კომპანიის ინფორმაციული სისტემების რისკების ანალიზისა და მართვის უახლესი საშუალებები მსოფლიოში, მათი დანერგვის პერსპექტივა და გამოწვევები საქართველოში

დავით კენკებაშვილი

ბიზნესის ადმინისტრირება და თანამედროვე ტექნოლოგიები

სამეცნიერო ხელმძღვანელი: ნინო ლორთქიფანიძე, მაგისტრი

ბიზნესისა და ტექნოლოგიების უნივერსიტეტი

თბილისი, 2019

როგორც ავტორი, ვაცხადებ, რომ ნაშრომი წარმოადგენს ჩემს ორიგინალურ ნამუშევარს, ხოლო სხვა ავტორების მიერ შექმნილი მასალები არის მოხსენებული ან ციტირებული სათანადო წესების შესაბამისად.

დავით კენკებაშვილი

_____

2019 წელი

აბსტრაქტი

წარმოუდგენელია ბიზნესის წარმოება თანამედროვე ცხოვრებაში ინფორმაციული ტექნოლოგიებისა და სისტემების გამოყენების გარეშე. დღესდღეობით უამრავი კომპანიის საქმიანობა დამოკიდებულია ინფორმაციული სისტემების უწყვეტ რეჟიმში ფუნქციონირებაზე და ამ დამოკიდებულების ზრდის პარალელურად იზრდება ინფორმაციულ სისტემებთან დაკავშირებული რისკებიც. აქედან გამომდინარე აქტუალური გახდა კომპანიის ინფორმაციული სისტემების რისკების ანალიზისა და მართვის უახლესი საშუალებების შესწავლა მსოფლიოს სხვადსხვა ქვეყანაში, ასევე მათი დანერგვის პერსპექტივა და გამოწვევები საქართველოში. წინამდებარე კვლევა შეისწავლის ინფორმაციული სისტემების ადუტისა და კონტროლის ასოციაციის მიერ შემოთავაზებულ, ინფორმაციული სისტემების რისკების ანალიზისა და მართვის, გადაწყვეტილებას. აღნიშნული გადაწყვეტილება წარმოადგენს კორპორაციული ინფორმაციული ტექნოლოგიების მართვის ერთ-ერთ ძირითად ნაწილს და განხილულია წიგნში COBIT. ნაშრომში აღწერილია რა არის COBIT, როგორია მისი სტრუქტურა და ძირითადი კომპონენტები. გარდა ამისა, წინამდებარე კვლევა მოიცავს მსოფლიოს სხვადასხვა ქვეყანაში არსებული კომპანიების მაგალითებსა და გამოცდილებას, რომლებმაც ინფორმაციულ სისტემებთან დაკავშირებული რისკების ანალიზისა და მართვის მიზნით დანერგეს COBIT. ნაშრომი ასევე მოიცავს საქართველოში მოღვაწე კომპანიებში არსებულ ინფორაციული სისტემების რისკების მართვის მიდგომებსა და პრაქტიკებს.

ABSTRACT

It is unthinkable to do business in modern life without using information technology and systems. Nowadays, activity of the company depends on the continuous functionality of information systems. And the risks associated with information systems are increasing simultaneously with the growth of this dependence. Hence, it has become the subject of the study of the latest methodologies and approaches of information system risk analysis and management in the different countries, as well as the prospects of their implementation and challenges in Georgia. This research will examine the decision proposed by the Information Systems Audit and Control Association about information sytems risk analysis and management. This decision is one of the key part of governance of enterprise information technology and is reviewed in the book - COBIT. The paper describes what is COBIT, its structure and basic components. In addition, this research includes examples and experiences of companies in different countries around the world who have implemented COBIT for analysis and management of risk related to information systems. The paper also covers the approaches and practices of information systems related risks within companies operating in Georgia.

სარჩევი

სურათებისა და ცხრილებისა ჩამონათვალი IV

აბრევიატურების ჩამონათვალი V

შესავალი 1

თავი 1. სამეცნიერო ლიტერატურის მიმოხილვა 5

1.1. რა არის და რა არ არის COBIT 8

1.2. COBIT 2019-ის სტრუქტურა 16

1.3. COBIT 2019-ის კომპონენტები 20

თავი 2. კომპანიის ინფორმაციული სისტემების რისკების ანალიზისა და მართვის უახლესი საშუალებები მსოფლიოში 34

2.1. ინფორმაციული ტექნოლოგიების კორპორატიული მართვის მდგომარეობა და ზეგავლენა ორგანიზაციებში 34

2.2. IT მართვა და ბიზნეს/IT თანხვედრა მცირე და საშუალო საწარმოებში 39

2.3. IT მართვის არარსებობა საფრთხეს უქმნის ბიზნესის ღირებულებებს 40

2.4. რისკების შეფასების მართვა COBIT 5-ის გამოყენებით 41

2.5. COBIT-ის დანერგვა ეკოპეტროლში IT-ის, მასთან დაკავშირებული რისკების და სტანდარტებთან შესაბამისობის სამართავად 44

2.6. COBIT-ის გამოყენება ჰოსპიტალში რისკების მართვისთვის 51

2.7. IT რისკების მართვა ბანკში 72

თავი 3. კომპანიის ინფორმაციული სისტემების რისკების ანალიზისა და მართვის უახლესი საშუალებების დანერგვის პერსპექტივა და გამოწვევები საქართველოში 86

3.1. ინფორმაციული უსაფრთხოების რისკების მართვის მექანიზმები 86

3.2. ინფორმაციული სისტემების რისკების ანალიზისა და მართვის საშუალებები სახელმწიფო ორგანიზაციებში 88

3.3. ინფორმაციული სისტემების რისკების ანალიზისა და მართვის საშუალებები ბანკებში 89

3.4. ინფორმაციული სისტემების რისკების ანალიზისა და მართვის საშუალებები დიდ კომპანიებში 91

3.5. ინფორმაციული სისტემების რისკების ანალიზისა და მართვის საშუალებები მცირე და საშუალო კომპანიებში 92

თავი 4. დასკვნა და რეკომენდაციები 94

ბიბლიოგრაფია 97

დანართი 1 - კითხვარი 99

სურათებისა და ცხრილებისა ჩამონათვალი

ცხრილი 1. 1 მართვისა და მენეჯმენტის მიზნები 18
ცხრილი 1. 2 შესაბამისი კორპორაციის და განხილვის მიზნები 18
ცხრილი 1. 3 თანხვედრის მიზნებისა და მაგალითების მეტრიკები 20
ცხრილი 1. 4 პროცესის გამოსახვა 21
ცხრილი 1. 5 ორგანიზაციული სტრუქტურა 23
ცხრილი 1. 6 ინფორმაციის დინებისა და ობიექტები 26
ცხრილი 1. 7 მრავალჯერადი პროცესების შედეგები 27
ცხრილი 1. 8 ადამიანების, უნარებისა და კომოეტენციები 31
ცხრილი 1. 9 ადამიანების, უნარებისა და კომოეტენციები 32
ცხრილი 1. 10 ადამიანების, უნარებისა და კომოეტენციები 32
ცხრილი 1. 11 ადამიანების, უნარებისა და კომოეტენციები 33

ცხრილი 2. 1 მე-2 დონის რისკების შედარება 75
ცხრილი 2. 2 RCA პროცესის ნაბიჯები 79
ცხრილი 2. 3 RACI მაგალითის გრაფიკი 81

სურათი 1. 1 COBIT-ის მიმოხილვა 11
სურათი 1. 2 COBIT-ის ძირითადი მოდელი 13
სურათი 1. 3 COBIT-ის მართვის სისტემის კომპონენტები 15
სურათი 1. 4 პროცესების შესაძლებლობების დონე 22

სურათი 2. 1 COBIT 5 მიზნების კასკადი 35
სურათი 2. 2 რესპოდენტების პროფილი კონტინენტების დონეზე 36
სურათი 2. 3 კომპონენტების მნიშვნელობა 36
სურათი 2. 4 დანერგვის/მენეჯმენტის დონე 37
სურათი 2. 5 სრული პროცესის საშუალო შეფასება 37
სურათი 2. 6 კავშირი IT-სთან დაკავშირებული მიზნებსა და ორგანიზაციული მიზნებს შორის .. 38

აბრევიატურების ჩამონათვალი

COBIT - Control Objectives for Information and Related Technology - ინფორმაციისა და მასთან დაკავშირებული ტექნოლოგიების კონტროლის მიზნები

IT - Information Technology - ინფორმაციული ტექნოლოგიები

GEIT - Governance of Enterprise Information Technology - კორპორაციული ინფორმაციული ტექნოლოგიების მართვა

GRC - Governance Risk and Compliance - მართვა, რისკები და შესაბამისობა

CEO - Chief Executive Officer - აღმასრულებელი დირექტორი

CIO - Chief Information Officer - ინფორმაციული დირექტორი

CFO - Chief Financial Officer - ფინანსური დირექტორი

COO - Chief Operating Officer - ოპერაციული დირექტორი

EDM - Evaluate, Direct and Monitor - შეფასება, მიმართვა და მონიტორინგი

APO - Align, Plan and Organize - განლაგება, დაგეგმვა და ორგანიზება

BAI - Build, Acquire and Implement - შენება, შეძენა და დანერგვა

DSS - Deliver, Service and Support - მიწოდება, მომსახურება და მხარდაჭერა

MEA - Monitor, Evaluate and Assess - მონიტორინგი, შეფასება და გაზომვა

DevOps - Software Development and Information Technology Operations - პროგრამული უზრუნველყოფის შემუშავება და ინფორმაციული ტექნოლოგიების ოპერაციები

AG - Alignment Goals - თანხვედრის მიზნები

EG - Enterprise Goals - კორპორაციული მიზნები

CMMI - Capability Maturity Model Integration - შესაძლებლობების სიმწიფის მოდელის ინტეგრაცია

ICT - Information and Communication Technology - ინფორმაციული და საკომუნიკაციო ტექნოლოგიები

SFIA - Skills Framework for the Information Age –IT პერსონალის უნარების აღწერის ყველაზე პოპულარული საშუალება მსოფლიოში

ISACA - Information Systems Audit and Control Association - ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაცია

SME - Small and Medium Enterprises - მცირე და საშუალო საწარმოები

COSO - Committee of Sponsoring Organizations of the Treadway Commission - კორპორაციული რისკების მართვის, შიდა კონტროლისა და თაღლითობის აღკვეთის ერთობლივი ინიციატივა

SAP - Systems, Applications and Products - სისტემები, აპლიკაციები და პროცედურები

HIS - Hospital Information System - ჰოსპიტალის ინფორმაციული სისტემა

PID - Personal Identification – პირადი საიდენტიფიკაციო ინფორმაცია

EUC - End User Computing - კომპიუტერის საბოლოო მომხმარებელი

MRSA - Methicillin Resistant Staphylococcus Aureus - მეთიცილინის რეზისტენტული სტეფილოკოკუს აურუსი

LAN - Local Area Network - ლოკალური ქსელი

PC - Personal Computer - პერსონალური კომპიუტერ

BPR - Business Process Reengineering - ბიზნეს პროცესის აღდგენა

HRM - Human Resource Management - ადამიანური რესურსების მართვა

DPC - Diagnosis Procedure Combination - დიაგნოზის პროცედურის კომბინაცია

DRG - Diagnosis Related Group - დიაგნოზთან დაკავშირებული ჯგუფი

PPS - Prospective Payment System – პერსპექტიული გადახდის სისტემა

MLHW - Ministry of Healthcare, Labor and Welfare - ჯანდაცვა, შრომისა და კეთილდღეობის მინისტრი

COF - Control Objective Framework - კონტროლების მიზნების ჩარჩო

RCA - Risk and Control Assessment - რისკისა და კონტროლის შეფასება

CISA - Certified Information System Auditor - სერტიფიცირებული ინფორმაციული სისტემების აუდიტორი

CA - Chartered Accountant - ჩარტერული ბუღალტერი

CSA - Control Self-Assessment - კონტროლის თვითშეფასება, რისკების მართვისა და კონტროლების შეფასების ტექნიკა

შესავალი

ინფორმაცია თანამედროვე ეკონომიკის ყველაზე ღირებული რესურსია. მისი დამუშავება შესაძლებლობას აძლევს მომხმარებელს გააუმჯობესოს საქმიანობის ეფექტურობა, გადააფასოს ბიზნეს მოდელები და გარდაქმნას ინდუსტრიები. ორგანიზაციები იყენებენ თანამედროვე ტექნოლოგიებს, რათა მოახდინონ ინფორმაციის ძალის სრულად რეალიზება. შედეგად, გახდნენ უფრო მეტად ინტელექტუალურები და ჩართულები ავტომატიზაციისა და ხელოვნური ინტელექტის გამოყენებით დახმარებით, აპლიკაციებისა და მონაცემთა საფუძვლიანი დამუშავების გამოყენებით და მოახდინონ კლიენტებთან, პარტნიორებთან და თანამშრომლებთან ურთიერთკავშირის სტიმულირება.

ინფორმაციისა და მონაცემების მოპოვების, შენახვის, გადაცემისა და დამუშავებისათვის გამოიყენება ინფორმაციული ტექნოლოგიები (IT). ინფორმაციული ტექნოლოგიების სისტემები ანუ ინფორმაციული სისტემები მოიცავს ყველა მყარ მოწყობილობას, პროგრამულ უზრუნველყოფასა და პერიფერიულ მოწყობილობას, რომელსაც იყენებს მომხმარებელთა ჯგუფები.

კომპანიის ინფორმაციული სისტემები წარმოადგენს მსხვილ კომპლექსურ პროგრამულ უზრუნველყოფებს, მყარ მოწყობილობებსა და ინსტრუმენტებს, რომლებიც გამოიყენება ძირითადი, ადმინისტრაციული და მხარდამჭერი პროცესებისთვის. ყოველდღიურად ეს სისტემები ამუშავებს ათასობით ტრანზაქციას, სადაც ხდება მონაცემების შეყვანა, მანიპულაცია და შენახვა, როგორც საოპერაციო ასევე ინფორმაციული მიზნებისთვის. შედეგად მიღებული ინფორმაციული რესურსები წარმოადგენს მნიშვნელოვან ინსტიტუციონალურ აქტივს, რომელიც გამოიყენება ანალიზისა და გადაწყვეტილების მიღებისთვის. მონაცემები გახდა ძირითადი პრიორიტეტი ყველა სახის ბიზნესისთვის. გავრცელდა და განვითარდა ტექნოლოგიები, რომლებიც ახდენენ მომხმარებელთა

მონაცემთა შეგროვებასა და გაანალიზებას ყოველდღიური ოპერაციების უკეთე განსაღვრისთვის, კონტექსტუალიზაციისა და ახალი ბიზნეს იდეების წარმოქმნის მიზნით.

ინფორმაციული ტექნოლოგიების განვითარებასთან ერთად იზრდება მასთან დაკავშირებული რისკები და საფრთხეები. მაშინ როდესაც კიბერ უსაფრთხოება (მონაცემთა და პირადი ინფორმაციის ქურდობა, წვდომების დაკარგვა) საზოგადოებრივი ყურადღების ცენტრშია, ორგანიზაციის ინფორმაციულ ტექნოლოგიებზე პასუხისმგებელი პირები აწყდებიან უამრავ რისკს, რომლებიც გავლენას ახდენენ კომპანიაზე, თანამშრომლებზე, მომხმარებლებსა და კლიენტებზე.

ინფორმაციული ტექნოლოგიების მართვის რისკების კრიტიკულ ზრდასთან ერთად, ორგანიზაციების საბჭოებისთვის, განსაკუთრებით ფინანსური სერვისების მომწოდებელი კომპანიებისთვის, გაიზარდა რისკების მართვასთან დაკავშირებული პასუხისმგებლობა. IT რისკები ჯერ კიდევ შესაძლებელია იყოს ისეთი რისკები, რომლის გაკონტროლებისთვისაც კომპანიის საბჭოს წევრები ყველაზე ნაკლებად არიან მომზადებულნი. როგორც წესი დირექტორთა მხოლოდ მინიმალურ რაოდენობას აქვს IT მიმართულების სიღრმისეული ცოდნა, ხოლო ძირითადი ნაწილი IT რისკებად აღიქვამს მხოლოდ კიბერ თავდასხმებსა და სისტემის ხელმისაწვდომობასთან დაკავშირებულ საკითხებს, როდესაც IT რისკები გავრცელებულია მთელს ორგანიზაციაში.

ტექნოლოგია არის შესანიშნავი მამოძრავებელი ძალა, თუმცა ასევე წარმოადგენს გავრცელებულ, პოტენციურად მაღალი ალბათობის რისკს. დღესდღეობით კიბერ რისკები ასოცირდება მონაცემთა ქურდობასთან, კომპრომეტირებულ ექუნთებთან, განადგურებულ ფაილებთან, გამორთულ ან დეგრადირებულ სისტემებთან. თუმცა, მხოლოდ ეს არ არის ინფორმაციულ სისტემებთან დაკავშირებული რისკები, რაზეც უნდა კონცერტრირდეს მენეჯმენტი და დირექტორთა საბჭო.

კომპანიები აწყდებიან რისკებს რომლის გამომწვევი მიზეზი ხშირ შემთხვევაში ბიზნესსა და IT სტრატეგიებს შორის თანხვედრის არ არსებობის, მენეჯმენტის გადაწყვეტილების, რომლის საფუძველზეც იზრდება IT გარემოს ღირებულება და კომპლექსურობა და არასაკმარისი ან შეუსაბამო კადრების შედაგად წარმოიქმნება.

კომპანიის ინფორმაციული სისტემები შესაძლებელია გახდეს მოძველებული, განადგურებული ან არაკონკურენტული რადგან თანამედროვე ტექნოლოგიების მუდმივი განვითარების შედეგად იქმნება სისტემები, რომლებსაც აქვთ შესაძლებლობა ნაკლები რესურსით მიაღწიოს მეტ სიმძლავრეს და ფლობდეს ისეთ შესძლებლობებს, რაც არ გააჩნდა მის გამოგონებამდე არსებულ სისტემებს. IT გარემოს რისკები კლასიფიცირდება სამ ძირითად კატეგორიად: ტექნიკური დონის რისკები, აპლიკაციის-მომხმარებლის დონის რისკები და ბიზნესის დონის რისკები. ფაქტია ისიც რომ ბევრი მმართველი გუნდი ვერ ახერხებს ბიუჯეტის სწორად განსაზღვრასა და ამ რისკებთან გამკლავებას. იმავდროულად, ტექნოლოგიებზე დაფუძნებული სტარტაფები და ფინანსური ტექნოლოგიები (ფინტეკი) არის ბიზნეს მოდელებისა და პროცესების თანამედროვე გამოწვევები, რომლებიც უსწრაფესად რეაგირებენ მიმდინარე მოთხოვნებზე.

კომპანიები აწყდებიან რისკებს, რომლებიც მომდინარეობს მათივე ინფორმაციული სისტემებიდან. როდასც საქმე ეხება ციფრული ტექნოლოგიების გამოყენებას, კიბერსუფრთხოება არის უმნიშვნელოვანესი, თუმცა არანაკლებ მნიშვნელოვანია ოპერაციული, სამართლებრივი, ფინანსური, რეპუტაციული და საზოგადოების წინაშე არსებულ ვალდებულებებთან დაკავშირებული რისკების მართვა. თითოეულ ორგანიზაციას, რომელიც შესაძლოა სხვებისგან განსხვავდებოდეს თავისი ტექნოლოგიური პროფილითა და რისკების მართვის მიდგომებით, ესაჭიროება წინასწარ განსაზღვრული და კონკრეტული რსიკების მართვის გეგმა.

რისკების სამართავად არ არის აუცილებელი იყო ექსპერტი IT სფეროში, მაგრამ საჭიროა ხედავდე IT გაემოში არსებულ სურათს თვალნათლივ, არსებობდეს ინტენსიური და ეფექტური კომუნიკაცია ბიზნესსა და IT-ის შორის, რათა შეძლო მისი გაკონტროლება და მართვა. იმისათვის რომ კომპანიებმა შექმნან ინფორმაციული სისტემების რისკების მართვის იდეალური მოდელი საჭიროა თავდაპირველად ჩამოაყალიბონ და დანერგონ IT-ის და მასთან დაკავშირებული პროცედურებისა და პროცესების მართვის სტრუქტურა და სტრატეგია.

წინამდებარე ნაშრომი მიზნად ისახავს მიმოიხილოს COBIT-ის შესაძლებლობები, მისი დანერგვისა და გამოყენების საშუალებები ინფორმაციული სისტემების რისკების ანალიზისა და მართვის კუთხით, ასევე წარმოაჩინოს დამატებით რა ღირებულებების შექმნა შეუძლია COBIT-ს სხვადასხვა სექტორში მოღვაწე კომპანიებისთვის. განახორციელოს IT კორპორაციული მართვის მიმოხილვა და განმარტება. მსოფლიოს მასშტაბით არსებული კომპანიების მაგალითზე წარმოაჩინოს მისი გამოყენების შედეგად შექმნილი ღირებულებები.

ნაშრომის მიზანია საქართველოში არსებულ, სხვადასხვა სეგმენტსა და სექტორში მოღვაწე კომპანიებში შეისწავლოს არსებული ინფორმაციული სისტემების რისკების ანალიზისა და მართვის მიდგომები. გაანალიზოს და შეაფასოს რამდენად კარგად არის გაგებული კომპანიის უმაღლესი მენეჯმენტის მხრიდან ინფორმაციული ტექნოლოგიების მნიშვნელობა და გავლენა მათ ბიზნესზე და იაზრებენ თუ არა, რომ ნებისმიერი რისკი, რომელიც დაკავშირებულია კომპანიის ინფორმაციულ სისტემებთან პირდაპირ კავშირშია მათი ბიზნესისა და საქმიანობის წარმატებასთან. ამისათვის განხორციელდა კვლევა, რომლის საფუძველზეც ჩატარდა ინტერვიუები საქართველოში არსებული 20 წარმატებული კომპანიის წარმომადგენლებთან. რესპოდენტებმა ისაუბრეს დამსაქმებელ კომპანიაში არსებული ინფორმაციული სისტემების რისკების ანალიზისა და მართვის მიდგომებზე, რომელსაც იყენებს კომპანია.

თავი 1. სამეცნიერო ლიტერატურის მიმოხილვა

ციფრული ტრანსფორმაციის ფონზე, ინფორმაციული ტექნოლოგიების მხარდაჭერა გადამწყვეტი გახდა კომპანიების მდგრადობისა და ზრდის შესანარჩუნებლად. ოდესღაც მმართველი საბჭოები (დირექტორთა საბჭოები) და უმაღლესი მენეჯმენტი ინფორმაციულ სისტემებთან დაკავშირებულ გადაწყვეტილებებს თავიდან ირიდებდნენ, ახდენდნენ დელეგირებას ან უბრალოდ აიგნორებდნენ. ხოლო დღესდღეობით უმრავლეს სექტორსა და ინდუსტირაში ასეთი დამოკიდებულება არ არის რეკომენდირებული. დაინტერესებული მხარეებისთვის ხშირად ღირებულებებს (მაგ.: სარგებლის რეალიზება ოპტიმალური ფასის მქონე რესურსებით რისკების ოპტიმიზაციასთან ერთად) ქმნის ბიზნეს მოდელების გაციფრულება, ეფექტური პროცესები, წარმატებული ინოვაციები და ა.შ. გაციფრულებული კომპანიები გადარჩენისა და ზრდის მიზნით სულ უფრო და უფრო მეტად დამოკიდებულნი ხდებიან ინფორმაციულ სისტემებზე.

კომპანიის რისკების მართვისთვის და ღირებულების შექმნისთვის ინფორმაციული სისტემების ცენტრალიზების გათვალისწინებით, ბოლო სამი ათწლეულის განმავლობაში განსაკუთრებული ყურადღება დაეთმო კორპორაციული ინფორმაციული ტექნოლოგიების მართვას (GEIT). GEIT არის კორპორაციული მმართველობის განუყოფელი ნაწილი. ის გამოიყენება საბჭოს მიერ, რომელიც ზედამხედველობას უწევს ორგანიზაციაში პროცესების, სტრუქტურების და რელაციური მექანიზმების განსაზვრას და დანერგვას, რაც საშუალებას აძლევს, როგორც ბიზნეს, ასევე IT პროფესიონალებს შეასრულონ მათზე დაკისრებული ვალდებულებები ბიზნესისა და ინფორმაციული სისტემების თანხვედრის ხელშეწყობის და ინფორმაციული სისტემების საშუალებით ბიზნესში განხორციელებული ინვესტიციებისგან ღირებულებების შექმნის მიზნით.

კორპორაციული ინფორმაციული სისტემების მართვა კონცენტრირებულია ისეთ საკითხებზე როგორიც არის, ღირებულებების მიღება ციფრული ტრანსფორმაციიდან და ციფრული ტრანსფორმაციის შედეგად გამოწვეული ბიზნეს რისკების შემცირებიდან. უფრო კონკრეტულად რომ ავღწეროთ კორპორაციული ინფორმაციული ტექნოლოგიების მართვის წარმატებით დანერგვის შედეგად მოსალოდნელია სამი ძირითადი ედეგი:

სარგებლის რეალიზება - მოიცავს ღირებულებების შექმნას კორპორაციისთვის ინფორმაციული ტექნოლოგიების გამოყენებით, ინფორმაციულ სისტემებში განხორციელებული ინვსტიციებიდან მომავალი ღირებულებების მხარდაჭერასა და ზრდას და იმ IT ინიციატივებისა და აქტივების თავიდან არიდებას, რომლებიც არ ქმნიან საკმარის ღირებულებას. ინფორმაციული სისტემების ღირებულებების ძირითადი პრინციპია მიზანზე მორგებული (fit-for-purpose) სერვისებისა და გადაწყვეტილებების მიწოდების უზრუნველყოფა განსაზღვრულ დროსა და ბიუჯეტში, რაც ქმინს მიზნობრივ ფინანსურ და არაფინანსურ სარგებელს. ღირებულებები, რომლებსაც უზრუნველყოფს ინფორამციული სისტემები უნდა იყოს პირდაპირ კავშირში იმ ღირებულებებთან, რომლებზეც ფოკუსირებულია ბიზნესი. ის ასევე უნდა შეფასდეს ისეთი გზით, რომელიც კომპანიაში ღირებულებების შექმნის პროცესში წარმოაჩენს ინფორმაციულ სისტემებში განხორციელებული ინვესტიციების გავლენასა და წვლილს.

რისკების ოპტიმიზაცია - გულისხმობს კომპანიის ფარგლებში ინფორმაციული სისტემების დანერგვასთან, გამოყენებასთან, ფლობასთან, ჩართულობასთან და ზეგავლენასთან დაკავშირებული ბიზნეს რისკების მართვას. ინფორმციულ სისტემებთან დაკავშირებული ბიზნეს რისკები მოიცავს ინფორმაციულ ტექნოლოგიებთან დაკავშირებულ მოვლენებს, რომლებსაც შეუძლიათ პოტენციური ზეგავლენა მოხდინონ ბიზნესზე. მაშინ, როდესაც ბიზნესისთვის ღირებულების მიწოდება ფოკუსირდება ღირებულების შექმნაზე, რისკების მართვა ფოკუსირდება ღირებულების შენარჩუნებაზე. ინფორმაციული სისტემების რისკების მართვა უნდა იყოს ინტეგრირებული კოპმანიის რისკების მართვის მიდგომებთან, რათა კომპანიის მხრიდან უზრუნველყოფილი იყოს

ინფორმაციულ ტექნოლოგიებზე ფოკუსირება. ის ასევე უნდა შეფასდეს ისეთი გზით, რომელიც წარმოაჩენს ღირებულებების შენარჩუნების მიზნით ინფორმაციულ სისტემებთან დაკავშირებული ბიზნეს რისკების ოპტიმიზაციის გავლენასა და წვლილს.

რესურსების ოპტიმიზაცია - უზრუნველყოფს სტრატეგიული გეგმის განხორციელებისათვის საჭირო შესაძლებლობების განსაზღვრას და საკმარისი, შესაბამისი და ეფექტური რესურსების მობილიზებას. რესურსების ოპტიმიზაცია უზრუნველყოფს ინტერგირებული, ეკონომიური IT რესურსების მობილიზებას, ახალი ტექნოლოგიების დანერგვას ბიზნესის მოთხოვნების შესაბამისად და მოძველებული სისტემების განახლებას ან ახლით ჩანაცვლებას. გამომდინარე იქიდან, რომ აპარატურისა და პროგრამული უზრუნველყოფების გარდა აღსანიშნავია ადამიანების მნიშვნელობაც, რესურსების ოპტიმიზაცია ფოკუსირდება ინფორმაციული ტექნოლოგიების პერსონალისათვის ტრენინგების ჩატარებაზე, თანამშრომელთა წახალისებასა და კომპეტენციების გაღრმავებაზე. არანკლებ მნიშვნელოვანი რესურსები არის მონაცემები და ინფორმაცია, ამიტომ ოპტიმალური ღირებულებების მისაღებად მონაცემებისა და ინფორმაციის ექსპლუატაცია არის რესურსების ოპტიმიზაციის კიდევ ერთი მნიშვნელოვანი ელემენტი. (ISACA 2018, 11-12)

"ორგანიზაციებში კორპორაციული ინფორმაციული ტექნოლოგიების მართვის მდგომარეობა და ზეგავლენა: საერთაშორისო კვლევის ძირითადი აღმოჩენები" კვლევის თანახმად, ორგანიზაციებში ცუდად შემუშავებული ან დანერგილი კორპორაციული ინფორმაციული ტექნოლოგიების მართვის მიდგომებით აკეთებენ უარესს ბიზნესისია და ინფორმაციული სისტემების სტრატეგიების და პროცესების თანხვედრისთვის. შედეგად ასეთი ორგანიზაციებისთვის ნაკლებად სავარაუდოა, რომ მიაღწიონ განსაზღვრულ ბიზნეს სტრატეგიებს და მოახდინონ იმ ღირებულებების რეალიზება, რომლებსაც ისინი მოელოდნენ ციფრული ტრანსფორმაციისგან.

აქედან გამომდინარე, ნათელია რომ კორპორაციული ინფორმაციული ტექნოლოგიების მართვა უნდა იყოს აღქმული და რეალიზებული უფრო ფართოდ, ვიდრე ხშირად განმეორებადი ინტერპრეტაცია მართვა, რისკები და შესაბამისობა

(GRC). აბრევიატურა GRC თავის თავში მოიაზრებს, რომ შესაბამისობა და მასთან დაკავშირებული რისკები წარმოადგენს მართვის სპექტრს. (Haes, Joshi, Grembergen, 2015)

COBIT - ინფორმაციული ტექნოლოგიების მართვის ჩარჩო

წლების განმავლობაში, ჩამოყალიბდა და განვითარდა საუკეთესო პრაქტიკის მქონე მოდელი, რაც ხელს უწყობს კორპორაციული IT-ის გაგების, მოდელირებისა და დანერგვის პროცესს . COBIT 2019 25 წელზე მეტია ამ სფეროში ვითარდება, არა მხოლოდ მეცნიერების ახალი ხედვის ჩართულობით, არამედ ამ ხედვათა პრაქტიკაში გამოყენებითაც.

