پژوهش‌های مدیریت عمومی
سال دوازدهم ، شماره چهل و سوم ، بهار ۱۳۹۸
صفحه ۲۴۹-۲۲۵

تاریخ دریافت : ۱۳۹۶/۱۲/۱۲
تاریخ پذیرش: ۱۳۹۷/۰۳/۱۹

The Effect of the Implementation of Information Security Management System (ISMS) and Information Technology Infrastructure Library (ITIL) on the Promotion of Information Systems and Information Technology Services Continues

Ahmad Salehi[1], *Zahra Vazife[2]

1-MSc, Information Technology Management, Faculty of Management and economics, University of Sistan and Baluchestan, Zahedan, Iran
2-Assistant Professor, Faculty of Management and Economics, University of Sistan and Baluchestan, Zahedan, Iran. (Corresponding Author). Email: vazife@mgmt.usb.ac.ir

Received: 03/03/2018; Accepted: 09/06/2018

Abstract

The purpose of this study was to investigate and analyze the factors affecting the upgrading of information systems and the continues of information technology services. Based on model, this research effective factors of implementation of Information Security Management System (ISMS) are 9 dimensions and effective factors of Information Technology Infrastructure Library (ITIL) are 5 dimensions were investigated and analyzed. This research is orientated, applied and descriptive. The average number of members of the statistical community in this study was 100 people, including managers and experts in the field of information security and IT services, public and private organizations, senior managers of companies providing management, technical, operational and educational services Information security and, ultimately, professors and experts with the field of activity or research in the field of security and IT services. The sample size was calculated based on Cochran method and data was collected by using a questionnaire tool for 80 members of the statistical community. For reliability of research variables, Cronbach's alpha coefficient and composite reliability have been used. Cronbach's alpha coefficient of all variables is greater than the minimum value of 0.65. To verify the construct validity (convergent), a confirmatory factor analysis was used. All mean values of extracted variance are more than 0.5, and therefore, the model of

measurement has an appropriate convergent validity. In this research, factor analysis, partial least squares and one-sample t-test were used to test the questions and fitness of the model. Based on the findings, the impact of the implementation of Information Security Management System and Information Technology Infrastructure Library on the promotion of information systems and the continuity of information technology services were confirmed and effective factors of expression and strategies for improving the status of organizations were presented.

Introduction

In today's world, the most important security concerns associated with information systems include the infiltration of information systems, the interruption and disruption of vital services, and theft, alteration or destruction of information. Approaches have been introduced to ensure information security. The Information Security Management System (ISMS) is a comprehensive approach to ensuring information security of organizations. On the other hand, the competitive business environment and the strong dependence on information technology services have led organizations to be judged on the basis of the ability to continuously and continuously provide services. Therefore, ensuring the continuity of information technology services is one of the most important issues that should be addressed in the business. The Information Technology Infrastructure Library (ITIL) is a framework for managing, delivering service and implementing IT activities in organizations. So, given the importance of the issue, the main question we are looking for in this study is whether the implementation of the information security management system and the IT infrastructure library in an organization promotes the information systems and the continuation of IT services?

Case study

Managers and experts in the field of information security and (ITS) Information technology services are governmental and private organizations that have implemented the Information Security Management System and the Information Technology Infrastructure Library in Zahedan and Mashhad. Top Managers of Providers of Management, Technical, Operational, and Educational Services for Information Security and Advice on the Implementation of the (IS) and (ITS) which have been licensed by the Ministry of Communications and Information Technology (ICT). Ultimately, professors, experts, and researchers are in the field of activity or research in the field of information security and information technology services.

Materials and methods

The present research is descriptive in nature and descriptive in terms of

method, quantitative and in process and applied in term of purpose. Data collection was done by using a questionnaire in Lekert scale MS. For collecting information on theoretical foundations and research literature, library resources, articles, e-resources, standards and authoritative journals have been used. To verify the validity of the model, a confirmatory factor analysis and Kolmogorov-Smirnov test were used to test the normal variables. Then, using the partial least squares method (PLS) and single sample t-test, the questionnaire has been studied.

Discussion and Conclusion

A correlation coefficient was used to confirm the relationship between the implementation of ISMS and ITIL in promotion information systems and the continuity of IT services, which was confirmed by the results of this hypothesis. Also, to investigate the impact of ISMS and ITIL implementation on the promotion of information systems and the continuity of IT services, partial least squares method was used, which was confirmed in all cases. According to the results of the analyzes, indicators such as defining goals and policies for managing service continuity, evaluating and identifying processes in the organization, prioritizing events in terms of its impact and urgencies, examining all information security incidents and the reasons for the occurrence And prevent it from re-establishing it; responding appropriately and learning about security incidents; defining and identifying identity information for employees to access information resources; monitoring network, router settings, switch and penetration testing at regular intervals; procurement and testing Backup information; Install antivirus and firewalls in the network; Take the necessary measures entry of authorized persons and the security of offices, rooms and facilities; the inclusion of security provisions in the design of the basic principles of configuration. It has the greatest impact on the upgrading of information systems and the continuity of IT services in organizations, and other indicators also have an impact but are less than socalled factors.

Key Words*:* Information Security, Information Security Management System, Information Systems, IT Service Continuity Management, Information Technology Infrastructure Library**.**

بررسی تأثیر پیاده‌سازی ISMS و ITIL بر ارتقاء سیستم‌های اطلاعاتی و تداوم خدمات فناوری اطلاعات

احمد صالحی* – دکتر زهرا وظیفه**

چکیده

پژوهش حاضر با هدف بررسی و تحلیل عوامل تأثیرگذار در ارتقاء سیستم‌های اطلاعاتی و تداوم خدمات فناوری اطلاعات انجام شده‌است. براساس مدل این پژوهش، عوامل مؤثر پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) در ۹ بُعد و عوامل مؤثر کتابخانه زیرساخت فناوری اطلاعات (ITIL) در ۵ بُعد موردبررسی و تحلیل قرارگرفته‌اند. این پژوهش از نوع توصیفی-پیمایشی است. متوسط تعداد اعضای جامعه آماری این پژوهش ۱۰۰ نفر در نظر گرفته شده که شامل مدیران و کارشناسان حوزه امنیت اطلاعات و خدمات فناوری اطلاعات سازمان‌های دولتی و خصوصی، مدیران ارشد شرکت‌های ارائه‌دهنده خدمات مدیریتی، فنی، عملیاتی و آموزشی امنیت اطلاعات و درنهایت اساتید و خبرگان با زمینه فعالیت یا پژوهش حوزه امنیت و خدمات فناوری اطلاعات است. حجم نمونه بر اساس جدول مورگان محاسبه و داده-ها با استفاده از ابزار پرسشنامه برای ۸۰ نفر از اعضای جامعه آماری ارسال و جمع‌آوری شده‌است. برای پایایی متغیرهای پژوهش از ضریب آلفای کرونباخ و پایایی ترکیبی استفاده شده‌است که ضریب آلفای کرونباخ تمامی متغیرها از حداقل مقدار ۰/۶۵ بیشتر است. برای بررسی روایی سازه (همگرا) از تحلیل عاملی تاییدی استفاده شد. تمامی مقادیر میانگین واریانس استخراج‌شده از ۰/۵ بیشتر هستند و بنابراین مدل اندازه‌گیری از روایی همگرای مناسب برخوردار است. در این پژوهش جهت آزمون سوالات و برازندگی مدل از روش تحلیل عاملی، حداقل مربعات جزئی و آزمون t تک نمونه‌ای استفاده شده‌است. بر اساس یافته‌ها، تاثیر پیاده‌سازی سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات بر ارتقاء سیستم‌های اطلاعاتی و خدمات فناوری اطلاعات تأیید گردید و عوامل تأثیرگذار بیان و راهکارهایی برای بهبود وضعیت سازمان‌ها ارائه شده‌است.

واژه‌های کلیدی: امنیت اطلاعات، سیستم مدیریت امنیت اطلاعات، سیستم‌های اطلاعاتی، مدیریت تداوم خدمات فناوری اطلاعات، کتابخانه زیرساخت فناوری اطلاعات.

