშვნელოვნების მიმზიდველობისა და სუსტი წერტილების აღქმა შესაძლო თავდამსხმელის მიერ;
- შემთხვევითი საფრთხის წყროებისთვის: გეოგრაფიული ფაქტორები, მაგალითად ქიმიურ ან ნავთობ ქარხნებთან სიახლოვე, ექსტრემალური მეტეოროლოგიური პირობების შესაძლებლობა, და ფაქტორები, რომლებმაც შესაძლოა გავლენა იქონიონ ადამიანურ შეცდომებსა და დანადგარების შეფერხებით ფუნქციონირებაზე;

- სუსტი წერტილები, როგორც ინდივიდუალური ასევე მათი ერთობლიობა;
- არსებული კონტროლის მექანიზმები და მათი ეფექტურობა სისუსტეების შემცირების თვალსაზრისით.

მაგალითად, ინფორმაციულ სისტემას შესაძლოა გააჩნდეს მომხმარებლის იდენტიფიკაციის შენიღბვის საფრთხის შემცველი სისუსტეები და რესურსების ბოროტად გამოყენების შესაძლებლობა. რესურსების ბოროტად გამოყენების ალბათობა არის დაბალი მნიშვნელობის, მიუხედავად მომხმარებლის აუტენტიფიკაციის არარსებობისა, რადგანაც რესურსების ბოროტად გამოყენების შესაძლებლობები შეზღუდულია.

სიზუსტის აუცილებლობიდან გამომდინარე, აქტივები შეიძლება დაჯგუფდეს, ან დაიყოს შემადგენელ ელემენტებად და სცენარები დაკავშირებული იყოს ამ ელემენტებთან. მაგალითად, გეოგრაფიული მდებარეობების მიხედვით, ერთი და იმავე ტიპის აქტივებისთვის შეიძლება არსებობდეს ცვალებადი საფრთხეები, ასევე ცვალებადია არსებული კონტროლის მექანიზმების ეფექტიანობა ასეთ სიტუაციაში.

**შედეგი:** ინციდენტების სცენარების ალბათობა (ხარისხობრივი ან რაოდენობრივი).

### *8.2.2.4 რისკების მიახლოებითი შეფასება*

**შემავალი რესურსები:** ინციდენტების სცენარების ჩამონათვალი მათი უარყოფითი შედეგებით აქტივებისა და ბიზნეს-პროცესებისთვის და ასევე მათი ალბათობა (რაოდენობრივი ან ხარისხობრივი).

**ქმედება:** ყველა მნიშვნელოვანი ინციდენტის სცენარისთვის შეფასებული უნდა იყოს რისკის დონე (მგს 27001:2011 (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები), პუნქტი 4.2.1 ე) 4))

**სახელმძღვანელო მითითებები:** რისკების მიახლოებითი შეფასება განაპირობებს რისკის ალბათობისა და მისი უარყოფითი შედეგების მნიშვნელობას. ეს მნიშვნელობა შეიძლება იყოს რაოდენობრივი ან ხარისხობრივი. რისკების მიახლოებითი შეფასება აერთიანებს და ეყრდნობა ალბათობასა და უარყოფით შედეგებს. დამატებით, იგი შეიძლება ითვალისწინებდეს ასევე გამართლებულ დანახარჯებს, დაინტერესებული პირების პრობლემებს, და სხვა ცვლადებს, რაც რისკების შეფასებითვის აუცილებელია. მიახლოებით შეფასებული რისკი წარმოადგენს ინციდენტის სცენარის და მისი უარყოფითი შედეგების ალბათობის კომბინაციას.

ინფორმაციული უსაფრთხოების რისკების შეფასების სხვადასხვა მეთოდების ან მიდგომების ნიმუშები იხილეთ **დანართში ე.**

**შედეგი:** რისკების ჩამონათვალი, მიკუთვნებული მნიშვნელობების დონეებით.

## 8.3 რისკების დონის დადგენა

**შემავალი რესურსები:** რისკების ჩამონათვალი, განსაზღვრული ფასეულობების დონეებით და რისკების შეფასების კრიტერიუმები.

**ქმედება:** რისკების დონე უნდა შედარდეს რისკების შეფასების და რისკებზე თანხმობის კრიტერიუმებთან (იხილეთ მგს 27001:2011 (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები), პუნქტი 4.2.1 ე) 4)).

**სახელმძღვანელო მითითებები:** რისკების დონის დადგენასთან და მის კრიტერიუმებთან დაკავშირებული გადაწყვეტილებები მიღებული უნდა იქნას ჯერ კიდევ გარემოს განსაზღვის დროს. ეს გადაწყვეტილებები და გარემო ხელხლა უნდა იქნას გადახედილი უფრო დეტალურად იმ შემთხვევაში, როდესაც კონკრეტული რისკის იდენტიფიკაცია უფრო მეტ ინფორმაციას იძლევა. რისკების დონის დასადგენად ორგანიზაციამ უნდა შეადაროს მიახლოებით შეფასებული რისკი (დანართში ე განხილული შერჩეული მეთოდებისა და მიდგომების გამოყენებით) რისკების დონის დადგენის კრიტერიუმებთან. გადაწყვეტილებების მისაღებად გამოყენებული რისკების დონის დადგენის კრიტერიუმები შეთავსებადი უნდა იყოს ინფორმაციული უსაფრთხოების რისკების მართვის შიდა და გარე გარემოსთან და უნდა ითვალისწინებდეს ორგანიზაციისა და დაინტერესებული პირების მიზნებს და ა.შ. რისკების დონის დადგენის დროს მიღებული გადაწყვეტილებები ძირითადად ეფუძნება რისკების მისაღებ დონეს. თუმცაღა, უარყოფითი შედეგები, ალბათობა და სანდოობის ხარისხი რისკების იდენტიფიკაციისა და ანალიზის დროს ასევე უნდა იქნას გათვალისწინებული. მრავალი დაბალი ან საშუალო დონის რისკების გაერთიანებამ შეიძლება გამოიწვიოს უფრო მაღალი დონის ყოვლისმომცველი რისკები და საჭირო ხდება მათზე შესაბამისი რეაგირება.

განხილული უნდა იქნას ასევე:

- *ინფორმაციული უსაფრთხოების მახასიათებლები:* თუ ორგანიზაციისთვის ერთი რომელიმე კრიტერიუმი არ არის მნიშვნელოვანი (მაგალითად: კონფიდენციალურობის დაკარგვა), მაშინ ყველა ამ კრიტერიუმის შემცველი რისკი უმნიშვნელოა
- *კონკრეტული აქტივის ან აქტივების ნაკრების მიერ უზრუნველყოფილი ბიზნეს-პროცესების ან ქმედებების მნიშვნელობა:* თუ პროცესი განისაზღვრა როგორც დაბალი მნიშვნელობის მქონე, მაშინ მასთან დაკავშირებულ რისკებსაც შესაბამისად ნაკლები ყურადღება მიექცევა, შედარებით მაღალი დონის გავლენის მქონე რისკებთან.

რისკების დონის დადგენა ითვალისწინებს რისკების ანალიზისას გამოვლენილ რისკებს, რათა მიღებული იქნას გადაწყვეტილებები სამომავლო ქმედებების განსახორციელებლად. გადაწყვეტილებები უნდა შეიცავდეს:

- უნდა განხორციელედეს თუ არა ქმედება;
- რისკების თავიდან აცილების პრიორიტეტები რისკების დადგენილი დონეების გათვალისწნებით.

რისკების დონის დადგენის ეტაპზე ხელშეკრულებით გათვალისწინებული, იურიდიული და მარეგულირებელი მოთხოვნები არის ის ფაქტორები, რომლებიც მხედველობაში უნდა იქნას მიღებული მიახლოებით შეფასებულ რისკებთან ერთად.

**შედეგი:** პრიორიტეტებად დალაგებული რისკების ჩამონათვალი (რისკების დონის დადგენის კრიტერიუმების თანახმად), რომელიც დაკავშირებულია ამ რისკების გამომწვევ ინციდენტრების სცენარებთან.

# 9 ინფორმაციული უსაფრთხოების რისკებთან მობყობა

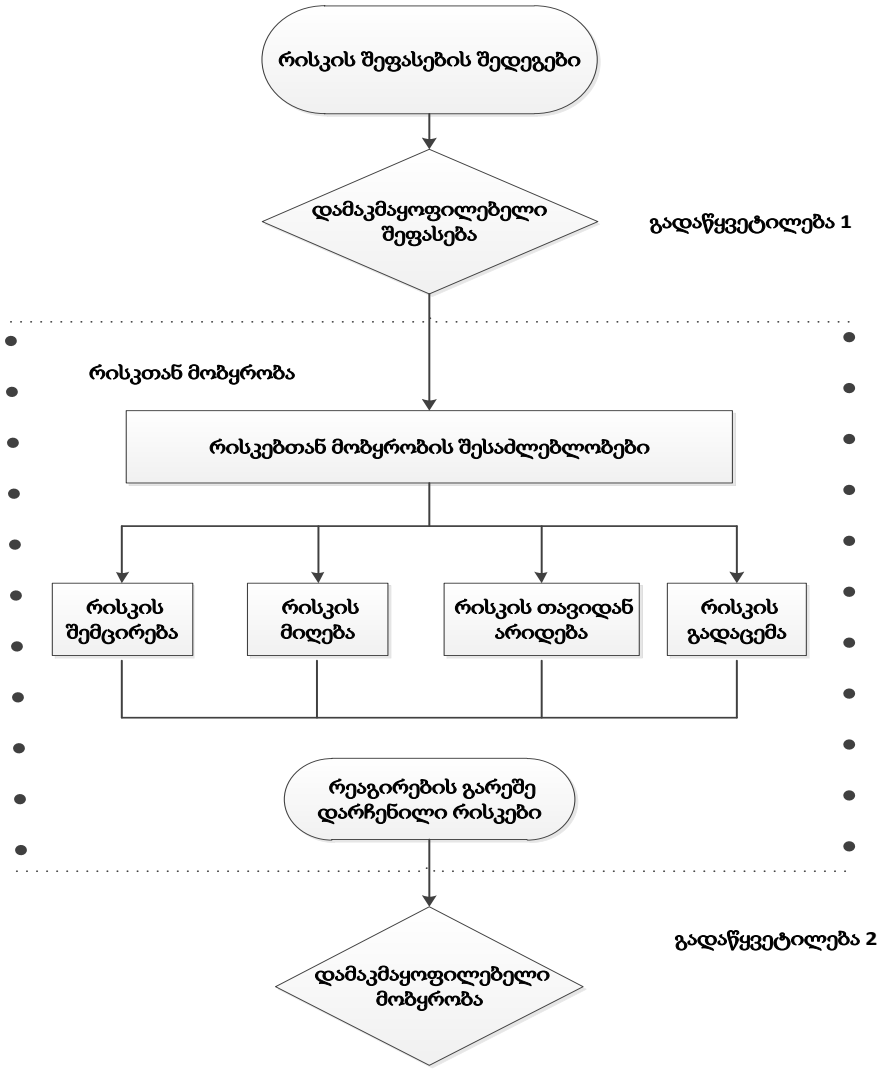
## 9.1 რისკებთან მობყრობის ზოგადი აღწერა

**შემავალი რესურსები:** პრიორიტეტებად დალაგებული რისკების ჩამონათვალი (რისკების დონის დადგენის კრიტერიუმების თანახმად), რომელიც დაკავშირებულია ამ რისკების გამომწვევ ინციდენტრების სცენარებთან.

**ქმედება:** შერჩეული უნდა იქნას რისკების შემცირების, მიღების , თავიდან არიდების ან გადაცემის კონტროლის მექანიზმები და უნდა განისაზღვროს რისკებთან მობყრობის გეგმა.

**სახელმძღვანელო მითითებები:** არსებობს რისკებთან მობყრობის ოთხი შესაძლებლობა: რისკის შემცირება (9.2), რისკის მიღება (9.3), რისკის თავიდან არიდება (9.4) და რისკის გადაცემა (9.5).

**შენიშვნა:** მგს 27001:2011 4.2.1. ვ) 2) გამოიყენებს ტერმინს „რისკის მიღება“ ნაცვლად ტერმინისა „რისკის დაშვება“.




**ნახაზი 2** გვიჩვენებს რისკებთან მობყრობის ქმედებას ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის ფარგლებში, რაც წარმოდგენილია **ნახაზზე 1.**

**ნახაზი 2 - რისკებთან მობყრობის ქმედება**

რისკებთან მობყორობის შესაძლებლობების არჩევა უნდა ეფუძნებოდეს რისკების შეფასების შედეგებს, ამ შესაძლებლობების განხორციელების მოსალოდნელ დანახარჯებს და მათგან მიღებულ შესაძლო მოგებებს.

თუკი რისკების დიდი რაოდენობით შემცირება შესაძლებელია შედარებით დაბალი დანახარჯებით, მაშინ ასეთი შესაძლებლობა უნდა იქნას გამოყენებული.

ზოგადად, რისკების არასასურველი შედეგები საკმაოდ უნდა შემცირდეს. მენეჯერებმა უნდა განიხილონ იშვიათი, მაგრამ ამვდროულად საკმაოდ მძიმე რისკები. ასეთ შემთხვევებში, ეკონომიკური თვალსაზრისით გაუმართლებელი კონტროლის მექანიზმები უნდა დაინერგოს (მაგალითად, ბიზნესის უწყვეტობის კონტროლი მაღალი დონის რისკების დასაფარად).

რისკებთან მობყრობის მოცემული ოთხი ვარიანტი არ არის ურთიერთგამომრიცხავი. ზოგიერთ შემთხვევაში ორგანიზაციამ შეიძლება მიმართოს ამ შესაძლებლობების კომბინაციებს, და ამგავარდ მოიპოვოს უპირატესობები, მაგალითად: რისკების ალბათობის შემცირება, მათი უარყოფითი შედეგების შემცირება, ნებისმიერი რეაგირების გარეშე დარჩენილი რისკის გადაცემა ან მიღება.

რისკებთან მობყრობის ზოგიერთმა შემთხვევამ შესაძლოა ეფექტიანი რეაგირება მოახდინოს ერთ ან რამდენიმე რისკზე (მაგალითად, ინფორმაციული უსაფრთხოების ტრენინგი და ინფორმირებულობა). რისკებთან მობყრობის გეგმამ უნდა განსაზღვროს ის პრიორიტეტულობა, რომლის მიხედვითაც უნდა განხორციელდეს ინდივიდუალურ რისკებთან მობყრობა და მათი ვადები. პრიორიტეტების დადგენა ხდება სხვადასხვა მექანიზმების, მათ შორის რისკების რანგირებისა და სარგებლიანობის ანალიზის მეშვეობით. ორგანიზაციის მენეჯერების პასუხისმგებლობაში შედის ურთიერთშესაბამისობაში მოიყვანონ კონტროლის მექანიზმების დანერგვის ხარჯები და ბიუჯეტი.

არსებული კონტროლის მექანიზმების იდენტიფიკაცია განსაზღვრავს, რომ არსებული კონტროლის მექანიზმები აჭარბებენ მიმდინარე დონეს, გამომდინარე ხარჯების შედარებიდან, მათ შორის ტექნიკური მხარდაჭერის ხარჯები. თუ დაიგეგმება ზედმეტი ან უსარგებლო კონტროლის მექანიზმების ამოგდება (განსაკუთრებით თუ ასეთი კონტროლის მექანიზმები იყოს მაღალი საექსპლუატაციო ხარჯებით), მაშინ გათვალისწინებული უნდა იქნას ინფორმაციული უსაფრთხოებისა და ხარჯების ფაქტორები. იმდენად, რამდენადაც კონტროლის მექანიზმები შესაძლოა ერთმანეთზე ახდენდნენ გავლენას, ზედმეტი კონტროლის მექანიზმების ამოდგებამ შეიძლება შეამციროს საერთო უსაფრთხოება. დამატებით უნდა აღინიშნოს, რომ ჭარბი კონტროლის მექანიზმების დატოვება შეიძლება უფრო იაფი იყოს ვიდრე მათი ამოგდება.
რისკებთან მოპყრობის შესაძლებლობების განხილვისას გათვალისიწნებული უნდა იქნას:

- თუ როგორ აღიქმება რისკი გავლენის ქვეშ მყოფი მხარეების მიერ;
- ამ მხარეებთან კომუნიკაციის ყველაზე მისაღები გზები.

გარემოს წინასწარი განსაზღვრა (7.2 - რისკების შეფასების კრიტერიუმები) უზრუნველყოფს ირუდიული და მარეგულირებელი მოთხოვნების შესახებ ინფორმაციას, რომელსაც უნდა აკმაყოფილებდეს ორგანიზაცია. ყველა პირობა - ორგანიზაციული, ტექნიკური, სტრუქტურული და ა.შ. - რომლებიც დადგინდა გარემოს განსაზღვრის დროს, აუცილებლად უნდა იქნას გათვალისწინებული რისკებთან მოპყრობისას.

რისკებთან მოპყრობის გეგმის შედგენის შემდეგ აუცილებლად უნდა განისაზღვროს რეაგირების გარეშე დარჩენილი რისკები. ეს პროცესი მოიცავს რისკების შეფასების განახლებასა და განმეორებად ციკლს, რომლის დროსაც მხედველობაში უნდა იქნას მიღებული შემოთავაზებული რისკებთან მობყრობით გამოწვეული მოსალოდნელი შედეგები. თუ რეაგირების გარეშე დარჩენილი რისკები ჯერ კიდევ არ პასუხობენ ორგანიზაციის მიერ განსაზღვრულ რისკების მიღების კრიტერიუმებს, მაშინ საჭირო ხდება რისკებთან მობყრობის ციკლის ხელახლა გაშვება მანამ, სანამ უზრუნველყოფილი აქ იქნება რისკის მიღება. დამატებითი ინფორმაციისთვის იხილეთ მგს 27002:2011 (ინფორმაციული ტექნოლოგია - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთხოების წესები და ნორმები), პუნქტი 0.3.

**შედეგი:** რისკებთან მობყრობის გეგმა და რეაგირების გარეშე დარჩენილი რისკები, რაც არის ორგანიზაციის მენეჯერების მხრიდან გადაწყვეტილების საგანი.

## 9.2 რისკების შემცირება

**ქმედება:** არჩეული კონტროლის მექანიზმების მეშვეობით უნდა შემცირდეს რისკის დონე იმგვარად, რომ შესაძლებელი გახდეს რეაგირების გარეშე დარჩენილი რისკის ხელახლა შეფასება მისი მიღების მიზნით.

**სახელმძღვანელო მითითება:** შერჩეული უნდა იყოს შესაბამისი კონტროლის მექანიზმები რისკების შეფასებისა და მათთან მობყრობის მოთხოვნების დასაკმაყოფილებლად. ასევე გათვალისწინებული უნდა იქნას როგორც რისკების მიღების კრიტერიუმები, ასევე იურიდიული, მარეგულირებელი და სახელშეკრულებო მოთხოვნები. მხედველობაში უნდა იქნას მიღებული კონტორლის მექანიზმების დანერგვის ხარჯები და ვადები, ტექნიკური, გარემოს და კულტურული ასპექტები. სწორად შერჩეულმა ინფორმაციული უსაფრთხოების კონტროლის მექანიზმებმა შესაძლებელია შეამციროს სისტემის მფლობელობის ხარჯები.

კონტროლის მექანიზმებმა ზოგადად შეიძლება უზრუნველყოს ერთი ან მეტი შემდეგი ტიპის დაცვის მექანიზმები: შესწორება, განადგურება, თავიდან არიდება, გავლენის შემცირება, აღმოჩენა, აღდგენა, მონიტორინგი და ინფორმირებულობა. კონტროლის მექანიზმის შერჩევისას მნიშვნელოვანია მათი შეძენის, დანერგვის, ადმინისტარციული, ოპერაციული, მონიტორინგისა და მხარდაჭერის ხარჯების შეფასება დასაცავი აქტივების ფასეულობასთან მიმართებაში. უფრო მეტიც, გათვალისწინებული უნდა იყოს რისკების შემცირების შედეგად მიღებული საინვესტიციო მოგებები და გარკვეული კონტროლის მექანიზმების მიერ ახალი ბიზნეს შესაძლებლობების პოტენციალი. ყურადღება უნდა გამახვილდეს სპეციალიზირებულ უნარ-ჩვევებზე, რაც აუცილებელია ახალი კონტროლის მექანიზმების განსაზღვრისა და დანერგვისათვის ან არსებული კონტროლის მექანიზმების შეცვლისთვის.
კონტროლების შესახებ დეტალურ ინფორმაციას იძლევა მგს 27002:2011.

