Universitatea Tehnică a Moldovei

Model practic de gestionare a riscurilor informaționale

Practical model of information risk management

Masterand:

Agapii Cristian

Coducător:

Conf. univ., dr. Beșliu Victor

Chișinău – 2020

Ministerul Educaţiei Culturii şi Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
FACULTATEA Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament: conf. univ., dr. Fiodorov Ion
Fiod
„19" decembrie 2020

Model practic de gestionare a riscurilor informaționale

Teză de master în Securitate Informațională

Masterand: Agapii (Agapii Cristian)
Conducător: (Beșliu Victor)

Chişinău – 2020

Adnotare:

Această teză de master a fost elaborată de studentul Agapii Cristian, grupa SI-181M, cu tematica „Model practic de gestionare a riscurilor informaționale”. Structura tezei este formată din: Introducere, 3 capitole, Concluzii și Anexe.

Abordarea acestei lucrări este determinată de necesitatea unor procese de analiză a riscurilor mult mai eficiente, rapide și în urma cărora va fi acumulată maximă informație utilă și care va descrie cu certitudine situația reală. Analiza riscurilor este un proces important în activitatea unei organizații.

Valoarea teoretică este fundamentată din analiza a mai multor surse din literatura de specialitate din domeniul securității informaționale și a analizei riscurilor, precum și conformarea cu cerințele standardelor internaționale (ISO 27001, ISO 27002, ISO 27005, CobiT, NIST, etc.) și cu bazele lugale cum ar fi hotărîri de guvern, ordine și sarcini tehnice (HG nr. 201 din 28.03.2017, etc.).

În primul capitol a acestei teze de master este descrisă analiza domeniului de studiu, unde au fost descrisă definirea managementului riscurilor precum și definiția de risc, necesitatea unei metodologii bine aranjată și structurată pentru a piermite ușurința procesului de colectare a informației și elaborarea documentației, cum se elaborează politici de gestionarea a riscurilor și însuce descrie un proces de gestionare și identificare a riscurilor.

În capitolul doi au fost analizate numeroase tehnici de gestionare a riscurilor, ca de exemplu: analizs SWOT, analiza GAP, Brainstorimiing și analiza CSM. Acestea prezentînd doar o etapă din întreg procesul de identificare și analiză a riscurilor.

În capitolul trei este prezentat însuși modelul de gestionare a riscurilor elaborat de către autor, acesta cuprinde cîteva etape cheie: identificarea resurselor, identificarea amenințărilor și vulnerabilităților, analiza de risc și tratarea riscurilor. Ca etapă finală a întregului proces se rezultă un Plan de tratare a riscurilor, acesta fiind documentul scop a întregului model elaborat în această teză de master.

În concluzie această teză de master putem spune că au fost abordate principalele probleme întîlnite în procesul de gestionare a riscurilor și modelul propus este unul practic, fiind implementat și aprobat într-o instituție.

Abstract

This master's thesis was elaborated by the student Agapii Cristian, group SI-181M, with the theme "Practical model of information risk management". The structure of the thesis consists of: Introduction, 3 chapters, Conclusions and Annexes.

The approach of this paper is determined by the need for processes of analysis of the risks more efficient, fast and after which will be accumulated maximum useful information and that will describe with certainty the real situation. Risk analysis is an important process in the activity of an organization.

The theoretical value is based on the analysis of several sources in the specialized literature in the field of information security and risk analysis, as well as in compliance with the requirements of international standards (ISO 27001, ISO 27002, ISO 27005, CobiT, NIST, etc.) and with the bases such as government decisions, orders and technical tasks (GD no. 201 of 28.03.2017, etc.).

In the first chapter of this master's thesis is described the analysis of the field of study, where the definition of risk management as well as the definition of risk was described, the need for a well-arranged and structured methodology in order to lose the ease of the information collection process and the documentation elaboration, as described develops risk management policies and then outlines a risk management and identification process.

In chapter two, many risk management techniques were analyzed, such as: SWOT analysis, GAP analysis, Brainstorimiing and CSM analysis. They present only one stage in the entire process of risk identification and analysis.

Chapter three presents the risk management model itself developed by the author, which includes several key steps: identifying resources, identifying threats and vulnerabilities, risk analysis and risk management. As a final stage of the entire process, a Risk Management Plan is the result, which is the purpose document of the entire model elaborated in this master's thesis.

In conclusion, this master's thesis can say that the main problems encountered in the risk management process were addressed and the proposed model is a practical one, being implemented and approved in an institution.

Cuprins

Introducere

Prezenta metodologie are ca scop îmbunătățirea procesului de management al riscurilor, prin parcurgerea etapelor de bază: identificarea, evaluarea, gestionarea și tratarea riscurilor. Prevederile se aplică de către personalul responsabil implicați în procesul de identificare, evaluare, stabilire a măsurilor de tratare și monitorizare a minimizării riscurilor.

Metodologia vizează resursele stabilite pe următoarele categorii - informaţii, hardware, software, personal, locaţie şi facilităţi, precum și procesele principale identificate, considerate în continuare ca categorie de resurse organizaționale.

Riscul este evenimentul capabil (în cazul producerii) să exercite o influență asupra desfășurării proiectului. Riscurile există în toate proiectele, dar nu neapărat se produc. Majoritatea experților sunt de părerea: cu cît mai degrabă va fi stabilit pericolul potențial, cu atît mai mult timp va rămane ca echipa de proiectanți să-l neutralizeze sau să minimizeze pierderile. Astfel, identificarea riscurilor trebuie efectuată la etapa incipientă a lucrărilor asupra IT-proiectului.

