ინფორმაციული ტექნოლოგიების (IT) აუდიტის სახელმძღვანელო შიდა აუდიტორებისთვის

ვერსია 1.0

2023 წლის 29 მაისი

THE WORLD BANK

ევროკავშირი საქართველოსთვის
The European Union for Georgia

EY
Building a better working world

სარჩევი

აბრევიატურების ჩამონათვალი

BCP	ბიზნეს უწყვეტობის გეგმა / ბიზნესის უწყვეტობის დაგეგმვა
CAATs	აუდიტორული შემოწმების ჩატარების კომპიუტერიზებული მეთოდები
COBIT	კონტროლის ამოცანები ინფორმაციისა და მასთან დაკავშირებული ტექნოლოგიისთვის
ISACA	საინფორმაციო სისტემების აუდიტის და კონტროლის ასოციაცია
IT	ინფორმაციული ტექნოლოგიები
ITIL	ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის ბიბლიოთეკა
GTAG	შიდა აუდიტორთა ინსტიტუტის მიერ მომზადებული ინფორმაციული ტექნოლოგიების რისკის და კონტროლის სისტემები
IIA	შიდა აუდიტორთა ინსტიტუტი
IAU	შიდა აუდიტის ერთეული
PIFC	სახელმწიფო შიდა ფინანსური კონტროლი

ტერმინთა განმარტებები

აპლიკაცია	კონკრეტული პროცესის შესასრულებლად და მხარდასაჭერად გამოყენებული კონკრეტული პროგრამული უზრუნველყოფა
აპლიკაციის კონტროლი	მონაცემების შეყვანასთან, დამუშავებასთან და დამუშავების შედეგების მიღებასთან დაკავშირებული კონტროლი, რომელიც უნიკალურია თითოეული აპლიკაციისთვის
ავტომატური კონტროლები	კონტროლის სისტემა, რომელიც მოქმედებს ადამიანის ჩარევის გარეშე
ბენჩმარკინგი	ორგანიზაციის ან პროექტის შედარება მსგავს შიდა ან გარე ორგანიზაციებთან ან პროექტებთან, პოტენციური გაუმჯობესების სფეროების დადგენისა და საუკეთესო პრაქტიკის გამოსავლენად
კონტროლების გარემო	ხელმძღვანელობისა და უმაღლესი ზედამხედველობის ორგანოს დამოკიდებულება და ქმედებები ორგანიზაციის შიგნით კონტროლის მნიშვნელობასთან დაკავშირებით; უზრუნველყოფს დისციპლინას და სტრუქტურას შიდა კონტროლის სისტემის პირველადი მიზნების მისაღწევად
კონტროლების ჩარჩო	კონცეფციების აღიარებული სისტემა, რომელიც მოიცავს შიდა კონტროლის ყველა ელემენტს
მაკორექტირებელი კონტროლი	IT კონტროლი, რომელიც გამოიყენება შეცდომების, თაღლითობის ან კონტროლის სხვა პრობლემების აღმოჩენის შემდეგ ზიანის შესამსუბუქებლად
მონაცემთა ბაზა	მონაცემთა ნებისმიერი საცავი კომპიუტერულ სისტემაში
აღმომჩენი კონტროლი	რეაქციული კონტროლის ტიპი, რომელიც აღმოაჩენს მომხდარ არასასურველ მოვლენებს
დაშიფვრა	მათემატიკური ალგორითმის გამოყენება მონაცემების ისე დასაფარად, რომ მათი წაკითხვა შეუძლებელი იყოს ციფრული გასაღების კოდის გარეშე
უწყებრივი რესურსების დაგეგმვის (ე. წ. „ERP“) სისტემები	ბიზნეს აპლიკაციების მოდულური კომპლექტი, რომელიც შეუფერხებლად აზიარებს მონაცემებს მოდულებს შორის, ყველა მონაცემის ერთ საცავში შესანახად
ორგანიზაციული რისკის მართვა (ე. წ. „ERM")	სტრუქტურირებული, თანმიმდევრული და უწყვეტი პროცესი მთელი ორგანიზაციის მასშტაბით, შესაძლებლობების და საფრთხეების იდენტიფიცირებისა და შეფასებისთვის, ასევე მათზე რეაგირებასთან დაკავშირებით გადაწყვეტილების მისაღებად და ანგარიშგების განსახორციელებლად, რომლებიც გავლენას ახდენენ მისი ამოცანების მიღწევაზე

ბრანდმაუერი (ე.წ. „Firewall“)	ტექნიკური უზრუნველყოფის/პროგრამული უზრუნველყოფის კომბინაცია, რომელშიც გაივლის ყველა კომუნიკაცია გარედან შიგნით ან შიგნიდან გარეთ და ბლოკავს არაავტორიზებულ ტრაფიკს
ინფორმაციული რისკი	რისკი იმისა, რომ საქმიანი გადაწყვეტილების მიღებისას გამოყენებული იქნება არასწორი ინფორმაცია
საინფორმაციო სისტემა	სტრატეგიული, მმართველობითი და საოპერაციო საქმიანობების ერთობლიობა, რომელიც მოიცავს ინფორმაციის და მასთან დაკავშირებული ტექნოლოგიების შეგროვებას, დამუშავებას, შენახვას, გავრცელებასა და გამოყენებას
ინფორმაციული ტექნოლოგიები	ტექნიკური უზრუნველყოფა, პროგრამული უზრუნველყოფა, საკომუნიკაციო და სხვა საშუალებები, რომლებიც გამოიყენება მონაცემთა ნებისმიერი ფორმით შესაყვანად, შესანახად, დასამუშავებლად, გადასაცემად და მისაღებად
შიდა აუდიტის სამსახური	დაწესებულების სტრუქტურული ერთეული, რომელიც უფლებამოსილია განახორციელოს შიდა აუდიტი “სახელმწიფო შიდა ფინანსური კონტროლის შესახებ” (PIFC) კანონის შესაბამისად
ინტერნეტი	ქსელების ერთობლიობა, რომელშიც დამუშავების სიმძლავრის და მონაცემების ნაწილი განკუთვნილია საჯარო გამოყენებისთვის
IT ზოგადი კონტროლი (ე. წ. „ITGC“)	IT კონტროლი, რომელიც ზოგადად ვრცელდება IT გარემოზე ან სისტემების, ქსელების, მონაცემების, ადამიანებისა და პროცესების მთლიან ნაკრებზე
„გამომძალველი“ მავნე პროგრამა (ე. წ. „Ransomware“)	მავნე პროგრამული უზრუნველყოფა, რომელიც შიფრავს ყველა ფაილს კომპიუტერზე ან კომპიუტერულ ქსელში. დეშიფრაციის კოდის სანაცვლოდ დამნაშავე სთხოვს მომხმარებელს გარკვეული თანხის გადახდას
რისკი	მოვლენის მოხდენის შესაძლებლობა, რომელიც ზეგავლენას იქონიებს მიზნების მიღწევაზე; რისკის გაზომვა წარმოებს ზეგავლენისა და ალბათობის მიხედვით
რისკის მადა	რისკის დონე, რომლის მისაღებადაც ორგანიზაცია მზადაა დასახული მიზნების მიღწევის პროცესში
რისკის შეფასება	რისკის გამოვლენა, შეფასება და მისი პრიორიტეტის განსაზღვრის პროცესი ან რისკის საფუძველზე ალტერნატივების შერჩევა
რისკის მართვა	პოტენციური შემთხვევების ან ვითარებების გამოვლენის, შეფასების, მართვის და კონტროლის პროცესი ორგანიზაციის მიზნების მიღწევასთან დაკავშირებით გონივრული რწმუნების უზრუნველსაყოფად
რისკზე რეაგირება	რისკის სამართავად განხორციელებული ქმედებები

პროცესის გავლა (ე. წ. „Walkthrough”)	პასუხისმგებელი პირის მიერ შიდა აუდიტორის თანდასწრებით პროცესზე ან ამოცანაზე განხორციელებული პროცესის ან ამოცანის ეტაპობრივი დემონსტრირება ან განმარტება

სამუშაო ფაილების ინდექსაცია

#	აუდიტის ფაზა	პროცედურის ინდექსი	აუდიტის დოკუმენტის დასახელება	მაგალითები
1	დაგეგმვა	110	დაგეგმვის მემორანდუმი	
	დაგეგმვა	120	აუდიტის ინიცირების წერილი	
	დაგეგმვა	130	გახსნითი შეხვედრის ოქმი	
	დაგეგმვა	140	IT პროცესების, IT რისკებისა და IT კონტროლების შესწავლა	*140.1 SAP წვდომის მართვის პროცესი* *140.2 SAP technical manual (example)*
	დაგეგმვა	150 და შემდეგ	დაგეგმვის სხვა დოკუმენტები	
2	განხორციელება	210	აუდიტის სამუშაო პროგრამა	
	განხორციელება	220	კონტროლის ტესტირების ფორმა	*220.1 SAP Access Provisioning Testing* *220.2 SAP Regular Access Review Testing*
	განხორციელება	230	IT ძირითადი პროცედურის ტესტირების ფორმა	*230.1 SAP Access Deprovisioning Substantive Testing*
	განხორციელება	240	აპლიკაციის კონტროლის ტესტირების ფორმა	
	განხორციელება	250	აუდიტის მიგნებების მატრიცა	
	განხორციელება	260	დასკვნითი შეხვედრის ოქმი	
	განხორციელება	270 და შემდეგ	სხვა განხორციელების დოკუმენტები	
3	ანგარიშგება	310	IT აუდიტის ანგარიში	
	ანგარიშგება	320	შიდა აუდიტის ხარისხის მიმოხილვის სია	
	ანგარიშგება	330 და შემდეგ	სხვა საანგარიშო დოკუმენტები	

შესავალი

წინამდებარე სახელმძღვანელოში წარმოდგენილია რისკზე დაფუძნებული და კონტროლზე ორიენტირებული მიდგომა, რომელიც ხელს უწყობს შიდა აუდიტის სუბიექტის ხელმძღვანელს, ორგანიზაციის ყველაზე კრიტიკული რისკების მაქსიმალური მოცვით, შეასრულოს დასახული მიზნები და ამ ფორმით უზრუნველყოს ორგანიზაციისთვის დამატებითი ღირებულების შექმნა

დოკუმენტში განხილული აუდიტორული მიდგომა წარმოადგენს ძირითადი პრინციპების, მითითებებისა და ინსტრუმენტების ერთობლიობას და არა მკაცრად გაწერილ ინსტრუქციას, რომელიც უნდა შესრულდეს პროფესიონალური მსჯელობის გამოყენების გარეშე.

ზოგადად, აღნიშნული მიდგომით განხორციელებული აუდიტი უნდა შეესაბამებოდეს ქვემოთ მოცემულ სტანდარტულ პრინციპებს, რომლებიც დეტალურად არის განხილული წინამდებარე სახელმძღვანელოს მომდევნო თავებში:

- **მჭიდრო კონტაქტი პროცესის მფლობელებთან**: აღნიშნული ითვალისწინებს რეგულარულ და მნიშვნელოვან დიალოგს შიდა აუდიტის ობიექტის ხელმძღვანელობასთან აუდიტის დაწყებამდე, აუდიტის განხორციელების პროცესში და მისი დასრულების შემდეგ. სახელმძღვანელოთი გათვალისწინებული სავალდებულო შეხვედრები, შუალედურ შედეგებთან ერთად, მიზნად ისახავს ინფორმაციის აქტიური მიმოცვლის ხელშეწყობას აუდიტორული შეფასების ფარგლებში გამოვლენილი რისკების, პრობლემებისა და კონტროლის შესახებ. გარდა ამისა, აღნიშნული უზრუნველყოფს აუდიტორული შეფასების მსვლელობისას „სიურპრიზების“ ალბათობის შემცირებას;

- **რისკზე დაფუძნებული აუდიტორული მიდგომა**: ამ მიდგომის უმთავრეს ქვაკუთხედს წარმოადგენს რისკებისა და მათი შემცირების მიზნით ხელმძღვანელობის მიერ დანერგილი კონტროლის მექანიზმების გამოვლენა და ეფექტიანობისა და პროდუქტიულობის შეფასება;

- **რისკის საერთო კრიტერიუმები**: ნარჩენი რისკის დადგენა ხდება რისკების სტანდარტული ტაქსონომიის მიდგომის გამოყენებით;

- **კოორდინაცია სხვა ფუნქციურ ერთეულებთან**: შიდა აუდიტის სუბიექტი წარმოადგენს დამოუკიდებელ ერთეულს, რომელიც უშუალოდ ექვემდებარება ორგანიზაციის ხელმძღვანელს და კონტროლისა და მონიტორინგის პასუხისმგებლობის მქონე სხვა ფუნქციურ ერთეულებთან კოორდინაციით ცდილობს ობიექტური მხარდაჭერა გაუწიოს საჯარო უწყების ხელმძღვანელობას, მარეგულირებელს ან გარე აუდიტორებს;

- **ორიენტირება აუდიტორული საქმიანობის ხარისხზე:** წინამდებარე სახელმძღვანელოს მნიშვნელოვან ასპექტს წარმოადგენს ხარისხის დამოუკიდებელი უზრუნველყოფის / გადახედვის პროცესი, რომელიც პერიოდულად ხორციელდება აუდიტორული შეფასების სხვადასხვა ეტაპზე. აღნიშნული ორიენტირებულია აუდიტორული შეფასების შედეგების სტანდარტიზებასა და მუდმივ გაუმჯობესებაზე.

წინამდებარე სახელმძღვანელო წარმოადგენს საქართველოს ფინანსთა სამინისტროს ჰარმონიზაციის ცენტრის (შემდგომში „ჰარმონიზაციის ცენტრი“) საკუთრებას და ვრცელდება საჯარო სექტორის შიდა აუდიტის სუბიექტებზე.

სახელმძღვანელო გადაიხედება ჰარმონიზაციის ცენტრის მიერ მინიმუმ წელიწადში ერთხელ. სახელმძღვანელოს ნებისმიერი ცვლილება მტკიცდება ჰარმონიზაციის ცენტრის მიერ და ემსახურება საჯარო სექტორის შიდა IT აუდიტორული შემოწმებების განხორციელების პრაქტიკებზე ზეგავლენის მქონე აუდიტორული მიდგომებისა ან მეთოდოლოგიური ცვლილების ზუსტ ასახვას და ყველა დაინტერესებული მხარის დროულ და ეფექტურ ინფორმირებას.

1 ინფორმაციული ტექნოლოგიების (IT) აუდიტის მიმოხილვა

საჯარო უწყებები სულ უფრო ხშირად მიმართავენ ინოვაციური ინფორმაციული ტექნოლოგიების (IT) გამოყენებას, რათა უზრუნველყონ მათი ფუნქციონირებისა და მათ მიერ გაწეული საჯარო სერვისების ეფექტიანობა და პროდუქტიულობა. გარდა ამისა, საჯარო სერვისების მიწოდების ფორმა სწრაფად იცვლება და ფიზიკური გარემოდან გადადის ციფრულ გარემოში. აღნიშნული მოითხოვს მთავრობებისგან სერვისების მიმწოდებელ, ერთგვარ ციფრულ პლატფორმად ჩამოყალიბებას და საინფორმაციო სისტემების ფუნქციონირებისთვის საჭირო ინფრასტრუქტურის უზრუნველყოფას.

ამასთანავე, რელევანტური და სანდო ინფორმაციის ხელმისაწვდომობა უმნიშვნელოვანეს ფაქტორს წარმოადგენს ინფორმირებული და ობიექტური გადაწყვეტილებების მიღების პროცესში. ინფორმაციის რელევანტურობა უზრუნველყოფილია ინფორმაციის დროულობითა და მისი დეტალიზების ხარისხით. გამოყენებული ინფორმაციული ტექნოლოგიები აჩქარებენ ინფორმაციის ხელმისაწვდომობას, ახდენენ მონაცემთა დახარისხებისა და დამუშავების ავტომატიზაციას და უზრუნველყოფენ მათ სიზუსტესა და მთლიანობას.

ზემოთ აღნიშნულის გათვალისწინებით, ეფექტური ეფექტიანი ინფორმაციული ტექნოლოგიების გამოყენება საშუალებას აძლევს საჯარო უწყებებს:

- უზრუნველყონ საქმიანობის მიზნების მიღწევა; შესრულება;
- გამოავლინონ და სათანადო რეაგირება მოახდინონ რისკებზე;
- უზრუნველყონ ორგანიზაციის შეუფერხებელი ზრდა და ადაპტირდნენ ახალ რეალობაში;
- ჰქონდეთ ეფექტური კომუნიკაცია ორგანიზაციის შიგნით და გარეთ;
- დროული რეაგირება ახლად წარმოქმნილ შესაძლებლობებზე.

კომპიუტერიზებულ საინფორმაციო სისტემებსა და მონაცემთა დამუშავების ციფრულ ფორმებზე გადასვლამ გამოიწვია მნიშვნელოვანი ტრანსფორმაცია იმ გარემოსი, რომელში ოპერირებაც უწევთ შიდა აუდიტის სუბიექტებს. შესაბამისად, შიდა აუდიტისთვის გადამწყვეტი მნიშვნელობა ენიჭება რთულ საინფორმაციო სისტემებთან დაკავშირებული რისკებისა და კონტროლის შეფასებისთვის საჭირო, სათანადო შესაძლებლობების და მიდგომების განვითარებას.

1.1 შიდა აუდიტის უფლებამოსილება

შიდა IT აუდიტი გადამწყვეტ როლს თამაშობს IT კონტროლის გარემოს მონიტორინგში იმის დასადასტურებლად, რომ აღნიშნული კონტროლის მექანიზმები მუშაობს დანიშნულებისამებრ და ამცირებს არსებულ რისკებს მისაღებ დონემდე. გარდა ამისა, IT აუდიტორები კონსულტაციას უწევენ ხელმძღვანელობას რისკის მართვის, შიდა კონტროლის საკითხებსა და სტანდარტული პრაქტიკების შესახებ. შესაძლოა, მონაწილეობა მიიღონ ამ სფეროებთან დაკავშირებულ სპეციალურ საკონსულტაციო პროექტებში.

აღნიშნული აქტივობები, ერთობლიობაში, ხელმძღვანელობას აწვდიან ტექნოლოგიებთან დაკავშირებულ შიდა კონტროლის სისტემის მიუკერძოებელ და ობიექტურ შეფასებას, ხელს

უწყობენ რისკის მართვის პროცესს და გარე დაინტერესებული მხარეების (მაგ., მარეგულირებლები, გარე აუდიტორები) მოლოდინების დაკმაყოფილებას.

როგორც წესი, შიდა აუდიტის სუბიექტი ახორციელებს ორი სახის მომსახურებას: მარწმუნებელი (აუდიტორული) და საკონსულტაციო.

საკონსულტაციო მომსახურება სრულდება კონკრეტული მოთხოვნების საფუძველზე, მიუხედავად იმისა, ფორმალიზებულია თუ არა მოთხოვნა. საკონსულტაციო მომსახურების გაწევისას, აუცილებელია, შიდა აუდიტორმა დაიცვას მიუკერძოებლობა და არ შეითავსოს მმართველობითი უფლებამოსილებები.

მარწმუნებელი IT აუდიტის განხორციელების პროცესი განხილულია მომდევნო თავებში.

შიდა აუდიტორის მოვალეობაა სამუშაოს შესრულებისას დაიცვას ეთიკის წესები და გამოიჩინოს პატიოსნება, მიუკერძოებლობა, ობიექტურობა, დამოუკიდებლობა, კონფიდენციალურობა და კომპეტენტურობა. გარდა ამ წესებისა, შიდა აუდიტორები პასუხისმგებელნი არიან, დაიცვან შიდა აუდიტორთა საერთაშორისო ინსტიტუტის (IIA), საინფორმაციო სისტემების აუდიტისა და კონტროლის ასოციაციისა (ISACA) და საქართველოს მთავრობის 2010 წლის 30 ივლისის N1016 „შიდა აუდიტორთან ეთიკის კოდექსის დამტკიცების შესახებ“ განკარგულების მიერ დადგენილი ეთიკის ნორმები, რომლებიც მოითხოვს შემდეგს:

- პროფესიული საქმიანობის შესრულებისას შიდა აუდიტორმა უნდა გამოიჩინოს პასუხისმგებლობა, დამოუკიდებლობა და კეთილსინდისიერება;
- არ უნდა მიიღონ შეგნებულად მონაწილეობა ისეთ უკანონო საქმიანობაში ან ჩაერთონ ისეთ ქმედებებში, რომლებითაც მოხდება შიდა აუდიტორის პროფესიის ან მისი დაწესებულების დისკრედიტაცია;
- შიდა აუდიტორი არ უნდა ეწეოდეს ისეთ საქმიანობას ან შევიდეს ისეთ ურთიერთობაში, რომელსაც შესაძლოა ჰქონდეს უარყოფითი ზეგავლენა. შიდა აუდიტორმა უნდა მოამზადოს ზუსტი და ობიექტური აუდიტორული ანგარიშები, რომლებიც ემყარება აუდიტორული სტანდარტების შესაბამისად მოპოვებული მტკიცებულებების გაერთიანებას და შეფასებას;
- პროფესიული ან სამართლებრივი ვალდებულების ფარგლებში, შიდა აუდიტორმა უნდა დაიცვას მიღებული ინფორმაციის ღირებულება და კონფიდენციალურობა და, საჭირო თანხმობისა და ავტორიზაციის მიღების გარეშე, არ უნდა გაუზიაროს სხვებს სამსახურებრივი ინფორმაცია;
- შიდა აუდიტორს უნდა ჰქონდეს შიდა აუდიტის ჩასატარებლად საჭირო ცოდნა და უნარები და უნდა ასრულებდეს მხოლოდ იმ სამუშაოს, რომლის შესასრულებლადაც მას გააჩნია საკმარისი ცოდნა, უნარები და გამოცდილება. IT აუდიტის ჩატარებაზე პასუხისმგებელი შიდა აუდიტორი პასუხისმგებელია საკუთარი პროფესიული კომპეტენციების მუდმივ გაუმჯობესებაზე;
- თუ IT აუდიტი ტარდება გუნდური ძალისხმევით, შიდა აუდიტის ჯგუფის უფროსმა უნდა უზრუნველყოს, რომ ჯგუფის წევრების საქმიანობა შეესაბამებოდეს პროფესიული ეთიკის მოთხოვნებს. შიდა აუდიტორი უნდა გაუმკლავდეს აუდიტის დროს წარმოქმნილ ნებისმიერ პრობლემას პროფესიული ეთიკისა და აუდიტის სტანდარტების შესაბამისად;

- იმ შიდა აუდიტორის მიმართ, რომელიც არ ემორჩილება პროფესიული ეთიკის მოთხოვნებს ან აუდიტის სტანდარტებს, უნდა გატარდეს დისციპლინარული ღონისძიებები;
- შიდა აუდიტორი პასუხისმგებელია, თვალი ადევნოს და დაიცვას ეთიკის კოდექსში განხორციელებული ცვლილებები.

1.2 IT აუდიტის მიზნები

IT აუდიტის მიზნები[1] მოიცავს შემდეგს:

- შესაბამისი ზოგადი კონტროლებისა და აპლიკაციის კონტროლების შეფასებას, რომლებიც გავლენას ახდენენ ინფორმაციული სისტემების მონაცემების სისრულეზე და სანდოობაზე, რაც, თავის მხრივ, გავლენას ახდენს შიდა აუდიტის ობიექტის ფინანსურ და სხვა ტიპის ანგარიშგებაზე და გადაწყვეტილების მიღების პროცესზე;
- რწმუნების გაცემას IT პროცესების შიდა აუდიტის ობიექტისთვის რელევანტურ სხვადასხვა კანონთან, მარეგულირებელ სტანდარტთან ან შიდა პოლიტიკასთან შესაბამისობის თაობაზე;
- რწმუნების გაცემას იმის თაობაზე, რომ IT რესურსები იძლევა ორგანიზაციის მიზნების ეფექტიანად და პროდუქტიულად მიღწევის შესაძლებლობას, და რომ შესაბამისი ზოგადი და აპლიკაციის კონტროლები ეფექტურია საინფორმაციო სისტემების გამოყენებასა და მართვაში ხარვეზების გამოვლენაში, პრევენციასა და გამოსწორებაში.

1.3 შიდა IT აუდიტის მასშტაბი

შიდა IT აუდიტის მასშტაბის განსაზღვრა გულისხმობს გადაწყვეტილების მიღებას შიდა აუდიტორული შემოწმების დონის, IT სისტემების და მათი ფუნქციონალის, IT პროცესების, მდებარეობებისა და აუდიტირებადი პერიოდის შესახებ. არსებითად, ეს პროცესი მოიცავს შიდა აუდიტის საზღვრების დადგენას.

ზოგადად, შიდა IT აუდიტს შესაძლოა ჰქონდეს საინფორმაციო სისტემებისა და პროცედურების დამოუკიდებელი შეფასების ფორმა ან განხორციელდეს ინტეგრირებული აუდიტის (მაგ., ფინანსური აუდიტი, ეფექტიანობის აუდიტი ან შესაბამისობის აუდიტი) ფარგლებში.

ფინანსური აუდიტი

შიდა აუდიტის ობიექტის ბუღალტრული აღრიცხვისა და ფინანსური ანგარიშგების შემოწმება საქართველოს კანონმდებლობასთან და სტანდარტებთან მათი შესაბამისობის დადგენის მიზნით. თავის მხრივ, შიდა IT აუდიტორის როლი მდგომარეობს იმაში, რომ შეაფასოს, რამდენად უზრუნველყოფენ ფინანსური ანგარიშგების პროცესებთან დაკავშირებული IT სისტემები და მათი IT კომპონენტები ფინანსური მონაცემების სისრულესა და სიზუსტეს.

[1] უმაღლესი აუდიტორული დაწესებულებების საერთაშორისო ორგანიზაციის (ე. წ. „INTOSAI“) საინფორმაციო სისტემების შესახებ სახელმძღვანელო (GUID 5100)

ეფექტიანობის აუდიტი

შიდა აუდიტის ობიექტის მიერ განხორციელებული ღონისძიებების, ოპერაციების, პროგრამების, დაწესებულების ორგანიზაციული მოწყობისა და სისტემების ობიექტური და საიმედო შეფასება მათი ეკონომიურობის, პროდუქტიულობისა და ეფექტიანობის პრინციპებთან შესაბამისობის დადგენისა და გაუმჯობესების პოტენციალის გამოვლენის მიზნით. თავის მხრივ, შიდა IT აუდიტორის როლი მდგომარეობს იმაშიც, რომ შეაფასოს, რამდენად აკმაყოფილებს გამოყენებული IT სისტემა მომხმარებელთა საჭიროებებს, ხომ არ აყენებს სისტემა ორგანიზაციას გაუმართლებელი რისკის წინაშე და რამდენად ქმნის სისტემა მოქალაქეებისთვის დათქმულ ღირებულებას.

შესაბამისობის აუდიტი

დაწესებულების საქმიანობის პოლიტიკასთან, გეგმებთან, პროცედურებთან, კანონებსა და სხვა მარეგულირებელ აქტებთან შესაბამისობის შემოწმება და შეფასება. შიდა IT აუდიტორის როლია, შეაფასოს შიდა აუდიტის ობიექტის IT სისტემების, IT პროცესებისა და კონტროლის მექანიზმების შესაბამისობა აუდიტის კრიტერიუმთან.

1.4 ინფორმაციული ტექნოლოგიების (IT) გამოყენებასთან დაკავშირებული რისკები

IT სამსახურის, ისევე როგორც შიდა აუდიტის, უპირველესი ინტერესის საგანს წარმოადგენს ინფორმაციასთან დაკავშირებული რისკები, მაგალითად, არაზუსტ ინფორმაციაზე დაყრდნობით გადაწყვეტილების მიღება. ინფორმაციული ტექნოლოგიების ფართომასშტაბიანმა ინტეგრაციამ ბიზნეს პროცესებში განაპირობა შიდა აუდიტის მიდგომის ცვლილება, კერძოდ, დროის კონკრეტულ მომენტში ისტორიულ მონაცემებზე რწმუნების გაცემის ნაცვლად სულ უფრო მეტად გამოიყენება მონაცემთა დამუშავების არსებული პროცესების სანდოობის შეფასება. თუ პროცესი არასწორად არის განსაზღვრული, შესაბამისად, მის მიერ წარმოებული მონაცემებიც ვერ იქნება სანდო.

ზოგადად, ინფორმაციული ტექნოლოგიების გამოყენება იძლევა ხელით შესრულებულ პროცესებთან დაკავშირებული რისკების მინიმუმამდე დაყვანის შესაძლებლობას, თუმცა ამავდროულად მას თან ახლავს სპეციფიკური რისკები, რომელიც შიდა აუდიტის მხრიდან მოითხოვს განსაკუთრებულ ყურადღებას. მსგავსი სპეციფიკური რისკების რამდენიმე მაგალითი მოცემულია ქვემოთ:

- **მატერიალური აუდიტირებადი კვალის ციფრულით ჩანაცვლება.** რიგ შემთხვევაში, შიდა აუდიტის ფარგლებში მატერიალური მტკიცებულები არ არის ხელმისაწვდომი, შესაბამისად, საჭიროა მათი მაკომპენსირებელი ციფრული მტკიცებულებების გამოვლენა და ტესტირება;
- **აპარატურული / პროგრამული უზრუნველყოფის გაუმართაობა.** მონაცემთა სამუდამო დაკარგვა (მაგ., გარემო პირობებით გამოწვეული დაზიანების, ელექტროენერგიის გათიშვა, სამოქალაქო არეულობა, ე. წ. „Ransomware“, და ბუნებრივი კატასტროფები) დაკავშირებულია დიდ ხარჯებთან;

- **სისტემური შეცდომები.** ინფორმაციული ტექნოლოგიების გამოყენება ამცირებს შემთხვევით შეცდომების (მაგ., სისტემაში მონაცემთა არასწორად შეყვანა) რიცხვს, მაგრამ, ამასთანავე, გაუმართავი კოდის შემთხვევაში, შესაძლოა გამოიწვიოს კონკრეტული ტიპის შეცდომების ავტომატური დუბლირება;
- **ადამიანის მხრიდან ნაკლები ჩართულობა.** IT სისტემები, ავტომატიზაციის საშუალებების გამოყენებით, ამცირებს ადამიანურ რესურსებზე გაწეულ ხარჯებს. თუმცა პრობლემების გამოვლენა მოითხოვს საბოლოო მომხმარებლების მხრიდან სისტემის მიერ დაბრუნებული მონაცემების ანალიზს აგრეგაციის შეძლებისდაგვარად დაბალ დონეზე;
- **წვდომის ავტორიზაცია.** სენსიტიურ ინფორმაციაზე დისტანციურად წვდომის გაზრდილი შესაძლებლობა, ასევე ზრდის არაავტორიზებული წვდომის რისკს;
- **ტრანზაქციების ავტომატური ავტორიზაცია.** ინფორმაციული სისტემები იძლევა ისეთი ოპერაციების ავტომატიზაციის შესაძლებლობას, რომლებიც ადრე საჭიროებდა პასუხისმგებელი პირის მიერ განხილვასა და ავტორიზებას. ავტორიზაციის ფუნქციონალის ეფექტურობაზე რწმუნების გაცემა დამოკიდებულია აპლიკაციის კონტროლებისა და შეყვანილი ინფორმაციის მთლიანობაზე;
- **განზრახ განხორციელებული დამაზიანებელი ქმედებები.** გარე პირებმა შეიძლება მნიშვნელოვანი ზიანი მიაყენონ ორგანიზაციას. ორგანიზაციის ნდობით აღჭურვილი, შიდა პირები კიდევ ერთი მნიშვნელოვანი საფრთხის მატარებელი წყაროა.

