



საბანკო სისტემაში შიდა აუდიტის როლი ინფორმაციული უსაფრთხოებისა და ბიზნეს უწყვეტობის პროექტში

რეზიუმე

ბიორბი ცაავა - სტუ-ს პროფესორი

ჯაბა ჯიქია - სტუ-ს დოქტორანტი

Mail: jaba.jikia@gmail.com

ზემოთ აღნიშნულდან გამომდინარე შემდეგი სახის მოკლე დასკვნის გაკეთება არის შესაძლებელი;

აღნიშნულია რომ სახელმწიფოს მხრიდან არარეგულირებული ბიზნეს უწყვეტობის გეგმის შემუშავებისას არსებობს რისკი, რომ ბანკის პოლიტიკაში არაკეთილსინდისიერად და გაუზრებლად დაგეგმილმა პროცედურამ კატასტროფის შემთხვევაში გამოიწვიოს ადამიანური დანაკარგები, რაც დაუშვებელია ნებისმიერი განვითარებული სახელმწიფოსთვის.

შეთავაზებულია რომ, ინციდენტების მართვის პროცედურაში ერთ-ერთ მოცულობით ქვეთავს წარმოადგენს ბიზნეს უწყვეტობის გეგმა, რომელიც ფაქტიურად არის პროცედურა/ინსტრუქცია თუ რა ეტაპები უნდა გაიაროს ბანკმა კატასტროფის და ფორსმაჟორული სიტუაციის შემთხვევაში. პირველ რიგში, პროცედურაში აღწერილი უნდა იყოს პროცესები, რომლებიც პრევენციული კვლევის დროს გამოვლინდა და ჩაითვადა ბანკის მუშაობისთვის შესაძლო ხელისშემშლელად.

მითითებულია რომ, ყველა დეპარტამენტის უფროსი პასუხისმგებელია თავისი თანამშრომლების ორგანიზებაზე და შემდგომ, ბანკის კალიდორებში არსებული ევაკუაციის გეგმის მიხედვით მათ უსაფრთხო გაყვანაზე. პასუხისმგებელი თანამშრომელი ვალდებულია მოკლედ გააცნოს თავის თანამშრომლებს აღნიშნული კატასტროფის შესახებ. კატასტროფის აღწერა, კატასტროფის მაშტაბი, სამოქმედო გეგმა.

სტატიაში გამოყენებული უცხო სიტყვები

1. BCP - (business continuity plan) - ბიზნესის უწყვეტობის გეგმა, რომელსაც დანიშნულებაც არის ბანკის შეუფერხებელი მუშაობის უზრუნველყოფა.

2. ინფორმაციული ტექნოლოგიების დეპარტამენტი - აი თი დეპარტამენტი, რომელიც პროგრამული და ქსელური რესურსით უზრუნველყოფს ბანკს.

3. ინციდენტი - მოვლენა რომელიც სცდება პროცესის სტანდარტულ მდგომარეობას.

4. კატასტროფა - პროცესი რომელიც ბანკისთვის მიიმე შედეგის მომტანია.