IT-ის აუდიტორიულ საზოგადოებაში ჩართვით COBIT-მა განავითარა უფრო ფართო და სრულყოფილი ინფორმაციული ტექნოლოგიების (IT) მართვისა და მენეჯმენტის მოდელი. ის ახლაც აგრძელებს თავი დაიმკვიდროს, როგორც საზოგადოდ მიღებულმა IT მართვის მოდელმა.

1.1. რა არის და რა არ არის COBIT

სანამ COBIT-ის განახლებულ მოდელს აღვწერთ, მნიშვნელოვანია ავხსნათ რა არის COBIT და რა არა.

COBIT არის IT მართვისა და მენეჯმენტის მოდელი, რომელიც გამიზნულია მთლიანი კორპორაციისათვის. კორპორაციული IT გულისხმობს ყველა იმ IT პროცესს, რომელსაც კომპანია ახორციელებს მიზნის მისაღწევად, მიუხედავად იმისა, თუ ორგანიზაციის რომელ ნაწილში ხდება ეს. სხვა სიტყვებით რომ ვთქვათ, კორპორაციული IT კი არ შემოიფარგლება მხოლოდ კომპანიის IT დეპარტამენტით, არამედ მოიცავს მას.

COBIT მოდელი ქმნის მკაფიო განსხვავებას მართვასა და მენეჯმენტს შორის. ეს ორი დისციპლინა მოიცავს სხვადასხვა აქტივობებს, მოითხოვს განსხვავებულ ორგანიზაციულ სტრუქტურებს და ემსახურება სხვადასხვა მიზნებს.

- მართვა უზრუნველყოფს რომ:
    1. დაინტერესებული მხარეების საჭიროებები, პირობები და არჩევანი შეფასდეს ისე, რომ განისაზღვროს დაბალანსებული და შეთანხმებული ორგანიზაციული მიზნები.
    2. განისაზღვროს მიმართულება პრიორიტეტების ჩამოყალიბებისა და გადაწყვეტილების მიღების საფუზველზე.
    3. საქმის შესრულება და შესაბამისობა გაკონტროლდეს შეთანხმებული მიმართულებისა და მიზნების მიხედვით.

კორპორაციათა უმეტესობაში, მართვა ევალება დირექტორთა საბჭოს, რომელიც იმყოფება თავმჯდომარის ხელმძღვანელობის ქვეშ. კონკრეტული მართვის მოვალეობები შესაძლოა დაევალოს გარკვეულ ორგანიზაციულ სტრუქტურებს შესაბამის დონეზე, განსაკუთრებით დიდი, რთული აგებულების მქონე კორპორაციებში.

- მენეჯმენტი გეგმავს, ქმნის, უძღვება და აკონტროლებს აქტივობებს,

    მართვის ორგანოს მიერ დადგენილი მიმართულებით, კორპორაციული მიზნების მისაღწევად.

კორპორაციათა უმეტესობაში, მართვა არის აღმასრულებელი მენეჯმენტის მოვალეობა, რომელიც იმყოფება აღმასრულებელი დირექტორის (CEO) ხელმძღვანელობის ქვეშ.

COBIT განსაზღვრავს კომპონენტებს, რათა აიგოს და შენარჩუნდეს მართვის სისტემა: პროცესები, ორგანიზაციული სტრუქტურები, პოლიტიკა და პროცედურები, ინფორმაციის დინება, კულტურა და ქცევა, უნარები და ინფრასტრუქტურა.

COBIT განსაზღვრავს დიზაინის ფაქტორებს, რომლებიც გათვალისწინებულ უნდა იქნას კორპორაციის მიერ, საუკეთესოდ მორგებული მართვის სისტემის შექმნისთვის.

COBIT მიმართავს მართვის საკითხებს, შესაბამისი მართვის კომპონენტების დაჯგუფებას მართვისა და მენეჯმენტის მიზნებთან, რომლებიც შეიძლება მოგვარდეს საჭირო შესაძლებლობების დონეზე.

აუცილებლია უნდა აღმოიფხვრას რამდენიმე გაუგებრობა COBIT-ის შესახებ:

- COBIT არ არის ორგანიზაციის მთლიანი IT გარემოს სრული აღწერა.
- COBIT არ არის მოდელი, რომლითაც ბიზნეს პროცესების ორგანიზება უნდა მოვახდინოთ.
- COBIT არ არის IT მოდელი, რომლითაც ხდება ყველა ტექნოლოგიის მართვა.

COBITარ წყვეტს ან მიუთითებს რომელიმე IT-სთან დაკავშირებულ გადაწყვეტილებაზე. ის არ წყვეტს რა არის საუკეთესო IT სტრატეგია, რა არის საუკეთესო არქიტექტურა და არც ღირებულების განსაზღვრის სახელმძღვანელო. რეალურად COBIT განსაზღვრავს ყველა კომპონენტს, რაც აღწერს რომელი გადაწყვეტილება უნდა იქნას მიღებული, როგორ და ვის მიერ.

COBIT 2019-ის მიმოხილვა

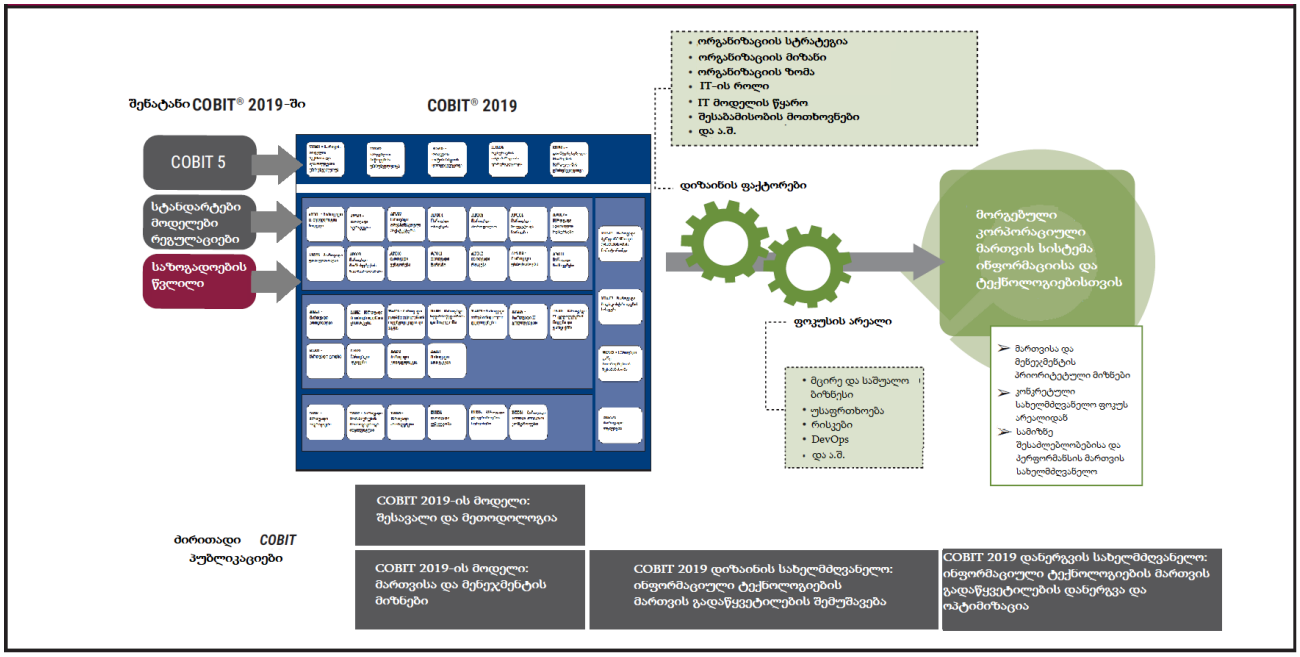
COBIT 2019-ის საერთო პროდუქტი არის ღია და მოდიფიცირებისთვის შექმნილი. ხელმისაწვდომია შემდეგი გამოცემები:

- *COBIT 2019-ის მოდელი: შესავალი და მეთოდოლოგია* წარმოადგენს COBIT 2019-ის ძირითად ცნებებს.
- *COBIT 2019-ის მოდელი: მართვისა და მენეჯმენტის მიზნები* სრულყოფილად აღწერს 40 მთავარ მართვისა და მენეჯმენტის მიზანს, მასში შემავალ პროცესებს და სხვა დაკავშირებულ კომპონენტებს. სახელმძღვანელო ასევე მიუთითებს სხვა სტანდარტებსა და მოდელებზე.
- *COBIT 2019-ის დიზაინის სახელმძღვანელო: IT მართვის გადაწყვეტილების შექმნა* იკვლევს მოდელირების ფაქტორებს, რომლებსაც შეუძლიათ მართვაზე გავლენის მოხდენა და მოიცავს კორპორაციაზე მორგებული მართვის სისტემის დაგეგმვას.

- *COBIT 2019-ის დანერგვის სახელმძღვანელო: IT მართვის გადაწყვეტილების დანერგვა და ოპტიმიზაცია* წარმოადგენს COBIT 5-ის დანერგვის სახელმძღვანელოს და ავითარებს გზამკვლევს მუდმივი მართვის გაუმჯობესებისთვის.

სურათ 1.1 გვიჩვენებს COBIT 2019-ის მაღალი დონის მიმოხილვას და წარმოაჩენს, თუ როგორ ფარავს სხვადასხვა გამოცემები სხვადასხვა ასპექტებს.

სურათი 1. 1 ***COBIT-ის მიმოხილვა***



შიგთავსი, რომელიც სურათი 1.1-ში მიჩნეულია სამიზნე არეალებად, მომავალში იქნება უფრო მეტი დეტალის შემცველი სახელმძღვანელო კონკრეტული თემების შესახებ.

მომავალში, COBIT მომხმარებელ საზოგადოებას მოუწოდებს შიგთავსის განახლების შეთავაზებისკენ, რათა ის გამოყენებულ იქნას, როგორც მუდმივად კონტროლირებადი უწყვეტი ბაზა და ასევე შენარჩუნდეს საბოლოო შეხედულებებსა და განვითარებებზე დაყრდნობილი მოდელი.

მომდევნო სექციები ხსნიან COBIT 2019-ში გამოყენებულ ძირითად კონცეფციებსა და ტერმინებს.

მართვისა და მენეჯმენტის მიზნების მიმოხილვა

იმისთვის, რომ IT-მ წვლილი შეიტანოს კორპორაციის მიზნების მიღწევაში, მრავალი მართვისა და მენეჯმენტის მიზანი უნდა იქნეს მიღწეული. მართვისა და მენეჯმენტის მიზნებთან დაკავშირებული ძირითადი კონცეფციებია:

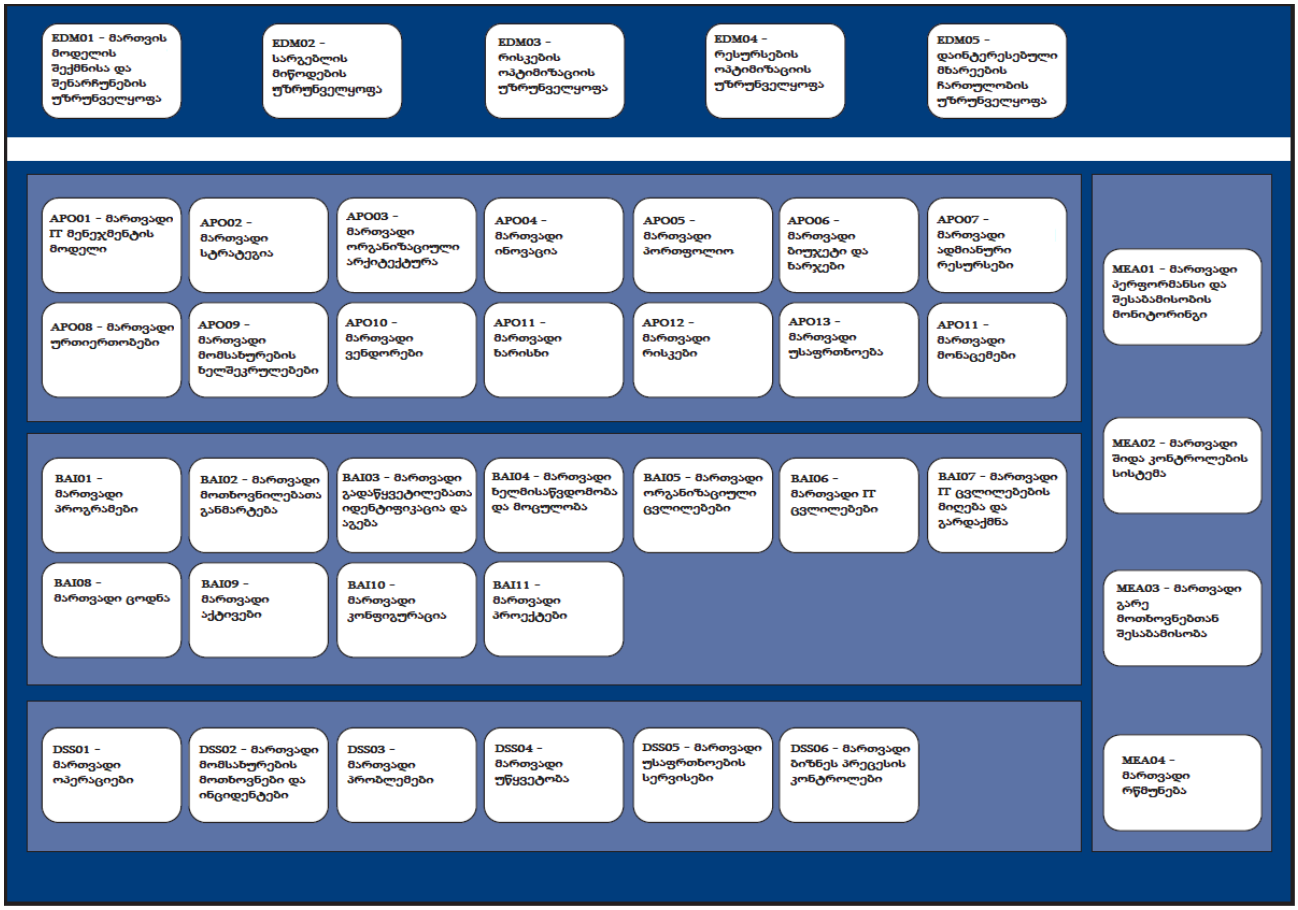
- მართვისა და მენეჯმენტის მიზანი ყოველთვის დაკავშირებულია ერთ პროცესთან (იდენტური ან მსგავსი სახელით) და სხვა სახის დაკავშირებული კომპონენტების სერიებთან, რათა დაეხმაროს კომპანიას მიზნების მიღწევაში.
- მართვის მიზნები დაკავშირებულია მართვის პროცესთან (გამოსახულია მუქ ლურჯ ფონზე სურათი 1.2-ში), ხოლო მენეჯმენტის მიზნები დაკავშირებულია მენეჯმენტის პროცესთან (გამოსახულია ცისფერ ფონზე სურათი 1.2-ში). საბჭოები და აღმასრულებელი მენეჯმენტი ანგარიშვალდებულნი არიან მართვის პროცესზე, ხოლო მენჯმენტის პროცესები არის უფროსი და საშუალო მენეჯმენტის მთავარი საქმიანობა.

მართვისა და მენეჯმენტის მიზნები COBIT-ში დაყოფილია 5 სფეროდ. ამ სფეროებს აქვთ დომეინის სახელები. დომეინები გამოხატავენ მათში შემცველი მიზნებისა და აქტივობის არეალს:

- მართვის მიზნები დაჯგუფებულია შემდეგ სფეროში: შეფასება, მიმართვა და კონტროლი (EDM). ამ სფეროში მართვის ორგანო აფასებს სტრატეგიულ პარამეტრებს, მიმართავს უფროს მენეჯმენტს არჩეული სტრატეგიული ვარიანტებისკენ და აკონტროლებს ამ სტრატეგიის მიღწევებს.
- მენეჯმენტის მიზნები გადანაწილებულია 4 სფეროში.
    - განლაგება, დაგეგმვა და ორგანიზება (APO) უკავშირდება IT ორგანიზებას, სტრატეგიას და მხარდამჭერ აქტივობებს.
    - აგება, შეძენა და დანერგვა (BAI) ეხება IT გადაწყვეტილების მიღებას, დანერგვას და მის გაერთიანებას ბიზნეს პროცესებში.
    - მიწოდება, მომსახურება და მხარდაჭერა (DSS) უკავშირდება IT სერვისების ოპერატიულ მიწოდებასა და მხარდაჭერას უსაფრთხოების ჩათვლით.

- მონიტორინგი, შეფასება და გაზომვა (MEA) უკავშირდება IT საქმიანობის მონიტორინგს და შესაბამისობას შიდა საქმიანობის მიზნებთან, შიდა კონტროლის მიზნებთან და გარე მოთხოვნებთან.

სურათი 1. 2 COBIT-ის ძირითადი მოდელი



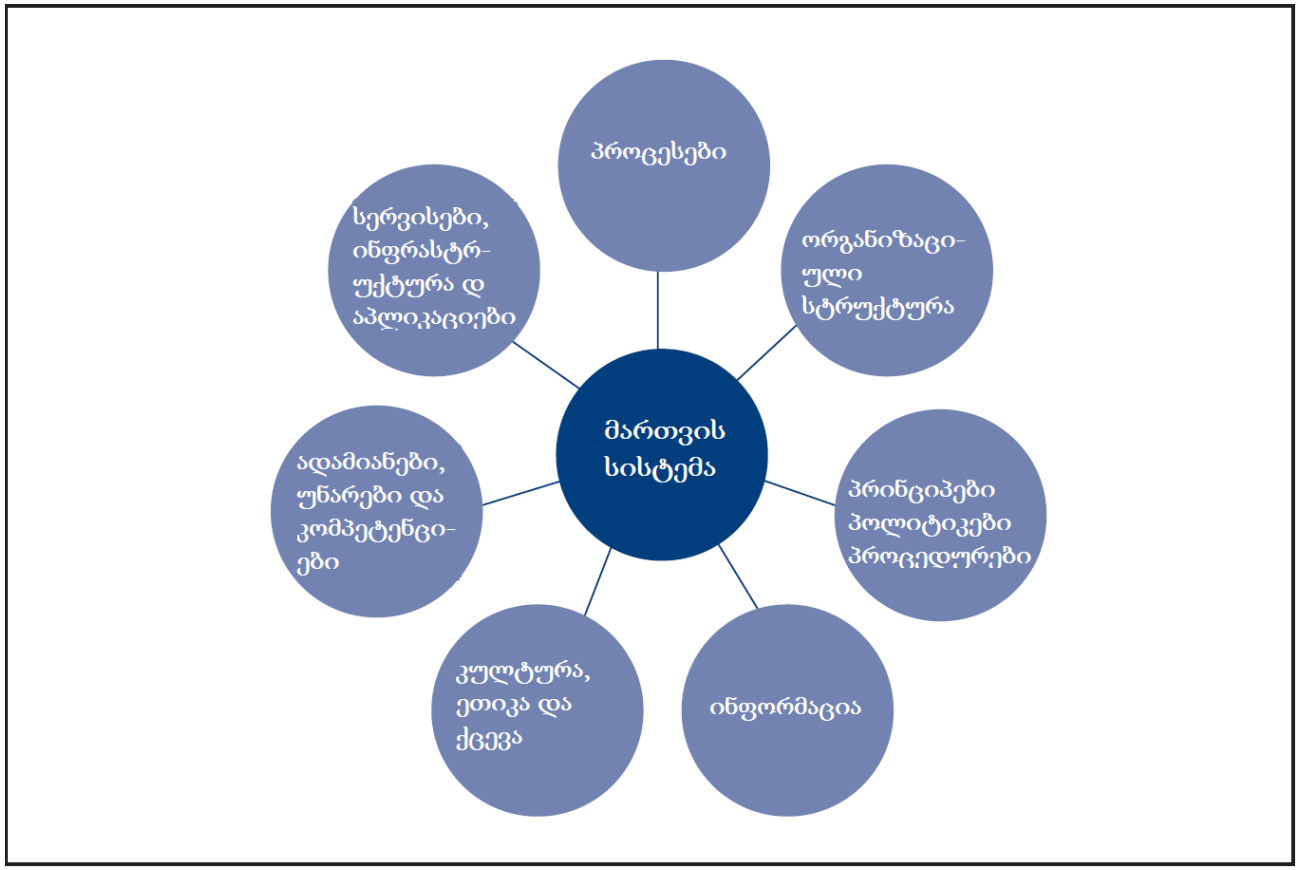
მართვის სისტემის კომპონენტები

იმისათვის, რომ მიაღწიოს მართვისა და მენეჯმენტის მიზნებს, თითოეულმა კორპორაციამ უნდა დააარსოს, მოარგოს და შეინარჩუნოს მრავალი კომპონენტისგან შემდგარი მართვის სისტემა.

- კომპონენტები არის ფაქტორები, რომლებიც ინდივიდუალურად და კოლექტიურად ხელს უწყობს კორპორაციის მართვის სისტემის კარგ ზემოქმედებას IT-ზე.
- კომპონენტები ურთიერთქმედებენ ერთმანეთთან, რის შედეგადაც ვიღებთ IT-ის მართვის ჰოლისტიკურ სისტემას.

- კომპონენტები შეიძლება იყოს სხვადასხვა სახის. ყველაზე ნაცნობი არის პროცესები. თუმცა, მართვის სისტემის კომპონენტები ასევე მოიცავს ორგანიზაციულ სტრუქტურებს; პოლიტიკასა და პროცედურებს; საინფორმაციო პუნქტებს; კულტურასა და ქცევას; უნარებსა და კომპეტენციებს; და სერვისებს, ინფრასტრუქტურასა და პროგრამულ უზრუნველყოფებს (სურათი 1.3).
- პროცესები აღწერენ გარკვეული მიზნების მისაღწევად დანერგილი პრაქტიკებისა და პროცესების ორგანიზებულ კომპლექტს. ასევე ქმნიან შედეგთა ერთობლიობას, რომლებიც ხელს უწყობენ სრულიად IT-სთან დაკავშირებული მიზნების მიღწევას.
- ორგანიზაციული სტრუქტურები არიან ძირითადი გადაწყვეტილების მიმღები პირები კორპორაციაში.
- პრინციპები, პოლიტიკა და მოდელები სასურველ ქცევას თარგმნიან პრაქტიკულ სახელმძღვანელოებად ყოველდღიური მენეჯმენტისთვის.
- ინფორმაცია არის მთლიანად გავრცელებული ნებისმიერ ორგანიზაციაში და მოიცავს ყველა ინფორმაციას, რომელიც წარმოშობილია და გამოყენებულია კორპორაციის მიერ. COBIT აქცენტს აკეთებს კორპორაციის მართვის სისტემის ეფექტური ფუნქციონირებისთვის საჭირო ინფორმაციაზე.
- პირთა და კორპორაციათა კულტურა, ეთიკა და ქცევა ხშირად არასწორად ფასდება, როგორც მართვისა და მენეჯმენტის აქტივობების წარმატების ფაქტორები.
- ადამიანები, უნარები და კომპეტენცია საჭიროა კარგი გადაწყვეტილების მისაღებად, სწორი მოქმედების გასაკეთებლად და ყველა აქტივობის წარმატებულად დასასრულებლად.
- სერვისები, ინფრასტრუქტურა და პროგრამები მოიცავს ინფრასტრუქტურას, ტექნოლოგიებს და პროგრამებს, რომლებიც კორპორაციას უზრუნველყოფენ მართვის სისტემით IT-ის პროცესებისათვის.

სურათი 1. 3 COBIT-ის მართვის სისტემის კომპონენტები



ყველა ტიპის კომპონენტები შეიძლება იყოს ზოგადი ან იყოს ზოგადი კომპონენტების ვარიანტები:

- ზოგადი კომპონენტები აღწერილია COBIT-ის ძირითად მოდელში (იხ. სურათი 1.2) და პრინციპში გამოიყენება ნებისმიერ სიტუაციაში. თუმცა, ისინი ბუნებით არიან ზოგადი კომპონენტები და ზოგადად პრაქტიკაში დანერგვამდე სჭირდებათ მოდიფიცირება.
- ვარიანტები დაფუძნებულნი არიან ზოგად კომპონენტებზე, მაგრამ მორგებულნი არიან კონკრეტულ მიზანს ან კონტექსტს სამიზნე არეალში (მაგ. ინფორმაციის უსაფრთხოებას, DevOps, კონკრეტულ რეგულაციას).

სამიზნე არეალი

სამიზნე არეალი აღწერს კონკრეტული მართვის თემას, დომენს ან საკითხს, რომელსაც შეიძლება განსაკუთრებული ყურადღება მიაქციოს მართვისა და მენეჯმენტის მიზნების ერთობლიობამ და მათმა კომპონენტებმა. სამიზნე არეალის მაგალითები აერთიანებს

მცირე და საშუალო ბიზნესებს, კიბერ-უსაფრთხოებას, ციფრულ ტრანსფორმაციას, მონაცემთა „ღრუბელში“ დამუშავებას (კომპიუტერის მოხმარებლისა და სერვერის ურთიერთობა, რომლის დროსაც კლიენტის ინფორმაცია მუშავდება და ინახება მოშორებულ სერვერზე, რაც საშუალებას იძლევა შემცირდეს მოხმარებლის აპარატურული და პროგრამული მოთხოვნები), კონფიდენციალურობას და DevOps (ანგარიშობს ორივეს, კომპონენტების ვარიანტებს და სამიზნე არეალსაც, რადგან DevOps არის მიმდინარე საკითხი მარკეტზე და აუცილებლად მოითხოვს სფეციფიკურ ხელმძღვანელობას, მის სამიზნე არეალად გადაქცევას. ის მოიცავს მრავალ ზოგად COBIT მოდელის მართვისა და მენეჯმენტის მიზნებს, განვითარების, ოპერატიულობის და კონტროლთან დაკავშირებული პროცესებისა და ორგანიზაციული სტრუქტურების ვარიანტებთან ერთად).

COBIT-ის მთავარი მოდელი არის ამ ნაშრომის ძირითადი საგანი და წარმოადგენს მართვის ზოგად კომპონენტებს. სამიზნე არეალი შეიძლება მოიცავდეს მართვის ზოგადი კომპონენტებისა და კონკრეტული კომპონენტების ვარიანტების კომბინაციას, რომელიც მორგებულია ამ სამიზნე არეალზე.

სამიზნე არეალი პრაქტიკულად შეუზღუდავია. ეს არის ის, რაც COBIT-ს ხდის ღიას. ახალი სამიზნე არეალი შესაძლოა დამატებულ იქნას საჭიროების შემთხვევაში ან იმის მიხედვით, თუ რა წვლილი შეაქვთ საგნის ექსპერტებსა და პრაქტიკოსებს COBIT-ის ღია მოდელში.

1.2. COBIT 2019-ის სტრუქტურა

COBIT 2019 წარმოადგენს მართვისა და მენეჯმენტის 40 ძირითად მიზანს (სურათი 1.2), მასში შემავალი პროცესების, სხვა დაკავშირებული კომპონენტების და დაკავშირებული სახელმძღვანელოების (როგორიცაა სხვა სტანდარტები და მოდელები) რეფერენსების სრულყოფილ აღწერას.

- დანამატები მოიცავს მეტ დეტალებს:
    1. ცხრილების შედარება, რომლებიც გვაუწყებენ მიზნების კასკადებს;
    2. ორგანიზაციული სტრუქტურების აღწერა;
    3. წყაროთა ცნობების სია

სამიზნე აუდიტორია

COBIT დაიწერა მთელი ორგანიზაციის ყველა პროფესიონალისთვის: ბიზნესის, აუდიტის, უსაფრთხოების, რისკების მართვის, IT და სხვა პრაქტიკოსების ჩათვლით, რომლებიც ისარგებლებენ დეტალური სახელმძღვანელოთი, COBIT-ის ძირითადი მოდელის მართვისა და მენეჯმენტის 40 მიზნის შესაბამისად.

მართვისა და მენეჯმენტის მიზნები

როგორც უკვე ავღნიშნე, COBIT 2019 მოიცავს მართვისა და მენეჯმენტის 40 მიზანს, რომელიც ორგანიზებულია 5 სფეროში (იხ. ცხრილი 1.1).

- მართვის დომენები
    1. შეფასება, მიმართვა და მონიტორინგი (EDM).
- მენეჯმენტის დომენები
    1. ჩამოწერა/განლაგება, დაგეგმვა და ორგანიზება (APO)
    2. აგება, შეძენა და დანერგვა (BAI)
    3. მიწოდება, მომსახურება და მხარდაჭერა (DSS)
    4. კონტროლი, შეფასება და გაზომვა (MEA)

მაღალი დონის დეტალური ინფორმაცია თითოეული მიზნისთვის (ცხრილი 1.1) მოიცავს:

- დომენის სახელს
- სამიზნე არეალს (COBIT 2019-ის შემთხვევაში, ეს არის მისი ძირითადი მოდელი)
- მართვისა და მენეჯმენტის მიზნის სახელს
- აღწერას
- მიზნის განსაზღვრებას

ცხრილი 1. 1 ***მართვისა და მენეჯმენტის მიზნები***

დომენი: <სახელი> მართვის/მენეჯმენტის მიზნები: <სახელი>	სამიზნე არეალი: <სახელი>
აღწერა	
<ტექსტი>	
მიზანი	
<ტექსტი>	

მიზნების კასკადი

მართვისა და მენეჯმენტის თითოეული მიზანი მხარს უჭერს ისეთი მიზნების თანხვედრის მიღწევას, რომლებიც დაკავშირებულნი არიან უფრო დიდ ორგანიზაციულ მიზნებთან.

მიზნების თანხვედრა, რასაც პირველადი კავშირი აქვს მართვისა და მენეჯმენტის მიზნებთან, ჩამოთვლილია მიზნების შემცველი დეტალური გზამკვლევის სექციაში მარჯვენა მხარეს (ცხრილი 1.2).