* کارشناس ارشد مدیریت فناوری اطلاعات، دانشکده مدیریت و اقتصاد، دانشگاه سیستان و بلوچستان، زاهدان، ایران.
** نویسنده مسئول- استادیار ، دانشکده مدیریت و اقتصاد، دانشگاه سیستان و بلوچستان، زاهدان، ایران.
vazife@mgmt.usb.ac.ir

مقدمه

در طول دو دهه‌ی گذشته، ماهیت سیستم‌های اطلاعاتی به‌طور عمده‌ای تغییریافته و تبدیل به بخش بزرگی از فرآیندهای کسب‌وکار شده‌است (*Siyadat & Saghafi, 2015*). اطلاعات، به یک دارایی استراتژیکی توسعه‌یافته و سیستم‌های اطلاعاتی به یک ابزار استراتژیکی برای سازمان‌ها و دولت‌ها تبدیل شده‌است. سیستم‌های اطلاعاتی نیز همواره در خطر سرقت اطلاعات، تغییر اطلاعات و ایجاد وقفه در خدمات‌رسانی هستند (*Taj Far, Mahmoudi, Reza Soltani, & Reza Soltani, 2014*). بدیهی است که در این شرایط روش‌های حفاظت فیزیکی به تنهایی قادر به تأمین امنیت نخواهند بود. لذا سازمان‌ها ناچار به‌کارگرفتن روش‌های جدید حفاظت اطلاعات و کنترل دسترسی‌ها به منابع سازمان شده‌اند. کرامر[1] (۲۰۰۶) بیان می‌کند، به‌منظور حل مسئله امنیت اطلاعات، سازمان نیازمند به‌کارگیری طیف گسترده‌ای از دانش، فناوری و قوانین سازمانی است. ازاین‌رو طراحی و پیاده‌سازی سیستم مدیریت امنیت اطلاعات[2] راهکاری جامع برای هر سازمان است. همچنین امروزه در سازمان‌ها علاوه بر برقراری مداوم امنیت فرآیندهای کسب‌وکار و سیستم‌های اطلاعاتی همه چیز به‌عنوان یک خدمت در نظر گرفته می‌شود که می‌تواند در ارتباط مستقیم یا غیرمستقیم با مشتری باشد، به‌کارگیری فناوری اطلاعات نیز به مدیریتِ خدمات در جهت کاهش هزینه‌های ارائه‌ی خدمات و بهبود کیفیت خدمات و درنتیجه به موفقیت سازمان در جلب رضایت مشتریان کمک می‌کند (*Esteves& Alves, 2013*)؛ از طرفی محیط رقابتی کسب‌وکار و وابستگی شدید به خدمات، باعث شده که سازمان‌ها بر پایه میزان توانایی در ارائه مستمر و دائمی خدمات، مورد ارزیابی قرار گیرند. هر سازمانی که با هدف پشتیبانی از فرایندهای کسب‌وکار، خدمات فناوری اطلاعات[3] را به مشتریانش تحویل می‌دهد به ساختار مناسبی نیاز دارد. در گذشته، این ساختار برمبنای کارکردها و توانایی‌های فنی بود. اما امروزه این رویکرد دیگر مناسب نیست. کتابخانه زیرساخت فناوری اطلاعات[4] برای سازمان‌ها یک راه بسیار خوب برای مدیریت کردن، تحویل خدمت و اجرا کردن فعالیت‌های فناوری اطلاعات در فرایندها می‌باشد (*Marta, Alberto & Silva, 2015*). ازآنجایی‌که یکی از حوزه‌های مدیریت خدمات، بحث امنیت است و با توجه به

1-Kraemer
2-Information Security Management System (ISMS)
3-Information Technology Service
4-Information Technology Infrastructure Library (ITIL)

انتشار بخشنامه‌های منتشرشده از سوی شورای عالی امنیت فضای تبادل اطلاعات کشور در سال‌های گذشته و مصوبه‌ها و بخشنامه‌های مختلف که پیاده‌سازی یکی از دیدگاه‌های فرآیندی، موسوم به سیستم مدیریت امنیت اطلاعات بر مبنای ISO 27001:2013 به کلیه سازمان‌های دولتی توصیه شده‌است (*Efta document, 2007; NAMA 2015*)، ضرورت پیاده‌سازی چنین سیستم‌هایی بیش‌ازپیش شده‌است. درعین‌حال در چارچوب کتابخانه زیرساخت فناوری اطلاعات مباحثی چون تداوم خدمات فناوری اطلاعات[1] و مدیریت حوادث که نقشی در پشتیبانی تداوم کسب‌وکار دارد مطرح شده‌است. بنابراین اهمیت مباحث مربوط به مدیریت خدمات فناوری اطلاعات و مدیریت امنیت سیستم‌های اطلاعاتی و تداوم خدمات کسب‌وکار بیش‌ازپیش نمایان می‌شود. تنها در صورتی که به این مفاهیم صحیح و منسجم پرداخته‌شود، در رشد و بقای سازمان‌ها تأثیر بسزایی می‌گذارد. در این پژوهش به این ارتباطات پرداخته‌می‌شود تا با به‌کارگیری این مفاهیم و شناسایی عوامل مؤثر به مدیریت یکپارچه و بهتری دست یابیم و در قالب مدیریت خدمات سرویس‌هایی دائمی ارائه دهیم. لذا با توجه به اهمیت موضوع، سؤال اصلی که در این تحقیق به دنبال پاسخی برای آن هستیم این است که آیا پیاده‌سازی سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات در یک سازمان باعث ارتقاء سیستم‌های اطلاعاتی و تداوم خدمات فناوری اطلاعات می‌شود؟

پیشینه نظری تحقیق

سیستم‌های اطلاعاتی

یک سیستم اطلاعاتی[2]، اطلاعات را برای یک هدف خاص، پردازش، ذخیره، تحلیل و توزیع می‌کند. مانند هر سیستم دیگر، سیستم اطلاعاتی شامل ورودی، پردازش و خروجی است. این سیستم ورودی را پردازش و خروجی را به کاربر یا به سیستم دیگر ارسال می‌کند (*Yaghoubi, shokouhi & Salavati, 2015*). یک سیستم اطلاعاتی را ازنظر فنی می‌توان به‌صورت مجموعه‌ای از مؤلفه‌های وابسته به هم تعریف کرد که اطلاعات را به‌منظور پشتیبانی از تصمیم‌گیری و کنترل در سازمان، گردآوری(یا بازیابی)، پردازش، ذخیره و توزیع می‌کند (*Laudon & Laudon, 2010*). در تمام انواع سیستم‌های اطلاعاتی، انسان‌ها، سخت‌افزارها، نرم‌افزارها، داده‌ها و شبکه‌ها پنج منبع اصلی سیستم‌های اطلاعاتی

1-IT Service Continuity
2-Information Systems

می‌باشند. منابع انسانی شامل کاربران نهائی و متخصصین سیستم‌های اطلاعاتی می‌باشد. منابع نرم‌افزاری شامل هم برنامه‌ها و هم رویه‌ها می‌باشد. منابع داده‌ها شامل پایگاه داده‌ها و پایگاه‌های دانش و منابع شبکه شامل شبکه‌ها و رسانه‌های ارتباطی است(*obrien, 2006*).

مفهوم سیستم مدیریت امنیت اطلاعات

سیستم مدیریت امنیت اطلاعات استانداردهایی را برای ایمن‌سازی فضای تبادل اطلاعات و سیستم‌های اطلاعاتی در سازمان‌ها ارائه می‌دهد. این استانداردها شامل مجموعه‌ای از دستورالعمل‌هایی است تا بتواند فضای تبادل اطلاعات یک سازمان را با اجرای یک طرح مخصوص به آن سازمان ایمن نماید. سیستم مدیریت امنیت اطلاعات، با به‌کارگیری یک فرایند مدیریت مخاطرات، از محرمانگی، صحت و دسترس‌پذیری اطلاعات محافظت می‌کند و به طرف‌های ذینفع این اطمینان را می‌دهد که مخاطرات، به میزان کافی مدیریت می‌شوند. توجه داشته باشید که سیستم مدیریت امنیت اطلاعات، با فرایندهای سازمان و ساختار مدیریتی کلان، یکپارچه بوده و بخشی از آن‌ها است و همچنین امنیت اطلاعات در طراحی، فرایندها، سیستم‌های اطلاعاتی و کنترل‌ها لحاظ می‌شود، بنابراین انتظار می‌رود که پیاده‌سازی یک سیستم مدیریت امنیت اطلاعات، منطبق با نیازهای سازمان باشد (*ISO/IEC 27001, 2013*).

