საბანკო სისტემაში შიდა აუდიტის როლი ინფორმაციული უსაფრთხოებისა და კლასიფიკაციის პროექტში

გიორგი ცაავა – სტუ-ს პროფესორი
ჯაბა ჯიქია – სტუ-სდოქტორანტი
Mail: jaba.jiqia@gmail.com

რეზიუმე

მსოფლიო ეკონომიკის განვითარების მიმდინარე ეტაპზე, სადაც უმთავრესი როლი მიენიჭა ინფორმაციის ელექტრონულ მატარებლებზე გადატანას და მათ დამუშავებას კიბერ სივრცეში, აუცილებელი შეიქმნა ინფორმაციული უსაფრთხოების ჩამოყალიბება და კორპორატიული მართვის სისტემებში მისი პრიორიტეტულობის განსაზღვრა. ნებისმიერი ფინანსური ინსტიტუტების და კერძოდ საბანკო სისტემის ძირითადი ინფორმაციული აქტივის დაცულობა კიბერ სივრცეში, პირდაპირ პროპორციული გახდა ამავე ინსტიტუტების არსებობასთან. კორპორატიული მმართველობის ნებისმიერი მნიშვნელოვანი სამსახურის არსებობა, შემოწმების და კონტროლის გარეშე წარმოუდგენელია. ამიტომ უდიდესი როლი ენიჭება შიდა აუდიტის სამსახურს ინფორმაციული უსაფრთხოების სისტემების აუდიტირებას.

სამუშაო პრაქტიკიდან გამომდინარე შეგვიძლია ვთქვათ, რომ საქართველოს რეალობაში ბოლომდე გააზრებული არ არის ინფორმაციული უსაფრთხოებასთან დაკავშირებული რისკები, რაც არ იძლევა საშუალებას გაძლიერდეს და ფეხი მოიკიდოს ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემებმა (ISMS information security management system), ამიტომ კვალიფიციური აუდიტის როლი უმნიშვნელოვანესია აღნიშნული სისტემის მნიშვნელობისა და პრობლემების მენეჯმენტისათვის მიწოდებისთვის. ჩვენი აზრით, კვალიფიციური აუდიტის დასკვნა უნიშვნელოვანესი დოკუმენტია თანამედროვე ტექნოლოგიური სპეციფიკის გამოსავლენად და გასააზრებლად.

სტატიაში შევეცდებით წარმოვაჩინოთ ძირითადი მნიშვნელობის საკითხები, განვსაზღვროთ რისკები, დონეების და პრიორიტეტულობის მიხედვით, ასევე ჩამოვაყალიბოთ რისკ მატრიცა და სისტემის მუშაობაზე პასუხისმგებელი პროცესები.

ჩვენი აზრით ყველა ფინანსური ინსტიტუტში ინფორმაციული უსაფრთხოების მართვის სისტემის ინტეგრაციისათვის პირველ რიგში აუცილებელია ინფრომაციული აქტივების კლასიფიკაცია.

ინფორმაციული აქტივი არის ნებისმიერი აქტივი, რომელიც შეიცავს ბანკის მუშაობისათვის საჭირო ინფორმაციას. ესეთი აქტივები შესაძლებელია იყოს ამობეჭდილი დოკუმენტი, კომპიუტერის მყარი დისკი, სერვერი, ქსელური მოწმობილობა და ნებისმიერი ელექტრონული დოკუმენტი. უსაფრთხოების უზრუნველსაყოფად, ბანკმა ინდა აღრიცხოს მის მფლობელობაში არსებული ყველა აქტივი, შეაფასოს კრიტიკულობის მიხედვით, დადგინოს რისკები და მიანიჭოს სტატუსი რომელიც განსაზღვრული იქნება 1 დან 10 ქულამდე სისტემით. აღნიშნული ეტაპის მნიშვნელობიდან გამომდინარე მიზანშეწონილია შიდა აუდიტის ჩართულობა. პირველ რიგში შიდა აუდიტის თანამშრომელთან ერთად უნდა შედგეს ინფორმაციული აქტივების კლასიფიკაციის გეგმა, რაც მოიცავს ბანკში არსებული ყველა სტრუქტურის სამუშაო პროცესისთვის საჭირო აქტივების აღრიცხვას. აუცილებელია ყველა სტრუქტურის კვალიფიციურ წარმომადგენელთან ინტერვიუს ჩატარება. რაც საშუალებას მოგვცემს სწორად ავღწეროთ ბანკისთვაის მშნიშვნელოვანი ყველა აქტივი. პრაქტიკა გვიჩვენებს, რომ აქტივის მფლობელთან ინტერვიუს დროს პასუხისმგებელი პირი ზედმეტად აფასებს მის მფლობელობაში არსებულ აქტივების მნიშვნელობას და ამის გამო კლასიფიცირებასაც რიგ შემთხვევებში ვერ ახდენს, ყველა თავის აქტივს აფასებს შეფასების შკალაში უმაღლესი ქულით, ამიტომ აუცილებელია ინტერვიუმდე განვუმარტოთ ინტერვიუვერს თუ რას გულისხმობს ესა თუ ის რისკი და რამდენად საზიანო იქნება აღნიშნული აქტივის დაზიანება ან დაკარგვა ბანკის ინფორმაციული უსაფრთხოებისათვის. რისკების შეფასების კრიტერიუმებად უნდა განვსაზღვროთ რამოდენიმე სახის შედეგი. ერთერთი უმთავრესი რისკი ბანკის აქტივების მიმართ არის ბიზნეს უწყვეტობა (ბუსინესს ცონტინუიტყ), რომელიც მოიცავს