საქართველოს საბანკო სისტემების განვითარებასთან ერთად აუცილებელი გახდა მისი თანამშრომლების და აქტივების უსაფრთხოების გაზრდა. საქართველოს ეროვნული ბანკის მეთვალყურეობის ქვეშ მყოფ ყველა ფინანსური ორგანიზაციას, დაევადა BCP-ბიზნესის უწყვეტობის გეგმის შემუშავება (ბანკის სამოქმედო გეგმა საგანგებო სიტუაციების დროს). აღნიშნული გეგმა, მრავალი პროტოკოლისგან შედგება. ბანკის უსაფრთხო სამუშაო გარემოს შესანარჩუნებისთვის, ერთერთი უმნიშვნელოვანესი პუნქტია საგანგებო საევაკუაციო გეგმა, რომელიც საგანგებო სიტუაციის დროს ბანკში მყოფი ყველა ადამიანის უსაფრთხო ევაკუირებას უზრუნველყოფს. ბანკის მიერ შემუშავებული გეგმა, პირველ რიგში უნდა იყოს ორიენტირებული ადამიანის სიცოცხლის გადარჩენაზე და მხოლოდ შემდეგ უნდა განიხილებოდეს სხვა, ნაკლებად მნიშვნელოვანი აქტივების გადარჩენისათვის შესასრულებელი სამუშაოები. სახელმწიფოს მხრიდან არარეგულირებული ბიზნეს უწყვეტობის გეგმის შემუშავებისას არსებობს რისკი, რომ ბანკის პოლიტიკაში არაკეთილსინდისიერად და გაუზრებლად დაგეგმილმა პროცედურამ კატასტროფის შემთხვევაში გამოიწვიოს ადამიანური დანაკარგები, რაც დაუშვებელია ნებისმიერი განვითარებული სახელმწიფოსთვის. ჩვენი კვლევების დროს მოვიძიეთ ინფორმაცია, სადაც აღწერილი იყო, რამოდენიმე დიდ საწარმოში ხანძრის შემთხვევის დროს მიმდინარე ქმედებები და შედეგები. შემდგომი ანალიზი აჩვენებს, რომ მიუხედავად თანამშრომლებისთვის გაცნობილი სამოქმედო გეგმისა და სტანდარტის მიხედვით გამოკრული საევაკუაციო გეგმებისა, 50 % შემთხვევების დროს მაინც შეინიშნება ქაოსი და არამიმდევრული ქმედებები. ევაკუაციის გეგმის შემუშავებისას გათვალისწინებული უნდა იქნას შენობის განლაგება, რომელიც სინქრონიზირებული უნდა იყოს შენობის გამტარობასთან, რაც რთულად დასადგენი და საპასუხისმგებლოა. აღნიშნული პროცესი მოითხოვს სპეციფიურ გა-



ნათლებას, შესაბამისი კომპეტენციის და ცოდნის მქონე თანამშრომლების ჩართულობას, ასეთის არარსებობის შემთხვევაში ბანკი ვალდებულია მოიწვიოს სპეციალისტი. პროექტების მაშტაბურობიდან გამომდინარე მასში ჩართული უნდა იყოს შემდეგი დეპარტამენტები:

- ინფორმაციული ტექნოლოგიების დეპარტამენტი.
- ოპერაციული რისკების დეპარტამენტი.
- შიდა აუდიტი.
- ინფორმაციული უსაფრთხოება.
- ფიზიკური უსაფრთხოება.
- მოწვეული სპეციალისტები.

ჩვენი კვლევის შედეგად მოძიებული ეროვნული ბანკის რეგულაციის ანალიზისას აღმოჩნდა, რომ იგი მოძველებულია და მისი მოთხოვნები არ არის აქტუალური დღევანდელი რეალობისთვის, როცა ტექნოლოგიების განვითარებამ შეცვალა ტექნოლოგიური გარემო.

აღნიშნული პროექტების დასაწერგად ბანკი ვალდებულია შექმნას რამოდენიმე დოკუმენტი:

- ინციდენტების მართვის პროცედურა (სადაც აღწერილი იქნება ყველა შესაძლო ინციდენტი)
- ინციდენტების შემდგომ რეაგირების გეგმა.
- ინციდენტების შემდგომი შეტყობინებების გეგმა.
- ევაკუაციის გეგმა.

ჩვენი აზრით ცალკე პროექტად უნდა განვიხილოთ „კატასტროფის შემდგომი აღდგენის გეგმა“. აღნიშნული პროცესი მოცულობიდან და სპეციფიკიდან გამომდინარე მოითხოვს ტექნიკური პერსონალის ჩართულობასაც.

ინციდენტების მართვის პროცედურაში ერთ-ერთ მოცულობით ქვეთავს წარმოადგენს ბიზნეს უწყვეტობის გეგმა, რომელიც ფაქტიურად არის პროცედურა/ინსტრუქცია თუ რა ეტაპები უნდა გაიაროს ბანკმა კატასტროფის და ფორსმაჟორული სიტუაციის შემთხვევაში. პირველ რიგში, პროცედურაში აღწერილი უნდა იყოს პროცესები, რომლებიც პრევენციული კვლევის დროს გამოვლინდა და ჩაითვალა ბანკის მუშაობისთვის შესაძლო ხელისშემშლელად. ესეთებია:

- ომი.
- ქვეყნის შიდა სამოქალაქო დაპირისპირება.
- მასიური არეულობა.
- ხანძარი.
- სტიქიური უბედურებები და ა.შ.