استانداردهای متعددی در کشورهای گوناگون برای ایجاد امنیت اطلاعات سازمانی تدوین و پیشنهاد شده‌است. در تاریخ ۲۵ سپتامبر ۲۰۱۳ پیش‌نویس نسخهٔ جدید استاندارد 27001 با نام ISO/IEC 27001: 2013[1] منتشر و جایگزین استاندارد قبلی، یعنی ISO/IEC 27001: 2005 شد(*Haufe, Colomo-Palacios, Dzombeta& Brandis, 2016*). از ویژگی‌های این استاندارد وجود ۱۱۳ کنترل امنیتی در قالب ۳۵ هدف کنترلی و ۱۴ حوزه شامل خط‌مشی، مدیریت دارایی، امنیت منابع انسانی، امنیت فیزیکی و محیطی، امنیت عملیات، امنیت ارتباطات، کنترل دسترسی، رمزنگاری، ارتباط با تأمین‌کنندگان، اکتساب، توسعه و نگهداری سیستم‌های اطلاعاتی، مدیریت حوادث امنیت اطلاعات، مدیریت تداوم کسب‌وکار و انطباق است که جنبه‌های گوناگون مدیریتی، عملیاتی و فنی را در یک سازمان پوشش می‌دهد (*ISO/IEC 27001, 2013*).

1-International Organization for Standardization/International Electrotechnical Commission

کتابخانه زیرساخت فناوری اطلاعات

کتابخانه زیرساخت فناوری اطلاعات (ITIL) رویکردی نظام‌مند برای عرضه خدمات فناوری اطلاعات ارائه می‌دهد. تفکر کتابخانه زیرساخت فناوری اطلاعات در دهه‌ی ۱۹۸۰، زمانی به وجود آمد که دولت انگلستان متوجه شد که سطح کیفی خدمات فناوری اطلاعات که در کشور ارائه می‌شود کافی و قابل‌قبول نیست. لذا مأموریت یافت تا بستر و چارچوبی ارائه کند، تا به کمک آن دولت انگلستان و بخش خصوصی از منابع فناوری اطلاعات به‌صورت بهینه و کارآمد و ازنظر مالی به‌صورت معتبر استفاده کنند (*Marta, Alberto& Silva, 2015*). به‌طورکلی می‌توان این‌طور بیان کرد که کتابخانه زیرساخت فناوری اطلاعات مجموعه‌ای از تجربه‌های موفق و بهترین افکار، الگوها و روش‌ها در زمینه مدیریت خدمات فناوری اطلاعات است که در یک سازمان گردش فرایندهای کسب‌وکار را مشخص می‌کند (*Norita, Noha& Faten, 2013*). کتابخانه زیرساخت فناوری اطلاعات را می‌توان یک خط‌کش دانست که مفاهیم تجربه‌شده را مستند کرده و با زبان واحد بیان می‌کند. به‌عبارت‌دیگر کتابخانه زیرساخت فناوری اطلاعات، مجموعه‌ای از مفاهیم و قوانین برای مدیریت فناوری اطلاعات است (*Ahmadi, 2016*): هدف اولیه آن رسیدن به یک سیستم مدیریت خدمات برای شرکت‌های فعال در زمینه فناوری اطلاعات و رضایت مشتری بود (*Steinberg, 2014*).

تداوم خدمات فناوری اطلاعات

طرح تداوم خدمات فناوری اطلاعات[1] تأثیر حوادث را بر خدمات فناوری اطلاعات به شکل خاص مورد بررسی قرار می‌دهد و برای حفظ و تداوم خدمات فناوری اطلاعات جهت پشتیبانی از تداوم عملیات کسب‌وکار در زمان بروز حادثه تلاش می‌کند. همچنین نقش ارزشمندی در پشتیبانی از فرآیند برنامه‌ریزی تداوم کسب‌وکار فراهم می‌کند. مدیریت تداوم خدمات فناوری اطلاعات[2]، به مدیریت قابلیت‌های سازمان در تداوم ارائه سطحی توافقی و از پیش تعیین‌شده از خدمات فناوری اطلاعات، به‌منظور پشتیبانی از نیازمندی‌های کسب‌وکار در شرایط بروز حوادث می‌پردازد. این حوادث محدوده وسیعی شامل خرابی یک سیستم یا یک برنامه کاربردی، تا از دست رفتن کامل دارایی‌های کسب‌وکار را دربرمی‌گیرد. مدیریت تداوم خدمات فناوری اطلاعات چارچوبی برای توسعه طرح‌های

1- IT Service Continuity Planning (ITSCP)
2- IT Service Continuity Management (ITSCM)

بازیابی ساختار فناوری اطلاعات در پشتیبانی از طرح‌های مدیریت تداوم کسب‌وکار ارائه می‌دهد. بنابراین می‌توان مدیریت تداوم خدمات فناوری اطلاعات را به‌عنوان بخش درونی از فرآیند مدیریت تداوم کسب‌وکار برای اطمینان از امکان ارائه خدمات فناوری اطلاعات قلمداد نمود (*Karimi Balan, 2009*).

پیشینهٔ تجربی

سونگ‌یانگ[1] و همکارانش (۲۰۱۷) در تحقیقی با عنوان " ارزیابی سیستم امنیت اطلاعات با استفاده از استدلال معنایی و رویکرد مبتنی بر گراف " دریافتند که با توجه به هدف‌قراردادن شرکت‌های مجهز به شبکه‌های بزرگ‌تر به جهت ارزش بالای اطلاعات کسب‌وکار و پیچیده بودن حملات سایبری، مهاجمان تلاش می‌کنند تا به عمق شبکه و اطلاعات آن نفوذ و دسترسی پیدا کنند. بنابراین یک الزام امنیتی مهم این است که متخصصین و مدیران شبکه دارای یک دانش مشترک برای به اشتراک گذاشتن امنیت اطلاعات باشند تا به‌سرعت به یکدیگر کمک کنند و به تهدیدات جدید پاسخ دهند. در این پژوهش یک چارچوب سیستم کارآمد برای مقابله با حمله و ارزیابی امنیت شبکه پیشنهاد شده است. ناوت هایف[2] و همکارانش (۲۰۱۶) در مطالعه فرآیندهای کلیدی ISMS بیان داشتند که استراتژی‌های ISMS باید با مأموریت سازمان، سیستم‌های نرم‌افزاری و سخت‌افزاری، آموزش‌ها و جوّ فرهنگی کارکنان سازمان هماهنگ و سازگار شود. سریکا[3] و همکارانش (۲۰۱۶) مسئله رویکرد چندبعدی را برای امنیت مدیریت شبکه بررسی کردند. به عقیده آن‌ها برای پیاده‌سازی ISMS باید پنج بُعد، دسترسی به اطلاعات و سیستم‌ها، امنیت ارتباطات، زیرساخت‌ها، مدیریت امن و امنیت توسعهٔ سیستم‌های اطلاعات مدنظر قرارگیرند. هامفریس[4] (۲۰۰۸) استانداردهای مدیریت امنیت اطلاعات: پذیرش، نظارت و مدیریت ریسک را بررسی کرده‌است. هامفریس به‌طور خاص در این پژوهش روی تهدیدات داخلی به‌عنوان مثالی از مسائل و مشکلات رو به رشدی که سازمان‌ها نیاز است با آن‌ها مواجه شوند تمرکز دارد و تفسیر می‌کند که چگونه استاندارد مدیریت امنیت اطلاعات در حل این مشکلات و تهدیدات، مفید واقع می‌شوند. سیادت و همکارانش (۲۰۱۷) در زمینهٔ

1-Songyang
2-Knut Haufe
3-Srikanta
4-Humphreys

چالش‌ها و راهکارهای موجود در پیاده‌سازی ISMS در نظام بانکی به مواردی از قبیل نگاه پروژه محور داشتن نسبت به بحث ISMS، نبود فرهنگ و پیش‌زمینه مناسب برای پیاده-سازی ISMS در سازمان، عدم آموزش پرسنل، تحلیل هزینه فایده این سیستم به‌عنوان بخشی از سیستم کلان مدیریتی سازمان جهت پیاده‌سازی موفق ISMS اشاره داشتند. امیدی‌فر (۲۰۱۵) در بررسی و رتبه‌بندی عناصر سیستم مدیریت امنیت اطلاعات در شرکت مخابرات خراسان جنوبی بیان می‌کند که ابعاد امنیت فیزیکی و محیطی و امنیت منابع انسانی سازمان مورد مطالعه از وضعیت مناسب برخوردار است. در بُعد کنترل دسترسی‌ها وضعیت نسبتاً مطلوب و در بُعد مدیریت دارایی‌ها و مدیریت رخدادهای امنیت اطلاعات شرایط مناسب نمی‌باشد. تاج‌فر و همکارانش (۲۰۱۴) به رتبه‌بندی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف پرداختند. آن‌ها معتقدند ناهمخوانی ساختار سازمانی با نیازهای سیستم مدیریت امنیت اطلاعات، عدم بلوغ سازمانی، برخوردار نبودن از کمیته راهبری شایسته و بی‌ثباتی مدیریت ارشد سازمان از مهم‌ترین موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات هستند *(Taj Far, Mahmoudi, Reza Soltani, & Soltani, 2014)*.