1.5 IT კონტროლის მექანიზმების მიმოხილვა

IT კონტროლის მექანიზმები უზრუნველყოფენ რწმუნებას ინფორმაციასა და ინფორმაციული სერვისების შესახებ და ხელს უწყობენ ორგანიზაციის მიერ ინფორმაციული ტექნოლოგიების გამოყენებასთან დაკავშირებული რისკების კონტროლს და შემცირებას.

ეფექტური IT კონტროლი უზრუნველყოფს უწყვეტ რწმუნებას, რომელიც გამყარებულია მტკიცებულებების საიმედო და უწყვეტი აუდიტირებადი კვალით. ტექნოლოგიების აუდიტის გლობალური სახელმძღვანელოს (GTAG 1) - „ინფორმაციული ტექნოლოგიების რისკი და კონტროლები“ - თანახმად, IT კონტროლების ამოცანაა უზრუნველყოს:

- მოქმედ რეგულაციებთან და კანონმდებლობასთან შესაბამისობა;
- ორგანიზაციის მიზნებთან შესაბამისობა;
- მონაცემთა სანდოობა.

აღნიშნული კონტროლები მოიცავს წერილობით პოლიტიკებს და მათ დანერგვას კოდირებულ ინსტრუქციებში, ფიზიკური წვდომის დაცვას და პასუხისმგებელი პირების მოქმედებებსა და ტრანზაქციებს, ავტომატურ რედაქტირებას და დიდი მოცულობის მონაცემების გონივრულ ანალიზს და ა. შ.

IT კონტროლის მექანიზმების მიზნები

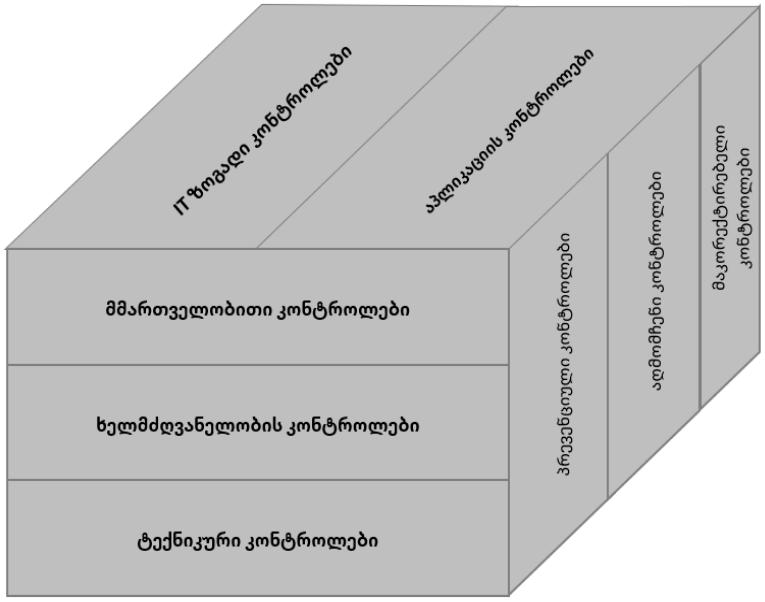
შიდა IT კონტროლის მიზნებია:

- ინფორმაციული აქტივების და რესურსების დაცვა;
- ინფორმაციის ხელმისაწვდომობა, სანდოობა და მასზე წვდომის სათანადო შეზღუდულობა;
- შესრულებულ აქტივობებზე მომხმარებელთა ანგარიშვალდებულების უზრუნველყოფა;
- მომხმარებელთა კონფიდენციალურობისა და მაიდენტიფიცირებელი მონაცემების დაცვა;
- მონაცემთა და სისტემების მთლიანობის უზრუნველყოფა;
- ხელმძღვანელობისთვის რწმუნების გაცემა, რომ ავტომატიზებული პროცესები სათანადოდ კონტროლდება;
- აუდიტირებადი კვალის წარმოება ყველა ავტომატიზებული და მომხმარებლის მიერ ინიცირებული ტრანზაქციისთვის.

კონტროლების მექანიზმების კლასიფიკაცია

კონტროლის მექანიზმების კლასიფიკაცია ხელს უწყობს მათი დანიშნულების გააზრებას და შიდა კონტროლის ერთიან სისტემაში მათ სწორ პოზიციონირებას (იხ. *სურათი 1: კონტროლის კლასიფიკაციები*). სწორი კლასიფიცირება შიდა აუდიტორს ეხმარება, უპასუხოს შემდეგ მნიშვნელოვან კითხვებს: არის თუ არა აღმომჩენი კონტროლის მექანიზმი ადეკვატური იმ შეცდომების გამოვლენისთვის, რომელთა აღკვეთაც შესაძლოა ვერ მოხერხდეს არსებული პრევენციული კონტროლის მექანიზმის მიერ? არის თუ არა მაკორექტირებელი კონტროლის მექანიზმი საკმარისი გამოვლენილი შეცდომების გამოსასწორებლად? რამდენად ეფექტურად შეუძლია პრევენციული კონტროლის მექანიზმს აპლიკაციის შეცდომების თავიდან არიდება?

კონტროლის მექანიზმების კლასიფიკაცია ხდება N1 დიაგრამაზე მოცემული კატეგორიების მიხედვით:



დიაგრამა 1: *კონტროლის მექანიზმების კლასიფიკაციები (წყარო: Global Technology Audit Guide (GTAG) 1, "Information Technology Risk and Controls," 2nd Edition)*

IT ზოგადი კონტროლები (ე. წ. „IT General Controls (ITGC)") და აპლიკაციის კონტროლები

- ზოგადი კონტროლის მექანიზმები ვრცელდება სისტემის ყველა კომპონენტზე, პროცესსა და მონაცემზე. ზოგადი კონტროლის მექანიზმები მოიცავს ისეთ სფეროებს, როგორიცაა: IT მმართველობა, რისკების მართვა, რესურსების მართვა, IT ოპერაციები, აპლიკაციების შემუშავება და მხარდაჭერა, მომხმარებლის მართვა, წვდომის უსაფრთხოება, ფიზიკური უსაფრთხოება, ცვლილებების მართვა, სარეზერვო ასლების მართვა და აღდგენა და ბიზნესის უწყვეტობა. ზოგადი კონტროლის მექანიზმების ნაწილი დაკავშირებულია საქმიანობასთან (მაგ., შეუთავსებელი მოვალეობების გამიჯვნა ან მმართველობის მექანიზმები), თუმცა მათი უმეტესობა სრულად ტექნიკურია (მაგ., პროგრამული ან ქსელის პროგრამული უზრუნველყოფის კონტროლი) და დამოკიდებულია მხარდამჭერ ინფრასტრუქტურაზე. ამგვარი კონტროლები არის შიდა აუდიტის ყურადღების საგანი, რადგან სწორედ ისინი, ერთობლიობაში ქმნიან ორგანიზაციის IT კონტროლების გარემოს. სუსტი და არასანდო ზოგადი კონტროლის მექანიზმების შემთხვევაში, შიდა აუდიტორს შესაძლოა მოუწიოს ტესტირების მიდგომის ცვლილება იმ სფეროებისთვის, რომლებზეც ზეგავლენას ახდენს არაეფექტური კონტროლის მექანიზმი;
- აპლიკაციის კონტროლი წარმოადგენს კონკრეტულ ბიზნეს პროცესთან ან სისტემასთან დაკავშირებულ ფუნქციონალს, რომელიც უზრუნველყოფს სისტემაში

მონაცემთა შეყვანის, დამუშავებისა და დაბრუნების კონტროლს. აპლიკაციის კონტროლი ასევე შეიძლება მოიცავდეს მონაცემთა რედაქტირებას, ბიზნეს-ფუნქციების გამიჯვნას (მაგ., ტრანზაქციის ინიცირება და ავტორიზაცია), ჯამური ბალანსების შედარებას, ტრანზაქციების აღრიცხვას და შეცდომების ანგარიშგებას. აპლიკაციის კონტროლი შესაძლოა იყოს სრულად ავტომატიზებული ან მოითხოვდეს ადამიანის ჩართულობას (მაგ., IT აპლიკაციის მიერ შესყიდვის ღირებულების გათვალისწინებით ტრანზაქციების სხვადასხვა პასუხისმგებელ პირებთან დამისამართება, მათი შემდგომი განხილვისა და დადასტურების მიზნით).

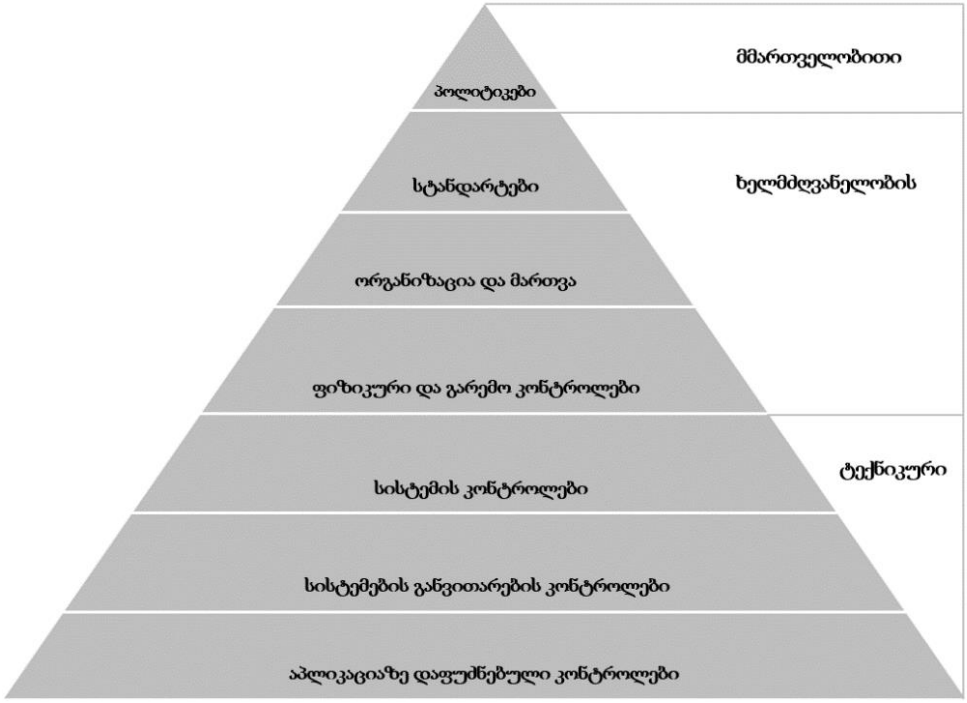
პრევენციული, აღმომჩენი და მაკორექტირებელი კონტროლის მექანიზმები

- პრევენციული კონტროლის მექანიზმების დანიშნულებაა თაღლითობის ან შეცდომების აღმოფხვრა მათ რეალიზებამდე. ამგვარი კონტროლის მექანიზმების მაგალითებს წარმოადგენს: ქსელური ეკრანი / ბრანდმაუერი (ე. წ. „Firewall“), სისტემებში მონაცემების შეყვანის ავტომატური ვალიდაცია (მაგ., თარიღის მხოლოდ წინასწარ განსაზღვრული ფორმატით შეყვანის შესაძლებლობა) ან პრივილეგირებულ ფუნქციებზე წვდომის მინიჭება მხოლოდ იმ პირებისთვის, რომლებიც საჭიროებენ ამგვარ წვდომას სამუშაო აღწერილობიდან გამომდინარე;
- აღმომჩენი კონტროლის მექანიზმების დანიშნულება შეცდომების / ხარვეზების დროული და ადეკვატური გამოვლენა, რომელთა აღკვეთაც ვერ მოხერხდა პრევენციული კონტროლის მექანიზმის საშუალებით. ისინი ამოქმედდებიან ხარვეზის წარმოშობის შემთხვევაში ან შესაძლოა ხორციელდებოდეს გარკვეული პერიოდულობით (მაგ., მომხმარებელთა წვდომის რეგულარული გადახედვა);
- მაკორექტირებელი კონტროლის მექანიზმები გამოიყენება ხარვეზების ან კონტროლის სხვა პრობლემების გამოვლენის შემთხვევაში. აღნიშნული კატეგორია მოიცავს კონტროლის მექანიზმების ფართო სპექტრს ხარვეზის გამოსწორების ავტომატური ფუნქციონალიდან ბიზნესის უწყვეტობის გეგმამდე, რომლის გააქტიურებაც ხდება საქმიანობის ოპერაციების და/ან დაკავშირებული IT რესურსების ხანგრძლივი პერიოდით შეფერხებისას. მაკორექტირებელი კონტროლის მექანიზმის მაგალითს წარმოადგენს, მომხმარებლების რეგულარული გადახედვის ფარგლებში გამოვლენილი არასაჭირო მომხმარებლების დროული გაუქმება.

IT მმართველობითი, ხელმძღვანელობის და ტექნიკური კონტროლის მექანიზმები

როლებისა და პასუხისმგებლობების შესაფასებლად, IT კონტროლები იყოფა სამ იერარქიულ დონედ: მმართველობითი, ხელმძღვანელობის და ტექნიკური.

აღნიშნული იერარქიული მოწყობა ხელს უწყობს, ერთის მხრივ, დასანერგი კონტროლის მექანიზმების შერჩევას და მეორეს მხრივ, IT საოპერაციო გარემოს შეფასებისას იმ სფეროების გამოვლენას, რომლებზეც ყურადღება უნდა გაამახვილოს შიდა IT აუდიტმა. იერარქიის კონტროლის მექანიზმების სხვადასხვა ტიპების იერარქიული სტრუქტურა წარმოდგენილია ქვემოთ მოცემულ დიაგრამა 2-ზე.



დიაგრამა 21: *IT კონტროლის მექანიზმების იერარქია (წყარო: Global Technology Audit Guide (GTAG) 1, "Information Technology Risk and Controls," 2nd Edition)*

- **მმართველობითი კონტროლის მექანიზმები** ემსახურება ზედამხედველობას და არა კონტროლების უშუალოდ განხორციელებას. მათზე პასუხისმგებლობა ეკისრება საჯარო დაწესებულების ხელმძღვანელს. ამის მაგალითს წარმოადგენს პოლიტიკები, რომლებიც განსაზღვრავენ, როგორ უნდა მოხდეს საჯარო დაწესებულების მასშტაბით ინფორმაციული ტექნოლოგიების სწორად გამოყენება, მონაცემთა უსაფრთხო დამუშავება, პროგრამული უზრუნველყოფის შემუშავება, ბიზნეს უწყვეტობის მართვა და ა. შ. პოლიტიკა უნდა დამტკიცდეს საჯარო დაწესებულების ხელმძღვანელის მიერ, უნდა იყოს გაზიარებული ყველა დაინტერესებულ მხარესთან და უზრუნველყოფდეს სწორი მოლოდინების ჩამოყალიბებას;
- **ხელმძღვანელობის კონტროლის მექანიზმები** ორიენტირებულნი არიან ორგანიზაციის პროცესების, ოპერაციების, აქტივებისა და სენსიტიური მონაცემების არსებული რისკების გამოვლენაზე, პრიორიტეტების განსაზღვრასა და შემცირებაზე. ამგვარ კონტროლის მექანიზმებს ფართო კავშირი აქვთ ორგანიზაციის სხვადასხვა სფეროსთან, რაც მოითხოვს ეფექტურ თანამშრომლობას ყველა დაინტერესებულ მხარეს შორის (მაგ., საჯარო დაწესებულების ხელმძღვანელის მოადგილეები). აღნიშნული მოიცავს შემდეგ დონეებს:
    - **სტანდარტები:** სისტემების შემუშავების (როგორც ორგანიზაციის შიგნით შემუშავებული, ასევე მესამე მხარეებისგან შეძენილი), პროგრამული უზრუნველყოფის კონფიგურაციის, აპლიკაციის კონტროლების, მონაცემთა არქიტექტურის სტანდარტები;

- **ორგანიზაცია და მართვა:** პასუხისმგებლობისა და ანგარიშვალდებულების მექანიზმების ორგანიზება და მართვა, შეუსაბამო მოვალეობების გამიჯვნის ჩათვლით, IT ინვესტიციების ფინანსური კონტროლი, IT ცვლილებების მართვა, პერსონალის კონტროლი და ა. შ.
- **ფიზიკური და გარემო უსაფრთხოება:** ფიზიკური და გარემოს კონტროლები გამოიყენება ისეთ საფრთხეებთან დაკავშირებული პოტენციური რისკების შესამცირებლად, როგორიც არის ხანძარი, მიწისძვრა, ან არაავტორიზებული წვდომა.
- **ტექნიკური კონტროლის მექანიზმები** მოიცავს დარჩენილ სამ დონეს და წარმოადგენს ფუნდამენტს თითქმის ყველა სხვა ორგანიზაციული IT კონტროლისთვის. მათი გამართულად მუშაობა უმნიშვნელოვანესია არსებული მმართველობითი და ხელმძღვანელობის კონტროლის მექანიზმების ეფექტურობის უზრუნველსაყოფად:
- **სისტემების კონტროლის მექანიზმები**, რომლებიც იძლევიან წვდომის უფლებების მართვის, შეუსაბამო მოვალეობების გამიჯვნის, სისტემებში შეღწევის პრევენციისა და გამოვლენის, მონაცემთა დაშიფვრის და ცვლილების მართვის შესაძლებლობას;

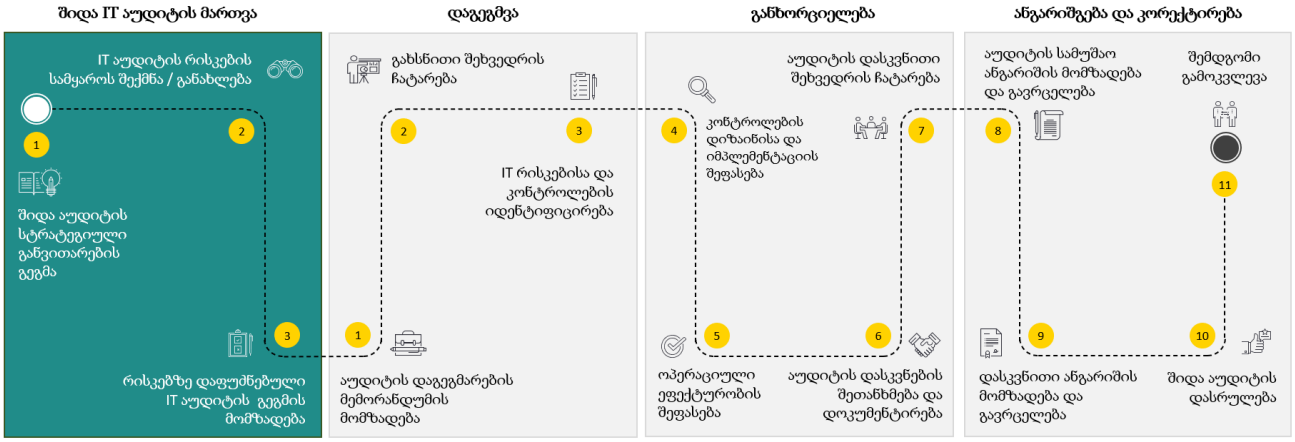
- **სისტემების განვითარების კონტროლის მექანიზმები**, მაგალითად, მომხმარებლის ტექნიკური მოთხოვნების დოკუმენტირება და მათი შესრულების დადასტურება, პროგრამული უზრუნველყოფის ტესტირება და სათანადო ტექნიკურ მხარდაჭერა და ა. შ.

- **აპლიკაციებზე დაფუძნებული კონტროლის მექანიზმები**, რომელიც უზრუნველყოფს სისტემაში შეყვანილი მონაცემის სიზუსტეს, სისრულეს, სისწორეს და მათი დანიშნულებისამებრ დამუშავებას; სისტემის მიერ დაბრუნებული მონაცემის სიზუსტეს და სისრულეს; მონაცემთა დამუშავების სრული სასიცოცხლო ციკლის კონტროლს.

კონტროლების კლასიფიკაცია ეხმარება შიდა აუდიტორებს კონტროლის მიზნისა და შიდა კონტროლის მთლიან სისტემაში მათი დანიშნულების უკეთ გაანალიზებაში და პასუხისმგებელი მხარეებისა და მათი ფუნქციების დადგენაში. აღნიშულის დახმარებით შიდა აუდიტს აქვს უკეთესი აღქმა იმისა, თუ როგორ არის მოწყობილი ორგანიზაციებში გამოყენებული ინფორმაციული ტექნოლოგიები.

1.6 IT აუდიტის პროცესი

ქვემოთ მოცემულ დიაგრამაზე ნაჩვენებია IT აუდიტის ზოგადი პროცესი, რომლის თითოეული ეტაპი დეტალურად არის განხილული მომდევნო თავებში:



დიაგრამა 3: *IT აუდიტის ძირითადი ეტაპებისა და აქტივობების სტანდარტიზებული და თანმიმდევრული ბლოკ-სქემა*

2 შიდა IT აუდიტის მართვა

დაგეგმვა წარმოადგენს შიდა აუდიტორული საქმიანობის უმნიშვნელოვანეს ეტაპს. წინამდებარე სახელმძღვანელო ითვალისწინებს შიდა IT აუდიტორული საქმიანობის დაგეგმვის სამ დონეს: შიდა აუდიტის სტრატეგიული დაგეგმვა, შიდა აუდიტის წლიური დაგეგმვა და შიდა აუდიტორული შემოწმების ინდივიდუალური გეგმა.

2.1 შიდა აუდიტის სტრატეგიული გეგმა

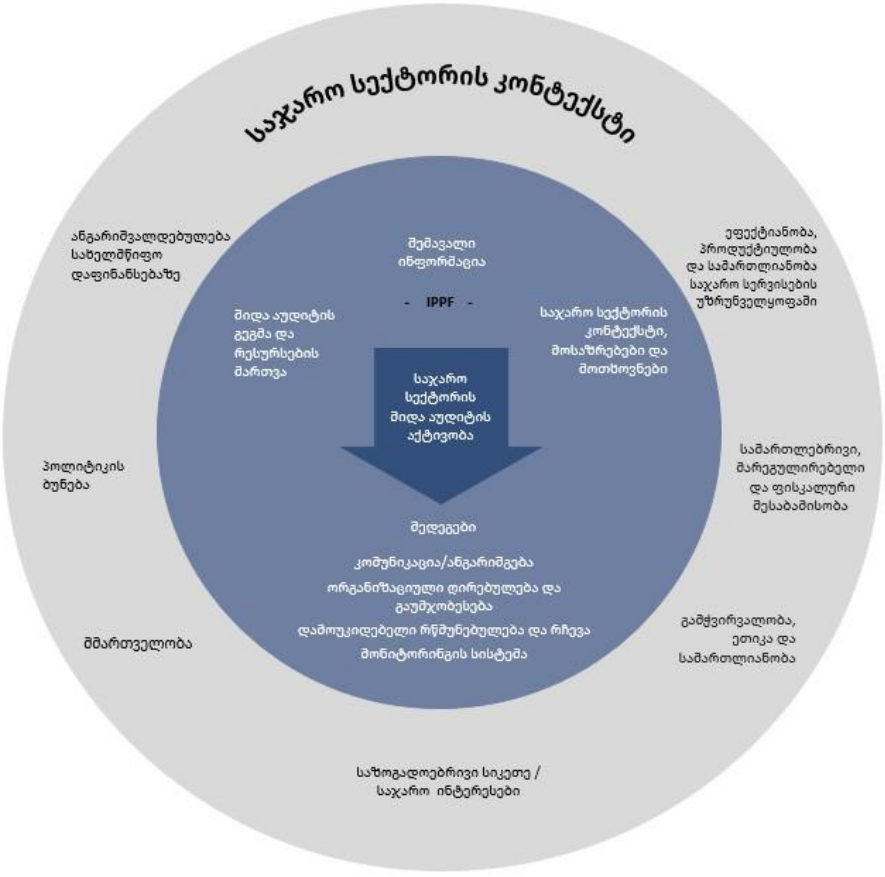
„სახელმწიფო შიდა ფინანსური კონტროლის შესახებ“ საქართველოს კანონის თანახმად, შიდა აუდიტის სტრატეგიულ გეგმას შეიმუშავებს შიდა აუდიტის სუბიექტის ხელმძღვანელი და ამტკიცებს დაწესებულების ხელმძღვანელი. შიდა აუდიტის სტრატეგიული გეგმა გამომდინარეობს დაწესებულების გრძელვადიანი მიზნებიდან, **მოიცავს სამწლიან პერიოდს** და განსაზღვრავს შიდა აუდიტის სუბიექტის სტრატეგიული განვითარების მიმართულებებს.

შიდა აუდიტის სტრატეგიული გეგმა უნდა ითვალისწინებდეს, როგორც საქმიანობის პროცესებთან, ასევე IT პროცესებთან და სისტემებთან დაკავშირებულ მიზნებსა და ამოცანებს. დოკუმენტი უნდა მოიცავდეს IT-სთან დაკავშირებულ ახალ და განვითარებად სფეროებს და უზრუნველყოფდეს არსებული და მომავალი მოთხოვნების ჭრილში ადამიანური რესურსების, საჭირო გამოცდილებისა და კომპეტენციების ანალიზს. აღნიშნული შესაძლოა მოიცავდეს პროგრამული უზრუნველყოფის განვითარებისა (მაგ., პროგრამული უზრუნველყოფის ე.წ. „ეჯაილ“ (Agile) მეთოდების გამოყენებით განვითარება) და შესყიდვის თანამედროვე მეთოდების, ღრუბლოვანი გამოთვლითი სერვისების (ე. წ. „Cloud as a Service“), ან ბლოკჩეინ ტექნოლოგიების გამოყენებას ციფრული სერვისების სანდოობის გასაზრდელად.

2.1.1 სახელმწიფო სექტორის შიდა აუდიტი და მისი სპეციფიკა

სტრატეგიული გეგმის მომზადებისას შიდა აუდიტის სუბიექტის ხელმძღვანელმა უნდა გაითვალისწინოს საჯარო სექტორის სპეციფიკა და კონტექსტი. უპირველეს ყოვლისა, შიდა აუდიტის სუბიექტის ხელმძღვანელმა უნდა გაითვალისწინოს დაწესებულების დანიშნულება - ემსახუროს საზოგადოებრივ კეთილდღეობას და დაიცვას კარგი მმართველობის პრინციპები, მათ შორის: ა) ანგარიშვალდებულება საზოგადოებისგან მიღებულ სახსრებზე და ბ) ეფექტიანობა, პროდუქტიულობა და სამართლიანობა საზოგადოებრივი სიკეთეებისა და სერვისების უზრუნველყოფაში.

გამჭვირვალობა და კეთილსინდისიერება მმართველობაში ხელს უწყობს დემოკრატიული პოლიტიკური სისტემების ზემოაღნიშნული ეთიკური პრინციპების დაცვას. კანონები და რეგულაციები, როგორც წესი, იმისთვის არსებობს, რომ ეს პრინციპები შესრულდეს პოლიტიკის შემუშავებისა და განხორციელებისას, ამდენად, საჯარო სექტორისთვის მუდმივ საზრუნავს წარმოადგენს შესაბამისობის უზრუნველყოფა. დიაგრამა N4 ასახავს ურთიერთკავშირს შიდა აუდიტის პროფესიონალურ პრაქტიკასა და საჯარო სექტორის კონტექსტს, საჯარო პოლიტიკასა და კანონმდებლობას შორის.



დიაგრამა 4: *საჯარო სექტორის შიდა აუდიტი*

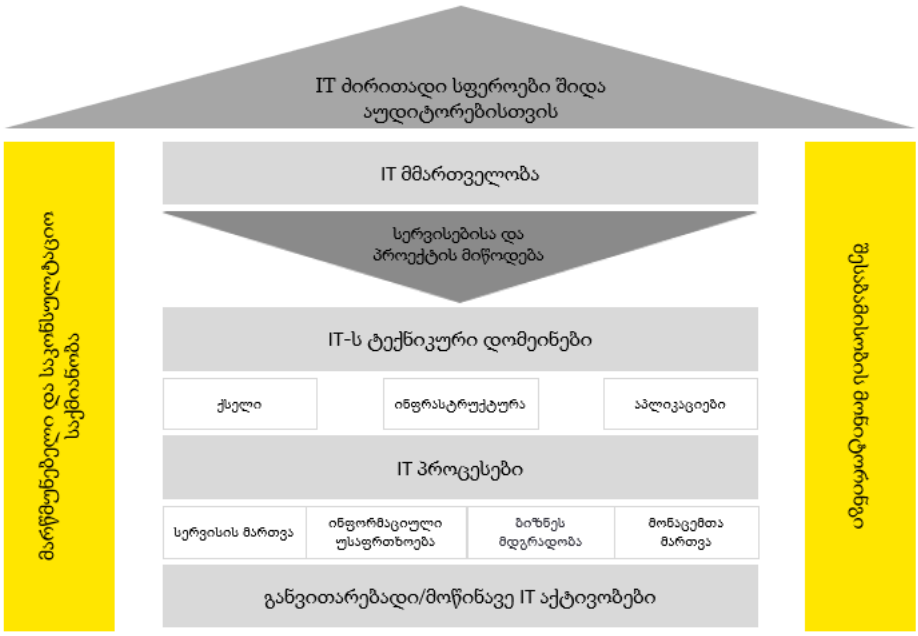
2.1.2 IT კომპეტენციები

შიდა აუდიტის სუბიექტის ხელმძღვანელისთვის ერთ-ერთ ყველაზე რთულ გამოწვევას წარმოადგენს IT რისკებზე ეფექტურად რეაგირებისთვის საჭირო კომპეტენციებისა და უნარების განვითარება შიდა აუდიტის ჯგუფში. შიდა აუდიტის სუბიექტის ხელმძღვანელს უნდა ესმოდეს, რომ ერთი შიდა აუდიტორი ერთდროულად ვერ მოახერხებს შიდა IT აუდიტორული შეფასების ყველა ამოცანის განხორციელებას და რომ, ხშირ შემთხვევაში, შიდა აუდიტის ჯგუფს ესაჭიროება შიდა აუდიტორები, რომლებიც უფრო მეტად სპეციალიზდებიან პოლიტიკებზე და შიდა აუდიტორები, რომლებიც უფრო გათვითცნობიერებული არიან აპლიკაციებსა და ინფრასტრუქტურულ ტექნოლოგიებში. მაგალითად, ქსელური ეკრანის (ე.წ. „Firewall“) კონფიგურაციის შიდა აუდიტისთვის საჭირო უნარები მნიშვნელოვნად განსხვავდება სარეზერვო ასლების მართვის პოლიტიკის შეფასებისთვის საჭირო უნარებისგან. აღნიშნულის გათვალისწინებით, გადამწყვეტი მნიშვნელობა ენიჭება შიდა აუდიტის სუბიექტის წინაშე არსებული ამოცანებისა და მათი ეფექტურად შესრულებისთვის საჭირო კომპეტენციების და უნარების შეთავსებას.