ცხრილი 1. 2 ***შესაბამისი კორპორაციის და განხილვის მიზნები***

მართვის/მენეჯმენტის მიზნები მხარს უჭერს მითითებული პირველადი კორპორაციებისა და თანხვედრის მიზნების მიღწევას:	
კორპორაციის მიზნები	**თანხვედრის მიზნები**
<კორპორაციის მიზნების რეფერენსები> <მიზნის აღწერა>	<თანხვედრის მიზნების რეფერენსები> <მიზნის აღწერა>

თანხვედრის მიზნები მოიცავს:

- AG01: IT-ის შესაბამისობასა და მხარდაჭერას ბიზნესის შესაბამისობისთვის კანონმდებლობასა და მარეგულირებლის მოთხოვნებთან
- AG02: IT-სთან დაკავშირებული მართვად რისკებს

- AG03: IT-ში განხორციელებული ინვესტიციებიდან და სერვისების პორტფოლიოდან მიღებულ სარგებელს
- AG04: ტექნოლოგიებთან დაკავშირებული ფინანსური ინფორმაციის ხარისხს
- AG05: IT სერვისების მიწოდებას ბიზნეს სერვისების შესაბამისად
- AG06: ბიზნესის მოთხოვნილებების ოპერაციულ გადაწყვეტილებებად გარდაქმნის სისწრაფეს
- AG07: ინფორმაციის უსაფრთხოებას, ინფრასტრუქტურის და აპლიკაციების დამუშავებასა და კონფიდენციალურობას
- AG08: აპლიკაციებისა და ტექნოლოგიების ინტეგრაციის მეშვეობით ბიზნეს პროცესების გააქტიურებას და მხარდაჭერას
- AG09: პროგრამების დროულად მიწოდებას ბიუჯეტის შესაბამისად და მოთხოვნილებებისა და ხარისხის სტანდარტების დაკმაყოფილებას
- AG10: IT მენეჯმენტის ინფორმაციის ხარისხს
- AG11: IT-ს შესაბამისობას შიდა პოლიტიკასთან
- AG12: ტექნოლოგიებისა და ბიზნესის კარგად მცოდნე კომპეტენტური და მოტივირებული პერსონალს
- AG13: ცოდნას, კვლევას და ინიციატივებს ბიზნეს ინოვაციებისთვის

ორგანიზაციული მიზნები მოიცავს:

- EG01: კონკურენტუნარიანი პროდუქტებისა და სერვისების პორტფოლიოს
- EG02: მართვად ბიზნეს რისკებს
- EG03: შესაბამისობას კანონმდებლობასა და რეგულაციებთან
- EG04: ფინანსური ინფორმაციის ხარისხს
- EG05: მომხმარებელზე ორიენტირებულ მომსახურების კულტურას
- EG06: ბიზნეს სერვისების უწყვეტობასა და ხელმისაწვდომობას
- EG07: მენეჯმენტის ინფორმაციის ხარისხს
- EG08: ბიზნეს პროცესების ფუნქციონირების ოპტიმიზაციას
- EG09: ბიზნეს პროცესების ხარჯების ოპტიმიზაციას

- EG10: პერსონალის უნარებს, მოტივაციასა და პროდუქტიულობას
- EG11: შიდა პოლიტიკასთან შესაბამისობას
- EG12: ციფრული ტრანსფორმაციის პროგრამების მართვას
- EG13: პროდუქტისა და ბიზნესის ინოვაციურობას

*ცხრილი 1. 3 **თანხვედრის მიზნებისა და მაგალითების მეტრიკები***

მართვის/მენეჯმენტის მიზნები მხარს უჭერს მითითებული პირველადი კორპორაციებისა და თანხვედრის მიზნების მიღწევას:	
კორპორაციის მიზნები	**თანხვედრის მიზნები**
<კორპორაციის მიზნების რეფერენსები> <მიზნის აღწერა>	<თანხვედრის მიზნების რეფერენსები> <მიზნის აღწერა>
კორპორაციის მიზნების მაგალითის მეტრიკები	**თანხვედრის მიზნების მაგალითის მეტრიკები**
<კორპორაციის მიზნების რეფერენსები> <მეტრიკები>	<თანხვედრის მიზნების რეფერენსები> <მეტრიკები>
<კორპორაციის მიზნების რეფერენსები> <მეტრიკები>	<თანხვედრის მიზნების რეფერენსები> <მეტრიკები>

1.3. COBIT 2019-ის კომპონენტები

პროცესები

თითოეული მართვისა და მენეჯმენტის მიზანი მოიცავს რამდენიმე პროცესის პრაქტიკას. თითოეული პროცესი შეიცავს ერთ ან მეტ აქტივობას. შეზღუდული რაოდენობის

მაგალითად აღებული საზომები თან ახლავს თითოეული პროცესის პრაქტიკას, რათა გაზომოს პრაქტიკის მიღწევები და მისი წვლილი მთლიანი მიზნების მიღწევაში (ცხრილი 1.4)

ცხრილი 1. 4 ***პროცესის გამოსახვა***

A. პროცესი

მართვის/მენეჯმენტის პრაქტიკა	**მაგალითად აღებული მეტრიკები**
<რეფერენსები> <სახელი> <აღწერა>	<მეტრიკები>

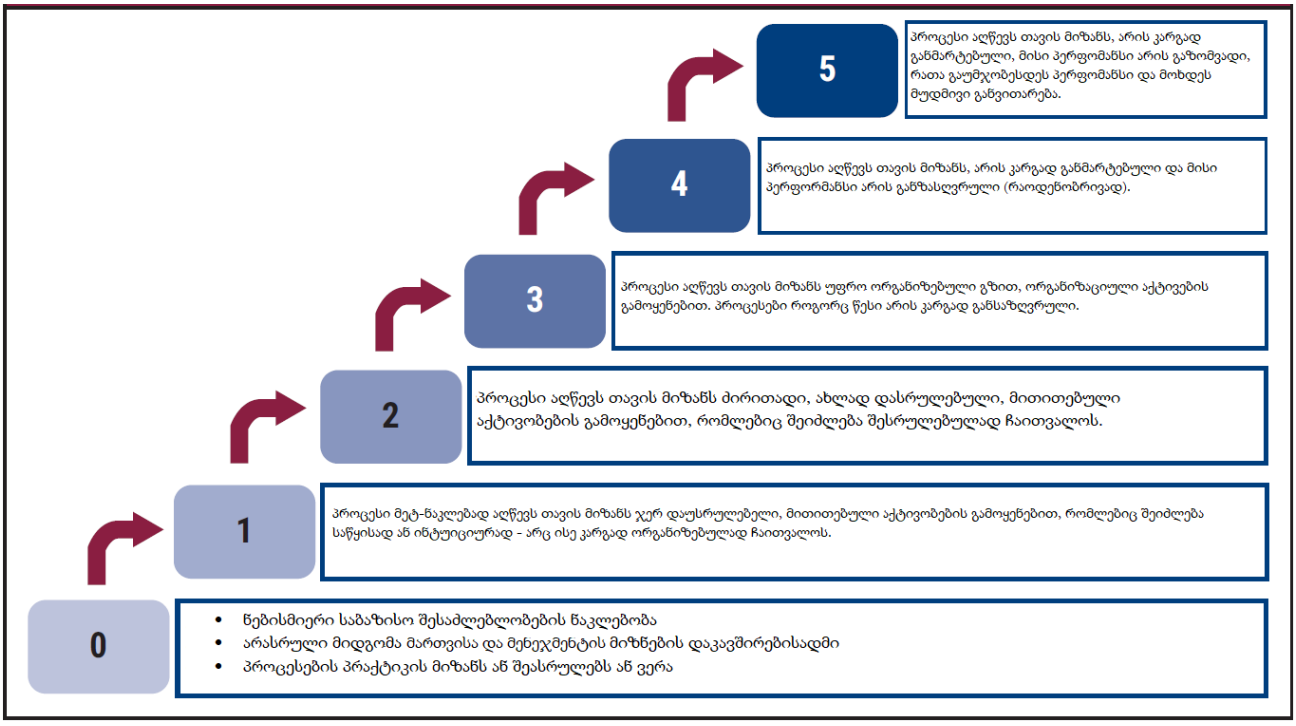
აქტივობები	**შესაძლებლობების დონე**
1. <ტექსტი>	<NR>
2. <ტექსტი>	<NR>
n. <ტექსტი>	<NR>

დაკავშირებული სახელმძღვანელო (სტანდარტები,მოდელები, შესაბამისობის მოთხოვნილებები)	**დეტალური რეფერენსი**
<სტანდარტული სახელი>	<ტექსტი>
<სტანდარტული სახელი>	<ტექსტი>

შესაძლებლობების დონე მინიჭებულია ყველა პროცესის აქტივობაზე, რაც სხვადასხვა შესაძლებლობების დონეზე პროცესების ზუსტი განმარტების საშუალებას იძლევა. პროცესი გარკვეული შესაძლებლობების დონეს აღწევს მაშინ, როცა ამ დონის ყველა აქტივობა წარმატებით სრულდება. COBIT 2019 მხარს უჭერს „შესაძლებლობების სიმწიფის მოდელის ინტეგრაციაზე“ (CMMI) დაყრდნობილ პროცესის სქემას, რომელიც

მერყეობს 0-დან 5-მდე. შესაძლებლობის დონე არის მეტრიკები იმისა, თუ რამდენად კარგად არის პროცესი დანერგილი და შესრულებული. სურათი 1.4 გამოსახავს მოდელს, ზრდადი შესაძლებლობების დონეს და მათ ზოგად მახასიათებლებს.

სურათი 1. 4 ***პროცესების შესაძლებლობების დონე***



ასევე, სხვა სტანდარტების რეფერენსები და სახელმძღვანელოები შეყვანილია ამ სექციაშიც (იხ. ცხრილი 1.4). დაკავშირებული სახელმძღვანელო ეხება ყველა სტანდარტს, მოდელს, შესაბამისობის მოთხოვნილებასა და სხვა ყველა გზამკვლევს, რომლებიც შეესაბამება მოცემულ პროცესს. დეტალური რეფერენსის არეალი დაკავშირებულ სახელმძღვანელოში გადმოგვცემს კონკრეტულ თავებს ან სექციებს.

თუ რომელიმე კონკრეტული კომპონენტისთვის არ არის განსაზღვრული სახელმძღვანელოს რეფერენსი, ესეიგი შესაბამისი რეფერენსები არ არის ცნობილი. პრაქტიკოს საზოგადოებას თავისუფლად შეუძლია დაკავშირებული სახელმძღვანელოების შემოთავაზება.

ორგანიზაციული სტრუქტურები

ორგანიზაციული სტრუქტურების მართვის კომპონენტები გვთავაზობენ პასუხისმგებლობისა და პროცესის პრაქტიკის ანგარიშვალდებულების დონეებს (ცხრილი 1.5). ჩარტებს აქვთ ინდივიუალური როლები, ისევე როგორც ორგანიზაციულ სტრუქტურებს, ბიზნესშიც და IT-შიც.

ცხრილი 1. 5 ***ორგანიზაციული სტრუქტურა***

B. ორგანიზაციული სტრუქტურები

ძირითადი მართვის/მენეჯმენტის პრაქტიკა	ორგანიზაციული სტრუქტურა 1	ორგანიზაციული სტრუქტურა 2	ორგანიზაციული სტრუქტურა 3	ორგანიზაციული სტრუქტურა 4	ორგანიზაციული სტრუქტურა 5	ორგანიზაციული სტრუქტურა 6	ორგანიზაციული სტრუქტურა 7	ორგანიზაციული სტრუქტურა 8 და ა.შ
<რეფერენსი> <სახელი>								

დაკავშირებული სახელმძღვანელო (სტანდარტები, მოდელები, შესაბამისობის მოთხოვნილებები)	დეტალური რეფერენსი
<სტანდარტული სახელი>	<ტექსტი>
<სტანდარტული სახელი>	<ტექსტი>

შემდეგი როლები და ორგანიზაციული სტრუქტურები განმარტებულია COBIT 2019-ის კონტექსტში:

- საბჭო
- აღმასრულებელი კომიტეტი
- აღმასრულებელი დირექტორი
- მთავარი ფინანსური ოფიცერი
- მთავარი ოპერაციული ოფიცერი
- მთავარი რისკების ოფიცერი
- მთავარი საინფორმაციო ოფიცერი
- მთავარი ტექნოლოგიების ოფიცერი
- მთავარი ციფრული ოფიცერი
- IT მართვის საბჭო
- არქიტექტურის საბჭო
- კორპორაციული რისკების კომიტეტი
- ინფორმაციული უსაფრთხოების მთავარი ოფიცერი
- ბიზნეს პროცესების მართვა
- პორტფელის მენეჯერი
- პროგრამების/პროექტების მართვის კომიტეტი
- პროგრამული მენეჯერი
- პროექტის მენეჯერი
- პროექტის მართვის ოფისი
- მონაცემთა მართვის ფუნქცია
- ადამიანური რესურსების ხელმძღვანელი
- ურთიერთობის მენეჯერი
- ხელმძღვანელი არქიტექტორი
- განვითარების ხელმძღვანელი
- IT ოპერაციების ხელმძღვანელი

- IT ადმინისტრაციის ხელმძღვანელი
- სერვის მენეჯერი
- ინფორმაციული უსაფრთხოების მენეჯერი
- ბიზნესის უწყვეტობის მენეჯერი
- კონფიდენციალურობის ოფიცერი
- იურიდიული მრჩეველი
- აუდიტი

სტრუქტურების ჩართულობის სხვადასხვა დონეები შეიძლება დაყოფილ იქნას პასუხისმგებელ და ანგარიშვალდებულ დონეებად.

- პასუხისმგებელი (R) როლები არიან მთავარი ოპერაციული მხარეები პრაქტიკების შესრულებასა და განზრახული შედეგების მიღწევაში. ვინ ასრულებს დავალებას? ვინ წარმართავს დავალებას?
- ანგარიშვალდებული (A) როლები კისრულებენ მთლიან ანგარიშვალდებულებას. პრინციპულად, ანგარიშვალდებულების განაწილება არ შეიძლება. ვინ არის ანგარიშვალდებული წარმატების მიღწევასა და დავალების შესრულებაზე?

თითოეული სფერო აღწერს ორგანიზაციულ სტრუქტურას, რომელსაც აკისრია პასუხისმგებლობა და/ან ანგარიშვალდებულება ამ სფეროს მიმართ. გზამკვლევში შესულია თითოეული როლისა და ორგანიზაციული სტრუქტურის დეტალური აღწერა. სხვა ორგანიზაციული სტრუქტურები პასუხისმგებლობის ან ანგარიშვალდებულების აღების გარეშე გამოტოვებულ იქნა, რათა გააუმჯობესონ ჩარტის წაკითხვის უნარიანობა.

პრაქტიკოსებს ჩარტების დასრულება შეუძლიათ ორი, როლებისა და ორგანიზაციული სტრუქტურის ჩართულობის დონით. ვინაიდან კონსულტირებული და ინფორმირებული როლების მინიჭება დამოკიდებულია ორგანიზაციულ კონტექსტსა და პრიორიტეტებზე, ისინი არ არიან შესულები ამ დეტალურ გზამკვლევში.

- კონსულტირებული (C) როლები არიან ინფორმაციის პრაქტიკის წარმომადგენლები. ვინ აწვდის მათ ინფორმაციას?
- ინფორმირებული (I) როლები ინფორმირებულნი არიან პრაქტიკის მიღწევებისა და/ან შედეგების შესახებ.

კორპორაციებმა ჩარტში უნდა მიმოიხილონ პასუხისმგებლობისა და ანგარიშვალდებულების, კონსულტირებული და ინფორმირებული როლებისა და ორგანიზაციული სტრუქტურების დონეები, კორპორაციის კონეტქსტის, პრიორიტეტებისა და სასურველი ტერმინოლოგიის მიხედვით.

შესაბამისად, სხვა სტანდარტებისა და დამატებითი სახელმძღვანელოს რეფერენსები შეყვანილია ორგანიზაციული სტრუქტურის კომპონენტების სექციაში. დაკავშირებული სახელმძღვანელო ეხება ყველა სტანდარტს, მოდელს, შესაბამისობის მოთხოვნილებებსა და სხვა სახელმძღვანელოებს, რომლებიც შეესაბამება მოცემულ ორგანიზაციულ სტრუქტურებსა და მათი პროცესებში ჩართულობის დონეებს.

ინფორმაციის დინება და ობიექტები

მართვის შემდეგი კომპონენტი წარმოადგენს სახელმძღვანელოს, ინფორმაციების დინებასა და ობიექტებზე, რომლებიც დაკავშირებულია პროცესთა პრაქტიკებთან. თითოეული პრაქტიკა მოიცავს შენატანს/საწყის წვლილსა და შედეგებს, წარმოშობისა და დანიშნულების მითითებით.

ზოგადად, თითოეული შედეგი იგზავნება ერთი ან გარკვეული რაოდენობის დანიშნულებისკენ, როგორც წესი COBIT-ის პროცესის პრაქტიკისკენ. ეს შედეგი შემდეგ ხდება მიმართულებისკენ მიმავალი საშუალება (ცხრილი 1.6).

ცხრილი 1. 6 ***ინფორმაციის დინებისა და ობიექტები***

C. კომონენტი: ინფორმაციის დინება და ობიექტები

მარვთვის/მენეჯმენტის პრაქტიკა	შენატანი/საწყისი წვლილი		შედეგები	
<რეფერენსები> <სახელი>	-დან	აღწერა	აღწერა	-მდე
	<რეფერენსები>	<ტექსტი>	<ტექსტი>	<რეფერენსები>

დაკავშირებული სახელმძღვანელო (სტანდარტები, მოდელები, შესაბამისობის მოთხოვნილებები)	დეტალური რეფერენსი
<სტანდარტული სახელი>	<ტექსტი>
<სტანდარტული სახელი>	<ტექსტი>

მრავალ შედეგს მაინც აქვს ბევრი დანიშნულება (მაგალითად COBIT-ის ყველა პროცესი ან ყველა პროცესი დომენის ფარგლებში). ეს შედეგები სამიზნე პროცესებში, შეტანილ/საწყის წვლილად არ არის ჩამოთვლილი, წაკითხვის სიმარტივის გამო. ასეთი შედეგების სრული სია იხილეთ ცხრილი 1.7-ში.

ზოგიერთი შენატანის/შედეგის," შიგთავსი" გადმოცემულია როგორც დანიშნულება, თუ ისინი დაყოფილია იგივე პროცესის აქტივობებში.

ცხრილი 1. 7 ***მრავალჯერადი პროცესების შედეგები***

ყველა პროცესის შედეგი		
ძირითადი პრაქტიკიდან	**შედეგის აღწერა**	**დანიშნულება**
APO 13.02	ინფორმაციის უსაფრთხოების რისკების მოგვარების გეგმა	ყველა EDM , ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA

მართვის პრაქტიკიდან	შედეგის აღწერა	დანიშნულება
EDM 1.01	კორპორაციის მართვის სახელმძღვანელო პრინციპები	ყველა EDM
EDM 1.01	გადაწყვეტილების მიღების მოდელი	ყველა EDM
EDM 1.02	კორპორაციის მართვის კომუნიკაცია	ყველა EDM
EDM 1.01	უფლებამოსილების დონეები	ყველა EDM
EDM1.03	პასუხი მართვის ეფექტურობასა და შესრულებაზე	ყველა EDM

მენეჯმენტის ყველა პროცესის შედეგი

მენეჯმენტის პრაქტიკიდან	შედეგის აღწერა	დანიშნულება
APO 1.01	მართვის სისტემის ფორმა	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
APO 1.01	პრიორიტეტული მართვისა და მენეჯმენტის მიზნები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
APO 1.02	IT მიზნების კომუნიკაცია	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
APO 1.02	კომუნიკაციის ადგილობრივი წესები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
APO 1.03	სამიზნე მოდელის ხარვეზების ანალიზი	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
APO 1.11	პროცესის განვითარების შესაძლებლობები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA

APO 2.05	IT სტრატეგია და მიზნები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
APO 2.06	კომუნიკაციის შეფუთვა	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
APO 11.03	ხარისხის მართვის სტანდარტები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
APO 11.04	სერვისის მიზნების და პროცესის ხარისხი და მეტრიკები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
APO 11.05	უწყვეტი განვითარებისა და საუკეთესო პრაქტიკების კომუნიკაცია	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
APO 11.05	კარგი პრაქტიკის მაგალითების გაზიარება	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
APO 11.05	ხარისხის მიმოხილვის საორიენტაციო შედეგები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 01.02	მონიტორინგის მიზნები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 01.04	პერფორმანსის ანგარიშები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 01.05	მაკორექტირებელი აქტივობები და დავალებები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 02.01	შიდა კონტროლის მონიტორინგის და ანგარიშების შედეგები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 02.01	ბენჩმარკინგის და სხვა შეფასებების შედეგები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA

MEA 02.03	თვითშეფასების მიმოხილვის შედეგები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 02.03	თვითშეფასების გეგმები და კრიტერიუმები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 02.04	კონტროლის ხარვეზები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 02.04	მაკორექტირებელი ქმედებები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 03.02	შეცვლილ მოთხოვებთან შესაბამისობების კომუნიკაციები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 04.02	გარანტიის გეგმები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 04.08	გარანტიის მიმოხილვის ანგარიში	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 04.08	გარანტიის მიმოხილვის შედეგები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA
MEA 04.09	მაკორექტირებელი ქმედებები	ყველა APO, ყველა BAI, ყველა DSS, ყველა MEA

შესაბამისად, სხვა სტანდარტებისა და დამატებითი სახელმძღვანელოს რეფერენსები შესულია ინფორმაციის დინებასა და ობიექტების კომპონენტში. დაკავშირებული სახელმძღვანელო ეხება ყველა სტანდარტს, მოდელს, შესაბამისობის მოთხოვნილებებს და სხვა სახელმძღვანელოს, რომელიც შეესაბამება მოცემული ინფორმაციის ელემენტებს.

ადამიანები, უნარები და კომპეტენციები

ადამიანების, უნარების და კომპეტენციების მართვის კომპონენტი განსაზღვრავს ადამიანურ რესურსებსა და უნარებს, რომლებიც მოითხოვება მართვისა და მენეჯმენტის მიზნების მისაღწევად. COBIT 2019-მა ეს სახელმძღვანელო დააფუძნა ინფორმაციული და საკომუნიკაციო ტექნოლოგიების (ICT), პროგრამული უზრუნველყოფის ინჟინერიისა და ციფრული ტრანსფორმაციის სფეროში მომუშავე პროფესიონალების უნარებისა და კომპეტენციების აღწერისა და მართვის მოდელზე (SFIA) (მე-6 ვერსია, 2015). ყველა ჩამოთვლილი უნარი დეტალურად აღწერილია SFIA მოდელში. დეტალური რეკომენდაციები წარმოადგენს უნიკალურ კოდს, რომელიც მორგებულია SFIA-ს სახელმძღვანელოს უნარებზე (ცხრილი 1.8).

ცხრილი 1. 8 ***ადამიანების, უნარებისა და კომოეტენციები***

D. ადამიანები, უნარები და კომპეტენციები		
უნარები	**დაკავშირებული სახელმძღვანელო (სტანდარტები, მოდელები, შესაბამისობის მოთხოვნილებები)**	**დეტალური რეფერენსები**
<სახელი>	SFIA v6, 2015	< SFIA-ს კოდი>
<სახელი>	SFIA v6, 2015	<SFIA-ს კოდი>

პოლიტიკა და პროცედურები

ეს კომპონენტი წარმოადგენს დეტალურ სახელმძღვანელოს პოლიტიკისა და პროცედურების შესახებ, რომლებიც მართვის ან მენეჯმენტის მიზნების შესაბამისია. შესაფერისი პოლიტიკისა და პროცედურების სახელი მოცემულია პოლიტიკის მიზნისა და შინაარსის აღწერით (ცხრილი 1.9).

სადაც საჭიროა,ყველგან შეყვანილია სხვა სტანდარტებისა და დამატებითი სახელმძღვანელოს რეკომენდაციები.დეტალური რეკომენდაციის არეალი გადმოგვცემს კონკრეტულ თავებს ან სექციებს შესაბამის სახელმძღვანელოში, სადაც მეტი ინფორმაცია შეიძლება იყოს მოცემული. წყაროთა სრული სია მოცემულია დანართ C-ში.

ცხრილი 1. 9 ***ადამიანების, უნარებისა და კომოეტენციები***

E. პოლიტიკა და პროცედურები			
შესაბამისი პოლიტიკა	**პოლიტიკის აღწერა**	**დაკავშირებული სახელმძღვანელო**	**დეტალური რეფერენსები**
<სახელი>	<აღწერა>	<სტანდარტული სახელი>	<ტექსტი>

კულტურა, ეთიკა და ქცევა

მართვის კომპონენტი კულტურის, ეთიკისა და ქცევის შესახებ წარმოადგენს დეტალურ სახელმძღვანელოს ორგანიზაციაში შემავალ სასურველ კულტურულ ელემენტებზე, რომლებიც მხარს უჭერენ მართვისა და მენეჯმენტის მიზნების მიღწევებს (ცხრილი 1.10). სხვა სტანდარტებისა და დამატებითი სახელმძღვანელოს რეკომენდაციები შეყვანილია ყველგან სადაც საჭიროა. დეტალური რეკომენდაციის არეალი გადმოგვცემს კონკრეტულ თავებს ან სექციებს შესაბამის სახელმძღვანელოში, სადაც მეტი ინფორმაცია შეიძლება იყოს მოცემული.

ცხრილი 1. 10 ***ადამიანების, უნარებისა და კომოეტენციები***

F. პოლიტკა და პროცედურები		
ძირითადი კულტურის ელემენტები	**დაკავშირებული სახელმძღვანელო**	**დეტალური რეფერენსები**
<სახელი>	<სტანდარტული სახელი>	<ტექსტი>

სერვისები, ინფრასტრუქტურა და აპლიკაციები

სერვისების, ინფრსატრუქტურისა და აპლიკაციების მართვის კომპონენტი წარმოადგენს დეტალურ სახელმძღვანელოს მესამე მხარის სერვისებზე, ინფრასტრუქტურის სახეობებზე და აპლიკანტების კატეგორიებზე, რომლებიც შეიძლება მიმართულ იქნეს მართვის ან მენეჯმენტის მიზნების მიღწევის მხარდასაჭერად. სახელმძღვანელო არის ზოგადი (რათა თავი აარიდოს კონკრეტული ვენდორებისა და პროდუქტების დასახელებას); თუმცა, ჩანაწერები მიმართულებას აძლევს ორგანიზაციებს, რათა შექმნან თავიანთი IT მართვის სისტემა (ცხრილი 1.11). (ISACA 2018, 9-25)

ცხრილი 1. 11 ***ადამიანების, უნარებისა და კომპეტენციები***

G. სერვისები, ინფრასტრუქტურა და აპლიკაციები
<სერვისების, ინფრასტრუქტურის ან აპლიკაციების კატეგორია>

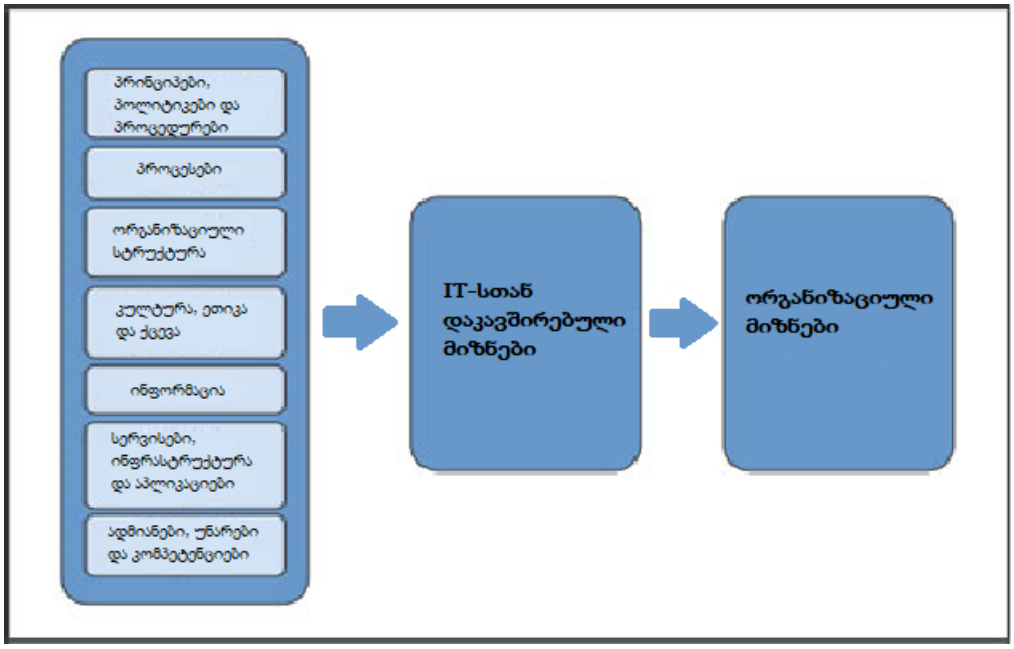
თავი 2. კომპანიის ინფორმაციული სისტემების რისკების ანალიზისა და მართვის უახლესი საშუალებები მსოფლიოში

2.1. ინფორმაციული ტექნოლოგიების კორპორატიული მართვის მდგომარეობა და ზეგავლენა ორგანიზაციებში

უკანასკნელი ორი ათწლეულის განმავლობაში, ორგანიზაციული რისკების მართვასა და ღირებულებების შექმნაში ინფორმაციული სისტემების ცენტრალიზების გათვალისწინებით, IT მართვის კონცეფცია იკავებს მნიშვნელოვან ადგილს მრავალი ორგანიზაციის დღის წესრიგში (Van Grembergen, W.; S. De Haes, 2008, 1-6). კომპანიები სულ უფრო მეტ ინვესტიციას ახორციელებენ კორპორაციული ინფორმაციული სისტემების მართვაში და ხშირად იყენებენ ისეთ საზოგადოდ მიღებულ და აღიარებულ ჩარჩოებსა და საუკეთესო პრაქტიკებს, როგორიც არის COBIT (S. De Haes; A. Joshi; Van Grembergen, W, 2015).

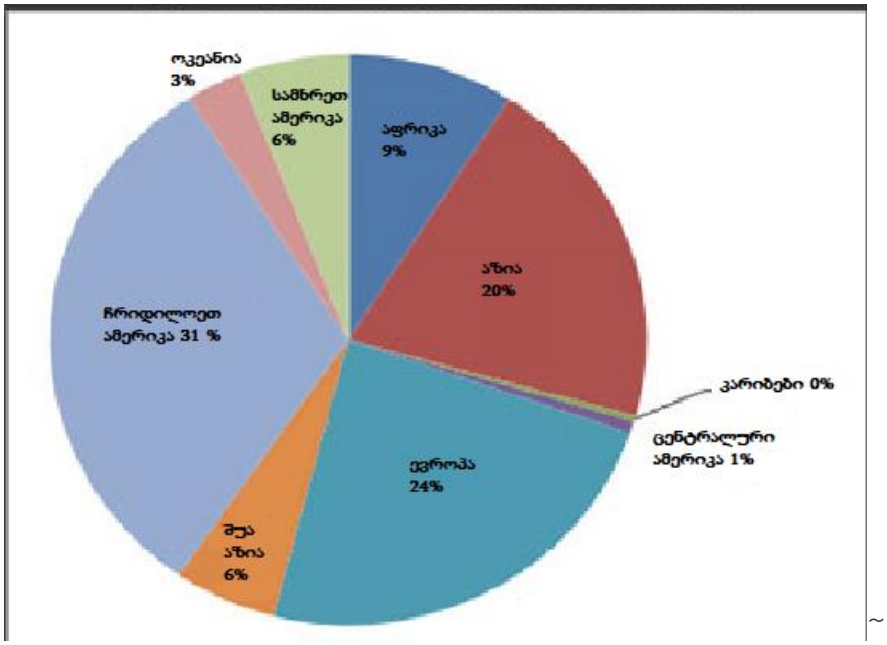
ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ შეკვეთილი საერთაშორისო კვლევა, რომელიც განახორციელა ანტვერპის უნივერსისტეტმა - ანტვერპის მენეჯმენტის სკოლამ, შეისწავლის როგორ ნერგავენ ორგანიზაციები კოროპრაციული ინფორმაციული სისტემების მართვას COBIT 5-ის გამოყენებით და მოაქვს თუ არა ამ ქმედებას კორპორაციული ღირებულებების შექმნა ამ ორგანიზაციისთვის. კ ვლევა გვაწვდის ინფორმაციას COBIT 5-ის შვიდი კომპონენტის ბენჩმარკინგის შესაბამისად და აღწერს სხვადასხვა ორგანიზაციებში COBIT-ის დანერგვის დონეს და შვიდი კომპონენტის დადებით კავშირს კომპანიის IT-სთან დაკავშირებული მიზნების მიღწევასთან მიმართებაში, რაც თავის მხრივ დაკავშირებულია ორგანიზაციის მიზნებთან (იხ. სურათი 2.1). ცხრილი 1-ში მოცემული მოდელი წარმოადგენს კვლევის ძირითად კონცეპტუალურ მოდელს.