نوریتا[1] و همکارانش (۲۰۱۳) در پژوهشی با عنوان "مدل پذیرش فناوری و نقشه راه برای موفقیت پیاده‌سازی ITIL" هدف از این پژوهش را پیشنهاد استفاده از مدل UTAUT[2] به‌عنوان یک مدل برای مدیریت فناوری اطلاعات، به‌ویژه ITIL بیان می‌کنند که به مدیران برای بهبود هرچه بهتر عملکرد کسب‌وکار، تصمیم‌گیری بهتر در مورد فرآیندهای کسب‌وکار و چگونگی پیاده‌سازی فرایندهای ITIL کمک می‌کند. وینفرد[3] و همکارانش (۲۰۱۱) در پژوهش اصطلاحات و مشخصه‌های ITSM[4] توضیحی در مورد هر یک از چارچوب‌های ITIL، مدیریت سطح خدمات، مدل COBIT[5] و مدیریت کسب‌وکار ارائه دادند. هدف این تحقیق این است تا میزان آشنایی و فهم مدیران فناوری اطلاعات را از استانداردها و چارچوب‌های فوق محک زنند. کاتر استیل[6] (۲۰۰۹)، در زمینهٔ دلایل،

1-Norita
2-Unified Theory of Acceptance and Use of Technology
3-Winfred
4-IT Service Management
5-Control Objectives for Information and related Technology
6-Carter-Steel

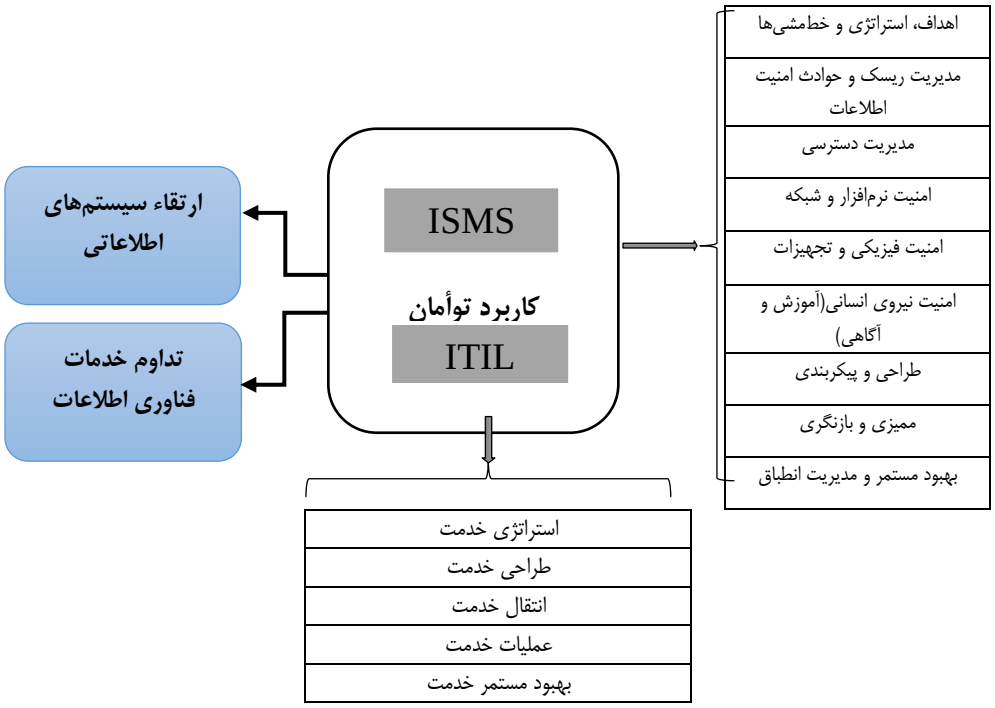
استراتژی‌ها و عوامل حیاتی موفقیت در پیاده‌سازی ITIL در سازمان‌های آمریکایی و استرالیایی ضمن تعیین عوامل حیاتی موفقیت در پیاده‌سازی این چارچوب بیان داشته است که پیاده‌سازی ITIL، می‌تواند ITSM را دگرگون کرده و به سازمان‌ها سود برساند، که برخی از این منافع عبارتند از: زیرساخت قابل پیش‌بینی‌تر، وضوح نقش‌ها و مسئولیت‌ها، کاهش وقفه در سیستم و خدمت بهبود هماهنگی میان تیم‌های کاری، خدمات بی‌نقص و مستقیم، فرایندهای ثابت و مستندشده ITSM در سازمان، ثبت مدام وقایع، بهبود سودآوری و بهره‌وری، کاهش هزینه‌ها و بهبود رضایت مشتری. حاجی‌زاده و خیّامی (۲۰۱۷) در پژوهش روش استقرار کتابخانه زیرساخت فناوری اطلاعات (ITIL) در دانشگاه‌های ایران ضمن مطالعه عوامل تسهیل‌کننده، موانع و چالش‌ها، روشی برای اجرای فرآیندهای ITIL پیشنهاد و بر اساس ITIL v.3 فرآیندهای میز خدمات، مدیریت حادثه، مدیریت مشکلات و مدیریت تغییر را بیان کردند که مدیران می‌توانند با استفاده از این چارچوب بهترین روش را برای تغییرات داخلی و مدیریت یا تمرکز نیازهای مشتریان و کارمندان اعمال کنند.

چارچوب نظری تحقیق

شکل (۱) مدل مفهومی پژوهش را نشان می‌دهد. متغیرهای مستقل در این پژوهش، سیستم مدیریت امنیت اطلاعات (ISMS) دارای ۹ بُعد و کتابخانه زیرساخت فناوری اطلاعات (ITIL) دارای ۵ بُعد می‌باشد و متغیرهای وابسته، ارتقاء سیستم‌های اطلاعاتی و تداوم خدمات فناوری اطلاعات می‌باشد که با توجه به بررسی استانداردهای موجود و پژوهش‌های پیشین مانند لاودن (۲۰۱۰)، اُبراین (۲۰۰۶)، سازمان استاندارد بین‌المللی(۲۰۱۳)، کنترل‌های امنیتی سیستم‌های اطلاعاتی و سازمان‌ها[1] (۲۰۱۳)، استانداردهای امنیتی[2] (۲۰۰۲)، روش‌های ایده‌آل مدیریت[3] (۲۰۱۱)، مجموعه راهنمای امنیت فضای تولید و تبادل اطلاعات در دستگاه‌های اجرایی (۲۰۱۵) و سند افتا شاخص‌های مهم در پیاده‌سازی سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات استخراج گردید تا با بررسی سازمان‌ها و مطابقت با این شاخص‌ها، بتوان عوامل و شاخص‌های مؤثر در ارتقاء سیستم‌های اطلاعاتی و خدمات فناوری اطلاعات را

1-Security and Privacy Controls for Federal Information Systems and Organizations
2-BS7799-2. (2002). ISMS-Specification with guidance for use.
3-Best Management Practice

استخراج و بیان نمود.



شکل ۱: مدل پژوهش (محققان)

سؤالات پژوهش

سؤال اصلی تحقیق:

آیا پیاده‌سازی سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات باعث ارتقاء سیستم‌های اطلاعاتی و تداوم خدمات فناوری اطلاعات می‌شود؟

سؤالات فرعی تحقیق:

- میزان تاثیر و وابستگی هر کدام از متغیرها در سیستم مدیریت امنیت و کتابخانه زیر ساخت فناوری اطلاعات بر هر بخش از متغیرهای ارتقا سیستم-های اطلاعاتی به منظور تداوم خدمات فناوری اطلات به چه میزان می‌باشد؟
- شاخص‌ها و معیارهای مؤثر پیاده‌سازی سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات جهت ارتقاء سیستم‌های اطلاعاتی و خدمات فناوری اطلاعات کدامند؟

روش تحقیق

- **روش پژوهش:** پژوهش پیش رو ازنظر ماهیت از نوع پژوهش‌های توصیفی و بـه لحـاظ روش، کمّی و ازنظر هدف کاربردی به شمار می‌رود.
- **ابزارگردآوری داده‌ها:** جمع‌آوری داده با استفاده از پرسشنامه و نوع مقیاس اندازه‌گیری طیف لیکرت می‌باشد. برای گردآوری اطلاعات در زمینهٔ مبانی نظری و ادبیات پژوهش، از منـابع کتابخانـه‌ای، مقالات، منابع الکترونیکی، استانداردها و مجله‌های معتبر استفاده شده‌است.
- **جامعه آماری، حجم نمونه و روش نمونه‌گیری:** جامعه آماری این تحقیق شامل:
  - مدیران و کارشناسان حوزه امنیت اطلاعات و خدمات فناوری اطلاعات سازمان‌های دولتی و خصوصی که اقدام به پیاده‌سازی سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات در شهر زاهدان و مشهد نموده‌اند که بدین منظور لیست سازمان‌های مذکور از اداره کل ارتباطات و فناوری اطلاعات خراسان رضوی و سیستان و بلوچستان تهیه شد؛
  - مدیران ارشد شرکت‌های ارائه‌دهنده خدمات مدیریتی، فنی، عملیاتی و آموزشی امنیت اطلاعات و مشاوره پیاده‌سازی سیستم مدیریت امنیت اطلاعات و خدمات فناوری اطلاعات که از سوی وزارت ارتباطات و فناوری اطلاعات پروانه فعالیت دریافت نموده‌اند که لیست و مشخصات این شرکت‌ها از سایت رسمی وزارت ارتباطات و فناوری اطلاعات کشور به‌دست‌آمده است؛
  - درنهایت اساتید، خبرگان و محققین با زمینه فعالیت یا پژوهش در حوزه‌ی امنیت اطلاعات و خدمات فناوری اطلاعات است.