2.1.3 IT საფუძვლები შიდა აუდიტორისთვის

შიდა აუდიტორთა ინსტიტუტის (ე. წ. „IIA“) მიერ შემუშავებული სახელმძღვანელო „IT საფუძვლები შიდა აუდიტორთათვის”, ეხმარება შიდა IT აუდიტორებს იმის გაცნობიერებაში, თუ როგორ ფუნქციონირებს ინფორმაციული ტექნოლოგიები ორგანიზაციაში და რა მნიშვნელოვან როლს ასრულებენ ისინი ორგანიზაციის წარმატებაში.

ზემოხსენებული სახელმძღვანელო მოიცავს IT-სთან დაკავშირებულ ძირითად საქმიანობებს და კონცეფციებს, რომლებიც ყველა შიდა აუდიტორმა უნდა იცოდეს.



დიაგრამა 5: *IT-სთან დაკავშირებული ძირითადი სფეროები შიდა აუდიტორებისთვის*

2.1.4 შიდა აუდიტის კომპეტენციის ჩარჩო

შიდა აუდიტორთა ინსტიტუტს (ე. წ. „IIA“) ასევე შემუშავებული აქვს შიდა აუდიტის კომპეტენციების ჩარჩო, რომელიც სთავაზობს შიდა აუდიტორებს IT პროფესიული განვითარების მკაფიო გეგმას, მათი კარიერის ყველა ეტაპზე. ჩარჩო განსაზღვრავს ცოდნის სხვადასხვა სტანდარტზე, სპეციფიკურ ფუნქციასა და ძირითად უნარზე ორიენტირებულ ოთხ სფეროს (პროფესიონალიზმი, განხორციელება, გარემო, ლიდერობა და კომუნიკაცია) სამი განსხვავებული კომპეტენციის დონით, რომლებიც ვითარდება ზოგადი ცოდნიდან, გამოყენებით ცოდნამდე და საბოლოოდ, ექსპერტულ ცოდნამდე.

ჩარჩო ასრულებს ეფექტური ინსტრუმენტის ან მრავალწლიანი სასწავლო გეგმის ფუნქციას, რომელიც შიდა აუდიტის სუბიექტის ხელმძღვანელს და დაწესებულების ხელმძღვანელებს ეხმარება შიდა აუდიტორთა კომპეტენციებში ნაკლოვანების იდენტიფიცირებასა და მათ გამოსწორებაში.

ცოდნის სფერო	კომპეტენციის დონე		
	ზოგადი ცნობიერება	გამოყენებითი ცოდნა	ექსპერტული ცოდნა
ინფორმაციული ტექნოლოგიები • მონაცემთა ანალიტიკა • უსაფრთხოება და კონფიდენციალობა • IT კონტროლების ჩარჩო	ინფორმაციული ტექნოლოგიების და მონაცემთა ანალიტიკის ძირითადი ცნებების ზოგადი ცოდნა	მონაცემთა ანალიტიკის და ინფორმაციული ტექნოლოგიების გამოყენება აუდიტორულ შეფასებაში	აუდიტის ფარგლებში მონაცემთა ანალიტიკისა და ინფორმაციული ტექნოლოგიების გამოყენების შეფასება
	ინფორმაციულ ტექნოლოგიებთან, ინფორმაციულ უსაფრთხოებასთან და მონაცემთა კონფიდენციალურობასთან დაკავშირებული ძირითადი რისკების ცოდნა	ინფორმაციულ ტექნოლოგიებთან, ინფორმაციულ უსაფრთხოებასთან და მონაცემთა კონფიდენციალურობასთან დაკავშირებული სხვადასხვა რისკის გამოვლენა და შეფასება	IT რისკების, ინფორმაციული უსაფრთხოებისა და მონაცემთა კონფიდენციალურობის მართვისათვის საჭირო რეკომენდაციების გაწევა
	IT საკონტროლო ჩარჩოების და ძირითადი IT კონტროლის მიზნების ცოდნა და გამოყენება	IT კონტროლების ჩარჩოს გამოყენება	IT კონტროლების ჩარჩოების გამოყენების შეფასება

ცხრილი 1: *შიდა აუდიტის კომპეტენციები*

2.1.4.1 პროფესიული სერტიფიკატები

ქვემოთ მოცემულია ინფორმაცია საერთაშორისოდ აღიარებული სხვადასხვა სერტიფიკატის შესახებ, რომლებიც კომპეტენციის ამაღლებისა და დადასტურების მიზნით შეუძლიათ მოიპოვონ შიდა IT აუდიტორებმა:

სერტიფიცირებული შიდა აუდიტორი (CIA)

ეს არის საერთაშორისო აღიარების მქონე უმნიშვნელოვანესი სერტიფიცირება შიდა აუდიტორებისთვის. შიდა აუდიტორთა ინსტიტუტის (IIA) ეს სერტიფიკატი, წარმოადგენს კრიტერიუმს, რომლის გამოყენებითაც შიდა აუდიტორებს შეუძლიათ შიდა აუდიტის სფეროში საკუთარი პროფესიონალიზმის დემონსტრირება. სერტიფიცირებული შიდა აუდიტორები საერთაშორისო მასშტაბით არიან აღიარებული მათი მართვის უნარებით, მათ შორის, ხელმძღვანელობით რისკების მართვის და კონტროლის, შიდა აუდიტის, ბიზნეს ანალიზის და ინფორმაციული ტექნოლოგიების, სტრატეგიული მართვის, მოლაპარაკებების წარმოების და ორგანიზაციული ქცევის განხორციელების ფუნქციების შესრულების მიმართულებით.

პერსონალურ მონაცემთა დაცვის სერტიფიცირებული პროფესიონალი (CIPP)

აღნიშნული წარმოადგენს გლობალურად აღიარებულ სერტიფიკატს, რომელიც ეხება ისეთ საკითხებს, როგორიცაა პერსონალური ინფორმაციის შეგროვება და დამუშავება, კორპორაციული პროგრამული უზრუნველყოფის ინსტალაცია და წაშლა, კონფიდენციალობის დაცვის წესები და სისტემური და ქსელური აპარატურული უზრუნველყოფის დაცვა. სერტიფიკატის წარმატებით მოპოვების შემთხვევაში პირი იღებს საჭირო ცოდნას IT პროდუქტების და სერვისების შემუშავების, ტესტირების, დანერგვისა და აუდიტორული შეფასების ფარგლებში კორპორაციული მონაცემების უსაფრთხოების და კონფიდენციალობის უზრუნველყოფის შესახებ.

სერტიფიცირებული ინფორმაციული სისტემების აუდიტორი (CISA)

სერტიფიცირებული ინფორმაციული სისტემების აუდიტორის სერტიფიკატს, რომელიც IT აუდიტის სფეროში ცოდნის ერთ-ერთი ყველაზე მნიშვნელოვანი დამადასტურებელია, გასცემს ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაცია (ISACA) იმ აუდიტორებზე, რომლებიც კონკრეტულ პირობებს აკმაყოფილებენ. ამ სერტიფიკატის მქონე პირები საერთაშორისოდ აღიარებულნი არიან ისეთ საკითხებზე, როგორიც არის აუდიტის პროცესი, ხელმძღვანელობა და საინფორმაციო სისტემების მართვა. ეს აღიარება ვრცელდება ისეთ სფეროებზე, როგორიცაა აქტივების შესყიდვა, განვითარება და ჩამოყალიბება, ფუნქციონირება, ტექნიკური მომსახურება, მხარდაჭერა და დაცვა. აღნიშნული საკითხები ასევე შეესაბამება ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის მიერ ჩამოყალიბებულ IT კომპეტენციების მოდელს.

ინფორმაციული უსაფრთხოების სერტიფიცირებული მენეჯერი (CISM)

ინფორმაციული უსაფრთხოების სერტიფიცირებული მენეჯერის სერტიფიკატს გასცემს ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაცია (ISACA). ინფორმაციული უსაფრთხოების სერტიფიცირებული მენეჯერის სერტიფიკატის მფლობელ პირებს აქვთ ცოდნა

და გამოცდილება ინფორმაციული უსაფრთხოების და რისკების მართვის, ინფორმაციული უსაფრთხოების პროგრამის შემუშავების, ინფორმაციული უსაფრთხოების პროგრამის მართვისა და ინციდენტების მართვის მიმართულებით.

სერტიფიცირებული ინფორმაციული სისტემების უსაფრთხოების პროფესიონალი (CISSP)

ინფორმაციული სისტემების უსაფრთხოების პროფესიონალის სერტიფიკატს გასცემს ინფორმაციული სისტემების უსაფრთხოების სერტიფიცირების საერთაშორისო კონსორციუმი (ISC)², დამოუკიდებელი ორგანიზაცია. ინფორმაციული სისტემების უსაფრთხოების პროფესიონალის სერტიფიკატი აღიარებულია, როგორც ერთ-ერთი ყველაზე მნიშვნელოვანი საერთაშორისო სერტიფიკატი ინფორმაციული უსაფრთხოების სფეროში.

რისკისა და საინფორმაციო სისტემების კონტროლის სერტიფიკატი (CRISC)

აღნიშნული სერტიფიკატი შექმნილია რისკის გამოვლენის, შეფასების, მასზე რეაგირებისა და მონიტორინგისთვის, ინფორმაციული სისტემების კონტროლების შექმნისა და მათი მონიტორინგის სფეროში გამოცდილების მქონე IT პროფესიონალებისთვის. ამ სერტიფიკატს გასცემს ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაცია (ISACA).

რისკის მართვის უზრუნველყოფის სერტიფიკატი (CRMA)

რისკის მართვის უზრუნველყოფის სერტიფიკატს გასცემს შიდა აუდიტორთა ინსტიტუტი. რისკის მართვის უზრუნველყოფის სერტიფიკატი შექმნილია შიდა აუდიტორებისთვის და რისკების მართვის პროფესიონალებისთვის, რომლებსაც აქვთ პასუხისმგებლობა ან გამოცდილება რისკის მართვის უზრუნველყოფის გაცემის, ხელმძღვანელობის პროცესების, ხარისხის უზრუნველყოფის ან კონტროლის თვითშეფასების მიმართულებით.

ინფორმაციის უზრუნველყოფის გლობალური სერტიფიკატი (GIAC)

GIAC არის ინფორმაციული უსაფრთხოების სფეროში დასაქმებული პირების უნარების დამადასტურებელი ორგანიზაცია. ამ მიმართულებით, ორგანიზაცია ინფორმაციული უსაფრთხოების სფეროს თანამშრომლებზე გასცემს უსაფრთხოების მართვის, სასამართლო ექსპერტიზის, მართვის, აუდიტის, პროგრამული უზრუნველყოფის უსაფრთხოების, კანონისა და უსაფრთხოების ექსპერტიზის სხვადასხვა დონის სერტიფიკატებს.

ამასთან, ჰარმონიზაციის ცენტრი კოორდინირებას უწევს შიდა აუდიტორთა სერტიფიცირების ეროვნულ პროგრამას, რომლის მიზანია საჯარო სექტორში მაღალი სტანდარტის დამკვიდრება და შიდა აუდიტორთა უწყვეტი პროფესიული განვითარება. დაინტერესების შემთხვევაში, შიდა

აუდიტის სუბიექტებს აქვთ შესაძლებლობა ჩაერთონ აღნიშნულ პროგრამაში, რომლის ერთ-ერთი მოდული ფარავს IT აუდიტთან დაკავშირებულ ძირითად საკითხებს.

2.1.5 აუდიტის ინსტრუმენტები

შიდა აუდიტის სუბიექტის ხელმძღვანელმა რეგულარულად უნდა განიხილოს შიდა აუდიტის ეფექტიანობისა და პროდუქტიულობის გაზრდის მიზნით დამატებითი შიდა აუდიტის ინსტრუმენტებისა და/ან ავტომატიზებული ტექნიკების გამოყენების საჭიროება და შესაძლებლობა. ზოგადად, შიდა აუდიტის ინსტრუმენტები მოითხოვს მნიშვნელოვან ინვესტიციას, ამიტომ კონკრეტული ინსტრუმენტის შესყიდვამდე შიდა აუდიტის სუბიექტის ხელმძღვანელმა ყურადღებით უნდა განიხილოს შერჩეული გადაწყვეტილების ხარჯ-სარგებლიანობის ურთიერთმიმართება.

შიდა აუდიტის ინსტრუმენტები შეიძლება დაიყოს ორ მსხვილ კატეგორიად: შიდა აუდიტის მხარდამჭერი ინსტრუმენტები, რომლებიც ხელს უწყობსნ შიდა აუდიტის საერთო მართვას (მაგ. შიდა აუდიტის მართვის სისტემა) და უშუალოდ ტესტირების ინსტრუმენტები, რომლებიც უზრუნველყოფენ შიდა აუდიტის ტესტირების აქტივობების ავტომატიზაციას (მაგ., მონაცემთა ანალიზის ინსტრუმენტები და შიდა აუდიტორული შემოწმების ჩატარების კომპიუტერიზებული მეთოდები, ე. წ. „CAAT“). კერძოდ, ტესტირების ინსტრუმენტები მოიცავს შემდეგს:

- **უსაფრთხოების ანალიზის ინსტრუმენტები.** ასეთი ინსტრუმენტების მნიშვნელოვანი მაგალითია ქსელის ანალიზის ინსტრუმენტები, რომლებიც აგროვებენ ინფორმაციას ქსელის შესახებ, ამოწმებენ ქსელის დიაგრამების სიზუსტეს, ახდენენ ქსელური მოწყობილობების იდენტიფიკაციას, რომლებიც დამატებით აუდიტორულ ყურადღებას საჭიროებენ, და აღწერენ, თუ რა რაოდენობით არის ტრაფიკი ნებადართული ქსელში;
- **მოწყვლადობის შეფასების ინსტრუმენტები.** ეს პროგრამული უზრუნველყოფა ავტომატურად ამოწმებს ცნობილ სისუსტეებს, როგორებიც არის სტანდარტული პაროლები ან პარამეტრები. შიდა აუდიტორებს შეუძლიათ გააქტიურონ ავტომატური ძიების ფუნქცია და ინსტრუმენტი ახდენს რეპორტის გენერირებას. იმის გამო, რომ ასეთმა ინსტრუმენტებმა შეიძლება გავლენა მოახდინოს შესამოწმებელი სისტემების მთლიანობაზე, მნიშვნელოვანია უსაფრთხოების ჯგუფთან ტესტების კოორდინაცია (ან უსაფრთხოების ჯგუფის მიერ ჩატარებული ტესტების შედეგების გამოყენება);
- **აპლიკაციის უსაფრთხოების ანალიზის ინსტრუმენტები.** მსხვილ ბიზნეს აპლიკაციებს და პროგრამულ გადაწყვეტებს (მაგ., „ERP“ სისტემები) ხშირად აქვთ მწარმოებლის მიერ შემუშავებული უსაფრთხოების ინსტრუმენტები, რომლებიც გამოიყენება სისტემის წინასწარ კონფიგურირებული წესების (მაგ., მომწოდებლის „საუკეთესო პრაქტიკა“, რომელიც შეიძლება შეფასდეს შესაბამისობაზე) მიმართ გასაანალიზებლად ან შეუთავსებელი მოვალეობების გამოჯვნის შესამოწმებლად.

2.2 შიდა აუდიტის წლიური გეგმა

ყოველი კალენდარული წლის ბოლოს ორგანიზაციის შიდა აუდიტის სუბიექტი იწყებს მომავალი წლის შიდა აუდიტის გეგმის მომზადებას. ეს გეგმა წარმოადგენს შიდა აუდიტის სუბიექტის მიერ წლის განმავლობაში შესასრულებელი სამუშაოების განრიგს.

შიდა აუდიტის წლიურ გეგმას არსებითი მნიშვნელობა აქვს წლის განმავლობაში შიდა აუდიტის საქმიანობის ეფექტიანი და პროდუქტიული განხორციელებისთვის და შიდა აუდიტის ყველა დაგეგმილი პროექტის წარმატებით და დროულად შესრულებისთვის.

წლიური დაგეგმვის პროცესში შიდა აუდიტის სუბიექტმა უნდა გამოიყენოს რისკზე დაფუძნებული მიდგომა, რათა უზრუნველყოს რესურსების ეფექტიანი გამოყენება და მოქნილობა, რაც, თავის მხრივ, შესაძლებელს გახდის ორგანიზაციის სტრუქტურაში ან მის ოპერაციებში განხორციელებულ ცვლილებებზე დროულ რეაგირებას. რისკზე დაფუძნებული შიდა აუდიტის წლიური გეგმის ფორმირება ითვალისწინებს რისკის ყოვლისმომცველ შეფასებას და ხელს უწყობს შიდა აუდიტს კონცენტრირება მოახდინოს ყველაზე მაღალი რისკის მქონე სფეროებზე.

2.2.1 რისკების სამყარო

რისკზე დაფუძნებული შიდა აუდიტის წლიური გეგმის მომზადების პირველი ნაბიჯს წარმოადგენს რისკის ყოვლისმომცველი სამყაროს შემუშავება, რომელსაც ასევე უწოდებენ „აუდიტის სამყაროს“. ის უზრუნველყოფს დაწესებულების, მისი სტრატეგიისა და ოპერაციების აღქმის ორგანიზებულ და თანმიმდევრულ მექანიზმს და წარმოადგენს უნიკალური რისკის (აუდიტის) სფეროების ერთობას.

რისკების სამყაროს შემუშავება იწყება ორგანიზაციის სტრატეგიისა და მიზნების გაგებით. IT სტრატეგიას, პროცესებსა და პროექტებს გადამწყვეტი როლი აქვთ საქმიანობის სტრატეგიებისა და მიზნების მიღწევაში, შესაბამისად, უზრუნველყოფილი უნდა იყოს შესაბამისობა მათ შორის. შიდა აუდიტის სუბიექტის ხელმძღვანელმა უნდა გააანალიზოს ხსენებული დოკუმენტები / ინფორმაცია და გამოავლინოს რისკის სფეროები, რომელთა რეალიზაციამაც შესაძლოა უარყოფითი ზეგავლენა იქონიოს ორგანიზაციის სტრატეგიისა და მიზნების მიღწევაზე. IT-ის და მასთან დაკავშირებული რისკების IT-ის იერარქიული მოდელის პრიზმაში განხილვა ეხმარება შიდა აუდიტის სუბიექტს აუდიტის სფეროებისა და პრიორიტეტების უკეთ გააზრებაში. IT-ის იერარქიული მოდელი შედგება შემდეგი შრეებისგან:

- **IT მართვის შრე.** ინფორმაციული ტექნოლოგიების მართვა მოიცავს ადამიანების, პოლიტიკების, პროცედურებისა და პროცესების ერთობლიობას, რომლებიც, თავის მხრივ, უზრუნველყოფენ IT სერვისებსა და ფიზიკური ობიექტების მართვას. ეს დონე აერთიანებს ისეთ საკითხებს, როგორიცაა: IT მმართველობა, უსაფრთხოების მართვა, სისტემების მონიტორინგი, პროგრამული უზრუნველყოფის განვითარება, დაგეგმვა, მომწოდებლების მართვა, პრობლემებისა და ინციდენტების მართვა, ცვლილებების მართვა, IT პროექტების მართვა და ავარიული აღდგენა. შემოწმება ფოკუსირებული იქნება მართვის პროცესში ჩართულ ადამიანებზე, მათ როლებსა და

პასუხისმგებლობებზე, არსებული პოლიტიკების, პროცედურებისა და პროცესების შესაბამისად შესრულებულ დავალებებზე და ნაკლებად ტექნოლოგიურ დეტალებზე;

- **გარე კავშირების შრე.** ინტერნეტთან გარე კავშირი, განსხვავებით სხვა გარე კავშირებიდან, მაგალითად, ბიზნეს პარტნიორებთან ან ღრუბლოვანი სერვისის მომწოდებლებთან, ხასიათდება სპეციფიკური რისკებითა და კონტროლებით. გარე ქსელის ყველა შემომავალი ან გამავალი კომუნიკაცია რისკად უნდა ჩაითვალოს, მკაცრად უნდა კონტროლდებოდეს და წარმოებდეს მათი მონიტორინგი რისკის დონის გათვალისწინებით. როგორც მინიმუმ, უნდა არსებობდეს ყველა შემომავალი და გამავალი წერტილის რეესტრი;
- **ტექნიკური ინფრასტრუქტურის შრე.** ძირითადი ბიზნეს აპლიკაციების ოპერაციული მხარდაჭერა და ფუნქციონირება უზრუნველყოფილია სხვადასხვა ტექნოლოგიის გამოყენებით, მათ შორის, ოპერაციული სისტემები, მონაცემთა ბაზები, ქსელები, მონაცემთა დამუშავების ცენტრები და ა. შ. აღნიშნული ტექნოლოგიები, თავის მხრივ, დაფუძნებული არიან შესაბამის ტექნიკურ ინფრასტრუქტურაზე. მნიშვნელოვანია გვესმოდეს, რომ ტექნიკური ინფრასტრუქტურის აუდიტი ითვალისწინებს როგორც ტექნიკური კონფიგურაციის პარამეტრების, ასევე მათ მართვასთან დაკავშირებული პროცესების (მაგ., პრივილეგირებული წვდომის მქონე მომხმარებლების მონიტორინგი) შეფასებას;
- **აპლიკაციების შრე.** აღნიშნული შრე მოიცავს, როგორც ტრანზაქციულ აპლიკაციებს (ორგანიზაციის მიერ შემუშავებული (ე. წ. „In-house Developed“), მომწოდებლისგან შეძენილი, ორგანიზაციის მიერ მორგებული (ე. წ. “Purchased and Customized”, გამოწერის პრინციპზე მომუშავე (ე. წ. „Subscribed“)), ასევე მხარდამჭერ აპლიკაციებს, რომლებიც ხელს უწყობს ბიზნეს პროცესებს, მაგრამ არ ამუშავებს ტრანზაქციებს (მაგ., ელექტრონული ფოსტა, მონაცემთა ანალიზი, მონაცემთა საცავები). ძირითადად, IT აუდიტის ყურადღება გამახვილებულია ტრანზაქციულ აპლიკაციებზე, თუმცა მხარდამჭერი აპლიკაციები (მაგ., გარე ანგარიშგების) შესაძლოა ასევე იყოს მნიშვნელოვანი IT რისკების შემცველი. ზოგიერთი აპლიკაცია საჭიროებს სპეციალიზებულ ცოდნას აუდიტის ჩასატარებლად.

რისკის სფეროების იდენტიფიცირება საჭიროებს გონივრულ განსჯას, ამიტომ მნიშვნელოვანია, რომ გადაწყვეტილება მიღებული იყოს ძირითად დაინტერესებულ მხარეებთან, საგნის ექსპერტებთან და აუდიტის სუბიექტის ხელმძღვანელთან კონსულტაციის საფუძველზე. აღნიშნული ხელს უწყობს რისკის სფეროების სწორი მასშტაბის განსაზღვრას და არტიკულირებას.

რისკის (აუდიტის) სფერო არ უნდა იყოს იმდენად დიდი, რომ ის ერთიანად ვერ შემოწმდეს ერთი აუდიტის ფარგლებში. ამავდროულად, ის არც ძალიან მცირე უნდა იყოს, რათა აუდიტის შედეგად წარმოებული ინფორმაცია შინაარსობრივად ღირებული იყოს და იძლეოდეს დამატებითი ანალიზის / შედარებითობის საშუალებას. რისკის (აუდიტის) სფეროს განსაზღვრისას, შიდა აუდიტორმა უნდა უზრუნველყოს, რომ რისკების ძირითადი სფეროების დაჯგუფება იძლეოდეს დამატებითი ღირებულების მატარებელ რწმუნებულებას ორგანიზაციისთვის.

იდენტიფიცირებული რისკის სფეროები განსაზღვრულია დოკუმენტში ***„001 რისკებზე დაფუძნებული IT აუდიტის გეგმის მომზადება“***, რომელშიც მოცემულია რისკის ყველაზე გავრცელებული სფეროები. შიდა აუდიტის სუბიექტის ხელმძღვანელმა პერიოდულად, სულ მცირე ყოველწლიურად, უნდა გადახედოს აუდიტის სამყაროს, რათა უზრუნველყოფილი იყოს მისი შესაბამისობა ორგანიზაციის სტრატეგიასთან და ძირითად მიზნებთან.

2.2.1.1 რისკის შეფასების მიდგომა

რისკის შეფასების მიზანია ნარჩენი რისკის საფუძველზე რისკის (აუდიტის) პრიორიტეტული სფეროების განსაზღვრა და შიდა აუდიტის შეზღუდული რესურსების მიმართვა ყველაზე მაღალი რისკის მატარებელ სფეროებზე. აუდიტის სამყაროს თითოეული რისკის სფეროს ნარჩენი რისკი ფასდება ორი ძირითადი ფაქტორით: თანდაყოლილი რისკი და კონტროლების გარემოს ეფექტურობა.

კონტროლის გარემოს შეფასება

კონტროლების გარემო ფასდება ქვემოთ აღწერილი მეთოდოლოგიისა და შეფასების ფაქტორების მიხედვით:

- **ზეგავლენა ორგანიზაციის მიზნების მიღწევაზე.** შიდა აუდიტის წლიური გეგმა უნდა ითვალისწინებდეს ორგანიზაციის ამოცანებს. ამ მიზნით უნდა შეფასდეს რისკის მატარებელი სფეროს ზეგავლენა ორგანიზაციის სტრატეგიული და ოპერაციული მიზნების მიღწევაზე. აღნიშნულის შესაფასებლად შიდა აუდიტის სუბიექტის ხელმძღვანელი იყენებს საკუთარ პროფესიულ განსჯას და დაკავშირებული პროცესების გაზომვად მიზნებს;
- **ოპერაციების კომპლექსურობა არის უზუსტობის, თაღლითობის ან გადაცდომის შემთხვევების და მათი დროულად გამოვლენის სირთულეების შესაძლო მიზეზი.** ტრანზაქციის სირთულე ფასდება ისეთი ფაქტორების ანალიზის გზით, როგორებიც არის ავტომატიზაციის დონე, ურთიერთდაკავშირებული და ურთიერთ-მოქმედი პროცესები, მესამე მხარეზე დამოკიდებულება, ტრანზაქციების დამუშავებისთვის საჭირო დრო და ა. შ.
- **წინა აუდიტის შედეგები.** აღნიშნული ფასდება რისკის (აუდიტის) სფეროში წინა აუდიტის ფარგლებში გამოვლენილი მიგნებების სიმწვავის საფუძველზე (მაგ., კონტროლის ხარვეზები / დარღვევები / თაღლითობის შემთხვევები);
- **აუდიტის რეკომენდაციების დანერგვის ხარისხი.** აღნიშნული ფასდება შემდგომი დაკვირვებებიდან (ე. წ. „Follow-up“) ან რეკომენდაციების შესრულების მონიტორინგიდან მიღებული მონაცემების საფუძველზე და დამოკიდებულია გამოსასწორებელი ქმედებების დროულად დანერგვაზე და ეფექტურობაზე;
- **წინა აუდიტის შემდეგ გასული დრო.** რაც უფრო დიდი დროა გასული წინა აუდიტიდან, მით უფრო ნაკლებად სანდოა რისკის (აუდიტის) სფეროში კონტროლის გარემოს ეფექტურობა;

- **შიდა კონტროლის გარემო.** ეს ფაქტორი ფასდება შიდა კონტროლის სისტემიდან ან შიდა აუდიტორული ანგარიშებიდან წარმოებული მონაცემების საფუძველზე. კონტროლების სუსტი გარემოს ნიშნებია პერსონალისა და ხელმძღვანელობის დენადობის მაღალი მაჩვენებლები, ხელმძღვანელობის მხრიდან ზედამხედველობის/კონტროლის დაბალი დონე, ძირითადი პროცესების/პროცედურების დოკუმენტირების არქონა, გადახრები დოკუმენტირებული პროცესებიდან, არა-რუტინული ოპერაციების დიდი მოცულობა და ა.შ.
- **მნიშვნელოვანი ცვლილებები აუდიტის სფეროში.** პროცესებში ცვლილებების მნიშვნელობა ფასდება პროცესის მფლობელებთან გასაუბრების საფუძველზე. გათვალისწინებული უნდა იყოს პროცესის რეინჟინერიასთან, სწრაფ ზრდასთან, ახალი პროდუქტების/მომსახურების გაშვებასთან, ახალი IT სისტემების დანერგვასთან, პერსონალის ან ხელმძღვანელობის ცვლილებებთან დაკავშირებული ცვლილებები. პროცესის სწრაფი და მნიშვნელოვანი ცვლილება, როგორც წესი, ზრდის ხარვეზების ალბათობას და ამცირებს პროცესის ეფექტიანობასა და პროდუქტიულობას;
- **რისკის მართვადობის ხარისხი.** ამ ფაქტორის შესაფასებლად მონაცემები მიიღება რისკების მართვის სამსახურიდან, ასეთის არსებობის შემთხვევაში.