ისეთ მოვლენებს, რომლის დადგომისას დგება ბანკის მუშაობის შეფერხება ან პარალიზება. შემდეგი მნიშვნელობის რისკი მოიცავს ფინანსურ დანაკარგს, რომლის დადგომისას ბანკს მოუწევს ფინანსური ზარალის მიღება და ბოლოს განვიხილავთ რეპუტაციულ რისკს, რომლის მნიშვნელობა შეიძლება მერყეობდეს უმაღლესიდან ყველაზე დაბალ შეფასებამდე, ეს დამოკიდებულია ბანკის ან ფინანსური ინსტიტუტის რეპუტაციაზე და ბაზრის მონოპოლიურ მდგომარეობაზე.

აღნიშნული შეფასების სისტემის განმარტების შემდეგ აუდიტორი და ინფორმაციული უსაფრთხოების ოფიცერი იწყებენ აქტივების აღრიცხვას და შეფასებას. აქტივს რისკის გარდა აუცილებელია მივანიჭოთ კლასიფიცირების სტატუსი. აქტივი შეიძლება იყოს სამი სახის;

- საჯარო
- შიდა მოხმარების
- კონფიდენციალური

აქტივის კლასიფიკაციაზე, პასუხისმგებელი პირები არისნ აქტივის შემქმნელი, მფლობელი თანამშრომელი, ინფორმაციული უსაფრთხოების ოფიცერი და აუდიტორი. მის გავრცელებაზე ყველა ის თანამშრომელია პასუხისმგებელი რომლებსაც აქვთ წვდომა ამა თუ იმ სტატუსის მქონე აქტივზე.

საჯარო აქტივები (PUBLIC). საჯარო აქტივები თავისუფალი აქტივებია, რომლებიც შეიძლება როგორც ბანკის შიგნით თანამშრომლისთვის იყოს გამოსაყენებელი, ასევე ბანკის გარეთაც გავრცელდეს. ესეთებს განეკუთვნება სარეკლამო და აქციების შინაარსის შემცველი ბროშურები, სარეკლამო ბანერები ინტერნეტ კონტენტი რომელზეც ბანკის შესახებ ინფორმაციაა განთავსებული და ა.შ.

შიდა მოხმარების ინფორმაციული აქტივები (INTERNAL), აღნიშნულ აქტივები განეკუთვნილია მხოლოდ ბანკის შიდა თანამშრომლებისათვის და ბანკთან დაკავშირებულ ავტორიზებული პირებისათვის. აღნიშნული აქტივების გარეთ მოხვედრა რათქმა უნდა არ არის სასურველი და მიზანშეწონილია მათი დაცვა, თუმცა მათი გასაჯაროების შემთხვევაში ბანკის მიმართ რაიმე რისკ ფაქტორის შემცველობა არ განიხილება და რაიმე ფინანსური ზარალის მომტანი ვერ შეიძლება გახდეს ბანკისთვის და მისი კლიენტებისთვის. მსგავსი აქტივებია; შიდა პოლიტიკები და პროცედურები, მომხმარებლის სახელმძღვანელოები, ტრენინგ მასალები/ბანკის შიდა განაწესი, ბიზნეს უწყვეტობის გეგმა (რომელიც მოიცავს ევაკუაციის და მსგავსი შინაარსის სამოქმედო გეგმებს) და ა.შ.