با توجه به اینکه افراد درگیر در حوزه مدیریت و نظارت امنیت اطلاعات و خدمات فناوری اطلاعات در سازمان‌های مذکور بین یک تا سه نفر بوده‌اند؛ متوسط تعداد اعضای جامعه آماری با توجه به لیست سازمان‌ها ۱۰۰ نفر درنظرگرفته شد. حداکثر حجم نمونه برای جامعه مورد مطالعه بر اساس جدول مورگان ۸۰ نفر تعیین و نمونه‌گیری به‌صورت تصادفی ساده انجام‌شده است. با توجه به حداکثر حجم نمونه، تعداد ۸۰ پرسشنامه به‌صورت مراجعه حضوری (تعدادی از پرسشنامه‌ها پس از چاپ به‌صورت حضوری توزیع گردید) و همچنین با بهره‌گیری از ویژگی‌های گوگل درایو[1] پرسشنامه به‌صورت الکترونیکی طراحی و از طریق

1-Google Drive

ایمیل برای پاسخ‌دهندگان ارسال شد که از این تعداد ۷۸ پرسشنامه برگشت داده شد و مورد تحلیل و ارزیابی قرار گرفت.

- **فنون تجزیه و تحلیل اطلاعات:** متغیرهای پژوهش، تعداد شاخص‌ها، ضریب آلفای کرونباخ و پایایی ترکیبی برای هر متغیر در جدول (۱) آمده است. همان‌طور که مشاهده می‌گردد، ضریب آلفای کرونباخ تمامی متغیرها از حداقل مقدار ۰/۶۵ بیشتر است(*Lee& Kim, 1999*).

جدول ۱: ضریب آلفای کرونباخ و پایایی ترکیبی متغیرهای پژوهش

متغیرهای پژوهش	ISMS	*ITIL*	ارتقاء سیستم‌های اطلاعاتی	تداوم خدمات IT
تعداد شاخص‌ها	۱۸	۱۳	۹	۷
آلفای کرونباخ	۰/۸۶۹	۰/۸۱۵	۰/۸۰۸	۰/۷۴۹
پایایی ترکیبی	۰/۸۹۰	۰/۸۵۲	۰/۸۵۴	۰/۸۲۳

بررسی روایی مدل (همگرا)

برای بررسی روایی سازه (همگرا) از تحلیل عاملی تأییدی استفاده شد. در انجام تحلیل عاملی، ابتدا باید از این مسئله اطمینان حاصل کرد که آیا می‌توان داده‌های موجود را برای تحلیل مورد استفاده قرارداد؟ بدین منظور از شاخص KMO و آزمون بارتلت استفاده شده‌است. همچنین برای بررسی روایی‌همگرا در مدل حداقل مربعات جزئی توسط معیار میانگین واریانس استخراج‌شده[1] مورد تحلیل قرار گرفت. همان‌طور که در جدول (۲) ملاحظه می‌شود تمامی مقادیر میانگین واریانس استخراج‌شده از ۰/۵ بیشتر هستند و بنابراین مدل اندازه‌گیری از روایی همگرای مناسب برخوردار است.

جدول ۲: نتایج شاخص KMO، آزمون کرویت بارتلت و میانگین واریانس استخراج‌شده

متغیرها	شاخص KMO	معناداری آزمون بارتلت	میانگین واریانس استخراج‌شده (AVE)
ISMS	۰.۷۳۳	۰.۰۰۰	۰/۶۱۶
ITIL	۰.۷۳۸	۰.۰۰۰	۰/۶۱۱
ارتقاء سیستم‌های اطلاعاتی	۰.۷۹۷	۰.۰۰۰	۰/۵۹۶
تداوم خدمات IT	۰.۷۴۵	۰.۰۰۰	۰/۶۰۴

1-Average variance Extracted (AVE)

بعد از مناسب تشخیص دادن مقدار شاخص KMO و معنادار شدن آزمون بارتلت، به منظور بررسی روایی همگرا باید مقدارهای بارعاملی استخراج‌شده بالای ۰/۳و مقدار معنادار بودن رابطه (t-value) در سطح اطمینان ۹۹ درصد بیشتر از ۲/۳۷ باشند درصورتی‌که مقدار بارعاملی برای شاخصی کمتر از ۰/۳ یا مقدار معنادار بودن رابطه کمتر از ۲/۳۷ باشد، باید شاخص مورد نظر از تجزیه و تحلیل کنار گذاشته شود *(Wixom&Watson, 2001)*.

جدول ۳: بررسی روایی همگرا مدل (سازه)

متغیر		شاخص	بارعاملی	(t-value)
سیستم مدیریت امنیت اطلاعات (ISMS) منبع: (ISO/IEC27001 , 2013), (NIST, 2013), (اداره کل نظام مدیریت امنیت اطلاعات (نما), ۱۳۹۴), (سند افتا, ۱۳۸۶)	Q3	تأیید اهداف و خط‌مشی‌ها تعریف‌شده توسط مدیریت ارشد	۰/۵۶۳	۷/۲۷۵
	Q4	سازگاری استراتژی‌های اتخاذشده با تغییرات محیط عملیاتی و تهدیدات محیطی	۰/۶۶۸	۹/۴۰۶
	Q10	بررسی کلیه حوادث امنیت اطلاعات و دلایل بروز و جلوگیری از تکرار مجدد آن	۰/۵۰۱	۴/۲۵۳
	Q12	واکنش و پاسخ مناسب و یادگیری از حوادث امنیتی به وجود آمده	۰/۶۴۰	۸/۳۳۶
	Q13	تعریف و مشخص کردن اطلاعات هویتی کارکنان برای دسترسی به منابع اطلاعاتی	۰/۶۲۹	۶/۶۱۶
	Q14	بازبینی دوره‌ای و به‌روزرسانی مخزن اطلاعات هویتی برای اطمینان از صحت اطلاعات	۰/۵۴۶	۵/۵۹۰
	Q18	پایش شبکه، تنظیمات روتر، سوئیچ و تست نفوذ در فواصل منظم	۰/۵۵۹	۷/۲۲۸
	Q20	ایجاد و پیاده‌سازی خط‌مشی حفاظت	۰/۶۹۱	۸/۹۶۵
	Q21	وجود سیستم تشخیص نفوذ جهت حفاظت از بدافزارها	۰/۶۵۷	۷/۹۵۷
	Q24	آزمون تشخیص نفوذ جهت شناسایی حملات هکرها و آسیب-پذیری‌ها	۰/۶۲۰	۸/۵۲۳
	Q26	نصب آنتی‌ویروس و فایروال‌ها در شبکه و به‌روزرسانی منظم آن	۰/۵۴۴	۴/۹۲۸
	Q27	شناسایی و ایجاد محوطه‌های امنیتی و لایه‌های امنیتی برای حفاظت از آن‌ها	۰/۵۲۹	۵/۹۱۱
	Q32	آموزش کارکنان در خصوص استانداردها و رویه‌های امنیتی و خدمات IT	۰/۵۶۳	۵/۷۸۱
	Q34	محرمانگی کلمه عبور هنگام انتقال و انتشار اطلاعات توسط کارکنان	۰/۴۱۰	۲/۸۵۱
	Q38	رعایت اصول اولیه پیکربندی، خدمات IT	۰/۴۹۰	۴/۲۴۸
	Q41	انجام فرآیند ممیزی پس از اجرای ISMS در سازمان	۰/۳۷۷	۳/۲۲۲
	Q45	انطباق فعالیت‌های امنیتی سازمان با استاندارد ISO27001	۰/۵۰۰	۴/۸۷۲
	Q47	انطباق تمامی خط‌مشی‌های امنیت اطلاعات باسیاست‌های سازمان	۰/۴۵۰	۳/۲۷۳
کتابخانه زیرساخت فناوری اطلاعات (ITIL) منبع:	Q1	تعریف اهداف و خط‌مشی‌ها برای مدیریت تداوم خدمات	۰/۶۰۹	۸/۹۷۹
	Q2	استراتژی‌های مناسب به‌منظور در دسترس بودن خدمات سازمان	۰/۵۴۸	۵/۸۸۴
	Q5	سنجش و مشخص کردن فرآیندها در سازمان	۰/۴۵۳	۴/۱۲۸
	Q6	بهره‌گیری مدیریت از خط‌مشی‌های به‌روز و تجربیات مستند خدمات IT	۰/۵۸۸	۷/۸۲۳