მიღებული პასუხებისა და მონაცემების გათვალისწინებით თითოეულ ფაქტორს ენიჭება 1-დან 3 ქულამდე. დეტალური კრიტერიუმები თითოეული ფაქტორისთვის მოცემულია ცხრილში ქვემოთ:

აღწერა/ქულა	1 ქულა	2 ქულა	3 ქულა
ზეგავლენა ორგანიზაციის მიზნების მიღწევაზე	არ არის პირდაპირ დაკავშირებული ორგანიზაციის მიზნების მიღწევასთან	დაკავშირებულია ორგანიზაციის მიზნების მიღწევასთან	პირდაპირ ზეგავლენა აქვს ორგანიზაციის მიზნების მიღწევაზე
ოპერაციების კომპლექსურობა	ოპერაციების კომპლექსურობა ფასდება შემდეგი ფაქტორების ანალიზით: ავტომატიზაციის დონე, ურთიერთდაკავშირებული და ურთიერთ-მოქმედი პროცესები, მესამე მხარეზე დამოკიდებულება და ა. შ.		
წინა აუდიტის შედეგები	თუ წინა აუდიტის შეფასება იყო „ეფექტური“, ან „საჭიროებს მცირედ გაუმჯობესებას“, მაშინ გამოიყენება 1 ქულა	თუ წინა აუდიტის შეფასება იყო „საჭიროებს მნიშვნელოვან გაუმჯობესებას“, მაშინ გამოიყენება 2 ქულა	თუ წინა აუდიტის შეფასება იყო „არადამაკმაყოფილებელი“ ან აუდიტის სფერო საერთოდ არ შეფასებულა, მაშინ გამოიყენება 3 ქულა
აუდიტორული რეკომენდაციების დანერგვის ხარისხი	გამოსასწორებელი ქმედებები განხორციელდა დათქმულ ვადებში და ფასდება დამაკმაყოფილებლად, ან დათქმული ვადები კვლავ ძალაშია	გამოსასწორებელი ქმედებები არ განხორციელებულა დათქმულ ვადებში, მაგრამ დაგვიანება არ აღემატება 6 თვეს	გამოსასწორებელი ქმედებები არ განხორციელებულა დადგენილ ვადებში და დაგვიანება აღემატება 6 თვეს, ან აუდიტის სფერო საერთოდ არ შეფასებულა

წინა აუდიტის შემდეგ გასული დრო	წინა აუდიტი ჩატარდა გასულ წელს	ბოლო აუდიტი განხორციელდა უკანასკნელი 3 წლის განმავლობაში, მაგრამ არა გასულ წელს	აუდიტი არ განხორციელებულა ბოლო 3 წლის მანძილზე ან აუდიტი საერთოდ არ ჩატარებულა
თანამშრომელთა დენადობა	თუ აუდიტის სფეროზე პასუხისმგებელ სტრუქტურულ ერთეულში ახალი თანამშრომლების რაოდენობა მერყეობს 0-20%-ში, მაშინ გამოიყენება 1 ქულა	თუ აუდიტის სფეროზე პასუხისმგებელ სტრუქტურულ ერთეულში ახალი თანამშრომლების რაოდენობა მერყეობს 20-50%-ში, მაშინ გამოიყენება 2 ქულა	თუ აუდიტის სფეროზე პასუხისმგებელ სტრუქტურულ ერთეულში ახალი თანამშრომლების რაოდენობა მერყეობს 50-100%-ში, მაშინ გამოიყენება 3 ქულა
მნიშვნელოვანი ცვლილებები აუდიტის სფეროში	აუდიტის სფეროში მნიშვნელოვანი ცვლილებები არ განხორციელებულა	აუდიტის სფეროში განხორციელდა უმნიშვნელო ცვლილებები	აუდიტის სფეროში განხორციელდა მნიშვნელოვანი ცვლილებები (მაგ. ხელმძღვანელის დანიშვნა, ახალი პროდუქტის/ მომსახურების გაშვება, პროცესის დიზაინის ცვლილება და ა. შ.)
რისკის მართვადობის ხარისხი	ამ რისკის ფაქტორის შესაფასებლად მონაცემები მიიღება რისკების მართვის სამსახურიდან, ასეთის არსებობის შემთხვევაში. მაღალი მართვადობა – 1 ქულა, დაბალი მართვადობა – 3 ქულა. თუ პრაქტიკაში არ ხდება რისკების შეფასება, მაშინ უნდა მიეთითოს 0 ქულა.		

ცხრილი 2: *შეფასების კრიტერიუმები თითოეული ფაქტორისთვის*

მნიშვნელობიდან გამომდინარე, ზემოთ მოცემულ თითოეულ ფაქტორს აქვს თავისი შეწონილი მნიშვნელობა, რომელიც გამოხატულია პროცენტული მაჩვენებლით. საბოლოო ჯამში, ყველა ფაქტორი ერთად ადგენს 100%-ს.

საბოლოოდ კონტროლების გარემო ფასდება შემდეგი ფორმულის გამოყენებით:

$$A = \sum_{i=1}^{8} (C_i * W_i)$$

სადაც:

A – რისკის (აუდიტის) სფეროს კონტროლების გარემოს შეწონილი შეფასებაა

i – შეფასებისას გამოყენებული ფაქტორების რაოდენობა (ჯამში 8)

C – i ფაქტორის მნიშვნელობა

W – i ფაქტორის შეწონილი მნიშვნელობა.

თანდაყოლილი რისკის შეფასება

წლიური დაგეგმვის მეორე ფაქტორად გასათვალისწინებელია რისკის (აუდიტის) სფეროებში არსებული თანდაყოლილი რისკები. კერძოდ, თანდაყოლილი რისკი ფასდება ქვემოთ

ჩამოთვლილი რისკის ფაქტორებისა და მათი რეალიზაციის ალბათობისა და რეალიზაციის შემთხვევაში გამოწვეული ზეგავლენის სიდიდის გათვალისწინებით.

რისკ ფაქტორები:

- IT რესურსების არაეფექტიანი მართვა;
- ბიზნეს სერვისების/ პროცესების შეფერხება;
- მონაცემთა დაკარგვა / არაავტორიზებული გამჟღავნება;
- ინფორმაციულ აქტივებზე არაავტორიზებული წვდომა / მათი არაავტორიზებული მოდიფიკაცია;
- IT/კიბერ თაღლითობა;
- შესაძლო ზარალი ჯარიმებიდან.

თავის მხრივ, ალბათობა და ზეგავლენა ფასდება ხარისხობრივი მიდგომის გამოყენებით ქვემოთ მოცემული შეფასების სისტემის შესაბამისად:

რეიტინგი	ალბათობა	ზეგავლენა
0	არ შეესაბამება	არ შეესაბამება
1	დაბალი	დაბალი
2	საშუალო	საშუალო
3	მაღალი	მაღალი

საბოლოოდ, თანდაყოლილი რისკი კონკრეტული რისკის (აუდიტის) სფეროსთვის გამოითვლება შემდეგი ფორმულის გამოყენებით:

$$B = \sum_{j=1}^{6} (L_j * I_j) \ / \ 6$$

სადაც:

B – თანდაყოლილი რისკის მაჩვენებელი რისკის (აუდიტის) სფეროსთვის

j – შეფასებისას გამოყენებული ფაქტორების რაოდენობა (ჯამში 6)

L – ალბათობის მნიშვნელობა j-სთვის

I - ზეგავლენის მნიშვნელობა j-სთვის.

ნარჩენი რისკის შეფასება

ნარჩენი რისკის რეიტინგი ემყარება თანდაყოლილი რისკის რეიტინგს და კონტროლის ეფექტურობის შეფასებას. რისკის რეიტინგი წარმოადგენს სფეროს ნარჩენი რისკის საერთო შეფასებას. რაც უფრო მაღალია რეიტინგი მით მეტი პრიორიტეტი უნდა მიენიჭოს აუდიტორული შემოწმების საჭიროებებს. შიდა აუდიტი იყენებს ნარჩენი რისკის ოთხ დონეს, ესენია: დაბალი,

ზომიერი, ზომიერად მაღალი და მაღალი. დონეების მიხედვით რისკის კლასიფიცირების ცხრილი წარმოდგენილია ქვემოთ:

თანდაყოლილი რისკი		კონტროლების გარემო		
		ადეკვატური	საჭიროებს ყურადღებას	სუსტი
	მაღალი	ზომიერი	ზომიერად მაღალი	მაღალი
	საშუალო	დაბალი	ზომიერი	ზომიერად მაღალი
	დაბალი	დაბალი	დაბალი	ზომიერი

მაღალი	ზომიერად მაღალი	საშუალო	დაბალი
აუდიტის სფერო, რომელშიც არსებობს ორგანიზაციაზე ნეგატიური ზეგავლენის ძალიან მაღალი ალბათობა კრიტიკული თანდაყოლილი რისკების არსებობის გამო. შესაძლოა არსებობდეს მნიშვნელოვანი მინიშნებები, რომ მინიმიზირების კონტროლები არ არის შემუშავებული და/ან არ ოპერირებენ დიზაინის შესაბამისად	აუდიტის სფერო, რომელშიც არსებობს ორგანიზაციაზე ნეგატიური ზეგავლენის ზომიერად მაღალი ალბათობა კრიტიკული თანდაყოლილი რისკების არსებობის გამო. შესაძლოა არსებობდეს მინიშნებები, რომ მინიმიზირების კონტროლები არ არის შემუშავებული და/ან არ ოპერირებენ დიზაინის შესაბამისად	აუდიტის სფერო, რომელშიც არსებობს ორგანიზაციაზე ნეგატიური ზეგავლენის საშუალო ალბათობა ზომიერი თანდაყოლილი რისკების არსებობის გამო. შესაძლოა არსებობდეს გარკვეული მინიშნებები, რომ მინიმიზირების კონტროლებს ესაჭიროებათ დიზაინის და/ან ოპერაციული ეფექტურობის გაუმჯობესება	აუდიტის სფერო, რომელშიც არსებობს ორგანიზაციაზე ნეგატიური ზეგავლენის დაბალი ალბათობა მცირე თანდაყოლილი რისკების არსებობის გამო. შესაძლოა არ არსებობდეს მინიშნებები, რომ მინიმიზირების კონტროლები არ არის შემუშავებული და/ან ეფექტურად არ მოქმედებს

2.2.2 წლიური გეგმა

რისკის შეფასების შედეგები, კერძოდ, ნარჩენი რისკი, შიდა აუდიტის სუბიექტის ხელმძღვანელს საშუალებას აძლევს განსაზღვროს აუდიტის პროექტების პრიორიტეტულობა და რისკების გონივრული დაფარვის უზრუნველსაყოფად ეფექტიანად და პროდუქტიულად მიმართოს აუდიტის შეზღუდული რესურსები ყველა რისკიან სფეროებზე. შიდა აუდიტი მიზნად ისახავს ქვემოთ მოცემული სიხშირით რწმუნებულების გაცემას იმ ძირითადი კონტროლის მექანიზმებზე, რომლებიც უზრუნველყოფენ ძირითადი რისკის სფეროების ეფექტურ მართვას:

მაღალი რისკის მატარებელი სფეროები	აუდიტი ჩატარდება 12 თვის ვადაში
ზომიერად მაღალი რისკის მატარებელი სფეროები	აუდიტი ჩატარდება 24 თვის ვადაში
საშუალო რისკის მატარებელი სფეროები	აუდიტი ჩატარდება 36 თვის ვადაში
დაბალი რისკის მატარებელი სფეროები	აუდიტი ჩატარდება 48 თვის ვადაში

მნიშვნელოვანია იმის დადგენა, ხომ არ ვრცელდება რისკის (აუდიტის) სფეროზე კანონმდებლობით ან რეგულაციით გათვალისწინებული სავალდებულო აუდიტის მოთხოვნა. ასეთი სფეროები, მიუხედავად ნარჩენი რისკის საერთო დონისა, განისაზღვრება მაღალი საჭიროების მქონე სფეროდ და, შესაბამისად, უნდა შემოწმდეს კანონით ან რეგულაციით დადგენილი ვადებში.

რისკის სფეროების გონივრული დაფარვის უზრუნველსაყოფად, შიდა აუდიტის სუბიექტის ხელმძღვანელს შეუძლია გამოიყენოს სხვადასხვა მიდგომის კომბინაცია, მაგალითად, სრულმასშტაბიანი აუდიტი, თემატური შეფასება და უწყვეტი მონიტორინგი.

კონკრეტულ პროექტზე აუდიტორული სამუშაოს დაწყებამდე შიდა აუდიტის სუბიექტმა უნდა განახორციელოს აუდიტის გეგმის გადახედვა. როგორც წესი, აღნიშნული უნდა მოხდეს აუდიტის სავარაუდო დაწყების თარიღის წინა კვარტალში. აუდიტის გეგმის გადახედვის მიზანია დადგინდეს:

- კვლავ რელევანტურია თუ არა დაგეგმილი აუდიტის ჩატარება?
- კვლავ მისაღებია თუ არა აუდიტის ჩატარების ვადები?
- კვლავ რელევანტურია თუ არა აუდიტის წლიურ გეგმაში გათვალისწინებული მასშტაბი და ბიუჯეტი?

ამასთან, თითოეული ზემოთ ჩამოთვლილი კითხვა მნიშვნელოვანია საჭირო რესურსების დასადგენად (მაგალითად, აუდიტის პერსონალის გათვალისწინება კონკრეტული პროექტისთვის ან პირიქით, სხვა პროექტებისთვის დროის გამოთავისუფლება). მოცემული კითხვები შემდგომში უფრო დეტალურად იქნება განხილული აუდიტის დავალების დაგეგმვის პროცესში.

აუდიტის გეგმის გადახედვისას ასევე გასათვალისწინებელია შემდეგი ფაქტორები:

- მნიშვნელოვანი ცვლილებები ბიზნეს, საკანონმდებლო, მარეგულირებელ ან გამოყენებული IT სისტემების გარემოში, რომლებმაც შესაძლოა გავლენა იქონიონ დაგეგმილი აუდიტის ჩატარების აუცილებლობაზე ან მიზანშეწონილობაზე, ან არსებითად შეცვალოს აუდიტის მასშტაბი ან ტიპი;
- ძირითადი ინდიკატორების უწყვეტი ან პერიოდული მონიტორინგის შედეგები, რომლებიც შესაძლოა მიუთითებდეს ორგანიზაციის რისკების ან მნიშვნელოვანი გარემოებების ცვლილებაზე;
- აუდიტის პერსონალის საერთო ხელმისაწვდომობა და დაგეგმილი აუდიტის პრიორიტეტულობა აუდიტის წლიურ გეგმაში მოხვედრილ სხვა აუდიტებთან და პროექტებთან შედარებით, ისევე როგორც სხვა სფეროების აუდიტის ვადებზე დამოკიდებულება.

ნებისმიერი გადაწყვეტილება შეთანხმებული უნდა იყოს აუდიტის სუბიექტის ხელმძღვანელთან.

ამ ინფორმაციაზე დაყრდნობით, შიდა აუდიტის სუბიექტმა ასევე უნდა გადააფასოს აუდიტის გეგმაში მითითებული პირველადი ბიუჯეტი (მათ შორის, აუდიტზე გამოყოფილი დრო და ხარჯები). ყოველწლიური დაგეგმვის პროცესის შემდეგ მომხდარი ცვლილებების

გათვალისწინებით, როგორც ორგანიზაციის შიგნით, ისე აუდიტის რესურსების ხელმისაწვდომობის მხრივ, შესაძლოა, პირველადი მასშტაბისა და ბიუჯეტის დეტალური დაგეგმვის დაწყებამდე, მიზანშეწონილი იყოს კორექტირება.

შიდა აუდიტის მიერ ზემოთ მოცემული ფაქტორების და გარემოებების შეფასების შემდეგ ხდება საბოლოო გადაწყვეტილების მიღება, ჩატარდეს დაგეგმილი აუდიტი, თუ მოხდეს მისი გადადება (მოგვიანებით წლის განმავლობაში ან მომდევნო წელს) ან საერთოდ იქნას ამოღებული აუდიტის გეგმიდან.

2.3 შიდა აუდიტის ინდივიდუალური გეგმა

შიდა აუდიტის ყველა პროექტისთვის, შიდა აუდიტის სუბიექტის ხელმძღვანელმა უნდა შეიმუშაოს და დაამტკიცოს აუდიტის ინდივიდუალური გეგმა, რომელიც აუცილებელია დასახული აუდიტის მიზნების ეფექტიანობისა და პროდუქტიულობის უზრუნველსაყოფად. ინდივიდუალური აუდიტის გეგმის მომზადების დეტალური ინსტრუქციები აღწერილია ქვემოთ, მე-3 თავში.

2.4 რეკომენდებული შაბლონები

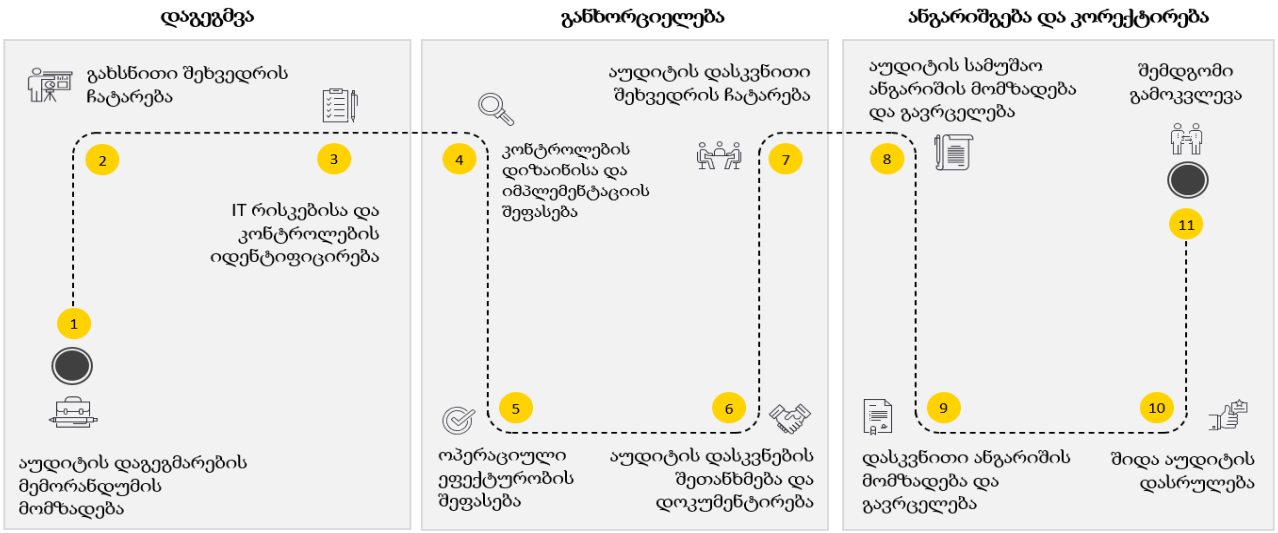
წლიური დაგეგმვის პროცესის გასაადვილებლად რეკომენდებულია შემდეგი შაბლონის გამოყენება

- **001 რისკებზე დაფუძნებული შიდა IT აუდიტის გეგმის მომზადება (შაბლონი).**

3 შიდა აუდიტის პროცესი

ამ თავში აღწერილია შიდა აუდიტორული პროექტების მართვის პროცესის ძირითადი ეტაპები და თითოეული მათგანის ეფექტურად განხორციელების მიდგომები. IT აუდიტის განხორციელების პროცესი, ზოგადად, არ განსხვავდება სხვა ტიპის შიდა აუდიტორული სამუშაოს განხორციელების პროცესისგან. შიდა აუდიტორი გეგმავს აუდიტს, ახდენს შესაბამისი რისკებისა და კონტროლების იდენტიფიცირებას და დოკუმენტირებას, აფასებს კონტროლის დიზაინს, იმპლემენტაციას და ოპერაციულ ეფექტურობას, აყალიბებს დასკვნებს მიგნებებს, რეკომენდაციებს და წარადგენს შიდა აუდიტორულ ანგარიშებს.

ქვემოთ მოცემულ დიაგრამა 6-ზე წარმოდგენილია IT აუდიტის ძირითადი ეტაპებისა და აქტივობების სტანდარტიზებული და თანმიმდევრული ხედვა:



დიაგრამა 6: *აუდიტის ძირითადი ეტაპებისა და აქტივობების სტანდარტიზებული და თანმიმდევრული ბლოკ-სქემა*

3.1 დაგეგმვა

დროული და სწორი დაგეგმვა გადამწყვეტ როლს თამაშობს შიდა IT აუდიტის პროექტის წარმატებით განხორციელებაში. ამ მიზნით, შიდა აუდიტის სუბიექტის ხელმძღვანელმა ან აუდიტის ჯგუფის უფროსმა (ე. წ. „Audit Team Leader (ATL)“) უნდა განსაზღვროს აუდიტის საერთო სტრატეგია და მოამზადოს **110 აუდიტის დაგეგმვის მემორანდუმი**. აღნიშნული დოკუმენტი ასახავს აუდიტის მიზნებს, მასშტაბს, ვადებს, რესურსების განაწილებას და აუდიტის მიდგომას და საბოლოოდ ხელს უწყობს **210 აუდიტის სამუშაო პროგრამის** შექმნას.

მიუხედავად იმისა, რომ IT აუდიტის ინდივიდუალური გეგმა ძირითადად ემთხვევა სხვა ტიპის აუდიტის გეგმებს, წინამდებარე სახელმძღვანელოს მიზნებისთვის, ყურადღება ეთმობა ქვემოთ მოცემულ დამატებით ფაქტორებს:

- გარკვეული IT სფეროების აუდიტს ახორციელებს IT აუდიტორთა სპეციალიზებული ჯგუფი, თუმცა IT მხარდაჭერის მქონე ბიზნეს პროცესების აუდიტი ითვალისწინებს ღირებულებათა სრულ ჯაჭვს და, შესაბამისად, მოითხოვს მჭიდრო თანამშრომლობას სხვა მიმართულების IT აუდიტის სპეციალისტებთან. ნაკლებად მნიშვნელოვანია, რომელი მხარე უძღვება პროექტს, ამ მხრივ, უმთავრეს ამოცანას წარმოადგენს, ეფექტური თანამშრომლობის გზით აუდიტის ოპტიმალური შედეგების უზრუნველყოფა;
- თუ ორგანიზაციაში არ არსებობს IT კონტროლების ჩარჩო, შიდა აუდიტის სუბიექტის ხელმძღვანელმა ან აუდიტის ჯგუფის უფროსმა უნდა შეარჩიოს ორგანიზაციის მიზნების და არსებული IT გარემოს შესაბამისი საუკეთესო ჩარჩო. აღნიშნული საკითხი დეტალურად არის განხილული წინამდებარე დოკუმენტის 3.1.1.1 „საწყისი დაგეგმვის განხორციელება“ თავის „პროექტების კრიტერიუმები“ ქვე-თავში;

- აუდიტის ტესტირების ინსტრუმენტები უნდა შეირჩეს ხარჯებისა და სარგებლის დეტალური ანალიზის საფუძველზე და ხელი უნდა შეუწყოს მონაცემთა ვრცელი მასივების თანმიმდევრულ და ეფექტიან შეფასებას;
- ხელმძღვანელობისთვის ანგარიშის სტრუქტურა უნდა ითვალისწინებდეს სამიზნე აუდიტორიისთვის მხოლოდ აუცილებელი ინფორმაციის დეტალიზაციის დონეს და არ უნდა ახდენდეს სასარგებლო ინფორმაციის გადაფარვას არასაჭირო დეტალებით.

მიუხედავად იმისა, რომ დაგეგმვის აქტივობები ძირითადად ხორციელდება აუდიტის საწყის ეტაპზე, აღნიშნული წარმოადგენს უწყვეტ პროცესს და უწყვეტად გრძელდება აუდიტის შემდეგ ეტაპებზეც.

3.1.1 შიდა აუდიტისთვის მომზადება

3.1.1.1 საწყისი დაგეგმვის განხორციელება

შიდა აუდიტის სუბიექტის ხელმძღვანელმა ან შიდა აუდიტის ჯგუფის უფროსმა უნდა ჩაატაროს დაგეგმვის წინარე შეხვედრა შიდა აუდიტის სუბიექტის თანამშრომლებთან, რათა განიხილოს წლიური შეფასების პროცესში გამოვლენილი IT რისკები, აუდიტირებად IT პროცესში არსებული რისკები და ჯგუფთან ერთად მიიღოს საბოლოო გადაწყვეტილება შიდა აუდიტის მიზნებთან დაკავშირებით.

ორგანიზაციისა და მისი გარემოს შესწავლა

რისკების გამოვლენისათვის, რისკზე დაფუძნებული მიდგომა, პირველ რიგში, მოითხოვს ორგანიზაციისა და მისი გარემოს დეტალურ შესწავლას. აუდიტორის გამოცდილება, ტექნიკური ცოდნა და განსჯის უნარი წარმოადგენს გადამწყვეტ ფაქტორს, რათა ყურადღება გამახვილდეს ანალიზისთვის საჭირო მხოლოდ საკვანძო და მნიშვნელოვან ინფორმაციაზე, რაც არასაჭირო ინფორმაციის უგულვებელყოფის გზით, იძლევა დროისა და სხვა რესურსების დაზოგვის შესაძლებლობას.

აუდიტის ობიექტისა და აუდიტირებადი პროცესის შესწავლის მიზნით საჭიროა შემდეგი ინფორმაციის გაანალიზება:

- IT-სთან დაკავშირებული ოპერაციული მიზნები ან/და ამოცანები;
- ორგანიზაციული სტრუქტურა;
- IT სამსახურის ორგანიზაციული სტრუქტურა (მაგ., ცენტრალიზებული ან დეცენტრალიზებული, ანგარიშგების და ზედამხედველობის სტრუქტურა);
- ძირითადი IT პროცესების იერარქია და მოდელი;
- ძირითადი IT პერსონალის კვალიფიკაცია და კომპეტენცია;
- IT პერსონალის დენადობა და ა.შ..

აღნიშნული ეტაპი მიზნად არ ისახავს უშუალოდ IT აუდიტის პროექტის ფარგლებში გასათვალისწინებელი ყველა რისკისა და სისუსტის გამოვლენას. ზოგადად, შიდა

აუდიტორები პასუხისმგებელნი არიან დაგეგმვის ეტაპის დასრულების შემდეგაც მაქსიმალური ყურადღება გამოიჩინონ შესაძლო რისკის მიმართ და პროექტის მსვლელობისას მოახდინონ მათი დროული მართვა.

პროექტის მიზნები

აუდიტის პროექტის მიზნები უნდა განისაზღვროს იმგვარად, რომ ხელი შეუწყოს ორგანიზაციის უნარს სათანადოდ მართოს ბიზნეს და IT რისკები ეფექტური მმართველობის, რისკების მართვისა და კონტროლის სისტემის მეშვეობით.

შიდა IT აუდიტის პროექტის მიზნები:

- უნდა შეესაბამებოდეს ორგანიზაციულ მიზნებს;
- უნდა ასახავდეს აუდიტირებად პროცესთან/აქტივობასთან დაკავშირებული IT რისკების წინასწარი შეფასების შედეგებს.

პროექტის მიზნების ჩამოსაყალიბებლად ინფორმაციის ძირითად წყაროებს წარმოადგენს:

- შიდა აუდიტის საგანთან მიმართებით ორგანიზაციის მისიის, ხედვის და მიზნების მიმოხილვა;
- შიდა აუდიტის წლიური გეგმის მიმოხილვა;
- წინა პროექტის შედეგების მიმოხილვა;
- გასაუბრება ძირითად დაინტერესებულ პირებთან. მსგავსი ინტერვიუები, როგორც წესი, ხელს უნდა უწყობდეს შიდა აუდიტის საგნის მიზნების, დიზაინის, ოპერაციების და კონტროლების გარემოს უკეთ გააზრებას.

აუდიტის კრიტერიუმები

აუდიტორული შეფასების განხორციელებამდე შიდა აუდიტის ჯგუფის უფროსმა უნდა შეარჩიოს შესაბამისი აუდიტის კრიტერიუმი. **აუდიტის კრიტერიუმი** წარმოადგენს სტანდარტს/სამიზნე მდგომარეობას, რომლის მიმართაც უნდა მოხდეს აუდიტის საგნის შეფასება.

გონივრული რწმუნება შესაძლებელია მიღებულ იქნას მხოლოდ იმ შემთხვევაში, თუ დასკვნები კეთდება რელევანტურ კრიტერიუმთან მიმართ შეფასების საფუძველზე.

არსებობს შიდა აუდიტის კრიტერიუმის სამი ძირითადი ტიპი:

- შიდა (მაგ., დაწესებულების პოლიტიკები და პროცედურები);
- გარე (მაგ., სახელმწიფო/ადგილობრივი თვითმმართველობის ორგანოს ან თანამდებობის პირის მიერ მიღებული სამართლებრივი აქტები და შეთანხმებები);
- წამყვანი პრაქტიკები (მაგ. ინდუსტრიული და პროფესიული სახელმძღვანელოები, საერთაშორის კონტროლების ჩარჩოები).

გარე, შიდა, თუ წამყვან პრაქტიკებზე დაფუძნებული კრიტერიუმი უნდა აკმაყოფილებდეს შემდეგ მახასიათებლებს:

კრიტერიუმი	მახასიათებლები
რელევანტური	რელევანტური კრიტერიუმის საფუძველზე იქმნება აუდიტის საგანთან დაკავშირებული ინფორმაცია, რომელიც ხელს უწყობს სამიზნე აუდიტორიის მიერ გადაწყვეტილების მიღების პროცესს
სრული	კრიტერიუმი სრულია, როდესაც მის საფუძველზე მომზადებულ ინფორმაციას აუდიტის საგნის შესახებ არ აკლია რელევანტური ფაქტორები, რომლებსაც შესაძლოა გავლენა ჰქონდეს ხელმძღვანელობის გადაწყვეტილებებზე
სანდო	სანდო კრიტერიუმი უზრუნველყოფს სხვა აუდიტორის მიერ იმავე გარემოებებში იდენტური დასკვნების გამოტანას
ნეიტრალური	ნეიტრალური კრიტერიუმი განაპირობებს მიუკერძოებელი ინფორმაციის მიღებას
გასაგები	გასაგები კრიტერიუმის გამოყენების შედეგად მიიღება ინფორმაცია და დასკვნები, რომლებიც ასევე მარტივად გასაგებია სამიზნე აუდიტორიისთვის
სასარგებლო	სასარგებლო კრიტერიუმის გამოყენება განაპირობებს იმგვარ მიგნებებსა და დასკვნებს, რომლებიც აკმაყოფილებს ინფორმაციასთან დაკავშირებით ხელმძღვანელობის საჭიროებებსა და მოლოდინებს

როგორც წესი, შიდა აუდიტის კრიტერიუმად გამოიყენება დარგის წამყვანი კონტროლების ჩარჩოები, რომელთა მიმართაც ფასდება IT პროცესებისა და დაკავშირებული კონტროლების დიზაინი და ოპერაციული ეფექტურობა. კონტროლების ჩარჩო ხელს უწყობს IT კონტროლების შესაბამისი დონის განსაზღვრას და მათი ეფექტურობის შემოწმებას.