არსებობს მრავალი პირობა, რამაც შესაძლოა გავლენა იქონიოს კონტროლის მექანიზმების შერჩევაზე. ტექნიკური ხასიათის შეზღუდვები, როგორებიცაა ფუნქციონირების მოთხოვნები, მართვადობა (ოპერაციული მხარდაჭერის მოთხოვნები) და თავსებადობის საკითხები, რომლებმაც შესაძლოა ხელი შეუშალონ კონკრეტული კონტროლის მექანიზმების გამოყენებას ან ბიძგი მისცენ ადმიანური ფაქტორით გამოწვეულ შეცდომას, რაც გამოიხატება როგორც კონტროლის მექანიზმის გაბათილებაში, უსაფრთხოების შესახებ მცდარი წარმოდგების შექმნაში, ასევე კონტროლის მექანიზმის არ ქონით რისკების გაზრდაში (მაგალითად: შესაბამისი ტრენინგის გარეშე მოითხოვო კომპლექსური პაროლები, რაც იძულებულს ხდის მომხმარებლებს ფურცელზე ჩაიწერონ პაროლები). ასევე შესაძლებელია, რომ კონტროლის მექანიზმმა გავლენა იქონიოს წარმადობაზე. მენეჯერებმა უნდა მიიღონ ისეთი გადაწყვეტილება, რომელიც დააკმაყოფილებს წარმადობის მოთხოვნებს და ამავდროულად უზრუნველყოფს ადექვატურ ინფორმაციულ უსაფრთხოებას. ამ ეტაპის შედეგი გახლავთ შესაძლო კონტროლის მექანიზმების ჩამონათვალი მათი დანახარჯების, სარგებელის და დანერგვის პრიორიტეტებთან ერთად.
კონტროლის მექანიზმების შერჩევისა და მათი დანერგვის დროს სხვადასხვა შეზღუდვები უნდა იქნას გათვალისწინებული. ტიპიურად:

- ვადები;
- ფინანსური შეზღუდვები;
- ტექნიკური შეზღუდვები;
- ოპერაციული;
- კულტურული;
- ეთიკური;
- გარემო პირობებისა;
- იურიდიული შეზღუდვები;
- ადვილად გამოყენებადი
- საკადრო შეზღუდვები;
- არსებული და ახალი კონტროლის მექანიზმების ინტეგრირების შეზღუდვები.

დამატებითი ინფორმაცია რისკების შემცირების შეზღუდვებთან დაკავშირებით იხილეთ **დანართში ვ.**

## 9.3 რისკების დაშვება

**ქმედება:** რისკის დაშვებისა და მასზე შემდგომი ქმედების განუხორციელებლობის შესახებ გადაწყვეტილება მიღებული უნდა იქნას რისკების დონის დადგენის საფუძველზე.

**სახელმძღვანელო მითითებები:** თუ რისკის დონე შეესაბამება რისკის მიღების კრიტერიუმებს, მაშინ არ არის აუცილებელი დამატებითი კონტროლის მექანიზმების დანერგვა და შესაძლებელია რისკის დაშვება (ანუ არ მოხდეს მასზე დამატებითი ქმედება).

## 9.4 რისკის თავიდან აცილება

**ქმედება:** ქმედება ან ვითარება, რომელიც განაპირობებს ცალკეული რისკების თავიდან აცილებას.

**სახელმძღვანელო მითითებები:** როდესაც იდენტიფიცირებული რისკები მიჩნეულია როგორც საკმაოდ მაღალი დონის, ან რისკებთან მოპყრობის სხვა ვარიანტების განხორციელების ხარჯები მეტია სარგებელზე, შესაძლოა აუცილებელი გახდეს გადაწყვეტილების მიღება რისკების მთლიანად აღმოფხვრის თაობაზე, რისთვისაც საჭიროა დაგეგმილი ან არსებული ქმედების ან ქმედებათა ნაკრების შეწყვეტა, ან იმ პირობების შეცვლა, რომლებშიც აღნიშნული ქმედების განხორციელება ხდება. მაგალითად, ბუნებრივი მოვლენებით გამოწვეული რისკების შემთხვევაში უფრო მისაღებია, ხარჯების დაზოგვის თვალსაზრისით, ინფორმაციის დამამუშავებელი მოწყობილობების ფიზიკური გადაადგილება უსაფრთხო ან კონტროლირებად ადგილას.

## 9.5 რისკების გადაცემა

**ქმედება:** რისკი უნდა გადაეცეს სხვა მხარეს, რომელიც უფრო ეფექტიანად განახორციელებს მის მართვას რისკის დონის დადგენის საფუძველზე.

**სახელმძღვანელო მითითებები:** რისკის გადაცემა გულისხმობს გადაწყვეტილებას ცალკეული რისკის გარე მხარისათვის გაზიარების შესახებ. რისკის გადაცემამ შეიძლება შექმნას ახალი რისკები ან გამოიწვიოს არსებულის, უკვე აღმოჩენილის შეცვლა. ამდენად აუცილებელი ხდება დამატებითი რისკის აღმოფხვრა.

რისკების გადაცემა შეიძლება განხორციელდეს დაზღვევის მეშვეობით, რაც მოიცავს უარყოფითი შედეგების დადგომი შემთხვევაში დახმარებას, ან ქვე-კონტრაქტორი პარტნიორის მეშვეობით, რომელიც ახორციელებს ინფორმაციული სისტემის მონიტორინგს და მიმართავს სასწრაფო ზომებს თავდასხმის შესაჩერებლად მანამ, სანამ იგი გამოიწვევს გარკვეული დონის ზარალს.

აღსანიშნავია, რომ შესაძლებელია პასუხისმგებლობების გადაცემა რისკის მართვის მიზნით, მაგრამ შეუძლებელია მოსალოდნელი ზეგავლენით გამოწვეული ვალდებულებების გადაცემა. მომხმარებლები, როგორც წესი, უარყოფით გავლენას მიაწერენ ორგანიზაციის შეცდომას.

# 10 ინფორმაციული უსაფრთხოების რისკების მიღება

**შემავალი რესურსები:** რისკებთან მობყრობის გეგმა და რეაგირების გარეშე დარჩენილი რისკები, რაც არის ორგანიზაციის მენეჯერების მხრიდან გადაწყვეტილების მიღების საგანი.

**ქმედება:** რისკების მიღების შესახებ გადაწყვეტილება და ამ გადაწყვეტილებაზე პასუხისმგებლობები უნდა დარეგისტრირდეს ოფიციალურად (დაკავშირებულია მგს 27001:2011 (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები), პარაგრაფი 4.2.1 თ)).

**სახელმძღვანელო მითითებები:** რისკებთან მობყრობის გეგმა აღწერს თუ როგორ უნდა მოვებყროთ რისკებს, რათა დაკმაყოფილებული იყოს რისკების მიღების კრიტერიუმები (იხილეთ პუნქტი 7.2 რისკების მიღების კრიტერიუმები). პასუხისმგებელმა მენეჯერებმა უნდა გადახედონ და დაამტკიცონ შემოთავაზებული რისკებთან მობყრობის გეგმები და რეაგირების გარეშე დარჩენილი რისკები, შესაბამისად დაარეგისტრირონ დამტკიცებასთან დაკავშირებული ნებისმიერი პირობები.

რისკების მიღების კრიტერიუმები არ არის მხოლოდ იმ ფაქტის განსაზღვრა, კონკრეტული რისკი ზღვარს ქვემოთ იმყოფება თუ ზემოთ, იგი უფრო კომპლექსური ხასიათისაა.

ზოგიერთ შემთხვევაში კონკრეტული რისკის დონე შეიძლება არ აკმაყოფილებდეს რისკების მიღების კრიტერიუმებს, რადგან გამოყენებული კრიტერიუმები არ ითვალისწინებენ გავრცელებულ მიდგომებს. მაგალითად, შესაძლოა ამტკიცებდნენ, რომ საჭიროა რისკების მიღება მისი თანმდევი მიმზიდველი სარგებელის გამო, ან რისკების შემცირების მაღალი ხარჯების გამო. ამგავრი ვითარებები მიუთითებენ, რომ რისკების მიღების კრიტერიუმები არაადექვატურია და შეძლებისდაგვარად უნდა იქნას გამოსწორებული. თუმცა, ყოველთვის არ არის შესაძლებელი რისკების მიღების კრიტერიუმების დროული შესწორება. ასეთ შემთხვევაში, გადაწყვეტილების მიმღები პირები იძლებულნი არიან თანხმობა განაცხადონ ისეთ რისკებზე, რომლებიც არ აკმაყოფილებენ მიღების სტანდარტულ კრიტერიუმებს. თუ ეს აუცილებელია, გადაწყევტილების მიმღებმა პირმა დეტალური კომენტარი უნდა გაუწეროს რისკს და თან დაურთოს მიღებული გადაწყვეტილების არგუმენტირება, თუ რატომ მოხდა რისკების მიღების სტანდარტული კრიტერიუმების უგულვებელყოფა.

**შედეგები:** თანხმობა მიღებული რისკების ჩამონათვალზე, მათ შორის არგუმენტაცია ისეთ რისკებზე, რომლებიც არ აკმაყოფილებენ ორგანიზაციის რისკების მიღების სტანდარტულ კრიტერიუმებს.

## 11 ინფორმაციული უსაფრთხოების რისკების შესახებ ინფორმირებულობა

**შემავალი რესურსები:** რისკების მართვის შედეგად მიღებული ყველანაირი ინფორმაცია რისკების შესახებ (იხილეთ ნახაზი 1).

**ქმედება:** რისკების შესახებ ინფორმაცია უნდა იყოს გაცვლილი ან ზიარი გადაწყვეტილების მიმღებ და სხვა დაინტერესებულ პირებს შორის.

**სახელმძღვანელო მითითებები:** რისკების შესახებ ინფორმირება წარმოადგენს შეთანხმების მიღწევას იმის თაობაზე, თუ როგორ უნდა მოხდეს რისკების მართვა რისკების შესახებ ინფორმაციის გაცვლისა და გაზიარების მეშვეობით გადაწყვეტილების მიმღებ და სხვა დაინტერესებულ პირებს შორის. ინფორმაცია შეიცავს რისკების არსებობას, რისკის შინაარს, ფორმას, ალბათობას, სირთულეს, დამუშავებას და მასზე თანხმობადობას, ასევე სხვა ფაქტორებსაც.

დაინტერესებულ პირებს შორის ეფექტური კომუნიკაცია მნიშვნელოვანია იმ თვალსაზრისით, რომ ამან შეიძლება მნიშვნელოვანი გავლენა იქონიოს მისაღებ გადაწყვეტილებებზე. კომუნიკაციამ უნდა უზრუნველყოს ის, რომ რისკების მართვის განხორციელებაზე პასუხისმეგებელ პირებს და დაინტერესებულ პირებს ესმოდეთ გადაწყვეტილებების მიღების საფუძველი და კონკრეტული ქმედებების საჭიროება. კომუნიკაცია არის ორმიმართულებიანი.

რისკის აღქმა იცვლება დაინტერესებული პირების საჭიროებების, პრობლემატური საკითხების, კონცეფციების სხვადასხვაგვარობის მიხედვით, რადგანაც დაკავშრებული არიან რისკებთან ან განსახილველ საკითხებთან. დაინტერესებული პირები სავარაუდოდ გამოთქვამენ მოსაზრებებს რისკების მიღების შესახებ, რაც დაფუძნებული იქნება მათ მიერ რისკის აღქმაზე. განსაკუთრებით მნიშვნელოვანია დაინტერესებული პირების მიერ რისკების აღქმა და ამ აღქმისგან მიღებული სარგებელი იყოს აღმოჩენილი და დოკუმენტირებული და ასევე ძირითადი მიზეზები ნათლად გასაგები და რეაგირებული.

რისკების კომუნიკაცია უნდა განხორციელდეს რათა მიღწეული იქნას შემდეგი:

- ორგანიზაციის რისკების მართვის შედეგების გარანტიების უზრუნველყოფა;
- რისკების შესახებ ინფორმაციის შეგროვება;
- რისკების შეფასების შედეგების გაზიარება და რისკებთან მობრყობის გეგმის წარმოდგენა;
- ინფორმაციული უსაფრთხოების დარღვევის ხდომილებისა და მისი უარყოფითი შედეგების თავიდან აცილება და შემცირება, რაც შესაძლოა გამოწვეული იყოს გადაწყვეტილების მიმღებ და დაინეტრესებულ პირებს შორის საერთო შეხედულებების არ არსებობის გამო;
- გადაწყვეტილების მიღების მხარდაჭერა;
- ინფორმაციული უსაფრთხოების შესახებ ახალი ცოდნის მიღება;
- სხვა მხარეებთან კოორდინაცია და ინციდენტების უარყოფითი შედეგების შემცირების მიზნით საპასუხო ქმედებების დაგეგმვა;
- გადაწყვეტილების მიმღები და დაინტერესებული პირებისთვის პასუხისმგებლობის გაცნობიერება რისკების დადგომის შემთხვევაში;
- ინფორმირებულობის გაუმჯობესება.

ორგანიზაციამ უნდა შეიმუშაოს რისკების შესახებ ინფორმირების გეგმები როგორც სტანდარტული ოპერაციების, ასევე განსაკუთრებული ვითარებებისთვის. ამდენად, რისკების შესახებ ინფორმირება უწყვეტი პროცესია.

გადაწყვეტილების მთავარ მიმღებ და დაინტერესებულ პირებს შორის კოორდინაცია მიღწეული უნდა იქნას შესაბამისი კომიტეტის შექმნით, სადაც განიხილება რისკების, მათი პრიორიტეტების და შესაბამისი მობყრობის, რისკების მიღების შესახებ.

მნიშვნელოვანია თანამშრომლობა ორგანიზაციის ისეთ სტრუქტურულ ერთეულებთან, როგორებიცაა, მაგალითად, საზოგადოებასთან ურთიერთობის ან ინფორმირებულობის სამსახური, რათა უზრუნველყოფილი იყოს რისკების ინფორმირებულობასთან დაკავშირებული ყველა ამოცანის კოორდინაცია.

**შედეგი:** ორგანიზაციის ინფორმაციული უსაფრთხოების რისკების მართვის პორცესის გაგება და მისი შედეგები.

## 12. ინფორმაციული უსაფრთხოების რისკების მონიტორინგი და მიმოხილვა

### 12.1. რისკ ფაქტორების მონიტორინგი და მიმოხლივა

**შემავალი რესურსი:** რისკების მართვის შედეგად მიღებული ყველა ინფორმაცია რისკების შესახებ (ნახაზი 1).

**ქმედება:** უნდა განხორციელდეს მონიტორინგი რისკებსა და მათ ფაქტორებზე (მაგალითად: აქტივების ფასეულობა, გავლენა, საფრთხეები, სუსტი წერტილები, ხდომილების ალბათობა) და უნდა მოხდეს მათი განხილვა, რათა ადრეულ ეტაპზევე აღმოჩენილი და იდენტიფიცირებული იყოს ორგანიზაციაში განხორციელებული ნებისმიერი ცვლილება, ასევე მოხდეს რისკების კომპლექსური სურათის განხილვა.

**სახელმძღვანელო მითითებები:** რისკები არ არის უცვლელი. საფრთხეები, სუსტი წერტილები, ალბათობა ან უარყოფითი შედეგები შეიძლება შეიცვალოს მოულოდნელად, წინასწარი მინიშნების გარეშე. ამდენად საჭიროა მუდმივი მონიტორინგი ამ ცვლილებების აღმოსაჩენად. ეს შეიძლება განხორციელდეს გარე სერვისების მიერ, ინფორმაცია ახალი საფრთხეებისა და სუსტი წერტილების შესახებ შესაძლოა მივიღოთ მესამე მხარეს მიერ.

ორგანიზაციამ უნდა უზრუნველყოს შემდეგი ფაქტორების უწყვეტი მონიტორინგი:

- რისკების მართვის ჩარჩოში დამატებული ახალი აქტივები;

- აქტივების ფასეულობის საჭირო ცვლილება, მაგალითად რომელიც შეიცვალა ბიზნეს მოთხოვნების შედეგად;
- შეუფასებელი, აქტიური საფრთხეები როგორც ორგანიზაციის შეგნით ასევე მის გარეთ;
- სისუსტეებით სარგებლობის გაზრდა შესაძლოა გამოწვეული იყოს როგორც ახალი ისე არსებული სისუსტეების ხარისხის მატებით;
- აღმოჩენილი სუსტი წერტილების მიერ გამოყენებადი სუსტი წერტილების განსაზღვრა, რომლებიც შეიძლება გამოყენებული იქნან ახალი ან ხელახლა გაჩენილი საფრთხეების მიერ;
- შეფასებული საფრთხეების, სუსტი წერტილების და რისკების მომატებული (გაზრდილი) გავლენა ან მისი უარყოფითი შედეგები მთლიანად, რაც იწვევს რისკის დაუშვებელ დონეს;
- ინფორმაციული უსაფრთხოების ინციდენტები.

ახალმა საფრთხეებმა, სუსტმა წერტილებმა ან ცვლილებებმა შესაძლოა გაზარდოს წარსულში დაბალ რისკად შეფასებული რისკების რაოდენობა. თუ რისკები არ იყოფა დაბალ ან დასაშვებ კატეგორიებად, მაშინ მათთან მობყრობა უნდა მოხდეს 9-ე პუნქტში განხილული ერთი ან მეტი ვარიანტების გამოყენებით.

ფაქტორები, რომლებიც გავლენას ახდენენ საფრთხეების ალბათობასა და მათ უარყოფით შედეგებზე, შეიძლება შეიცვალოს, ისევე როგორც ის ფაქტორები, რომლებიც გავლენას ახდენენ რისკებთან მობყრობის სხვადასხვა ვარიანტების შესაბამისობასა და ღირებულებაზე. ძირითადი ცვლილებები, რომლებიც გავლენას ახდენენ ორგანიზაციაზე, აუცილებლად უნდა იქნას განხილული. რისკების მონიტორინგი რეგულარულად უნდა მეორდებოდეს და რისკებთან მობყრობის შერჩეული ვარიანტები პერიოდულად უნდა გადაიხედოს.

რისკის მონიტორინგის შედეგი შესაძლოა წარმოადგენდეს შემავალ რესურსს  სხვა რისკის განხილვისთვის. ორგანიზაციამ რეგულარულად უნდა მიმოიხილოს ყველა რისკი და ასევე თუ როდის იჩენს თავს ძირითადი მნიშვნელოვანი ცვლილებები (თანახმად მგს 27001:2011 (ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთოების მართვის სისტემები - მოთხოვნები), პუნქტი 4.2.3)).

**შედეგი:** რისკების მართვის უწყვეტი თანხვედრა ორგანიზაციის ბიზნეს მიზნებთან, ასევე რისკების მიღების კრიტერიუმებთან.

## 12.2 რისკების მართვის მონიტორინგი, განხილვა და გაუმჯობესება

**შემავალი რესურსი:** რისკების მართვის შედეგად მიღებული ყველა ინფორმაცია რისკების შესახებ (ნახაზი 1).

**ქმედება:** ინფორმაციული უსაფრთხოების რისკების მართვის პროცესზე უნდა ხორციელდებოდეს მუდმივი მონიტორინგი, ხდებოდეს მისი მიმოხილვა და აუცილებლობის შემთხვევაში მისი გაუმჯობესება.

**სახელმძღვანელო მითითებები:** მუდმივი მონიტორინგი და მიმოხილვა აუცილებელია, რათა უზრუნველყოფილი იქნას გარემოს, რისკების შეფასების შედეგების და რისკებთან მობყრობის, ასევე მართვის გეგმის აუცილებლობის შენარჩუნება ვითარებების შესაბამისად.

ორგანიზაციამ უნდა უზრუნველყოს ინფორმაციული უსაფრთხოების რისკების მართვის პროცესისა და მასთან დაკავშირებული ქმედებების შესატყვისობა მოცემულ მომენტში არსებულ ვითარებებთან. ნებისმიერი პროცესისა თუ ქმედებების შეთანხმებული გაუმჯობესების შესახებ უნდა ეცნობოს შესაბამის მენეჯერებს, რათა უზრუნველყოფილი იქნას რისკების ან რისკების ელემენტების აღმოჩენა, მათი სათანადოდ შეფასება და ასევე გატარებული იქნას საჭირო ღონისძიებები და მიღებული იქნას შესაბამისი გადაწყვეტილებები რისკების რეალისტურ აღქმაზე, გაცნობიერებაზე და მათზე რეაგირების მოხდენაზე.

დამატებით უნდა აღინიშნოს, რომ ორგანიზაციამ რეგულარულად უნდა აკონტროლოს რისკებისა და მისი ელემენტების საზომი კრიტერიუმების აქტუალურობა ბიზნეს მიზნებთან, სტრატეგიებთან და პოლიტიკებთან მიმართებაში, ასევე ადექვატურად გათვალისწინებული უნდა იყოს ბიზნესის გარემოს ცვლილებები ინფორმაციული უსაფრთხოების რისკების მართვის პროცესში. მონიტორინგი და მიმოხილვა უნდა ეხებოდეს:

- იურიდიულ და გარემოებრივ პირობებს;
- კონკურენტულ გარემოს;
- რისკების შეფასებებისადმი მიდგომას;
- აქტივების ფასეულობას და კატეგორიებს;
- გავლენის კრიტერიუმებს;
- რისკების დონის დადგენის კრიტერიუმებს;
- რისკების მიღების კრიტერიუმებს;
- მფლობელობის ხარჯებს;
- საჭირო რესურსებს.

ორგანიზაციამ უნდა უზრუნველყოს, რომ რისკების შეფასების და რისკებთან მობყრობის რესურსები მუდმივად ხელმისაწვდომია რისკების გადახედვის, ახალი ან სახეცვლილი საფრთხეებისა ან სუსტი წერტილების რეაგირებისთვის, და ასევე მენეჯმენტისთვის რჩევის მიცემა.