სურათი 2. 1 ***COBIT 5 მიზნების კასკადი***



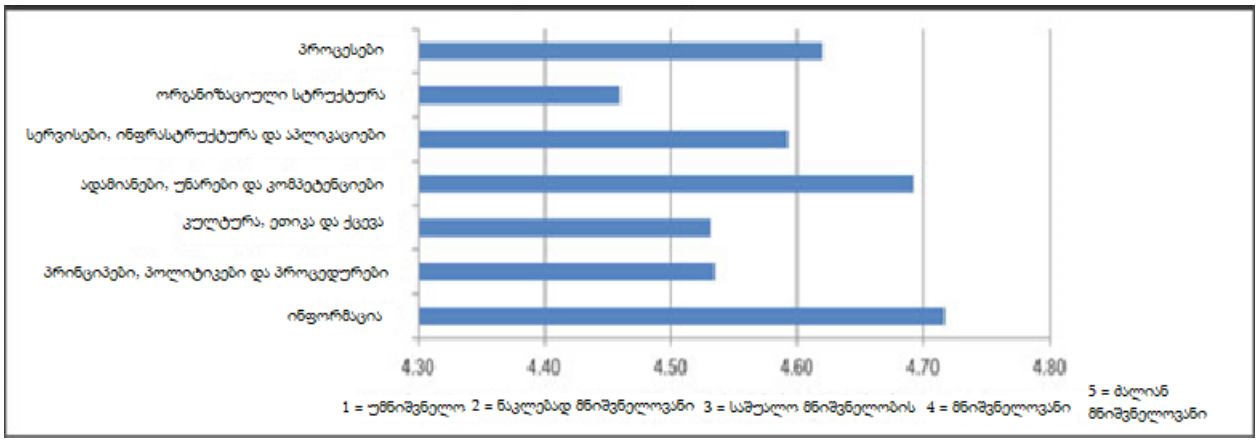
ანტვერპის მენეჯმენტის სკოლის მიერ შესრულებული კვლევა განხორციელდა ონლაინ გამოკითხვის საფუძველზე. ბიზნეს, IT და აუდიტის მენეჯერები სხვადასხვა ინდუსტრიებიდან იყვნენ მოწვეულნი, რათა მონაწილეობა მიეღოთ ონლაინ გამოიკითხვაში. კითხვარი აწყობილი იყო ისე, რომ შეეფასებინა COBIT-ის კომპონენტები სხვადასხვა მიმართულებით (მნიშვნელობა, მენეჯმენტი/დანერგვის სტატუსი, დანერგვის სიმარტივე, წვლილი) და ორგანიზაციების პროგრესირება IT-სთან დაკავშირებული მიზნებისა და ორგანიზაციული მიზნების მიღწევასთან ერთად. საბოლოო კვლევა ჩატარდა 2014 წლის 24 ივლისიდან 1 სექტემბრამდე. კითხვარი შეავსო 896-მა რესპოდენტმა მსოფლიოს მასშტაბით (იხ. სურათი 2.2).

სურათი 2. 2 ***რესპოდენტების პროფილი კონტინენტების დონეზე***



კვლევის შედეგებიდან გამომდინარე შესაძლებელია ითქვას, რომ კობიტის 7 კომპონენტიდან ყველაზე მნიშვნელოვანი კომპონენტები არის ინფორმაცია; ადმიანები, უნარები და კომპეტენციები; პროცესები (იხ. სურათი 2.3).

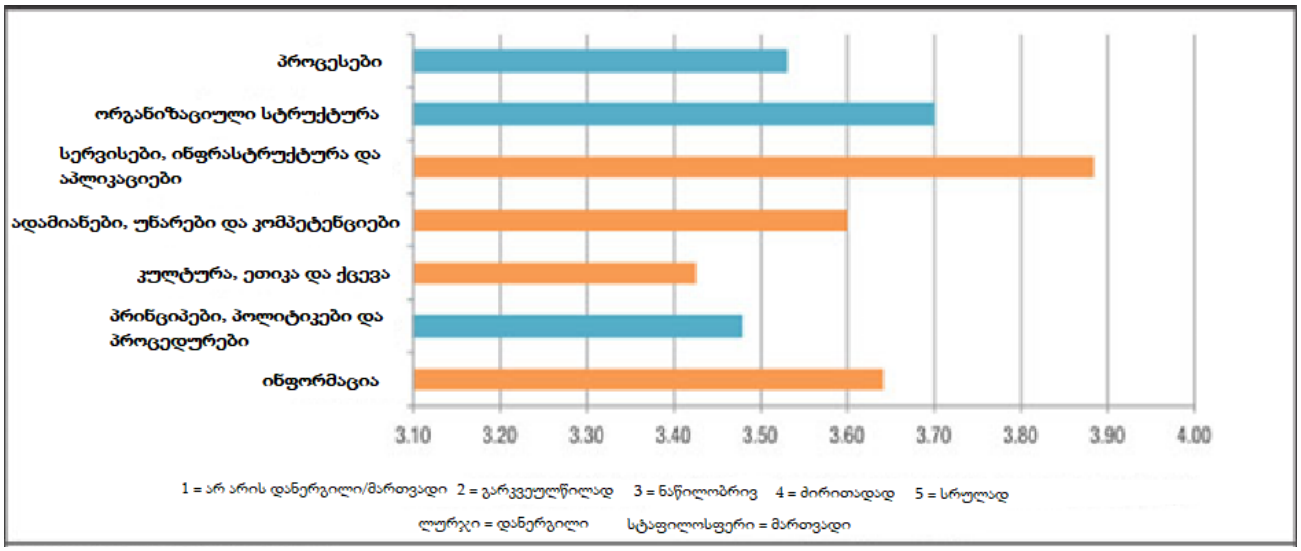
სურათი 2. 3 ***კომპონენტების მნიშვნელობა***



რესპოდენტებმა ასევე უპასუხეს კითხვაზე თუ როგორი იყო COBIT 5-ის კომპონენტების დანერგვის ან მენეჯმენტის სტატუსი, რის საფუძველზეც გამოვლინდა, რომ ყველაზე კარგად დანერგილი კომპონენტები არის სერვისები, ინფრასტრუქტურა და

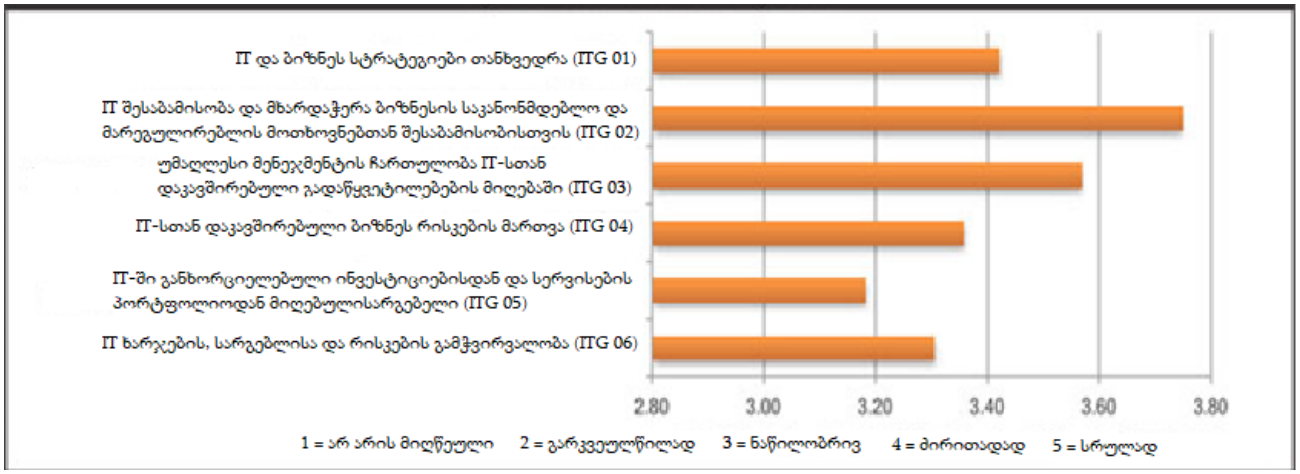
აპლიკაციები; ინფორმაცია. ხოლო ყველაზე მაღალი მენეჯმენტის სტატუსი აქვს ორგანიზაციულ სტრუქტურას (იხ. სურათი 2.4).

სურათი 2. 4 ***დანერგვის/მენეჯმენტის დონე***



კვლევა ასევე მოიცავდა სიღრმისეულ ანალიზს, სადაც აქცენტი გაკეთდა პროცესებზე. რესპოდენტებმა შეაფასეს COBIT 5-ის 37 პროცესის დანერგვის სტატუსი 5 ბალიანი სისტემით. სურათი 2.5 გვაჩვენებს დომენის დონის ქულებს. საშუალო ქულა თითოეული დომენისთვის არის 3-ზე მაღალი, რაც გულისხმობს, რომ გამოკითხვაში მონაწილე ორგანიზაციებს აქვთ საშუალო, „ნაწილობრივ“ დანერგილი პროცესები. სურათი 2.5 ასევე წარმოაჩენს, რომ მიწოდების, სერვისისა და მხარდაჭირს (DSS) დომენის პროცესების, რომლებიც არის ოპერაციული და მხარდაჭერის პროცესების რეალური აღსრულების ტიპი, დანერგვის სტატუსი უფრო მაღალია სხვა დომენებთან შედარებით.

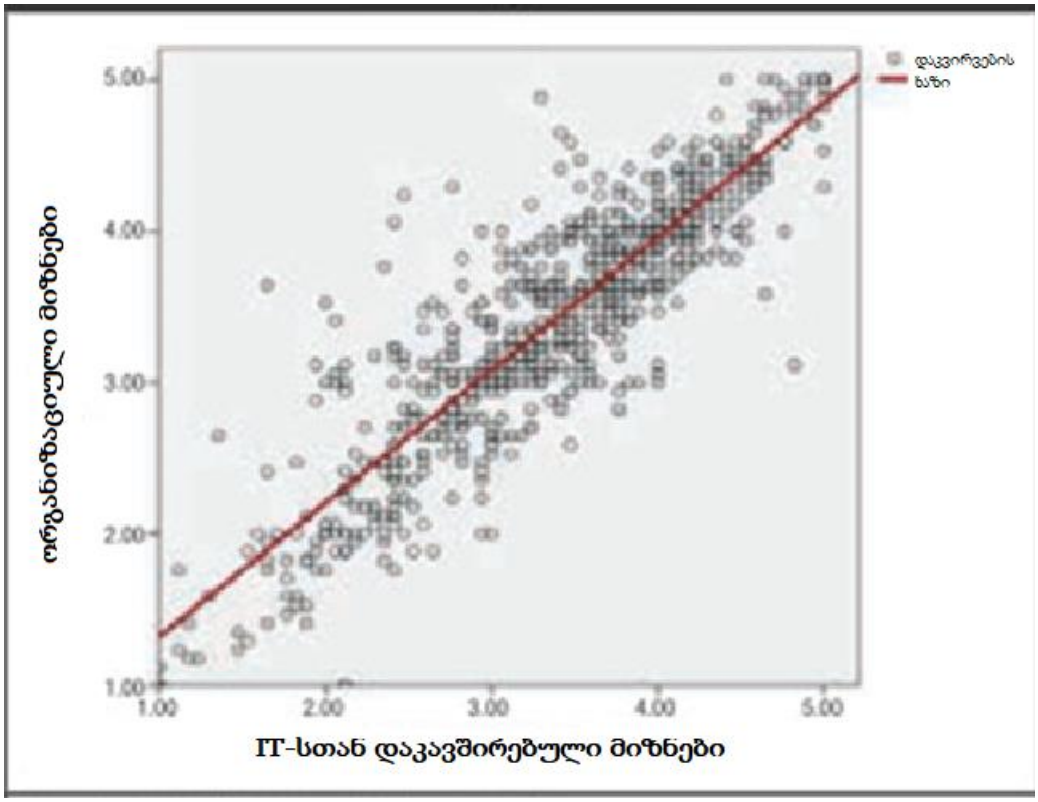
სურათი 2. 5 ***სრული პროცესის საშუალო შეფასება***



რესპოდენტებმა აღნიშნეს რომ შეფასების, მართვისა და მონიტორინგის (EDM) დომენის დანერგვის სტატუსი უფრო დაბალია დანარჩენ დომენებთან შედარებით. აღნიშნული ფაქტი შეიძლება აიხსნას იმით, რომ ეს პროცესი მოითხოვს მაღალი დონის აღმასრულებელი და არაღმასრულებელი საბჭოების ჩართულობას. ამგვარად, ეს შედეგები არის გამოწვევა საბჭოების წევრებისთვის.

საბოლოო ჯამში წინამდებარე კვლევა ადასტურებს ძლიერ პოზიტიურ დამოკიდებულებას IT-სთან დაკავშირებულ მიზნებსა და ზოგადი ორგანიზაციული მიზნების მიღწევას შორის, რაც გულისხმობს, რომ IT-სთან დაკავშირებული პროცესების შედეგები პოზიტიურ კავშირშია ორგანიზაციის ზოგად მიზნებთან (იხ. სურათ 2.6).

სურათი 2. 6 ***კავშირი IT-სთან დაკავშირებული მიზნებსა და ორგანიზაციული მიზნებს შორის***



გრაფიკში არსებული ხაზი გულისხმობს პოზიტიურ კორელაციას ორგანიზაციის მიზნებსა და IT მიზნებს შორის.

ანტვერპის მენეჯმენტის სკოლის მიერ განხორციელებული კვლევის შედეგებიდან გამომდინარე შესაძლებელია ითქვას, რომ პროფესიონალები იაზრებენ და აღიარებენ COBIT-ის მიერ შემოთავაზებულ შესაძლებლობებს კორპორაციული ინფორმაციული

სისტემების მართვის საუკეთესო საშუალებად. COBIT-ის თითოეული კომპონენტი არის ძალიან მნიშვნელოვანი და მათი დანერგვის სტატუსის მაღალი მაჩვენებელი ნათლად გამოხატავს დადებით კორელაციას IT-სთან დაკავშირებული მიზნების მიღწევისას. შედეგები ასევე წარმოაჩენს, რომ IT-სთან დაკავშირებული მიზნების მიღწევა ძლიერ კავშირშია ორგანიზაციული მიზნების მიღწევასთან, რაც ადასტურებს COBIT-ში შემოთავაზებულ კონცეპტუალურ კასკადურ მოდელს.

2.2. IT მართვა და ბიზნეს/IT თანხვედრა მცირე და საშუალო საწარმოებში

IT მართვასთან დაკავშირებული უამრავი პროექტი იყო ინიცირებული სხვადასხვა კომპანიებსა და სახელმწიფო ინსტუტციებში, რათა მიეღწიათ უკეთეს თანხვედრას ორგანიზაციის მიზნებსა და IT-ის შორის და მიეღოთ უმაღლესი მენეჯმენტის აუცილებელი ჩართულობა ღირებულებების შექმნაში IT-ში განხორციელებული ინვესტიციების შედეგად. ფინანსურ სექტორში არსებული კომპანიები, რომლებმაც მიაღწიეს ბიზნესისა და IT-ის მაღალი ხარისხის თანხვედრას, როგორც წესი იყენებენ IT მართვის პრაქტიკებს (Van Grembergen, W.; S. De Haes, 2010).

IT მართვის ჩარჩო განისაზღვრება, როგორც ერთერთი აუცილებელი პირობა ბიზნესისა და IT-ის თანხვედრის უმაღლესი დონის მისაღწევად (Weill, P.; J. W. Ross, 2004). პიტერ ვეილისა და ჯეინი ვენზელ როსის წიგნი დაფუძნებულია ორ ძირითად კვლევასა და მრავალ მასთან დაკავშირებულ პროექტზე. მათი უახლესი კვლევა მოიცავს 256 ორგანიზაციის გამოკითხვას ამერიკის, ევროპისა და აზიის ქვეყნებიდან, რომელიც ჩაატარა პიტერ ვეილმა 2001-დან 2003-წლამდე. ეს საქმიანობა ასევე მოიცავს 32 რეალური საქმიანობის სრულად შესწავლას. მეორე კვლევა არის 40 რეალური საქმიანობის ანალიზი, რომელიც შეიმუშავა ჯეინი როსმა 1999-2003 წლებში და ძირითადი აქცენტები კეთდებოდა ინფორმაციული სისტემების არქიტექტურასა და ბიზნეს სტრატეგიას შორის არსებულ კავშირებზე.

არ იყო ცნობილი ზემოთხსენებული აღმოჩენები ვრცელდებოდა თუ არა მცირე და საშუალო ორგანიზაციებზე (SME). სტივენ დე ჰაესის, როგიერ ჰაესთის და უიმ ვან გრემბერგერის კვლევა ფოკუსირდება ჰოლანდიაში არსებულ SME სეგმენტში შემავალ კომპანიებზე და აღწერს ამ სეგმენტში არსებული ორგანიზაციების ბიზნესისა და IT-ის თანხვედრასთან და IT მართვის პრაქტიკებთან დაკავშირებულ აღმოჩენებს.

სტატია იწყება ბიზნესისა და IT-ის თანხვედრის და IT მართვის ზოგადი დონის აღწერით. ხოლო საბოლოოდ განიხილება შედეგები, თუ როგორ იყო აღქმული ბიზნესისა და IT-ის თანხვედრა და როგორ იყო დანერგილი IT-ის მართვა ჰოლანდიაში არსებულ მცირე და საშუალო კომპანიებში.

აღნიშნული კვლევის ძირითადი დასკვნა მდგომარეობს იმაში, რომ ჰოლანდიაში არსებულ მცირე და საშუალო კომპანიებში ბიზნესისა და IT-ის თანხვედრა სხვა საერთაშორისო მაჩვენებლებთან შედარებოთ ნაკლებია. უფრო მეტიც, აღმოჩნდა, რომ შერჩეულ ორგანიზაციებში, სადაც მაღალია ბიზნესისა და IT-ის თანხვედრა დანერგილია საუკეთესო IT-ის მართვის პრაქტიკები და პირიქით. მიუხედავად იმისა, რომ კვლევაში მონაწილე ორგანიზაციების რიცხვი იყო მცირე (6 კომპანია), აღნიშნული კვლევის შედეგები თანხვედრაშია დიდ კომპანიებში ჩატარებული მსგავსი კვლევის შედეგებთან, სადაც გამოვლინდა იგივე, დადებითი ტენდენციები IT მართვასა და ბიზნესისა და IT-ის თანხვედრას შორის.

2.3. IT მართვის არარსებობა საფრთხეს უქმნის ბიზნესის ღირებულებებს

მათთვის ვისაც მიაჩნია, რომ კორპორაციული IT-ის მართვის ნებისმიერი ფორმის არსებობა უკეთესია ვიდრე IT-ის მართვის არ ქონა, მნიშვნელოვანია გაითვალისწინონ ფაქტი, რომ IT მართვის უხარისხო სისტემა არის IT-ის წარუმატებლობის დოკუმენტირებული მიზეზი (McCue, 2007). სინამდვილეში, ცუდად დაგეგმილმა IT-ის მართვამ შესაძლოა გამოიწვიოს ძალიან მნიშვნელოვანი ზარალი, როგორც ფინანსური, ასევე რეპუტაციული. აღნიშნული ფაქტის ნათელი მაგალითი არის

შოტლანდიის სამეფო ბანკი, რომელიც სუსტი IT-ის მართვის გამო დიდი ბრიტანეთის ფინანსური სერვისების მარეგულირებლის მხრიდან დაჯარიმდა 5.6 მილიონი ბრიტანული ფუნტით (Tung, 2010).

IT რისკები, კორპორაციული IT მართვის ძირითადი დომენი, რეალიზდა შოტლანდიის სამეფო ბანკის შემთხვევაში, არა მხოლოდ ბანკის მიზნების კომპრომეტირებით, არამედ როგორც რეალური ფინანსური და ენით აღუწერელი რეპუტაციული ზარალი, რომელსაც შესაძლებელია მოჰყოლოდა დამატებითი ფინანსური ზარალი. ირონიულია აზრი, რომ კორპორაციული IT მართვის დანერგვის ძირითადი მიზეზი არის IT რისკების ოპტიმიზაცია, როგორც ორგანიზაციის მიზნების მიღწევის გეგმის ნაწილი. რეალურად, IT რისკების მართვა მიიჩნევა იმდენად მნიშვნელოვნად, რომ ის დღესდღეობით მოქცეულია კომპანიის რისკების მართვის დღის წესრიგის სათავეში დიროქტორთა საბჭოებისა და უმაღლესი მენეჯმენტისათვის მსოფლიოს მასშტაბით, ციფრული ტრანსფორმაციის თანამედროვე პარადიგმაში ოპერაციების და ინფრასტრუქტურის გარდაქმნის შესაძლებლობის გათვალისწინებით, ისინი მიისწრაფვიან გახდნენ მეტად კონკურენტუნარიანები ბაზარზე არსებულ ციფრულ ორგანიზაციებთან მიმართებაში (Saulez, 2017).

2.4. რისკების შეფასების მართვა COBIT 5-ის გამოყენებით

როგორც ამერიკის შეერთებული შტატების რეგიონალური სასურსათო ჯაჭვია დაფუძნებული მსხვილ ქალაქსა და მის რაიონებში ასეთივე სწრაფი ზრდა განიცადა FamilyGrocer-მა (სახელწოდება შეცვლილია) ტერიტორიების შესყიდვითა და ახალი მაღაზიების გახსნით. ფოკუსირებულია რა, მიწოდების უწყვეტ ეფექტურობაზე, FamilyGrocer-ი პროდუქციის უმეტეს ნაწილს თავის მაღაზიებში სასაქონლო საწყობის მეშვეობით ავრცელებს, რომელიც ასევე მოიცავს საოფისე და IT რესურსებსაც. რისკების გათვალისწინებით რომელიც დაკავშირებულია კონსოლიდირებულ ოპერაციებთან, IT ორგანიზაციამ მოიპოვა დირექტორთა საბჭოს მანდატი, რათა ოფიციალურად მართოს

IT-თან დაკავშირებული რისკები. მანდატის მიხედვით IT ორგანიზაციული რისკები უმაღლესი დონით უნდა შეფასდეს, უმეტესად შიდა გამოცდილებიდან. IT ორგანიზაციას საბჭომ ასევე მოსთხოვა წარმოედგინა რისკების სამართავად შემუშავებული მიმდინარე პროგრამა.

IT ორგანიზაცია სიამოვნებით გაწევრიანდა ინფო-ტექის საკვლევ ჯგუფში რათა ადვილად ხელმისაწვდომი ყოფილიყო პრაქტიკული კვლევები და მიმწოდებელის შესარჩევი ინსტრუქციები. ბუნებრივია, შემდეგი ნაბიჯი ინფო-ტექთან ჩართულობით, COBIT-ზე დაფუძნებული ოპერაციების სემინარის ჩატარება იყო რისკების მართვის შესახებ.

ინფო-ტექმა დაიწყო მუშაობა COBIT 5-ზე, მისი მკაფიო და მოკლე ჩარჩოს გამო, IT ძირითადი პროცესების სამართავად (პროცესების ურთიერთქმედებისა და დოკუმენტაციის მოთხოვნებთან ერთად). COBIT არის IT აუდიტორებისა და სხვა IT პროფესიონალების მიერ გამოყენებული სანდო ჩარჩო, მეტწილად პრაქტიკულ სტრატეგიებში, უსაფრთხოებასა და რისკებში.

ერთ კვირიანი მუშაობის განმავლობაში, IT მენეჯმენტის გუნდის ძირითადი წევრები, ასევე მთავარი ინფორმაციული ოფიცერი (CIO) მუშაობდნენ მეთოდისტებთან ერთად, რათა ჩამოეყალიბებინათ თავიანთი შეხედულებები და მოსაზრებები, COBIT-ის გამოყენებით აღეწერათ თავიანთი ცოდნა IT რისკებში და მოემზადებინათ შესაბამისი ანალიზისათვის.

რისკების შეფასება დაიწყო COBIT 5-ის EDM03 და APO12 მართვის პრაქტიკის შესწავლით, შეფასების, მიმართვისა და მონიტორინგის (EDM) და განლაგების, დაგეგმვისა და ორგანიზების (APO) COBIT-ის დომენების შესაბამისად და გარკვეული შესაძლებლობების დადგენის მიზნით უბრალო თვით-შეფასებით.

IT ორგანიზაციამ დაადგინა, რომ ადგილზე არ ფუნქციონირებდა IT რისკების მართვის პროცესები და შესაბამისად მიენიჭა ნულოვანი დონე. გუნდმა მიზნად დაისახა მიეღწია მეორე დონისათვის (რეგულირებადი პროცესები) სამუშაო პროდუქტების ტექნიკური მახასიათებლების მართვის შესაძლებლობებით. IT ორგანიზაციამ გააფართოვა ინფო-

ტექის პროექტის განხორციელების გამამარტივებელი ფუნქციონირება და მეთოდოლოგია რათა ჩაეტარებინა უმაღლესი დონის გონებრივი იერიში გუნდის მთავარ წევრებთან, კლიენტი ორგანიზაციისათვის IT რისკ-ფაქტორების დასადგენად.

ამის შემდეგ გუნდმა იმუშავა რათა გამოევლინათ რისკების შემთხვევები, დაედგინათ ქმედების სუბიექტი და საფრთხის შემცველი ტიპი. შემუშავდა პრიორიტეტების რუბრიკა რათა დაეხარისხებიათ რისკების შემთხვევები. გუნდმა გამოავლინა (პროგრესში მყოფი პროგრამები) და დაადგინა (Net-New პროგრამები) (ტერმინი - ცოტას გაყიდვით გაყიდე მეტი) დრო/რესურსების საჭიროებები პრიორიტეტული რისკების ფაქტორების შესამცირებლად.

საბოლოოდ გუნდმა მიიღო კრიტიკული გადაწყვეტილება, დაედგინა IT ორგანიზაციის მიმდინარე რისკების მართვის ფორმა. ეს მოიცავდა როლებისა და პასუხისმგებლობების განსაზღვრას, აქტივობების მართვას, ინფორმაციის შეგროვების მაჩვენებლებს და სარეკომენდაციო გეგმებს.

გადაწყვეტილების მიღებისთანავე დაიშიფრა თითოეული მათგანი შესაბამის პროგრამულ სახელმძღვანელოებში, სტანდარტულ ოპერაციულ პროცედურებში, შეფასების ინსტრუმენტებში, პროექტის მოთხოვნებში და კომუნიკაციებისა და რეკომენდაციების შაბლონებში.

სამუშაო შეხვედრის ძირითადი შედეგები მოიცავდა:

1. IT რისკების შემთხვევების კატალოგი: როგორც ზემოთ არის აღნიშნული, კატალოგში აღწერილი იყო არამხოლოდ რისკების შემთხვევები, არამედ ინტენსიური შემცირების სტრატეგიებიც, IT პროექტის მოთხოვნების ინიცირება, როგორც გარდაუვალი საჭიროება საგნისა რომელიც არ იყო პროექტის კალენდარში.
2. IT რისკების მართვის პროგრამის სახელმძღვანელო: ამ დოკუმენტში ჩანიშნული იყო კრიტიკული გადაწყვეტილებები, რომელიც მოიცავდა გუნდის მოხსენებებს რისკების სიმძიმისა და ალბათობის შეფასების შესახებ. დოკუმენტში აღწერილია

მიმდინარე IT რისკების მართვის ხელმძღვანელი კომიტეტის პროცესი, რომელშიც მონაწილეობდა გუნდი.

3. პრეზენტაცია ფირმის საბჭოსათვის, IT რისკების მართვის შეფასებასა და პროგრამაზე: ამ პრეზენტაციამ აღწერა მუშაობის დროს მიღებული პროგრესი, ხაზი გაესვა რისკ ფაქტორებსა და შესწორებებს, მოთხოვნილი იქნა დამატებითი ბიუჯეტი და შეჯამდა მიმდინარე რისკების მართვის პროგრამა ბორდისათვის.

FamilyGrocer-მა მთლიანი სამუშაო პროცესიდან და მოთხოვნილი დოკუმენტაციიდან აღმოაჩინა რომ პროცესის დანერგვა შემდეგი ორშაბათიდან უნდა დაეწყო, ამავდროულად შესაბამისი აუცილებელი ქმედებები იყო საჭირო ტექნოლოგიებში, ხალხსა და პროცესებში გამოვლენილი ხარვეზების შესამსუბუქებლად. შემდეგ კვირას CIO-მ საბჭოს წარუდგინა სამუშაოს შეჯამება, რომელშიც აღინიშნა თავდაპირველი IT რისკების შეფასების საფუძვლიანობა და მიმდინარე რისკების მართვის პროგრამა, რომელიც შემუშავდა სემინარზე. ორი თვის შემდეგ, რისკებთან გამკლავების პროგრესი კვლავ ძლიერი რჩება და IT ლიდერები კვლავაც განაგრძობენ მიმდინარე რისკების მართვის პროგრამის შესაბამისად მუშაობას. (Vince Londini)

2.5. COBIT-ის დანერგვა ეკოპეტროლში IT-ის, მასთან დაკავშირებული რისკების და სტანდარტებთან შესაბამისობის სამართავად

Ecopetrol S.A. არის ვერტიკალურად ინტეგრირებული ნავთობგადამამუშავებელი და ბუნებრივი აირისა და ნავთობის მომპოვებელი და მწარმოებელი კომპანია. 2007 წელს Ecopetrol-მა განაახლა კორპორაციული სტრატეგიები, მკაფიოდ განსაზღვრული მიღწევების ზრდით შემდეგი წლებისათვის, რაც ორგანიზაციულ სტრუქტურასა და პროცესებში მნიშვნელოვან ცვლილებებსა და გაუმჯობესებას მოითხოვდა და სტრატეგიულ მიზნებს ეყრდნობოდა.

შედეგად, გაჩნდა მნიშვნელოვანი საკვანძო მოვლენები, როგორიცაა კომპანიის სამართლებრივი ტრანსფორმაცია, საერთაშორისო ოპერაციების დაწყება და შიდა კონტროლის სისტემის გაძლიერების მიზნით COSO სისტემის დანერგვა. 2008 წლის სექტემბერში, კომპანიამ თავისი აქციები ნიუ-იორკის საფონდო ბირჟაზე გაიტანა.

სტრატეგიულ განლაგებასთან ერთად, კომპანიის სიტუაციიდან გამომდინარე, დროული და ეფექტური რეაგირება რომ მოეხდინა, 2008-ში ინფორმაციული ტექნოლოგიების დანაყოფმა, IT მართვის სისტემის გასაუმჯობესებლად გადაწყვიტა გაეერთიანებია IT მართვის სისტემა, რომელიც სათანადო ჩარჩოზე იქნებოდა დაფუძნებული რისთვისაც შეირჩა COBIT-ი, როგორც შესაფერისი IT მართვის ჩარჩო.

