International Journal of Information Security and Privacy
Volume 20 • Issue 1 • January-December 2026

Critical Success Factors for an Effective Security Risk Management Program:
An Exploratory Case Study

Jason A. Williams
http://orcid.org/0000-0002-3417-440X
Augusta University, USA

Humayun Zafar
Kennesaw State University, USA

Saurabh Gupta
http://orcid.org/0000-0002-5622-341X
Kennesaw State University, USA
Received: October 9th, 2025 | **Accepted:** March 5th, 2026

ABSTRACT

This paper evaluates the perceived effectiveness of the security risk management (SRM) programs at a Fortune 500 firm. Layers of management and staff participated in the study. Perceived effectiveness of their SRM programs was based on nine critical success factors (CSFs). Interviews confirmed six initial CSFs (Executive Management Support, Organizational Maturity, Open Communication, Risk Management Stakeholders, Team Member Empowerment, and Holistic View of an Organization) that were extracted from the literature. They were confirmed and synthesized with three additional CSFs (Security Maintenance, Corporate Security Strategy, and Human Resource Development). Implications for SRM are discussed.

KEYWORDS

Information Security, Security Risk Management, Critical Success Factors

INTRODUCTION

According to an Ernst & Young Global Information Security Survey (Bandyopadhyay et al. 2009), organizations are increasingly recognizing information security risks and are improving the effectiveness of their information security programs. However, a large portion (64%) of the survey respondents indicated that the level of employee security awareness was either a significant or a considerable challenge in meeting their information security initiatives. Lack of compliance with information security policies is a major problem (Siponen and Vance 2010). In addition, outsider threats, such as viruses and system penetration attacks continue to increase in cost and complexity.

Security risk management (SRM) refers to a series of mechanisms put in place by an organization to counter or prevent information security related events (Blakley et al. 2001). An (Williams et al. 2024) information security event may include factors such as insider threats, malware, and unauthorized access. Examples of mechanisms that prevent security events include implementation of clearly defined information security policies, secure computing practices, and employee training programs (Spears and Barki 2010; Williams et al. 2024). Since SRM impacts the organization as a whole and focuses

DOI: 10.4018/IJISP.404388

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

on confidentiality, integrity, and availability of data, it is imperative that effective SRM policies and practices be established and followed.

SRM is not a standalone activity. Instead, it is a series of interrelated activities that take place throughout an organization (Dhillon 2007). This means addressing potential threats in all organizational assets, whether they be equipment, processes, data, or facilities (Gibson and Igonor 2020) and establishing and executing security policies. Considering the overarching impact of an SRM program, it is surprising to note that little research has been conducted to understand what constitutes an effective SRM program.

Kotulic (2001) developed an instrument that provided a starting point for the development of theory-based guidelines to measure the efficacy of SRM programs. His model included a direct relationship between executive management support and SRM program effectiveness. In order to be effective, security controls must be in line with the goals and objectives of an organization (Khansa and Liginlal 2011; Spears and Barki 2010; Williams et al. 2019) Therefore, it is important to focus on the information needed to attain these goals and objectives.

One systematic method to identify and measure organizational goals and objectives is through the use of critical success factors (CSFs). CSFs are things that must go well to ensure success for a manager or an organization (Rockart 1979). We contend that employee understanding of CSFs as they relate to SRM can allow an organization to maximize the overall effectiveness of its SRM program. Therefore, we expanded upon Kotulic's research by incorporating a modified version of the CSF method.

The purpose of this study is to identify CSFs as they relate to SRM, as perceived by both management and staff. Currently, no studies have focused on the shared understanding of CSFs between management and staff. Staff may have varying perspectives of the CSFs that executive management set in place to ensure SRM effectiveness. This can impact the actual effectiveness of SRM programs.

Initial CSFs were extracted from the literature, which provides insight into recurring patterns of actions that are considered important for effective functioning in an organization (Kahn et al. 1964). Through a series of interviews, we extracted additional CSFs, which formed our holistic list of CSFs which were prioritized with a Q-sort.

The remainder of this paper is organized as follows. First, we provide a literature review, focusing on CSFs and SRM. Next, we describe our mixed method research design, along with detailed discussion of both qualitative and quantitative portions of the study. This is followed by detailed discussion of the results and contributions to practice. We conclude the paper by discussing limitations and suggestions for future research.

LITERATURE REVIEW OF CRITICAL SUCCESS FACTORS

This section first focuses on studies that investigated the critical success factors concept, followed by studies pertaining to organizational information security.

Critical Success Factors (CSF)

The CSF method was initially proposed (Rockart 1979) to help CEOs specify their information needs related to critical firm issues so that systems could be developed to meet those needs. CSFs are intended performance consequences of systems and behaviors within the firm, which are strongly related to the achievement of desired firm objectives. Benefits of CSFs include 1) identifying factors to focus management scrutiny, 2) establishing measures for evaluation, 3) focusing attention on significant data to be collected, 4) accommodating change within an organization, and 5) assisting in the planning process (Rockart 1979).

In information systems, the CSF method has been introduced as a mechanism for aligning IT planning with the strategic direction of an organization (Rockart 1979). User acceptance is a major benefit of using the CSF method. Managers seem to intuitively understand the thrust of the CSF

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/critical-success-factors-for-an-effective-security-risk-management-program/404388

Related Content

dDelega: Trust Management for Web Services
Michele Tomaiuolo (2013). *International Journal of Information Security and Privacy (pp. 53-67).*
www.irma-international.org/article/ddelega/95142

Chaos Synchronization
Hassan Salariehand Mohammad Shahrokhic (2011). *Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption (pp. 152-182).*
www.irma-international.org/chapter/chaos-synchronization/43289

Enforcing Privacy on the Semantic Web
Abdelmounaam Rezgui, Athman Rouguettayaand Zaki Malik (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 3713-3727).*
www.irma-international.org/chapter/enforcing-privacy-semantic-web/23321

Diversity and Inclusion: Harnessing the Power of Inclusivity for Business Success
G. Meena, R. Vettriselvan, Deepa Rajesh, Palanivel Rathinasabapathi Velmuruganand Revanth Kumar A. (2025). *Security and Strategy Models for Key-Solving Institutional Frameworks (pp. 203-234).*
www.irma-international.org/chapter/diversity-and-inclusion/380675

Software Defined Intelligent Building
Rui Yang Xu, Xin Huang, Jie Zhang, Yulin Lu, Ge Wuand Zheng Yan (2015). *International Journal of Information Security and Privacy (pp. 84-99).*
www.irma-international.org/article/software-defined-intelligent-building/148304