რისკების მართვის მონიტორინგმა შესაძლოა გამოიწვიოს გამოყენებული ხელსაწყოების, მეთოდოლოგიის ან მოწყობილობების შეცვლა ან დამატება, რაც დამოკიდებულია:

- აღმოჩენილ ცვლილებებზე;
- რისკების შეფასების რიგითობაზე;
- ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის ამოცანაზე (მაგალითად: ბიზნეს უწყვეტობა, ინციდენტებისადმი მოქნილობა, შესაბამისობა);
- ინფორმაციული უსაფრთხოების რისკების მართვის პორცესის ობიექტზე) (მაგალითად: ორგანიზაცია, ბიზნეს ერთეული, ინფორმაციული პროცესი, მისი ტექნიკური განხორციელება, გამოყენება, ინტერნეტთან კავშირი).

**შედეგი:** ორგანიზაციის ბიზნეს მიზნებისათვის ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის მუდმივი აუცილებლობა და პროცესის განახლება.

# დანართები

## დანართი ა

### ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის ფარგლებისა და საზღვრების დადგენა

#### ა.1 ორგანიზაციის შესწავლა

ორგანიზაციის შეფასება - ორგანიზაციის შესწავლა წარმოადგენს იმ მახასიათებელი ელემენტების განსაზღვრას, რომელიც განაპირობებს ორგანიზაციის ინდეტურობას. ეს ეხება ორგანიზაციის მიზნებს, ბიზნესს, მისიებს, ფასეულობებსა და სტრატეგიებს.

სირთულე მდგომარეობს ორგანიზაციის სტრუქტურულ მოწყობაში. ამ სტრუქტურის იდენტიფიცირება უზრუნველყოფს ყოველი სტრუქტურული ერთეულის როლისა და მნიშვნელობის გაცნობიერებას ორგანიზაციის მიზნების მიღწევის თვალსაზრისით.

*მაგალითად, ის ფაქტი, რომ ინფორმაციული უსაფრთხოების მენეჯერი ანგარიშვალდებულია უმაღლესი რანგის მენეჯერთან და არა ი.ტ. მენეჯერთან, მიუთითებს ინფორმაციული უსაფრთხოებაში უმაღლესი რანგის მენეჯერის ჩართულობაზე.*

ორგანიზაციის მთავარი მიზანი - ორგანიზაციის მთავარი მიზანი განაპირობებს თავად ორგანიზაციის არსებობას (მისი საქმიანობის სფერო, ბაზრის სეგმენტი, და ა.შ.)

**<u>ბიზნესი</u>:** ორგანიზაციის ბიზნესი, რაც განპირობებულია მისი ტექნიკითა და თანამშრომლების პროფესიული ცოდნით, საშუალებას აძლევს ორგანიზაციას შეასრულოს თავისი მისია. ორგანიზაციის ბიზნესი არის სპეციფიკური ორგანიზაციის საქმიანობის სფეროდან გამომდინარე და ხშირად ორგანიზაციის კულტურას განსაზღვრავს.

**<u>მისია</u>:** ორგანიზაცია მისიის შესრულებით აღწევს დასახულ მიზნებს. ამ მისიის განსაზღვრისათვის უნდა მოხდეს გაწეული მომსახურებებისა და/ან წარმოებული პროდუქციის იდენტიფიცირება საბოლოო მომხმარებელთან მიმართებაში.

**<u>ფასეულობები:</u>** ფასეულობები არის ის მთავარი პრინციპები და მკაცრად განსაზღვრული ქცევის კოდექსი, რაც გამოიყენება ბიზნესის განხორიცელებისთვის. ეს შესაძლოა უკავშირდებოდეს კადრებს, გარე კლიენტებთან ურთიერთობას (მომხმარებლები და ა.შ.), მოწოდებული პროდუქტებისა და გაწეული მომსახურებების ხარისხთან.

*მაგალითად ავიღოთ ორგანიზაცია, რომელის მიზანიცაა საჯარო სერვისები, ხოლო ბიზნესი კი არის ტარნსპორტი; მისია კი მდგომარეობს ბავშვების სკოლაში და სკოლიდან ტრანსპორტირებაში. ასეთი ორგანიზაციის ფასეულობა (ღირებულებები) არის სერვისის პუნქტუალურად განხორციელება და უსაფრთხოება ტრანსპორტირების დროს.*

**ორგანიზაციის სტრუქტურა:** არსებობს სტრუქტურის სხვადასხვა ტიპები:

- დივიზიური სტრუქტურა: ყოველ ქვეგანყოფილებას ყავს თავისი მენეჯერი, რომელიც პასუხისმგებელია საკუთარი სტრუქტურული ერთეულის სტარტეგიულ, ადმინისტრაციულ და ოპერაციულ გადაწყვეტილებებზე
- ფუნქციონალური სტრუქტურა: ფუნქციონალური უფლებამოსილებები გამოიყენება პორცედურებზე, სამუშაოს ხასიათზე და ხანდახან გადაწყვეტილებები და დაგეგმვა (მაგალითად, წარმოება, ინფორმაციული ტექნოლოგიები, ადამიანური რესურსები, მარკეტინგი და ა.შ.)

შენიშვნები:

- დივიზიური სტრუქტურის მქონე ორგანიზაციაში არსებული ქვეგანყოფილება შესაძლოა ორგანიზებული იყოს ფუნქციონალურად და პირიქით;
- ორგანიზაციას შეიძლება ქონდეს მატრიცული სტრუქტურა ორივე ტიპის სტრუქტურის ელემენტების არსებობის შემთხვევაში;
- ნებისმიერ ორგანიზაციულ სტრუქტურაში შეიძლება გაიმიჯნოს შემდეგი დონეები:
  - გადაწყვეტილების მიღების დონე (სტრატეგიული მიმართულებების განსაზღვრება);
  - ლიდერის დონე (კოორდინაცია და მენეჯმენტი);
  - ოპერაციული დონე (წარმოება და მხარდაჭერა).

**ორგანიზაციის სქემა:** ორგანიზაციული სტრუქტურა წარმოდგენილია სქემატურად. მან ხაზი უნდა გაუსვას ანგარიშგებისა და უფლებამოსილებების დელეგირების მიმართულებებს, მაგრამ უნდა შეიცავდეს სხვა ურთიერთობებსაც, რომლებიც, თუნდაც არ ეფუძნებოდნენ ოფიციალურ უფლებამოსილებებს, მაინც მიეკუთვნებიან ინფორმაციულ ნაკადს.

**ორგანიზაციის სტრატეგია:** მოითხოვს ორგანიზაციის სახელმძღვანლო პრინციპების ფორმალურ გამოხატვას. ორგანიზაციის სტრატეგია განსაზღვრავს საჭირო მიმართულებებსა და განვითარებას, რათა სარგებელი იქნას მიღებული დაგეგმილი ცვლილებებისგან და მიმდინარე საკითხებისგან.

### ა.2 ორგანიზაციაზე მოქმედი შეზღუდვების ჩამონათვალი

გათვალისწინებული უნდა იყოს ორგანიზაციაზე მოქმედი და მისი ინფორმაციული უსაფრთხოების ორიენტაციის განმსაზღვრელი ყველა შეზღუდვა. ამ შეზღუდვების წყარო შესაძლოა იყოს ორგანიზაციის შიგნით, ასეთ შემთხვევაში იგი ახორციელებს კონტროლს მათზე ან ორგანიზაციის გარეთ და, ამდენად, არ ექვემდებარება განხილვას. ყველაზე მნიშვნელოვან შეზღუდვებს მიეკუთვნებიან რესურსებიდან გამომდინარე შეზღუდვები (ბიუჯეტი, ადამიანური რესურსები) და კრიტიკული ვითარებებიდან გამომდინარე შეზღუდვები.

ორგანიზაციას აქვს მიზნები (ბიზნესთან, ქცევსთან და ა.შ დაკავშირებით), რომლებსაც უსახავს განხორციელების გარკვეულ გზებს, რაც შესაძლოა იყოს დროში ხანგრძლივად გაწერილი. იგი განსაზღვრავს თუ რა უნდა იყოს მიღწეული რა საშუალებებით. ამ გზის განსაზღვრისას, ორგანიზაციამ უნდა გაითავლისწინოს ტექნოლოგიური წინსვლა და პროფესიული ცოდნა, მომხმარებლების სურვილები და ა.შ. ეს მიზანი შეიძლება გამოიხატოს როგორც ოპერაციული ან განვითარების სტრატეგიის მიზანი, მაგალითად, საოპერაციო ხარჯების ჩამოჭრა, მომსახურების ხარისხის გაუმჯობესება და ა.შ.

ეს სტრატეგიები სავარაუდოდ შეიცავენ ინფორმაციას ან ინფორმაციულ სისტემას. ორგანიზაციის იდენტურობის, მისიისა და სტრატეგიების მახასიათებლები არის სწორედ ის ფუნდამენტალური ელემენტები, რომლებიც გამოიყენება პორბლემის ანალიზისას, რადგანაც ინფორმაციული უსაფრთხოების ასპექტის დარღვევამ შეიძლება გამოიწვიოს ამ სტრატეგიული მიზნების ხელახლა გადახედვა. დამატებით უნდა აღინიშნოს, რომ ინფორმაციული უსაფრთხოების მოთხოვნების შეთავაზება რჩება შესატყვისობაში ორგანიზაციაში მოქმედ წესებთან.
შეზღუდვების ჩამონათვალი შეიცავს:

<u>პოლიტიკური ხასიათის შეზღუდვებს</u>

ეს ეხება სახელმწიფო ადმინისტრაციებს, საჯარო ინსტიტუტებს და უფრო ზოგადად ნებისმიერ ორგანიზაციას, რომელმაც უნდა იხელმძღვანელოს სახლმწიფო გადაწყვეტილებებით. ეს არის ჩვეულებრივ მთავრობის ან გადაწყვეტილების მიმღები ორგანოს მიერ მიღებული სტრატეგიული ან ოპერაციული მიმართულების გადაწყვეტილებები და აუცილებლად უნდა იქნას გამოყენებული.

*მაგალითად, ინვოისებისა და ადმინისტრაციული დოკუმენტების კომპიუტერიზაცია წარმოაჩენს ინფორმაციული უსაფრთხოების პრობლემებს.*

<u>სტარტეგიული ხასიათის შეზღუდვები</u>

ორგანიზაციის სტრუქტურის ან მიმართულებების დაგეგმილმა ან შესაძლო ცვლილებებმა შესაძლოა განაპირობოს შეზღუდვები. ისინი ასახულია ორგანიზაციის სტრატეგიულ ან ოპერაციულ გეგმებში.

*მაგალითად, სენსიტიური ინფორმაციის გაზიარების საერთაშორისო თანამშრომლობამ შეიძლება აუცილებელი გახადოს ხელშეკრულებები უსაფრთხო გაცვლის შესახებ.*

## ტერიტორიული შეზღუდვები

ორგანიზაციის სტრუქტურამ ან მიზანმა შეიძლება წარმოაჩინოს ისეთი სპეციფიკური შეზღუდვები, როგორებიცაა ადგილმდებარეობების დისტრიბუცია მთელი ქვეყნის ტერიტორიაზე ან საზღვარგარეთ.

*მაგალითად, საფოსტო სერვისები, საელჩოები, ბანკები, დიდი ინდუსტრიული ჯგუფების ფილიალები და ა.შ.*

## ეკონომიკური და პოლიტიკური კლიმატის მიერ შექმნილი შეზღუდვები

ორგანიზაციის ოპერაციები შეიძლება უკიდურესად შეცვალოს სპეციფიურმა მოვლენებმა, როგორებიცაა გაფიცვები ან ეროვნული ან საერთაშორისო კრიზისები.

*მაგალითად, სერიოზული კრიზისის დროსაც კი უნდა გრძელდებოდეს ზოგიერთი სერვისის მიწოდება.*

## სტრუქტურული შეზღუდვები

ორგანიზაციის სტრუქტურულმა მოწყობამ (მაგალითად, დივიზიური, ფუნქციონალური ან სხვა) შეიძლება გამოიწვიოს სპეციფიკური ინფორმაციული უსაფრთხოების პოლიტიკის არსებობა და უსაფრთხოების ორგანიზაცია, რომელიც ადაპტირებული იქნება სტრუქტურასთან.

*მაგალითად, საერთაშორისო სტრუქტურამ უნდა შეძლოს თითოეული ქვეყნისთვის სპეციფიკური უსაფრთხოების მოთხოვნების შესაბამისობაში მოყვანა.*

## ფუნქციონალური შეზღუდვები

ფუნქციონალური შეზღუდვები თავს იჩენს პირდაპირ ორგანიზაციის ზოგადი ან სპეციფიკური მისიებიდან.

*მაგალითად, ორგანიზაციამ, რომელიც ოპერაციებს ახორციელებს მთელი დღე-ღამის განმავლობაში, უნდა უზრუნველყოს საკუთარი რესურსების მუდმივი ხელმისაწვდომობა.*

## პერსონალთან დაკავშირებული შეზღუდვები

ეს შეზღუდვები მნიშვნელოვანწილად ცვალებადი ხასიათისაა. ისინი დაკავშირებულია: პასუხისმგებლობის დონესთან, დაქირავებასთან, კვალიფიკაციასთან, ტრენინგთან, უსაფრთხოების შესახებ ინფორმირებულობასთან, მოტივირებულობასთან, ხელმისაწვდომობასთან და ა.შ.

*მაგალითად, თავდაცვის სფეროში მოღვაწე ორგანიზაციის მთელ პერსონალს სჭირდება ავტორიზაცია კონფიდენციალურობის მაღალი დონის შემცველი ინფორმაციის გამოსაყენებლად.*

## ორგანიზაციის კალენდარით გამოწვეული შეზღუდვები

ეს შეზღუდვები შეიძლება გამოიწვიოს ახალმა ან რესტრუქტურირებულმა ეროვნულმა ან საერთაშორისო პოლიტიკის ცვლილებამ ან ახლის ჩამოყალიბებამ.

*მაგალითად, უსაფრთხოების განყოფილების შექმნა*

## მეთოდებთან დაკავშირებული შეზღუდვები

ორგანიზაციისთვის პროფესიული ცოდნის შესაბამისი მეთოდები გამოყენებული უნდა იყოს ისეთ ასპექტებში, როგორებიცაა პროექტის დაგეგმვა, სპეციფიკაცია, განვითარება და ასე შემდეგ.

*მაგალითად, ამგვარი ტიპური შეზღუდვა არის ორგანიზაციის იურიდიული ვალდებულებების ჩართვის აუცილებლობა უსაფრთხოების პოლიტიკაში.*

## კულტურული ხასიათის შეზღუდვები

ზოგიერთ ორგანიზაციაში სამუშაო ჩვევები ან ძირითადი საქმიანობა აპირობებენ ორგანიზაციის სპეციფიკურ „კულტურას“, რაც შეიძლება შეუსაბამობაში აღმოჩნდეს უსაფრთხოების კონტროლის მექანიზმებთან. ეს კულტურა განპირობებულია სხვადასხვა ასპექტებით, მათ შორის განათლება, ინსტრუქცია, პროფესიული გამოცდილება, სამუშაოს გარეთ გამოცდილება, მოსაზრებები, შეხედულებები, ფილოსოფია, რწმენა, სოციალური სტატუსი და ა.შ.

## ბიუჯეტური შეზღუდვები

რეკომენდირებული უსაფრთხოების კონტროლის მექანიზმები შეიძლება საკმაოდ მაღალი ხარჯებით ხასიათდებოდეს. მიუხედავად იმისა, რომ არ არის ყოველთვის სასურველი, უსაფრთხოებაში ინვესტირება დანახარჯების ეფექტურობას ეფუძნებოდეს, ორგანიზაციის ეკონომიკური დეპარტამენტის მიერ მოითხოვება ეკონომიკური დასაბუთება.

*მაგალითად, კერძო სექტორსა და ზოგიერთ საჯარო ორგანიზაციაში, უსაფრთხოების კონტროლებზე გაწეული ხარჯები არ უნდა აღემატებოდეს რისკების პოტენციურ შედეგებთან დაკავშირებულ ხარჯებს. ამდენად,უმაღლესი რანგის მენეჯმენტმა უნდა შეაფასოს და დაიანგარიშოს რისკები უსაფრთხოებასთან დაკავშრებული ზედმეტი (გადაჭარბებული) ხარჯების თავიდან აცილების მიზნით.*

## ა.3 ორგანიზაციის საკანონმდებლო და მარეგულირებელი აქტების ჩამონათვალი

უნდა განისაზღვროს ორგანიზაციისთვის შესაბამისი აუცილებელი მარეგულირებელი მოთხოვნები. ესენია კანონები, დადგენილებები, ორგანიზაციაში არსებული სპეციფიკური რეგულაციები ან შიდა და გარე რეგულაციები. ეს ასევე შეეხება ხელშეკრულებებსა და შეთანხმებებს და უფრო ზოგადად ნებისმიერი სახის იურიდიულ ან მარეგულირებელ ვალდებულებებს.

## ა.4 ვადებზე მოქმედი შეზღუდვების ჩამონათვალი

შეზღუდვების განსაზღვრისას შესაძლოა გაკეთდეს ისეთი შეზღუდვების ჩამონათვალი, რომლებიც გავლენას ახდენენ გავრცელების ფარგლებზე და ემორჩილება ქმედებებს. ისინი შესაძლოა დაემატოს ზემოთ განსაზღვრულ ორგანიზაციულ შეზღუდვებს. შემდეგი პარაგრაფი წარმოადგენს შეზღუდვების შესაძლო ტიპების არასრულ ჩამონათვალს.

### არსებული პროცესების მიერ გამოწვეული შეზღუდვები

პროგრამული უზრუნველყოფის პროექტები არ ხორციელდება იმავდროულად. ზოგიერთი დამოკიდებულია  არსებულ პროცესებზე. იმ შემთხვევაშიც კი, თუ პროცესი შეიძლება დაიყოს ქვე-პროცესებად, პროცესი მაინც არ განიცდის გავლენას სხვა პროცესის ქვე-პროცესების მხრიდან.

### ტექნიკური შეზღუდვები

ინფრასტრუქტურასთან დაკავშირებული ტექნიკური შეზღუდვები ძირითადად განპირობებულია სარგებლობაში მყოფი ტექნიკით და პროგრამული უზრუნველყოფით და ასევე იმ შენობით ან ადგილმდებარეობით, სადაც მიმდინარეობს კონკრეტული პროცესები:

- ფაილები (ორგანიზაციასთან, მედია მენეჯმენტთან, წვდომის წესებთან დაკავშირებული მოთხოვნები და ა.შ.);
- ზოგადი არქიტექტურა (ტოპოლოგიასთან (ცენტრალიზებული, განაწილებული, კლიენტ-სერვერული), ფიზიკურ არქიტექტურასთან დაკავშრებულ მოთხოვნებთან);
- პროგრამული უზრუნველყოფა (სპეციფიკურ პროგრამულ დიზაინთან, საბაზრო სტანდარტებთან და ა.შ. დაკავშრებული მოთხოვნები);
- პროგრამული პაკეტები  (სტანდარტებთან, შეფასების დონეებთან, ხარისხთან, ნორმებისა და უსაფრთხოების შეთავსებადობასთან დაკავშრბეული მოთხოვნები);
- აპარატურა (სტანდარტებთან, ხარისხთან, ნორმებთან, თავსებადობასთან დაკავშირებული მოთხოვნები და ა.შ.);
- საკომუნიკაციო ქსელები (დაფარვასთან, სტანდარტებთან, სიმძლავრესთან, სანდოობასთან და ა.შ. დაკავშირებული მოთხოვნები);
- შენობის ინფრასტრუქტურა (სამოქალაქო მშენებლობასთან, შენობებთან, მაღალ ძაბვასთან, დაბალ ძაბვასთან და ა.შ. დაკავშირებული მოთხოვნები).

### ფინანსური შეზღუდვები

ინფორმაციული უსაფრთხოების კონტროლის მექანიზმების დანერგვა ხშირად შეზღუდულია ბიუჯეტის მიერ, რისი გაღებაც ორგანიზაციას შეუძლია. თუმცა ბიუჯეტის განაწილება

უსაფრთხოებისათვის უნდა განიხილებოდეს უსაფრთხოების შესწავლის საფუძველზე და მხოლოდ ამის შემდეგ უნდა იქნას გათავლისწინებული ფინანსური შეზღუდვები.

გარემოს შეზღუდვები

გარემოს შეზღუდვები წარმოიშობა იმ ეკონომიკური და გეოგრაფიული გარემოდან, რომელშიც მიმდინარეობს პროცესები: ქვეყანა, კლიმატი, ბუნებრივი რისკები, გეოგრაფიული სიტუაცია, ეკონომიკური კლიმატი და ა.შ.

დროის შეზღუდვები

უსაფრთხოების კონტროლის მექანიზმების დანერგვისთვის საჭირო დრო უნდა მოიაზრებოდეს ინფორმაციული სისტემის გაუმჯობესების შესაძლებლობასთან ერთად; თუ განხორციელების დრო არის ძალიან ხანგრძლივი, მაშინ რისკებისთვის განკუთვნილი კონტროლის მექანიზმები შეიძლება შეიცვალოს. დრო არის გადაწყვეტილებებისა და პრიორიტეტების შერჩევის გადამწყვეტი ფაქტორი.