გარდა ამისა, აღნიშნული ჩარჩოები ეხმარება ორგანიზაციის ხელმძღვანელობას:

- IT კონტროლების ამოცანების/მიზნების სწორად ფორმულირებაში;
- ინფორმაციული ტექნოლოგიების ბიზნეს პროცესებთან და კონტროლის ჩარჩოებთან თავსებადობის უზრუნველყოფაში;
- ძირითადი IT სფეროების გამოვლენაში და მათ სწორად ორგანიზებაში;
- პროცესის მოდელის შექმნაში, რომელიც ლოგიკურად აჯგუფებს IT პროცესებს.

IT კონტროლების ჩარჩოს შერჩევა გულისხმობს გადაწყვეტილების მიღებას, თუ რომელი მოდელი მოუტანს ორგანიზაციას ყველაზე მეტ სარგებელს, ვინაიდან ორგანიზაციის მასშტაბით მოდელს იყენებს კონტროლის პასუხისმგებლობის მქონე თანამშრომლების დიდი რაოდენობა. უნდა აღინიშნოს, რომ ჩარჩოები შემუშავებულია ფართო გამოყენებისთვის და არცერთი მათგანი არ ითვალისწინებს ყველა ტიპის საქმიანობას ან IT მოწყობას. შესაბამისად, შერჩეული ჩარჩო უნდა მოერგოს კონკრეტული ორგანიზაციისა და მისი გარემოს საჭიროებებს.

დარგის წამყვანი IT კონტროლების ჩარჩოები

კონტროლის ამოცანები ინფორმაციული და დაკავშირებული ტექნოლოგიებისთვის (ე. წ. „COBIT“)

„COBIT“ არის საინფორმაციო სისტემების აუდიტისა და კონტროლის ასოციაციის (ე. წ. „ISACA“) მიერ შექმნილი, საერთაშორისო აღიარების მქონე ჩარჩო, რომელიც ეხმარება ორგანიზაციებს:

- IT როლის და ორგანიზაციულ სტრატეგიაში მისი ადგილის განსაზღვრაში;
- IT-ს და მისი შედეგების გაუმჯობესებაში;
- IT რესურსებისგან მეტი ღირებულების შექმნაში, მარეგულირებელი მოთხოვნების დაკმაყოფილებაში და ცნობიერების ამაღლების გზით IT რისკების უკეთ მართვაში.

IT ინფრასტრუქტურის ბიბლიოთეკა (ე. წ. „ITIL“)

ე. წ. „ITIL“ არის მართვის ჩარჩო, რომელიც აყალიბებს IT სერვისების მიწოდების საუკეთესო პრაქტიკებს. ITIL-ის მიზანია დაეხმაროს ორგანიზაციებს შექმნან პროგნოზირებადი IT გარემო, ისევე როგორც პროცესების გამარტივებით და ეფექტიანობის გაუმჯობესების შესაძლებლობების გამოვლენით, უზრუნველყონ მომხმარებლები საუკეთესო მომსახურებით.

IT აუდიტის ფარგლებში, ITIL-ის კრიტერიუმად გამოყენება ხელს უწყობს პრობლემების იდენტიფიცირებას და გადაჭრას, ასევე ბიზნეს მიზნებისა და საუკეთესო პრაქტიკის შესაბამისად IT სერვისის მიწოდების შეფასებას.

ISO/IEC 27001 უსაფრთხოების სტანდარტი

ISO/IEC 27001 არის უსაფრთხოების საერთაშორისო სტანდარტი, რომელიც ასახავს ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) შემუშავების, დანერგვის, მხარდაჭერისა და მუდმივი გაუმჯობესების მოთხოვნებს. ის წარმოადგენს ორგანიზაციის მიერ ინფორმაციული აქტივების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დაცვის სისტემურ მიდგომას.

სტანდარტი სთავაზობს ორგანიზაციებს კონტროლების ჩარჩოს, რათა დაეხმაროს მათ რისკების მინიმიზაციისთვის საჭირო კონტროლების გამოვლენაში და დანერგვაში.

შიდა ორგანიზაციული და ISO 27001 სტანდარტის მოთხოვნებთან შესაბამისობის დასადასტურებლად, ორგანიზაციამ, წინასწარ განსაზღვრული ინტერვალებით, უნდა უზრუნველყოს შიდა აუდიტის ჩატარება.

ინფორმაციულ ტექნოლოგიებთან, ინფორმაციულ უსაფრთხოებასა და/ან პერსონალურ მონაცემთა დაცვასთან დაკავშირებული ადგილობრივი რეგულაციები

საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მონაცემთა დამმუშავებლებს ავალდებულებს შეიმუშაონ ორგანიზაციული და ტექნიკური ღონისძიებები, რათა უზრუნველყონ მონაცემთა დაცვა შემთხვევითი ან უკანონო განადგურებისაგან, ცვლილებისგან, გამჟღავნებისგან, მოპოვების ან სხვა სახის არაკანონიერი გამოყენებისგან.

კანონის თანახმად, ორგანიზაციულ-ტექნიკური ღონისძიებები მიმართული უნდა იყოს ფიზიკური პირების უფლებებსა და თავისუფლებებთან დაკავშირებულ რისკებზე, რაც გულისხმობს მონაცემთა დამუშავების პრინციპების ეფექტურად დაცვას და კანონით გათვალისწინებულ სხვა ვალდებულებებს.

საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ

2012 წლიდან საქართველოში მოქმედებს კანონი ინფორმაციული უსაფრთხოების შესახებ, რომელიც საქართველოს მთავრობის დადგენილებით განსაზღვრულ კრიტიკული ინფორმაციული სისტემების სუბიექტებისთვის (შემდგომში - „სუბიექტი“) აყალიბებს ინფორმაციული უსაფრთხოების მინიმალურ სტანდარტებს.

კანონი ავალდებულებს სუბიექტებს დანერგონ ინფორმაციული უსაფრთხოების მართვის სისტემა (შემდგომში - „იუმს“).

ზემოაღნიშნული კანონი და სხვა კანონქვემდებარე ნორმატიული აქტები ახდენენ ისეთი IT და ინფორმაციული უსაფრთხოების საკითხების რეგლამენტირებას, როგორიცაა წვდომის კონტროლი, ინფორმაციის კლასიფიკაცია და მართვა, ფიზიკური და გარე უსაფრთხოება, სარეზერვო ასლების დაცვა და სხვა. შესაბამისად, შიდა აუდიტის სამსახურს შეუძლია მათი აუდიტის კრიტერიუმის სახით გამოყენება.

აუდიტის მასშტაბი

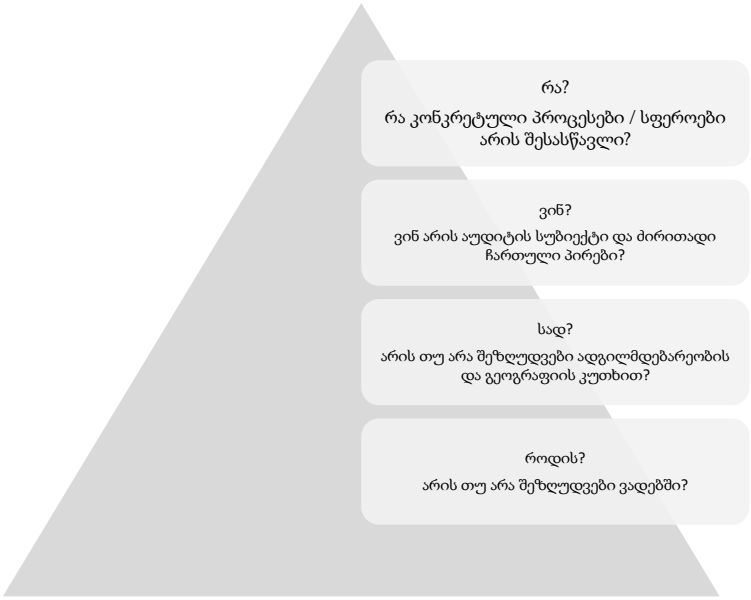
აუდიტის მიზნების, კრიტერიუმებისა და პროცედურების ერთობლიობა განსაზღვრავს პროექტის მასშტაბს. თავის მხრივ, პროექტის მასშტაბი აყალიბებს საზღვრებს, კონკრეტულად რისი დაფარვა უნდა მოხდეს შიდა აუდიტის ფარგლებში. აგრეთვე, ის შესაძლოა აღწერდეს შიდა აუდიტორული შემოწმების სახეობას, ფორმებს, მოცულობას და უზრუნველყოფდეს დამატებითი დამხმარე ინფორმაციის წარმოდგენას.

შიდა აუდიტის მიზნებსა და მასშტაბს განსაზღვრავს შიდა აუდიტის ჯგუფის უფროსი. საკონსულტაციო პროექტების (მაგ., შესყიდვების განყოფილება გეგმავს პროგრამული უზრუნველყოფის შეძენას და ავტომატიზაციას) შემთხვევაში, მიზნები და მასშტაბი ერთობლივად განისაზღვრება შიდა აუდიტის ჯგუფის უფროსისა და საკონსულტაციო მომსახურების მიმღების მიერ.

როგორც წესი, პროექტის მასშტაბის განსაზღვრისას ყურადღება ექცევა შემდეგ ფაქტორებს:

- შიდა აუდიტის მიზნები;
- დაკავშირებული რისკების პირველადი შეფასება;
- აუდიტის საგნის საზღვრები;
- ქვე-პროცესები;
- საქმიანობის ადგილმდებარეობა და გეოგრაფია;
- IT გარემო და მისი კომპონენტები;
- შიდა აუდიტის არსებული რესურსები (ადამიანური/სხვა).

პროექტის მასშტაბი ასევე უნდა ითვალისწინებდეს, მესამე მხარის კონტროლქვეშ არსებულ სისტემებს, დოკუმენტებს, პერსონალსა და ფიზიკურ ადგილმდებარეობას.



დიაგრამა 7: *აუდიტის მასშტაბის განმსაზღვრელი ფაქტორები*

3.1.1.2 შიდა აუდიტის ჯგუფის შერჩევა

აუდიტის პროექტის ხარისხი და აუდიტის ობიექტის საერთო კმაყოფილება მნიშვნელოვნად არის დამოკიდებული შიდა აუდიტის ჯგუფის წევრების მხრიდან კონკრეტული საქმიანობისა და გამოყენებული IT პროგრამული გადაწყვეტების ცოდნის ხარისხზე. აუდიტის დაგეგმვისას აუდიტის სუბიექტის ხელმძღვანელმა უნდა განსაზღვროს ძირითადი IT უნარები და კომპეტენციები, რომლებიც საჭიროა შერჩეული პროექტის წარმატებისთვის. განსაკუთრებული ყურადღება უნდა დაეთმოს ისეთ უნარებსა და კომპეტენციებს, რომელთათვისაც შეიძლება საჭირო გახდეს წინასწარი ზომების მიღება (მაგ., ტრენინგების ორგანიზება, გარე რესურსების გამოყენება (ე. წ. „Outsourcing“), ან კონკრეტული გამოცდილების მქონე შიდა აუდიტორის გამოთავისუფლება სხვა პროექტებიდან).

ჯგუფის შერჩევისას შიდა აუდიტის ჯგუფის უფროსმა უნდა გაითვალისწინოს შემდეგი ფაქტორები:

- **შიდა აუდიტის მიზნები და მათი ზეგავლენა საჭირო უნარებსა და კომპეტენციებზე.** ტექნიკურ ცოდნასთან ერთად, ჯგუფის ხელმძღვანელმა, ასევე უნდა გაითვალისწინოს სოციალური (ე. წ. „Soft“) უნარების საჭიროება, განსაკუთრებით ისეთი სენსიტიური სფეროების აუდიტის დროს, როგორიცაა IT მმართველობა. ამ პროექტის განსახორციელებლად შესაძლოა საჭირო გახდეს გამოცდილი და მაღალი რეპუტაციის მქონე პერსონალის ჩართვა;
- **საჭირო ცოდნისა და უნარების მქონე პერსონალის ხელმისაწვდომობა.** სწორად გამოყენების შემთხვევაში, სპეციალიზებული IT უნარები წარმოადგენს ფასდაუდებელ რესურს. თუ ხელმისაწვდომი აუდიტორების უნარები არ არის საკმარისი, აუდიტის ჯგუფის უფროსმა უნდა განიხილოს დამატებითი ტრენინგის საჭიროება, ან უფრო ინტენსიური ზედამხედველობა აუდიტის პროცესში;
- **შიდა აუდიტის ვადები.** აღნიშნული შესაძლოა იწვევდეს სირთულეებს თუ ანგარიში საჭიროა შესაბამისობის დადასტურების ან კომპლექსური შესწავლის (ე. წ. „Due Diligence“) მიზნებისთვის. გარდა ამისა, შესაძლოა აუცილებელი იყოს აუდიტის დროული დასრულება სხვა მნიშვნელოვან პროექტებზე გადასასვლელად;
- **აქტივობის პრიორიტეტულობა.** შესაძლოა საჭირო გახდეს აუდიტორის გეგმით გათვალისწინებული უფრო მაღალი პრიორიტეტის მქონე აუდიტში ჩართვა.

ზემოაღნიშნული ანალიზის საფუძველზე, შიდა აუდიტის ჯგუფის მხარდაჭერის ან არსებული რესურსების, უნარებისა და კომპეტენციების შევსების მიზნით, შესაძლოა საჭირო გახდეს გარე მომსახურების გამოყენება.

3.1.1.3 ბიუჯეტის განსაზღვრა

ბიუჯეტის დადგენა წარმოადგენს პროექტის დაგეგმვის მნიშვნელოვან ასპექტს. ხშირად ის წარმოადგენს პროექტის კონტროლის ძირითად მექანიზმს.

პროექტის ბიუჯეტი მოიცავს ინფორმაციას გამოყოფილი დროის შესახებ, რადგან დრო არის შიდა აუდიტორული საქმიანობის მთავარი ფაქტორი. ბიუჯეტით განსაზღვრული ვადები უნდა იყოს რეალისტური და შესრულებადი.

ქვემოთ მოცემულ ფაქტორებს შესაძლოა ზეგავლენა ქონდეთ პროექტის დაგეგმილ ვადაზე:

- შიდა აუდიტის ჯგუფის კოლექტიური უნარები და გამოცდილება;
- ლოგისტიკა მატერიალურ-ტექნიკური მომარაგება (მაგ.: კლიენტის ხელმისაწვდომობა, ადგილმდებარეობა, მივლინებისა და მგზავრობისთვის საჭირო დრო);
- ტექნოლოგიების ხელმისაწვდომობა, რომელიც სასარგებლო ან საჭიროა პროექტის წარმატებით განსახორციელებლად.

3.1.1.4 შიდა აუდიტის წერილის მომზადება

შიდა აუდიტის ობიექტი და სხვა დაინტერესებული მხარეები, შიდა აუდიტის წლიური გეგმის ან შიდა აუდიტის სუბიექტის ხელმძღვანელთან კომუნიკაციის საფუძველზე, მოსამზადებელი ეტაპის დაწყებამდე, შესაძლოა წინასწარ ფლობდნენ ინფორმაციას დაგეგმილი აუდიტის შესახებ. თუმცა, შიდა აუდიტის ობიექტისთვის აუდიტის შესახებ ოფიციალური შეტყობინების გაგზავნა იძლევა აუდიტის დაწყების ფორმალურ უფლებამოსილებას. გარდა ამისა, მნიშვნელოვანია, ყველა ჩართულ მხარეს ჰქონდეს.

მკაფიო წარმოდგენა აუდიტის ზოგადი მასშტაბისა და ვადების შესახებ. ოფიციალური შეტყობინებისთვის, როგორც წესი, გამოიყენება აუდიტის წერილი, რომელსაც შიდა აუდიტის სუბიექტის ხელმძღვანელი უგზავნის ძირითად დაინტერესებულ მხარეებს.

3.1.1.5 გახსნითი შეხვედრის ჩატარება

მიუხედავად იმისა, რომ ჩვეულებრივ აუდიტის ჯგუფის უფროსი, ფიზიკური აქტივობების დაწყებამდე, ხვდება ან ესაუბრება აუდიტის ობიექტს, გახსნითი შეხვედრა მიანიშნებს ადგილზე შესასრულებელი სამუშაოების ოფიციალურ დაწყებაზე. როგორც პირველი ოფიციალური კონტაქტი შიდა აუდიტსა და აუდიტის ობიექტის ხელმძღვანელობას შორის, გახსნითი შეხვედრა საჭიროებს საფუძვლიან დაგეგმვას და მომზადებას.

გარდა ამისა, გახსნითი შეხვედრა განსაზღვრავს შემდგომი პროექტის კურსს. კარგი პრეზენტაციის შედეგად ჩამოყალიბებული ნდობა უზრუნველყოფს გაუმჯობესებულ ურთიერთთანამშრომლობას და უფრო ეფექტურ აუდიტს. პირველი კონტაქტი დიდ გავლენას ახდენს აუდიტის ობიექტის საერთო შთაბეჭდილებაზე, თუ რამდენად კარგად იცნობს შიდა აუდიტის ჯგუფი აუდიტირებად საქმიანობას და რამდენად არის მზად აუდიტის წარმატებით განსახორციელებლად.

აუდიტის ჯგუფის უფროსს ასევე უნდა ესმოდეს, რომ აუდიტორული საქმიანობა ხშირად იწვევს გაურკვევლობას და წინააღმდეგობას აუდიტის ობიექტში. ამრიგად, გახსნითი შეხვედრა, აუდიტის ობიექტისთვის აუდიტის შედეგად მიღებული პოტენციური სარგებლის განმარტების მიღებით, წარმოადგენს საუკეთესო შესაძლებლობას ამგვარი გაურკვევლობის ან წინააღმდეგობის აღმოსაფხვრელად.

3.1.1.6 დაგეგმვის მემორანდუმის შემუშავება

დაგეგმვის ეტაპზე შეგროვებული ინფორმაცია ზუსტად უნდა აისახოს დაგეგმვის მემორანდუმში შიდა აუდიტის სუბიექტის ხელმძღვანელის ან აუდიტის ჯგუფის უფროსის მიერ. კერძოდ, დაგეგმვის მემორანდუმი უნდა აყალიბებდეს ზოგად ხედვას ორგანიზაციის შესახებ და მოიცავდეს აუდიტირებად IT პროცესებს და დაკავშირებულ სტრუქტურულ ერთეულებს, აუდიტის მიზნებს, კრიტერიუმებს, მასშტაბს, დაკავშირებულ რისკებს, ბიუჯეტს, ვადებს და ძირითადი პროცესის მფლობელ(ებ)ის საკონტაქტო ინფორმაციას. ამასთან, დაგეგმვის მემორანდუმი უნდა აღწერდეს სფეროებს, რომლებიც ვერ მოხვდნენ აუდიტის საბოლოო მასშტაბში. ასეთი გადაწყვეტილების არგუმენტები ასევე უნდა იყოს დოკუმენტირებული. დეტალური ინფორმაციისთვის იხილეთ **130 დაგეგმვის მემორანდუმის შაბლონი.**

3.1.2 IT პროცესების გაგება

აუდიტის საგნის, მიზნებისა და მასშტაბის განსაზღვრისა და დაგეგმვის მემორანდუმის შემუშავების შემდეგ, შიდა აუდიტმა უნდა შეადგინოს აუდიტირებადი IT პროცესების აღწერის დოკუმენტი. აღნიშნული, თავის მხრივ, ხელს უწყობს IT რისკებისა და კონტროლების გამოვლენას და შესაბამისი აუდიტორული პროცედურების დაგეგმვას.

IT პროცესი არის აქტივობების ერთობლიობა, რომელიც უზრუნველყოფს IT გარემოს გამოყენებით ბიზნესის საჭიროებების დაკმაყოფილებას (მაგ., პროგრამული უზრუნველყოფის ცვლილება, მომხმარებლებისთვის წვდომის უზრუნველყოფა, მომხმარებლების წვდომის გაუქმება, კომპიუტერული პროგრამების ფუნქციონირების მონიტორინგი).

აუდიტირებადი პროცესის შესწავლის მიზნით შიდა აუდიტის ჯგუფი იყენებს ქვემოთ ჩამოთვლილი მიდგომების კომბინაციას:

- IT ხელმძღვანელობისა და IT პროცესების განხორციელებაში უშუალოდ ჩართული პერსონალის დეტალური გამოკითხვა;
- პროცესის ფარგლებში გამოყენებულ მეთოდებსა და პროცედურებზე დაკვირვება;
- სახელმძღვანელოების, სისტემური დოკუმენტაციის, პროცედურების და სხვა წერილობითი ინსტრუქციების განხილვა;
- პროცესის დეტალური გავლა (ე. წ. „walkthrough“).

აუდიტის დოკუმენტაცია უნდა აღწერდეს, როგორც ხელით შესასრულებელ, ასევე ავტომატიზებულ დამუშავების პროცედურებს. ორივე ტიპის დამუშავების პროცედურების განხილვა არსებით როლს თამაშობს არსებული კონტროლის სისტემის შესახებ სრული წარმოდგენის შექმნაში. რთული ან უჩვეულო სისტემების გამოყენების შემთხვევაში, შიდა აუდიტის ჯგუფმა უშუალოდ უნდა იმუშაოს გამოყენებული ტექნოლოგიების ხელმძღვანელობასთან, რათა მოიპოვოს სრულყოფილი წარმოდგენა ძირითადი პროცედურების შესახებ.

დოკუმენტაციის მომზადებისას, შიდა აუდიტის ჯგუფი ფოკუსირებული უნდა იყოს პროცესის მიზანზე, მფლობელზე, პროცესის ეტაპზე, შემავალ ინფორმაციაზე და პროცესის შედეგებზე, ნაცვლად სრული პროცესის დეტალური და ვრცელი დოკუმენტაციის მომზადებისა, რაც ძალიან შრომატევადი და ძვირია.

შერჩეული IT პროცესის დიზაინის დოკუმენტირებისთვის აუდიტორმა უნდა გამოიყენოს დოკუმენტის შაბლონი „**140 IT პროცესის, რისკების და კონტროლების შესწავლა**“.

3.1.2.1 IT რისკებისა და კონტროლების იდენტიფიცირება

IT პროცესის აღქმის გათვალისწინებით, შიდა აუდიტმა უნდა განსაზღვროს პროცესთან დაკავშირებული რისკები და არსებული შემარბილებელი კონტროლის მექანიზმები. თითოეული მნიშვნელოვანი ქვე-პროცესისთვის უნდა განისაზღვროს შემდეგი ინფორმაცია:

- **დაკავშირებული რისკი** - ნალბათობა ისეთი მოვლენის მოხდენისა, რომელმაც შესაძლოა უარყოფითი გავლენა იქონიოს ორგანიზაციის მიზნების მიღწევასა და ამოცანების შესრულებაზე;
- **კონტროლის მექანიზმი** - ქმედებების ერთობლიობა, მიმართული რისკის მინიმიზაციაზე; უზრუნველყოფს ხარვეზების პრევენციას, მათ გამოვლენას ან გამოსწორებას;
- **კონტროლის სახეობა** - პრევენციული / აღმომჩენი / მაკორექტირებელი / მიმართული;
- **კონტროლის ტიპი** - მანუალური / ავტომატური;
- **კონტროლის სიხშირე** - მაგ., ყოველკვირეული, ყოველდღიური და ა. შ.

უმთავრეს მიზანს წარმოადგენს იმ ძირითადი კონტროლების იდენტიფიცირება, რომლებიც იძლევიან გონივრულ რწმუნებას იმის თაობაზე, რომ მათ შეუძლიათ დაკავშირებული რისკის ეფექტურად პრევენცია, ან დროულად გამოვლენა და გამოსწორება.

მაშინაც კი, როდესაც კონტროლების ერთობლიობა მთლიანობაში ეფექტურია, ცალკეული კონტროლის წვლილი ამ შედეგში, როგორც წესი, განსხვავდება და არათანაბარია. პროცესის აღწერის საფუძველზე, შიდა აუდიტმა ყურადღებით უნდა შეისწავლოს თითოეული კონტროლის როლი კონტროლის ერთიან სისტემაში. პროფესიული განსჯის გამოყენებით, აუდიტორმა უნდა გამოავლინოს ის „ძირითადი“ კონტროლი, რომლიც უზრუნველყოფს იდენტიფიცირებული რისკის პრევენციას, გამოვლენას ან გამოსწორების.

კონტროლების გამოვლენის შემდეგ, შიდა აუდიტორმა უნდა განსაზღვროს თითოეული კონტროლის დიზაინის პირველადი ეფექტურობა. აღნიშნული გულისხმობს იმის შეფასებას, თუ რამდენად შეუძლია კონტროლს არსებული ფორმით დაკავშირებული რისკის მისაღებ დონემდე შემცირება. შიდა აუდიტის წინასწარი შეფასება თითოეული კონტროლის დიზაინის ეფექტურობის შესახებ მოცემული უნდა იყოს ფორმებში **„140 IT პროცესების, რისკებისა და კონტროლების შესწავლა“** და **„210 აუდიტის სამუშაო პროგრამა“**. თუ კონტროლი არსებული ფორმით ვერ ახერხებს რისკის მისაღებ დონემდე შერბილებას, მაშინ კონტროლის ოპერაციული ეფექტურობის შეფასება კარგავს აზრს და ასეთი მიგნება ხარვეზის სახით უნდა აისახოს დოკუმენტში **„250 აუდიტის მიგნებების მატრიცა“**. თუმცა, გამონაკლისის სახით, აუდიტის მიგნების გასამყარებლად, შიდა აუდიტს შეუძლია განახორციელოს ამგვარი არაეფექტური კონტროლის შეზღუდული ტესტირება.

3.2 რეკომენდებული შაბლონები

დაგეგმვის ეტაპზე რეკომენდირებულია შემდეგი შაბლონების გამოყენება:

- **110 დაგეგმვის მემორანდუმი (შაბლონი);**
- **130 გახსნითი შეხვედრის ოქმი (შაბლონი);**
- **140 IT პროცესის, რისკების და კონტროლების შესწავლა (შაბლონი).**

3.3 განხორციელება

ამ ეტაპის მთავარი მიზანია პროცესის საკუთარი აღქმის დადასტურება დაგეგმვის ეტაპზე მიღებული ინფორმაციის საფუძველზე, კონტროლის დიზაინისა და დანერგვის ეფექტურობის შეფასება, შიდა აუდიტის პროცედურების დაგეგმვა, რომელიც უზრუნველყოფს საკმარისი და შესაბამისი აუდიტორული მტკიცებულებების მოპოვებას, და ბოლოს, დაგეგმილი აუდიტის პროცედურების შესრულება - დასკვნის მომზადების მიზნით.

3.3.1 პროცესის ჩვენეული აღქმის დადასტურება და კონტროლების დიზაინისა და იმპლემენტაციის შეფასება

ამ ეტაპზე შიდა აუდიტორმა უნდა დაადასტუროს პროცესის მისეული აღქმა, რომელიც მიიღო დაგეგმვის ეტაპზე და გააკეთოს დასკვნა IT კონტროლების დიზაინისა და მათი იმპლემენტაციის ეფექტურობასთან დაკავშირებით, პროცესის გავლის (ე.წ. „Walkthrough“) გამოყენებით.

3.3.1.1 პროცესის გავლა (ე.წ. „Walkthrough“)

პროცესის გავლის მიზანია ერთი მაგალითის (ე.წ. „sample of one“) გამოყენებით დაადგინოს, მოქმედებს და დანერგილია თუ არა პოლიტიკა და პროცედურები ისე, როგორც შემუშავებულია.

პროცესის გავლა მოიცავს პროცესის ან ამოცანის ეტაპობრივ დემონსტრირებას ან ახსნას, რომელსაც ახორციელებს პროცესის მფლობელი ან სხვა პასუხისმგებელი პირი შიდა აუდიტორის თანდასწრებით. შიდა აუდიტორმა უნდა გამოიყენოს პროცესის გავლა პროცესის უკეთ გასაგებად და კონტროლის ფაქტობრივი მდგომარეობის შესამოწმებლად - კერძოდ, რომელი კონტროლები მოქმედებს ჩვეულებრივ საქმიანობაში, რადგან ისინი ეფექტიანი და პროდუქტიულია რეალურ სამყაროში შესასრულებლად, და რომელია ზოგიერთ შემთხვევებში ან მუდმივად გამოტოვებული, შეცვლილი ან შეცდომით შესრულებული.

შიდა აუდიტორი ადასტურებს პროცესის საკუთარ აღქმას იმ პერსონალის გამოკითხვით და დაკვირვებით, რომელიც უშუალოდ იღებს მონაწილეობას კონტროლის განხორციელებაში, განიხილავს დოკუმენტებს, რომლებიც გამოიყენება და იქმნება კონტროლის გამოყენების შედეგად, და დამხმარე დოკუმენტებს ადარებს რეალურ ჩანაწერებს. მიუხედავად იმისა, რომ ძირითადი კონტროლი შეიძლება დაექვემდებაროს შემდგომ ტესტირებას, პროცესის მფლობელის აღქმა კონტროლის რეალური გამოყენების შესახებ მნიშვნელოვანია მისი ეფექტურობის შესახებ დასკვნის ფორმირებისთვის. ტიპური პროცესის გავლა შედგება შემდეგი კომპონენტებისგან:

- კითხვების დასმა კონტროლის განმახორციელებელი პირისთვის/გუნდისთვის;
- დაკავშირებული დოკუმენტების/კონტროლის მტკიცებულების მიმოხილვა;
- დამხმარე დოკუმენტების (მაგ., მტკიცებულებები, კონფიგურაციის აღწერის დოკუმენტები) შედარება სისტემის ჩანაწერებთან;
- პროცესის მფლობელის მიერ თვით-იდენტიფიცირებული პრობლემების დადასტურება.

პროცესის გავლის შედეგებზე დაყრდნობით, შიდა აუდიტორმა უნდა შეაფასოს დიზაინისა და იმპლემენტაციის ეფექტურობა. თითოეული გამოვლენილი კონტროლისთვის, შიდა აუდიტმა უნდა შეაფასოს, შესაძლებელია თუ არა რომ კონტროლი, დამოუკიდებლად ან ერთობლივად იყოს ეფექტური მიზნის მისაღწევად. ეს სრულდება იმის დადგენით, არის თუ არა თითოეული რელევანტური რისკი ეფექტურად შერბილებული ან გამოვლენილი და კორექტირებული იდენტიფიცირებული კონტროლების საშუალებით.