Ecopetrol S.A. არის კოლუმბიის უმსხვილესი ინტეგრირებული ნავთობკომპანია დაახლოებით 7000 დასაქმებული თანამშრომლით. არის მსოფლიოს 40 ნავთობკომპანიასა და ლათინური ამერიკის ოთხ მსხვილ ნავთობკომპანიას შორის. გარდა კოლუმბიისა, რომელიც ეკოპეტროლის მთლიანი წარმოების 60%-ს მიითვლის, კომპანია ჩართულია ბრაზილიაში, პერუსა და ამერიკის შეერთებულ შტატებში (მექსიკის ყურე) ნავთობის მოპოვებასა და წარმოებაში. Ecopetrol-ი ასევე მნიშვნელოვნად იღებს მონაწილეობას ბიო-საწვავის წარმოებაში.

ჟურნალი ფორბსი აღნიშნავს, რომ „ ის იმყოფება 2000 უმსხვილეს კომპანიას შორის მსოფლიოში'' (აპრილი, 2010), ყოველწლიური სიის მიხედვით Ecopetrol-ს 222-ე ადგილი უჭირავს, შემდეგი მონაცემებით: გაყიდვები $14.26 მილიარდი, მოგება $2.40 მილარდი, აქტივები $27.20 მილიარდი და საბაზრო ღირებულება $54.14 მილიარდი.

ეკოპეტროლის კორპორაციული მართვის კოდექსი მოიცავს საუკეთესო კორპორაციულ პრაქტიკას ბიზნეს ეთიკის, სწორი ადმინისტრირებისა და კომპანიის კონტროლის შესანარჩუნებლად. ეს საშუალებას აძლევს კომპანიას კონკურენცია გაუწიოს და ამავდროულად პატივი სცეს აქციონერებს, ინვესტორებსა და სხვა დაინტერესებულ მხარეებს რაც დაფუძნებულია მკაფიო პოლიტიკაზე, მენეჯმენტის გამჭვირვალობასა და საქმიანობის შესახებ ინფორმაციის გამჟღავნებაზე, რაც თავის

მხრივ დაინტერესებულ მხარეებს უფრო მეტ ნდობას უჩენს ბაზარზე. Ecopetrol- ის შიდა კონტროლის სისტემა საერთაშორისო სტანდარტების ფარგლებშია (COSO).

ეკოპეტროლის ინფორმაციული ტექნოლოგიების განყოფილება ექვემდებარება სერვისისა და ტექნოლოგიის ვიცე-პრეზიდენტს და ხელმძღვანელობს კომპანიის მართვის ორ ძირითად ფრონტს: IT გადაწყვეტილებების განვითარებასა და დანერგვას და ინფორმაციული ტექნოლოგიებისა და ინფრასტრუქტურული მომსახურების გაწევას ბიზნეს პროცესების მხარდასაჭერად.

ინფორმაციული ტექნოლოგიების განყოფილება, რომელსაც ჰყავს დაახლოებით 150 დასაქმებული თანამშრომელი, პასუხისმგებელია IT მართვის უზრუნველყოფაზე. მას აქვს ძალიან ძლიერი შიდა სტრუქტურა, რომელიც განაწილებულია ისე, რომ აკმაყოფილებს ბიზნესის განვითარების პროექტებს, დანერგვას, ოპერაციებისა და გადაწყვეტილებების მხარდაჭერას და უზრუნველყოფს საჭირო მომსახურებას. გარდა ამისა, იგი მოიცავს მართვისა და არქიტექტურის განყოფილებას და ინფორმაციული უსაფრთხოების სფეროს, რომელიც წარმოაჩენს IT განყოფილების მაღალ დონეს, რომელიც უძღვება IT მართვასთან, რისკებთან და შესაბამისობასთან დაკავშირებულ პროცესებს.

2008 წელს , ინფორმაციული ტექნოლოგიების განყოფილებამ აირჩია COBIT, როგორც სათანადო IT მართვის ჩარჩო, IT მართვის სისტემის გასაერთიანებლად COBIT- ის შემდეგ მახასიათებლებზე დაყრდნობით:

- IT მიზნებს აკავშირებს ბიზნესის მიზნებს.
- იძლევა ბიზნესზე ორიენტირებულ უკეთეს თანხვადრას.
- მენეჯმენტისათვის გასაგებ ენაზე იძლევა IT-ის საქმიანობის აღწერას.
- პროცესის ორიენტირებაზე დაყრდნობით, გამოხატავს მკაფიო უფლებასა და პასუხისმგებლობებს.
- მიღებულია მესამე მხარეებისა და რეგულატორებისათვის.

- საერთო ენის გამონახვის გამო ყველა დაინტერესებული მხარისათვის გასაგები ხდება.
- აკმაყოფილებს COSO და Sarbanes-Oxley-ს მოთხოვნებს, IT კონტროლის გარემოსთვის.

2008 წლის ბოლო კვარტალში, ეკოპეტროლის ინფორმაციული ტექნოლოგიების განყოფილებამ განსაზღვრა სახელმძღვანელოები, პროცესები და კონტროლის მიზნები რათა დაენერგა COBIT. ანალოგიურად, განყოფილებამ განსაზღვრა შიდა რესურსები, რომლებიც ხელს შეუწყობდა სისტემის დანერგვას და გამოყო საჭირო რესურსები გარე კონსულტანტების დასაქირავებლად.

გუნდმა მიიღო პროექტი, რომელიც განსაკუთრებულ ყურადღებას უთმობდა შემდეგ საკითხებს:

- რესურსების განაწილება და ინტერდისციპლინარული გუნდი IT-არეალის ფარგლებში ჩართულ წარმომადგენლებთან ერთად.
- ბიზნეს ერთეულებთან და სხვა მხარდამჭერ ერთეულებთან ურთიერთობების განსაზღვრა და ძირითად სფეროებთან: ფინანსებთან, რისკების მართვასთან, სტრატეგიასთან, ხარისხთან და შიდა და გარე აუდიტთან ურთიერთკავშირი.
- IT მხარდაჭერის იმ გუნდთან ინტეგრაცია და კონვერგენცია სატრანსპორტო ოპერაციებში, რომლებსაც მანამდე ჰქონდათ დანერგილი COBIT.
- ბიზნეს პროექტებთან თანხვედრა: შიდა კონტროლის სისტემის გაძლიერება (COSO) და შესაბამისობა (Sarbanes-Oxley Act). ჩვენ განვიხილეთ სხვადასხვა ბიზნეს ინიციატივები და მიმდინარე პროექტები, რათა უზრუნველგვეყო კოორდინაცია და ინტეგრაცია.
- მენეჯმენტის უმაღლესი დონის ანგარიშის შედგენა, შემდგომი ყოველკვირეული შეხვედრები პროექტთან დაკავშირებით.
- თავდაპირველი განცხადებების იდენტიფიკაცია (Sarbanes-Oxley, მაღალი კომპონენტი SAP- ში) და სხვა. ამავდროულად ამ განცხადებებთან

დაკავშირებული ადამიანების, რესურსებისა და სხვა კრიტიკული ბიზნეს პროცესების გაგება.

ეკოპეტროლმა გადაწყვიტა COBIT-ის 28 პროცესის დანერგვა, პრიორიტეტი მიენიჭა კონტროლის მიზნებს, რომლებიც მხარს უჭერენ Sarbanes-Oxley-ის შესაბამისობას. ინფორმაციულმა განყოფილებამ შეიმუშავა შიდა დავალება ამ პროცესების სიმწიფის დონის დასადგენად. მას შემდეგ, რაც დადგინდა, რომ ისინი საშუალო სიმწიფის მეორე დონეზე იმყოფებოდნენ, გუნდმა გამოავლინა ხარვეზები და შეიმუშავა სამოქმედო გეგმები ყველაზე კრიტიკული პროცესებისთვის მე-3 დონის მისაღწევად.

პროექტის გუნდმა შეიმუშავა პროცესების დიზაინი და დოკუმენტაცია, შემდგომში, ოპერაციის დანერგვისა და მონიტორინგის საჭირო ცვლილებების დასრულების მიზნით. შედეგად, 2009 წლის ივნისისთვის, განყოფილებამ დანერგა და უზრუნველყო 14 უმაღლესი პრიორიტეტის მქონე COBIT-ის პროცესი. 2009 წლის დეკემბრისთვის 28-ვე პროცესი იყო დანერგილი.

2009 წლის მეორე ნახევარსა და 2010 წლის პირველ კვარტალში, შიდა და გარე აუდიტი შემუშავდა Sarbanes-Oxley შესაბამისობის დასადგენად. ჩატარდა რამდენიმე ღონისძიება ძირითადი IT პროცესებისა და კონტროლების გასაუმჯობესებლად. შედეგად, გარე აუდიტმა განაცხადა, რომ რაიმე მნიშვნელოვანი ნაკლოვანებები ან სუსტი მხარეები არ გამოვლენილა IT კონტროლში, რომელიც CIO-ს, CFO-ს, CEO-ს ან აუდიტორების მიერ წარდგენილ ანგარიშში უნდა ყოფილიყო.

2009 წლის დეკემბერში, COBIT-ის პროექტმა მიიღო კომპანიის ჯილდო და საუკეთესოდ იქნა აღიარებული პროექტის გუნდის შრომის ინტენსიურობა, ინიციატივა და გუნდური მუშაობა.

2009 წლის ბოლო კვარტალში ინფორმაციული ტექნოლოგიების განყოფილებამ დაიქირავა გარე კონსულტანტები, რათა ჩაეტარებინა COBIT-ის თოთხმეტი კრიტიკული პროცესის სიმწიფის დონის შეფასება. შეფასებამ დაადასტურა თორმეტ პროცესში 3-ე დონის, ხოლო 2 პროცესში 4-ე დონის მიღწევა.

2010 წელს, IT განყოფილებამ შექმნა მდგრადი და ოპტიმალური გეგმა IT მართვის სისტემისათვის, რომელიც ეფუძნებოდა კომპლექსურ ხედვას, ორგანიზაციული და ოპერატიული მოდელის და ინფორმაციული ტექნოლოგიების გაძლიერებით IT პროცესებისა და კონტროლის ავტომატიზაციას.

კომპანიამ ასევე მოახდინა IT შესაბამისობის რესტრუქტურიზაცია COBIT-ის პრაქტიკის ჩარჩოს მითითებებით.

ძირითადი საკითხები, რამაც შესანიშნავი შედგები მოიტანა COBIT-ის დანერგვის პირველ წელს ეკოპეტროლის IT მართვის სისტემაში:

- COBIT- ის დანერგვა ჩამოყალიბდა როგორც პროექტი, სამუშაო გეგმის დეტალური აღწერით, მკაფიოდ განსაზღვრული დეტალებით, პროექტის მართვისათვის გუნდური მუშაობის გადანაწილებით, რისკების მართვით და დროისა და მიწოდების კონტროლით.
- გუნდს ჰქონდა მენეჯმენტის სრული მხარდაჭერა, უზრუნველყოფილი იყო მიღწევების ყოველკვირეული ანგარიშებით და ნებისმიერი სახის გადახრებისა თუ ქმედებების შესახებ ჰქონდათ ინფორმაცია.
- კომპანიამ დაიქირავა ცნობილი სპეციალიზებული საკონსულტაციო ფირმები, რომელებსაც ჰყავდათ ღრმა ცოდნისა და დიდი გამოცდილების მქონე გუნდები.
- შეიქმნა ცვლილებების მართვის, დასატრენინგებელი აქტივობებისა და პროფესიული აკრედიტაციის ფრონტი.
- პროექტების დაგეგმვა, განვითარება და შედეგები ეფექტურად ესადაგებოდა კომპანიას.
- მეთვალყურეებისა და კონტროლზე პასუხისმგებლების მიერ დამუშავების პროცესის ძიება.
- პროექტი კარგად იყო ინტეგრირებული ყველა სფეროსთან, სინერგიები ბერკეტის ქვეშ იყო მოქცეული, განსაკუთრებით IT მხარდაჭერის გუნდთან

სატრანსპორტო ოპერაციებში, რომელმაც ადრინდელი ძალისხმევის შედეგები და ბიზნესმენთა პერსპექტივები უზრუნველყო.

- შეიქმნა პრაქტიკისა და მართვის სასწავლო გაკვეთილების გაერთიანება.
- განისაზღვრა მდგრადობის სტრატეგიები და პროცესების შემდგომი ოპტიმიზაცია.
- IT განყოფილება ეფექტურად ურთიერთქმედებდა აუდიტის ჯგუფებთან.
- განსაკუთრებული ყურადღება დაეთმო მოვალეობების, წვდომის კონტროლების, უწყვეტობის გეგმის, პროგრამული უზრუნველყოფის შემოუშავებისა და ინფორმაციული უსაფრთხოების საკითხების სეგრეგაციას.
- მატერიალურ დონეზე ჩატარდა შეფასებები კომპეტენტური და დამოუკიდებელი მესამე მხარის მიერ.
- 20-ზე მეტმა თანამშრომელმა ჩააბარა COBIT- ის გამოცდა და მიიღო COBIT- ის სერტიფიკატი.
- რამდენიმე თანამშრომელი იყო ან გახდა ISACA- ის წევრი, რაც იმას ნიშნავდა რომ უფრო გაუადვილდებოდათ ხელმძღვანელობა.
- ეკოპეტროლმა ეროვნული და საერთაშორისო ნავთობისა და გაზის კომპანიების ბენჩმარკინგი განახორციელა.

ეკოპეტროლი გეგმავს, 2010 წელი დაასრულოს - IT მართვის სისტემებში COBIT-ის 31 პროცესის მე-3 დონეზე დანერგვითა და 2011 წლისათვის 4-ე დონეზე გასვლით. ინფორმაციული ტექნოლოგიების განყოფილება სწავლობს მონახაზ დოკუმენტაციას COBIT 5-ის შესახებ და გეგმავს მის დანერგვას, როგორც კი ეს შესაძლებელი იქნება. ეკოპეტროლი ასევე ავრცელებს თავისი IT მართვის სისტემის პრაქტიკას და COBIT-ს მის ბიზნესში ჩართულ კომპანიებზე კოლუმბიაში, პერუსა და ბრაზილიაში. IT მართვის სისტემა ჩაერთვება კორპორაციულ მართვის სისტემაში რათა უზრუნველყოს პრაქტიკის ინტეგრაცია და რეგულირება. ეკოპეტროლმა ძლიერი საფუძველი ჩაუყარა IT მართვის, რისკების მართვისა და შესაბამისობის კონსოლიდაციას IT მართვის სისტემის ინტეგრაციით, რაც განხორციელებული იქნა COBIT-ის მიერ და მდგრადი სტრუქტურისა და პროცესზე დაფუძნებული ოპტიმიზაციის მოდელის მეშვეობით. (ISACA)

2.6. COBIT-ის გამოყენება ჰოსპიტალში რისკების მართვისთვის

სამედიცინო დაწესებულებებში IT შეიძლება იყოს ორმაგად სასარგებლო: შეუძლია შეამციროს რისკები და რისკფაქტორები. სათანადო ოპერაციული რისკების მართვის გარეშე, IT რისკების მართვა ვერ მოხერხდება. ავტორის გამოცდილების გათვალისწინებით, COBIT არის აუცილებელი მიდგომა სამედიცინო დაწესებულებებისათვის, რათა შეძლოს ინფორმაციული სისტემების დანერგვა და ოპერაციული რისკების მართვა მთლიანი ჰოსპიტალისთვის. ეს სტატია განმარტავს თუ როგორ იქნა გამოყენებული COBIT „თაკედას მთავარ საავადმოფოში'' რომელიც იაპონიაში, ფუკუშიმას პრეფექტურაში, აიზუ-ვაკამაცუში მდებარეობს.

თავიდან ჰოსპიტალის ინფორმაციული სისტემის (HIS) პროექტის დანერგვის პროცესი ეფუძნებოდა COBIT-ის მეთოდს, რომელიც წარმატებით დასრულდა და შესაბამისი კონტროლებიც დაინერგა.

როგორც ბევრმა COBIT-ის მომხმარებელმა გააცნობიერა, საჭირო და შესაბამისი COBIT-ის კონტროლების გამოვლენა შესაძლებელია დიდი დაბრკოლება გამხდარიყო. ამ შემთხვევაში ორგანიზაციამ აღმოაჩინა რომ კონტროლის მექანიზმების სუბიექტების იდენტიფიცირების შემდეგ ადვილი იქნებოდა COBIT-ის კონტროლების გამოვლენა.

COBIT 4.1 სახელმძღვანელოს მიხედვით, ორგანიზაციამ დაიწყო IT დაბალანსებული შედეგების ცხრილის დანერგვა.

IT დაბალანსებული შედეგების ცხრილი მუშაობს COBIT-თან ერთად და შეფასებულია განსაზღვრული საქმიანი მიზნებისთვის. COBIT პროცესი უზრუნველყოფს კურსს ზოგადი საქმიანობის მიზნებიდან IT მიზნებისკენ და IT პროცესებისაკენ. ეს იძლევა მეტრიკულ ინდიკატორთა მაჩვენებლებს, რის საფუძველზეც შესაძლებელია მონიტორინგის დანერგვა და IT პერფომანსის შეფასება.

სამედიცინო დაწესებულებებში რისკების ფაქტორები რამდენიმე სახისაა: სამედიცინო (მაგ. სამედიცინო შეცდომები, ჰოსპიტალის ინფექციები, ცდომილებები), ფინანსური (მაგ., არასაინკასაციო გადასახადები, ჰოსპიტალში დასარჩენი შემცირებული ვადები, ხარჯების მართვა) და მარეგულირებელი (მაგ., სტაჟიორების მიღება, ელექტრონული განცხადებები). რისკების სამართავად და ჰოსპიტალის ინფორმაციული სისტემის მოქმედებაში მოსაყვანად საჭიროა Top-down (ზემოდან-ქვემოთ) მიდგომა. სწორედ აქ ერთვება COBIT.

რა თქმა უნდა, იაპონიაში, ისევე როგორც ბევრ ქვეყანაში, პირადი მონაცემების დაცვა ძალიან მნიშვნელოვანი საკითხია, განსაკუთრებით ჯანდაცვის ინდუსტრიაში, რომელიც ამ სფეროში, იაპონიის მონაცემთა დაცვის და ასევე ადრე მიღებული ჯანდაცვის ჩანაწერთა დაცვის კანონის მიხედვით იმართება. მკაცრად იკრძალება ჯანდაცვის შესახებ ჩანაწერების დამატებით ლოკაციებზე განთავსება. გარდა ამისა, ჯანდაცვის შესახებ ჩანაწერებთან დაკავშირებული სისტემები (ქსელები) ვერ უკავშირდება გარე ქსელებს (დასაშვებია მხოლოდ დახურული ქსელი). ამასთანავე სამედიცინო მკურნალობის ანაზღაურების მოთხოვნის მონაცემების გადატანა შესაძლებელია მხოლოდ ელექტრონული მედიის, სპეციალურად გამოყოფილი ხაზის ან დახურული ქსელის მეშვეობით. ამრიგად, მონაცემთა დაცვასთან დაკავშირებული რისკები რა თქმა უნდა მნიშვნელოვანია იაპონიაში და ამიტომაც არ იყო ამ პროექტის განხორციელების ძირითადი ინიციატივა. სხვა ჯანდაცვის ორგანიზაციებს რომ წამოეწყოთ მსგავსი ინიციატივა, შესაძლებელია აღნიშნული საკითხის უფრო ღრმა დეტალებში განხილვა, ძალიან მნიშვნელოვანი ყოფილიყო რისკებისა და კონტროლების გადახედვისას.

დაბალანსებული შედეგების ცხრილით დაწყება

თავდაპირველად განისაზღვრა ორგანიზაციის სტრატეგია, რასაც IT სტრატეგიის განსაზღვრა მოჰყვა, რომელიც დეტალებში იქნა დაშლილი. პირველ ეტაპზე შესწავლილ იქნა ჰოსპიტალის IT რისკები, არსებულ რისკთან ერთად, ასევე რისკების დაშვებისა და ტოლერანტობის დონეები. სტრატეგიის განსაზღვრისას მნიშვნელოვანია გვახსოვდეს, რომ ღირებულების მენეჯმენტის მიზანი მხარს უჭერს ბიზნესის მიზნის

მიღწევას; რისკების მართვის მიზანი კი არის ხელი შეუშალოს ბიზნესის მიზნების მიღწევას. ტრადიციული დაბალანსებული შედეგების ცხრილის მიდგომის გამოყენებით, ჰოსპიტალის პრეზიდენტის მიერ შექმნილი HIS-ის აღმასრულებელმა კომიტეტმა, ჰოსპიტალის მთავარ მენეჯმენტთან ერთად განიხილა რისკების ფაქტორები.

მთავარი მენეჯმენტის ხედვა და მისია ძალიან მნიშვნელოვანია მთლიანად ჰოსპიტალის ინფორმაციული სისტემისათვის. თუკი HIS-ი არ დაეთანხმება მენეჯმენტის ხედვას და მისიას, მაშინ სისტემა გამოუსადეგარი გახდება. გუნდმა განსაზღვრა შემდეგი მიზნები სრული HIS-ისათვის, ტოპ-მენეჯმენტის ხედვის გათვალისწინებით:

- უზრუნველყოფილი იქნას უსაფრთხოებისა და პერსონალური ინფორმაციის მონაცემთა დაცვის მაღალი დონე.
- გაზარდოს სამედიცინო მომსახურების მაღალი დონე.
- სამედიცინო შეცდომების მინიმალიზაცია (არაკეთილსინდისიერი პრაქტიკა).
- სწრაფი რეაგირება საზოგადოებრივ საჭიროებებზე.
- გაუმჯობესდეს ჰოსპიტალსა და საზოგადოებას შორის ინფორმაციის გაცვლის პროცესი.
- პერსონალის უნარებისა და ცოდნის ამაღლება.
- ახალი გამოწვევების იდენტიფიცირება და მოგვარება.
- უწყებასთან თანამშრომლობის დაწყება.
- ჯანდაცვის, სამკურნალო და საექთანო საქმიანობისათვის დახმარების სრული მხარდაჭერა.
- კვლევისთვის უკეთესი გარემოს შექმნა ექიმებისათვის და ჰოსპიტალში ჯანდაცვისა და მასთან დაკავშირებული ინფრასტრუქტურის გაუმჯობესება.

მომხმარებელთა კმაყოფილების სტრატეგიული გადანაწილება

ჰოსპიტალისთვის მომხმარებლები არიან პაციენტები და საზოგადოების ის ნაწილი, რომელსაც ის ემსახურება. შემდეგი ნაბიჯი იყო მომხმარებელთა კმაყოფილების მაჩვენებლების განსაზღვრა, ან ღირებულებისა და რისკების მასშტაბების შკალა. თუ

დადგენილი დონე უფრო მაღალია, ვიდრე მიმდინარე დონე, მაშინ ეს იქნება ღირებულების შექმნა, ხოლო თუ დადგენილი დონე დაბალია მიმდინარე დონეზე, მაშინ შესაძლებელია რისკების რეალიზება. გუნდმა გამოავლინა რისკებისა და ღირებულების შეფასების შემდეგი არეალები:

- პაციენტის კმაყოფილების გაუმჯობესება - სწრაფი რეაგირება, მკურნალობის პერიოდის შემცირება, მკურნალობის მეთოდების ფართო არჩევანი, ინფორმირებული თანხმობის ფორმის სისრულე და ინფორმაციის გამჟღავნება.
- ჰოსპიტალებსა და კლინიკებს შორის თანამშრომლობის გაუმჯობესება იგივე სფეროში (ჯანდაცვის ზონა) - ინფორმაციის სწრაფი გაზიარება, საუკეთესო სამედიცინო საინფორმაცო ცენტრი, საჭიროების შემთხვევაში ადგილობრივ ხელისუფლებასთან თანამშრომლობა, ადგილობრივი მოსახლეობის ჯანდაცვის სტანდარტების დაცვა და სწრაფი რეაგირება სასწრაფო სამედიცინო მომსახურებებზე.
- საზოგადოების საერთო კმაყოფილების გაუმჯობესება - სამედიცინო ინფორმაციის გავრცელება და უკეთესი მომსახურება ჯანმრთელი ადამიანებისათვის ჯანმრთელობის შენარჩუნების მიზნით.

სტრატეგიული გადანაწილება ფინანსებში

ფინანსურ საკითხებთან მიმართებაში, გუნდმა გამოავლინა შეფასებისა და რისკების შკალის შემდეგი არეალები:

- ზრდა - ჯანმრთელობის დაზღვევის მსურველთა სამედიცინო ხარჯების ანაზღაურების სიზუსტე, მოგების გაზრდა და შესაფერისი სამედიცინო პრაქტიკის გადახდადი ობიექტები.
- რენტაბელობა - თვითღირებულების ხარჯების შემცირების აქტივობები და ინფორმაციის მიღება დანახარჯების ანალიზის შესახებ.
- ლიკვიდურობა - იმ ფაქტორების გაანალიზება, რომლებიც განსაზღვრავენ ფულადი ნაკადების ღირებულებას და აღჭურვილობისა და მოწყობილობების უკეთესი კონტროლი, რომლებიც ითვლიან ფიქსირებულ აქტივებს.

- სტაბილურობა - პერსონალის ხარჯების კონტროლი (შრომის ანაზღაურება)

შიდა პროცესების სტრატეგიული გადანაწილება

შიდა პროცესის გათვალისწინებით, არსებობს მრავალი რისკ-ფაქტორები და დაბრკოლებები. პირადობის იდენტიფიცირების მონაცემებთან (PID) დაკავშირებული პრობლემები აქაც შეიძლება იმალებოდეს. გუნდმა განიხილა:

- სამედიცინო სერვისების ხარისხის გაუმჯობესება - აუცილებელი სტანდარტული სამედიცინო მკურნალობა, არსებითი კლინიკური გზა და აუცილებელი სამედიცინო კვლევები და საკვლევი გარემო ექიმებისათვის.
- სამედიცინო რისკების მართვა - სამედიცინო პრაქტიკის მონიტორინგი, ადმინისტრაციის მიერ შესყიდულ წამლებზე დეტალური მონიტორინგი სამედიცინო შეცდომების მინიმალიზაცია (მაგ. ცდომილებები, არაკეთილსინდისიერი პრაქტიკა) და პრობლემის ანალიზი.
- ბიზნეს პროცესების გაუმჯობესება - პროცესების გამარტივება და დაჩქარება და სტანდარტული და პროფესიული პროცესების დაყოფა.
- ინფორმაციის გამოყენება - ინფორმაციის გაფართოება და ცოდნის გაზიარების გარემო (დაფუძნებული ‘’საჭიროა რომ იცოდე’’, ‘’საჭიროა რომ გააკეთო’’ ბაზაზე) და საბოლოო მომხმარებლის კომპიუტერირების (EUC) ხელშეწყობა.

ცოდნა და ზრდა

ბოლო BSC არეალი მოიცავს აზრს "რა შეგვიძლია ვისწავლოთ და როგორ შეგვიძლია გავზარდოთ". ეს არეალი შეიძლება ადვილი ჩანდეს, მაგრამ არსებობს უფრო ღრმა პრობლემები. ახალი როლები და მოვალეობები მოითხოვს დაკომპლექტებას და ასევე პერსონალის მხრიდან მღელვარებას შეიძლება ქონდეს ადგილი (მაგალითად, "ეს არ არის ჩემი საქმე, ეს სხვისი გასაკეთებელია"). ეს არეალი მკაცრად დამოკიდებულია ხელმძღვანელობის განზრახვებზე და ყველა თანამშრომელი უნდა მოიაზრებოდეს სამედიცინო მკურნალობისა და მარეგულირებელი საკითხების მცოდნედ. გუნდი ფოკუსირდა შემდეგზე:

- პერსონალის პროფესიონალიზმის გაუმჯობესება - პროფესიული ცოდნის გაზიარება, ელექტრონული ინფორმაციის შეგროვება და გარემოს ანალიზი.
- პასუხისმგებლობისა და მოვალეობების ოპტიმიზაცია - მოვალეობებისა და პასუხისმგებლობების გადაცემის მხარდაჭერა და ოპტიმიზაცია და ინფორმაციული გარემოს შესაფერისი დაცვა.
- უწყვეტი განათლება - ცოდნის სტატუსის მართვის დანერგვა, სიახლეების გაზიარება ჰოსპიტალის მასშტაბით, სწავლის შესაძლებლობის გაზრდა და გარემო ცვლილებებზე სწრაფი რეაგირება და მოქნილობა.

რისკების მართვა

შესაფერისი რისკების მართვის დასადგენად, მნიშვნელოვანია მოსამზადებელი ფაზა. სავალდებულოა შემდეგი ღონისძიებების გატარება:

- ტექსტის სტანდარტიზირება (დაავადების სახელწოდება ან აბრევიატურა) - სამედიცინო ფორმულირება ყველა განყოფილებაში სხვანაირი იყო. მაგ. „HT„ შეიძლებოდა ყოფილიყო „ჰიპერტენზია“ (სისხლის მაღალი წნევა), ან ჰიპოტენზია (სისხლის დაბალი წნევა).
- მსოფლიო მასშტაბით ნორმირებული დაავადების დასახელების ცვლილება - თითქოს ადვილია, მაგრამ ძალიან რთულია ყველა სამედიცინო განყოფილების მიხედვით სახელის შეცვლა. აუცილებელია, ყველა მსოფლიო სტანდარტების შესაბამისი იყოს.
- სამედიცინო პროცესების სტანდარტიზირება - თითოეული სამედიცინო განყოფილება დამოუკიდებლად მოქმედებდა და იყენებდა მასზე მორგებულ სამედიცინო პროცესებს. ყველამ უნდა გამოიყენოს სტანდარტული პროცესები.
- პაციენტის ისტორიის უნიფიცირება - თავდაპირველად, გუნდმა აღმოაჩინა რომ თითოეული სამედიცინო განყოფილება ერთი პაციენტისათვის ძალიან ბევრ თავისებურ ჩანაწერს აკეთებდა. ჩანაწერი კი უნდა ყოფილიყო ერთგვარი.
- მედიკამენტების დასახელებების სტანდარტიზირება - ერთი და იგივე დაავადებისათვის არსებობს სხვადასხვანაირი წამლები მსგავსი

დასახელებებით, მაგ. მკერდის კიბოს სამკურნალოდ გამოიყენება ტაქსოლი (პაკლიტაქსელი) და ტაქსოტერე (დოკატაქსელი), ამ შემთხვევაში სტანდარტიზება დამაბნეველი გახდებოდა.

თუ ფორმულირების სტანდარტიზაცია არ შესრულდება, ელექტრონული სამედიცინო ჩარტის სისტემების ლექსიკონიც ვერ დაინერგება და ეს შეიძლება გახდეს სამედიცინო შეცდომების მიზეზი. რის შემთხვევაშიც, დაავადების სახელი და შესაბამისი ზრუნვა ნამდვილად ვერ იქნება სისტემის შესაბამისი. თუ სამედიცინო პროცესების სტანდარტიზაცია არ სრულდება, HIS ხდება სამართავად საკმაოდ რთული და საჭიროებს ინდივიდუალურ მიდგომას. ასეთი სისტემა იქნება ძვირი და გახდება ადამიანური შეცდომების მიზეზი. ეს აქტოვობებები კარგად კონტროლირებადია PO6, PO7, PO9-ის მიერ და COBIT-ში აპლიკაციების კონტროლით.