მეთოდებთან დაკავშირებული შეზღუდვები

ორგანიზაციის პროფესიული ცოდნისთვის მისაღები მეთოდები გამოყენებული უნდა იქნას პროექტის დაგეგმვისთვის, სპეციფიკაციისთვის, დამუშავებისთვის და ა.შ.

ორგანიზაციული შეზღუდვები

ორგანიზაციული მოთხოვნებიდან შეიძლება წარმოიქმნას სხვადასხვა შეზღუდვები:

- ოპერაციული (შეფერხებებთან, სერვისის მიწოდებასთან, დაკვირვებასთან, მონიტორინგთან, საგანგებო გეგმებთან, გაუარესებული ხარისხით ფუნქციონირებასთან და ა.შ. დაკავშირებული მოთხოვნები);
- ექსპლუატაცია (ინციდენტების გადაჭრასთან, პრევენციულ ქმედებებთან, სწრაფ კორექტირებასთან და ა.შ. დაკავშირებული მოთხოვნები);
- ადამიანური რესურსების მართვა (ოპერატორების და მომხმარებლების ტრენინგთან, ისეთი თანამდებობების როგორებიცაა სისტემური ადმინისტრატორი ან მონაცემთა ადმინისტრატორის კვალიფიკაციასთან და ა.შ. დაკავშირებული მოთხოვნები);
- ადმინისტრაციული მენეჯმენტი (პასუხისმგებლობებთან და ა.შ. დაკავშირებული მოთხოვნები);
- პროგრამული უზრუნველყოფის შემუშავება (დამუშავების საშუალებებთან, პორგრამული უზურნველყოფის ავტომატიზებულ შემუშავებასთან, მიღებაზე კონტროლის გეგმასთან, დასაფუძნებელ ორგამიზაციასთან და ა.შ. დაკავშირებული მოთხოვნები);
- ორგანიზაციის გარეთ ურთიერთობების მართვა (მესამე მხარის ურთიერთობებთან, კონტრაქტებთან და ა.შ. საორგანიზაციო საკითხებთან დაკავშირებული მოთხოვნები).

# დანართი ბ

## აქტივების იდენტიფიკაცია და ფასეულობის დადგენა  და გავლენის შეფასება

### ბ.1 აქტივების იდენტიფიკაციის ნიმუშები

აქტივებზე ფასის დადგენისთვის ორგანიზაციამ თავდაპირველად უნდა გამოავლინოს საკუთარი აქტივები (დეტალურობის სასურველ დონეზე). აქტივები შეიძლება დაიყოს ორ ჯგუფად:

- ძირითადი აქტივები:
    - ბიზნეს-პროცესები და ქმედებები
    - ინფორმაცია
- ყველა ტიპის დამხმარე აქტივები (რომლებსაც ემყარება მიზნების ძირითადი ელემენტები):
    - აპარატურა
    - პროგრამები
    - ქსელი
    - პერსონალი
    - ადგილმდებარეობა
    - ორგანიზაციული სტრუქტურა

### ბ.1. 1 ძირითადი აქტივების იდენტიფიკაცია

გავრცელების სფეროს ზუსტად აღწერის მიზნით უნდა ითქვას, რომ ეს ქმედება მდგომარეობს ძირითადი აქტივების იდენტიფიცირებაში (ბიზნეს-პროცესები და ქმედებები, ინფორმაცია). იდენტიფიცირება უნდა განახორციელოს პროცესის შერეულმა სამუშაო ჯგუფმა (მენეჯერები, ინფორმაციული სისტემების სპეციალისტები და მომხმარებლები).

ძირითადი აქტივები, როგორც წესი, არის კონკრეტული ძირითადი პროცესები და ინფორმაცია. სხვა ძირითადი აქტივებიც, როგორებიცაა ორგანიზაციის პროცესები, რომლებიც გამოიყენებიან ინფორმაციული უსაფრთხოების პოლიტიკისა ან ბიზნეს უწყვეტობის გეგემის შემუშავებისას, შეიძლება ასევე გათავლისწინებული იქნან. მიზნებიდან გამომდინარე, ზოგიერთი კვლევა საერთოდ არ მოითხოვს მიზნის შემადგენელი ყველა ელემენტის ამომწურავ ანალიზს. ასეთ შემთხვევაში, კვლევის ჩარჩოები უნდა შემოიფარგლოს მიზნის ძირითადი ელემენტებით.

ძირითადი აქტივები არის ორი ტიპის:

1 <u>ბიზნეს-პროცესები (ან ქვე-პორცესები) და ქმედებები, მაგალითად:</u>

- პროცესები, რომელთა დაკარგვა ან დეგრადაცია შეუძლებელს გახდის ორგანიზაციის მისიის განხორციელებას;

- საიდუმლო პროცესების შემცველი პროცესები ან სამესაკუთრეო ტექნოლოგიის პორცესები;
- პროცესები, რომელთა მოდიფიკაციამაც შესაძლოა საკმაოდ დიდი გავლენა მოახდინოს ორგანიზაციის მისიის შესრულებაზე;
- პროცესები, რომლებიც აუცილებელია ორგანიზაციისათვის ხელშეკრულებით გათვალისწინებულ, იურიდიულ ან მარეგულირებელ მოთხოვნებთან შესატყვისობისათვის;

2 <u>ინფორმაცია:</u>

ძირითადი ინფორმაცია შეიცავს:

- ორგანიზაციის მისიის ან ბიზნესის განხორციელებისთვის სასიცოცხლო ინფორმაციას;
- პირადი ინფორმაცია, როგორც განსაზღვრულია კანონში;
- სტარტეგიული მიმართულებებით განსაზღვრული მიზნების მისაღწევად საჭირო სტრატეგიული ინფორმაცია;
- ძვირადღირებული ინფორმაცია, რომლის შეგროვება, შენახვა, დამუშავება და გადაცემა მოითხოვს დროის ხანგრძლივ ინტერვალს ან/და მისი შეძენის ღირებულება მაღალია.

პროცესები და ინფრომაცია, რომლებიც არ არიან გამოვლენილი როგორც მგრძნობიარე, ამ ქმედების შემდეგ მათ არ ექნებათ განსაზღვრული კლასიფიკაცია. ეს კი ნიშნავს იმას, რომ თუ ასეთი პროცესები ან ინფორმაცია არის საფრთხის ქვეშ დაყენებული (დისკრედიტირებული), ორგანიზაცია მაინც შეძლებს საკუთარი მისიის წარმატებით განხორციელებას.

უნდა აღინიშნოს, რომ ისინი ხშირად მემკვიდრეობით იღებენ სენსიტიური პორცესებისა და ინფორმაციის დაცვის კონტროლის მექანიზმებს.

### 8.1.2 დამხმარე აქტივების ჩამონათვალი და აღწერა

გავრცელების სფერო მოიცავს აქტივებს, რომლებიც უნდა იქნას იდენტიფიცირებული და აღწერილი. ამ აქტივებს გააჩნია სუსტი წერტილები, რომლებითაც შეიძლება ისარგებლოს საფრთხემ, რათა გააუარესოს ძირითადი აქტივები (პროცესები და ინფორმაცია). ისინი სხვადასხვა ტიპისაა:

## <u>აპარატურა</u>

აპარატურა შედგება პროცესის მხარდამჭერი ყველა ტიპის ფიზიკური ელემნეტისაგან.

<u>მონაცემთა დამუშავების მოწყობილობები (აქტიური)</u>

ინფორმაციის დამუშავების ავტომატური მოწყობილობა დამოუკიდებლად მუშაობისათვის საჭირო ელემენტების ჩათვლით.

**ტრანსპორტირებადი მოწყობილობები**

პორტატული კომპიუტერული მოწყობილობა.

მაგალითად: პორტატული კომპიუტერი, პირადი ციფრული ასისტენტი (Personal Digital Assistant)

**ფიქსირებული მოწყობილობა**

ორგანიზაციის საკუთერბაში არსებული კომპიუტერული მოწყობილობის გამოყენება.

მაგალითად: სერვერი, მიკროკომპიუტერი როგორც სამუშაო პერსონალური კომპიუტერი.

**დამუშავების პერიფერიული მოწყობილობები**

კომპიუტერთან საკომუნიკაციო პორტის მეშვეობით (სერიული, პარალელული , და ა.შ.) მიერთებული მოწყობილობები მონაცემების შეტანის, მიწოდებისა ან გადაცემის მიზნით.

მაგლითად: პრინტერი, დისკი

**მონაცემთა მატარებელი (პასიური)**

ეს არის მონაცემთა ან ფუნქციების შენასხვისთვის საჭირო მატარებლები.

**ელექტრონული მედია (მატარებელი)**

ინფორმაციის მატარებელი, რომელიც შეიძლება მიურთდეს კომპიუტერს ან კომპიუტერულ ქსელს მონაცემების შენახვის მიზნით. მიუხედავად მათი კომპაქტურობისა, ისინი საკმაოდ დიდი მოცულობის მონაცემებს შეიცავენ. შესაძლებელია მათი გამოყენება სტანდარტული კომპიუტერული მოწყობილობებით.

მაგალითად: კომპაქტ დისკი, სარეზერვო კოპიების ჩაწერისა და შენახვის კარტრიჯი, შესაერთებელი მყარი დისკი, ფლეშ- მეხსიერება, მაგნიტური ფირი.

**სხვა მატარებლები:**

სტატიკური, არაელექტრონული მატარებლები.

მაგალითად: ქაღალდი, სლაიდი, ტრანსპარანტი, დოკუმენტაცია, ფაქსი.

## პროგრამული უზრუნველყოფა

პროგრამული უზრუნველყოფა შედგება ყველა იმ პროგრამისაგან, რომელიც ხელს უწყობს მონაცემთა დამუშავების ფუნქციონირებას.

**ოპერაციული სისტემა**

კომპიუტერის ყველა პროგრამა, რომელიც ქმნის ოპერაციული ბაზის, საიდანაც ეშვება სხვა დანარჩენი პროგრამები (სერვისები ან აპლიკაციები). იგი შეიცავს ბირთვულ და საბაზისო ფუნქციებს ან სერვისებს. არქიტექტურიდან გამომდინარე, ოპერაციული სისტემა შეიძლება იყოს მონოლითური ან შედგებოდეს მიკრო-ბირთვისაგან და სისტემური სერვისების ნაკრებისგან. ოპერაციული სისიტემის ძირითადი ელემენტები მოიცავს მოწყობილობათა მართვის სერვისს (CPU, მეხსიერების, დისკის, და ქსელური ინტერფეისის), დავალებების და პროცესების მართვის სერვისს და მომხმარებლების უფლებათა მართვის სერვისებს.

**სერვისული, საექსპლუატაციო ან ადმინისტრაციული პროგრამები**

სერვისი რომელიც სრულყოფილს ხდის ოპერაციულ სისტემებს და არ არის მომხმარებლების და სხვა პროგრამების პირდაპირ დაქვემდებარებაში.

**პაკეტური ან სტანდარტული პროგრამები**

სტანდარტულ და პაკეტურ პროგრამებს ახაიათებს სრული კომერციალიზაცია. ისინი ემსახურებიან მომხმარებლებს და პროგრამებს, და არ არიან სპეციფიურები ბიზნესისთვის.

მაგალითად: მონაცემთა ბაზების მართვის, ელექტრონული შეტყობინებების, ჯგუფურული დამუშავების და ვებ სერვერის პროგრამული უზრუნველყოფა.

## ბიზნეს პროგრამები (ბიზნესის მხარდამჭერი პროგრამები)

**სტანდარტული ბიზნეს პროგრამები** კომერიცული პროგრამა, რომელიც აძლევს მომხმარებლებს წვდომის შესაძლებლობას საკუთარ ინფორმაციულ სისტემაზე მათთვის საჭირო სერვისებსა და ფუნქციებზე.

მაგალითად: ბუღალტერიის პროგრამა, მანქანა-დანადგარების კონტროლის პროგრამა, კლიენთებთან ურთიერთობის პროგრამა, თანამშრომელთა კომპეტენტურობის მართვის პროგრამა, ადმინისტრაციული პროგრამა და ა.შ.

**სპეციფიკური ბიზნეს პროგრამები** ეს არის პროგრამა, რომელშიც სხვადასხვა ასპექტები (თავდაპირველი მხარდაჭერა, ექსპლუატაცია, გაუმჯობესება და ა.შ.) სპეციალურად შემუშავებული იქნა, რათა მომხარებლისთვის ხელმისაწვდომი ყოფილიყო ის სერვისები და ფუნქციები, რომლებასც მოითხოვენ ინფორმაციული სისტემისგან.

მაგალითად: ტელეკომის ოპერატორების კლიენტების ანგარიშ-ფაქტურების მართვა.

## ქსელი

ქსელის ტიპი შედგება ყველა იმ სატელეკომუნიკაციო მოწყობილობისგან, რომელიც გამოიყენება ინფორმაციული სისტემის სხვადასხვა, ფიზიკურად დაშორებული კომპიუტერებისა და სისტემის ელემენტების ერთმანეთთან დასაკავშირებლად.

**მატარებელი (მედია) და მხარდაჭერა**

კომუნიკაციისა და ტელეკომუნიკაციის მატარებლები და მოწყობილობები ხასიათდებიან ძირითადად ფიზიკური და ტექნიკური მავენებლებით (ორწერტილიანი point-to-point, broadcast ტრანსლაცია) და კომუნიკაციის პროტოკოლებით (ლინკი ან ქსელი - OSI 7-layer-ის 2 და 3 დონე).

მაგალითად : საჯარო სატელეფონო ქსელი (PSTN), ასიმეტრიული ციფრული კავშირი (ADSL), უსადენო ქსელის პროტოკოლი (e.g. WiFi 802.11).

### აქტიური ან პასიური რელე (ტრანსლატორი)

ეს ქვე-ტიპი მოიცავს ყველა იმ მოწყობილობას, რომელიც არ არის კომუნიკაციის საბოლოო წერტილი, არამედ არიან შუამავალი გადამცემი მოწყობილობები. ხშირ შემთხვევაში ისინი იმართება დაშორებულად.

მაგალითად: ხიდი (bridge), მარშრუტიზატორი(router), hub, კომუტატორი(switch),

### საკომუნიკაციო ინტერფეისი

დამუშავების მოწყობილობების საკომუნიკაციო ინტერფეისები დაკავშირებულია დამუშავების მოწყობილობებთან.

მაგალითად: პაკეტური კავშირის რადიო სერვისი (GPRS).

## პერსონალი

თანამშრომლების ტიპი შედგება ინფორმაციულ სისტემაში ჩართული ადამიანების ჯგუფისგან.

### გადაწყვეტილების მიმღები პირი

გადაწყვეტილების მიმღები პირები არიან ძირითადი აქტივების მფლობელები (ინფორმაცია და ფუნქციები) და ორგანიზაციის ან სპეციფიკური პროექტების მენეჯერები.

მაგალითად: ტოპ მენეჯმენტი, პროექტის ლიდერი.

### მომხმარებლები

მომხმარებლები არიან ის თანამშრომლები, რომლებიც თავიანთი საქმიანობიდან გმომდინარე დაკავშრებული არიან სენსიტიურ ელემენტებთან და აქვთ განსაკუთრებული პასუხისმგებლობა. მათ შესაძლოა ქონდეთ ინფორმაციულ სისტემასთან წვდომის განსაკუთრებული უფლებები ყოველდღიური დავალებების შესასრულებლად.

მაგალითად: ადამიანური რესურსების მართვა, ფინანსების მართვა, რისკების მართვა.

### საოპერაციო/მხარდაჭერის პერსონალი

ეს პერსონალი უზრუნველყოფს ინფორმაციული სისტემის ოპერირებას და მხარდაჭერას. მათ აქვთ ინფორმაციულ სისტემაზე წვდომის განსაკუთრებული უფლებები ყოველდღიური დავალებების შესასრულებლად.

მაგალითად: სისტემური ადმინისტრატორი, მონაცემების ადმინისტრატორი, სარეზერვო ასლების უზრუნველყოფა , მხარდაჭერა, აპლიკაციების დანერგვის ოპერატორი, უსაფრტხოების ოფიცრები.

### პროგრამისტები

პროგრამისტები დაკავებული არიან ორგანიზაციის პროგრამული უზრუნველყოფის განვითარებით. მათ აქვთ  მაღალი დონის წვდომის უფლება ინფომაციული სისტემების ნაწილზე , მაგრამ არ იყენებენ რეალურ საწარმოო მონაცემებს.

მაგალითად: ბიზნეს აპლიკაციების პროგრამისტები.

## ნაგებობა

მიზნების განსახორციელებლად საჭირო საოპერაციო ადგილი.

### ადგილმდებარეობა

#### გარე გარემო

იგულისხმება ყველა ის ადგილმდებარეობა, რასაც ორგანიზაციის უსაფრთხოების საშუალებები არ მიესადაგება.

მაგალითად:: პერსონალის საცხოვრებელი, სხვა ორგანიზაციის ფარგლები

#### ფარგლები

ეს ადგილი შემოსაზღვრულია ორგანიზაციის პერიმეტრით. შეიძლება იყოს ფიზიკური საზღვარი/ ბარიერი შენობის გარშემო.

მაგალითად: დაწესებულება, შენობები.

#### ზონა

ზონა ორგანიზაციის შენობის შიგნით არსებული ინფორმაციის დამუშავების ინფრასტრუქტურის ფიზიკურად დაცვადი საზღვარია.

მაგალითად: ოფისები, დაცული წვდომის ზონები, უსაფრთხო ზონა.

#### არსებითი სერვისები

ორგანიზაციის მოწყობილობების ფუნქციონირებისთვის საჭირო ყველა სერვისი.

#### კომუნიკაცია

ოპერატორის მიერ გაწეული სატელეკომინიკაციო სერვისები და მოწყობილობები.

მაგალითად: სატელეფონო ხაზები, შიდა სატელეფონო ქსელები.

#### კომუნალური ინფრასტრუქტურა

სერვისები და საშუალებები (წყაროები და გაყვანილობა) ინფორმაციული ტექნოლოგიების მოწყობილობებისა და პერიფერიების ენერგიით უზრუნველსაყოფად.

მაგალითად: დაბალი ძაბვის მოწოდება, ინვერტორი, ელექტრული წრედები.

წყლით მომარაგება

დასუფთავების სამსახური

ჰაერის გაგრილებისა და გაწმენდის სერვისები და საშუალებები (მოწყობილობები)

მაგალითად: ცივი წყლის მილები.

## ორგანიზაცია

ორგანიზაციის ტიპი აღწერს ორგანიზაციულ სტრუქტურას, რომელიც შედგება დავალებისთვის გამოყოფილი პერსონალის სტრუქტურისა და ამ სტრუქტურების მაკონტროლებელი პროცედურებისაგან.

### ადმინისტრაცია

ესენი არის ის ორგანიზაციები, რომლებისგანაც კონკრეტული (შესასწავლი) ორგანიზაცია იღებს უფლებამოსილებებს. ისინი შეიძლება იყოს იურიდიულად დაქვემდებარებული ან გარე ორგანიზაციები. ამან შეიძლება გამოიწვიოს შესასწავლი ორგანიზაციისთვის რეგულაციების, გადაწყვეტილებებისა და ქმედებების შეზღუდვები.

მაგალითად: ადმინისტრაციული ორგანო, ორგანიაციის სათავო ოფისი.

### ორგანიზაციის სტრუქტურა

იგი შედგება ორგანიზაციის სხვადახვა სტრუქტურული ერთეულებისგან, რომლებსაც აკონტროლებს ორგანიზაციის ხელმძღვანელობა.

მაგალითად: ადამიანური რესურსების მართვა, ინფორმაციული ტექნოლოგიების მართვა, შესყიდვების მართვა, ბიზნეს ერთეულების მართვა, შენობის უსაფრთხოება, სახანძრო სამსახური, აუდიტის მართვა.

### პროექტის ან სისტემის ორგანიზაცია

ეს ეხება სპეციფიკური პროექტის ან სერვისისადმი ორგანიზაციის მიდგომას.

მაგალითად: ახალი პროგრამული უზრუნველყოფის დამუშავების პროექტი, ინფორმაციული სისტემის მიგრაციის პროექტი.

### კონტრაქტორები/მომწოდებლები/მწარმოებლები

ეს ის ორგანიზაციებია, რომლებიც ორგანიზაციას უზრუნველყოფენ სერვისებით ან რესურსებით და ამ ურთიერთობას ამყარებენ ხელშეკრულებით.

მაგალითად: ტექნიკური მართვის სამსახური, მესამე მხარის მიერ უზრუნველყოფილი, საკონსულტაციო კომპანიები.