ოპერაციული ეფექტურობის შემდგომი შეფასებისთვის უნდა შეირჩეს მხოლოდ ისეთი IT კონტროლები, რომლებსაც აქვთ ეფექტური დიზაინისა და იმპლემენტაციის შეფასებები. შერჩეული კონტროლის მექანიზმებთან მიმართებით საბოლოო შეფასება აღრიცხულია აუდიტის სამუშაო პროგრამაში.

3.3.1.2 შიდა აუდიტის სამუშაო პროგრამის შემუშავება

შიდა აუდიტის სამუშაო პროგრამაში შეჯამებულია დაგეგმვის ფაზაში შესრულებული სამუშაოების შედეგები, ასევე IT პროცესების აღქმა, რისკებისა და კონტროლების იდენტიფიკაცია და IT კონტროლების დიზაინისა და იმპლემენტაციის შეფასება. შიდა აუდიტის ჯგუფისთვის ეს დოკუმენტი წარმოადგენს შიდა აუდიტის პროცესის ძირითად სახელმძღვანელოს.

გამოვლენილი რისკებისა და კონტროლების საპასუხოდ, შიდა აუდიტორებმა უნდა მოამზადონ ჩასატარებელი პროცედურებისა და ტესტების კონკრეტული ჩამონათვალი. დეტალური ინფორმაცია წარმოდგენილია ქვემოთ, **ოპერაციული ეფექტურობის შეფასების** თავში.

შიდა აუდიტის სამუშაო პროგრამა შიდა აუდიტის ჯგუფის უფროსმა უნდა დაამტკიცოს, მანამდე სანამ ჯგუფი დაიწყებს კონტროლების ოპერაციული ეფექტურობის ტესტირებას და აუდიტის ძირითადი პროცედურების ინტენსიურად შესრულებას. თუმცა, ძირითადი სამუშაოების დროს მიღებული ახალი ინფორმაციისა და ცოდნის გათვალისწინებით, შიდა აუდიტის სამუშაო პროგრამის კორექტირება შესაძლებელია შიდა აუდიტის ჯგუფის უფროსის მიერ დროული დამტკიცების შემთხვევაში.

3.3.2 ოპერაციული ეფექტურობის შეფასება

შიდა აუდიტორმა უნდა ჩაატაროს IT კონტროლის ოპერაციული ეფექტურობის ტესტირება იმის დასადგენად, ფუნქციონირებდა თუ არა IT კონტროლი მისი დიზაინის შესაბამისად აუდიტის პერიოდში. შიდა აუდიტორმა უნდა გაითვალისწინოს დიზაინის ატრიბუტები, რომლებიც მას ეფექტურს ხდის და შეიმუშაოს ტესტები იმის დასადგენად, იყო თუ არა წარმოდგენილი ან/და შესაბამისად ფუნქციონირებადი

ტესტირების ზოგადი ტექნიკები

შიდა აუდიტორს საკმარისი და შესაბამისი მტკიცებულებების მოსაპოვებლად შეუძლია არჩევანი გააკეთოს სხვადასხვა და ხშირად ერთმანეთის შემავსებელ ტექნიკებს შორის. შიდა აუდიტორმა უნდა შეინარჩუნოს გონივრული თანაფარდობა მტკიცებულების სანდოობასა და ამ

მტკიცებულების შეგროვების ტექნიკასთან დაკავშირებულ დროსა და რესურსებთან. ასეთი ტექნიკები მოიცავს შემდეგს:

- **გამოკითხვა:** პროცედურა გულისხმობს ინფორმაციის მოძიებას შესაბამისი პირებისგან, როგორც შიდა აუდიტის ობიექტის შიგნით, ასევე მის ფარგლებს გარეთ. გამოკითხვა, როგორც წესი, ფართოდ გამოიყენება აუდიტის განმავლობაში და ავსებს სხვა აუდიტორულ პროცედურებს. გამოკითხვა გამოსადეგია მაშინ, როდესაც მტკიცებულება არ არსებობს ან გაურკვეველია. უშუალოდ პროცედურა ხშირად ნაკლებად სანდოა, ვიდრე აუდიტორული მტკიცებულების სხვა ფორმები და შესაძლოა საჭირო გახდეს მისი სხვა ტესტირების ტექნიკასთან ერთად გამოყენება. მაგალითად, IT-ის ხელმძღვანელების გამოკითხვით შიდა აუდიტორს შეუძლია შეაგროვოს მრავალფეროვანი ინფორმაცია კონტროლის ეფექტურობის შესახებ, თუმცა პასუხები გამყარებული უნდა იყოს სხვა ტექნიკით;
- **დაკვირვება:** ფაქტობრივი დაკვირვება მოიცავს იმ თანამშრომლებზე უშუალო ვიზუალურ დაკვირვებას, რომლებიც ასრულებენ სამუშაოს, ასევე სხვა ფაქტებსა და მოვლენებზე დაკვირვებას. დაკვირვება იძლევა აუდიტორულ მტკიცებულებებს პროცესის ან პროცედურის განხორციელებასთან დაკავშირებით, მაგრამ ის შეზღუდულია დროის კონკრეტულ მომენტში, როდესაც ხდება დაკვირვება. მიუხედავად იმისა, რომ შიდა აუდიტორმა უნდა გაითვალისწინოს საკუთარი დასწრების გავლენა, დაკვირვებამ შესაძლოა უზრუნველყოს მნიშვნელოვანი მტკიცებულების მიღება თანამშრომლების სათანადოდ მომზადების და მათ მიერ პროცესის რეალურად განხორციელების შესახებ კონტროლის დიზაინის შესაბამისად. მაგალითად, შიდა აუდიტორს შეუძლია დააკვირდეს რედაქტირებისა და პაროლის კონტროლის ვერიფიკაციას. თუმცა, დაკვირვება იძლევა მტკიცებულებებს კონტროლის შესახებ მხოლოდ აუდიტორის თანდასწრებით. ასე რომ, შიდა აუდიტორს სჭირდება სხვა მტკიცებულებები, რომ დარწმუნდეს მთელი პერიოდის განმავლობაში კონტროლის იმავე სახით ფუნქციონირებაში;
- **შემოწმება და მოკვლევა:** შიდა აუდიტს შეუძლია შეაგროვოს მტკიცებულება ინსპექტირების, წაკითხვის, მოკვლევის, დამხმარე დოკუმენტების შესწავლის (ფიზიკური თუ ელექტრონული) ფორმატით და შედარების გზით. შიდა აუდიტორმა უნდა განიხილოს ნებისმიერი შემოწმებული დოკუმენტის სანდოობა და გაითვალისწინოს თაღლითობის რისკი ან/და შემოწმებული დოკუმენტების არა ავთენტურობა. აღნიშნული მეთოდი შეიძლება მოიცავდეს აპლიკაციაზე წვდომისთვის სისტემის მომხმარებლის მხოლოდ ერთი საიდენტიფიკაციო მონაცემის (ID) ფლობის ინსპექტირებას. ასევე მნიშვნელოვანია სასერვერო ოთახის და შესაბამისი კონტროლების ფიზიკური ინსპექტირება, მაგალითად: კარი, საკეტები, კვამლის დეტექტორები, ხანძარსაწინააღმდეგო სიგნალიზაცია და ცეცხლმაქრები, უწყვეტი კვების წყაროები (UPS) და სხვა გარემოსდაცვითი კონტროლები;
- **ხელახალი შესრულება (ე. წ. „Reperformance“):** შიდა აუდიტორები ამოწმებენ კონტროლის სიზუსტეს დავალების ხელახალი შესრულებით, რამაც შეიძლება წარმოადგინოს კონტროლის ოპერაციული ეფექტურობის პირდაპირი მტკიცებულება. ხელახალი შესრულება შესაძლოა განხორციელდეს ხელით ან აუდიტორული

კომპიუტერული ტექნიკის გამოყენებით. მაგალითად, შიდა აუდიტორს შეუძლია მოამზადოს ტრანზაქციის ფაილი, რომელიც შეიცავს ცნობილ შეცდომებს და განსაზღვროს, წარმატებით აფიქსირებს თუ არა აპლიკაცია შეცდომებს და აწარმოებს თუ არა მათ შესახებ ანგარიშგებას. რთულ ტექნიკურ საკითხებთან დაკავშირებით შეიძლება საჭირო გახდეს გარე ექსპერტის მოწვევა;

- **ანალიტიკური მიმოხილვის პროცედურები:** ამ პროცედურის გამოყენება შეიძლება როგორც რისკის ანალიზისას, ასევე აუდიტორული მტკიცებულებების შეგროვებისას. აუდიტის მტკიცებულება შეიძლება შეგროვდეს მონაცემების შედარებით, ცვლილებების გამოკვლევით, ან ისეთი კავშირების იდენტიფიცირებით, რომლებიც არ შეესაბამება მოსალოდნელ ისტორიულ მონაცემებს ან აუდიტორის წარსულ გამოცდილებას.

აუდიტორებმა უნდა გამოიყენონ გამოცდილება და პირადი განსჯა ტესტირების ტიპისა და მასშტაბის განსაზღვრისას. განსაკუთრებით მნიშვნელოვანია, რომ შიდა აუდიტმა გაითვალისწინოს აუდიტორული მტკიცებულებების სანდოობა ტესტების შემუშავებისა და შეფასებისას.

3.3.3 IT კონტროლის დიზაინის ტესტი

შიდა აუდიტორი განსაზღვრავს ტესტირების პროცედურების ბუნებას, ვადებსა და მასშტაბს, საკმარისი და შესაბამისი აუდიტორული მტკიცებულების მოსაპოვებლად იმის შესახებ, რომ ტესტირებისთვის შერჩეული IT კონტროლები ეფექტურად ფუნქციონირებს აუდიტის პერიოდის განმავლობაში. ტესტირებაში არაპროგნოზირებადობის შესატანად და ცვალებად გარემოებებზე რეაგირებისთვის, შიდა აუდიტორმა წლიდან წლამდე უნდა შეცვალოს IT კონტროლების ტესტების ბუნება, დრო და მასშტაბი.

3.3.3.1 IT კონტროლის ტესტირების პროცედურის ბუნება

შიდა აუდიტორმა უნდა განსაზღვროს დაგეგმილი ტესტირების პროცედურების ბუნება, რაც ხელს შეუწყობს იმის გარკვევას, ოპერირებდა თუ არა IT კონტროლის მექანიზმის დიზაინის შესაბამისად აუდიტირებადი პერიოდის განმავლობაში. ტესტირების პროცედურები მოიცავს შემდეგს:

- გამოკითხვა
- IT კონტროლების შესრულებაზე დაკვირვება
- IT კონტროლის შესრულების შედეგად წარმოქმნილი მტკიცებულებების შემოწმება და მოკვლევა
- IT კონტროლების ხელახლა შესრულება.

ტესტირების თითოეული პროცედურის ბუნება დეტალურად აღწერილია „***ტესტირების ზოგადი ტექნიკების***“ თავში.

ზოგადად, IT კონტროლის მექანიზმების ტიპების (ავტომატიზებული ან ნაწილობრივ ავტომატიზებული) მიხედვით შესაძლოა განსხვავდებოდეს:

- მისი ფუნქციონირების დადასტურებისთვის არსებულ მტკიცებულებების ტიპი;
- აუდიტორული პროცედურის ბუნება, რომელიც საჭირო IT კონტროლის აუდიტირებადი პერიოდის მანძილზე ეფექტურად ოპერირების შესახებ გონივრული რწმუნებულების მიღებისთვის;
- აუდიტორული პროცედურების ბუნება, რომელიც აუცილებელია გონივრული რწმუნების მისაღებად, ფუნქციონირებდა თუ არა IT კონტროლი ეფექტიანად აუდიტის პერიოდში.

შეიძლება არსებობდეს მტკიცებულება, რომელიც IT კონტროლის შესრულების მაჩვენებლებზე მეტყველებს. თუმცა, შეიძლება საჭირო გახდეს დამატებითი პროცედურები მისი ეფექტურობის დასადგენად.

მაგალითი

- არსებობს ფიზიკური მტკიცებულება, რომელიც მიუთითებს, რომ წვდომის პერიოდული გადახედვა ჩატარდა, მაგრამ არ არსებობს მტკიცებულება მისი ეფექტურობის დასადასტურებლად, რადგან მომხმარებლების დიდი რაოდენობის მიუხედავად ცვლილებები არ გამოვლენილა. შიდა აუდიტორს შეუძლია განახორციელოს მოკვლევა და თავიდან შეასრულოს IT კონტროლის ზოგიერთი ნაწილი, რათა მოიპოვოს მტკიცებულება მისი ეფექტურობის შესახებ
- ორგანიზაციას შეუძლია წარმოადგინოს სისტემის კონფიგურაციის ანგარიში, როგორც IT კონტროლის მტკიცებულება. ასეთი ანგარიში შესაძლოა არ წარმოადგენდეს IT კონტროლის ეფექტური მუშაობის დამადასტურებელ მტკიცებულებას, რადგან გვერდის ავლით შესაძლებელია სისტემის გარკვეული კონფიგურაციების შეცვლა ან გამორთვა. შესაძლებელია საჭირო გახდეს იმის ტესტირება, რომ ეს პარამეტრები ნამდვილად მუშაობს. ამის განხორციელება შესაძლებელია აუდიტის პერიოდის განმავლობაში ამ პარამეტრებზე რამდენჯერმე დაკვირვებით, იმის დასადასტურებლად, რომ არ მომხდარა მათი ცვლილება. ალტერნატიულად, შესაძლოა მიზანშეწონილი იყოს ორგანიზაციის პერიოდული ვალიდაციის კონტროლის იდენტიფიცირება და ტესტირება, იმის დასადასტურებლად რომ სისტემის კონფიგურაციები შეესაბამება პოლიტიკებს ან, რომ ცვლილებების შემთხვევაში ხდება შეტყობინების გაგზავნა.

3.3.3.2 IT კონტროლის ტესტირების პროცედურის დრო

IT კონტროლის ტესტირებისთვის შესაფერისი დროის შერჩევისას, შიდა აუდიტორმა უნდა გაითვალისწინოს ისეთი ფაქტორები, როგორიცაა: ეხება თუ არა აუდიტის მიზნები კონკრეტულ მომენტს ან პერიოდს, ხელმისაწვდომი მტკიცებულების ტიპი (მაგ. ბევრი IT კონტროლის გამართული მუშაობის მტკიცებულება ხელმისაწვდომია მხოლოდ ტესტირებისას), IT კონტროლის მნიშვნელობა ან კრიტიკულობა აუდიტის მიზნებთან მიმართებაში და ა.შ.

ელექტრონულ სისტემებში მტკიცებულება შეიძლება ხელმისაწვდომი იყოს მხოლოდ დროის შეზღუდული პერიოდის განმავლობაში, სანამ მოხდება მასზე სხვა ინფორმაციის გადაწერა ან მოხდება პროგრამული უზრუნველყოფის ჩანაცვლება ახალი ვერსიით. შიდა აუდიტორმა უნდა გამოიყენოს პროფესიული განსჯა IT კონტროლზე ტესტირების ჩატარების შესაბამისი დროის განსაზღვრისას.

3.3.3.3 IT კონტროლის ტესტირების პროცედურის მასშტაბი

შიდა აუდიტორი ამოწმებს IT კონტროლს, რათა მიაღწიოს გონივრულ რწმუნებას მისი, IT კონტროლის, ეფექტური ფუნქციონირების შესახებ აუდიტის სრულ პერიოდზე. შიდა აუდიტორი იღებს გადაწყვეტილებას აუდიტორული პროცედურის მასშტაბების შესახებ, ე.ი. განსაზღვრავს შესამოწმებელ რაოდენობას პროფესიული განსჯის საფუძველზე, შეფასებულ რისკს, რწმუნების ხარისხს, რომლის მიღებასაც გეგმავს აუდიტორი, ასევე აუდიტის პროცედურისთვის შერჩევის ყველაზე შესაფერის მეთოდს და ა.შ. მაგალითად, CAAT-ების გამოყენებით შეიძლება ელექტრონული ჩანაწერების უფრო დიდი რაოდენობით ტესტირება. იხილეთ მომდევნო თავში - **პოპულაციის ტესტირება და შერჩევა** წარმოდგენილი განმარტებები.

მაგალითი

ორგანიზაციას შეიძლება ჰქონდეს ინტერნეტ წვდომის ბევრი წერტილი ან მონაცემთა ბაზის რამდენიმე პარალელურ რეჟიმში მომუშავე ვერსია. შიდა აუდიტორმა უნდა გამოიყენოს პროფესიული განსჯის უნარი შესარჩევი ელემენტების რაოდენობის და მათი შერჩევის მეთოდის განსაზღვრისას. ზოგადად, ასეთი განსჯა მოიცავს დაკავშირებული ინფორმაციული სისტემების რისკის განხილვას, კონკრეტული ელემენტების მნიშვნელობას ან კრიტიკულობას შესაბამისი კონტროლის მიზნების მისაღწევად, ქსელის კომპონენტის მდებარეობას აუდიტის ინტერესის ძირითად სფეროებთან მიმართებით და თანმიმდევრულობას კომპონენტების კონფიგურაციაში.

3.3.3.4 პოპულაციის ტესტირება და ნიმუშის შერჩევა

შიდა აუდიტორმა უნდა დააზუსტოს კონტროლის დიზაინი, რათა განსაზღვროს პოპულაცია, რომელთან მიმართებაშიც გამოიყენება კონტროლი. პოპულაცია, რომლიდანაც შეირჩევა ელემენტები, უნდა შეესაბამებოდეს აუდიტის სპეციფიკურ მიზნებს.

პოპულაცია არის იმ მონაცემთა სიმრავლე, რომლისთვისაც სურს შიდა აუდიტორს დასკვნის გაკეთება. პოპულაცია შეიძლება შედგებოდეს ყველა ელემენტისგან ან ელემენტების ქვე-სიმრავლისგან, რომლისთვისაც შიდა აუდიტორი იყენებს შერჩევას აუდიტის დასახული მიზნის მისაღწევად. პოპულაციის განსაზღვრისას შიდა აუდიტორი ადგენს, რომ პოპულაცია არის:

- შესაფერისი შიდა აუდიტის კონკრეტული მიზნისთვის
- სრული.

საერთო IT პროცესს დაქვემდებარებული ერთეულების პოპულაციები (მაგ., ცვლილების მართვა 2 აპლიკაციისთვის) შეიძლება ტესტირებისთვის გაერთიანდეს. ეს მიდგომა შესაძლებელს ხდის შემცირდეს შერჩეული ელემენტების რაოდენობა და ამავდროულად იძლევა IT პროცესის

ოპერაციული ეფექტურობის და ძირითადი კონტროლების შეფასების საფუძველს, რომლებიც ახდენენ მრავალი IT აპლიკაციისა და IT გარემოს კომპონენტების მხარდაჭერას.

განმარტება

ერთი საერთო IT პროცესი შესაძლოა ემსახურებოდეს რამდენიმე IT აპლიკაციას ან სხვა IT გარემოს კომპონენტებს, როდესაც ორგანიზაციაში ამ IT პროცესის აქტივობები არსებითად ერთნაირად წარიმართება იმ პირების მიერ, რომლებიც ექვემდებარებიან ერთი და იმავე პოლიტიკებს, ზედამხედველობას და იყენებენ ერთი და იმავე ტექნოლოგიებს. ასეთ პროცესებს მოიხსენიებენ, როგორც საერთო IT პროცესებს, რადგან ისინი გამოიყენება IT გარემოს მრავალი კომპონენტისთვის. ასეთ შემთხვევაში, საერთო IT პროცესის პოპულაციები (მაგ., ცვლილებების მოთხოვნა დამტკიცების გზით, ან წვდომის მოთხოვნები და დასტურები) შეიძლება გაერთიანდეს ტესტირების მიზნებისთვის.

საერთო IT პროცესების გამოსავლენად შიდა აუდიტორმა უნდა განსაზღვროს ცენტრალიზებისა და საერთო გამოყენების დონე შემდეგ სფეროებში:

- **პოლიტიკა** - გამოიყენება თუ არა ერთი და იგივე პოლიტიკები სხვადასხვა IT აპლიკაციებისთვის, ადგილმდებარეობებისთვის ან IT გარემოს კომპონენტებისთვის
- **პერსონალი** - არიან თუ არა ერთი და იგივე პირები პასუხისმგებელნი ძირითადი აქტივობების შესრულებასა და მონიტორინგზე ან/და ექვემდებარებიან თუ არა ისინი ერთსა და იმავე ზედამხედველობას
- **აქტივობები** - ერთნაირად ხორციელდება თუ არა ძირითადი აქტივობები
- **ტექნოლოგია** - გამოიყენება თუ არა IT პროცესის აქტივობებში არსებული ერთი და იგივე ინსტრუმენტები (მაგ. ინსტრუმენტი, რომელსაც გადააქვს ცვლილებები სატესტო გარემოდან რეალურ გარემოში ან ინსტრუმენტი, რომელიც აუქმებს ან შლის წვდომას) მრავალი IT აპლიკაციისთვის ან IT გარემოს კომპონენტისთვის.

მაგალითი

ცვლილებების მართვის პროცესი მოითხოვს, რომ ყველა ცვლილების მოთხოვნა დარეგისტრირდეს Help Desk-ის სისტემაში, რომელიც შემდგომ გამოიყენება ამ პროცესში არსებული სხვა და სხვა ეტაპის, მათ შორის დასტურების, დასრულებისა და დოკუმენტირების სტატუსის მონიტორინგისთვის. იმის მტკიცებულებად, რომ მრავალი IT აპლიკაცია მიჰყვება ერთი და იმავე პროცესს, შიდა აუდიტორს შეუძლია შეამოწმოს ინფორმაცია Help Desk სისტემაში, და დაადასტუროს რომ არსებობს მინიმუმ ერთი ცვლილება თითოეული IT აპლიკაციიდან. იმ IT აპლიკაციებისთვის, რომლების შესახებაც არ არის ინფორმაცია წარმოდგენილი Help Desk-ში, შიდა აუდიტორმა უნდა განახორციელოს მოკვლევა და დაადგინოს ამის მიზეზი (მაგ., ამ IT აპლიკაციებში არ განხორციელებულა ცვლილება, თუ ეს IT აპლიკაცია საერთო IT პროცესს არ მისდევს, და შესაბამისად Help Desk სისტემაში არ რეგისტრირდება ცვლილების მოთხოვნები)

მხოლოდ Help Desk სისტემის მონაცემების გაანალიზება არ იძლევა პოპულაციის სისრულის გარანტიას, იმ შემთხვევაში, როდესაც Help Desk სისტემა წარმოადგენს ცვლილებების მართვის პროცესში IT კონტროლის შესამოწმებელი პოპულაციის წყაროს.

შერჩევის მიდგომა

შიდა აუდიტორმა უნდა შეარჩიოს კონტროლის ტესტირებისთვის საჭირო ელემენტები შემთხვევითი ან სისტემატური შერჩევის მეთოდის გამოყენებით. მიზანი არის

რეპრეზენტატიული ელემენტების შერჩევა და შედეგების ექსტრაპოლაცია პოპულაციაზე, ამიტომ შერჩევა უნდა მოხდეს მიკერძოების გარეშე.

შერჩევის ზომის განსაზღვრისას შიდა აუდიტორმა უნდა გაითვალისწინოს კონტროლის ბუნება, სიხშირე და პოპულაციის ზომა. ყველა ეს კომპონენტი მნიშვნელოვანია შერჩევის პროცესში.

კონტროლების ტესტირებისთვის შერჩეული ელემენტების მინიმალური ზომა მოცემულია ქვემოთ:

სიხშირე	შერჩევის ზომა
დღეში რამდენჯერმე	25
ყოველდღიურად	25
ყოველკვირეულად	5
ყოველთვიურად	3
ყოველკვარტლურად	2
წელიწადში ორჯერ	1
ყოველწლიურად	1

ცხრილი 3: *შესარჩევი ნიმუშების ზომის მატრიცა*

შერჩეული მინიმუმ 25 (ე.წ. „Test-of-25“) ელემენტი მიგვანიშნებს, რომ პოპულაცია დიდია (ანუ 250-ზე მეტი შემთხვევა). გარკვეული ტიპის კონტროლისთვის შიდა აუდიტორმა შესაძლოა დააიდენტიფიციროს კონტროლის შემთხვევების მცირე რაოდენობა კონტროლის ტიპისთვის, რომელიც ხშირად მოქმედებს. ამ პირობებში, თუ კონტროლის შემთხვევების რაოდენობა არის:

- 50-დან 250 შემთხვევამდე, შერჩეული ელემენტების მინიმალური რაოდენობა უნდა იყოს პოპულაციის 10%;
- 50-ზე ნაკლები, შიდა აუდიტორმა უნდა შეარჩიოს 5 ელემენტი, ან 100%, თუ პოპულაცია 5-ზე ნაკლებია.

მოცემულ ცხრილში ნახსენებ შერჩეულ ელემენტების რაოდენობებს გააჩნია სტატისტიკური საფუძველი. ზოგადად, 25 შერჩეული ელემენტი მიგნებების ან გამონაკლისების გარეშე იძლევა 90%-იან სტატისტიკურ სანდოობას, რომ გამონაკლისის მაჩვენებელი პოპულაციაში არ აღემატება 10%-ს.

შერჩევის გაკეთება შესაძლებელია, მაგალითად, MS Excel-ში შემთხვევითი რიცხვების გენერირების ფუნქციის ან შერჩევის სპეციალური ინსტრუმენტების გამოყენებით.

შიდა აუდიტორი პოპულაციის ყველა ელემენტს იმგვარად უნდა მიუდგეს, რომ თითოეულს ჰქონდეს შერჩევაში მოხვედრის თანაბარი ალბათობა. გარდა ამისა, შიდა აუდიტორი უნდა დარწმუნდეს, რომ საბოლოო შერჩევაში მოხვდება მინიმუმ ერთი ელემენტი მაინც თითოეული IT აპლიკაციის თუ IT გარემოს სხვა კომპონენტიდან.

მაგალითი

ცვლილებების მართვისთვის სამ IT აპლიკაციაში გამოიყენება საერთო IT პროცესი. მოცემული აუდიტის პერიოდისთვის სამივე IT აპლიკაციისთვის ცვლილებების პოპულაცია შეადგენს 450 ელემენტს. IT აპლიკაცია A – 17 ელემენტი, IT აპლიკაცია B - 140 და IT აპლიკაცია C - 293. გაერთიანებული პოპულაციიდან ტესტირების მიზნებისთვის შემთხვევითი პრინციპით შეირჩევა 25 ელემენტი, თითოეული IT აპლიკაციისთვის ცვლილებების რაოდენობის გათვალისწინების გარეშე.

შერჩევის მეთოდოლოგია უნდა იყოს გაფორმებული ტესტირების დოკუმენტის თავფურცელზე, რომელიც არის ნებისმიერი ტესტირების დოკუმენტის ნაწილი და რომელიც მოიცავს ძირითად ინფორმაციას, როგორიც არის მიზნები, მასშტაბი, პოპულაცია, შერჩევის ზომა, შერჩევის მეთოდოლოგია, შესრულებული პროცედურები და ა.შ.

3.3.4 IT კონტროლების ტესტირება

შემუშავებული ინფორმაციული ტექნოლოგიების კონტროლების ტესტირებები უნდა განხორციელდეს თითოეულ შერჩეულ ელემენტზე საკმარისი აუდიტორული მტკიცებულებების შეგროვებით. ტესტირებამდე უნდა განიხილებოდეს ნებისმიერი შესაბამისი ინფორმაცია, რამაც შეიძლება მოითხოვოს კონტროლის დაგეგმილი ტესტების დამატება, წაშლა ან განახლება.

თუ შიდა აუდიტორი, მისი ცოდნისა და დოკუმენტების საფუძველზე, გამოავლენს ცვლილებას IT კონტროლში, ის უნდა:

- გაერკვეს ცვლილებებში;
- განაახლოს დოკუმენტაცია ცვლილებების ასახვის მიზნით;
- დაადასტუროს მისეული აღქმა პროცესის გავლის მეშვეობით;
- დაადგინოს აუდიტის შესაბამისი რეაგირების ღონისძიებები.

IT კონტროლის ტესტირებისას შიდა აუდიტორმა უნდა:

- შეაფასოს აუდიტორული მტკიცებულების სახით მოპოვებული ინფორმაციის შესაბამისობა და სანდოობა;
- შეინარჩუნოს პროფესიული სკეპტიციზმი აუდიტორული მტკიცებულებების სანდოობის განსაზღვრისას, თაღლითური ქმედებების შესაძლებლობის გათვალისწინებით;
- ინფორმაციის სანდოობაში ეჭვის შეტანის შემთხვევაში, თუ ერთი წყაროდან მოპოვებული აუდიტორული მტკიცებულება არ შეესაბამება მეორე წყაროს, ან თუ შიდა აუდიტის პროცედურის შედეგები არ შეესაბამება სხვა შიდა აუდიტის პროცედურის შედეგებს, აუდიტორმა ის უნდა განიხილოს, როგორც კონტროლის პოტენციური გამონაკლისი. ეს, თავის მხრივ, შიდა აუდიტორისგან მოითხოვს აუდიტის შესაბამისი პასუხის განსაზღვრას და ზეგავლენის შეფასებას შიდა აუდიტის სხვა სფეროებზე, ასევე დროულ კომუნიკაციას შიდა აუდიტის ჯგუფის ხელმძღვანელთან და/ან შიდა აუდიტის სუბიექტის ხელმძღვანელთან.

მაგალითი

როდესაც ადმინისტრატორების სიის ეკრანის გამოსახულებაზე (ე.წ. „Screenshot“) არ ჩანს იმ სერვერის დასახელება, რომლიდანაც მოხდა ამ სიის აღება, ან თარიღი და დრო, შიდა აუდიტორმა, ფიზიკური ინსპექციის საფუძველზე უნდა შეადაროს IT აპლიკაციაში არსებული ინფორმაცია ეკრანის გამოსახულებაზე არსებულ ინფორმაციას.

მტკიცებულება

საბოლოო დასკვნის გამოსატანად აუდიტის მტკიცებულებების შეგროვება ხდება აუდიტის თითოეული მიზნისთვის. გადაწყვეტილება იმის შესახებ, თუ რომელი ტიპის მტკიცებულება უნდა მოიძიოს შიდა აუდიტორმა ან რა რაოდენობის მტკიცებულებაა საკმარისი, მოითხოვს პროფესიულ განსჯას. ასეთი განსჯის მხარდასაჭერად აუცილებელია მტკიცებულების ძირითადი ატრიბუტის ცოდნა.