IT-ის გავება

რა თქმა უნდა IT-მ შეიძლება შეამციროს ისეთი რისკები, როგორიცაა დაავადებების ურთიერთ დამოკიდებულების შემოწმება, მედიკამენტების უკუჩვენება, კლიენტის/პაციენტის კმაყოფილება, სამედიცინო შეცდომები და არასწორი წამლებისა და საოპერაციო ხარჯების მონიტორინგი. მაგრამ, რა ხდება სხვა IT რისკ-ფაქტორების დროს? მაგალითად, შეიძლება თუ არა სამედიცინო ინსტრუმენტების (PC) სტერილიზაცია მდუღარე წყალში? (მხოლოდ ახლახანს დაიწყეს ბითუმად მოვაჭრეებმა გასტერილებადი ინსტრუმენტების მიწოდება). რა მოხდება თუ MRSA (ბაზისური ეპიდემიოლოგია - მეთიცილინზე რეზისტენტული (Staphylococcus aureus) ინფექცია გავრცელდება? ელექტრომაგნიტურმა ტალღამ (Wi-Fi) შეიძლება შეაფერხოს ზუსტი სამედიცინო აღჭურვილობის მოქმედება. თუ ლოკალური ქსელის (LAN) სადენები უერთდება ტერმინალებს, ასეთი ქსელები შეიძლება დავირუსდეს. დენის უკმარისობის შემთხვევაში რა შეიძლება მოხდეს? რთულია ქაღალდზე არსებული პაციენტის ისტორიის მოპარვა, მაგრამ შიდა (ავტორიზებული) პერსონალისათვის ადვილია ელექტრონული სამედიცინო სქემური მონაცემების მოპარვა. გარდა ამისა, თუ

ექიმი ვერ ამუშავებს PC-ს სწრაფად, რა შეიძლება მოხდეს? თუ ექიმს შეჰყავს არასწორი დაავადების სახელი ან მონაცემები, რა მოხდება? თუ არ არსებობს სისტემის აღდგენის შესაბამისი პროცესი, რა მოხდება? IT-ისათვის დღეში 24 საათი, წელიწადში 365 დღე ოპერაციული რისკების მართვა ფაქტიური გარემოებაა.

პირველი ეტაპის შეჯამება

IT რისკსა და ოპერაციულ რისკს აქვთ ურთიერთდამოკიდებულება. და ეს შეიძლება ორმაგად სასარგებლოც კი იყოს რისკების შემცირებასა და უკვე არსებულ რისკ-ფაქტორში. IT, ბიზნეს პროცესები და ადამიანური ფაქტორები ერთდროულად უნდა განიხილებოდეს. გარდა ამისა, თუ ვინმეს სურს გაზარდოს ღირებულება, რისკებიც გაიზრდება. თუ სანდო რისკების მართვის გარემო დამკვიდრდება, შეიქმნება ღირებულება. რისკებისა და ღირებულების დაშორება შეუძლებელია.

ამიტომ ორგანიზაციას დაჭირდა აშკარად გამოეყო კლინიკური და IT რისკების მართვის სუბიეტები და ობიექტები, განესაზღვრა შესაფერისი სისტემური მოთხოვნები და ახალი ბიზნეს პროცესები, მკაფიოდ განესაზღვრა ტექნიკური პარამეტრების ინდიკატები და დაედგინა შესაფერისი ახალი ბიზნეს და IT მართვის/კონტროლის პროცესები.

ეს ამოცანები რომ შეესრულებინა, ორგანიზაციამ შექმნა შემდეგი ჰოსპიტალის ინფორმაციული სისტემების (HIS) ინტეგრირებული გუნდები:

1. გადაწყვეტილებების მიღების ხელმძღვანელი კომიტეტი - ამ კომიტეტის წევრები იყვნენ ტოპ-მენეჯმენტის წევრები და სხვა გუნდის ლიდერები.
2. სისტემის ინტეგრაციისა და ბიზნეს პროცესის რესტრუქტურიზაციის (BPR) ხელშემწყობი გუნდი - ამ გუნდებს დაემატა ჯგუფის ლიდერები და ქვე-ლიდერები. ამ სამუშაო ჯგუფებმა დაასრულეს ახალ IT გარემოზე დაფუძნებული ახალი ბიზნეს პროცესების დიზაინი და რეალიზება. როგორც ამ პროექტის კონსულტანტმა, ავტორმა განსახილველად წარმოადგინა HIS მოთხოვნათა სპეციფიკაცები, ტიპიური HIS ფუნქციები და ტექნოლოგიური ოპერაციების თანმიმდევრულობის გრაფიკები.ამ გუნდის ფარგლებში ჩამოყალიბდა შემდეგი სამუშაო ჯგუფები:

- ექიმთა სამუშაო პროცესის ინოვაციების სამუშაო ჯგუფი
- ექთნების სამუშაო პროცესის ინოვაციების სამუშაო ჯგუფი
- პალატების სამუშაო პროცესის ინოვაციების სამუშაო ჯგუფი
- მედიცინასთან დაკავშირებული (მაგ.ბუღალტერია) საკითხების პროცესის ინოვაციების სამუშაო ჯგუფი

3. სისტემის ინტეგრაციის საკონტროლო ჯგუფი - ამ ჯგუფის წევრები იყვნენ ლიდერები და ქვე-ლიდერები. ეს გუნდი აკონტროლებდა შემდეგ ჯგუფებს:
   - შიდა სისტემის განყოფილება
   - სისტემის განვითარების ვენდორები.

კლინიკური და ინფორმაციული რისკების მართვის სუბიექტებს/ობიექტებს შორის სხვაობა

რისკების მართვის სუბიექტი/ობიექტი, დასაწყისში შერეულად იყო აღწერილი, ახლა კი საჭიროა მისი განცალკევება, რის შემდეგაც უნდა გაირკვეს რომელი მხარე (მაგ. ექიმები, ექთნები, სამედიცინო პერსონალი, IT განყოფილების პერსონალი) რაზე არის პასუხისმგებელი რისკების მართვისათვის, იმის მიხედვით თუ ვის რა ადგილი უჭირავს (მაგ. დაგეგმვის ფაზა, დიზაინის ფაზა, განვითარების ფაზა, დანერგვის ფაზა, ოპერაციული ფაზა).

რატომ იქნა გამოყენებული COBIT

ჰოსპიტალის რისკების მართვის ბუნებრივი დონე იყო 1. თითქმის ყველა შემთხვევაში, ჰოსპიტალი და მისი პერსონალი ძალიან სერიოზულად რეაგირებდა რაიმე შემთხვევაზე, სანამ მიხვდებოდნენ IT რისკების მართვის აუცილებლობას, მათი მართვის სტილი არ იყო დაგეგმილი.

იმის გამო რომ ჰოსპიტალისთვის კრიტიკული საკითხი იყო შესაფერისი, კარგად ორგანიზებული, ეფექტური და ქმედითი რისკების მართვის დამკვიდრება, რადგან HIS ძალიან კომპლექსურია და მისი ოპერირებისათვის გადამწყვეტია. ჰოსპიტალის პერსონალი დროში იყო შეზღუდული და რისკების მართვის ცოდნაც არ გააჩნდათ.

აქედან გამომდინარე, საჭირო იყო სწრაფი გაანალიზება და IT მართვის დანერგვის აუცილებლობა.

შედეგად, შეირჩა COBIT 4.1 და წარმატებითაც დამტკიცდა, თუ გავითვალისწინებთ იმას თუ როგორი შეზღუდული დროის ინტერვალში დანერგა ჰოსპიტალმა IT რისკებთან დაკავშირებული მართვა/კონტროლი. ჰოსპიტალის გუნდმა შეისწავლა COBIT დეტალურად, რომ გამოევლინათ რა იყო გასაკეთებელი IT-სთან დაკავშირებული რისკების სამართავად.

COBIT როგორც საცნობარო მასალა (რისკების მართვის თვალსაზრისით)

COBIT 4.1 პროცესი PO1: სტრატეგიული IT გეგმის განსაზღვრა ძალიან მნიშვნელოვანი იყო, რადგან ჰოსპიტალმა მიმართა ბიზნეს-IT ტექნოლოგიების სწორად განაწილებას. (PO1.1). მოცემული სტატია აღწერს სხვა მნიშვნელოვან COBIT

4.1 პროცესებს, რომლებიც ჰოსპიტალმა განახორციელა IT-სთან დაკავშირებულ რისკების მართვაზე, რომელიც თითოეულ ფაზაშია დაშლილი.

დაგეგმვის ფაზა

1. კონტროლის გარემოს ელემენტების განსაზღვრა IT შესაბამისობისათვის, ჰოსპიტალის ფილოსოფიასთან და ოპერაციულ სტილთან მიმართებაში, როგორც აღწერილია PO6.1. PO6.2 კორპორაციული IT რისკებისა და კონტროლის ჩარჩო-ში, PO6.3 *IT პოლიტიკის მართვა,* PO6.4 პოლიტიკა, სტანდარტი და პროცედურების დანერგვა და PO6.5 IT მიზნებისა და მიმართულების კომუნიკაციის გათვალისწინება. აქამდე, ექიმებს, ექთნებს, მედიცინის მუშაკებსა და ტოპ-მენეჯმენტს შორის კომუნიკაცია არც ისე მყარი იყო. ჯგუფებს შორის არ ტარდებოდა ოფიციალური შეხვედრები. HIS პროექტის დანერგვით, ამ ჯგუფებს შორის ოფიციალური შეხვედრები რეგულარული გახდა, კომუნიკაციის გაუმჯობესებასთან ერთად.
2. PO7 IT ადამიანური რესურსების მართვა - ეს პროექტი ნერგავდა სრულიად ახალ სისტემებს; აქედან გამომდინარე, ადამიანური რესურსების მართვა (HRM) ძალიან მნიშვნელოვანი იყო, განსაკუთრებით PO7.3 როლების დანაწილებით, რაც მეტი ახალი პასუხისმგებლობა და როლი განისაზღვრებოდა, მით მეტი ახალი

მოვალეობების აუცილებლობა გაჩნდებოდა. მაგ. ახალი მედიკამენტები, მკურნალობის მეთოდები და კლინიკაში შემოსვლები მუდმივად მოძრაობაშია. აქედან გამომდინარე ამის შეფასება და ლექსიკონების განახლება HIS-ში ახალი ძალიან მნიშვნელოვანი დავალება იყო. დაზღვევის საკითხებიც ხშირად განახლებადია, მნიშვნელოვანია ასევე სამედიცინო მკურნალობის ხარჯების ტაბულის სისტემის განახლებაც. PO7.4 პერსონალის მომზადება, - IT- უსაფრთხოებასთან დაკავშირებული სასწავლო პროგრამა და ინფორმირებულობა მნიშვნელოვანი იყო, და PO 7.5 მნიშვნელოვანი იყო ცალკეული პირების დამოკიდებულებაც. პაციენტის საქმის ჩანაწერები დელიკატური პირადი ინფორმაციაა; ამიტომ ყველა თანამშრომელმა უნდა გაიგოს და იცოდეს მონაცემთა უსაფრთხოების მნიშვნელობა. თუ პაციენტის საქმისწარმოების მონაცემები დარღვეულია, ჰოსპიტალმა შეიძლება დაკარგოს საზოგადოების ნდობა, გარდა ამისა, განიცადოს პოტენციური ფინანსური ზარალი სასამართლო პროცესების გამო.

3. PO9 IT რისკების მართვა და შეფასება - რა თქმა უნდა ამ კონტროლის მიზნები იყო მთავარი გასაღები. აუცილებელი იყო PO9.1 IT რისკების მართვის ჩარჩო, PO9.2 რისკების კონტექსტის დაწესება, PO9.3 მოვლენის იდენტიფიკაცია, PO9.4 რისკების შეფასება PO9.5 რისკზე რეაგირება და PO 9.6 რისკების სამოქმედო გეგმის მონიტორინგი. პროექტის წევრებმა გააანალიზეს რისკების მართვის ჩარჩოსა და პროცესების მნიშვნელობა. შედეგად მათ დაგეგმეს პროცესები და შეუდგნენ მათ დანერგვას. მათ ასევე ჩამოაყალიბეს სამედიცინო რისკების მართვის, ფინანსებისა და IT ორგანიზაცია.
4. PO10 პროექტის მართვა- PO10.9 არ უნდა დაგვავიწყდეს პროექტის რისკების მართვა. PO10.11 პროექტის ცვლილების კონტროლი და PO10.13 პროექტის შესრულების გაზომვა. მნიშვნელოვანია ანგარიში და მონიტორინგი. ცხრილი, ხარჯი, ხარისხი და რისკების კრიტერიუმი მთავარი გასაღებია. მაგ. ერთი ფაზიდან მეორეში გადასასვლელი დრო მკაცრად განსაზღვრა ტოპ-მენეჯმენტმა, ასე რომ პროექტის გადავადება შეუძლებელი იყო. ხარჯების დაზოგვისათვის, სისტემის დამუშავება (ბიზნეს პროცესები) დარეგულირდა და უფრო გამარტივდა. ასე რომ თავიდან იქნა

აცილებული ზედმეტად საქონლის მორგება კლიენტების კონკრეტული მოთხოვნების გათვალისწინებით; ხარისხიანი და მაღალი დონის რისკების კრიტერიუმის მისაღწევად მთლიანი ჰოსპიტალის პერსონალი იყო ჩართული და განმეორდა პროტოტიპის შექმნა.

შემუშავებისა და განვითარების ფაზა

1. AI1 ავტომატური გადაწყვეტილებებლის გამოვლენა- AI1.2 რისკების ანალიზის ანგარიში რისკების მართვის მნიშვნელოვანი რესურსი იყო. რომ დაედგინათ, რისკების მართვის სტატუსის ანალიზის ბევრი მაჩვენებელი გამოვლინდა და მოგვარდა,შესაბამისი რაოდენობრივი დონეების მაჩვენებლები იქნა გაწერილი და პერსონალს დაევალა ამ მაჩვენებლების გაზომვა.
2. ოპერაციის გააქტიურება და გამოყენება - მნიშვნელოვანია იმის გარანტია რომ სისტემასთან დაკავშირებულ ყველა ადამიანს შეეძლოს სისტემის დამუშავება და ოპერირება. ამიტომ, ამ პროექტს ადრეულ ეტაპზევე მიეწოდა კლავიატურის სწავლების პროგრამული უზრუნველყოფა, ყველას, ვინც ნაკლებად იცოდა. და სისტემის შესამოწმებლად და ახალი პრობლემების გამოსავლენად ბევრჯერ გამოიცადა.
3. მონტაჟი და გადაწყვეტილების აკრედიტება და ცვლილებები - რთული პერიოდი იყო, რადგანაც დადგენილი დრო ახლოვდებოდა. მომზადების გარეშე AI7.1 მიერთებული AI7.9-ზე შეიძლება არ ჩამჯდარიყო ვადებში. გარკვეული ვადების განმავლობაში ბევრი წინააღმდეგობა იყო მოსალოდნელი. ამიტომაც, გადამწყვეტი იყო სარეზერვო ღონისძიებებისთვის და განმეორებითი სიძნელეებისათვის საპასუხო მზადყოფნა.

ოპერირების ფაზა

- DS1 მომსახურების დონეების განსაზღვრა და მართვა - DS1.1 მომსახურების დონის მართვის ჩარჩო ოპერირებს ჰოსპიტალის ფარგლებში. აუთსორსინგი არ ყოფილა გამოყენებული. ამ ფაქტზე დაყრდნობით ჩამოყალიბდა ჩარჩო. მაგალითად, გარანტირებული უნდა იყოს მაღალი მომსახურების დონე კლინიკური დანიშნულების მქონე სისტემებისათვის. DS1.2 მომსახურების განმარტება, 24

საათიანი და წელიწადში 365 დღის განმავლობაში მნიშვნელოვანია კლინიკისათვის, მაგრამ არა სამედიცინო პერსონალისათვის. ბიზნეს მახასიათებლების მიხედვით უნდა განისაზღვროს სერვისის-დონის ჩარჩო. DS1.5 აუცილებელია მომსახურების დონის მიღწევის ანგარიში და მონიტორინგი უწყვეტი სრულყოფისათვის.

- DS3 ტექნიკური პარამეტრებსა და ფუნქციონალური აქტივობის მართვა - ამ პროცესში აუცილებელი იყო ყველა საკონტროლო მიზანი (DS3.1-დან DS3.5-მდე) მაგალითად, სისტემური შეფერხება არ არის დაშვებული კრიტიკული კლინიკური სისტემებისთვის. ამიტომ, მომზადდა და შემოწმდა ბევრი სარეზერვო სისტემა.
- უწყვეტი მომსახურების გარანტია - HIS-ისთვის ეს რა თქმა უნდა მნიშვნელოვანია. ბევრი საგანგაშო საკითხი, კატასტროფა და ა.შ გამოვლინდა და საპასუხო მოქმედება განიხილა და განისაზღვრა.
- სისტემური უსაფრთხოების გარანტია - პაციენტთა მონაცემები რა თქმა უნდა გადამწყვეტია და ამიტომაც უმაღლესი დონის უსაფრთხო გარემო უნდა იქნას გარანტირებული. PO7-ის დამუშავებით უმაღლესი დონის ინფორმაციული დაცვის გარემო შეიქმნა და დადგინდა შეფასება და უწყვეტი მონიტორინგი.
- DS7 მომხმარებლის სწავლება და დატრენინგება - ექიმებმა უნდა გამოიყენონ პერსონალური კომპიუტერები. თუ არ იყენებენ, საკმარისად ვერ დაზოგავენ დროს პაციენტებისათვის და შეცდომებიც დაფიქსირდება. მნიშვნელოვანია მუდმივი სწავლება. სამედიცინო გამოკვლევის შემდეგ, ექიმებს უტარდებოდათ ტრენინგი თუ როგორ გამოეყენებიათ ახალი სისტემები ეფექტურად.
- DS11 მონაცემთა მართვა - ესეც DS5-ვით მნიშვნელოვანია, უმაღლესი დონის მონაცემთა მართვა იქნა პიველ რიგში დაყენებული. როგორც უკვე აღინიშნა, ახალი მედიკამენტები და სამედიცინო მკურნალობა მუდმივად ვითარდება. აუცილებელია ლექსიკონების შენახვა. განისაზღვრა მონაცემთა რეზერვისა და დაცვის პროცედურები და დაიწყო მათი პრაქტიკაში გამოყენება.
- DS12 ფიზიკური გარემოს მართვა - მნიშვნელოვანია DS12.2 ფიზიკური უსაფრთხოების გაზომვა და DS12.3 ფიზიკური ხელმისაწვდომობა. ტერმინალებისა და IT-ისთან დაკავშირებული მოწყობილობების რაოდენობა მკვეთრად გაიზარდა.

ასევე გაიზარდა სერვერების რაოდენობაც. ხელახლა დამონტაჟდა ტერმინალური დაცვის ადგილები, და პერსონალზე გადანაწილდა პასუხისმგებლობები. ასევე შემოწმდა და ამოქმედდა სასერვერო ოთახები.

ტექნიკური პარამეტრების/მონიტორინგის მაჩვენებლების იდენტიფიცირება

ახალი ბიზნეს და IT პროცესები სათანადოდ უნდა გაიზომოს და შემოწმდეს. COBIT ME1 პროცესების დამუშავებით, დადგინდა ჩამოთვლილი მაღალი დონის მაჩვენებლები, თითოეული დაბალანსებული შედეგების ცხრილის არეალისათვის (BSC), ასე რომ ისინი შეიძლება გამოყენებულ იქნას ჰოსპიტალის აღმასრულებელი პირების ანგარიშებად (ME1.5). ამ მაჩვენებლებით შეფასდა IT ტექნიკური მახასიათებლები და მოექცა დაკვირვების ქვეშ (ME1.1, ME1.3 and ME1.4). ამგვარად ჰოსპიტალის ხელმძღვანელობას შეუძლია დროულად გაითავისოს ჰოსპიტალის მიმდინარე სტატუსი და გადადგას შემდეგი ნაბიჯები (ME1.6).

1. მაღალი დონის მაჩვენებლები:
    - ხელმძღვანელობის ხედვებთან დაკავშირებული:
        - პირადი ინფორმაციის მონაცემთა დაცვის უსაფრთხოების დონე
        - სამედიცინო მომსახურების დონის ამაღლება და დაცვა
        - სამედიცინო შეცდომების მინიმიზაცია (ექიმის დაუდევრობა)
        - სწრაფი რეაგირება საზოგადოების საჭიროებებზე
        - ინფორმაციის გაზიარება ჰოსპიტალისა და საზოგადოებას შორის
        - კადრების კვალიფიკაციისა და ცოდნის ამაღლება
        - ახალი გამოწვევები
    - მისიის გაცნობა:
        - თითოეულ დაწესებულებაში ჯგუფებს შორის თანამშრომლობა (სისტემები და ინფორმაცია)

- ჯანდაცვის, სამკურნალო და საექთნო საქმის სრული მხარდაჭერის სისტემა
- კარგი დამხმარე სისტემების ჩამოყალიბება და შემდეგ ექიმების კვლევითი საქმიანობის გარემოს შექმნა და ჯანდაცვის საიტებზე ამ შედეგების განთავსება.

2. მომხმარებლის კმაყოფილების მაჩვენებლები:

- პაციენტის კმაყოფილების დონის გაუმჯობესება:
  - სამედიცინო მკურნალობის რეზერვაციის პროცენტული რაოდენობა
  - ლოდინის დრო სამედიცინო გამოკვლევისთვის
  - მკურნალობის საშუალო პერიოდები (კლასიფიცირებულია დაავადების მიხედვით)
  - მიწოდებულ ინფორმაციაზე კმაყოფილების დონე
  - პაციენტების მიერ კონსულტაციის მიღების რაოდენობის გაზრდა
  - კმაყოფილების დონე, რომელიც მოჰყვა კონსულტაციას
  - ინფორმირებული თანხმობის აღსრულების პროცენტული რაოდენობა
- თანამშრომლობის დონის გაუმჯობესება ჰოსპიტალებსა და კლინიკებს შორის(ჯანდაცვის ზონა):
  - კლინიკებს შორის, ექიმთან მიმართვიანობით პაციენტების რაოდენობა ჯანდაცვის ზონის ფარგლებში.
  - იგივე ჯანდაცვის ზონაში, კლინიკაში გადაყვანილ პაციენტთა თანაფარდობა (პაციენტები, რომელთაც შეუძლიათ იმკურნალონ მათ სახლთან ახლოს მდებარე კლინიკაში)
  - კლინიკაში გადაყვანილ პაციენტებზე სწრაფი რეაგირების მოხდენა

- თანამშრომელი კლინიკების კმაყოფილების დონე
- მაღალი დონის სამედიცინო აღჭურვილობის გამოყენება
- სანდო სამედიცინო ტესტების თანაფარდობის გაზრდა

- ადგილობრივი ხელისუფლების კმაყოფილების გაუმჯობესება:
  - ადგილობრივი ხელისუფლების მიერ, საყოველთაო ჯანდაცვის პროგრამების მიღების რაოდენობა
  - ჰოსპიტალში სასწრაფო დახმარების მიღება
  - გადაუდებელი პაციენტების მიღება (ჰოსპიტალიზაცია)
- საზოგადოების საერთო კმაყოფილების გაუმჯობესება:
  - პაციენტები საშუალო ჯანდაცვის ზონის გარეთ
  - სამედიცინო მომსახურების ზონაში მცხოვრები ადამიანების კმაყოფილების დონე

3. ფინანსებთან დაკავშირებული მაჩვენებლები:
   - ზრდა:
     - დაზღვეულთა მხრიდან, სამედიცინო მკურნალობის ხარჯების ანაზღაურების მოთხოვნების რიცხვი და რაოდენობა.
     - მოთხოვნის დაგვიანებისა და დაგვიანებული ანაზღაურების რაოდენობა
     - სამედიცინო მკურნალობისა და მოთხოვნის კორესპოდენციის სიზუსტე
     - მოგების სტატუსი (კლასიფიცირებულია სამედიცინო და სხვა განყოფილებების მიერ)
   - ალბათობა:

- ბილინგის ოდენობა და ღირებულება (პაციენტებიდან, დაავადებებიდან და დღეებიდან გამომდინარე)
- მედიკამენტების ღირებულების ოდენობა
- შესყიდვის ღირებულება და ბილინგის ოდენობა
- მიწოდების ღირებულება და სამედიცინო დანადგარების რაოდენობა
- საწოლის მოხმარების რაოდენობა (კლასიფიცირებულია სამედიცინო განყოფილების მიერ)

- ლიკვიდურობა
  - დაუხარისხებელი შემოსავლის აღდგენა
  - იჯარის ეფექტური გამოყენება
  - ფიქსირებული აქტივების რაოდენობა
  - საფონდო ბრუნვა
  - ჩაწოლილი საქონელი
- სტაბილურობა
  - პერსონალის ხარჯების რაოდენობა (მაგ. სამედიცინო სასულიერო მსახურები)
  - აუთსორსინგის გამოყენება
  - ფიქსირებული ღირებულების რაოდენობა

4. შიდა პროცესებთან დაკავშირებული მაჩვენებლები
   - სამედიცინო მომსახურების ხარისხის გაუმჯობესება.
     - პაციენტთა რაოდენობა, ვინც მიმართა კლინიკებს
     - დისპერსიული ანალიზის შედეგი

- დღეში ჰოსპიტალიზაციის საშუალო რაოდენობა (კლასიფიცირებულია დაავადების მიხედვით)
- ექიმების ნაშრომთა და პრეზენტაციების რაოდენობა, ექიმთა მიერ გაცემული დანიშნულებების რაოდენობა
- ქირურგიული ოპერაციების რაოდენობა
- მნიშვნელოვანი სამეანო სტატუსი
- სპეციალიზებული ექთნების რაოდენობა
- ავადმყოფის გეგმიური მიღებისა და გაწერის რაოდენობა

- სამედიცინო რისკების მართვა
  - სამედიცინო შეცდომათა შემთხვევები (ცდომილებები, არაკეთილსინდისიერი პრაქტიკა)
  - ჰოსპიტალის ინფექციების შემთხვევები
  - წოლისგან მიღებული დალურჯების შემთხვევები(ნაწოლები)
  - შესრულებული მითითებების რაოდენობა სამედიცინო მენეჯმენტზე
  - გვერდითი მოვლენების შესახებ ინფორმაციის მიწოდების რაოდენობა
- ბიზნეს პროცესების გაუმჯობესება
  - ჰოსპიტალის ბიზნეს პროცესების მოცულობის თანაფარდობა
  - მექანიკური პროცესების, ავტომატურ ბიზნეს პროცესებთან თანაფარდობა
  - სტანდარტული პროცესების, ავტომატურ ბიზნეს პროცესებთან თანაფარდობა
  - პროფესიული პროცესების თანაფარდობა რომელსაც აქვს სისტემური მხარდაჭერა

- ინფორმაციის დამუშავება
    - ინფორმაციისა და ცოდნის გაფართოებისა და დამუშავების თანაფარდობა
    - კომპიუტერების სიმძლავრის დამუშავების თანაფარდობა
    - მომხმარებლის მიერ კომპიურეტული აპლიკაციების დამუშავების სტატუსი (EUC)

5. სწავლისა და ზრდის მაჩვენებლები
    - პერსონალის პროფესიული ზრდის გაუმჯობესება
        - ჰოსპიტალში ინტელექტუალური საკუთრებისა და პროფესიული ცოდნის გაფართოების სტატუსი
        - ელექტრონულად დაგროვილი ცოდნის სტატუსი და მისი გამოყენება
        - პერსონალის ინფორმაციულობის დონე
    - როლებისა და პასუხისმგებლობების ოპტიმიზაცია:
        - მნიშვნელოვანი ინფორმაციული მხარდაჭერა გადაწყვეტილებების მიღების პროცესში
        - გადაწყვეტილების მიღების პროცესების გამჭვირვალობის გაუმჯობესება
        - ორგანიზაციული როლებისა და პასუხისმგებლობების გადანაწილება და ინფორმაციული სისტემებისათვის ავტორიზაციის მინიჭება
        - ინფორმაციული უსაფრთხოების სტატუსი
    - მუდმივად სწავლის მსურველი ორგანიზაცია:

- ინტელექტუალური საკუთრების და პროფესიული ცოდნის გამოყენების სტატუსი
- პერსონალის განათლება, სასწავლო პროგრამები და მონაწილეობის სტატუსი
- ცოდნის გასაზიარებელი სისტემების განახლებისა და გაფართოების სტატუსი

მარეგულირებელი საკითხების გათვალისწინება

რეგულაციები მუდმივად ახლდება, ამიტომაც, მოქნილობა და სწრაფი რეაგირება ძალიან მნიშვნელოვანია. მაგალითად, ძალიან აქტუალურია შემდეგი საკითხები:

- დიაგნოსტიკის საპროცესო კომბინაციაზე (DPC) რეაგირება (იაპონიის მარეგულირებელი საკითხები)(მსგავსია დიაგნოსტიკურ ჯგუფთან/პერსპექტიული გადახდის სისტემასთან(DRG/PPS))- სათანადო რეაგირებისათვის, დეტალური ხარჯების ანალიზის ფუნქციები გაერთიანდა HIS-ში. ამან შესაძლებელი გახადა თითოეული პაციენტისა და დაავადების ხარჯების კონტროლი.
- მთავარი რეგიონალური ჰოსპიტალის კოორდინირებული სახელმწიფო ჯანდაცვა - ძალიან მნიშვნელოვანია ინფორმაციის გაცვლა ერთ ზონაში მყოფ ჰოსპიტალისა და კლინიკებს შორის. ასევე უმნიშვნელოვანესი საკითხია პაციენტის საქმის ჩანაწერების მონაცემთა დაცვა.
- სამედიცინო ხარჯების ელექტრონული უწყისების წარმოდგენა (სამედიცინო დაზღვევისათვის) - ამ ფუნქციების ინტერფეისი განსაზღვრულია იაპონიის შრომის, ჯანდაცვისა და სოციალური უზრუნველყოფის სამინისტროს მიერ.(MLHW), ამიტომაც საჭიროა სწრაფი და სწორი რეაგირება.

სათანადო რეაგირების მიზნით, აუცილებელია გარე მოთხოვნების შესაბამისობის უზრუნველყოფასთან დაკავშირებული კონტროლი ME3. მსგავსი ახალი რეგულაციების შესასრულებლად, მენეჯმენტმა მხარი უნდა აუბას რეგულაციებს (ძირითადად MLHW-ს).

ამისათვის საჭიროა HIS-ის განახლება. ზოგჯერ, MLHW ითხოვს სამედიცინო მკურნალობის ჩანაწერებისა და მასთან დაკავშირებული პროცესების გარე აუდიტს. ამისათვის კი ჰოსპიტალი მზად უნდა იყოს.