## 8.2 აქტივების ფასეულობის დადგენა

აქტივების იდენტიფიკაციის შემდგომი საფეხური არის შკალის და თითოეული აქტივისათვის ამ შკალაზე კრიტერიუმების შესაბამისი ადგილის განსაზღვრა, რაც დაფუძნებული იქნება ფასეულობის დადგენაზე. ორგანიზაციაში არსებული აქტივების უმრავლესობას ახასიათებს მრავალფეროვნება, აქედან გამომდინარე ის აქტივები, რომლებსაც აქვთ ფულადი ღირებულება, შეფასებულები იქნებიან ეროვნულ ვალუტაში, ხოლო ხარისხობრივი ფასეულობის მქონე აქტივები რანგირებულები იქნებიან შემდეგი ნიმუშის მიხედვით, მაგალითად „ძალიან დაბალი“, „ძალიან მაღალი“. ორგანიზაცია იღებს გადაწყვეტილებას რაოდენობრივი ან ხარისხობრივი შკალის გამოყენების შესახებ, შეფასების ორივე ტიპი შეიძლება გამოყენებული იქნას ერთი და იმავე აქტივის შეფასებისთვის.

აქტივების ხარისხობრივი შეფასებისას გამოყენებული ტიპიური ტერმინებია: უმნიშვნელო, ძალიან დაბალი, დაბალი, საშუალო, მაღალი, ძალიან მაღალი, და კრიტიკული. ორგანიზაციისათვის შესატყვისი ტერმინების არჩევანი და არეალი მკაცრად არის დამოკიდებული ორგანიზაციის უსაფრთხოების საჭიროებაზე, ორგანიზაციის მასშტაბსა და სხვა ორგანიზაციული ხასიათის ფაქტორებზე.

**კრიტერიუმები**

ყოველი აქტივისათვის ფასეულობის დადგენის საფუძველი უნდა იყოს გარკვეული კრიტერიუმები, რომლებიც ერთმნიშვნელოვნად უნდა იქნას ჩამოყალიბებული. ეს არის აქტივების შეფასების ერთ-ერთი ყველაზე რთული ასპექტი, რადგან შესაძლოა ზოგიერთი აქტივის ფასეულობა დადგენილი იყოს სუბიექტურად და ამასთანავე სხვადასხვა ინდივიდების მიერ. აქტივის ფასეულობის განსაზღვრის შესაძლო კრიტერიუმები მოიცავს მის თავდაპირველ დანახარჯებს, მისი შეცვლის ან ხელახლა წარმოების დანახარჯებს, ან მისი ფასეულობა შეიძლება იყოს აბსტრაქტული, მაგალითად: ორგანიზაციის რეპუტაციის ფასეულობა.

აქტივების შეფასების კიდევ ერთი საფუძველი არის ინციდენტის შედეგად კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დაკარგვასთან დაკავშირებული ხარჯები. ასევე გათვალისწინებული უნდა იქნას წარმოშობის წყაროსთან ცალსახა შესაბამისობა, ანგარიშვალდებულება, აუტენტურობა და სანდოობა. ასეთი შეფასება იძლევა მნიშვნელოვან ელემენტების საზომ ერთეულებს აქტივის ფასეულობისა და მათი შეცვლის ხარჯებისათვის, რომელიც ეფუძნება უსაფრთხოების ინციდენტებიდან გამომდინარე ბიზნესის უარყოფითი შედეგების შეფასებას. განსაკუთრებული მნიშვნელობა ენიჭება იმას, რომ ამგვარი მიდგომა პასუხისმგებელია იმ შედეგებზე, რომლებიც რისკების შეფასების ფაქტორებისთვის აუცილებლობას წარმოადგენენ.

არსებობს აქტივები, რომლებსაც შეფასების კურსის მიმდინარეობისას შეიძლება ქონდეთ რამდენიმე ფასეულობა. მაგალითად: ბიზნეს გეგმა შეიძლება შეფასებული იქნას გეგმის შესრულებაზე დახარჯული დროის, აგრეთვე შემავალი მონაცემებისთვის საჭირო დროის და

კონკურენტისთვის მისი ფასეულობის საფუძველზე. ყოველი დადგენილი ფასეულობა ხშირ შემთხვევაში მნიშვნელოვნად განსხვავდებიან ერთმანეთისგან. საბოლოო ანალიზისას დიდი ყურადღებით უნდა დადგინდეს აქტივის ფასეულობა ან ფასეულობები, რადგანაც საბოლოოდ მინიჭებული ფასეულობა ერთვება იმ რესურსების განსაზღვრაში, რომლებიც აქტივის დაცვასთანაა დაკავშირებული.

<u>საერთო კრიტერიუმები</u>

საბოლოო ჯამში აქტივის ყველა შეფასება უნდა იქნას დაყვანილი საერთო კრიტერიუმების ბაზამდე. ეს კი მიიღწევა ქვემოთ ჩამოთვლილი კრიტერიუმების დახმარებით. აქტივის კონფიდენციალურობის, მთლიანობის, ხელმისაწვდომობის, წარმოშობის წყაროსთან ცალსახა შესატყვისობის, ანგარიშვალდებულების, აუტენტურობის ან საიმედოობის დარღვევის შედეგად შესაძლო შედეგების შეფასებისას გამოყენებული უნდა იქნას შემდეგი კრიტერიუმები:

- საკანონმდებლო და/ან რეგულაციების დარღვევა;
- ბიზნეს წარმადობის გაუარესება;
- კეთილი ნების დაკარგვა/ რეპუტაციაზე უარყოფითი გავლენა;
- პირად ინფორმაციასთან დაკავშირებული დარღვევა;
- პირადი უსაფრთხოების საფრთხის ქვეშ დაყენება;
- მავნე გავლენები კანონის ძალით იძულებაზე;
- კონფიდენციალურობის დარღვევა;
- საზოგადოებრივი წესრიგის დარღვევა;
- ფინანსური დანაკარგები;
- ბიზნეს ქმედებების წყვეტა;
- გარემოს უსაფრთხოების საფრთხის ქვეშ დაყენება.

უარყოფითი შედეგების შეფასების სხვა მიდგომები შეიძლება იყოს:

- სერვისის შეწყვეტა
  - სერვისის გაწევის უუნაროობა;
- მომხმარებლის ნდობის დაკარგვა
  - შიდა ინფორმაციული სისიტემის საიმედოობის დაკარგვა;
  - რეპუტაციისთვის ზიანის მიყენება;
- შიდა ოპერაციების შეწყვეტა
  - თავად ორაგნიზაციის გაჩერება;
  - დამატებითი შიდა ხარჯები.
- მესამე მხარის ოპერაციის შეწყვეტა
  - ორგანიზაციასთან მესამე მხარის თანამშრომლობის შეწყვეტა;
  - სხვადასხვა ტიპის ზიანი;
- კანონისა და/ან რეგულაციების დარღვევა

- კანონით განსაზღვრული ვალდებულებების შესრულების უუნაროობა.

- ხელშეკრულების დარღვევა
  - ხელშეკრულებით განსაზღვრული ვალდებულებების შესრულების უუნაროობა.
- თანამშრომლების/მომხმარებლების საფრთხის ქვეშ დაყენება
  - ორგანიზაციის თანამშრომლების/მომხმარებლების საფრთხე.
- მომხმარებლების პირადი ცხოვრების ხელყოფა;
- ფინანსური დანაკარგები;
- განსაკუთრებული შემთხვევის ან შეკეთების ფინანსური დანახარჯები:
  - თანამშრომლების,
  - მოწყობილობების,
  - კვლევების, ექსპერტების ანგარიშის საფუძველზე;
- ქონების/ ფონდების/აქტივების დაკარგვა;
- მომხმარებლების, მომწოდებლების დაკარგვა;
- სასამართლო პროცესები და ჯარიმები;
- კონკურენტული უპირატესობების დაკარგვა;
- ტექნოლოგიურ/ტექნიკურ სფეროში ლიდერობის დაკარგვა;
- ეფექტიანობის/სანდოობის დაკარგვა;
- ტექნიკური რეპუტაციის დაკარგვა;
- მოლაპარაკების წარმოების უპირატესობის დასუსტება;
- ინდუსტრიული კრიზისი (გაფიცვები);
- სამთავრობო კრიზისი;
- გათავისუფლება (სამსახურიდან დათხოვნა);
- მატერიალური ზარალი.

ეს ის კრიტერიუმებია, რომლებიც აქტივების შესაფებისას უნდა იქნა გათვალისწინებული. შეფასებების განხორციელებისთვის, ორგანიზაციამ უნდა შეარჩიოს მისი ბიზნესის ტიპისა და უსაფრთხოების მოთხოვნებისთვის საჭირო კრიტერიუმები. ეს შეიძლება გულისხმობდეს, რომ ზოგიერთი ზემოთ ჩამოთვლილი კრიტერიუმი არ იყოს შესაბამისი, ასევე საჭირო გახდეს სხვა კრიტერიუმების დამატება ამ ჩამონათვალში.

**შკალა**

კრიტერიუმების დადგენის შემდეგ, ორგანიზაციამ უნდა შეათანხმოს მთელი ორგანიზაციის მასშტაბით მისი გამოყენების შკალა. პირველ ეტაპზე უნდა გადაწყდეს დონეების რაოდენობა. არ არსებობს რაიმე წესი, რომელიც განსაზღვრავდა ყველაზე შესატყვისი დონეების რაოდენობას. რაც უფრო მეტია დონეების სიმრავლე მით უფრო მეტია გრანულირების დონე, მაგრამ ხანდახან ჭარბი დიფერენცირება ართულებს შესაბამის მიკუთვნებულობას. როგორც წესი, ორგანიზაციის მიერ შეიძლება გამოყენებული იქნას 3-დან (მაგალითად: დაბალი, საშუალო და მაღალი) 10-მდე

დონეების რაოდენობა, რაც შეესაბამება ორგანიზაციის მიდგომას მთელი რისკების შეფასების პროცესისადმი.

ორგანიზაციამ შესაძლოა თავად განსაზღვროს აქტივის შეფასების საკუთარი ლიმიტები, როგორც მაგალითად: „დაბალი“, „საშუალო“, ან „მაღალი“. ეს ლიმიტები შერჩეული კრიტერიუმების თანახმად უნდა იქნას შეფასებული (მაგალითად: შესაძლო ფინანსური დანაკარგებისთვის იგი მოცემული უნდა იყოს ფულადი სახით, ხოლო პირადი უსაფრთხოების საფრთხის ქვეშ დაყენების თვალსაზრისით მხედველობაში უნდა იქნას მიღებული, რომ ფულადი შეფასება ასეთ შემთხვევაში რთულდება და ყველა ორგანიზაციისთვის არ იქნება გამოსადეგი). საბოლოოდ მთლიანად ორგანიზაციაზეა დამოკიდებული გადაწყვიტოს თუ რა მოიზარება „დაბალი“ ან „მაღალი“ შედეგების ქვეშ. უარყოფითი შედეგი, რომელიც მაგალითად შეიძლება დამღუპველი იყოს პატარა ორგანიზაციისთვის, ძალიან დიდი ორგანიზაციისთვის იგი შეიძლება იყოს დაბალი ან უმნიშვნელო.

**<u>დამოკიდებულებები</u>**

რაც უფრო მეტად საჭირო და რაოდენობრივად მოცულობითია ბიზნეს-პროცესების მხარდამჭერი აქტივები, მით უფრო დიდია ამ აქტივების ფასეულობა. აქტივების დამოკიდებულება ბიზნეს პროცესებზე და სხვა აქტივებზე უნდა განისაზღვროს, რადგანაც ამან შესაძლოა გავლენა იქონიოს აქტივების ფასეულობაზე. მაგალითად, მონაცემების კონფიდენციალურობა შენარჩუნებული უნდა იქნას მთელი მისი სასიცოცხლო ციკლის განმავლობაში, ყველა ეტაპზე, მათ შორის შენახვა და დამუშავება. მაგალითად, მონაცემთა შენახვის და დამუშავების პროგრამების უსაფრთხოების საჭიროება პირდაპირ კავშირში უნდა იყოს შენახული ან დამუშავებული მონაცემების კონფიდენციალურობის ფასეულობასთან. ასევე, თუ ბიზნეს პროცესი ემყარება პროგრამის მიერ დამუშავებული კონკრეტული მონაცემების მთლიანობას, ასეთ შემთხვევაში ამ პროგრამის შემავალ რესურსს უნდა გააჩნდეს შესაბამისი საიმედოობა. გარდა ამისა, ინფორმაციის მთლიანობა დამოკიდებულია მისი შენახვისა და დამუშავებისთვის გამოყენებულ აპარატურასა და პროგრამებზე. ასევე აპარატურა, თავის მხრივ, დამოკიდებულია კვების მოწოდებასა და შესაძლო კონდიცირებაზე. ამგვარად, ინფორმაცია დამოკიდებულებების შესახებ ხელს უწყობს ასევე საფრთხეების და ცალკეული სუსტი წერტილების იდენტიფიკაციას. დამატებით უნდა აღინიშნოს, რომ ეს უზრუნველყოფს აქტივებს მიენიჭოთ ჭეშმარიტი ფასეულობა (დამოკიდებულებითი ხასიათის ურთიერთობიდან გამომდინარე), დაცვის შესაბამისი დონის მითითებით.

სხვა აქტივებზე დამოკიდებული აქტივების ფასეულობები შეიძლება შეიცვალოს შემდეგნაირად:

- თუ დამოკიდებული აქტივების ფასეულობები (მაგალითად: მონაცემების) უფრო დაბალია ან ტოლია განხილული აქტივისა (მაგალითად: პროგრამა), მაშინ მისი ფასეულობა რჩება იგივე
- თუ დამოკიდებული აქტივის ფასეულობები (მაგალითად, მონაცემები) უფრო დიდია, ვიდრე განხილული აქტივისა (მაგალითად, პროგრამა), მაშინ იგი უნდა გაიზარდოს:

- დამოკიდებულების ხარისხის შესაბამისად;
- სვა აქტივების ფასულობების შესაბამისად.

ორგანიზაციას შეიძლება გააჩნდეს აქტივები, რომლებიც ხელმისაწვდომია მრავალჯერადი სახით, მაგალითად: რეალიზებული პროგრამების ასლები ან მთელს ოფისში გამოყენებული ერთი და იგივე ტიპის კომპიუტერი. მნიშვნელოვანია ამის გათვალისწინება აქტივების შეფასების დროს. ერთი მხრივ, ასეთი აქტივების გამოვლენა რთულია, ამდენად ყურადღება უნდა დაეთმოს ყოველი მათგანის იდენტიფიკაციას; მეორე მხრივ, მათი გამოყენება შეიძლება ხელმისაწვდომობის პრობლემების შესამცირებლად.

<u>შედეგი</u>

ამ ეტაპის საბოლოო შედეგი არის აქტივებისა და მათი ფასეულობების ჩამონათვალი, რაც დაკავშირებულია შემდეგი სახის ხარჯებთან:

- გახმაურება;
- კონფიდენციალურობის შენარჩუნება;
- დაცვა;
- მოდიფიკაცია (მთლიანობის, აუტენტურობის, წარმოშობის წყაროსთან ცალსახა შესატყვისობის და ანგარიშვალდებულების შენრარჩუნება/დაცვა);
- ხელმიუწვდომლობისა და განადგურების (ხელმისაწვდომობისა და საიმედოობის დაცვა);
- შეცვლა.

### 8.3 გავლენის შეფასება

ინფორმაციული უსაფრთხოების ინციდენტმა შეიძლება გავლენა მოახდინოს ერთზე მეტ აქტივზე ან აქტივის მხოლოდ რომელიმე ნაწილზე. გავლენა დაკავშირებულია ინციდენტის წარმატების ხარისხზე. აქედან გამომდინარე ვიღებთ საკმაოდ მნიშვნელოვან სხვაობას აქტივის ფასეულობასა და ინციდენტის მიერ გამოწვეულ გავლენას შორის. გავლენა მოიზარება როგორც მყისიერი (ოპერატიული) ეფექტის ან სამომავლო (ბიზნეს) ეფექტის მქონე, რაც ამასთანავე გულისხმობს ფინანსურ და საბაზრო შედეგებს.
მყისიერი (ოპერატიული) გავლენა არის პირდაპირი ან ირიბი.

<u>პირდაპირი:</u>

1. აქტივის (ან მისი ნაწილის) შეცვლის ფინანსური ღირებულება
2. ახალი აქტივის ან სარეზერვო ასლის შეძენის, კონფიგურაციის და ინსტალაციის ღირებულება
3. ინციდენტის შედეგად შეჩერებული ოპერაციების ღირებულება, მანამ სანამ არ იქნება აღდგენილი სერვისის მაწარმოებელი აქტივი (აქტივები)
4. ინფორმაციული უსაფრთხოების დარღვევის გავლენის შედეგები

ორიბი:

1. ალტერნატიული ღირებულება (აქტივის შეცვლის ან შეკეთებისთვის საჭირო ფინანსური რესურსების გამოყენება სადმე სხვაგან)
2. შეწყვეტილი ოპერაციების ღირებულება
3. უსაფრთხოების დარღვევის შედეგად მიღებული ინფორმაციის პოტენციურად არასათანადოდ გამოყენება
4. ფორმალური და მარეგულირებელი ვალდებულებების დარღვევა
5. ქცევის ეთიკის კოდექსის დარღვევა

პირველი შეფასების დროს (ყოველგვარი კონტროლის მექანიზმების გარეშე) გავლენის შედეგი და აქტივის ფასეულობა საკმაოდ მსგავსია. ამ აქტივის (აქტივების) ყოველი შემდგომი ციკლის დროს გავლენა იქნება განსხვავებული (როგორც წესი უფრო დაბალი), გამომდინარე დანერგილი კონტროლის მექანიზმების არსებობდიდან და ეფექტიანობიდან.

## დანართი გ

**ტიპიური საფრთხეების ნიმუშები**

ქვემოთ მოცემული ცხრილი წარმოადგენს ტიპიური საფრთხეების მაგალითებს. ეს ჩამონათვალი შეიძლება გამოყენებული იქნას საფრთხეების შეფასების პროცესში. საფრთხე შეიძლება იყოს განზრახ შექმნილი, შემთვევითი ან გარემო პირობების (ბუნებრივი) მიერ შექმნილი და შეიძლება გამოიწვიოს, მაგალითად, ძირითადი/არსებითი სერვისების დაზიანება ან დარღვევა. შემდეგი ცხრილი მიუთითებს ყოველი საფრთხის ტიპს, სადაც გ ნიშნავს განზრახ შექმნილს, შ - შემთხვევითს, ხოლო ბ - ბუნების/გარემოს მიერ წარმოქმნილს. გ გამოიყენება ყველა იმ განზრახ ქმედებეზე, რომლებიც მიმართულია ინფორმაციული აქტივებისკენ, შ გამოიყენება ყველა ადამიანურ ქმედებასთან, რამაც შესაძლოა დააზიანოს ინფორმაციული აქტივები, ხოლო ბ გამოიყენება ყველა იმ ინციდენტთან მიმართებაში, რასაც საფუძვლად არ უდევს ადამიანური ქმედებები. საფრთხეების ჯგუფი არ არის პრიორიტეტების მიხედვით დალაგებული.

| **ტიპი** | **საფრთხე** | **წარმოშობა /წყარო** |
|---|---|---|
| ფიზიკური ზიანი | ხანძარი | შ,გ,ბ |
| | წყლით გამოწვეული ზიანი | შ,გ,ბ |
| | დაბინძურება | შ,გ,ბ |
| | დიდი ავარია | შ,გ,ბ |
| | მოწყობილობის ან მატარებლის განადგურება | შ,გ,ბ |
| | მტვერი, კოროზია, გაყინვა | შ,გ,ბ |
| ბუნებრივი მოვლენები | კლიმატის პირობები | ბ |
| | სეისმური პირობები | ბ |
| | ვულკანი | ბ |
| | მეტეოროლოგიური პირობები | ბ |
| | წყალდიდობა | ბ |
| ძირითადი სერვისების დარღვევა | კონდიცირების ან წყალმომარაგების სისტემის გაფუჭება | შ, გ |
| | კვების მოწოდების გათიშვა | შ,გ,ბ |
| | სატელეკომუნიკაციო მოწყობილობების გაფუჭება | შ,გ |
| რადიაციით გამოწვეული დაზიანება | ელექტრომაგნიტური რადიაცია | შ,გ,ბ |
| | თერმული რადიაცია | შ,გ,ბ |
| | ელექტრომაგნიტური იმპულსები | შ,გ,ბ |
| ინფორმაციის საფრთხის ქვეშ დაყენება | საფრთხის შემცველი შემაფერხებელი სიგნალების დაჭერა | გ |
| | დისტანციური დაკვირვება (შპიონაჟი) | გ |
| | მოსმენა | გ |
| | მედია მატარებლების ან დოკუმენტების ქურდობა | გ |
| | მოწყობილობების ქურდობა | გ |

| | | |
|---|---|---|
| | დაბრაკული მედია მატარებლების ხელმეორედ გამოყენება | გ |
| | გახმაურება | შ, გ |
| | მონაცემები არასაიმედო წყაროებიდან | შ, გ |
| | არასანქცირებული შეღწევა აპარატურის მეშვეობით | გ |
| | არასანქცირებული შეღწევა პროგრამის მეშვეობით | შ, გ |
| | ადგილმდებარეობის ამოცნობა | გ |
| ტექნიკური გაუმართაობები | მოწყობილობის გაფუჭება | შ |
| | მოწყობილობის შეფერხებებით ფუნქციონირება | შ |
| | ინფორმაციული სისტემის გადატვირთულობა | შ, გ |
| | პროგრამის შეფერხებებით მუშაობა | შ |
| | ინფორმაციული სისტემის მხარდაჭერის პროცესის დარღვევა | შ, გ |
| არაავტორიზებული ქმედებები | მოწყობილობის არაავტორიზებული გამოყენება | გ |
| | პროგრამის თაღლითური კოპირება | გ |
| | ფალსიფიცირებული ან დაკოპირებული პროგრამის გამოყენება | შ, გ |
| | მონაცემების დამახინჯება | გ |
| | მონაცემების არალეგალური დამუშავება | გ |
| ფუნქციების საფრთხის ქვეშ დაყენება | შეცდომები გამოყენებისას | შ |
| | უფლებების ბოროტად გამოყენება | შ, გ |
| | უფლებების ფალსიფიცირება | გ |
| | ქმედებების უარყოფა | გ |
| | თანამშრომლების ხელმისაწვდომობის დარღვევა | შ, გ, ბ |