არსებობს 3 ძირითადი ატრიბუტი, რომელიც ასოცირდება მისაღებ აუდიტორულ მტკიცებულებასთან:

- **საკმარისობა** - მტკიცებულებათა რაოდენობის საზომი - საკმარისი მტკიცებულება უნდა შეგროვდეს და შეფასდეს ისე, რომ ინფორმირებული და მიუკერძოებელი პირი იგივე მტკიცებულებებზე დაყრდნობით დაეთანხმოს შიდა აუდიტორის მიგნებებსა და დასკვნებს;
- **სანდოობა** - მტკიცებულების წყაროს შესაბამისობისა და სანდოობის საზომი - ზოგადად მტკიცებულება უფრო სანდოა, თუ მიღებულია სანდო დამოუკიდებელი წყაროდან, ვიდრე შიდა აუდიტის ობიექტისგან. ასევე მტკიცებულება უფრო სანდოა თუ მიღებულია პირდაპირი ფიზიკური შეფასების, დაკვირვების, გამოთვლის და ინსპექტირების გზით, ვიდრე არაპირდაპირი, დოკუმენტირებულია, ვიდრე ვერბალურად გადმოცემული და დადასტურებულია, ვიდრე წარმოდგენილია ერთადერთი წყაროდან;
- **რელევანტურობა** - მტკიცებულების შესაბამისობის საზომი – მტკიცებულება ლოგიკურად უნდა შეესაბამებოდეს იმ მოთხოვნას, რომელსაც ადასტურებს.

მტკიცებულებების ადეკვატურობის განხილვისას შიდა აუდიტორმა უნდა გაითვალისწინოს, რომ:

- შიდა აუდიტი მიზნად ისახავს გონივრულ, მაგრამ არა აბსოლუტურ რწმუნებულებას;
- არასრულმა მონაცემებმა შესაძლოა გაართულოს გონივრული დასკვნების გაკეთება;
- ვრცელი მტკიცებულებების გამოკვლევა შეიძლება იყოს არაგონივრული, არაეფექტიანი და არაპროდუქტიული;
- მტკიცებულება უნდა იყოს გონივრულად რეპრეზენტატიული შესასწავლ ან განსახილველ პოპულაციასთან მიმართებაში.

რა არის ორგანიზაციის მიერ გენერირებული ინფორმაცია?

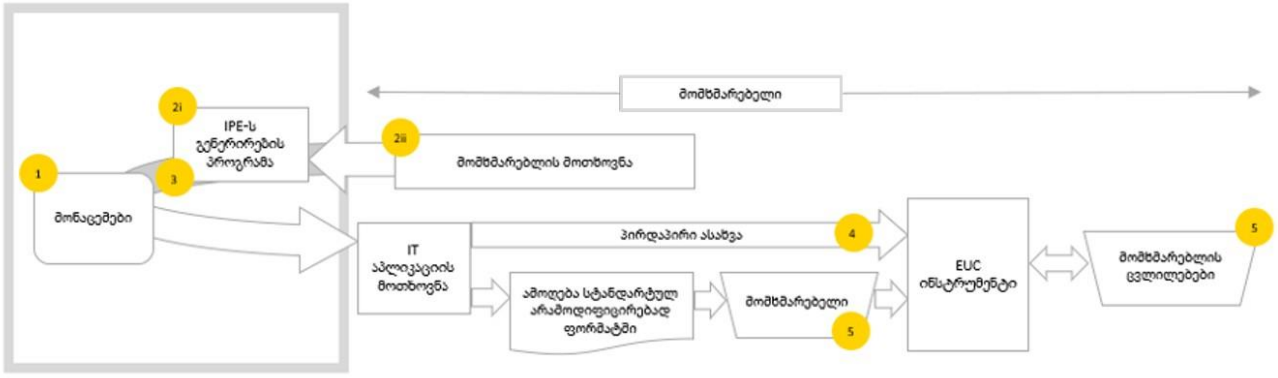
ორგანიზაციის მიერ გენერირებული ინფორმაცია (ე. წ. „Information Produced by the Entity (IPE)“) არის ნებისმიერი ინფორმაცია, რომელიც შექმნილია ორგანიზაციის მიერ IT აპლიკაციების, მომხმარებლების გამოთვლითი ინსტრუმენტების (ე. წ. „End-user Computing (EUC) Tools“) ან სხვა საშუალებების (მათ შორის, ხელით მომზადებული ინფორმაცია) გამოყენებით. IPE გვხვდება შემდეგ სიტუაციებში:

- როდესაც ხელმძღვანელობა იყენებს მას ტესტირების ფარგლებში მოხვედრილი კონტროლებისთვის;
- როდესაც ის გამოიყენება აუდიტორული მტკიცებულების სახით;
- როდესაც ის გამოიყენება კონტროლის ან ძირითადი პროცედურის ტესტირების ელემენტების შესარჩევ პოპულაციად.

ორგანიზაციის მიერ გენერირებული ინფორმაციის (IPE) სისრულე და სიზუსტე

როგორც წესი, ორგანიზაციები იყენებენ IT აპლიკაციებსა და მონაცემთა ბაზებს მონაცემთა შესაგროვებლად, დასამუშავებლად და შესანახად, ანგარიშებში/რეპორტებში შესაბამისი ინფორმაციის გადასატანად, ასევე EUC ინსტრუმენტებსა და მონაცემთა ფაილებში. შედეგი არის IPE, როდესაც ის გამოიყენება აუდიტის მიზნებისთვის.

ობიექტის IT აპლიკაციიდან IPE-ს შექმნის პროცესი აღწერილია ქვემოთ და ილუსტრირებულია გრაფიკზე.



დიაგრამა 8: ***IPE გენერირების პროცესი დაკავშირებული რისკებით***

მომხმარებელი ითხოვს ინფორმაციას IT აპლიკაციიდან ან პირდაპირ მონაცემთა ბაზიდან („მომხმარებლის მოთხოვნა“ დიაგრამაზე). ინფორმაციის გენერირებისას შესაძლებელია მომხმარებელმა შეიყვანოს სხვადასხვა ვარიანტი ან აირჩიოს შემდეგი - ანგარიშის ნომერი, კომპანიის კოდი, თარიღის დიაპაზონი ან გამომავალი მონაცემების ფორმა. ეს არჩევანი (ე.წ. პარამეტრები) გამოიყენება IPE-ის გენერირების პროგრამაში („IPE გენერირების პროგრამა“

დიაგრამაზე). მომხმარებლის მიერ შეყვანილი პარამეტრების საფუძველზე, IPE-ის განსაზღვრის პროგრამა ირჩევს მითითებულ მონაცემებს მონაცემთა ბაზიდან (დიაგრამაზე „მონაცემები“) და გამოაქვს ინფორმაცია მითითებული ფორმატით („პირდაპირი ასახვა“ და „EUC ინსტრუმენტი“ დიაგრამაზე ან „გამომავალი მონაცემები ჩვეულებრივ არა მოდიფიცირებადი ფორმატით“). მისაღები ინფორმაციის ფორმატიდან გამომდინარე, ინფორმაცია შეიძლება შეიცვალოს მომხმარებლების მიერ, რომლებსაც შეუძლიათ მასზე წვდომა („მომხმარებლის მოქმედებები“ დიაგრამაზე).

ქვემოთ მოცემულ ცხრილში წარმოდგენილია ძირითადი რისკები და აუდიტის კითხვების ნიმუშები თითოეული **IPE** რისკის კატეგორიისთვის:

რისკის აღმნიშვნელი	რისკი	კითხვები
1	IT აპლიკაციის მიერ დამუშავებული მონაცემები, საიდანაც მზადდება IPE, არ არის სრული ან ზუსტი	• როგორ შეიძლება დადგინდეს, იყო თუ არა წყაროს ინფორმაცია მთლიანად და ზუსტად შეტანილი IT აპლიკაციაში? ანუ, არის თუ არა ყველა ტრანზაქცია შეტანილი და ზუსტად არის ისინი შეტანილი თუ არა? • როგორ შეუძლია აუდიტორს დარწმუნდეს, რომ IPE-ს ამოღებამდე IT აპლიკაციაში შეყვანილი ინფორმაცია დამუშავდა ზუსტად, როგორც ხელით, ასევე ავტომატური აქტივობებით?
2ii	მომხმარებლის მიერ შეყვანილი პარამეტრები შეუსაბამოა	• როგორ ამოწმებს აუდიტორი, რომ მომხმარებლის მიერ IPE-ის გენერირებისთვის შეყვანილი პარამეტრები (როგორებიცაა თარიღები ან საქმიანობის ერთეულები) სათანადოა და ასახავს საჭირო ინფორმაციას დანიშნულებისამებრ?
2i	IT აპლიკაციიდან IPE-ში ამოღებული მონაცემები არ არის მიზნობრივი ინფორმაცია ან არ არის სრული	• როგორ ადასტურებს აუდიტორი, რომ პროგრამა კონფიგურირებულია ყველა მოსალოდნელი ინფორმაციის ამოღებაზე? • როგორ ადასტურებს აუდიტორი, რომ ნებისმიერი გამოთვლა ან ცვლილება, რომელიც ჩანს IPE-ში, არის ზუსტი? • როგორ ადასტურებს აუდიტორი, რომ ნებისმიერი შესაბამისი კატეგორიზაცია, რომელიც ჩანს IPE-ში, არის ზუსტი და შეესაბამება მოლოდინებს?
3	IPE-ის შექმნისას შესრულებული გამოთვლები ან კატეგორიზაცია არაზუსტია	
4	IT აპლიკაციიდან გამომავალი მონაცემები იკარგება EUC ინსტრუმენტზე გადაცემისას	• როგორ შეიძლება დადასტურდეს, რომ პროგრამიდან გამომავალი მონაცემები არ დაიკარგა გადაცემის დროს?
5	EUC ინსტრუმენტის გამოყენებით შექმნილი,	• როგორ შეუძლია აუდიტორს დარწმუნდეს, რომ IPE-ს კონტროლის და აუდიტის პროცედურებში ჩართვამდე

	დამატებული ან შეცვლილი (მათ შორის გამოთვლები და კატეგორიზაცია) ინფორმაცია არასრული, არაზუსტი ან შეუსაბამოა	მომხმარებელმა არასწორად არ დაამატა, შეცვალა ან წაშალა ინფორმაცია, ან რომ არ შეიყვანა არაზუსტი გამოთვლები EUC ინსტრუმენტის გამოყენებით? • თუ გადაცემა გულისხმობს ფაილის ექსპორტს პროგრამიდან, რომელიც წარმოქმნის IPE-ს, და შემდეგ ამ ფაილის ცალკე იმპორტს EUC ინსტრუმენტში, როგორ შეუძლია აუდიტორს დაადგინოს, შეიცვალა თუ არა ინფორმაცია დაიმპორტებამდე?

ცხრილი 4: **IPE რისკის მატრიცა**

3.3.4.1 IT კონტროლების გამონაკლისები და ხარვეზები

კონტროლის გამონაკლისის გამოვლენის შემთხვევაში, შიდა აუდიტორმა უნდა:

- მოიკვლიოს და შეისწავლოს გამონაკლისის ბუნება და მიზეზი;
- განსაზღვროს გამონაკლისი სისტემატურია თუ შემთხვევითი;
- შეაფასოს გამონაკლისის გავლენა შიდა აუდიტის დაგეგმილ პროცედურებსა და აუდიტის სხვა სფეროებზე.

კონტროლის პოტენციური გამონაკლისების გამოკვლევისას, შიდა აუდიტორმა შესაძლოა დაადგინოს, რომ IT პროცესისა და მასთან დაკავშირებული კონტროლის საწყისი აღქმა არასწორი იყო. ამ შემთხვევაში შიდა აუდიტორმა უნდა:

- გაიაზროს ცვლილებები;
- განაახლოს დოკუმენტაცია მათი სწორად ასახვისთვის;
- დაადასტუროს საკუთარი აღქმა კრიტიკული ანალიზის საფუძველზე;
- განსაზღვროს შიდა აუდიტის შესაბამისი პასუხი.

როდესაც შიდა აუდიტორს აქვს დამაჯერებელი მტკიცებულება, რომ კონტროლის გამონაკლისი შემთხვევითი მოვლენაა, მან უნდა განსაზღვროს შიდა აუდიტის შესაბამისი პასუხი, კერძოდ, გაზარდოს შერჩეული ელემენტების რაოდენობა იმის დასადასტურებლად, რომ შეცდომის ხდომილება პოპულაციაში მისაღებ დიაპაზონშია.

თუ შიდა აუდიტორი დაასკვნის, რომ კონტროლის გამონაკლისი სისტემატურია, მან არ უნდა გაზარდოს შერჩეული ელემენტების რაოდენობა, არამედ დაასკვნას, რომ გამონაკლისი არის შიდა კონტროლის ხარვეზი და კონტროლი შეაფასოს ***არაეფექტურად***.

იმის გათვალისწინებით, რომ კონკრეტულ კონტროლს აქვს რამდენიმე ატრიბუტი, შიდა აუდიტორმა უნდა განიხილოს გამოიწვევს თუ არა აღნიშნული კონტროლის არაეფექტურობა, მთლიანი IT კონტროლის ხარვეზს. როდესაც კონტროლის ატრიბუტთან დაკავშირებული საკითხი ხელს უშლის კონტროლს რომ შესაბამისად გაუმკლავდეს რისკს, შიდა აუდიტორმა უნდა შეაფასოს კონტროლი როგორც ***არაეფექტური***. როდესაც კონტროლის ატრიბუტთან დაკავშირებული საკითხი არ არის იმდენად მნიშვნელოვანი, რომ გავლენა მოახდინოს კონტროლის მთლიან სარგებლიანობაზე რისკის აღმოსაფხვრელად, შიდა აუდიტორმა უნდა შეაფასოს კონტროლი, როგორც ***ეფექტური*** და დაასაბუთოს, თუ რატომ არ იწვევს არასაკმარისი ატრიბუტი მთლიანი კონტროლის ხარვეზს.

მაგალითი

IT კონტროლი, რომელიც უზრუნველყოფს პაროლების ადეკვატურ პარამეტრებს IT აპლიკაციაზე არაავტორიზებული წვდომის რისკის შესამცირებლად, ზოგადად მოიცავს რამდენიმე ატრიბუტს, მაგალითად:

- პაროლის მინიმალური სიგრძე, სირთულე და როგორ ხდება სირთულის განსაზღვრა
- პაროლის ცვლილების სიხშირე
- შეზღუდვა წინა გამოყენებულ პაროლებზე და ა.შ.

დაფიქრდით არის თუ არა ადეკვატური 180 დღეში ერთხელ პაროლის ცვლილება, მაშინ როდესაც 90 დღე უფრო ტიპურია. თუ პაროლების სხვა ასპექტები შესაბამისია, შესაძლებელია გავაკეთოთ დასკვნა კონტროლის ეფექტურობის შესახებ

3.3.4.2 არაეფექტური IT კონტროლის შეფასებაზე რეაგირება

არაეფექტურ IT კონტროლზე რეაგირებების ქმედებები შემდეგია:

- სხვა IT კონტროლის იდენტიფიცირება და ტესტირება (რომელსაც უწოდებენ მაკომპენსირებელ კონტროლს), რომელიც საკმარისად ამცირებს რისკს მისაღებ დონემდე იმ IT პროცესში, რომელიც დაკავშირებულია არაეფექტურ კონტროლთან.

მაგალითი

იდენტიფიცირებულია IT აპლიკაციაზე მომხმარებლის წვდომის დროულად შეწყვეტის პრობლემა. IT აპლიკაციაში შესვლა არ არის დაკავშირებული ქსელის საერთო მომხმარებელთან (ე. წ. „Single Sign-on“). ქსელის დონეზე წვდომის დროული შეწყვეტის პრობლემა არ არის გამოვლენილი. ქსელის კონტროლი მიჩნეულია საკმარისად ზუსტად, IT აპლიკაციის დონეზე ხარვეზის შემცველ კონტროლის დასაკომპენსირებლად.

- IT ძირითადი პროცედურების ტესტირების ჩატარება გონივრული რწმუნების მისაღებად უზრუნველყოფს, რომ IT პროცესში არსებული რისკი, რომელიც დაკავშირებულია არაეფექტურ კონტროლთან, არ იქნა გამოყენებული. IT ძირითადი პროცედურების ტესტირება, როგორც წესი, პოპულაციის ელემენტების 100%-ზე ტარდება.

მაგალითი

„IT დეველოპერებს შეუძლიათ რეალურ გარემოში ცვლილებების დანერგვა“ რისკის შემცირება არ ხდება კონტროლის მიერ, რადგან დეველოპერებს აქვთ ასეთი წვდომა და არ ხდება მათი ქმედებების მონიტორინგი. შიდა აუდიტორმა უნდა მოიპოვოს აუდიტის პერიოდში განხორციელებული სისტემის მიერ გენერირებული პროგრამული ცვლილებების სრული სია და განახორციელოს პროცედურები იმ გონივრული რწმუნების მისაღებად, რომ დაინერგა მხოლოდ ავტორიზებული და ტესტირებული ცვლილებები.

3.3.5 აუდიტის მიგნებების მატრიცის მომზადება

შიდა აუდიტორებმა უნდა გამოიყენონ **აუდიტის მიგნებების მატრიცა** გამოვლენილი მიგნებების დოკუმენტირებისთვის. მიგნებები უნდა მოიცავდეს მდგომარეობას, კრიტერიუმებს, მიზეზსა და შედეგს და სიმძიმის შეფასებას.

აუდიტის მიგნებების მატრიცა გამოიყენება, შიდა აუდიტის დროს, აუდიტის მიგნებების აუდიტის სუბიექტთან სწრაფად გაზიარების მიზნით (დასკვნითი შეხვედრისა და შიდა აუდიტის ანგარიშის მომზადებამდე).

3.3.5.1 შიდა აუდიტის მიგნებების ელემენტები

მიგნებები აორგანიზებენ შიდა აუდიტის პროცედურების დროს აღმოჩენილ ფაქტებს. როგორც წესი, მიგნებას აქვს შემდეგი მახასიათებლები, რომლებსაც ჩვეულებრივ უწოდებენ ხუთ „C“-ს:

- **მდგომარეობა (ე.წ. „Condition“).** - მდგომარეობა არის ობიექტური მტკიცებულება, რომელსაც შიდა აუდიტორი აღმოაჩენს შემოწმების დროს (არსებული მდგომარეობა);
- **კრიტერიუმები (ე.წ. „Criteria“).** - კრიტერიუმები არის სტანდარტები, საზომები ან მოლოდინები, რომლებიც გამოიყენება შეფასებისას ან /და გადამოწმებისას (სამიზნე მდგომარეობა);
- **მიზეზი (ე.წ. „Cause“).** - მიზეზი არის სამიზნე და არსებულ მდგომარეობებს შორის სხვაობის განმაპირობებელი ფაქტორი. ძირეული მიზეზის (ე.წ. „Root Cause“) იდენტიფიცირება შესაძლოა წარმოადგენდეს გამოწვევას ზოგიერთ აუდიტში. ეს ნიშნავს იმის იდენტიფიცირებას, თუ რა უნდა გამოსწორდეს ამ მდგომარეობის განმეორების თავიდან ასაცილებლად და არა უბრალოდ ისეთი რეკომენდაციის გაცემას, რომელიც მხოლოდ ამჟამინდელ მდგომარეობას გამოასწორებს;
- **შედეგი (ე.წ. „Consequence“).** - რისკი ან ზემოქმედება, რომლის წინაშეც დგება შიდა აუდიტის ობიექტი მდგომარეობასა და კრიტერიუმებს შორის აცდენის შემთხვევაში;
- **მაკორექტირებელი ქმედება (ე.წ. „Corrective action“).** - მიგნების მაკორექტირებელი ქმედების კომპონენტი შეიძლება შეიცავდეს რეკომენდაციებსა და სამოქმედო გეგმებს.

შიდა აუდიტორმა რაც შეიძლება ადრე უნდა დაიწყოს პოტენციური საუკეთესო პრაქტიკებისა და პოტენციური რეკომენდაციების მოსაზრებების განხილვა, განსაკუთრებით რისკის მაღალი დონის მქონე სფეროებში. შიდა აუდიტის განხორციელების ეტაპზე შიდა აუდიტორმა უნდა დატესტოს პოტენციური რეკომენდაციები (მათ შორის, განიხილოს შესაძლო ალტერნატივები) ჯგუფში რეგულარულად განხილვით, რათა შეაფასოს მათი შესაბამისობა, ხარჯ-ეფექტურობა და განხორციელებადობა. „მოულოდნელობის გამორიცხვის“ მიდგომის ფარგლებში, შიდა აუდიტორმა შიდა აუდიტის ობიექტთან ერთად უნდა განიხილოს პოტენციური რეკომენდაციები აუდიტის მიმდინარეობისას, მათი პირობითი სტატუსის ახსნით. ასეთი მოქმედება იძლევა

რეკომენდაციების მიზანშეწონილობისა და ეკონომიურობის შესწავლის საშუალებას, სანამ ისინი შეტანილი იქნება ანგარიშის სამუშაო ვერსიაში. ის ასევე, შესაძლებელს გახდის შიდა აუდიტის ობიექტის მხარდაჭერის მოპოვებას შემოთავაზებულ ცვლილებებთან დაკავშირებით და მიანიჭებს მას თანაზიარობას შეთავაზებულ მოქმედებებზე და შესაბამისად, მზადყოფნას მდგომარეობის გამოსწორებაზე პასუხისმგებლობის ასაღებად.

3.3.5.2 აუდიტის მიგნებების რეიტინგი

გარკვეული ხარისხობრივი და რაოდენობრივი ფაქტორების, ასევე ორგანიზაციაზე პოტენციური გავლენის და მისი ხდომილების ალბათობის შეფასების საფუძველზე, აუდიტის დროს იდენტიფიცირებულ მიგნებებს უნდა მიენიჭოს რისკის რეიტინგი - **სერიოზული, მაღალი, ზომიერი, დაბალი** ან **პროცესის გაუმჯობესება**,

შიდა აუდიტის მიგნების რეიტინგი არის ეფექტური საკომუნიკაციო ინსტრუმენტი თითოეული დაკვირვების მნიშვნელობის გადმოსაცემად და შეუძლია დაეხმაროს ხელმძღვანელობას სამოქმედო გეგმების პრიორიტეტულობის განსაზღვრაში, ხოლო შიდა აუდიტორებს, შემდგომი მონიტორინგის პრიორიტეტების განსაზღვრაში. ინდივიდუალური დაკვირვების რეიტინგების გათვალისწინება გავლენას ახდენს შიდა აუდიტის საერთო დასკვნაზე.

მიგნებების ინდივიდუალური რეიტინგების გათვალისწინება გავლენას ახდენს აუდიტის საერთო დასკვნაზე.

კლასიფიკაცია	*განმარტება*
დაბალი	დაბალი რისკის მქონე მიგნებას აქვს ან შეიძლება ჰქონდეს შეზღუდული ან მინიმალური გავლენა ორგანიზაციაზე რისკის ნებისმიერ განზომილებაში, მაგრამ მაინც მოითხოვს ყურადღებას, რათა შენარჩუნდეს დამაკმაყოფილებელი კონტროლის გარემო. აღნიშნული კლასიფიკაციის მქონე მიგნებების გამოსწორებაზე პასუხისმგებლობას იღებს ორგანიზაციის ხელმძღვანელობა
ზომიერი	საშუალო რისკის მიგნებას აქვს ან შეიძლება ჰქონდეს მნიშვნელოვანი გავლენა ორგანიზაციაზე რისკის ერთ ან რამდენიმე განზომილებაში. ასეთი მიგნებები საჭიროებს კორექტირებას, რომ აუდიტის სფეროში შენარჩუნდეს დამაკმაყოფილებელი კონტროლის გარემო. ხელმძღვანელობა პასუხისმგებელია მაკორექტირებელი ღონისძიებების განსაზღვრაზე და მათ დროულ განხორციელებაზე
მაღალი	მაღალი რისკის მიგნებას აქვს ან შეიძლება ჰქონდეს არსებითი გავლენა ორგანიზაციაზე რისკის ერთ ან რამდენიმე განზომილებაში (მაგ., კონფიდენციალურობა, უწყვეტობა, მთლიანობა). მოითხოვს ორგანიზაციის ხელმძღვანელობის აქტიურ ჩართულობას, რათა დაუყოვნებლივ მოხდეს საჭირო ზომების განსაზღვრა და განხორციელება. თუ მიგნების დაუყოვნებლივ გამოსწორება ვერ ხერხდება, დროებითი მაკომპენსირებელი კონტროლები უნდა დაინერგოს
სერიოზული	სერიოზული რისკის მიგნებას აქვს ან შეიძლება ჰქონდეს მნიშვნელოვანი არასასურველი ზეგავლენა ორგანიზაციის მიზნების მიღწევაზე და, სავარაუდოდ,

	გავრცელდება ორგანიზაციის სხვა მიმართულებებზეც. მოითხოვს დაუყოვნებლივ ანგარიშგებას ორგანიზაციის დირექტორთან
გაუმჯობესება	მიუხედავად იმისა, რომ მიგნება არ არის კონტროლის ხარვეზი, იგი წარმოადგენს კონტროლის დიზაინის ან პროცესის გაუმჯობესების შესაძლებლობას. ხელმძღვანელობამ უნდა განიხილოს რეკომენდაცია და თავისი შეხედულებისამებრ მოახდინოს რეაგირება

ცხრილი 5: *მიგნებების კლასიფიკაცია*

შიდა აუდიტის სუბიექტის ხელმძღვანელს ეკისრება საბოლოო პასუხისმგებლობა შიდა აუდიტის ანგარიშის რეიტინგებზე და იმის უზრუნველყოფაზე, რომ შიდა აუდიტის დროს შესრულებული სამუშაო და ინდივიდუალური მიგნებები განხილულ და შეფასებულ იქნა ზემოაღნიშნული მითითებების შესაბამისად.

3.3.6 დასკვნითი შეხვედრა

შიდა აუდიტის განხორციელების ეტაპის საბოლოო ფაზა არის ობიექტის ხელმძღვანელობასთან დასკვნითი შეხვედრის ჩატარება, რომლის მიზანია მიგნებებისა და საერთო დასკვნების, ისევე როგორც წინასწარი რეკომენდაციების შეჯამება და განხილვა. მიგნებები, რომლებიც განიხილება დასკვნით შეხვედრაზე, არ უნდა იყოს მოულოდნელი შიდა აუდიტის ობიექტისთვის, რადგან მათ ამის შესახებ უკვე უნდა ჰქონდეთ მიღებული ინფორმაცია შუალედური შეხვედრების დროს. ზოგიერთ დაბალი რისკის საკითხზე შესაძლოა ადგილი ჰქონდეს სიტყვიერ კომუნიკაციას აუდიტის მსვლელობისას. ეს ვერბალური საკითხები და რეკომენდაციები არ შედის საბოლოო ანგარიშში, თუმცა განხილულია დასკვნით შეხვედრაზე.

დასკვნითი შეხვედრა შიდა აუდიტის ჯგუფს აძლევს კიდევ ერთ ფორმალურ შესაძლებლობას განიხილოს აუდიტის შედეგები წერილობითი ფორმით და გააკეთოს კომენტარები საჭიროების შემთხვევაში. დასკვნითი შეხვედრა შიდა აუდიტის სუბიექტისთვის არის მოსამზადებელი ეტაპი შიდა აუდიტის დასკვნითი ანგარიშისთვის. საბოლოო შეთანხმება, თუ როგორ უნდა გადაიჭრას საკითხები, მიღწეული უნდა იქნას სწორედ დასკვნით შეხვედრაზე. დასკვნითი შეხვედრის ოქმები დოკუმენტურად უნდა გაფორმდეს და გავრცელდეს, საჭიროებიდან გამომდინარე.

3.4 რეკომენდებული შაბლონები

შემდეგი შაბლონების გამოყენება რეკომენდებულია განხორციელების (საველე სამუშაოების) ეტაპზე:

- **140 IT პროცესების, რისკებისა და კონტროლების შესწავლა (შაბლონი);**
- **210 აუდიტის სამუშაო პროგრამა (შაბლონი);**
- **220 კონტროლის ტესტირების ფორმა (შაბლონი);**
- **230 IT ძირითადი პროცედურის ტესტირების ფორმა (შაბლონი);**
- **240 IT აპლიკაციის კონტროლის ტესტირების ფორმა (შაბლონი);**

- **250 აუდიტის მიგნებების მატრიცა (შაბლონი).**

3.5 ანგარიშგება და გამოსწორება

ძირითადი სამუშაოების დასრულების, ისევე როგორც, პროცესის მფლობელებთან შიდა აუდიტის დასკვნების შეთანხმების შემდეგ, შიდა აუდიტორმა ხელმძღვანელობისგან პასუხის მისაღებად უნდა მოამზადოს შიდა აუდიტის ანგარიში ყველა იდენტიფიცირებულ საკითხზე.

შიდა აუდიტის დასკვნა არის ყველაზე ეფექტური და მნიშვნელოვანი საშუალება, რომლითაც შიდა აუდიტი აჯამებს და შესაბამის მხარეებს აცნობს აუდიტის შედეგებს და რომლის საფუძველზეც შეიძლება ჩამოყალიბდეს სამოქმედო გეგმები IT პროცესებთან დაკავშირებული შიდა კონტროლის ხარვეზების აღმოსაფხვრელად.

3.5.1 შიდა აუდიტის ანგარიშის სამუშაო ვერსიის მომზადება და გავრცელება

შიდა აუდიტის სამუშაო ანგარიშის შედგენამდე, შიდა აუდიტმა უნდა განიხილოს, შეაგროვა თუ არა საკმარისი მტკიცებულებები დასკვნის მოსამზადებლად. შიდა აუდიტის ანგარიში უნდა იყოს ფაქტებზე დამყარებული, ობიექტური და შეესაბამებოდეს **IT აუდიტის ანგარიშის** ფორმატს.

მოძველებულმა, არაკორექტულმა და უხარისხო შიდა აუდიტის ანგარიშებმა შესაძლოა დააზიანოს შიდა აუდიტის მიერ შესრულებული სამუშაოს მნიშვნელობა. შიდა აუდიტის ანგარიშის შედგენისას შიდა აუდიტორებმა უნდა გამოიჩინონ სიფრთხილე და თავიდან აიცილონ:

- მნიშვნელოვანი შეცდომები და გამოტოვებული საკითხები;
- ენა, რომელიც არის ზედმეტად ტექნიკური ან სავსე ჟარგონებით;
- დაკვირვებები და რეკომენდაციები, რომლებიც არ არის მკაფიოდ ჩამოყალიბებული;
- დამაკმაყოფილებელი საქმიანობის არ აღიარება;
- მასშტაბის შეზღუდვების განუსაზღვრელობა ან გამოტოვება;
- ანგარიშების დაგვიანებული გამოცემა ან არასათანადო მხარეებისთვის მიწოდება.