კონფიდენციალური ინფორმაციული აქტივი (CONFIDENTIAL), ეს არის აქტივი რომელზეც განსაზღვრულ ადამიანებს შეიძლება ქონდეც წვდომა. ესეთი აქტივის დაკარგვა და გავრცელება გამოიწვევს ბანკისთვის, მისი თანამშრომლებისთვის, ან კონტრაქტორი ორგანიზაციებისათვის ზიანის მიყენებას, რამაც შესაძლოა ძლიერ რისკფაქტორების ფინანსურ, რეპუტაციულ ან სამართლებრივ გააქტიურება გამოიწვიოს. ესეთ უმთავრეს აქტივს ბანკში წარმოადგენს კლიენტის ან თანამშრომლის პერსონალური ინფორმაცია, რომლის კონფიდენციალურობას და დაცვას უზრუნველყოფს ეროვნული ბანკის რეგულაცია და პერსონალური მონაცემთა დაცვის ინსპექტორის აპარატი. ასევე აღსანიშნავია რომ 2018 წლის 25 მაისს მიღებული რეგულაცია GDPR ევროკავშირის ქვეყნების მოქალაქეების პირადი მონაცემთა დაცვის შესახებ, ბევრად ართულებს მოთხოვნებს ბანკების მიმართ.

საკრედიტო ან სადეპოზიტო პორტფელი, ფინანსური ანგარიშგებები, აუდიტორული დასკვნები, მონაცემთა ბაზები, პაროლები, კრიპტოგრაფული გასაღებები და ა.შ. ზუსტად ბოლოს განმარტებული კონფიდენციალური აქტივის განსაზღვრისათვის არის აღნიშნული სამუშაო ჩასატარებელი. აღნიშნული სამუშაოს შედეგად უნდა მივიღოთ ბანკში არსებული ყველა აქტივის კლასიფიცირება რისკის შეფასების გათვალისწინებით.

ზემოთ აღნიშნულდან გამომდინარე შემდეგი სახის მოკლე დასკვნის გაკეთება არის შესაძლებელი;

1. აღნიშნულია რომ, საჯარო აქტივები თავისუფალი აქტივებია, რომლებიც შეიძლება როგორც ბანკის შიგნით თანამშრომლისთვის იყოს გამოსაყენებელი, ასევე ბანკის გარეთაც გავრცელდეს. ესეთებს განეკუთვნება სარეკლამო და აქციების შინაარსის შემცველი ბროშურები, სარეკლამო ბანერები ინტერნეტ კონტენტი რომელზეც ბანკის შესახებ ინფორმაციაა განთავსებული და ა.შ.

2. შეთავაზებულია რომ, შიდა მოხმარების ინფორმაციული აქტივები (INTERNAL), აღნიშნულ აქტივები განეკუთვნილია მხოლოდ ბანკის შიდა თანამშრომლებისათვის და ბანკთან დაკავშირებულ ავტორიზებული პირებისათვის. აღნიშნული აქტივების გარეთ მოხვედრა რათქმა უნდა არ არის სასურველი და მიზანშეწონილია მათი დაცვა.

3. მითითებულია რომ, კონფიდენციალური ინფორმაციული აქტივი (CONFIDENTIAL), ეს არის აქტივი რომელზეც განსაზღვრულ ადამიანებს შეიძლება ქონდეც წვდომა. ესეთი აქ-

ტივის დაკარგვა და გავრცელება გამოიწვევს ბანკისთვის, მისი თანამშრომლებისთვის, ან კონტრაქტორი ორგანიზაციებისათვის ზიანის მიყენებას, რამაც შესაძლოა ძლიერ რისკფაქტორების ფინანსურ, რეპუტაციულ ან სამართლებრივ გააქტიურება გამოიწვიოს.

გამოყენებული ლიტერატურა

ასათიანი ვლ., ცაავა გ.-კომერციული ბანკების საქმიანობის ფინანსური ანალიზი (თეორია, მეთოდოლოგია და პრაქტიკა). თბილისი, გამომცემლობა "დანი". 2014. 500 გვ.

THE ROLE OF INTERNAL AUDIT IN THE BANKING SYSTEM IN THE INFORMATION SECURITY AND CLASSIFICATION PROJECT

GIORGI TSAAVA - professor of GTU
JABA JIQIA - PhD student of GTU
Mail: jaba.jiqia@gmail.com

Summary

1. It is noteworthy that public assets are free assets that may be used for employee inside the bank as well as outside the bank. These include brochures containing advertising and promotions, advertising banners, internet content containing information about the bank, etc.

2. It is suggested that information assets of internal consumption (INTERNAL) are designed only for the internal employees of the bank and authorized persons related to the bank. Of course, it is not desirable to let these assets appear outside the bank and it is advisable to protect them.

3. It is indicated that a confidential information asset (CONFIDENTIAL) is an asset that specific people may have access to. The loss and distribution of such an asset will cause damage to the Bank, its employees or contractor organizations, which may result in financial, reputable or legal activation of risk factors.