შესაბამისი ყურადღება უნდა დაეთმოს ისეთ საფრთხეებს, რომელთა წარმოშობის წყაროც არის ადამიანი. ქვემოთ მოცემული ცხრილი აჩვენებს სპეციფიკურად დაჯგუფებულ ამგვარ საფრთხეებს:

| **საფრთხის წარმოშობის წყარო** | **მოტივაცია** | **შესაძლო შედეგები** |
|---|---|---|
| ჰაკერი, კრაკერი | გამოწვევა;<br>ეგო;<br>აჯანყება;<br>სტატუსი;<br>ფული; | • ჰაკეროზა<br>• სოციალური ინჟინერია<br>• სისტემის გატეხვა<br>• სისტემაზე არასანქცირებული წვდომა |

| | | |
|---|---|---|
| კომპიუტერული დამნაშავე | ინფორმაციის განადგურება;<br>ინფორმაციის სააშკარაოზე არალეგალური გამოტანა;<br>ფულადი მოგება;<br>მონაცემთა არაავტორიზებული ცვლილება; | • კომპიუტერული დანაშაული (მაგ: კიბერ ნადირობა)<br>• თაღლითობა<br>• ინფორმაციული მექრთამეობა<br>• იმიტაცია<br>• სისტემაში ძალისმიერი ჩარევა |
| ტერორისტი | შანტაჟი;<br>განადგურება;<br>მავნე გამოყენება;<br>შურისძიება;<br>პოლიტიკური მიღწევები/მოგება;<br>სამიზნე ჯგუფის ათვისება; | • ბომბი/ტერორიზმი<br>• იფორმაციული ომი<br>• სისტემაზე თავდასხმა (მაგ: სერვისებზე გადანაწილებული უარის თქმა)<br>• სისტემაში შეღწევა<br>• სისტემის დანაშაულისთვის გამოყენება |
| ინდუსტრიული შპიონაჟი (დაზვერვა, კომპანიები, უცხოური მთავრობა, სხვა სახელისუფლებო ინტერესები) | კონკურენტუნარიანობის უპირატესობა;<br>ეკონომიკური შპიონაჟი; | • თავდაცვის უპირატესობა<br>• პოლიტიკური უპირატესობა<br>• ეკონომიკური ექსპლუატაცია<br>• ინფორმაციის ქურდობა<br>• პირადი ცხოვრების ხელშეუხებლობის დარღვევა<br>• სოციალური ინჟინერია<br>• სისტემაში შეღწევა<br>• - სისტემაზე არაავტორიზებული წვდომა (კლასიფიცირებულ, საკუთრების, და/ან ტექნოლოგიასთან დაკავშირებულ ინფორმაციაზე წვდომა) |
| ინსაიდერები (ცუდად ინფორმირებული, განაწყენებული, ბოროტი განზრახვების მქონე, უყურადღებო, არაკეთილსინდისიერი ან გაგდებული | ცნობისმოყვარეობა;<br>ეგო;<br>დაზვერვა;<br>ფულადი მოგება;<br>შურისძიება;<br>არაწინასწარგანზრახული შეცდომები და დაშვებები (მაგ: მონაცემთა შეყვანის შეცდომა, პროგრამული შეცდომა) | • თანამშრომელზე თავდასხმა<br>• შანტაჟი<br>• ორგანიზაციის საკუთრების შესახებ ინფორმაციის ნახვა<br>• კომპიუტერის არასწორი მოხმარება<br>• თაღლითობა და ქურდობა<br>• ინფორმაციით მექრთამეობა<br>• ფალსიფიცირებული, კორუმპირებული მონაცემების შეტანა<br>• მოსმენა<br>• მავნე კოდი (მაგ: ვირუსი, ლოგიკური |

| | | |
|---|---|---|
| თანამშრომლები) | | ბომბა, ტროას ცხენი)<br>• პირადი ინფორმაციის გაყიდვა<br>• სისტემური შეცდომა<br>• სისტემაში შეღწევა<br>• სისტემაზე დივერსია<br>• სისტემაზე არაავტორიზებული წვდომა |

## დანართი დ

### სუსტი წერტილები და მათი შეფასების მეთოდები

### დ.1 სუსტი წერტილების ნიმუშები

ქვემოთ მოცემული ცხრილი გვიჩვენებს სუსტი წერტილების მაგალითებს უსაფრთხოების სხვადასხვა ჭრილში, ასევე ნაჩვენებია საფრთხეების ნიმუშები, რომლებმაც შესაძლოა ისარგებლონ აღნიშნული სუსტი წერტილებით. ჩამონათვალი დახმარებას გაუწევს საფრთხეებისა და სუსტი წერტილების შეფასებას, რათა დადგენილი იქნას ინციდენტის სცენარები. ასევე აღნიშნულია, რომ ზოგიერთ შემთხვევაში სხვა საფრთხეებსაც შეუძლიათ გამოიყენონ ეს სუსტი წერტილები.

| ტიპები | სუსტი წერტილების მაგალითები | საფრთხეების მაგალითები |
|---|---|---|
| აპარატურა | არადამაკმაყოფილებელი ექსპლუატაცია/მედია მატარებლების შენახვის არასწორი ინსტალაცია | ინფორმაციული სისტემის ექსპლუატაციის დარღვევა |
| | პერიოდული შეცვლის სქემის არარსებობა | მოწყობილობის ან მედია მატარებლების განადგურება |
| | ნესტის, მტვერის, დაბინძურებისადმი მგრძნობელობა | მტვერი, კოროზია, ყინვა |
| | ელექტრომაგნიტური გამოსხივებისადმი მგრძნობელობა | ელექტრომაგნიტური გამოსხივება |
| | კონფიგურაციის ცვლილების ეფექტური კონტროლის არარსებობა | შეცდომა მოხმარებისას |
| | ძაბვის ცვლილებისადმი მგრძნობელობა | კვების მიწოდების დაკარგვა |
| | ტემპერატურის ცვლილებისადმი მგრძნობელობა | მეტეოროლოგიური მოვლენები |
| | დაუცავი საცავი | დოკუმენტების ან მედია მატარებლების ქურდობა |
| | უყურადღებობა (შენახვის და დასაწყობების დროს) | დოკუმენტების ან მედია მატარებლების ქურდობა |
| | უკონტროლო კოპირება | დოკუმენტების ან მედია მატარებლების ქურდობა |
| პროგრამული უზრუნველყოფა | პროგრამული უზრუნველყოფის არადამაკმაყოფილებელი ტესტირება ან საერთოდ ტესტირების გარეშე დატოვება | უფლებების ბოროტად გამოყენება |
| | პროგრამული უზრუნველყოფის კარგად | უფლებების ბოროტად |

| | | |
|---|---|---|
| | ნაცნობი ნაკლოვანებები | გამოყენება |
| | „Logout“ (სისტემიდა გამოსვლის) არ შესრულება სამუშაო ადგილის დატოვებისას | უფლებების ბოროტად გამოყენება |
| | მონაცემთა მედია მატარებლის ხელახლა გამოყენება მასზე არსებული ინფორმაციის წესისამებრ წაშლის გარეშე | უფლებების ბოროტად გამოყენება |
| | აუდიტის საკონტროლო ჩანაწერის არარსებობა | უფლებების ბოროტად გამოყენება |
| | წვდომის უფლებების არასწორი მიკუთვნება | უფლებების ბოროტად გამოყენება |
| | ფართოდ გავრცელებული პროგრამული უზრუნველყოფები | მონაცემების დამახინჯება |
| | პროგრამული უზრუნველყოფის მიერ მცდარი მონაცემების გამოყენება | მონაცემების დამახინჯება |
| | მომხმარებლის რთული ინტერფეისი | შეცდომები გამოყენებაში |
| | დოკუმენტაციის არარსებობა | შეცდომები გამოყენებაში |
| | არაკორექტული პარამეტრების დაყენება | შეცდომების გამოყენებაში |
| | არაკორექტული თარიღი | შეცდომები გამოყენებაში |
| | იდენტიფიკაციისა და აუტენტიფიკაციის მექანიზმების არარსებობა, მაგალითად მომხმარებლის აუტენტიფიკაცია | უფლებების ფალსიფიცირება |
| | დაუცავი პაროლების ცხრილები | უფლებების ფალსიფიცირება |
| | პაროლების არასათანადო მართვა | უფლებების ფასლიფიცირება |
| | უსარგებლო სერვისების ჩართვა | მონაცემების არალეგალური დამუშავება |
| | განუვითარებელი ან ახალი პროგრამული უზრუნველყოფა | სოფტის ფუნქციონირების დარღვევა |
| | ბუნდოვანი ან არასრული სპეციფიკაცია დეველოპერებისთვის | პროგრამული უზრუნველყოფის ფუნქციონირების დარღვევა |
| | ცვლილების ეფექტური კონტროლის მექანიზმის არარსებობა | პროგრამული უზრუნველყოფის ფუნქციონირების დარღვევა |
| | პროგრამული უზრუნველყოფის | პროგრამულ |

| | | |
|---|---|---|
| | არაკონტროლირებადი ჩამოტვირთვა და გამოყენება | უზრუნველყოფაზე არასანქცირებული ქმედებების განხორციელება |
| | სარეზერვო ასლების არარსებობა | პორგრამული უზრუნველყოფის ფუნქციონირების დარღვევა |
| | შენობის, კარების და ფანჯრების ფიზიკური დაცვის არარსებობა | მონაცემების მედია მატარებლების ან დოკუმენტაციის ქურდობა |
| | მენეჯმენტის ანგარიშების წარმოების ჩავარდნა | მოწყობილობების არაავტორიზებული გამოყენება |
| ქსელი | შეტყობინებების გაგზავნა/მიღების დასტურის არარსებობა | ქმედებაზე უარი |
| | საკომუნიკაციო ქსელის დაუცველობა | მოსმენა |
| | დაუცველი მგრძნობიარე ტრაფიკი | მოსმენა |
| | კაბელების არასწორი მიერთება | სატელეკომუნიკაციო მოწყობილობების ჩავარდნა |
| | ჩავარდნის ერთადერთი წერტილი | სატელეკომუნიკაციო მოწყობილობების ჩავარდნა |
| | გამგზავნისა და მიმღების აუტენტიფიკაციისა და იდენტიფიკაციის არარსებობა | უფლებების ბოროტად გამოყენება |
| | დაუცველი ქსელის არქიტექრურა | დისტანციური შპიონაჟი |
| | ღია ფორმატში პაროლების გაგზავნა | დისტანციური შპიონაჟი |
| | ქსელის არაადექვატური მართვა (მარშრუტიზაციის მოქნილობა) | ინფორმაციული სისტემის დახშირვა (saturation) |
| | საჯარო სარგებლობის ქსელთან კავშირის დაუცველობა | მოწყობილობების არაავტორიზებული გამოყენება |
| პერსონალი | პერსონალის არარსებობა | პერსონალი ხელმისაწვდობის დარღვევა |
| | დაქირავების არაადექვატური პროცედურები | მოწყობილობების და მონაცემთა მედია მატარებლების განადგურება |
| | უსაფრთხოების შესახებ არასაკმარისი ტრენინგი | შეცდომები გამოყენებაში |
| | აპარატურისა და პროგრამული | შეცდომები გამოყენებაში |

| | | |
|---|---|---|
| | უზრუნველყოფის არასწორი გამოყენება | |
| | უსაფრთხოების შესახებ ინფორმირებულობის ნაკლოვანება | შეცდომები გამოყენებაში |
| | მონიტორინგის მექანიზმების ნაკლოვანება | მონაცემთა არალეგალური დამუშავება |
| | გარედან შესრულებულ სამუშაოებზე ზედამხედველობის ნაკლოვანება ან გასუფთავების უკონტროლობა | დოკუმენტების ან მონაცემთა მედია მატარებლების ქურდობა |
| | ტელეკომუნიკაციისა და შეტყობინებების სწორად გამოყენების პოლიტიკის ნაკლოვანება | მოწყობილობის არაავტორიზებული გამოყენება |
| ადგილმდებარეობა | შენობის ან ოთახების არაადექვატური ან უყურადღებო კონტროლი | მოწყობილობის ან მონაცემთა მედია მატარებლების განადგურება |
| | წყალდიდობისკენ მიდრეკილი ადგილმდებარეობა | წყალდიდობა |
| | არასტაბილური ენერგოგანაწილება | კვების მიწოდების გათიშვა |
| | შენობის, კარების და ფანჯრების ფიზიკური დაცვის არარსებობა | მოწყობილობების ქურდობა |
| ორგანიზაცია | მომხმარებლის რეგისტრაციისა და ხელახალი რეგისტრაციის ფორმალური პროცედურის ნაკლოვანება | უფლებების ბოროტად გამოყენება |
| | წვდომის უფლებების რევიზიის ფორმალური პროცედურის ნაკლოვანება | უფლებების ბოროტად გამოყენება |
| | მომხმარებლების და/ან მესამე მხარის არასაკმარისი უზრუნველყოფა (უსაფრთხოებასთან დაკავშირებით) | უფლებების ბოროტად გამოყენება |
| | ინფორმაციის დამუშავებისთვის საჭირო აპარატურის მონიტორინგის პროცედურების ნაკლოვანება | უფლებების ბოროტად გამოყენება |
| | რეგულარული აუდიტის ნაკლოვანება | უფლებების ბოროტად გამოყენება |
| | რისკების იდენტიფიკაციის და შეფასების პროცედურების ნაკლოვანება | უფლებების ბოროტად გამოყენება |
| | ადმინისტრატორისა და ოპერატორის ლოგებში დაფიქსირებული მცდარი ანგარიშები | უფლებების ბოროტად გამოყენება |
| | სერვისის ექსპლუატაციაზე არაადექვატური რეაგირება | ინფორმაციული სისტემის გამოყენებადობის დარღვევა |

| | | |
|---|---|---|
| | მხარდაჭერის დონეზე დადებული შეთანხმების ნაკლოვანებები | ინფორმაციული სისტემის გამოყენებადობის დარღვევა |
| | ცვლილებების კონტროლის პროცედურის ნაკლოვანება | ინფორმაციული სისტემის გამოყენებადობის დარღვევა |
| | იუმს-ის დოკუმენტაციის კონტროლის ფორმალური პორცედურის ნაკლოვანება | მონაცემების დამახინჯება |
| | იუმს-ის ჩანაწერების რევიზიის ფორმალური პროცედურის ნაკლოვანება | მონაცემების დამახინჯება |
| | საჯაროდ ხელმისაწვდომი ინფორმაციის ავტორიზაციის ფორმალური პროცესის ნაკლოვანება | არასანდო წყაროების მონაცემები |
| | ინფორმაციული უსაფრთხოების პასუხისმგებლობების არასათანადო განაწილება | ქმედებების უარყოფა |
| | უწყვეტობის არასათანადო გეგმები | მოწყობილობის ფუნქციონირების ჩავარდნა |
| | ელექტრონული ფოსტის გამოყენების პოლიტიკის ნაკლოვანება | შეცდომები გამოყენებაში |
| | ორგანიზაციის ოპერაციებში პროგრამული უზრუნველყოფის წარდგენის პროცედურის ნაკლოვანება | შეცდომები გამოყენებაში |
| | ადმინისტრატორის და მომხმარებლის ლოგებში ჩანაწერების ნაკლოვანება | შეცდომები გამოყენებაში |
| | კლასიფიცირებული ინფორმაციის დამუშავების პორცედურების ნაკლოვანება | შეცდომები გამოყენებაში |
| | სამუშაო აღწერილობებში ინფორმაციული უსაფრთხოების პასუხისმგებლობების არაჯეროვნად ასახვა | შეცდომები გამოყენებაში |
| | შეუსაბამო უზრუნველყოფა (ინფორმაციულ უსაფთხოებასთან დაკავშირებით) თანამშრომლებთან მიმართებაში ან უზურნველყოფის ნაკლოვანება | მონაცემთა არალეგალური დამუშავება |
| | ინფორმაციული უსაფრთხოების ინციდენტის შემთხვევაში განსაზღვრული დისციპლინარული | აპარატურის ქურდობა |

| | | |
|---|---|---|
| | პროცესის ნაკლოვანება | |
| | მობილური კომპიუტერის გამოყენების შესახებ ფორმალური პოლიტიკის ნაკლოვანება | აპარატურის ქურდობა |
| | შენობის გარეთ არსებული აქტივების კონტროლის მექანიზმის ნაკლოვანება | აპარატურის ქურდობა |
| | „სუფთა მაგიდისა და სუფთა ეკრანის“ არასათანადო პოლიტიკა | დოკუმენტაციისა და მონაცემთა მედია მატარებლების ქურდობა |
| | ინფორმაცის დამუშავების აპარატურის ავტორიზაციის ნაკლოვანება | დოკუმენტაციისა და მონაცემთა მედია მატარებლების ქურდობა |
| | უსაფრთხოების დარღვევაზე მონიტორინგის მექანიზმების დადგენის ნაკლოვანება | დოკუმენტაციისა და მონაცემთა მედია მატარებლების ქურდობა |
| | მენეჯმენტის მიერ რეგულარული მიმოხილვების ნაკლოვანება | აპარატურის არაავტორიზებული გამოყენება |
| | უსაფრთხოების შესუსტების ანგარიშის პროცედურების ნაკლოვანება | აპარატურის არაავტორიზებული გამოყენება |
| | ინტელექტუალურ უფლებებთან შესაბამისობის უზრუნველყოფის პროცედურის ნაკლოვანება | კოპირებული ან ფალსიფიცირებული პროგრამული უზრუნცველყოფის გამოყენება |

## დ.2 ტექნიკური სისუტეების შეფასების მეთოდები

პროაქტიური მეთოდები, როგორიცაა, მაგალითად, ინფორმაციული სისტემის ტესტირება გამოიყენება იმ სუსტი წერტილების დასადგენელად, რომლებიც დამოკიდებულია ინფორმაციული და საკომუნიკაციო ტექნოლოგიების სისტემების კრიტიკულობასა და ხელმისაწვდომ რესურსებზე (მაგალითად: გამოყოფილი სახსრები, ხელმისაწვდომი ტექნოლოგიები, ტესტირების ჩატარების გამოცდილების მქონე პირები). ტესტირების მეთოდები მოიცავს:

- სუსტი წერტილების ავტომატურად სკანირების ინსტრუმენტს/საშუალებას;
- უსაფრთხოების ტესტირებას და შეფასებას;
- შეღწევადობის ტესტს;

- კოდის განხილვას.

სუსტი წერტილების ავტომატურად სკანირების საშუალებები გამოიყენება ჰოსტების ჯგუფის ან ცნობილი სუსტი წერტილების შემცველი სერვისების ქსელის სკანირებისთვის (მაგალითად, სისტემა საშუალებას იძლევა განხორციელდეს ანონიმური ფაილის გადაცემის ოქმი (FTP), ელექტრონული ფოსტის ტრანსლირება (sendmail relaying). თუმცა უნდა აღინიშნოს, რომ ავტომატური სკანირებით იდენტიფიცირებული პოტენციური სუსტი წერტილები შეიძლება საერთოდ არ წარმოადგენდნენ რეალურ სუს წერტილებს სისტემის გარემოსთან მიმართებაში. მაგალითად, ავტომატური სკანირების ზოგიერთი საშუალება პოტენციური სუსტი წერტილების რანგირებას ახდენენ ადგილმდებარეობის გარემოსა და მოთხოვნების გათვალისიწინების გარეშე. ავტომატური სკანირების შედეგად აღმოჩენილი ზოგიერთი პოტენციური სუსტი წერტილი შესაძლოა გარკვეული ადგილმდებარეობისთვის არ წარმოადგენდეს სუსტ წერტილს, მაგრამ კონფიგურირებული იყოს როგორც სუსტი წერტილი გარემოს მოთხოვნებიდან გამომდინარე. თუმცა, ტესტირების ამ მეთოდმა შესაძლოა გამოიწვიოს მცდარი შედეგები.