(BMP, 2011), (ITIL, 2011)	Q7	مشخص کردن دارایی‌ها برای ارزیابی ریسک	۰/۶۱۴	۷/۴۸۳
	Q9	اولویت‌بندی مناسبی از رویدادها ازنظر تأثیر و فوریت‌های آن	۰/۵۵۶	۵/۱۸۳
	Q11	گزارش‌دهی منظم نقاط ضعف و رویدادهای خدمات IT	۰/۵۴۸	۵/۸۸۴
	Q28	اقدامات لازم برای حصول اطمینان از کیفیت خدمات IT	۰/۶۳۴	۹/۴۰۶
	Q33	آگاهی تمامی کارکنان از نقش و وظایف خود در سازمان	۰/۳۸۲	۳/۰۶۷
	Q36	آموزش‌های ارائه‌شده به کارکنان در فواصل منظم	۰/۵۶۹	۵/۳۷۹
	Q42	ممیزی‌هایی به‌منظور شناسایی نارسایی موجود و بالقوه در سازمان	۰/۵۰۹	۵/۳۳۹
	Q44	تست و پیاده‌سازی تکنیک‌های بازیابی مطابق با ITIL	۰/۵۹۸	۷/۰۰۵
	Q46	فرآیندی مستمر جهت بازسازی فعالیت‌ها به‌منظور تداوم اطلاعاتی خدمات IT	۰/۵۸۸	۷/۸۱۲
ارتقاء سیستم‌های اطلاعاتی منبع: BS & BS 7799) ISO/IEC, (2005, (لاودن, ۲۰۱۰), (أبراین, ۲۰۰۶)	Q15	مشخص کردن نیازمندی‌های دسترسی از راه دور برای سیستم‌های اطلاعاتی	۰/۶۳۷	۶/۹۸۵
	Q16	کنترل الکترونیکی ورود و خروج کاربران به سیستم‌های اطلاعاتی	۰/۵۶۱	۶/۰۰۳
	Q17	مشخص کردن دسترسی با اضافه شدن هر کاربر به سیستم‌های اطلاعاتی	۰/۵۴۶	۴/۳۸۶
	Q19	تهیه و آزمایش نسخه‌های پشتیبان اطلاعات و نرم‌افزارها در فواصل منظم	۰/۷۰۶	۴/۸۴۳
	Q23	پایش منظم شبکه سازمان برای امنیت داده‌های سیستم‌های اطلاعاتی خود	۰/۶۲۰	۷/۴۱۸
	Q25	تفکیک شبکه دسترسی به داده‌های اطلاعاتی برای کاربران سطوح مختلف	۰/۶۲۱	۵/۳۵۴
	Q29	قرار دادن تمامی تجهیزات و سیستم‌های اطلاعاتی در محیطی استاندارد و امن	۰/۶۷۵	۱۰/۶۴۱
	Q30	وجود فرایندی برای امنیت تجهیزات و سیستم‌های اطلاعاتی خارج سازمان	۰/۶۵۰	۶/۸۴۰
	Q39	پیکربندی سیستم‌های اطلاعاتی بر اساس اولویت دارایی‌های اطلاعاتی	۰/۶۳۲	۶/۳۷۷
تداوم خدمات فناوری اطلاعات منبع : (BMP, 2011) (2013 , INSO)	Q8	تهیه طرح مدیریت و مقابله با مخاطرات شناخته‌شده جهت تداوم خدمات IT	۰/۶۴۰	۹/۲۶۷
	Q22	تفکیک شبکه داخلی سازمان(اینترانت) و شبکه اینترنت	۰/۴۹۴	۴/۴۱۶
	Q31	وجود اصول تعیین استاندارد جهت مدیریت سرورهای ارائه‌دهنده خدمات IT	۰/۷۱۰	۱۰/۸۴۳
	Q35	رعایت اصول اولیه پیکربندی، خدمات IT	۰/۷۰۴	۱۰/۰۵۶
	Q37	ممیزی‌هایی به‌منظور شناسایی نارسایی موجود در خدماتIT	۰/۵۹۷	۵/۱۱۱
	Q40	پیاده‌سازی الکترونیکی کلیه خدمات سازمانی	۰/۷۳۹	۹/۱۸۱
	Q43	بررسی و پالایش منظم خدمات جهت حصول اطمینان از کارایی آن‌ها	۰/۵۲۵	۴/۸۱۸

همان‌طور که مشاهده می‌شود تمامی مقدارهای شاخص‌های مربوط به متغیر مکنون، بالاتر از ۰/۳ است. بنابراین می‌توان گفت مدل اندازه‌گیری از پایایی کافی در زمینه شاخص‌های متغیرهای پژوهش برخوردار است و t-value مقدار معنادار بودن رابطه

شاخص‌ها با متغیر مکنون در سطح اطمینان ۹۹ درصد نشان می‌دهد که این مقدار معمولاً به‌عنوان مؤلفه‌های روایی مرتبط با تحلیل عاملی تأییدی معرفی می‌شوند و برای تمامی مقدارهای بیشتر از ۲/۳۷ می‌باشد. بنابراین ابزار پژوهش از روایی مناسب برخوردار است و برای سنجش سیستم مدیریت امنیت اطلاعات، کتابخانه زیرساخت فناوری اطلاعات، ارتقاء سیستم‌های اطلاعاتی و تداوم خدمات فناوری اطلاعات شاخص‌های مناسبی محسوب می‌شوند.

برای آزمون نرمال بودن متغیرها، از آزمون کولموگروف ـ اسمیرنوف که رایج‌ترین استفاده از این آزمون بررسی نرمال بودن توزیع داده‌ها می‌باشد، استفاده شد و نتیجه گرفته‌شد که تمامی متغیرهای تحقیق دارای توزیع نرمال می‌باشند.

یافته‌های پژوهش

به منظور تحلیل داده‌های پژوهش از تحلیل‌های گوناگون استفاده شده‌است. در ابتدا جدول (۴) ماتریس ضرایب همبستگی بین متغیرها را نشان می‌دهد که تمامی این ضرایب در سطح اطمینان ۹۹ درصد معنادار هستند.

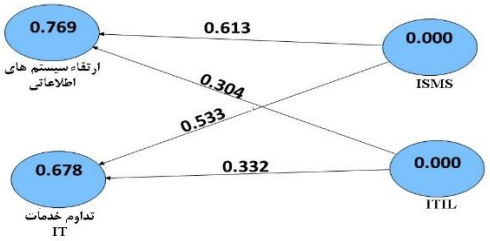
جدول ۴: ماتریس همبستگی بین متغیرهای پژوهش

متغیر	ISMS	تداوم خدماتIT	ITIL	ارتقاء سیستم‌های اطلاعاتی
ISMS	۱/۰۰			
تداوم خدماتIT	۰/۷۹۹	۱/۰۰		
ITIL	۰/۸۰۵	۰/۷۶۰	۱/۰۰	
ارتقاء سیستم‌های اطلاعاتی	۰/۸۵۸	۰/۸۴۳	۰/۷۹۷	۱/۰۰

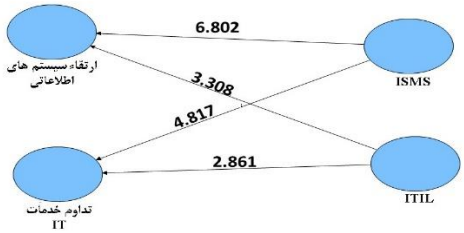
سپس با استفاده از روش حداقل مربعات جزئی (PLS[1]) و آزمون t تک نمونه‌ای، به آزمون پرسش‌های پژوهش پرداخته شده‌است. روش حداقل مربعات جزئی (PLS) یکی از روش‌های آماری چند متغیره محسوب می‌شود *(Fornell& Larcker, 1981)* که ضرایب را به‌گونه‌ای تعیین می‌کند که مدل حاصله، بیشترین قدرت تفسیر و توضیح را دارا باشد؛ *(Liljander, Polsa& Van Riel, 2009)*.