აპლიკაციების კონტროლი

როგორც COBIT 4.1-შია აღწერილი, აპლიკაციების კონტროლიც მნიშვნელოვანია რისკების სამართავად. ამისათვის უნდა ჩატარდეს შესაბამისი IT აუდიტი:

1. AC1 წყაროს მონაცემთა მომზადება და ორიგინალთან შესაბამისობის დადგენა- პაციენტთა ჩანაწერები ძალიან მნიშვნელოვანია. ''საჭიროა იცოდე, საჭიროა გააკეთო''-ბაზაზე დაყრდნობით, მონაცემთა მომზადებაზე უფლებამოსილია შესაბამისი პერსონალი. წვდომაც, ისევე როგორც ID ბარათები და პაროლები, კატეგორიის მიხედვით აქვთ ექიმებს, ექთნებსა და სამედიცინო პერსონალს. წვდომის უფლების განახლებისათვის ზრუნავს HR მენეჯმენტი.
2. AC2 წყაროს მონაცემთა შეგროვება და შესვლა - პაციენტთა მკურნალობის შესახებ გადაწყვეტილებების ხელმისაწვდომობა დაშვებულია მხოლოდ ექიმებისათვის. ყველა სხვა პერსონალს ეკრძალება პაციენტთა ჩანაწერების შეყვანა ან განახლება. პაციენტის შესახებ ყველა სიახლე იწერება და წაშლისგან დაცულია. ასევე იწერება და პერიოდულად მოწმდება ყველა შესვლა.
3. 3. AC3 ზუსტი, სრული და უტყუარი შემოწმება- სამედიცინო საქმეების ექსპერტი პერსონალი ამას ყოველთვის ამოწმებს, თავიანთ ცოდნასა და გამოცდილებაზე დაყრდნობით. მაგალითად, პაციენტის საქმის ჩანაწერების აუდიტს კანონი ითხოვს. პაციენტის საქმის შესახებ ჩანაწერებთან ერთად, HIS-ში IT აუდიტორის როლი ძალიან მნიშვნელოვანი ხდება.
4. AC5 შედეგების გადახედვა, შეთანხმება და შეცდომის მართვა-მაგალითად, ფინანსურ ლიკვიდურობაზე პირდაპირ აისახება დაზღვეული პაციენტების მიერ, მკურნალობის ხარჯების ანაზრაურების მოთხოვნა. პაციენტებისათვის მკურნალობის საფასურის გამოთვლა, ახლა უკვე ავტომატურად ხდება, ასე რომ

შემცირდა მედიცინის მუშაკთა საქმე, რადგან ისინი ახლა უფრო მეტად კონცენტრირებული მოთხოვნების სიზუსტის შემოწმებაზე არიან.

შედეგები

COBIT 4.1 ძალიან სასარგებლო გამოდგა IT-სთან დაკავშირებული რისკების მართვის/ კონტროლის დაწესების გამო.

IT მიზნები კავშირში უნდა იყოს ბიზნესის მიზნებთან და IT მონაცემთა გამოტანა თავისთავად ვეღარ იქნება საბოლოო შედეგი. აქედან გამომდინარე, საჭიროა უწყვეტი მონიტორინგი და შეფასება ბიზნესის თვალსაზრისით. დაწესდა ამ ჰოსპიტალის IT რისკების მართვის ათვლის წერტილი. თუმცა რაღაც საკითხები მაინც მოითხოვს მუდმივ გაუმჯობესებას. მაგალითად, სამედიცინო დაწესებულებების ზოგიერი IT რისკები არ არის გარკვეული. ამიტომ, აუცილებელია რისკების მართვის სისტემის მუდმივად გაუმჯობესება. ხშირად გამოდის ახალი წამლები, ინერგება ახალი სამედიცინო მკურნალობის მეთოდები და ახალი რეგულაციები, რომლებიც რისკების მუდმივად მართვას მოითხოვენ. (Masatoshi Kajimoto)

2.7. IT რისკების მართვა ბანკში

ეს სიტუაცური ანალიზი რეალური მაგალითია, თუ როგორ გამოიყენება COBIT-ი IT რისკების სამართავად მსოფლიო ბანკში. COBIT ეფექტურად იქნა გამოყენებული რისკების სამართავად ტექნოლოგიების გუნდებს შორის, რათა დარწმუნებულიყვნენ რომ შესაფერისი IT მართვისა და IT უზრუნველყოფის პროცესი ნამდვილად დამუშავდებოდა ბანკებს შორის.

ზოგადი ინფორმაცია

მოცემულ სიტუაციაში ბანკი არის გლობალური კონგლომერატი 50-ზე მეტ ქვეყანაში არსებული ოპერაციებით და მსოფლიო მასშტაბით 125 ათასზე მეტი დასაქმებული თანამშრომლით. მსოფლიო მასშტაბით არიან ბანკის ტექნოლოგიური ჯგუფები რათა

დაეხმარონ ბიზნესის გლობალურ ხაზებს. IT გუნდები მოიცავენ განვითარების ცენტრებს, რომლებიც ბანკის ნაწილია და ასევე გარე რესურსების მოზიდვით მოვაჭრეებსა და IT ინფრასტრუქტურისა და სერვისების მხარდამჭერ ტექნოლოგიურ ბექ-ოფისებს. ბანკს ჰქონდა უამრავი მართვისა და გარანტიის მოდელი და პროცესები სხვადასხვა რეგიონებიდან და ლოკაციებიდან იმართებოდა სხვადასხვა გუნდების მიერ. აქედან გამომდინარე, ძირითადი გამოწვევა ტექნოლოგიურ გუნდებს შორის, იყო საერთო მართვისა და უზრუნველყოფის პროცესების შექმნა.

ტექნოლოგიური მართვისა და უზრუნველყოფის პროგრამა შემუშავებული იყო რისკების მართვის ჩარჩოს მიხედვით, ეფექტური რისკების და კონტროლის მართვის უზრუნველსაყოფად.

შემუშავდა ჩარჩო არსებული რისკებისა და კონტროლის მართვის სისუსტეების სამართავად:

- შეუსაბამო პროცესები შესაბამისობის შეფასებისა და ტესტირებისთვის
- ცალკეული კონტროლის საცავის ნაკლებობა, რის შედეგადაც კონტროლის გაორმაგება ხდება
- მკაფიო, რისკების შეფასების დასრულების განმეორებითი პროცესების ნაკლებობა

მოსალოდნელი იყო ახალი ჩარჩოს შექმნა, ტექნოლოგიური გუნდების გასააქტიურებლად რათა გასაგები ყოფილიყო არსებითი ოპერაციული რიკსები და მათი გავლენა ფართო ორგანიზაციებზე, შემდეგი პუნქტების მეშვეობით:

- მიმართვის სფეროები, სადაც რისკები არ იყო ეფექტურად კონტროლირებადი
- ტექნიკური აღმასრულებლებისათვის, უფლების მინიჭება, რათა ეჩვენებინათ მარეგულირებელი პასუხისმგებლობების ეფეტურობა.
- საერთო პლატფორმის გამოყენება რეგიონისა და ქვეყნის მასშტაბით ყველა მარეგულირებელი მოთხოვნების შესახებ
- ტექნოლოგიური რისკების ეფექტურად შეაფასება და სუსტი მხარეების კონტროლი, რომლებსაც შეიძლება გავლენა მოეხდინა ბიზნესზე.

- რეგიონებსა და ოფისებში სტანდარტული პროცედურების დანერგვა, რათა უზრუნველყოფილიყო თანმიმდევრულობა და არ მომხდარიყო ანგარიშების დუბლირება.

COBIT-ის გამოყენება

სამართავმა ჯგუფმა გადაწყვიტა გამოეყენებინა COBIT როგორც სტანდარტული ჩარჩო. პროფესიონალების გუნდმა -რისკების, IT უსაფრთხოებისა და შტატების Sarbanes-Oxley-ს აქტის პროცესის ექსპერტებთან ერთად- შეადგინეს ჩარჩოები და ნიმუშები. გუნდმა თავიდან სამ არეალზე იმუშავა:

- ჩარჩოს გამოყენების განსაზღვრა - სამიზნე ჩარჩოს კონტროლი(COF)
- ''ორგანიზმების'' სტანდარტული განმარტების იდენტიფიკაცია, რომლის მიხედვითაც რისკები და კონტროლი უნდა შეფასებულიყო-მთავარი ორგანიზმის მართვის მოდელი.
- რისკების მართვის პროცესის იდენტიფიცირება- რისკებისა და კონტროლის შფასება (RCA)

მომდევნო სექციაში არწერილია, ახალი რისკების მართვის ჩარჩოს პროცესის განვითარების მთავარი ნაბიჯები.

საფეხური 1 COF-ის განსაზღვრა

COBIT-ის მიერ დადგინდა COF-ი, რისკების ეფექტური ტექნოლოგიების ოფისებისა და საწარმოს საუკეთესო სტანდარტული პრაქტიკის დასაკავშირებლად .COF-ის დაგდგენისას სამი მიზანი გამოიკვეთა:

1. გამოყენებული უნდა იქნას როგორც რისკებისა და კონტროლის ეფექტურად შემფასებელი ინსტრუმენტი, ტექნოლოგიების ფარგლებში.
2. გამოყენებული უნდა იქნას როგორც ანგარიშის ჩარჩო, იმის საჩვენებლად თუ როგორ აკმაყოფილებს ტექნოლოგიები რეგულაციების მოთხოვნების ანგარიშს, Sarbanes-Oxley-ის ჩათვლით.

3. გამოყენებული უნდა იქნას როგორც სასწრაფო დახმარება, რომ აამუშაოს მართვის გარანტიები.

COF-ს განსახორციელებელი ნაბიჯებისათვის COBIT-ის გამოყენება მოიცავდა:

- ძირითადი რისკების იდენტიფიცირება - ადრე არსებული ინფორმაციის საფუძველზე განისაზღვრა და გაჩერდა პირველი დონის ძირითადი რისკები. ამან გამოავლინა ტექნოლოგიებთან, ოპერაციებთან, ხალხთან, სამართლებრივ და მარეგულირებელ, ფინანსურ ანგარიშებთან, ფინანსურ დანაშაულთან, ბრენდთან და ცვლილებებთან დაკავშირებული თანდართული რისკები.
- II დონის რისკების იდენტიფიცირება- II დონეზე, ძირითადი რისკები კიდევ უფრო გაფუჭდა. როგორც მაგალითად, ''ძირითადი ტექნოლოგიური რისკები'' გაირღვა:
  - IT სისტემების დიზაინი/ტესტირების შეუსაბამობის გამო.
  - IT სისტემებზე წვდომის არქონის გამო
  - IT უსაფრთხოების სიმცირის გამო
- კონტროლის მიზნების იდენტიფიცირება - თითოეული მე-2 დონის რისკისათვის, კონტროლის მიზნები იდენტიფიცირებული იქნა COBIT-ის გამოყენებით. ცხრილი 2.1 აჩვენებს მე-2 დონის რისკების შდარებას კონტროლის მიზნებთან, თითოეული ტექნოლოგიური რისკების გამოვლენით.

ცხრილი 2. 1 ***მე-2 დონის რისკების შედარება***

IT სისტემების დიზაინი/ტესტირების შეუსაბამობა	IT სისტემებზე წვდომის არქონა	IT უსაფრთხოება

• PO2 ინფორმაციის არქიტექტურის განსაზღვრა • PO3 ტექნოლოგიური მიმართულების განსაზღვრა • PO8 ხარისხის მართვა • PO10 პროექტების მართვა • Al 1 ავტომატური გადაწყვეტილებების იდენტიფიკაცია • AI2 პროგრამული უზრუნველყოფის აპლიკაციის მიღება და შენახვა • Al3 ტექნოლოგიური ინფრასტრუქტურის მიღება და შენახვა • Al6 ცვლილებების მართვა • Al7 გადაწყვეტილებების და აკრედიტების უფლება და დაყენება	• AI2 პროგრამული უზრუნველყოფის აპლიკაციის მიღება და შენახვა • Al3 ტექნოლოგიური ინფრასტრუქტურის მიღება და შენახვა • Al5 IT რესურსების მიწოდება • DS1 მომსახურების დონეების განსაზღვრა და მართვა • DS3 ტექნიკური მახასიათებლების მოცულობა და მართვა • DS4 უწყვეტი სერვისის გარანტია • DS8 სერვისის ადგილის მართვა და გარემოებები • DS10 პრობლემის მართვა • DS11 მონაცემთა მართვა • DS12 ფიზიკრი გარემოს მართვა • DS13 ოპერაციების მართვა	• PO2 ინფორმაციის არქიტექტურის განსაზღვრა • PO4 IT პროცესების, ორგანიზაციებისა და ურთიერთობების განსაზღვრა. • PO9 IT რისკების მართვა და წვდომა • AI2 პროგრამული უზრუნველყოფის აპლიკაციის მიღება და შენახვა • DS5 სისტემური უსაფრთხოების გარანტია • DS11 მონაცემთა მართვა • DS12 ფიზიკრი გარემოს მართვა

საფეხური 1-ის სარგებელი

ამ ჩარჩოების დანერგვამდე, თითოეულ ობიექტს,ორგანიზაციას და ლოკაციას ჰქონდა თავისებური კონტროლის მექანიზმი. COBIT-ი დაეხმარა თითოეული რისკების ტიპის, ცალკეული სიის კონტროლის მართვასა და განვითარებაში COBIT-ის საჭირო კონტროლთან შესაბამისობით.თავის მხრივ, ამან ხელი შეუწყო თითოეული ტიპის რისკების დადასტურებაში, რამაც ატესტაციისა და ანგარიშგების პროცესებზე, მთავარ აღმასრულებლებში ნდობა გამოიწვია. მოგვიანებით, განვითარდა რისკების შეფასების პროცესი,რისკებისა და კონტროლის დასადგენად. ამან გარანტია მიცა იმას, რომ

შესაფერისი კონტროლი გადანაწილდებოდა ძირითადი რისკებისა და მე-2 დონის რისკების გადასაფარად.

საფეხური 2 - ობიექტების იდენტიფიცირება რისკებისა და კონტროლის სამართავად.

განისაზღვრა მართვის მოდელის ძირითადი ერთეულები, რათა მოეცვა IT აგების ბლოკები, რის მიხედვითაც უნდა წარმოდგენილიყო რისკებისა და კონტროლის შეფასება. IT აგების ბლოკები ლოგიკურადაა ერთმანეთთან დაკავშირებული, რომ ტექნოლოგიური ოფისის კანონის ფარგლებში, ანგარიშგების მიზნით, უზრუნველყოს რისკებისა და კონტროლის შეფასება მთლიანი მხარდაჭერის სერვისებისათვის.

IT აგების ბლოკები განისაზღვრა, როგორც:

- პროცესის ორგანიზმები - ეს წარმოადგენს IT გარემოს მხარდასაჭერ, საკონტროლო და სამართავ პროცესს. ნებისმიერი კონრტოლის საკითხი პროცესის ორგანიზმებში, გავლენას იქონიებდა ბევრ IT სერვისზე. მაგ. კონტროლის ცვლილება არის ყოვლისმომცველი უმეტეს IT სერვისებზე.
- სერვისის მხარდაჭერის ორგანიზმები - პროცესებისა და ტექნოლოგიური ორგანიზმების დაკავშირება შესაძლებლობას იძლევა შესრულდეს უწყვეტი რისკებისა და კონტროლის შეფასება მხარდაჭერის სერვისებისათვის, მაგ. ტექნოლოგიურ ერთეულებს შორის რისკების ინტერფეისი, მომსახურების დონის რისკები უწყვეტი IT სერვისისათვის და ინტეგრაციის რისკები (განყოფილებებს შორის განკარგვის მართვა).
- ტექნოლოგიური ორგანიზმები - წარმოადგენს ‘’ტრადიციულ’’ IT კომპნენტებს. მაგ. სერვისებს, აპლიკაციებს, ქსელებსა და დაცვის მექანიზმებს (firewalls). ძირითადი ტექნოლოგიური ერთეულების იდენტიფიცირებისათვის, რომლებიც უზრუნველყოფენ თითოეული სერვისის მხარდაჭერას, გამოყენებული იქნა სერვისის რუკები და RCA პროცესი.
- პროექტის ორგანიზმები - მანამდე,სანამ ზედა 20 სერვისზე პროექტის ორგანიზმები გავლენას ვერ ახდენს, ძალიან მნიშვნელოვანია რომ ნებისმიერი კონტროლისა და რისკების შესახებ ინფორმაციის მიღება ოპერატიული გახდეს.ეს მიზნობრივ

სახელმწიფო კონტროლს საშუალებას მისცემს შეაფასოს, კავშირი იქონიოს და შეატყობინოს რეალურ დროში ახალი განვითარების / პროექტის ცვლილებები.ზედა 20 სერვისის ზოგიერთი მაგალითი მოიცავს ბანკომატის დაკავშირებას და საბაზისო საბანკო მომსახურების მხარდაჭერის სერვისებს.

ბანკის მეთოდი IT მომსახურების განსასაზღვრად, პირდაპირ კავშირშია IT მომსახურების კატალოგთან. როგორც მისი IT სერვისის კატალოგის ნაწილი, 20-ვე მასზე დამყარებული მთავარი სერვისიც ინდენტიფიცირებული იქნა მხარდაჭერის სერვისებისათვის.თითოეული მხარდაჭერის სერვისისათვის შეიქმნა მომსახურების რუკა. მომსახურების რუკები ასახავენ ტექნოლოგიურ კომპონენტებს რომლებიც დაკავშირებულია ერთმანეთთან უწყვეტი მომსახურების უზრუნველსაყოფად.

თითოეული პროცესის ორგანიზმი და ტექნოლოგიური ორგანიზმი განსხვავებულია და შეიძლება იყოს დაკავშირებული მრავალრიცხოვან დამხმარე სერვისებთან. შედეგად, ძირითადი ორგანიზმების მართვის მოდელი მოქნილია და შეუძლია როგორც საჭიროა, მხარი დაუჭიროს დამატებითი IT სერვისების გაფართოებას. ერთეულებს შორის კავშირები საშუალებას იძლევა მოახდინოს აგრეგაცია ბოლომდე შევსებული მომსახურების რისკების პროფილის უზრუნველსაყოფად, რაც მნიშვნელოვანია მენეჯმენტისათვის და სხვადასხვა კლასტერების მართვისათვის საერთო ერთეულებში.

საფეხური 2-ის სარგებელი

ახალი რისკების მართვის პროცესის დანერგვამდე, თითოეულ რეგიონს, ქვეყანს და ა.შ. ბანკის საკუთარი რისკებისა და კონტროლის მატრიცები ჰქონდა. რისკებისა და კონტროლის შეფასება ეფუძნებოდა, რეგიონის ფარგლებში რისკების მართვაზე მომუშავე თითოეული გუნდის გაგებას, და არ იყო ფოკუსირებული "საბოლოო შედეგზე", კერძოდ, კლიენტების მომსახურების რისკების გავლენაზე. COBIT-ი დაეხმარა ძირითადი სერვისების გამოვლენაში, რომელსაც გავლენა ჰქონდა ბიზნესსა და მომხმარებელზე და კონტროლზე ახდენდა ფოკუსირებას.აღნიშნული რისკების გამოვლენის შემდეგ, COBIT- ის ფარგლებში დაფუძნებული კონტროლის მექანიზმები შეჩერდა და შეფასდა კონტროლის ეფექტურობისათვის,კლიენტთა მომსახურებაზე

გავლენის იდენტიფიცირებით.ამან გამოიწვია შემთხვევების საერთო რაოდენობის შემცირება და მომხმარებელთა/ან მომხმარებელთა მომსახურებაზე გავლენის შემთხვევების შემცირება.

საფეხური 3 - RCA პროცესების განსაზღვრა და დანერგვა

პროცესის მიმოხილვა ცხრილი 2.2-ში ხაზს უსვამს რისკების შეფასების 5 საფეხურს.

თითოეული საფეხურის ფარგლებში, ძირითადი ამოცანები იქნა გამოვლენილი. განისაზღვრა რიგი ინსტრუმენტების/პროცესების თანაშემწეებისა, რისკების შეფასების აღწერილობის, კალენდარული დაგეგმარებისა და მიწოდებისათვის, და გამოიკვეთა ცხრილი 2.2-ში.

ცხრილი 2. 2 ***RCA პროცესის ნაბიჯები***

ჩართულობა	• დაინტერესებული მხარეების ჩართვა • ბიზნეს მიზნების ან მომსახურების დონის შეთანხმების გაგება • RCA საზღვრები
მომზადება	• შესაბამისი ზოგადი ინფორმაციის მიღება • ძირითადი რისკების იდენტიფიცირება • RCA-ს მოსამზადებელი ნიმუში
შეფასება	• დაინტერესებული მხარეების დისკუსიაში ჩართვა • უკიდურესი რისკების შეფასება • კონტროლის შეფასება • მოსალოდნელი რისკების შეფასება
დასრულება	• RCA- დასრულება • ღია რისკებისათვის მაკორექტირებელი მოქმედების შესახებ თანხმობა

	• მაკორექტირებელი ქმედებებისა და მოსალოდნელი რისკების შესახებ დამტკიცების მიღება
ატვირთვა	• RCA-ს ატვირთვა ინსტრუმენტებში (tool) • კონტროლების შეყვანა კონტროლის საცავში • მოძველებული რისკების ნარჩენების ამოღება

საერთო RCA პროცესის განვითარების მიზანი იყო იმის უზრუნველყოფა რომ რისკების ანალიზი და კონტროლი გუნდების მასშტაბურად თანდმევი იყო . ერთი ინსტრუმენტი იყო მარტივი Excel ნიმუში, რომელმაც განსაზღვრა რისკებისა და კონტროლის ინფორმაციის მიღება. შემდეგ თარგი გაიყინა რათა ყველა ობიექტს შეძლებოდა მისი გამოეყენება, ნიმუში განისაზღვრა შემდეგი ძირითად ინფორმაციის მისაღებად:

- ძირითადი და მე-2 დონის რისკები
- Sarbanes-Oxley-კონტროლის მოთხოვნების ცნობარი
- კონტროლის მფლობელი
- კონტროლის შეფასება-ეფექტურობა,არაეფექტურობა
- ქმედებები ეფექტური კონტროლის დანერგვის მიზნით
- დახურვის სამოქმედო დეტალები-მოქმედების მფლობელი, სამიზნე თარიღი

შაბლონები შეივსო რისკებისა და კონტროლის მფლობელის მიერ და გადაეგზავნათ ცენტრალური რისკების გუნდებს გადასახედად. რის შემდეგაც ისინი შეყვანილი იქნა რისკების მართვის ინსტრუმენტებში,რათა დაეწყოთ დასახური ქმედებები და ღია რისკების შესახებ მოხსენებები. თითოეული მიმაგრებული იყო:

- ერთეულის მფლობელებთან - როგორც წესი RCA- ის მფლობელები
- რისკების მფლობელებთან - რისკზე პასუხისმგებელი მფლობელები
- კონტროლის მფლობელებთან - კონტროლის ეფექტურობის შენარჩუნებაზე პასუხისმგებელი მფლობელები

- ქმედების მფლობელებთან - არაეფექტური კონტროლის შედეგად გამოვლენილი ქმედებების მფლობელები

საფეხური 3-ის სარგებელი

სასწავლო პროგრამების მეშვეობით, ტერმინები: ობიექტის/RCA მფლობელები, რისკების მფლობელები, კონტროლის მფლობელები და მოქმედების მფლობელები განმარტებული იქნა პასუხისმგებლობის, ანგარიშვალდებულების, კონსულტირებისა და ინფორმირებულობის (RACI) გრაფიკის გამოყენებით. (იხ. ცხრილი 2.3 მაგალისთისათვის.) პასუხისმგებლობები ასევე შედარებული იქნა პერსონალის სამუშაოს აღწერასთან და წარმოდგენის შეფასების კრიტერიუმთან.

ცხრილი 2. 3 ***RACI მაგალითის გრაფიკი***

რისკები/კონტროლი/ქმედება	CEO	COO	რისკების ოფიცერი	ობიექტის ხელმძღვანელი	უსაფრთხოების უფროსი	HR უფროსი
ფიზიკური უსაფრთხოების მართვა	I	C,I	C,I	A	R	
ფიზიკური უსაფრთხოების ინციდენტებზე ანგარიშგება	I	A	C,I	C,I	R	C,I

ცხრილი 2.3-ის მაგალითი განმარტავს, რომ იმის მიუხედავად რომ ობიექტის ხელმძღვანელი ანგარიშვალდებული იყო ფიზიკური უსაფრთხოების მიმდინარე გეგმის უზრუნველყოფაზე, ძირითადი ოპერაციების ოფიცერი (COO) ანგარიშვალდებული იყო ინციდენტებსა და მასთან დაკავშრებულ ქმედებებზე. დასაქმებულთა და მიმწოდებელთა ნებისმიერ ქმედებაზე ადამიანური რესურსების განყოფილება (HR) იყო ინფორმირებული.

საფეხური 4 - დაინტერესებული მხარეების სწავლება

ერთ-ერთი ძირითადი გამოწვევა, ყველა დაინტერესებული მხარისთვის, რომლებსაც გააჩნიათ სხვადასხვა ბექგრაუნდი და რისკებისა და პროცესების სხვადასხვაგვარი გაგება, მთლიანი პროცესების ახსნა იყო სხვადასხვა ლოკაციებზე. აღნიშნულ

გამოწვევასთან გამკლავება სხვადასხვა დონეზე სხვადასხვა ტრენინგის პროგრამების უზრუნველყოფით მოხერხდა. ამან მოიცვა:

- რისკების ექსპერტების შექმნა (როგორც წესი, გამოცდილებითა და სერთიფიკატებით, როგორიცაა სერტიფიცირებული ინფორმაციული სისტემების აუდიტორი [CISA®] და სერტიფიცირებული ბუღალტერი [CA]) რეგიონებსა და ოფისებში, რომლებიც ტრენინგ-ტრენერის პროგრამის ფარგლებში მომზადდნენ. ასეთი რესურსები გამოყენებული იყო დაინტერესებული მხარეების მომზადებაში.
- აუდიენციისათვის ტრენინგის ჩატარება რისკების ექპერტების მიერ. ობიექტის მფლობელებისათვის, მარტივი პროცესის გადასახედად, უზრუნველყოფილი იქნა სავალდებულო ტრენინგი კომპიუტერის გამოყენებით. რისკებისა და კონტროლის მფლობელებისათვის, ტრენინგი დეტალურად, მაგლითებისა და ტესტების გამოყენებით იქნა ჩატარებული, როგორც ოთახებში და სხვადასხვა ლოკაციებზე, ასევე ვებ-სესიებით.
- შეთავაზება, როგორც აუცილებელი სწავლების პროგრამის ნაწილი , ინფორმირებულობის ტრენინგის სესია, რომელმაც ახსნა პროცესები და უზრუნველყო კავშირები და კონტაქტები ადგილობრივი რისკების ექპერტებისათვის ორგანიზაციის ფარგლებში, დამატებითი ინფორმაციისა და მითითებებისათვის.
- სემინარის მოწყობა დაინტერესებულ მხარეებში შესაბამისი ინფორმაციის გასავრცელებლად. რასაც უნდა გამოეწვია ნებისმიერი რისკების შეფასების პროცესი.ტრენინგის რესურსები სხვადასხვა ლოკაციებზე იქნა გამოყენებული კონტროლის თვითშეფასების (CSA) გასამარტივებლად.
- მოვალეობის აღწერის მოდიფიცირება და განვითარების პროცესების წარმოდგენა სპეციფიკური ამოცანებისა და რისკების კონტროლის გასათვალისწინებლად.

საფეხური 4-ის სარგებელი

Top-Down (ზემოდან ქვემოთ მიდგომა)-მეთოდის მიხედვით, რისკების მართვის მნიშვნელობა მისაღები და ორგანიზაციის ყველა დონეზე ძალიან ეფექტური იყო.

საფეხური 5 - ანგარიშგების ინსტრუმენტი

თითოეული ობიექტის რისკებისა და კონტროლის საცავთა შესანახად გამოყენებული იქნა მარტივი ცხრილი. ობიექტებს შორის, რისკების ჯგუფის წევრებმა გამოიყენეს Excel-ის ცხრილები რისკების, ქმედებისა და ა.შ. გასაკონტროლებლად, თუმცა იყო მოთხოვნა, რომ ყოფილიყო ცალკეული, საერთო მონაცემთა ბაზის საცავი,რათა შენახულიყო ორგანიზაციის მასშტაბის რისკები და კონტროლები. შესაბამისად, განვითარდა ინსტრუმენტი რათა შესაძლებელი ყოფილიყო ორგანიზაციის ყველა ერთეულის ინფორმაციის ერთად შენახვა. ამან შესაძლებელი გახადა:

- "სერვისთან" დაკავშირებული ყველა რისკების მონიტორინგი
- ყველა რისკებისა და კონტროლის ინფორმაციის საცავის ცენტრალიზება
- RCA პროცესში განსაზღვრული და შეთანხმებული ყველა ქმედების მონიტორინგი
- ქმედებებისა და ინციდენტების დახურვის მონიტორინგი
- უფროსი აღმასრულებლებისათვის რისკების შესახებ ანგარიშის შედგენა, რომელიც დაფუძნებული იყო სპეციფიკურ მოთხოვნებსა და რისკების დონეებზე
- მარეგულირებლების მოთხოვნების საფუძველზე ანგარიშგება, საერთო, ერთი რისკებისა და კონტროლების მონაცემთა ბაზიდან.

საფეხური 5-ის სარგებელი

რისკების, კონტროლისა და ქმედების ცალკეული საცავი გამოყენებული იყო სადაზღვევო გუნდების მიერ მათ ანგარიშებში, რომელიც განკუთვნილი იყო ინფორმაციული სამსახურის უფროსისათვის (CIO) და ასევე ტექნიკური მონაცემების მაღალ დონეზე კონტროლისათვის.

შედეგები

თითქმის ორი წელი დასჭირდა ახალი პროცესის სრულ განვითარებასა და დანერგვას. სანამ მთავარი ჯგუფი იყო პასუხისმგებელი პროცესების განვითარებაზე, სალოკაციო რისკების რესურსები იყო ხელშემწყობი ორგანო განხორციელებისათვის, სწავლებისათვის და ა.შ. მას შემდეგ რაც სხვადასხვა ლოკაციებზე გეგმის შემსრულებლები გახდნენ გუნდის ნაწილი, მათი უკუკავშირის მეშვეობით ხდებოდა სასურველი ცვლილებები და შესწორებები, რამაც ხელი შეუწყო პროცესის ვადების გაუმჯობესებას.

ამ ინიციატივის სხვა რეალური სარგებელი მოიცავდა:

- პროცესის დანერგვამდე, არსებობდა 500-ზე მეტი ერთეული, რომლებისთვისაც ხდებოდა რისკებისა და ჯკონტროლების მონიტორინგი. ეს რიცხვი ოპტიმიზირებულია 100 ერთეულამდე, რაც შესაძლებელი გახდა ძირითადი ობიექტების მართვის მოდელის დანერგვის შედეგად.
- პროცესის დანერგვამდე, იდენტიფიცირებული იყო 1000-ზე მეტი კონტროლი. რაოდენობა შემცირდა როგორც კი თითოეული კონტროლი დაუკავშირდა COBIT-ის ჩარჩოს. მსოფლიო დონეზე, კონტროლის რიცხვი შემცირდა დაახლოებით 350-მდე.
- აღნიშნული პრაქტიკა დაეხმარა ბანკს ემართა რისკებისა და კონტროლების პროცესი Sarbanes-Oxley-სა და სხვა მარეგულირებლის მოთხოვნების შესაბამისად.
- პროცესების საცავი, ინსტრუმენტებში, დაეხმარა თანმიმდევრობის შენარჩუნებაში. ეს გაკეთდა რისკების ჯგუფის ფარგლებში, ცალკე ქვე-ერთეულის შექმნით, რათა შეემოწმებინათ თითოეული RCA-ს ხარისხი, სანამ შეიტანდნენ RCA ინტრუმენტებში.