ზემოთ აღნიშნულ გეგმაში ყველა ინციდენტზე უნდა იყოს შესაბამისი განსაზღვრული პროცედურა, რომელიც უნდა მოიცავდეს ყველა დეპარტამენტის ქმედებების კოორდინაციას რათა არ მოხდეს რესურსის და დროის უმიზეზოდ დაკარგვა. ინციდენტების მართვის

პროტოკოლის ერთ-ერთი მნიშვნელოვანი ნაწილია პასუხისმგებელ პირებზე შეტყობინების გაგზავნის მატრიცა, რომელშიც განისაზღვროს კონკრეტული ინციდენტის შემთხვევაში ვისთვის და რა მეთოდით უნდა მოხდეს შეტყობინების გაგზავნა. მაგ. ხანძრის შემთხვევაში ინფორმაცია უნდა მიეწოდოს ფიზიკურ უსაფრთხოებას, ყველა დეპარტამენტსი უფროსსა და სახანძრო სამსახურს. შეტყობინების ტიპები ინციდენტის მიხედვით შეიძლება განსხვავდებოდეს: მოკლე ტექსტური, ელექტრონული საფოსტო შეტყობინება, ტელეფონის ზარი. აღნიშნული ქმედება არის პირველი ეტაპი ინციდენტის დაფიქსირების შემდეგ. სტანდარტული ქმედებების მიმდევრობა გამოიყურება შემდეგნაირად:

- კატასტროფის დადგენა.
- საგანგებო სიტაციების სამსახურის გამოძახება.
- ინფორმაციის მიწოდება პასუხისმგებელი პირებისთვის.
- სიტუაციის შეფასება.
- განგაშის სიგნალის ხმოვანი შეტყობინება.
- ევაკუაცია.

მნიშვნელოვანი ეტაპი არის ევაკუაციის გეგმა. ყველა დეპარტამენტის უფროსი პასუხისმგებელია თავისი თანამშრომლების ორგანიზებაზე და შემდგომ, ბანკის კალიდორებში არსებული ევაკუაციის გეგმის მიხედვით მათ უსაფრთხო გაყვანაზე. პასუხისმგებელი თანამშრომელი ვალდებულია მოკლედ გააცნოს თავის თანამშრომლებს აღნიშნული კატასტროფის შესახებ. კატასტროფის აღწერა, კატასტროფის მაშტაბი, სამოქმედი გეგმა. თანამშრომლებმა თავის მხრივ შეძლებისდაგვარად უნდა გამორთონ მოწყობილობები, დაკეტონ საცავი, გავიდნენ კალიდორში და არ ისარგებლონ ლიფტით. გეგმაში უნდა იყოს ასახული ძირითადი და სარეზერვო გასასვლელები, რომლებიც არ უნდა იყოს დაკეტილი ან რამე ბარიერის მქონე. ყველა თანამშრომლის გაყვანის შემდეგ ევაკუაციის გეგმაში ნაჩვენებია ადგილი ბანკთან ახლოს, სადაც უნდა მოხდეს ყველა თანამშრომლის შეკრება. შეკრების შემდეგ დეპარტამენტის უფროსი ითვლის თავის თანამშრომელს და ატყობინებს უსაფრთხოებას, გამოყვანილი თანამშრომლების რაოდენობის შესახებ. მხოლოდ ევაკუირების და საფრთხის გადავლის შემდეგ, უსაფრთხოების თანამშრომლებმა შეძლებისდაგვარად უნდა დაიცვან საცავი და სასერვერო ოთახი.

როგორც კვლევამ აჩვენა, მსგავსი შემთხვევების მცირე ალბათობიდან გამომდინარე ზემოთ ხსენებულ გეგმას არასოდეს ექცევა სათანადო ყურადღება. თანამშრომლები არ ეცნობიან ევაკუაციის პროცედურას, ისევე როგორც საევაკუაციო გეგმას. ამიტომ საგანგებო სიტუ-