ამ ხარვეზების თავიდან აცილება შესაძლებელია საბოლოო ანგარიშის დამტკიცებამდე მისი ყურადღებით მომზადებითა და განხილვით.

3.5.1.1 ანგარიშის შინაარსი და სტრუქტურა

შიდა აუდიტის ანგარიშის შინაარსი და დეტალიზაციის დონე უნდა განისაზღვროს აუდიტორიის საჭიროებების მიხედვით. შიდა აუდიტორმა, ანგარიშების მომზადებისას, უნდა განიხილოს შემდეგი საკითხები აუდიტორიის შესახებ:

- ვინ არის ანგარიშის ყველაზე მნიშვნელოვანი მიმღები?
- რამდენად ინფორმირებულნი არიან აუდიტორული საქმიანობის შესახებ?

- როგორ გეგმავენ ანგარიშის გამოყენებას?
- რა სახის გავლენა ექნება მიგნებებს ადრესატზე?

შიდა აუდიტის ანგარიშში შეჯამებული უნდა იყოს აუდიტის მიზნები, კრიტერიუმები, მასშტაბი, მიგნებები, დასკვნები და რეკომენდაციები. ანგარიში უნდა იყოს სიღრმისეული, ნათელი და საკმარისი მტკიცებულებების შემცველი. მნიშვნელოვანია იმის უზრუნველყოფა, რომ ყველა რელევანტური საკითხი, რომელიც გამოვლინდა შიდა აუდიტის პროცესში განხილული იყოს ანგარიშში. დეტალური სტრუქტურა იხილეთ IT აუდიტის ანგარიშის შაბლონში.

შიდა აუდიტის ანგარიშის ძირითადი ელემენტები აღწერილია ქვემოთ:

მიზნები და მასშტაბი: ეს თავი, როგორც წესი, აღწერს შიდა აუდიტის მიზანს, ამოცანებს, კრიტერიუმებს, მასშტაბსა და მასშტაბის შეზღუდვას, ასეთის არსებობის შემთხვევაში. შიდა აუდიტის ანგარიშში მიზნები და მასშტაბი უნდა შეესაბამებოდეს დაგეგმვის დამტკიცებულ მემორანდუმს;

დაკვირვება: დაკვირვებები, რომლებიც ასევე იწოდება როგორც მიგნებები, მოიცავს მდგომარეობას, კრიტერიუმებს, მიზეზს, ეფექტს და შეფასებას. დაკვირვებები უნდა დაიწეროს ისე, რომ შესაბამისმა მხარემ გაიგოს და მიიღოს შიდა აუდიტის რისკის შეფასება, ისევე როგორც მისი გავლენა ორგანიზაციულ მიზნებზე. დაკვირვებები უნდა იყოს გამყარებული მტკიცებულებებით, მოკლე და ორგანიზებული, მარტივი ენით დაწერილი, და განმარტავდეს თუ როგორი მდგომარეობაა დადგენილ კრიტერიუმებთან შედარებით;

დაკვირვების რეიტინგი: ეს არის ეფექტური საკომუნიკაციო ინსტრუმენტი თითოეული დაკვირვების მნიშვნელობის გადმოსაცემად და შეუძლია დაეხმაროს ხელმძღვანელობას სამოქმედო გეგმების პრიორიტეტულობის განსაზღვრაში, ხოლო შიდა აუდიტორებს, შემდგომი მონიტორინგის პრიორიტეტების განსაზღვრაში. ანგარიშში ცალკეული დაკვირვების რეიტინგების გათვალისწინება, გავლენას ახდენს შიდა აუდიტის საერთო დასკვნაზე. შეფასების კრიტერიუმები მოცემულია ***მე-7 ცხრილში.;***

დასკვნა: ანგარიშგების პროცესის ერთ-ერთი საბოლოო და კრიტიკული ნაბიჯია აუდიტის პროცესთან დაკავშირებით საერთო დასკვნის მომზადება. საჭიროების შემთხვევაში დასკვნის მიწოდება შესაძლებელია მოსაზრებების სახით. შიდა აუდიტის მოსაზრების სახით გაზიარებული დასკვნა წარმოადგენს შიდა კონტროლების გარემოს მთლიან შეფასებას, რომელიც ეფუძნება აუდიტის დროს შესრულებულ სამუშაოს და გამოვლენილი მიგნებების სიმძიმეს. ასეთ შემთხვევაში, შიდა აუდიტორებმა უნდა შეისწავლონ არა მხოლოდ ცალკეული მიგნებები, არამედ მათი ერთმანეთთან ურთიერთქმედებაც.

ცალკეული მიგნებების შეფასების მიდგომის მსგავსად, შიდა აუდიტის მოსაზრების/დასკვნის შეფასების შკალა გამოიყენება, როგორც მეთოდოლოგია, რომელსაც ემატება შიდა აუდიტორის განსჯა, გამოცდილება და ზედამხედველობა. IT პროცესების საერთო ადეკვატურობის, შესაბამისობის ან ეფექტურობის შესაფასებლად, გამოიყენება შემდეგი შეფასების შკალა:

აუდიტორული მოსაზრების/დასკვნის შეფასება	
ეფექტური	შეფასებული კონტროლის გარემო არის ეფექტური და რელევანტური, რათა უზრუნველყოს რისკების მართვის ეფექტურობისა და ორგანიზაციის დასახული მიზნების წარმატებით მიღწევის გონივრული რწმუნებულება
საჭიროა გარკვეული გაუმჯობესება	აუდიტის შედეგად გამოვლინდა კონტროლის სისტემის რამდენიმე სისუსტე, თუმცა, შეფასებული კონტროლის გარემო არის ეფექტური და რელევანტური, რათა უზრუნველყოს რისკების მართვის ეფექტურობისა და ორგანიზაციის დასახული მიზნების წარმატებით მიღწევის გონივრული რწმუნებულება
საჭიროა მნიშვნელოვანი გაუმჯობესება	აუდიტის შედეგად გამოვლინდა კონტროლის სისტემის არაერთი სისუსტე. შეფასებული კონტროლის გარემო არ იძლევა რისკების მართვის ადეკვატურობისა და ორგანიზაციული მიზნების მიღწევის უზრუნველყოფის გონივრულ რწმუნებულებას
არადამაკმაყოფილებელი	აუდიტის შედეგად გამოვლინდა კონტროლის გარემოს სისტემური პრობლემები. შეფასებული კონტროლის გარემო არაეფექტურია და არ იძლევა რისკების მართვის და ორგანიზაციული მიზნების მიღწევის შესაძლებლობის გონივრულ რწმუნებულებას

რეკომენდაციები: რეკომენდაციები იძლევა ეფექტიან და პროდუქტიულ გზას მდგომარეობასა და კრიტერიუმებს შორის გამოვლენილი სხვაობის აღმოსაფხვრელად. ისინი იყოფა ორ კატეგორიად - მდგომარეობაზე დამყარებულ და ძირეულ მიზეზებზე დაფუძნებულ რეკომენდაციებად:

- **მდგომარეობაზე დაფუძნებული რეკომენდაციები:** უზრუნველყოფს შუალედურ გზას არსებული მდგომარეობის გამოსასწორებლად (მაგ., შეუსაბამო წვდომის გაუქმება);
- **მიზეზზე დაფუძნებული რეკომენდაციები:** საჭირო ქმედებები მდგომარეობის/დაკვირვების ხელახლა განმეორების თავიდან ასაცილებლად. ძირეულ მიზეზებზე დაფუძნებული რეკომენდაციები, როგორც წესი, უფრო გრძელვადიანი გზაა და შეიძლება მოიცავდეს მეტ დროს (მაგ., წვდომების განხილვის პოლიტიკის შექმნა და დანერგვა).

რეკომენდაციების ფორმულირებისას განიხილება შემდეგი საკითხები:

- მოქმედება, რომელიც ყველაზე პრაქტიკული და ეკონომიურია ხარვეზის აღმოსაფხვრელად;
- მიზნები, რომლებიც მხედველობაში უნდა იქნეს მიღებული მაკორექტირებელი ქმედებების რჩევისას;
- მოსაზრებები ხელმძღვანელობისთვის გაუმჯობესებული მოქმედების განსასაზღვრად;
- არჩევნები/ალტერნატივები და როგორ იზომება ისინი მიზნებთან მიმართებაში;
- საუკეთესო არჩევანი/ალტერნატივა ყველაზე ნაკლები გვერდითი ეფექტით;

- მექანიზმი, რომელიც უნდა იყოს შეთავაზებული, მაკორექტირებელი ქმედებების გასაკონტროლებლად მათი გატარების შემდეგ.

3.5.1.2 შიდა აუდიტის ანგარიშის გავრცელება

შიდა აუდიტის სამუშაო ანგარიში (ანგარიშის პროექტი) უნდა გადაეცეს პროცესების ძირითად მფლობელებს და დაინტერესებულ მხარეებს. ის უნდა გამოიცეს შეთანხმებულ ვადაში. შეფერხების/გადავადების შემთხვევაში, მიზეზები უნდა ეცნობოს შიდა აუდიტის ობიექტს.

ანგარიშის სამუშაო ვერსიის გავრცელება ხარისხის კონტროლის უმნიშვნელოვანესი პროცესია, რომელიც უნდა განხორციელდეს თითოეული აუდიტის შემთხვევაში. ის შიდა აუდიტის ობიექტს აძლევს შესაძლებლობას დაეთანხმოს ან არ დაეთანხმოს შიდა აუდიტორის მიგნებებს / დასკვნებს.

იმ შემთხვევაში, თუ ადგილი აქვს მნიშვნელოვან უთანხმოებას შიდა აუდიტის ობიექტს და შიდა აუდიტის სუბიექტს შორის, შესაძლოა მოეწყოს შეხვედრა აღნიშნული უთანხმოებების განსახილველად, რომელსაც შიდა აუდიტის ობიექტისა და შიდა აუდიტის სუბიექტის წარმომადგენლებთან ერთად დაესწრება დაწესებულების ხელმძღვანელი. შეხვედრაზე უნდა მოხდეს უთანხმოებების განხილვა და საბოლოო პოზიციების შეჯერება.

შიდა აუდიტის ობიექტის საბოლოო კომენტარები წერილობით უნდა დაფიქსირდეს დასკვნით ანგარიშში.

3.5.2 დასკვნითი ანგარიშის მომზადება და გავრცელება

დასკვნითი ანგარიში უნდა გამოიცეს სამუშაო ანგარიშის პასუხის გაცემიდან მოკლე ვადაში. ის უნდა მოიცავდეს შიდა აუდიტის ობიექტის პასუხებს (მაგ., შეიძლება აღიარებულ იქნას ქმედებები, რომლებიც განხორციელდა ხელმძღვანელობის მიერ საბოლოო ანგარიშის გაცემამდე) და თან უნდა ახლდეს განხორციელებული ცვლილებების შემაჯამებელი დოკუმენტი.

საბოლოო ჯამში, დასკვნითი ანგარიში უნდა იყოს დამტკიცებული და ხელმოწერილი შიდა აუდიტის სუბიექტის ხელმძღვანელის მიერ. თუმცა, მის გავრცელებამდე, შიდა აუდიტის სუბიექტის ხელმძღვანელმა უნდა განახორციელოს 4.1 ქვეთავში აღწერილი შიდა ხარისხის შემოწმება, რათა დარწმუნდეს, რომ მოთხოვნილი ამოცანები შესრულებულია, ყველა სავალდებულო ფორმა სათანადოდ არის დოკუმენტირებული, რომ გამოტანილი დასკვნა გამყარებულია საკმარისი მტკიცებულებებით და რეკომენდაციები შეესაბამება ორგანიზაციის საქმიანობის მიზნებს. შიდა ხარისხის შემოწმება მნიშვნელოვანი ნაბიჯია ამ სახელმძღვანელოსთან შესაბამისობისთვის და აუდიტის დასახული მიზნების მისაღწევად.

3.5.2.1 შიდა აუდიტის შედეგების გაზიარება უფროს ხელმძღვანელობასთან

საბოლოო ანგარიშის გამოცემის შემდეგ, შიდა აუდიტის ჯგუფთან თანამშრომლობით, შიდა აუდიტის ობიექტის ხელმძღვანელობამ უნდა წარმოადგინოს სამოქმედო გეგმა, რომელიც მოიცავს შემდეგ კომპონენტებს:

- **შეთანხმებული ქმედება:** ქმედებები, რომლებიც განხორციელდება ხელმძღვანელობის მიერ არსებული მდგომარეობისა და გამომწვევი მიზეზების გამოსასწორებლად, რაც შესაძლებელს გახდის მომავალში მათი განმეორების თავიდან აცილებას. ხელმძღვანელობის სამოქმედო გეგმები უნდა შეესაბამებოდეს შიდა აუდიტის რეკომენდაციებს. თუ ხელმძღვანელობა არ ეთანხმება შიდა აუდიტის დაკვირვებას ან მის მიერ გამოვლენილ ფაქტებს, შეთანხმების მისაღწევად დამატებითი დეტალების მიწოდებაა შესაძლებელი, ან ხელმძღვანელობამ უნდა წარმოადგინოს სათანადო ახსნა განსახილველად და გადაწყვეტილების მისაღებად;
- **პასუხისმგებელი პერსონალი:** განსაზღვრულ პირს ან ჯგუფს, რომელიც პასუხისმგებელია მოქმედებაზე. ეს შეიძლება იყოს აქტივობის/პროცესის მფლობელი, მენეჯერი ან უფროსი ხელმძღვანელი;
- **სამოქმედო გეგმის შესრულების ვადა:** სამოქმედო გეგმის დასრულების სამიზნე თარიღი. შიდა აუდიტის ჯგუფმა უნდა უზრუნველყოს, რომ შემოთავაზებული ვადები შეესაბამებოდეს რისკის დონეს.

შიდა აუდიტორმა არასოდეს არ უნდა აიღოს პასუხისმგებლობა გამოვლენილ პრობლემაზე. ეს დაარღვევს აუდიტორის დამოუკიდებლობას. მიგნებებში წამოჭრილი ყველა პრობლემა უნდა ჩაითვალოს შიდა აუდიტის ობიექტის საკუთრებად და აქედან გამომდინარე მათი გამოსწორება წარმოადგენს ობიექტის ხელმძღვანელობის მოვალეობას.

შიდა აუდიტის საბოლოო ანგარიში კლასიფიცირებულია, როგორც კონფიდენციალური და, შესაბამისად, დაცული უნდა იყოს სათანადო ზომებით არაავტორიზებული წვდომის ან გამჟღავნების თავიდან ასაცილებლად.

3.5.3 შიდა აუდიტის დასრულება

დასკვნითი ანგარიშის გამოცემის შემდეგ, შიდა აუდიტის ჯგუფის ხელმძღვანელმა და/ან შიდა აუდიტის სუბიექტის ხელმძღვანელმა უნდა გამართონ დასკვნითი შეხვედრა ობიექტის ხელმძღვანელობასთან, რომ მათგან მიიღონ დაპირება განსაზღვრული სამოქმედო გეგმების შესრულებასთან დაკავშირებით.

აუდიტის დოკუმენტაციის დაარქივება და შენახვა აუდიტის დასრულების პროცესის კიდევ ერთი მნიშვნელოვანი ეტაპია. ამ ეტაპის მიზანია გარკვეული პერიოდის განმავლობაში უზრუნველყოს შიდა აუდიტის დოკუმენტაციისა და ჩანაწერების უსაფრთხოდ შენახვა, სამართლებრივი და მარეგულირებელი მოთხოვნების შესაბამისად, ასევე აუდიტის პროცესის მტკიცებულების უზრუნველსაყოფად. ქვემოთ მოცემულია ძირითადი შესასრულებელი ნაბიჯები:

- **აუდიტორული დოკუმენტაციის დაარქივება:** აუდიტის დოკუმენტაცია მოიცავს შიდა აუდიტის დროს მოპოვებულ ყველა ჩანაწერს, ანგარიშს და სხვა მტკიცებულებებს. აუდიტის დოკუმენტაცია უნდა ინახებოდეს განსაზღვრული პერიოდის განმავლობაში, რომელიც შეიძლება განსხვავდებოდეს აუდიტის ტიპის, მოქმედი კანონებისა და ნორმატიული აქტების მიხედვით. შიდა აუდიტის ჯგუფის ხელმძღვანელმა უნდა უზრუნველყოს, რომ ყველა დოკუმენტაცია, როგორც ფიზიკური, ასევე ელექტრონული, სათანადოდ იქნეს მარკირებული/კოდირებული,

ორგანიზებული და ინახებოდეს უსაფრთხო ადგილზე ინფორმაციის კონფიდენციალურობისა და მთლიანობის უზრუნველსაყოფად;

- **აუდიტის დოკუმენტაციის შენახვა:** აუდიტის დოკუმენტაციის შენახვის ვადა დამოკიდებულია მოქმედ საკანონმდებლო და მარეგულირებელ მოთხოვნებზე. აუდიტის დაარქივებული დოკუმენტაცია რეგულარულად უნდა შემოწმდეს დაწესებული შენახვის პოლიტიკის შესაბამისად, მოთხოვნების დაცვის უზრუნველსაყოფის მიზნით;
- **აუდიტის დოკუმენტაციის განადგურება:** შენახვის ვადის გასვლის შემდეგ, აუდიტის დოკუმენტაცია უსაფრთხოდ უნდა განადგურდეს, რაც გულისხმობს დაშრედერებას (დაქუცმაცებას), დაწვას ან სხვა საშუალებებს, ისეთი ფორმით, რომ ინფორმაციაზე წვდომა ვერ მოხერხდეს არაუფლებამოსილი პირების მხრიდან.

3.5.4 შემდგომი გამოკვლევა

შიდა აუდიტის სუბიექტის ხელმძღვანელმა უნდა ჩამოაყალიბოს სისტემა აუდიტის რეკომენდაციების შესრულების სტატუსზე თვალყურის დევნებისთვის. გამოკვლევის პროცედურა მოიცავს შიდა აუდიტის ობიექტთან დადასტურებას, რომ მაკორექტირებელი ქმედებები განხორციელდა შეთანხმებულ ვადებში და მოხდება ხელახალი ტესტირების ჩატარება რისკის ეფექტურად მინიმიზების უზრუნველსაყოფად.

მიგნება არ ჩაითვლება გამოსწორებულად, სანამ ხელახალი ტესტირება არ დაადასტურებს რომ:

- განხორციელებული კონტროლი შემუშავებულია და ოპერირებს ეფექტურად;
- დაკავშირებული რისკი შემცირებულია მისაღებ დონემდე.

აუდიტის ობიექტის ხელმძღვანელობის მიერ რისკის მიღების შემთხვევაში, შიდა აუდიტის სუბიექტის ხელმძღვანელმა უნდა:

- განსაჯოს აღნიშნული გადაწყვეტილების გონივრულობა;
- შეატყობინოს ორგანიზაციის უმაღლეს ხელმძღვანელს, თუ მიაჩნია, რომ მოცემული რისკის დონე მიუღებელია ორგანიზაციისთვის.

აუდიტის ობიექტის ხელმძღვანელს ანგარიშგება ღია / შეუსრულებელი რეკომენდაციების / მიგნებების შესახებ ხორციელდება მინიმუმ კვარტალში ერთხელ. შემდგომი გამოკვლევის ქმედებები დოკუმენტირებულია და ინახება სამუშაო დოკუმენტებში, წინამდებარე სახელმძღვანელოს შესაბამისად.

3.6 რეკომენდებული შაბლონები

ანგარიშგებისა და კორექტირების ეტაპზე რეკომენდირებულია შემდეგი შაბლონების გამოყენება:

- **310 IT აუდიტის ანგარიში (შაბლონი);**
- **320 შიდა აუდიტის ხარისხის მიმოხილვის საკონტროლო სია (შაბლონი).**

4 ხარისხის კონტროლი

4.1 შიდა აუდიტის ხარისხის კონტროლი

შიდა აუდიტის ხარისხის კონტროლი გულისხმობს შიდა აუდიტის სუბიექტის ხელმძღვანელის მიერ განხორციელებულ სისტემატურ პროცესებს შიდა აუდიტის ფუნქციის მთლიანობის, ობიექტურობისა და დამოუკიდებლობის შესანარჩუნებლად და იმის უზრუნველსაყოფად, რომ შიდა აუდიტის სუბიექტის მიერ შესრულებული სამუშაო აკმაყოფილებდეს მოქმედ პროფესიულ სტანდარტებს, ისევე როგორც შიდა აუდიტის პრინციპებს და სახელმძღვანელო მითითებებს.

დამოუკიდებლობის და ობიექტურობის შემოწმებასთან, კომპეტენციის და პროფესიონალიზმის შენარჩუნებასთან, ასევე ხარისხის უზრუნველყოფის და გაუმჯობესების პროგრამასთან ერთად, შიდა აუდიტის ხარისხის კონტროლის ერთ-ერთი ძირითადი ელემენტია პროექტის ზედამხედველობა და მიმოხილვა.

კერძოდ, შიდა აუდიტის ანგარიშის გავრცელებამდე შიდა აუდიტის სუბიექტის ხელმძღვანელმა უნდა გადახედოს და შეაფასოს სავალდებულო ფორმების სათანადო დოკუმენტაცია (მაგ., დაგეგმვის მემორანდუმი, სამუშაო პროგრამა, მიგნებების მატრიცა და ა.შ.), ასევე საბოლოო დასკვნა და რეკომენდაციები. მიმოხილვის უპირველესი მიზანია ხელი შეუწყოს აუდიტის დოკუმენტებთან დაკავშირებული ნებისმიერი ხარვეზის (რომელიც გავლენას ახდენენ დასკვნაზე) სწრაფ გამოვლენას და გამოსწორებას, ისევე როგორც აუდიტის პროცესში გამოვლენილი ნებისმიერი პრობლემის / არაპროდუქტიულობის აღმოფხვრას, რომელიც მოითხოვს სტრატეგიულ გადაწყვეტილებას მომავალში მისი განმეორების თავიდან ასაცილებლად.

ამ მიზნით, შიდა აუდიტის სუბიექტის ხელმძღვანელმა უნდა გამოიყენოს შიდა აუდიტის ხარისხის მიმოხილვის საკონტროლო ჩამონათვალის ფორმა. ფორმა უნდა შეივსოს თითოეული აუდიტისთვის და უნდა ინახებოდეს პოლიტიკის შესაბამისად.

ამასთან, შიდა აუდიტის სუბიექტის ხელმძღვანელმა უნდა უზრუნველყოს ჩატარებული პროცედურების შესაბამისობა ჰარმონიზაციის ცენტრის შიდა აუდიტის ხარისხის მართვის სახელმძღვანელოს მოთხოვნებთან.

4.2 უწყვეტი მონიტორინგი

უწყვეტი მონიტორინგის ღონისძიებები შედგება რეგულარულად განხორციელებადი პროცედურებისგან, რომელიც მიზნად ისახავს საწარმოს საქმიანობის, მისი შიდა კონტროლის გარემოს და გარე ფაქტორების ცვლილების მონიტორინგს. ამასთან, უწყვეტი მონიტორინგის პროგრამის მიზანია შიდა აუდიტის რისკის ხელახალი შეფასება და აუდიტის გეგმის კორექტირება.

უწყვეტი მონიტორინგის პროგრამის ელემენტები მოიცავს შემდეგს:

- **ხელმძღვანელობასთან შეხვედრებში მონაწილეობა:** ხელმძღვანელობამ შეიძლება გამართოს შეხვედრები მიმდინარე ინიციატივების ან ქმედებების განსახილველად რისკის სფეროებზე რეაგირების მიზნით. ამ შეხვედრებზე შიდა აუდიტის დასწრების მიზანია მიმდინარე მოვლენების გაგება და გაზრდილი რისკის ინდიკატორების იდენტიფიცირება.

თემები, რომლებიც საჭიროებს დამატებით განხილვას, შეიძლება მოიცავდეს სისტემის განვითარების განმახორციელებელ გუნდებს, არსებულ პროცესებში ან შიდა კონტროლში მნიშვნელოვან ცვლილებებს, ხელმძღვანელობის მოქმედებებს მარეგულირებელ შემოწმებებსა და სხვა მნიშვნელოვან ინიციატივებთან დაკავშირებით;

- **საკვანძო მმართველობითი ანგარიშების მიმოხილვა:** მმართველობითი ანგარიშები შეიძლება მიუთითებდეს უჩვეულო ტენდენციებზე, კონტროლის გაუქმებაზე ან აქტივობებზე, რომლებიც შესაძლებელია იყოს გაზრდილი რისკის მაჩვენებელი. აღნიშნული ანგარიშგებები რეგულარულად უნდა განიხილებოდეს ხელმძღვანელობასთან. შიდა აუდიტის მიერ მათი განხილვის სიხშირეს შიდა აუდიტი რისკის მნიშვნელობიდან გამომდინარე;

- **გარე მოვლენების მონიტორინგი:** გარე მოვლენებს შეიძლება ჰქონდეს გავლენა საქმიანობასა და რისკებზე. შესაძლო გავლენის მქონე გარე ფაქტორები მოიცავს ინდუსტრიის მოვლენებს, მარეგულირებელ მოვლენებს, ეკონომიკურ ტენდენციებს, ბუღალტრული აღრიცხვის ახალ სტანდარტებს და ა.შ. მუდმივი მონიტორინგისთვის შიდა აუდიტმა უნდა გამოავლინოს გარე კრიტიკული მოვლენები, რომლებიც დაკავშირებულია მათი საქმიანობის მიმართულებასთან/ფუნქციურ სფეროსთან;

- **მიმდინარე მოვლენები / ტენდენციები:** მიმდინარე მოვლენებმა ან ტენდენციებმა შეიძლება გამოიწვიოს რისკის დონის გაზრდა ან წარმოქმნას ახალი რისკები. მიმდინარე მოვლენები შეიძლება მოიცავდეს ცვლილებებს საინფორმაციო სისტემებში, ძირითადი საქმიანობის პროცესებში ან შიდა კონტროლში; ახალ ან ცვალებად პროდუქტებში ან მომსახურებაში; ცვლილებებს ორგანიზაციულ სტრუქტურაში ან ახალ კადრებში; ახალ ან ფორმირებად რისკებს; ან რისკებს, მზარდი მნიშვნელობით. შიდა აუდიტმა უნდა გამოავლინოს მეთოდი, რომ თვალი ადევნოს მიმდინარე მოვლენებს ან ტენდენციებს საქმიანობის მითითებულ სფეროებში. მათ სფეროში მიმდინარე მოვლენების შესასწავლად, მიმდინარე მოვლენების მონიტორინგს, შესაძლოა ჰქონდეს ხელმძღვანელობასთან პერიოდული შეხვედრების გამართვის, ხელმძღვანელობის შეხვედრებში მონაწილეობის ან საკვანძო ხელმძღვანელობითი (ან მმართველობითი) ანგარიშგებების განხილვის ფორმა.

უწყვეტი მონიტორინგის ღონისძიებების შედეგების ასახვის მიზნით შიდა აუდიტმა უნდა განაახლოს წლიური აუდიტის გეგმა, გადახედოს აუდიტის სიას და განაახლოს რისკის შეფასების დოკუმენტები.

4.3 აუდიტორული დოკუმენტების მარკირება

IT აუდიტის დოკუმენტების მკაფიო და აღწერილობითი დასახელების სტანდარტი გადამწყვეტია დოკუმენტის შინაარსის ზუსტად გადმოცემის უზრუნველსაყოფად. დოკუმენტის სათაურის სიზუსტე შეიძლება გაუმჯობესდეს კონკრეტული ტერმინოლოგიის გამოყენებით ან/და ბუნდოვანი/ზოგადი სათაურების თავიდან აცილების გზით. გარდა ამისა, კარგად ცნობილი და ადვილად გასაგები აბრევიატურების ან შემოკლებების გამოყენებამ, დოკუმენტის სრული სახელის მითითებასთან ერთად, შეიძლება კიდევ უფრო გაზარდოს სათაურის სიცხადე და აღქმა.

ზემოაღნიშნულის გათვალისწინებით, დოკუმენტების დასახელების სტანდარტში გამოიყენება შემდეგი ფორმატი:

XX.YY – დოკუმენტის სახელწოდება (აპლიკაციის ან/და პროცესის სახელწოდებასთან ერთად)

სადაც:

XX	აუდიტის პროცედურის ინდექსი (იხილეთ ქვემოთ მოცემული ცხრილი)
YY	დოკუმენტის უნიკალური ნომერი
დოკუმენტის სახელწოდება	დოკუმენტის შინაარსობრივი აღწერა

#	აუდიტის ეტაპი	პროცედურის ინდექსი	აუდიტორული დოკუმენტის სახელწოდება	მაგალითები
1	დაგეგმვა	110	დაგეგმვის მემორანდუმი	
	დაგეგმვა	120	აუდიტის ინიცირების წერილი	
	დაგეგმვა	130	გახსნითი შეხვედრის ოქმი	
	დაგეგმვა	140	IT პროცესების, რისკებისა და კონტროლების შესწავლა	*140.1 SAP წვდომის ხელმძღვანელობის პროცესი* *140.2 SAP ტექნიკური სახელმძღვანელო (მაგალითი)*
	დაგეგმვა	150 და ა. შ.	დაგეგმვის სხვა დოკუმენტები	
2	განხორციელება	210	აუდიტის სამუშაო პროგრამა	
	განხორციელება	220	კონტროლის ტესტირების ფორმა	*220.1 SAP წვდომის უზრუნველყოფის ტესტი* *220.2 SAP რეგულარული წვდომის მიმოხილვის ტესტი*
	განხორციელება	230	IT ძირითადი პროცედურის ტესტირების ფორმა	*230.1 SAP წვდომის გაუქმების ძირითადი ტესტი*
	განხორციელება	240	აპლიკაციის კონტროლის ტესტირების ფორმა	

	განხორციელება	250	აუდიტის მიგნების მატრიცა	
	განხორციელება	260	დასკვნითი შეხვედრა	
	განხორციელება	270 და ა. შ.	სხვა განხორციელების დოკუმენტები	
3	ანგარიშგება	310	აუდიტის ანგარიშის შაბლონი	
	ანგარიშგება	320	შიდა აუდიტის ხარისხის მიმოხილვის სია	
	ანგარიშგება	330 და ა. შ.	სხვა საანგარიშგებო დოკუმენტები	