ტრეინინგების ძირითადი პაკეტი, რისკების ჯგუფის მიერ, განიხილებოდა, როგორც ერთერთი ყველაზე მნიშვნელოვანი და ღირებული პროდუქტი, რომელიც

განსაზღვრული იყო აუდიენციისთვის. მაგალითისთვის, 15 წუთიანი სასწავლო პაკეტი ყველა ობიექტის მფლობელისათვის (როგორც წესი, ესენი იყვნენ ცენტრალური ხელმღვანელები თითოეულ ქვეყანასა და რეგიონში) შემუშავდა და დაინერგა ელექტრონული სწავლების პორტალის გამოყენებით, როდესაც დეტალური პროცესის სასწავლო პაკეტი შემუშავდა რისკებისა და კონტროლის მფლობელებისათვის. (Jitendra Barve)

თავი 3. კომპანიის ინფორმაციული სისტემების რისკების ანალიზისა და მართვის უახლესი საშუალებების დანერგვის პერსპექტივა და გამოწვევები საქართველოში

3.1. ინფორმაციული უსაფრთხოების რისკების მართვის მექანიზმები

ინფორმაციულ და საკომუნიკაციო საკითხებთან დაკავშრებული სტანდარტების და ინფორმაციული უსაფრთხოების პოილიტიკის შემუშავება და მისი გატარება საჯარო სექტორში არის საჯარო სამართლის იურიდიული პირის (სსიპ) იუსტიციის სახლის მონაცემთა გაცვლის სააგენტოს მიზანი. სააგენტო არეგულირებს კრიტიკული ინფორმაციული სისტემის სუბიექტებს, რომელიც განსაზღვრულია საქართველოს მთავრობის დადგენილება №312-ით. მონაცემთა გაცვლის სააგენტომ შეიმუშავა ისეთი პოლიტიკები, როგორიც არის საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“, მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება №2 „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ და მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება №7 „ინფორმაციული აქტივების მართვის წესების დამტკიცების შესახებ“ და სხვა.

გარდა საჯარო სექტორისა, ინფორმაციულ სისტემებთან დაკავშირებული რეგულაციები ვრცელდება კერძო სექტორზეც, თუმცა ამ შემთხვევაში მხოლოდ კომერციულ ბანკებს აქვთ გარკვეული ვალდებულებები. საქართველოს კანონმდებლობის შესაბამისად, კომერციული ბანკების მარეგულირებლ ორგანოდ განისაზღვრა საქართველოს ეროვნული ბანკი. საქართველოს ეროვნული ბანკის მიერ ვრცელდება შემდეგი რეგულაციები: საქართველოს ეროვნული ბანკის პრეზიდენტის ბრძანება №47/04 „კომერციული ბანკების მიერ საოპერაციო რისკების მართვის შესახებ დებულების დამტკიცების თაობაზე“ და საქართველოს ეროვნული ბანკის პრეზიდენტის ბრძანება

№56/04 „კომერციული ბანკების კიბერუსაფრთხოების მართვის ჩარჩოს დამტკიცების შესახებ“. რაც შეეხება კერძო სექტორში არსებულ კომპანიებს, რომლებიც არ ეწევიან საბანკო საქმიანობას, საქართველოს კანონმდებლობის შესაბამისად არ გააჩნიათ ინფორმაციული სისტემების მართვასა და უსაფრთხოებასთან დაკავშირებული ვალდებულებები.

საქართველოში არსებული კომპანიების ინფორმაციული სისსტემების რისკების ანალიზისა და მართვის მიდგომების შესწავლის მიზნით განხორციელდა თვისებრივი კვლევა. კვლევის მიზანს წარმოადგენდა საქართველოში მოღვაწე კომპანიების წარმომადგენლებთან არასტანდარტულ კითხვარზე დამყარებული ჩაღრმავებული ინტერვიუს საფუძველზე, პრაქტიკაში გამოყენებული ინფორმაციული სისტემების რისკების შეფასებისა და მართვის მიდგეომების იდენტიფიცირება. ანკეტაში არსებული კითხვების უმრავლესობა იყო ღია ტიპის და მოითხოვდა რესპოდენტებისგან არსებული სიტუაციის ანალიზსა და ხშირ შემთხვევაში კომპანიის კრიტიკულად კონფიდენციალური ინფორმაციის გაზიარებას, რის გამოც გამოკითხულთა უმრავლესობამ მოითხოვა ანონიმურობისა და ინფორმაციის კონფიდენციალურობის დაცვა.

კითხვარისა და ინტერვიუს დახვეწის მიზნით, სრულმასშტაბიანი გამოკითხვის ჩატარებამდე განხორციელდა პილოტური ინტერვიუ, რის საფუძველზეც დადგინდა კითხვარის ვალიდურობა.

კვლევის არეალალად განისაზღვრა თბილისი და შეირჩა ისეთი კომპანიები, რომლებსაც სათავო ოფისი აქვთ თბილისის ფარგლებში, ხოლო მათი ბიზნეს ოპერაციები დამოკიდებულია ინფორმაციული ტექნოლოგიების გამოყენებაზე. კვლევაში მონაწილეობის მისაღებად შეირჩა საქართველოში მოღვაწე კომპანიები სხვადასხვა სეგმენტიდან (მცირე - 5-50 დასაქმებული, საშუალო - 50-500 დასაქმებული და მსხვილი ბიზნსი 500+ დასაქმებული) და სხვადასხვა სექტორიდან (ფინანსური, ჰოსპიტალური, სატელეკომუნიკაციო, საკონსულტაციო და ენერგეტიკული). გამოკითხულთა შორის იყვნენ როგორც კერძო, ასევე სახელმწიფო ორგანიზაციების

წარმომადგენლები. სულ განხორციელდა 20 ინტერვიუ, რის საფუძველზეც მოხდა შედეგების ანალიზი და ინტერპრეტირება.

კვლევის შედეგებზე დაყრდნობით შეიძლება ითქვას, რომ სახელმწიფო სექტორში არსებულ კრიტიკული ინფორმაციული სისტემის სუბიექტებსა და სხვა ორგანიზაციებს გააჩნიათ ინფორმაციული სისტემების რისკების ანალიზისა და მართვის განსაზღვრული, დოკუმენტირებული და პრაქტიკაში დანერგილი მიდგომები. შეიძლება ითქვას, რომ მსგავსს მიდგომებს იყენებენ კომერციული ბანკების 70%-ზე მეტი, თუმცა გვხვდება ბანკებიც, სადაც დღემდე უგულვებელყოფენ ინფორმაციული სისტემების რისკების მართვის თანამედროვე მიდგომებს. საქმე ბევრად უფრო რთულად არის ბიზნესის სხვა სექტორებში, რადგან კომპანიების მხოლოდ მცირე ნაწილი ახორციელებს ინფორმაციულ სისტემებთან დაკავშირებული რისკების ანალიზსა და მართვას. რაც შეეხება მცირე და საშუალო ბიზნესის სეგმენტში არსებულ კომპანიებს, შეიძლება ითქვას, რომ მხოლოდ ერთეულებს აქვთ ინფორმაციული სისტემების რისკების მართვის განსაზღვრული, დოკუმენტირებული და პრაქტიკაში დანერგილი მიდგომები, ხოლო ამ კომპანიების ძირითადი ნაწილი გახლავთ საერთაშორისო ორგანიზაციების წარმომადგენლობები და/ან საქმიანობის სპეციფიკიდან გამომდინარე ჰყავთ მარეგულირებლები, რომელიც ავალდებულებს ამა თუ იმ საერთაშორისო სტანდარტთან შესაბამისობას.

3.2. ინფორმაციული სისტემების რისკების ანალიზისა და მართვის საშუალებები სახელმწიფო ორგანიზაციებში

სახელმწიფო ორგანიზაციაბში მოიაზრება საჯარო სამართლის იურიდიული პირები და ის ორგანიზაციები, რომელთა საქმიანობაც განისაზღვრება საქართველოს კანონმდებლობით. სწორედ ასეთ ორგანიზაციებზე ვრცელდება სსიპ მონაცემთა გაცვლის სააგენტოს მიერ შემუშავებული რეგულაციები. აღნიშნული რეგულაციები დაფუძნებულია ISO 27000 საერთაშორისო სტანდარტებზე და მოიცავს ინფორმაციული

უსაფრთხოების მართვის საკითხებს, რომელიც თავის თავში მოიაზრებს ინფორმაციულ სისტემებთან დაკავშირებული რისკების იდენტიფიცირებასა და მართვას. ასეთ ორგანიზაციებში დანერგილი ინფორმაციული უსაფრთხოების მართვის სისტემები მოიცავს კანონმდებლობით გათვალისწინებულ მინიმალურ მოთხოვნებს, მათ შორის ინფორმაციული სისტემების რისკების ანალიზსა და მართვას. ამ მიზნით მათ შეიმუშავეს და დანერგეს რიგი პოლიტიკები და პროცედურები, რაც ითვალისწინებს:

- აქტივების ინვენტარიზაციასა და კლასიფიკაციას.
- საფრთხეებისა და სისუსტეების იდენტიფიცირებას.
- კონტროლის მექანიზმების იდენტიფიცირებას.
- აქტივების შესაბამისად რისკების განსაზღვრას.
- რისკების ანალიზს.
- რისკების შეფასებას.
- რისკის დონის დადგენას.
- გადაწყვეტილების მიღებას სხვადასხვა დონის რისკებთან მობყრობისთვის.
- რისკებთან გამკლავებისთვის კონტროლების შემუშავებასა და დანერგვას.

ზემოთ ხსენებულ პროცესების ინიცირება ხდება წინასწარ განსაზღვრული პერიოდულობით ან მნიშვნელოვანი ცვლილების შემთხვევაში. საბოლოო გადაწყვეტილების მიღება სპეციალურად შექმნილი საბჭოს კრებაზე ხდება, რომლის წევრებიც აუცილებლად არიან უმაღლესი მენეჯმეტის წარმომადგენლები.

3.3. ინფორმაციული სისტემების რისკების ანალიზისა და მართვის საშუალებები ბანკებში

საქართველოში მოღვაწე კომერციულ ბანკები, კანონმდებლობის შესაბამისად, რეგულირდებიან საქართველოს ეროვნული ბანკის მიერ. „კომერციული ბანკების მიერ საოპერაციო რისკების მართვის შესახებ დებულების“ თანახმად ბანკები ვალდებულები

არიან განსაზღვრული ჰქონდეთ რისკების მართვის პროცესის სასიცოცხლო ციკლი, რომელიც უნდა მოიცავდეს:

- რისკების იდენტიფიცირებას, კონტროლის მექანიზმების შემუშავებას და დანერგვას;
- რისკების მონიტორინგს და ანგარიშგებას;
- რისკების შერბილებას(მიტიგირებას) და ნარჩენი რისკების შეფასებას.

აღნიშნული რეგულაცია არ ავალდებულებს ბანკებს ინფორმაციულ სისტემებთან დაკავშირებული რისკების აღნიშნული სქემით დამუშავებას, თუმცა ითვალისწინებენ რა ინფორმაციული სისტემების მნიშვნელობას თანამედროვე ცხოვრებაში და საბანკო საქმიანობაში, ასევე მასთან დაკავშირებული საფრთხეებისა და რისკების მუდმივ ზრდას, მათ უმრავლესობას შემუშავებული აქვთ სპეციალური პოლიტიკები და პროცედურები რომლის შესაბამისადაც ახორციელებენ რისკების მართვას.

ინტერვიუს საფუძველზე დადგინდა, რომ ბანკ 1-ში რისკების ანალიზისა და მართვისთვის გამოყენებული მეთოდოლოგია შეესაბამება ISO 27000 საერთაშორისო სტანდარტებს, ისევე როგორც სახელმწიფოს მიერ მართვად ორგანიზაციებში.

ბანკ 1-ში ინფორმაციული სისტემების რისკების შეფასებას კოორდინირებას უწევს, ასევე სისუსტეებისა და საფრთხეების იდენტიფიცირებას ახორციელებს ინფორმაციული უსაფრთხოების განყოფილება, ხოლო გავლენის შეფასებასა და ალბათობის დათვლას ახორციელებს რისკების მენეჯერი.

ბანკ 2-ში და ბანკ 3-ში ინტერვიუების საფუძველზე გაირკვა, რომ ისინი არამხოლოდ რისკების ანალიზსა და მართვას ახორციელებენ თანამედროვე სტანდარტების შესაბამისად, არამედ მათ დანერგვილი აქვთ ინფორმაციული ტექნოლოგიების კორპორაციული მართვის ჩარჩო COBIT 5-ის შესაბამისად. უკანასკნელი შეფასების შედეგად განისაზღვრა, რომ აღნიშნულ ბანკებში COBIT 5-ის სიმწიფის დონე განისაზღვრებოდა 2 – 3 ქულებს შორის, რაც იმის მაჩვენებელია, რომ პროცესები აღწევს თავის მიზანს და პროცესები როგორც წესი, არის კარგად განსაზღვრული. კითხვაზე, თუ რა დრო დაჭირდათ აღნიშნული მაჩვენებლის მისაღწევად, ორივე ბანკის

წარმომადგენლის პასუხი იყო დაახლოვებით 3 წელი. როგორც გაირკვა მართვის ჩარჩოს დანერგვის ყველაზე რთული ეტაპი შემუშავებული დოკემნტების შესაბამისად პროცედურების აწყობა იყო. თუმცა, პროცესების აწყობიდან რამდენიმე თვეში ორივე ბანკმა შეძლო დაენახათ შედეგი, რაც აისახა ბანკის ფინანსურ შემოსავლებზე, როგორც წარმომადგენლებმა აღნიშნეს „ბანკის ბრუნვა COBIT 5-ის დანერგვის სიმწიფის დონის ზრდის პირდაპირპროპორციულად იზრდებოდა“. კორპორაციული IT მართვის დანერგვის შედეგად ბანკებში შეიცვალა ორგანიზაციული კულტურაც, რაც გამოიხატა იმაში, რომ ბიზნესს გაუჩნდა ხედვა მთლიან პროცესზე და შესაძლებელი გახდა ნებისმიერი საკითხის მარტივად გადაწყვეტა.

მიუხედავად იმისა, რომ ბანკების ძირათი ნაწილი ინფორმაციული სისტემების რისკების ანალიზისა და მართვისთვის იყენებს მსოფლიოში ფართოდ გავრცელებულ სტანდარტებსა და საუკეთესო პრაქტიკებს, ქართულ საბანკო სექტორში მაინც გვხვდება ბანკი 4, სადაც ინტერვიუს საფუძველზე დადგინდა, რომ მათ არ გააჩნიათ ინფორმაციული სისტემების რისკების ანალიზისა და მართვის პრაქტიკა. როგორც ბანკი 4-ის წარმომადგენელმა აღნიშნა ისინი იყენებენ საუკეთესო პრაქტიკებსა და გამოცდილებას ინფორმაციული სისტემების ტექნიკურად გამართული მდგომარების შესანარჩუნებლად, აქვთ ასევე დაცვის თანამედროვე სისტემები და აკმაყოფილებენ მარეგულირებლის მიერ დაწესებულ მოთხოვნებს, თუმცა არ გააჩნიათ დოკუმენტირებული პოლიტიკები და პროცედურები, რის საფუძველზეც მოახდენენ IT რისკების შეფასებასა და მართვას.

3.4. ინფორმაციული სისტემების რისკების ანალიზისა და მართვის საშუალებები დიდ კომპანიებში

კვლევაში მონაწილეობა მიიღო მსხვილი ბიზნესის 6-მა წარმომადგენელმა სხვადსხვა სექტორიდან. მათგან მხოლოდ 2-მა რესპოდენტმა აღნიშნა, რომ მათ კომპანიაში არსებობს ინფორმაციული სისტემების რისკების ანალიზისა და მართვის

დოკუმენტირებული და პრაქტიკაში გამოყენებული მიდგომები. თუმცა ჩაღრმავებული კითხვების დასმის შემდეგ დადგინდა, რომ პროცესები ყოველთვის არ მიმდინარეობს მათივე შემუშავებული პოლიტიკებისა და პროცედურების შესაბამისად. აღნიშნული გამომდინარეობს იქიდან, რომ კომპანიებს არ ჰყავთ შესაბამისი რაოდენობის სპეციალისტები, რათა მუდმივად ხდებოდეს მონიტორინგი და მხარდაჭერა დოკუმენტირებული პოლიტიკებისა და პროცედურების სრული დანერგვისთვის.

დარჩენილი 4 კომპანიის წარმომადგენელმა, რომლებსაც არ გააჩნიათ ინფორმაციული სისტემების რისკების ანალიზისა და მართვის მიდგომები აღნიშნეს, რომ ტექნიკური სპეციალისტების დახმარებით მაქსიმალურად ზრუნავენ IT ინფრასტრუქტურაზე. ისინი ახერხებენ, რომ მათ ინფრასტრუქტურაში დამუშავებული ინფორმაციისთვის არ დაირღვეს კონფიდენციალურობა, მთლიანობა და ხელმისაწვდომობა. რესპოდენტებმა აღნიშნეს, რომ უმაღლესი მენეჯმენტი აზრით ინფორმაციული სისტემების რისკების ანალიზისა და მართვის თანამედროვე სტანდარტებთან შესაბამისობაშ მოყვანის შემთხვევაში, ხარჯი უფრო მეტი იქნება ვიდრე გაუთვალისწინებელი რისკებიდან გამოწვეული ინციდენტებისგან მიღებული ზეგავლენა, რაც პირდაპირ აისახება ფინანსებში.

3.5. ინფორმაციული სისტემების რისკების ანალიზისა და მართვის საშუალებები მცირე და საშუალო კომპანიებში

მცირე და საშუალო კომპანიებში დაახლოვებით ისეთივე მიდგომით აფასებენ ინფორმაციული სისტემების რიკების ანალიზისა და მართვის საკითხს, როგორც დიდი კომპანიების ძირითად ნაწილში. გამოკითხული 10 კომპანიის წარმომადგენლიდან, 8 რესპოდენტმა აღნიშნა, რომ უმაღლესი მენეჯმენტისგან მოდის მხოლოდ მოთხოვნა იმასთან დაკავშირებით, რომ უზრუნველყოფილი იყოს IT-ის გამართული მუშაობა იმ რესურსებით რაც გააჩნიათ. მათ ასევე არ აქვთ არანაირი ვალდებულება მარეგულირებლებისაგან და არ ჭირდებათ ინფორმაციული სისტემების რისკების ანალიზისა და მართვის წინასწარ განსაზღვრული მიდგომები თავიანთი საქმიანობის

სფეროში. სწორედ ამიტომ ისინი უზრუნველყოფენ მხოლოდ ტექნიკური მხარის გამართულად მუშაობას და ამისათვის იყენებენ ფართოდ გავრცელებულ საუკეთესო პრაქტიკებს.

საქართველოში მოღვაწეობენ ისეთი კომპანიებიც, რომლთა მასშტაბებიც თანამშრომელთა რაოდენობიდან გამომდინარე ხვდებიან საშუალო ბიზნესის სეგმენტში, თუმცა საქმიანობის სფეროსა და სხვა მიზეზების გათვალისწინებით მათ აქვთ წინასწარ განსაზღვრული ინფორმაციული სისტემების რისკების ანალიზისა და მართვის დოკუმენტირებული მიდგომები, რომლელიც შეესაბამება თანამედროვე სტანდარტებსა და მარეგულირებლების მოთხოვნებს. საშუალო კომპანია 1-ის წარმომადგენელმა აღნიშნა, რომ მათი ძირითადი საქმიანობა დაკავშირებულია ბარათების პროცესინგთან და ფინანსურ ტრანზაქციებთან, რის გამოც რეგულირდება ისეთი კომპანიების მიერ, როგორიც არის ვიზა და მასტერქარდი. იმისათვის რომ მათ შეძლონ ვიზასთან, მასტერქარდთან და სხვა მსგავს კომპანიებთან თანამშრომლობა, აღებული აქვთ ვალდებულება, დააკმაყოფილონ PSI DSS სტანდარტის მოთხოვნები, რაც ასევე მოიცავს წინასწარ შემუშავებული და დამტკიცებული ინფორმაციული რისკების ანალიზისა და მართვის პროცესებისა და პროცედურების შესაბამისად მოქმედებას.

საშუალო კომპანია 2-ის წარმომადგენელთან ინტერვიუს საფუძველზე დადგინდა, რომ მის კომპანიასაც აქვს ვალდებულება, იყოს ინფორმაციული უსაფრთხოების სტანდარტებთან შესაბამისობაში და დანერგილი აქვთ ISO 27001 ინფორმაციული უსაფრთხოების მართვის სისტემის საერთაშორისო სტანდარტი, რომელიც მოიცავს მოთხოვნებს ინფორმაციული სისტემების რისკების ანალიზსა და მართვასთან დაკავშირებით. საშუალო კომპანია 2 არის ევროპის ერთ-ერთ ქვეყანაში დაფუძნებული ორგანიზაციის წარმომადგენელი საქართველოში, რომელსაც გააჩნია წარმომადგენლობა მსოფლიოს მრავალ ქვეყანაში, ლოკალურად დარეგისტრირებული კომპანიების სახით და თითოეული მათგანის მართვისა და მენეჯმენტის მოთხოვნები მომდინარეობს ცენტრალური ოფისიდან.

თავი 4. დასკვნა და რეკომენდაციები

მრავალ ქვეყანაში არესბული კომპანიების ანალიზის საფუძველზე შესაძლებელია ითქვას, რომ ინფორმაციული სისტემების რისკების ანალიზისა და მართვის უახლესი საშუალებების გამოყენება უმნიშვნელოვანესია ბიზნესუწყვეტობისთვის, კომპანიების მდგრადობისა და ზრდის შესანარჩუნებლად.

საქართველოში განხორციელებული კვლევის საფუძველზე წარმოჩინდა მნიშვნელოვანი ინფორმაცია ადგილობრივ ბაზარზე მოღვაწე კომპანიებთან დაკავშირებით. კვლევამ ცხადყო, რომ საქართველოში მოღვაწე კომპანიების მხოლოდ იმ ნაწილს აქვს განსაზღვრული ინფორმაციული სისტემების ანალიზისა და მართვის მიდგომები, რომლებსაც გააჩნიათ ვალდებულებები მარეგულირებლის მხრიდან.

გარდა ადგილობრივი კომპანიებისა, საქართველოში ასევე მოღვაწეობენ უცხოური კომპანიების წარმომადგენლები, სადაც ორგანიზაციული პრაქტიკიდან გამომდინარე, ცენტრალური ოფისიდან მოდმინარეობს სტანდარტებთან შესაბამისობის მოთხოვნები.

განხორციელებული კვლევის საფუძველზე შეიძლება ითქვას, რომ ინფორმაციული სისტემების რისკების ანალიზისა და მართვის მიდგომების მხრივ საქართველოში არსებულ კომპანიებში ფიქსირდება უკიდურესად დაბალი მაჩვენებლები.

საქართველოში დაფუძნებული კომპანიების უმაღლესი მენეჯმენტი მიჩნევს, რომ მათ არ სჭირდებათ დამატებით ხარჯების გაწევა ინფორმაციული სისტემების რისკების შეფასებისა და ანალიზისთვის, რადგან თვლიან რომ მასთან დაკავშრებული ხარჯები შესაძლებელია აღემატებოდეს იმ რისკების შედეგად გამოწვეულ ხარჯებს რაც შეიძლება მათი რეალიზების შემთხვევაში წარმოიქმნას.

როგორც კვლევიდან გამომდინარე ირკვევა, ასეთი კომპანიების უმაღლესი მენეჯმენტი ვერ აცნობიერებს ინფორმაციული სისტემების კრიტიკულობასა და მნიშვნელობას თანამედროვე ცხოვრებაში წარმატებული ბიზნესის არსებობისათვის. მიუხედავად იმისა,

რომ მათ არასოდეს განუხორციელებიათ ინფორმაციული სისტემების რისკების ანალიზი და შეფასება, თუ რა საფრთხეებს ქმნის და რა შედეგები შეიძლება გამოიწვიოს ინფორმაციულ სისტემებთან დაკავშირებულმა რისკებმა, მაინც თვლიან, რომ მათთვის ინფორმაციული ტექნოლოგიები არ არის მნიშვნელოვანი და არ ღირს მასში ინვესტიციების განხორციელება.

თუ გავითვალისწინებთ მსოფლიოსა და საქართველოში არსებული იმ კომპანიების მაგალითზე მიღებულ გამოცდილებას, რომლებმაც თავიანთ პრაქტიკაში უკვე დანერგეს COBIT და მიაღწიეს სიმწიფის საკმაოდ კარგ მაჩვენებლს, დავინახავთ, რომ COBIT-ის დანერგვით იფარება არა მხოლოდ უსაფრთხოებასთან და რისკების მართვასთან დაკავშირებული საკითხები, არამედ გვაძლევს შესაძლებლობას რესურსების ოპტიმიზაციითა და სტრატეგიების განსაზღვრით საგრძნობლად შევამციროთ გაუთვალისწინებელი ხარჯები და გავზარდოთ კომპანიის შემოსავლები და მოგება.

COBIT-ს აქვს უპირატესობა, უზრუნველყოს ეფექტური ხელმძღვანელობა და სტრატეგია ბიზნესისა და IT-ის მართვის კარგი გადაწყვეტილებების, რესურსების პერფორმანსის ანალიზის და IT მართვის ჩამოყალიბების პარალელურად, მას ასევე შეუძლია მაქსიმალურად გაზარდოს დროსა და ხარჯებთან დაკავშირებული სარგებელი. ადმიანები, ორგანიზაციული სტრუქტურა და ტექნოლოგიები არის ყველაზე მნიშვნელოვანი ფაქტორები, რაც განსაზღვრავს COBIT-ის დანერგვის წარმატებას. ეს სამი ფაქტორი ჩართულია ინფორმაციული სისტემების რისკების შემცირებაში, IT სერვისების განვითარებასა და დაინტერესებული მხარეებისთვის ინფორმაციის ხელმისაწვდომობის გაუმჯობესებაში.

წინამდებარე კვლევას ჰქონდა შეზღუდული არეალი და მოიცავდა ინფორმაციული სისტემების რისკების ანალიზისა და მართვის მიდგომებს.კვლევის შედეგად წარმოჩენილი პრობლემის ერთერთ საუკეთესო გადაწყვეტილებად შესაძლებელია აღიარებული იყოს COBIT-ის დანერგვა კომპანიაში.

გამომდინარე იქიდან, რომ ქართული კომპანიების უმაღლესი მენეჯმენტი ჯერ კიდევ ვერ აცნობიერებს რა პრობლემების წინაშე შეიძლება აღმოჩნდეს მათ ბიზნესი უახლოს

მომავალში, ვფიქრობ საქართველოში უნდა გაიზარდოს ცნობიერება ინფორმაციული სისტემების რისკების არსებობისა და ბიზნესზე მათი ზეგავლენის შესახებ.

შესაძლებელია აღნიშნული კვლევის შედეგებისა და რეკომენდაციების უკეთ გააზრების მიზნით, შემდგომი კვლევისათვის შეფასდეს რამდენად ცნობილია სხვადსხვა სექტორში მოღვაწე კომპანიების უმაღლესი მენეჯმენტისთვის ინფორმაციული სისტემების მნიშვნელობა, მათი გამოყენებით მიღებული ღირებულებები და მათთან დაკავშირებული რისკების არსებობა. ასევე ჩატარდეს კვლევა და შეფასდეს რა ზარალის მოტანა შეუძლია კომპანიისთვის ინფორმაციული რისკების ანალიზისა და მართვის უგულვებელყოფას.

ბიბლიოგრაფია

ISACA. 2018. *COBIT 2019 Framework: Introduction and Methodology.* USA: ISACA.

ISACA. 2018. *COBIT 2019 Framework: Governance and Management Objectives.* USA: ISACA.

Van Grembergen, W.; S. De Haes; *Practices in IT Governance and Business/IT Alignment,* INFORMATION SYSTEMS CONTROL JOURNAL, VOLUME 2, 2008 https://www.researchgate.net/publication/228968843_Practices_in_IT_governance_and_businessIT_alignment

S. De Haes; A. Joshi; Van Grembergen, W.; *State and Impact of Governance of Enterprise IT in Organizations: Key Findings of an International Study,* ISACA Journal Volume 4, 2015 https://www.isaca.org/Journal/archives/2015/Volume-4/Pages/state-and-impact-of-governance-of-enterprise-it-in-organizations.aspx

Van Grembergen, W.; S. De Haes; *Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value*, Springer, USA, 2009

Weill, P.; J. Ross; *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, USA, 2004

Steven De Haes, Rogier Haest and Wim Van Grembergen; *IT Governance and Business-IT Alignment in SMEs*, ISACA Journal Volume 6, 2015 https://www.isaca.org/JOURNAL/ARCHIVES/2010/VOLUME-6/Pages/IT-Governance-and-Business-IT-Alignment-in-SMEs.aspx#5

McCue, A.; "Poor IT Governance Key to Project Failures," *ZDNet*, 29 March 2007, https://www.zdnet.com/article/poor-it-governance-key-to-project-failures/

Jonathan Saulez, MarketWorks, "Lack of IT Governance Is Putting Business Value at Risk," ITWeb, 23 July 2017, https://www.itweb.co.za/content/O2rQGqA5xnzqd1ea

Tung, L.; "Bank Fined $9.7m Over Poor IT Governance," ITNews, 5 August 2010, https://www.itnews.com.au/news/bank-fined-97m-over-poor-it-governance-223608 , http://www.fsa.gov.uk/pages/Library/Communication/PR/2010/130.shtml

Londini, Vince. COBIT Case Study: Risk Assessment Management Using COBIT 5. ISACA. http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Risk-Assessment-Management-Using-COBIT-5.aspx

ISACA. COBIT Case Study: Implementing COBIT for IT Governance, Risk and Compliance at Ecopetrol S.A. ISACA. http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Ecopetrol.aspx

Kajimoto, Masatoshi. COBIT Case Study: Using COBIT to Aid in Hospital Risk Management, Part 1. ISACA. http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Using-COBIT-to-Aid-in-Hospital-Risk-Management.aspx

Kajimoto, Masatoshi. COBIT Case Study: Using COBIT to Aid in Hospital Risk Management, Part 2. ISACA. http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Using-COBIT-to-Aid-in-Hospital-Risk-Management-Part-2.aspx

Barve, Jitendra. COBIT Case Study: IT Risk Management in a Bank. ISACA. http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-IT-Risk-Management-in-a-Bank.aspx

დანართი 1 - კითხვარი

1. დანერგილია თუ არა კობიტი თქვენ კომპანიაში?
2. რა დრო დაჭირდა კობიტის დანერგვას?
3. რა პერიოდის შემდეგ დაინახეთ შედეგი?
4. რა პრობლემებთან იყო დაკავშირებული კობიტის დანერგვა?
5. რა ზეგავლენა იქონია კობიტის დანერგვამ ინფორმაციულ სისტემებთან დაკავშირებული რისკებზე?
6. ზაგადად რა განსხვავება, შედეგი მიიღეთ კობიტის დანერგვის შემდეგ ინფორმაციულ სისტემებთან მიმართებაში?
7. რა ზეგავლენა იქონია კობიტის დანერგვამ კომპანიაზე?
8. გაქვთ თუ არა განსაზღვრული ჩარჩო ინფორმაციული სისტემების რისკების ანალიზისა და მართვისათვის?
9. ინფორმაციული სისტემების რისკების ანალიზისა და მართვისათვის რა მიდგომებს იყენებთ?
10. რამდენად არის ჩართული კომპანიის ტოპ მნეჯმენტი IT მართვაში?
11. რამდენ არის ჩართული კომპანიის ტოპ მნეჯმენტი IT რისკების მართვაში?