1- Partial Least Squares

بر اساس مقادیر ضریب مسیر بین متغیرهای مکنون (متغیرهای پژوهش) که در شکل (۲) و شکل (۳) مشاهده می‌شود و این مقادیر در جداول (۵) و (۶) نشان داده‌شده است می‌توان گفت:



شکل ۳: مدل پژوهش در حالت تخمین ضرایب مسیر



شکل ۴: مدل پژوهش در حالت معناداری ضرایب (T- VALUE)

جدول ۵: ضرایب مسیر، آماره t و ضریب تعیین (متغیر وابسته: ارتقاء سیستم‌های اطلاعاتی)

متغیر مستقل	ضریب مسیر (β)	آماره t	R^2
ISMS	۰/۶۱۳	۶/۹۷۵	۰/۷۶۸
ITIL	۰/۳۰۴	۳/۴۳۴	

با توجه به ضریب مسیر ۰/۶۱۳ و همچنین آماره t به مقدار ۶/۹۷۵ می‌توان گفت: سیستم مدیریت امنیت اطلاعات (ISMS) در سطح اطمینان ۹۹ درصد در یک سازمان باعث ارتقاء سیستم‌های اطلاعاتی می‌شود.

با توجه به ضریب مسیر ۰/۳۰۴ و همچنین آماره t به مقدار ۳/۴۳۴ می‌توان گفت: کتابخانه زیرساخت فناوری اطلاعات (ITIL) در سطح اطمینان ۹۹ درصد در یک سازمان باعث ارتقاء سیستم‌های اطلاعاتی می‌شود.

مقدار ضریب تعیین چندگانه (R^2) برابر ۰/۷۶۸ شده‌است بر این اساس متغیرهای سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات روی‌هم‌رفته توانسته ۷۶ درصد از متغیر ارتقاء سیستم‌های اطلاعاتی را پیش‌بینی کند. ۲۴ درصد باقیمانده، خطای پیش‌بینی می‌باشد.

جدول ۶: ضرایب مسیر، آماره t و ضریب تعیین (متغیر وابسته: تداوم خدمات فناوری اطلاعات)

متغیر مستقل	ضریب مسیر (β)	آماره t	R^2
ISMS	۰/۵۳۲	۴/۴۷۸	۰/۶۷۶
ITIL	۰/۳۳۱	۲/۶۳۰	

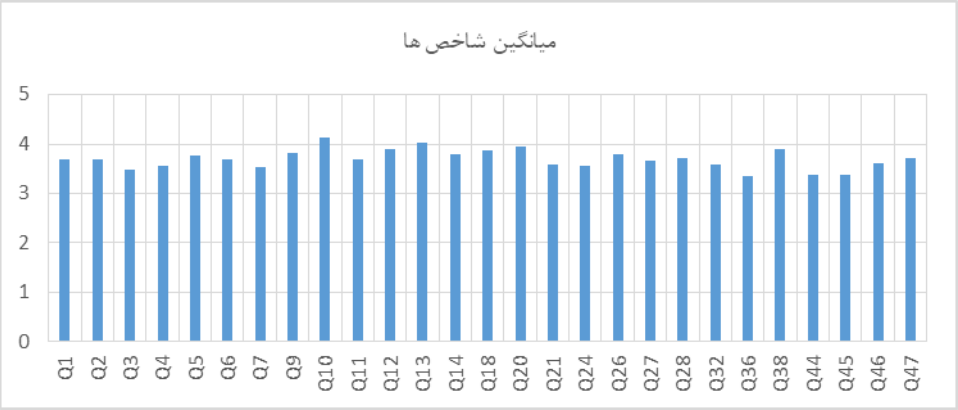
با توجه به ضریب مسیر ۰/۵۳۲ و همچنین آماره t به مقدار ۴/۴۷۸ می‌توان گفت: سیستم مدیریت امنیت اطلاعات در سطح اطمینان ۹۹ درصد در یک سازمان باعث تداوم خدمات فناوری اطلاعات می‌شود.

با توجه به ضریب مسیر ۰/۳۳۱و همچنین آماره t به مقدار ۲/۶۳۰ می‌توان گفت: کتابخانه زیرساخت فناوری اطلاعات در سطح اطمینان ۹۹ درصد در یک سازمان باعث تداوم خدمات فناوری می‌شود.

مقدار ضریب تعیین چندگانه (R^2) برابر ۰/۶۷۶ شده‌است؛ بر این اساس متغیرهای سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات روی‌هم‌رفته توانسته ۶۷ درصد از متغیر تداوم خدمات فناوری اطلاعات را پیش‌بینی کند. ۳۳ درصد باقیمانده، خطای پیش‌بینی می‌باشد.

با توجه به اینکه تمامی متغیرهای پژوهش دارای توزیع نرمال می‌باشند، بنابراین برای آزمون سؤالات فرعی پژوهش از روش‌های پارامتری استفاده شده‌است و چون مقدار میانگین یک جامعه با یک عدد مقایسه می‌شود از آزمون t تک نمونه‌ای استفاده شده‌است. بنابراین با توجه به نتایج آزمون t تک نمونه‌ای که در نمودار (۱) نشان داده‌شده است می‌توان گفت شاخص‌هایی که دارای میانگین بیشتر از ۳ و آماره t بیشتر از ۱/۹۶ و سطح معناداری (Sig) کمتر از ۰/۰۵ باشد. به‌عنوان شاخص‌ها و معیارهای مؤثر در ارتقاء سطح سیستم‌های اطلاعاتی و تداوم خدمات فناوری اطلاعات در سازمان و همچنین به‌عنوان

عوامل کلیدی در اجرا و پیاده‌سازی موفق آن می‌باشند؛ (عنوان شاخص‌های نمودار (۱) در جدول (۳) ذکر شده‌است).



نمودار ۱: میزان اثرگذاری شاخص‌های مؤثر پژوهش

بحث و نتیجه‌گیری

در این بخش خلاصه نتایج و یافته‌های پژوهش جهت پاسخ به سؤالات پژوهش ارائه می‌گردد:

آیا پیاده‌سازی سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات در یک سازمان باعث ارتقاء سیستم‌های اطلاعاتی و تداوم خدمات فناوری اطلاعات می‌شود؟

برای تأیید رابطه میان پیاده‌سازی ISMS و ITIL در ارتقاء سیستم‌های اطلاعاتی و تداوم خدمات فناوری اطلاعات از ضریب همبستگی استفاده‌شده که بر اساس نتایج این فرضیه تأیید گردید همچنین برای بررسی تأثیر پیاده‌سازی ISMS و ITIL در ارتقاء سیستم‌های اطلاعاتی و تداوم خدمات فناوری اطلاعات از روش حداقل مربعات جزئی استفاده گردید که در تمامی موارد فرضیات تأیید شد.

شاخص‌ها و معیارهای مؤثر پیاده‌سازی ISMS و ITIL جهت ارتقاء سیستم‌های اطلاعاتی و خدمات فناوری اطلاعات در سازمان کدامند؟ با توجه به نتایج تحلیل‌ها شاخص‌هایی همچون تعریف اهداف و خطمشی‌ها برای مدیریت تداوم خدمات؛ سنجش و مشخص کردن فرآیندها در سازمان؛ اولویت‌بندی مناسبی از رویدادها ازنظر تأثیر و فوریت‌های آن؛ بررسی کلیه حوادث امنیت اطلاعات و دلایل بروز و جلوگیری از تکرار

مجدد آن؛ واکنش و پاسخ مناسب و یادگیری از حوادث امنیتی به وجود آمده؛ تعریف و مشخص کردن اطلاعات هویتی برای دسترسی کارکنان به منابع اطلاعاتی؛ پایش شبکه، تنظیمات روتر، سوئیچ و تست نفوذ در فواصل منظم؛ تهیه و آزمایش نسخه‌های پشتیبان اطلاعات؛ نصب آنتی‌ویروس و فایروال‌ها در شبکه؛ اقدامات لازم برای حصول اطمینان از ورود افراد مجاز و امنیت دفاتر، اتاق‌ها و امکانات؛ لحاظ قرار دادن موارد امنیتی در طراحی اصول پایه پیکربندی. دارای بیشترین تأثیر بر ارتقاء سیستم‌های اطلاعاتی و تداوم خدمات فناوری اطلاعات در سازمان‌ها می‌باشند و سایر شاخص‌ها نیز دارای تأثیر اما به میزان کمتر از عوامل ذکرشده می‌باشند.

