MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microeletronică
Departamentul Ingineria Software și Automatică

Admis la susținere
Șef departament:
Fiodorov Ion, conf. univ.
____
„_____”_____________________ 2021

Governance, Risk & Compliance (GRC) Capability Model the pathway to principled performance

Teză de master

Student:	**Dantiș Ion,** **SI-201M**
Conducător:	**Bulai Rodica,** **asistent universitar**

Chișinău, 2022

Abstract

An integrated Governance, Risk and Compliance (GRC) is one of the most important business requirements in any organization to tackle any cybersecurity threat. The absence of scientific references regarding GRC is leading to a dispersion of concepts involving this topic. Without boundaries and correct domain definition, poor implementation of GRC solutions can lead to low performances and high vulnerabilities for organizations. This research paper discusses the GRC model framework in det ail and its ability in providing correct information workflow and proposes a set of high-level concepts covering the GRC domain. The key functions of governance, risk and compliance and their associations, resulting in a reference conceptual model for integrated GRC are presented. The GRC model is evaluated by comparing the GRC capability model with information security management system (ISMS) and key comparisons are made for risk assessment between GRC and ISMS with an evaluation framework.

Keywords: *governance, risk, compliance, management, assessment.*

Rezumat

Un model de guvernanță, risc și conformitate (GRC) integrat este una dintre cele mai importante cerințe de afaceri din orice organizație pentru a aborda orice amenințare de securitatea cibernetică. Absența referințelor științifice referitoare la GRC duce la o dispersie a conceptelor care vizează acest subiect. Fără limite și definirea corectă a domeniului, implementarea defectuoasă a soluțiilor GRC poate duce la performanțe scăzute și vulnerabilități severe în cadrul organizațiilor. Această lucrare de cercetare evidențiază în detaliu cadrul modelului GRC și capacitatea necesară acestuia de a furniza un flux de lucru corect al informațiilor, precum și propune un set de concepte de nivel înalt care acoperă domeniul GRC. Sunt prezentate funcțiile cheie ale guvernanței, riscului și conformității și asocierile acestora, rezultând un model conceptual de referință pentru GRC integrat. Modelul GRC este evaluat prin compararea modelului de capacitate GRC cu sistemul de management al securității informațiilor (ISMS) și se identifică comparațiile cheie pentru evaluarea riscurilor între GRC și ISMS cu un framework de evaluare.

Cuvinte-cheie: *guvernanță, risc, conformitate, management, evaluare.*

CONTENTS

INTRODUCTION

Information technology (IT) is critical and valuable to our society. IT systems support business processes by storing, processing, and communicating critical and sensitive business data. In addition, IT systems are often used to control and monitor physical industrial processes. For example, our electrical power supply, water supply and railroads are controlled by IT systems. The increase in hacking, the vulnerability of our computer systems and networks to physical attacks and natural disasters, the need to protect the integrity of financial accounting records and privacy and safety concerns, have resulted in the release of a number of security regulations & standards that pertain to information systems in recent years. Security is often thought of as a triage of confidentiality, integrity and availability.

Cyber security assessments need to keep these IT systems in secure continuous working mode and thus, have a focus on availability and integrity of datasets. For instance, because of the consequence of a potential cyber-attack, it is recommended that IT systems should not be updated before extensive testing, and network-based vulnerability assessment.

The research paper attempts to bring about a common understanding of what constitutes the universe of integrated GRC model. Currently, the most complete and recognized framework for integrated GRC was developed by the "Open Compliance & Ethics Group" (OCEG). OCEG is a non-profit organization that uniquely helps other organizations to enhance corporate culture and integrate governance, risk management, and compliance processes.

The paper than describes practices to implement and manage GRC activities containing domain level concepts representing a high level of integration between the following sub-domains: governance, risk management and compliance. To fulfill the scope of the research paper, there were established some main objectives and goals:

- to clearly define and analyze the universe of integrated GRC model with reference to the investigation for the developed by the "Open Compliance & Ethics Group" (OCEG);
- to showcase how a GRC model ensures correct information workflow with examples;
- to compare the benefits of GRC and ISMS in risk assessment.

The methodology applied is divided according to the two processes of design research in information system, build and evaluate. The build process is composed by two stages: constructing the definition and conceptual model construction for a GRC. The first stage, construct definition, has two main milestones: conceptual domain establishment and conceptual definition within the set up boundaries established. This is done by understanding the different components, elements, practices, actions and controls for a GRC model. The evaluation process is composed by only one stage and underscores the quality assessment.

RESOURCES

1. Scott MITCHELL, GRC Capability Model (Red Book), lulu.com; 3rd edition January 20, 2017);
2. "Need: The Need for ISMS". Threat and Risk Management. European Union Agency for Network and Information Security. Retrieved 16 June 2018, [quoted 21.09.2021]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/need;
3. Best practices in GRC convergence, 01 June 2018. [quoted 07.10.2021]. Available: https://www.risk.net/risk-management/1499363/best-practices-grc-convergence;
4. GRC Management: Best Practices Framework for More Effective Governance, Risk, and Compliance Management. [quoted 26.10.2021]. Available: https://www.marcosassi.com.br/grc-management-best-practices-framework-for-more-effective-governance-risk-and-compliance-management;
5. IBM Cloud Education, 18 June 2020, GRC. [quoted 02.11.2021]. Available: https://www.ibm.com/cloud/learn/grc#:~:text=A%20governance%2C%20risk%2C%20and%20compliance,and%20meeting%20regulatory%20compliance%20requirements;
6. TIPTON, H.F.; KRAUSE, M. (2010), Information Security Management Handbook, Volume 3, (6th ed.). CRC Press. pp. 100–02;
7. KATSICAS, SOKRATIS K. (2009). "35". In Vacca, John (ed.). Computer and Information Security Handbook. Morgan Kaufmann Publications. Elsevier Inc. p. 605;
8. "Inventory of Risk Management / Risk Assessment Methods"., ENISA EU. [quoted 18.11.2021]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/inventory-of-risk-management-risk-assessment-methods-1;
9. Technical Department of ENISA Section Risk Management, Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools, Publication date: Jun 01, 2006;
10. Joint Task Force Transformation Initiative, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. [quoted 23.11.2021]. Available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/archive/2014-06-05;
11. CAMPBELL, T. (2016). "Chapter 1: Evolution of a Profession". Practical Information Security Management: A Complete Guide to Planning and Implementation. APress. pp. 1–14. [quoted 30.11.2021]. Available: https://books.google.md/books?id=sbWiDQAAQBAJ&pg=PA1&redir_esc=y#v=onepage&q&f=false;

12. European Union Agency for Network and Information Security. Threat and Risk Management, Retrieved 16 June 2018. [quoted 07.12.2021]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/need;
13. Third Party GRC Maturity Model - A New Paradigm in Governing Third Party Relationships. [quoted 09.12.2021]. Available: https://grc2020.com/product/third-party-grc-maturity-model/.