Majoritatea companiilor activitatea cărora ține de elaborarea de proiect a produselor program (PP), alcătuiesc propriile clasificatoare de riscuri, bazate atît pe cunoștințele teoretice, cît și pe experiența de realizare a proiectelor. În cele mai dese cazuri, complexitatea factorilor de risc este divizată convențional în cei obiectivi și subiectivi. La factorii obiectivi raportăm: modificarea datelor inițiale, condițiilor Beneficiarului, furnizarea întîrziată a utilajului, precum și circumstanțele de forță majoră.

O altă variantă de clasificare a riscurilor este clasificarea lor în cele interne și externe. Această modalitate este utilizată pentru definirea simplificată a pericolelor potențiale și măsurilor de contracarare a acestora. Pe de o parte, sunt formate riscurile ce țin de activitatea firmei-proiectante, iar pe de altă parte riscurile, la care este supus Beneficiarul. Schema prezentată se complică și în cazul, în care firma-proiectant transmite o parte din lucrari unei terțe organizații de subantrepriză. În această situație apare terța parte și respectivele riscuri ce nu trebuie trecute cu vederea.

Impactul, ori consecințele riscului reprezintă influența riscului produs asupra posibilității de realizare a unor componente anumite ale planului. Impactul se referă, de regulă, la costul, graficul și caracteristicile tehnice ale produsului elaborat. Spre exemplu, la elaborarea PP impactul riscului poate avea ca efect necorespunderea produsului exigentelor Beneficiarului, ba mai mult ca atît el poate deveni de-a dreptul inutil. Impactul adeseori parcurge o perioadă latent din momentul apariției riscului pînă la apariția modificării rezultante in sistem. Pentru evaluarea impactului riscului sunt de regulă, utilizate unități conventionale ori scara calitativă (spre exemplu, impactul neglijabil, neesențial, esențial, mare, catastrofal). Pentru lucrul cu riscurile pozitive se impune extinderea scării în mod corespunzător.

Concluzii

Elaborînd această teză de master și avînd ca scop elaborarea unui model practice de gestiune a riscurilor informaționale, a fost studiat domeniul securității informaționale și anume ramura managementul riscurilor, dar și securitatea organizației și a tuturor activelor. Analiza riscurilor fiind o ramură foarte importantă în activitatea unei organizații și nu numai. Riscurile la rîndul lor conduc la decizii de securitate, de aceea este essential de a detecta care sunt acestea, pentru a evita costuri adăugătoare și situații neconforme cep oat adduce mari breșe în activitatea, dar și bugetul organizației. Identificarea metodei de gestionare a riscurilor este foarte importantă, aceasta avînd un rol important în analiza și raportarea rezultatelor conforme, precum și gestionarea bugetului și a activelor implicate în procesul de analiză.

În acest sens a fost elaborate următoarea metodă de gestionarea a riscurilor, fiind conformă standardelor internaționale din categoria ISO 27000. Metodologia data este practică și ușor de asimilat, dat fiind faptul că aceasta deja este implementată într-o instituție I.P. „Centrul de Tehnologii Informaționale în Finanțe”.

Întreaga metodologie este împărțită în patreu etape. La prima etapă este identificarea și clasificarea resurselor organizației, de asemenea identificarea unui grad de impact asupra activelor. Apoi urmează etapa de identificare a amenințărilor și vulnerabilităților sistemului informațional, acestea fiind clasificate confor standardului ISO 27001:2013. După efectuarea analizei amenințărilor identificate și clasificate, s-a prezentat și implementat soluții care minimizează riscurile, asigurînd astfel, confidențialitatea, integritatea și disponibilitatea datelor. La următoarea etapă se completează „Nomenclatorul riscurilor”, la acestă etapă sunt identificate procesele și activele cele mai vulnerabile care necesită stabilirea unor norme mai adecvate de securitate. Și ca etapă finală se documentează „Planul de tartare a riscurilor”, acesta conține reguli și indici pentru ridicarea nivelului de securitate a proceselor, sau a activelor.

Această teză de master a fost elaborată conform cerințelor, au fost abordate principalele probleme întîlnite în procesul de gestionare a riscurilor și modelul propus este unul practic, acoperind necesitățile principale pentru un proces de identificare și analiză a riscurilor.

Bibliografie

1. Standardul ISO/IEC 27001:2013 Information security management. [Resursă electronică]. - Regim de access: http://www.pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf [25.11.2019].
2. ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls [Resursă electronică]. - Regim de access: http://www.pqm-online.com/assets/files/pubs/translations/std/iso-mek-27002-2013.pdf [25.11.2019].
3. ISO/IEC 27005, Information technology — Security techniques — Information security risk management [Resursă electronică]. - Regim de access: http://mahdi.hashemitabar.com/cms/images/Download/ISO/iso-iec-27005-2011-english.pdf [25.11.2019].
4. ISO 31000:2009, Risk management — Principles and guidelines [Resursă electronică]. - Regim de access: http://www.amu.kz/fotos-news/vstrecha_rectora_so_stud_31_oct/ISO%2031000-2009.pdf [28.11.2019].
5. „Fundamentals of Risk Management: Understanding Evaluating and Implementing Effective Risk Management" - Paul Hopkin.
6. „Security Risk Management: Building an Information Security Risk Management Program from the Ground Up" – Evan Wheeler.
7. ISACA, CobiT 3rd edition – Control Objectives.
8. „Enterprise risk management a common framework for the entire organization" – Philip E. J. Green (Copyright © 2016 Elsevier Inc. All rights reserved).
9. „Information security risk analysis" third edition – Thomas R. Peltier (© 2010 by Taylor and Francis Group, LLC).
10. „Risk management concepts and guidance" fifth edition – Carl L. Pritchard (© 2015 by Taylor & Francis Group, LLC).