უსფართხოების ტესტირება და შეფასება (STE) არის შემდეგი ტექნიკა, რომელიც გამოიყენება ინფორმაციული საკომუნიკაციო ტექნოლოგიების სისტემის სუსტი წერტილების იდენტიფიკაციისთვის რისკების შეფასების პროცესში. იგი მოიცავს ტესტის გეგმის შემუშავებასა და შესრულებას (მაგალითად: ტესტის სცენარი, ტესტის პროცედურები, და ტესტის მოსალოდნელი შედეგები). სისტემის უსაფრთხოების ტესტირების მიზანია ტესტირება ჩაუტარდეს ინფორმაციული საკომუნიაკციო ტექნოლოგიების სისტემის უსაფრთხოების კონტროლის მექანიზმების ეფექიანობა, რადგანაც უნდა მოხდეს მათი გამოყენება ოპერაციულ გარემოში. მიზანი არის, რომ გამოყენებული კონტროლის მექანიზმები პასუხობენ აპარატურისა და პროგრამული უზრუნველყოფისთვის დამტკიცებულ უსაფრთხოების სპეციფიკაციებს და ახორციელებენ ორგანიზაციის უსაფრთხოების პოლიტიკას ან შეესაბამებიან დარგობრივ სტანდარტებს.

შეღწევადობის ტესტი გამოიყენება უსაფრთხოების კონტროლის მექანიზმების განხილვის სრულყოფისათვის და იმის უზრუნველსაყოფად, რომ ინფორმაციული საკომუნიკაციო ტექნოლოგიის სისტემის სხვადასხვა ასპექტები უსაფრთხოდ არიან. შეღწევადობის ტესტი, რისკების შეფასების პროცესში მისი გამოყენებისას, შეიძლება გამოყენებული იქნას ასევე იმის შესაფასებლად, თუ რამდენად შესწევს უნარი ინფორმაციულ საკომუნიკაციო სისტემას გაუძლოს სისტემის უსაფრთხოების დარღვევის ჩაფიქრებულ მცდელობებს. მისი მიზანია, ინფორმაციული საკომუნიკაციო სისტემის ტესტირება საფრთხის წყაროს იდენტიფიცირების თვალსაზრისიდან გამომდინარე და ინფორმაციულ საკომუნიკაციო სისტემაში დაცვის სქემების პოტენციური ჩავარდნების იდენტიფიცირებისათვის.

კოდის განხილვა არის ყველაზე ამომწურავი გზა სუსტი წერტილების შეფასებისთვის (და ყველაზე ძვირადღირებული).

უსაფრთხოების ტესტირების შედეგების გამოყენება დაეხამრება სისტემის სუსტი წერტილების იდენტიფიკაციას.

აუცილებლად უნდა აღინიშნოს, რომ შეღწევადობის საშუალებები და ტექნიკები იძლევიან მცდარ შედეგებს, თუ სუსტი წერტილები უკვე მავნე მიზნებისთვის არის გამოყენებული. სუსტი წერტილების მავნე მიზნებისთვის გამოსაყენებლად პიროვნებამ სათანადოდ უნდა იცოდეს სისტემის/თანხლების/პაჩების დაყენება სატესტო სისტემაზე. თუ ტესტირებისას ეს მონაცემები არ არის ცნობილი, მაშინ შესაძლოა წარუმატებული აღმოჩნდეს კონკრეტული სუსტი წერტილის მავნე მიზნებისთვის გამოყენება (მაგალითად: gain remote reverse shell); თუმცა, ყოველთვის შეიძლება სატესტო სისტემის გადატვირთვა ან განადგურება. ასეთ შემთხვევაში ტესტირებული ობიექტი უნდა განიხილებოდეს როგორც სუსტი წერტილი.

მეთოდები მოიცავს შემდეგ ქმედებებს:

- ადამიანების და მომხმარებლებისთვის ინტერვიუს ჩატარება;
- კითხვარები;
- ფიზიკური ინსპექტირება (დაკვირვება);
- დოკუმენტის ანალიზი.

# დანართი ე

## ინფორმაციული უსაფრთხოების რისკების შეფასებისადმი მიდგომები

### ე.1 ინფორმაციული უსაფრთხოების რისკების მაღალი დონის შეფასება

მაღალი დონის შეფასება იძლევა ქმედებების პრიორიტეტულობისა და ქრონოლოგიის შესაძლებლობას. სხვადახვა მიზეზების, მაგალითად ბიუჯეტის, გამო შესაძლოა ვერ მოხერხდეს ყველა კონტროლის მექანიზმის ერთდროულად დანერგვა და მხოლოდ ყველაზე კრიტიკულ რისკზე მოხდება რეაგირება რისკთან მობყრობის პროცესში. ეს შესაძლოა იყოს წინასწარი ქმედება რისკების დეტალური მართვისთვის, თუ მათი განხორციელება განზრახულია ერთი ან ორი წლის შემდეგ. ამ მიზნების მისაღწევად, მაღალი დონის შეფასება შეიძლება დაიწყოს უარყოფითი შედეგების მაღალი დონის შეფასებით, ნაცვლად საფრთხეების, სუსტი წერტილების, აქტივებისა და შედეგების სისტემური ანალიზისა.

მაღალი დონის შეფასების დაწყების კიდევ ერთი მიზეზი არის ის, რომ მოხდეს მენეჯმენტის ცვლილებასთან (ან ბიზნეს უწყვეტობასთან) დაკავშირებულ სხვა გეგმებთან სინქრონიზაცია.
მაღალი დონის რისკების შეფასების ციკლი შეიძლება მოიცავდეს:

- მაღალი დონის რისკების შეფასება შეიძლება მიმართული იყოს ორგანიზაციის უფრო გლობალური ხედვისა და მისი ინფორმაციული სისტემისაკენ, ამასთან გათავლისწინებული უნდა იყოს ტექნოლოგიური ასპექტები ბიზნესისგან დამოუკიდებლად. გარემოს ანალიზი უფრო მეტად კონცენტრირებულია ბიზნესისა და ოპერაციულ გარემოზე, ვიდრე ტექნოლოგიურ ელემენტებზე.
- მაღალი დონის რისკების შეფასება შეიძლება მიმართული იყოს საფრთხეების უფრო შეზღუდულ ჩამონათვალზე, ან განსაზღვრულ სფეროში დაჯგუფებულ სუსტ წერტილებზე, ან პროცესის დასაჩქარებლად, იგი შეიძლება კონცენტრირებული იყოს რისკების ან თავდასხმების სცენარებზე, ნაცვლად მათ ელემენტებზე კონცენტრირებისა.
- მაღალი დონის რისკების შეფასებისას წარმოდგენილი რისკები უფრო ხშირად უფრო ზოგადი რისკების სფეროდანაა, ვიდრე სპეციფიკური იდენტიფიცირებული რისკები. ისევე როგორც სცენარები ან საფრთხეები არიან დაჯგუფებული ზონებად, რისკთან მობყრობა ასევე იძლევა ამ ზონაში კონტროლის მექანიზმების ჩამონათვალს. რისკთან მოპყრობასთან დაკავშრებული ქმედებები თავდაპირველად იძლევა საერთო კონტროლის მექანიზმების შემოთავაზებისა და არჩევის შესაძლებლობას, ეს კონტროლის მექანიზმები ძალაშია მთელი სისტემისთვის.

მაღალი დონის რისკების შეფასების უპირატესობებია:

- საწყისი მარტივი მიდგომის გამოყენება შესაძლებელია გასნაზღვრავდეს რისკების შეფასების პროგრამის მიღებას.
- შესაძლებელი უნდა იყოს ორგანიზაციული ინფორმაციული უსაფრთხოების პროგრამის სტარტეგიული სურათის შექმნა, მაგალითად: იგი დახმარებას გაუწევს სათანადო დაგეგმვას.
- რესურსები და ფულადი სახსრები გამოყენებული იქნება იქ, სადაც ყველაზე მეტადაა მომგებიანი და პირველ რიგში რეაგირება მოხდება იმ სისტემებზე, რომლებიც ყველაზე მეტ დაცვას საჭიროებენ.

იქედან გამომდინარე, რომ რისკების საწყისი ანალიზი სრულდება მაღალ დონეზე და ნაკლები სიზუსტით, ერთადერთი შესაძლო ნაკლი არის ის, რომ ზოგიერთი ბიზნეს-პროცესი ან სისტემა შესაძლოა არ იყოს იდენტიფიცირებული როგორც ეს საჭიროა მომდევნო, უფრო დეტალური შეფასებისას. აღნიშნული ფაქტი შესაძლოა თავიდან იქნას აცილებული თუ არსებობს ორგანიზაციისა და მისი ინფორმაციისა და სისტემის შესახებ ადექვატური ინფორმაცია, მათ შორის ინფორმაციული უსაფრთხოების ინციდენტების შეფასების შედეგად მოპოვებული ინფორმაცია.

მაღალი დონის რისკების შეფასება მოიაზრებს ინფორმაციული აქტივების ბიზნეს ფასეულობას, და რისკებს ორგანიზაციის ბიზნეს თვალსაზრისებიდან გამომდინარე. პირველი (თავდაპირველი) გადაწყვეტილების მიღებისას (იხილეთ ნახაზი 1), რამდენიმე ფაქტორი განსაზღვრავს არის თუ არა მაღალი დონის შეფასება რისკის აღმოფხვრის ადექვატური; ეს ფაქტორები შეიძლება იყოს:

- სხვადასხვა ინფორმაციული აქტივების მეშვეობით მისაღწევი ბიზნეს მიზნები;
- ორგანიზაციის ბიზნესის დამოკიდებულება ყოველი ინფორმაციული აქტივის ხარისხზე, მაგალითად: ცალკელულ აქტივებზეა დამოკიდებული არის თუ არა ორგანიზაციის გადარჩენისთვის მის მიერ განსაზღვრული ფუნქციები კრიტიკული ან ბიზნესის ეფექტური მართვა არის თუ არა დამოკიდებული აქტივებზე, ან კონფიდენციალურიბაზე, მთლიანობაზე, ხელმისაწვდომობაზე, წარმოშობის წყაროსთან ცალსახა შესააბმისობაზე, ანგარიშვალდებულებაზე, აუტენტურობაზე, და შენახული ინფორმაციის საიმედოობაზე;
- თითოეულ ინფორმაციულ აქტივში ინვესტირების დონე, გამომდინარე აქტივის განვითარებიდან, ექსპლუატაციიდან ან შეცვლიდან, და
- ინფორმაციული აქტივები, რომლებისთვისაც ორგანიზაცია პირდაპირ ადგენს ფასეულობას.

როდესაც ეს ფაქტორები შეფასებულია, მაშნ გადაწყვეტილების მიღება უფრო ადვილია. თუ აქტივის მიზნები უკიდურესად მნიშვნელოვანია ორგანიზაციისთვის ბიზნესის სამართავად, ან თუ აქტივები ხასიათდებიან მაღალი დონის რისკიანობით, მაშინ მომდევნო ციკლი, რისკების დეტალური შეფასება, უნდა განხორციელდეს ცალკეული ინფორმაციული აქტივისათვის (ან აქტივის ნაწილისთვის).

ზოგადი წესი გახლავთ: თუ ინფორმაციული უსაფრთხოების არარსებობამ შეიძლება გამოიწვიოს ორგანიზაციისთვის, მისი ბიზნეს პროცესებისათვის ან აქტივებისათვის უარყოფითი შედეგები, მაშინ რისკების შეფასების შემდეგი ციკლი, უფრო დეტალურ დონეზე, აუცილებელია პოტენციური რისკის იდენტიფიცირებისათვის.

## ე.2 ინფორმაციული უსაფრთხოების რისკების დეტალური შეფასება

ინფორმაციული უსაფრთხოების რისკების დეტალური შეფასების პროცესი მოიცავს აქტივების იდენტიფიკაციას და ფასეულობის დადგენას, ამ აქტივების საფრთხეების და სუსტის წერტილების შეფასებას. ამ ქმედებების შედეგები გამოიყენება რისკების შესაფასებლად და შემდეგ რისკებთან მიბყრობის იდენტიფიცირებისათვის.

დეტალურობა მოითხოვს, როგორც წესი, მნიშვნელოვან დროს, ძალისხმევასა და კომპეტენტურ ცოდნას, და ამდენად შესაბამისობაში იქნება მაღალი დონის რისკის შემცველი ინფორმაციული სისტემებისთვის.

ინფორმაციული უსაფრთხოების რისკების დეტალური შეფასების საბოლოო ეტაპი არის საერთო რისკების შეფასება, რაც ამ დანართის მიზანია.

შედეგები შესაძლია შეფასდეს რამდენიმე სახით, მათ შორის რაოდენობრივი, მაგალითად: ფულადი, და ხარისხობრივი საზომებით (რაც ემყარება ისეთ ატრიბუტებს, როგორებიცაა საშუალო, ზომიერი და მნიშვნელოვანი), ან გამოყენებული იქნას ორივე მეთოდი ერთობლივად. საფრთხის ხდომილების ალბათობის შეფასებისთვის უნდა დადგინდეს დროის ის პერიოდი, რომლის ფარგლებშიც აქტივებს ექნებათ ფასულობა ან საჭიროება იმისა, რომ იქნან დაცულები. სპეციფიკური საფრთხის ალბათობის ხდომილებაზე გავლენას ახდენს შემდეგი:

- აქტივის მიმზიდველობა, ან შესაძლო თანმდევი გავლენა როდესაც ადამიანის მიერ განზრახ შექმნილ საფრთხესთან გვაქვს საქმე
- აქტივის სუსტის წერტილის სიძლიერედ გარდაქმნის სიმარტივე, როდესაც საქმე გვაქვს ადამიანის მიერ განზრახ შექმნილ საფრთხესთან
- საფრთხის აგენტის ტექნიკური შესაძლებლობები, რაც გამოიყენება ადამიანის მიერ განზრახ შექმნილ საფრთხეებთან, და
- სუსტი წერტილების მავნე მიზნებისთვის გამოყენების მიმართ მგრძნობელობა, რაც გამოიყენება როგორც ტექნიკური ასევე არატექნიკური ხასიათის სუსტი წერტილების მიმართ

სხვადასხვა მეთოდების არსებობის შემთხვევაში გამოიყენება ასევე ცხრილები, რაც აერთიანებს სუბიექტურ და ემპირიულ საზომებს. მნიშვნელოვანია ორგანიზაციამ გამოიყენოს მისთვის

კომფორტული მეთოდი, რომელსაც ედნობა და რომელიც შედეგად იძლევა განმეორებად შედეგებს. ქვემოთ მოცემულია ცხრილზე დაფუძნებული ტექნიკების ნიმუშები.

### ე.2.1 ნიმუში 1 მატრიცა წინასწარ განსაზღვრული ფასეულობებით

რისკების შეფასების ამ ტიპის მეთოდებში ფაქტიური ან დაგეგმილი (proposed) ფიზიკური აქტივების ფასეულობა დგინდება შეცვლის ან რეკონსტრუქციის ხარჯებიდან გამომდინარე (მაგალითად: რაოდენობრივი საზომები). ეს ხარჯები შემდგომ კონვერტირებულია (გადატანილია) ხარისხობრივ შკალაზე, რომელიც ასევე ინფორმაციისთვის გამოიყენება (იხილეთ ქვემოთ). ფაქტიური ან დაგეგმილი პროგრამული აქტივები ფასდებიან იმავენაირად, როგორც ფიზიკური აქტივები, შესყიდვის ან რეკონსტრუქციის ხარჯების იდენტიფიცირებით და შემდგომ მათი ხარისხობრივ შკალაზე გადატანით. დამატებით უნდა ითქვას, რომ თუ მოიძებნება ისეთი პროგრამა, რომელსაც გააჩნია საკუთარი შიდა მოთხოვნები კონფიდენციალურობის ან მთლიანობის მიმართ (მაგალითად, თუ წყაროს კოდი თვისთავად არის კომერიცული თვალსაზრისით მგრძნობიარე), მაშინ იგი იმავენაირად შეფასდება როგორც ინფორმაცია.

ინფორმაციის ფასეულობის შესახებ აუცილებელია გასაუბრება შერჩეულ ბიზნეს მენეჯრებთან („მონაცემთა მფლობელები“), რომლებსაც შეუძლიათ ოფიციალურად ისაუბრონ მონაცემების შესახებ, განსაზღვრონ სარგებლობაში მყოფი, ან დაცული, დამუშავებული ან ხელმისაწვდომი მონაცემების ფასეულობა და მგრძნობიარობა. ინტერვიუები ამარტივებენ ინფორმაციის მგრძნობიარობის და ფასეულობის შეფასებას გამომდინარე ყველაზე ცუდი სცენარებიდან, რაც შესაძლოა მოსალოდნელი იყოს მავნე ბიზნეს შედეგებიდან, რასაც თავის მხრივ აპირობებს არაავტორიზებულად ინფორმაციის სააშკარაოზე გამოტანა, არაავტორიზებული მოდიფიკაცია, არა-ხელმისაწვდომობა და განადგურება.

შეფასება სრულფასოვნად ჩაითველბა თუ გამოყენებული იქნება შეფასების სახელმძღვანელო მითითებები, რაც მოიცავს ისეთ საკითებს როგორებიცაა:

- პირადი უსაფრთხოება;
- პირადი ინფორმაცია;
- იურიდიული და მარეგულირებელი ვალდებულებები;
- კანონის გამოყენება;
- კომერიცული და ეკონომიკური ინტერესები;
- ფინანსური დანაკარგი/ქმდებების ჩავარდნა;
- საზოგადოებრივი წესრიგი;
- ბიზნეს პოლიტიკა და ოპერაციები;
- კეთილი ნების დაკარგვა;
- მომხმარებელთან (კლიენტთან) კონტრაქტი ან შეთანხმება.

სახელმძღვანელო მითითებები აიოლებენ ციფრულ შკალაზე ფასეულობის იდენტიფიკაციას, როგორიცაა მაგალითად 0-დან 4-მდე შკალა ნაჩვენები ნიმუშის სახით ქვემოთ შკალაზე, რაც საშუალებას იძლევა განხორციელებული იყოს რაოდენობრივი ფასეულობის დადგენა და ასევე ლოგიკური, ხარისხობრივი ფასეულობის განსაზღვრა იქ, სადაც რაოდენობრივი ფასეულობა არ დგინდება, მაგალითად: ადამიანური სიცოცხლის საფრთხის ქვეშ დაყენება.

შემდეგი მნიშვნელოვანი საფეხური არის ყოველი საფრთხის ტიპისათვის, აქტივების ყოველი ჯგუფისათვის კითხვარების დასრულება, რათა შესაძლებელი გახდეს საფრთხეების დონეების (ხდომილების ალბათობა) და სუსტი წერტილების დონეები შეფასება (საფრთხეების მეირ ადვილად გამოყენებადი, მავნე შედეგების გამომწვევი). თითოეულ კითხვაზე გაცემულ პასუხს თან ახლავს განმარტება. ეს კომენტარები აკუმულირებულია ცოდნის ბაზაში და რანგირებულია. იგი ახდენს საფრთხეების დონეების და სუსტი წერტილების იდენტიფიცირებას შკალაზე (დაბალიდან მაღალის ჩათვლით), რაც წარმოადგენს საჭიროებისამებრ შედეგების ტიპებს შორის სხვაობებს, როგორც ნაჩვენებია ქვემოთ მატრიცაზე. კითხვარის სრულყოფისათვის საჭიროა ინფორმაციის შეგროვება ინტერვიუების მეშვეობით შესაბამის ტექნიკურ პერსონალთან, თანამშრომლებთან, ფიზიკური ადგიმდებარეობის ინსპექციასთან და ასევე დოკუმენტაციის განხილვის მეშვეობით.

აქტივების ფასეულობებ, საფრთხეებისა და სუსტი წერტილების დონეები, რაც აუცილებელია შედეგების ყოველი ტიპისათვის, დაჯგუფებულია ქვემოთ ნაჩვენებ მატრიცაზე, რათა მოხდეს ყოველი კომბინაციისათვის რისკის მნიშვნელოვანი საზომის იდენტიფიცირება შკალაზე 0-დან 8-მდე ქულების გამოყენებით. ფასეულობები მატრიცაზე განლაგებულია სტრუქტურულად.

**ცხრილი ე.1.ა**

| | საფრთხის ხდომილების ალბათობა | **დაბალი** | | | **საშუალო** | | | **მაღალი** | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | მავნე მიზნებისთვის გამოყენების სიმარტივე | დ | ს | მ | დ | ს | მ | დ | ს | მ |
| აქტივის ფასეულობა | 0 | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |
| | 1 | 1 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| | 2 | 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |
| | 3 | 3 | 4 | 5 | 4 | 5 | 6 | 5 | 6 | 7 |
| | 4 | 4 | 5 | 6 | 5 | 6 | 7 | 6 | 7 | 8 |

ყოველი აქტივისათვის გათვალისწინებული უნდა იყოს სუსტი წერტილები და მათთან დაკავშირებული საფრთხეები. თუ სუსტი წერტილი არსებობს მასთან დაკავშირებული საფრთხის გარეშე, ან საფრთხე სუსტი წერტილის გარეშე, მაშინ რეალურად რისკი არ არსებობს (მაგრამ უნდა მიედევნოს თვალყური, ვითრების შეცვლის თვალსაზრისით). მატრიცაზე შესაბამისი სტრიქონი იდენტიფიცირებულია აქტივის ფასეულობით, ხოლო შესაბამისი სვეტი კი საფრთხის ხდომილების ალბათობით და მავნე მიზნებისთვის მისი გამოყენების სიმარტივით. მაგალითად, თუ აქტივის ფასეულობა არის 3, საფრთხე არის „მაღალი“ და სუსტი წერტილი კი „დაბალი“, რისკის საზომი კი არის 5. დავუშვათ აქტივის ფასეულობა არის 2, მაგალითად მოდიფიკაციისათვის, საფრთხის დონე არის „დაბალი“ და მავნე მიზნებისთვის მისი გამოყენება არის „მაღალი“, მაშინ რისკის საზომი არის 4. გამომდინარე საფრთხეების ალბათობების კატეგორიების რაოდენობიდან, მავნე მიზნებისთვის მარტივად გამოყენების კატეგორიებიდან და აქტივების შეფასების კატეგორეიბიდან, ორგანიზაციას შეუძლია საკუთარი საჭიროებისამებრ დაადგინოს  მატრიცის ზომა. დამატებითი სვეტები და სტრიქონები მოითხოვენ დამატებით რისკების საზომებს. ამ მიდგომის ფასეულობა მდგომარეობს სამიზნე რისკების რანგირებაში.