აციის დროს შესაძლოა მიიმე შედეგებით დასრულდეს ესა თუ ის ფორსმაჟორული სიტუაცია. ამის აღმოსაფხვრელად და იმის დასადგენად რამდენად კარგად არის შემუშავებული ბიზნეს პროცესების უწყვეტობის გეგმა და რამდენად მორგებულია რეალურ გარემოს, ბანკი პერიოდულად უნდა ატარებდეს სატესტო ევაკუაციას, რომელიც რეალურ პირობებთან მაქსიმალურად იქნება მიახლოებული. ტესტირების დაგეგმვას და ჩატარებას უსაფრთხოებასთან ერთად აკვირდება და სწავლობს აუდიტის სამსახური, რადგან არ არსებობს მეთოდი რეალური ტესტირების გარეშე შეაფასო ბანკის თანამშრომლების მზაობა ფორს მაჟორის მიმართ. მხოლოდ რეალურ რეჟიმში ჩატარებული ტესტირება მოგვცემს ზუსტი შეფასების საშუალებას. ტესტირება უნდა ხდებოდეს პერიოდულად მინიმუმ წელიწადში 2 ჯერ. ტესტირების დასრულების შემდეგ აუდიტის სამსახური ყველა პუნქტის მიხედვით ამოწმებს შესაბამის კონტროლებს;

- ინციდენტის დაფიქსირების დროს იმუშავა თუ არა ელექტრონულმა მოწყობილობებმა.
- შეტყობინებები გაეგზავნათ თუ არა

ბამოყენებული

1. ასათიანი ვლ., ცაავა გ.-კომერციული ბანკების საქმიანობის ფინანსური ანალიზი (თეორია, მეთოდოლოგია და პრაქტიკა). თბილისი, გამომცემლობა „დანი“. 2014. 500 გვ
2. ცაავა გ., ხანთაძე გ. - „საბანკო საქმე“ (თეორია, მეთოდები და პრაქტიკა), სახელმძღვანელო. - თბილისი, გამომცემლობა „დანი“, 2014. - 600 გვ.
3. ISO 9001:1987 Model for quality assurance in

შესაბამის პასუხისმგებელ პირებს.

- რა ტიპის შეტყობინებები გაეგზავნათ, შესრულდა თუ არა შეტყობინებების მატრიცაში გაწერილი ყველა პროტოკოლი.

- ევაკუაციის დაწყების შემდეგ შეიქმნა თუ არა ქაოსი და არეგულირებდა თუ არა პასუხისმგებელი პირები აღნიშნულ სიტუაციას.

- გაეგზავნა თუ არა შესაბამის ორგანოებს შეტყობინება დროულად (ამ შემთხვევაში სახანძრო სამსახურში შესულ შეტყობინების დროს უნდა შედარდეს ინციდენტის დაფიქსირების დროს).

- შეიკრიბა თუ არა ყველა თანამშრომელი შეკრების ადგილას და კოორდინაცია თუ ხდებოდა უსაფრთხოებისა და სხვა ღეპარტამენტის უფროსებს შორის და ა.შ.

მხოლოდ ამ ინფორმაციის გაანალიზების შემდეგ ხდება შესაძლებელი, აუდიტის სამსახურმა მიიღოს გადაწყვეტილება შესაბამისობის შესახებ.

აღნიშნული პროცედურა პერიოდულად უნდა იქნეს გადახედული ბანკში მიმდინარე ცვლილებების შესაბამისად.

ლიტერატურა

- design, development, production, installation, and servicing .2012
4. ISO 9002:1987 Model for quality assurance in production, installation, and servicing.2012
 5. ISO/IEC 27001 Information security management 2013
 6. Internal Auditing's Role in Risk Management, Sponsored by Oracle and The IIA Research Foundation, March, 2011.

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

GIORGI TSAAVA - professor of GTU

JABA JIQIA - PhD student of GTU

Mail: jaba.jiqia@gmail.com

Summary

It is noted that in the process of developing a non-regulated business continuity plan by the state, there is a risk that the procedure planned dishonestly and in a mindless manner in the bank's policy will result in catastrophic human losses that is inadmissible for any developed state.

It is suggested that one of the large subdivisions of the Incident Management Procedure is a business continuation plan, which is actually a procedure / instruction on which steps the bank must undergo in case of disaster and force majeure. In the first place, the procedure should describe the processes that were detected during preventive research and considered to be possibly interfering with the bank's work.

It is indicated that each head of all departments is responsible for organizing their employees and then taking them out safely according to the evacuation plan in the bank's corridors. The responsible employee is obliged to briefly inform its staff about the disaster, provide disaster description, information about the catastrophe scale, action plan.