WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber-security Risks' Impact on the Added Value of Consulting Services for IT-security Management Systems in Holding Companies

Pooja. S .Totare , Prof. M. Rokade

Pooja..S.Totare ,At/Post Pimpalwandi,Tal Junnar,Dist Pune. India
Prof. M.. Rokade ,At/post Otur,Tal Junnar Dist Pune. India.

A B S T R A C T

Many efforts to implement IT-security management systems do not always yield the desired results. They occasionally necessitate higher integrated expenses than anticipated. One cause for this is a lack of effective cyber risk management procedures. This assertion is especially true when it comes to selecting and implementing reliable IT-security management technologies when delivering consulting services. This article examines a cyber-security system implementation scenario. This project was implemented with the help of a well-known consulting firm. When delivering consulting services to Holding firms, the examples presented highlight the selection of IT-security metrics and the usage of various IT-security management systems.

Keywords: Integrated management system; security; IT-security; audit; cyber-security management; consulting; risk management; standard; integrated management system; security; IT-security; audit.

1.INTRODUCTION

In order to understand and analyse their relationships while establishing a cyber-security system for Holding Companies, it is necessary to look at the existing language for the objectives of this article. It is suggested that not only traditional sources – such as the ISO 9000 series (https://www.iso.org/standard/45481.html) – be used as dictionaries, but also a variety of expert techniques that can aid in the development of a consistent language. are the numbers. It is suggested that you start with descriptions of business operations that are targeted at generating added value (not only for external customers, but also for a variety of internal consumers). There is reason to think that business processes, as a valuable asset of modern Holding Companies, are vulnerable to hazards, including IT-security concerns.

PROBLEM STATEMENT

It appears suitable to develop a vision of the IT-Security Management System, which has a substantial impact on Holding Companies and necessitates the implementation of a cyber-security risk management system [10] – [15]. In practice, business process owners in Holding Companies anticipate risks from specialist services (IT or/and IT-security, Management office, accounting, etc.) [6] – [9].

Identify and assess issue locations where losses could occur. The term "loss" encompasses not only the direct financial costs of an IT-security Management System (ISMS), but also the loss of intangible assets (reputation, goodwill), which can havea negative impact on added value.

As a result, for the identified issue areas, appropriate procedures (within the scope of applicable management systems) should be established in advance to prevent such a violation (and, as important, the identification of the fundamental causes of the violation). Such management systems include information security (ISO/IEC 27001), business continuity (ISO/IEC 22301), and IT-service management (ISO/IEC 20000:1).

To establish a successful ISM, it is clear that moving from the application of individual management systems to the deployment of an Integrated Management System (IMS) is required [7] – [9]. This is how the ISMS and cyber-risk system creation problems are solved..

APPROACHES THAT ARE WELL-KNOWN

There are a number of techniques to developing contemporary IMS, some of which are advocated as "best practices" forHolding Companies:

- The ISO approach, in which different management systems are implemented (according to ISO, over 1 million implementations of ISO 9001, more than 39 thousand implementations of ISO/IEC 27001, and more than 5,000 implementations of ISO/IEC 20000:1). Only 12% of all projects have incorporated IMS, according to statistics.
- The approach to standardization described by the USSR's Union Committee for Standardization (led by V. S. Emelyanov from 1940 to 1946), according to which proposed standards were rejected if the indicators were concentrated on one industry without considering the others. In 1943, for example, 488 3 standards were authorized while 71 projects were turned down.
- M. Greaves proposed the "digital doubles" paradigm in 2002, which governs the use of mirrored information in object management throughout the entire Life-cycle management (LCM). The most important are "operating doubles," which need a lot of computing power (Pflops) on high-performance servers.
- Due to uneven coverage of functions, complexity of installation, mandatory engagement of several staff, and high total cost of ownership, GRC-class solutions (Governance, Risk, Compliance) presented by the largest software companies (e.g., RSA, Oracle, SAP, etc.) are not commonly employed.

TOOLS FOR CYBER-SECURITY

Considering the unpleasant experience of communicating with consultants (including the aforementioned), For example, the ISMS team used the well-knownISO standard. 9001, 14001, 22150, 27001, 45001, and ISO 9001, 14001, 22150, 27001, 45001, and ISO 9001, 14001, 22150, ISO standards 19011, 31000, 38500, and 39000 arealso available. 37000 is a series of computers. Taking into account the particulars of the situation ISMS and cyber-security system deployment for the It was found that two sets of tools are required by Holding Company.

MANAGEMENT SYSTEMS CYBER-THREATS

Creating an ISMS and a cyber-security system is very different from consulting projects for simple Quality Management Systems (QMS), which are well-known around the world and used by large Russian corporations like Gazprom. The cyber-security system is unique in that the management object is not well-known operations of hydrocarbon raw material extraction, transportation, processing, and marketing, but objects of investment intangible generation – the essence of the ISMS.

The IMS should be backed by the cybersecurity system, which should take into account a large number of aspects referred to as "external issues" and "internal issues" in ISO standards. Another feature of integration was established within the cyber-security system's framework: ISMS risks, including consulting risks, were incorporated into the IMS's "single management framework".

CONCLUSION

When establishing an ISMS in the Holding Company, it is required to do so in accordance with the Place figures and tables at or near the top or bottom of columns where possible. Large figures and tables may span across both columns. Figure captions must be below the figures; table captions must be above the tables. Avoid placing figures and tables before their first mention well-known ISO standards 9001, 14001, 22150, 27001, 45001, and so on.

It's also crucial to consider future ISO standards in the works, such as the 37500, 38500, and 30401 series. These needs should be taken into account as much as feasible when consulting firms are sought, and standard risk management methods should be established and maintained from the start of the life- cycle management process. The recommended strategy will provide manageable conditions for producing additional revenue from the Holding Company's cyber security system installation.

REFERENCES

[1] Pawel A. Lontsikh1, Natalya P. Lontsikh, Elena Y.Golovina, Olga M. Safonova2. 2020 International Conference on Quality Management, Transport and Information Security, Information Technologies National Research Irkutsk State Technical University Irkutsk, Russia

[2] Monika D.Rokade ,Dr.Yogesh kumar Sharma,‖Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic.‖ IOSR Journal of Engineering (IOSR JEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719

[3] Monika D.Rokade ,Dr.Yogesh kumar Sharma‖MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset‖, 2021 InternationalConference on Emerging Smart Computing and Informatics (ESCI),IEEE

[4] Monika D.Rokade, Dr. Yogesh Kumar Sharma. (2020). Identification of Malicious Activity for Network Packet using Deep Learning. *International Journal of Advanced Science and Technology*, *29*(9s), 2324 - 2331.

[5] Sunil S.Khatal ,Dr.Yogesh kumar Sharma, ―Health Care Patient Monitoring using IoT and MachineLearning.‖,

[6] IOSR Journal of Engineering (IOSR JEN), ISSN(e): 2250-3021, ISSN (p): 2278-8719

[7] Sunil S.Khatal ,Dr.Yogesh kumar Sharma, ―Data Hiding In Audio-Video Using Anti Forensics Technique ForAuthentication ", IJSRDV4I50349,Volume : 4, Issue : 5

[8] Sunil S.Khatal Dr. Yogesh Kumar Sharma. (2020). Analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. *International Journalof Advanced Science and Technology*, *29*(9s), 2340 - 2346.