ე.1.ბ) ცხრილზე წარმოდგენილი მატრიცა გამომდინარეობს ინციდენტის სცენარის ალბათობის მოსაზრებიდან, და იგი დაკავშირებულია ბიზნესზე გავლენასთან. ინციდენტის სცენარის ალბათობა მოცემულია სუსტი წერტილების მავნე მიზნებისთვის გამოყენების საფრთხის ზოგიერთი ალბათობით. ცხრილი ასახავს ამ ალბათობას ბიზნესზე გავლენასთან მიმართებაში, რაც დაკავშირებულია ინციდენტების სცენართან. შედეგად მიღებული რისკი გაიზომება შკალაზე 0-დან 8-დე მაჩვენებლით, რაც შესაძლოა შეფასდეს რისკებზე თანხმობის კრიტერიუმებთან მიმართებაში.  რისკების მოცემული შკალა შეიძლება ასახავდეს ასევე ზოგადად რისკების რეიტინგს. მაგალითად:

- დაბალი რისკი: 0 – 2
- საშუალო რისკი: 3 – 5
- მაღალი რისკი: 6 – 8

**ცხრილი ე.1 ბ)**

| | ინციდენტის სცენარის ალბათობა | ძალიან დაბალი (ძალიან ნაკლებად რეალური) | დაბალი (ნაკლებად რეალური) | საშუალო (შესაძლო) | მაღალი (რეალური) | ძალიან მაღალი (ხშირი) |
|---|---|---|---|---|---|---|
| ბიზნესზე გავლენა | ძალიან დაბალი | 0 | 1 | 2 | 3 | 4 |
| | დაბალი | 1 | 2 | 3 | 4 | 5 |
| | საშუალო | 2 | 3 | 4 | 5 | 6 |
| | მაღალი | 3 | 4 | 5 | 6 | 7 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | ძალიან მაღალი | 4 | 5 | 6 | 7 | 8 |

**ე.2.2 მაგალითი 2 საფრთხეების რანგირება რისკების გაზომვის მეშვეობით**

ე.2-ზე ნაჩვენები მატრიცა ან ცხრილი შეიძლება გამოყენებული იქნას შედეგების ფაქტორებთან (აქტივების ფასეულობა) და საფრთხეების ხდომილების ალბათობასთან მიმართებაში (სუსტი წერტილების ასპექტების გათავლისწინება). პირველი ნაბიჯი არის შედეგების შეფასება (აქტივების ფასეულობა) წინასწარ განსაზღვრულ შკალაზე, მაგალითად 1-დან 5-ის ჩათვლით, თითოეული საფრთხის ქვეშ მყოფი აქტივისათვის (სვეტი „ბ“ ცხრილზე). შემდეგი ნაბიჯი არის საფრთხის ხდომილების ალბათობის შეფასება წინასწარ განსაზრვრულ შკალაზე, მაგალითად 1-დან 5-ის ჩათვლით ყოველი საფრთხისთვის (სვეტი „გ“). მესამე საფეხური კი არის რისკის ზომის გამოთვლა გამრავლების ფუნქციით (ბ × გ). საბოლოოდ საფრთხეები რანგირებულია მასთან დაკავშირებული რისკების ზომის თანახმად. გასათვალისწინებელია, რომ ამ მაგალითში 1 აღებულია როგორც ყველაზე დაბალი შედეგი და ხდომილების ყველაზე დაბალი ალბათობა.

**ცხრილი ე.2**

| საფრთხის აღმწერი (ა) | შედეგის (აქტივის) ფასეულობა (ბ) | საფრთხის ხდომილების ალბათობა (გ) | რისკის გაზომვა (დ) | საფრთხის რანგირება (ე) |
|---|---|---|---|---|
| საფრთხე ა | 5 | 2 | 10 | 2 |
| საფრთხე ბ | 2 | 4 | 8 | 3 |
| საფრთხე გ | 3 | 5 | 15 | 1 |
| საფრთხე დ | 1 | 3 | 3 | 5 |
| საფრთხე ე | 4 | 1 | 4 | 4 |
| საფრთხე ვ | 2 | 4 | 8 | 3 |

ზემოთ მოცემული ცხრილი უჩვენებს იმ პროცედურას, რომელიც საშუალებას იძლევა განსხვავებული საფრთხეები განსხვავებული შედეგებით და ხდომილების ალბათობებით შედარდეს ერთმანეთთან და რანგირებული იყოს პრიორიტეტების მიხედვით. ზოგიერთ შემთხვევაში საჭიროა ფულადი ფასეულობის დაკავშრება ემპირიულ შკალასთან.

### ე.2.3 მაგალითი 3 რისკების ხდომილების ალბათობის ფასეულობისა და შესაძლო შედეგების შეფასება

ამ მაგალითში ხაზგასმულია ინფორმაციული უსაფრთხოების ინციდენტების უარყოფითი შედეგები (მაგალითად, ინციდენტების სცენარები) და პრიორიტეტული სისტემების განსაზღვრა.

ამის განხორციელება ხდება თითოეულ რისკზე და აქტივზე ორის ფასეულობის შეფასებით, რაც ერთობლივად განსაზღვრავს თითოეული აქტივის ქულას. როდესაც სისტემის ყევლა აქტივის ქულები შეჯამებულია, მაშინ განისაზღვრება ამ სისტემისთვის რისკის საზომი.
პირველ რიგში, ყოველ აქტივს მიენიჭება ფასეულობა. ეს ფასეულობა დაკავშრებულია პოტენციურ არასასურველ შედეგებთან, რაც გამოწვეულია აქტივისთვის საფრთხის შექმნით.

შემდეგ დგინდენა ალბათობის ფასეულობა. იგი ფასდება საფრთხის მოხდენის ალაბთობისა და სუსტი წერტილის მავნე მიზნებისთვის მარტივად გამოეყენებათობის კომბინაციით, იხილეთ ცხრილი ე.3, რომელიც წარმოადგენს ინციდენტის სცენარის ალბათობას.

**ცხრილი ე.3**

| **საფრთხის ალბათობა** | **დაბალი** | | | **საშუალო** | | | **მაღალი** | | |
|---|---|---|---|---|---|---|---|---|---|
| სუსტი წერტილების დონეები | დ | ს | მ | დ | ს | მ | დ | ს | მ |
| ინციდენტების სცენარების ალბათობის ფასეულობა | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |

შემდეგ, აქტივის/საფრთხის ქულა განისაზღვრება აქტივის ფასეულობისა და ალბათობის ფასეულობის გადაკვეთით ცხრილში ე.4. აქტივის/საფრთხის ქულები დაჯამებულია აქტივის ჯამური ქულის მისაღებად. ეს ციფრი გამოიყენება სისტემის მაფორმირებელ აქტივებს შორის განსხვავების წარმოსაჩენად.

**ცხრილი ე.4**

| აქტივის ფასეულობა | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| ალბათობის ფასეულობა | | | | | |
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 5 |
| 2 | 2 | 3 | 4 | 5 | 6 |
| 3 | 3 | 4 | 5 | 6 | 7 |
| 4 | 4 | 5 | 6 | 7 | 8 |

საბოლოო ნაბიჯი არის ყველა აქტივის საერთო ქულების დაჯამება სისტემის აქტივებისათვის, რაც უზრუნველყოფს სისტემის ქულას. ეს გამოიყენება სისტემებს შორის განსხვავების წარმოსაჩენად და იმის განსაზრისათვის, თუ რომელი სისტემის დაცვას უნდა მიენიჭოს პრიორიტეტი.
შემდეგ მაგალითებში მოცემული ფასეულობები შემთხვევითაა არჩეული.

დავუშვათ, რომ სისტემას „ს“ აქვს სამი აქტივი ა1, ა2, და ა3. ასევე დავუშვათ, რომ ამ სისტემისთვის არსებობს ორი საფრთხე ს1 და ს2. ა1-ის ფასეულობა იყოს 3, ა2-ის 2 და ა3-ს კი 4.
თუ ა1-სთვის და ს1-სთვის საფრთხის ალბათობა არის დაბალი და სუსტი წერტილების გამოყენებადობის მაჩვენებელი არის საშუალო, მაშინ ალბათობის ფასეულობა არის 1 (იხილეთ ცხრილი 3).

ზემოთ მოცემული მაგალითები ინფორმაციულ სისტემაზე დაყდრნობით უჩვენებს, რომ მსგავსი მიდგომები შეიძლება იქნას გამოყენებული ბიზნეს პროცესების მიმართ.

## დანართი ვ

### რისკების შემცირებსთან დაკავშირებული შეზღუდვები

რისკების შემცირების შეზღუდვების განხილვისას გათვალისწინებული უნდა იქნას შემდეგი შეზღუდვები:

***<u>დროის შეზღუდვები:</u>***

დროის შეზღუდვების მრავალი ტიპი არსებობს. მაგალითად, კონტროლის მექანიზმები უნდა დაინერგოს ორგანიზაციის მენეჯერბისათვის მისაღებ დროის გარკვეულ პერიოდში. დროის შეზღუდვის სხვაგვარი ტიპი არის კონტროლის მექანიზმის დანერგვის შესაძლებლობა სისტემის ან ინფორმაციის სიცოცხლის ხანგრძლივობის მანძილზე. დროის შეზღუდვის მესამე ტიპი არის ორგანიზაციის მენეჯერების მიერ დადგენილი დროის პერიოდი, რომელიც არის შესაბამისი პერიოდი ცალკეული რისკების მისაღებად.

***<u>ფინანსური შეზღუდვები:</u>***

კონტროლის მექანიზმების დანერგვა და ექსპლუატაცია არ უნდა იყოს რისკების ფასეულობაზე მეტად ძვირადღირებული, გარდა იმ შემთხვევებისა, როდესაც შესაბამისობა არის აუცილებელი (მაგალითად: კანონმდებლობასთან შესაბამისობა). ყველაფერი უნდა გაკეთდეს იმისათვის, რომ არ იქნას ბიუჯეტი გადაჭარბებული და კონტროლის მექანიზმების მეშვეობით მიღწეული იქნას ფინანსური უპირატესობები. თუმცა, ზოგიერთ შემთხვევაში შეუძლებელია მიღწეული იქნას სასურველი უსაფრთხოება და დასაშვებ რისკებზე თანხმობის დონე, რაც განპირობებულია ბიუჯეტით. ამ სიტუაციის გადაჭრა დამოკიდებულია ორგანიზაციის მენეჯერების გადაწყვეტილებებზე.

დიდი ყურადღება უნდა მიექცეს იმ შემთხვევას, თუ ბიუჯეტი ამცირებს დასანერგი კონტროლის მექანიზმების რაოდენობას ან ხარისხს, რადგანაც მან შეიძლება გამოიწვიოს უფრო დიდი რაოდენობის რისკების დაშვება, ვიდრე ეს დაგეგმილია. კონტროლის მექანიზმებისთვის დადგენილი ბიუჯეტი უნდა გამოყენებოდეს მხოლოდ როგორც შეზღუდვა.

***<u>ტექნიკური შეზღუდვები:</u>***

ტექიკური ხასიათის პრობლემები, როგორიცაა, მაგალითად, პროგრამული უზრუნველყოფებისა და აპარატურის არათავსებადობა, ადვილად შეიძლება იქნას თავიდან აცილებული თუ ისინი გათვალისწინებული იყო კონტროლის მექანიზმების არჩევისას. დამატებით უნდა ითქვას, რომ არსებული პროცესებისა და სისტემისადმი კონტროლის მექანიზმების რეტროსპექტული დანერგვა ხშირად გართულებულია ტექნიკური ხასიათის შეზღუდვებით. ამ სირთულეებმა შესაძლოა კონტროლის მექანიზმების ბალანსი გადაიტანოს უსაფრთხოების პროცედურული და ფიზიკური ასპექტებისკენ. აუცილებელია გადახედული იქნას ინფორმაციული უსაფრთხოების

პროგრამა უსაფრთხოების მიზნების მისაღწევად. ეს შესაძლოა მოხდეს მაშინ, როდესაც კონტროლის მექანიზმები არ პასუხობენ რისკების შემცირების მოსალოდნელ შედეგებს წარმადობის შემცირების გარეშე.

***ოპერაციული შეზღუდვები:***

ოპერაციულმა შეზღუდვებმა, მაგალითად: 24×7 ფუნქციონირების და ამავდროულად სარეზერვო ასლების შექმნის აუცილებლობა, შესაძლოა გამოიწვიოს კონტროლის მექანიზმების კომპლექსური და ძვირადღირებული დანერგვა, თუ ის დასაწყისშივე არ არის გათვალისწინებული დიზაინში.

***კულტურული შეზღუდვები:***

კულტურილი ხასიათის შეზღუდვები კონტროლის მექანიზმების არჩევისას შესაძლოა სპეციფიკური იყოს ქვეყნისთვის, სექტორისთვის, ორგანიზაციისა ან ორგანიზაციის დეპარტამენტისთვისაც კი. არ შეიძლება ყველა ქვეყანაში ყველა კონტროლის მექანიზმის გამოყენება. კულტურული ასპექტების იგნორირება არ შეიძლება, რადგანაც ბევრი კონტროლი დაფუძნებულია თანამშრომლების აქტიურ მხარდაჭერაზე. თუ თანაშრომლებს არ ესმით კონტროლის მექანიზმის აუცილებლობა ან არ მიიჩნევენ მათ კულტურული თვალსაზრისით დასაშვებად, მაშინ კონტროლის მექანიზმი დროთა განმავლობაში გახდება უშედეგო. მაგალითად, ხელჩანთის გაჩხრეკვა ევროპის ზოგიერთ ქვეყნებში შესაძლოა იყოს დასაშვები, მაგრამ ახლო აღმოსავლეთში.

***ეთიკური შეზღუდვები:***

ეთიკურ შეზღუდვებს შეიძლება ქონდეთ მნიშვნელოვანი შედეგები კონტროლის მექანიზმებთან მიმართებაში, რადგანაც ეთიკები სოციალური ნორმებიდან გამომდინარე იცვლებიან. ამან შესაძლოა ხელი შეუშალოს ისეთი კონტროლის მექანიზმების დანერგვას, როგორიცაა მაგალითად ელექტრონული ფოსტის სკანირება ზოგიერთ ქვეყანაში. ინფორმაციის დაცვა ასევე შეიძლება შეიცვალოს რეგიონის ან მთავრობის ეთიკიდან გამომდინარე. ეს შეიძლება უფრო მეტად პრობლემატური იყოს ზოგიერთ დარგობრივ სექტორში, ვიდრე სხვაგან, მაგალითად მთავრობა და ჯანდაცვა.

***გარემოს შეზღუდვები:***

გარემო პირობებმა შესაძლოა გავლენა იქონიონ კონტროლის მექანიზმების არჩევაზე, მაგალითად ადგილმდებარეობის ხელმისაწვდომობა (space availability), კლიმატის ექსტრემალური პირობები, ახლომდებარე ბუნებრივი და ურბანული გეოგრაფია. მაგალითად, სეისმური მდგრადობა შესაძლოა საჭირო იყოს ზოგ ქვეყანაში, ზოგში კი არა.

***იურიდიული შეზღუდვები:***

იურიდიულმა ფაქტორებმა, როგორებიცაა პირადი მონაცემების დაცვა ან ინფორმაციის დაცვისათვის კრიმინალური კოდექსის უზრუნველყოფა, შესაძლოა გავლენა მოახდინონ კონტროლის მექანიზმების არჩევაზე. საკანონმდებლო და მარეგულირებელმა შესაბამისობამ შეძლება სავალდებულო გახადოს კონტროლის მექანიზმის ზოგიერთი ტიპი, მათ შორის მონაცემთა დაცვა და ფინანსურ აუდიტი; მათ ასევე შუძლიათ ხელი შეუშალონ ზოგიერთი კონტროლის მექანიზმის გამოყენებას, მაგალითად დაშიფვრა. სხვა კანონებმა და რეგულაციებმა, როგორებიცაა შრომითი ურთიერთობების კანონმდებლობა, სახანძრო დეპარტამენტი, ჯანდაცვა და უსაფრთხოება, და ეკონომიკური სექტორის რეგულაციები და ა.შ., შესაძლოა გავლენა მოახდინონ კონტროლის მექანიზმის არჩევაზეც.

***გამოყენების სიმარტივე:***

ადამიანისა და ტექნოლოგიის არადამაკმაყოფილებელმა ინტერფეისმა შეიძლება გამოიწვიოს ადამიანური ფაქტორით განპირობებული შეცდომები (ოპერატორის მიერ დაშვებული) და განაპირობოს კონტროლის მექანიზმის გამოუსადეგრობა. კონტროლი მექანიზმები არჩეული უნდა იქნას მათი გამოყენების სიმარტივის გათვალისწინებით, რათა მიღწეული იქნას რეაგირების გარეშე დარჩენილი რისკების დასაშვები დონე. რთულად გამოსაყენებადი კონტროლის მექანიზმები გავლენას ახდენენ მათ ეფექტიანობაზე, რადგანაც მომხმარებლები ეცდებიან გვერდი აუარონ ან იგნორირება მოახდინონ მათზე შეძლებისდაგვარად. ორგანიზაციის შიგნით არსებულმა რთულმა კონტროლის მექნიზმებმა წვდომაზე შესაძლოა ბიძგი მისცეს მომხმარებლებს მონახონ წვდომის ალტერნატიული, არაავტორიზებული მეთოდები.

***საკადრო შეზღუდვები:***

კონტროლის მექანიზმების დანერგვისათვის საჭირო სპეციფიკური უნარ-ჩვევების ხელმისაწვდომობა და მისი ხელფასში ასახვა, ასევე თანამშრომლების გადაადგილება ურთიერთსაწინააღმდეგო ოპერაციულ პირობებში აუცილებლად უნდა იქნას გათავლისწინებული. გამოცდილება შესაძლოა არ აღმოჩნდეს ადვილად ხელმისაწვდომი დაგეგმილი კონტროლის მექანიზმების დანერგვისათვის ან გამოცდილება აღმოჩნდეს ზედმეტად ძვირადღირებული ორგანიზაციისთვის. სხვა ისეთ ასპექტებს, როგორიცაა მაგალითად პერვონალის ერთი ჯგუფის მიერ მეორე ჯგუფის წევრების დისკრიმინაციის ტენდენცია, შესაძლოა დიდი მნიშვნელობა ქონდეთ უსაფთხოების პოლიტიკისა და პრაქტიკისათვის. სამუშაოსთვის სწორად შერჩეული ადამიანების დაქირავების საჭიროებამ შეიძლება გამოიწვიოს სამუშაოზე მათი აყვანა უსაფრთხოების გადამოწმების დასრულებამდე. სამუშაოზე აყვანამდე უსაფრთხოების გადამოწმების დასრულება არის ნორმალური (სტანდარტული) და ყველაზე უსაფრთხო წესი.

***<u>არსებული და ახალი კონტროლის მექანიზმების ინტეგრირებით განპირობებული შეზღუდვები:</u>***

ახალი კონტროლის მექანიზმების ინტეგრაცია არსებულ ინფრასტრუქტურაში და კონტროლის მექანიზმების ერთმანეთზე დამოკიდებულება ხშირად უყურადღებოდაა დატოვებული. ახალი კონტროლი მექანიზმები ადვილად ვერ დაინერგება, თუ ადგილი აქვს შეუსაბამობას ან არსებულ კონტროლის მექანიზმებთან შეუთავსებლობას. მაგალითად, ბიომეტრული მახასიათებლების გამოყენების გეგმამ ფიზიკური წვდომის კონტროლისთვის შეიძლება გამოიწვიოს კონფლიქტი არსებულ PIN-ზე დაფუძნებულ სისტემასთან. არსებული კონტროლის მექანიზმების დაგეგმილი კონტროლის მექანიზმებით შეცვლის ხარჯი უნდა შეიცავდეს იმ ელემენტებს, რომლებიც უნდა დაემატოს რისკების აღმოფხვრის საერთო ხარჯებს. შერჩეული კონტროლის მექანიზმი შესაძლოა არ განხორციელდეს არსებული კონტროლის მექანიზმებში ჩარევის გამო.