چه راهکارهایی می‌توان برای پیاده‌سازی هرچه بهتر ISMS و ITIL در سازمان ارائه داد؟ با توجه به تحلیل‌های صورت گرفته و بر اساس ابعاد ذکرشده در مدل مفهومی پژوهش راهکارهایی که می‌توان ارائه داد؛ به این شرح می‌باشد: در بُعد ممیزی و بازنگری، که پس از اجرای ISMS و ITIL در سازمان‌ها انجام می‌شود باید انجام منظم فرآیند ممیزی بهبود یابد چراکه به علت هزینه‌بر بودن انجام فرآیند ممیزی، بسیاری از سازمان‌ها پس از اجرای ISMS و ITIL آن را به‌صورت منظم انجام نمی‌دهند. در بُعد مدیریت ریسک و حوادث امنیت اطلاعات، به‌صورت دوره‌ای و مستمر گزارش‌ها و خروجی نرم‌افزارها و سخت‌افزارهای امنیتی سازمان مورد تحلیل و قبل از تبدیل‌شدن به مشکل راهکارهای لازم جهت رفع آن‌ها ارائه گردد. در بُعد امنیت نیروی انسانی (آموزش و آگاهی) آموزش‌های ارائه‌شده به کارکنان باید در فواصل منظم صورت بگیرد و تمامی کارکنان طبق خط‌مشی امنیت اطلاعات عمل کرده و از نقش خود برای دستیابی به تداوم خدمات در سازمان آگاهی یابند. در بُعد طراحی و پیکربندی، هرگونه پیکربندی و اعمال تغییرات سخت‌افزاری و نرم‌افزاری در چارچوب طرحی منظم قرارگرفته و مجوز اعمال تغییرات نیز بایستی از سوی افراد مطلع، متخصص و دارای اختیارات کافی تأیید گردد. در بُعد امنیت نرم‌افزار و شبکه، تشکیل تیمی متخصص در قاب کمیته امنیت جهت پایش شبکه، تفکیک شبکه داخلی (اینترانت) و شبکه اینترنت برای امنیت سیستم‌های اطلاعاتی و خدمات سازمان. در بُعد مدیریت دسترسی، فرآیندی طراحی گردد که بر اساس آن فرد و یا سازمانی که خواهان استفاده از منابع اطلاعاتی سازمان است قبل از هر اقدامی احراز صلاحیت گردد و پس‌ازآن کلیه فعالیت‌ها کنترل گردد؛ پس از پایان استفاده از سرویس‌ها و دارایی اطلاعاتی نیز دسترسی‌های ایجادشده منقضی گردد. در بُعد بهبود مستمر و مدیریت انطباق، میزان انطباق فعالیت‌های

امنیتی سازمان با الزامات قانونی و قراردادی مرتبط با امنیت اطلاعات مانند استاندارد IS027001 و بهره‌گیری از تجربیات موفق فناوری اطلاعات مانند چارچوب ITIL در حوزه سیستم‌های اطلاعاتی و خدمات فناوری اطلاعات بهبود و ارتقاء یابد.

پژوهش حاضر، نتیجه پژوهش‌های قبلی در زمینه سیستم مدیریت امنیت اطلاعات و خدمات فناوری اطلاعات در کشور را مورد تأیید قرار می‌دهد. تاج فر و همکاران در پژوهش خود به این نتیجه رسیدند که ناهمخوانی ساختار سازمانی با نیازهای سیستم مدیریت امنیت اطلاعات، برخوردار نبودن از کمیتهٔ راهبری شایسته و بی‌ثباتی مدیریت ارشد سازمان مهم‌ترین موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات می‌باشد(*Taj Far, Mahmoudi, Soltani,Soltani، 2014*). همچنین مدیری و مسعودی(۲۰۱۱) نشان دادند که خط‌مشی‌های مدیریت امنیت اطلاعات محدوده وسیعی را شامل می‌شوند و اکثر آن‌ها عمومی هستند و تفاوت چندانی بین سازمان‌ها قائل نمی‌شوند لذا داشتن دید جامع به مدیریت امنیت اطلاعات و تصمیم‌گیری درست در مورد آن کمک بسزایی خواهد کرد. در پژوهشی دیگر که توسط محمدی و همکاران(۲۰۱۳) در زمینه شناسایی و دسته‌بندی عوامل حیاتی موفقیت پیاده‌سازی چارچوب کتابخانه زیرساخت فناوری اطلاعات در ایران صورت گرفت نتایج حاصل از تحلیل عاملی اکتشافی مبین آن بود که پنج عامل سازمانی، انسانی، مدیریت پروژه، مدیریتی و فرایندی بر اجرای موفق کتابخانه زیرساخت فناوری اطلاعات تأثیر معنی‌داری دارند. در پژوهش حاضر این نتیجه به دست آمد که پیاده‌سازی سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات بر ارتقاء سیستم‌های اطلاعاتی و خدمات فناوری اطلاعات دارای تأثیر مستقیم و مثبت می‌باشد و همچنین ۱۱ شاخص که در پیاده‌سازی موفق سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات مؤثر هستند، شناسایی و بیان گشت و درنهایت راهکاری‌های در جهت رفع نقایص موجود در پیاده‌سازی سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات برای رسیدن به عملکرد و انسجام بهتر برای ارتقاء سطح سیستم‌های اطلاعاتی و خدمات فناوری اطلاعات ذکر گردید. بنابراین از نتایج این پژوهش می‌توان در جهت پیاده‌سازی هر چه‌بهتر سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات در سازمان‌های دولتی و خصوصی در حوزه خدمات فناوری اطلاعات و سیستم‌های اطلاعاتی استفاده نمود. بی‌شک یافته‌های این پژوهش می‌تواند در سازمان‌های دیگر نیز مورداستفاده و بررسی قرار گیرد.

References

1-Ahmadi, H. (2016). Information Technology Infrastructure Library(ITIL)for Managers, Experts, Professors and Students. Tehran: Sahadanesh publisher. (In Persian)

2- BMP. (2011). Best Management Practice(2011). IT Service Management-ITIL,recieved from:< http://www.best-management-practice.com> [16/03/2017].

3_ BS 7799 & ,BS ISO/IEC, 2. (2005). Information technology-Security techniquesInformation security management systems .

4-Carter-Steel, A. (2009). summary of ITIL aadoption survery responenses thicnical Report. itSMF Australia 2009 Conference.University of Southen Australia.

5-Esteves, R. & Alves, P. (2013). Implementation of an Information Technology Infrastructure Library Process – The Resistance to Change. Procedia Technology (9), pp.505-510.

6-Efta document. (2007). Strategic security document for the information exchange of the country. Ministry of Communications and Information Technology.Iran. (In Persian)

7-Fornell, C., & Larcker, D. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research, 18(1), pp. 39-50.

8-Haji zadeh, A., & khayami, S. (2017). Investigation of the Infrastructure Information Technology Library at(ITIL) Iranian Universities. Third Conference on Computer Science and Information Technology.Tehran. (In Persian)

9-Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K.& Stantchev, V. (2016). ISMS core processes: A study. Procedia Computer Science 100,pp.339-346.

10-Humphreys, E. (2008). Information security Management standards: Compliance, governance risk management. Information security Technical Report, ,13(4),pp.247-255.

11-ISO/IEC 17799 ,BS7799-2.(2002).ISMS-Specification with guidance for use ISO/IEC 17799 Information Technology-Code of practice for information security.

12-ISO/IEC27001. (2013). Information technology — Security techniques —Information security management systems—Requirements. <http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail>[05/02/2017].

13-ITIL.(2011).The ITILToolkit. www.itil.org.uk/kit.html>[25/06/2017].

14-Karimi Balan, Z. (2009). ITIL IT Service Management Information Management Model. Second International Electronic Conference, Tehran Research Institute for Information and Communication Technology (JIT). (In Persian)
15-Kraemer, S. (2006). An adversarial viewpoint of human and organizational factors in computer and information security. A dissertation for the degree of Doctor Philosophy at the university of Wisconsin-Madison.
16-Laudon, K., & Laudon, J. (2010). Management Information Systems. (S. Mostafavi, & S. Hosseini, Trans.) Tehran: Fadak Isatis. (In Persian)
17-Lee, J.& Kim, Y. (1999). Effect of partnership quality on IS outsourcing success: conceptual frameworkand empirical validation. Journal of Management information systems, 15(4), pp. 29-61.
18-Liljander, V., Polsa, P.& Van Riel, A. (2009). Modeling consumer responses to an apparel store band: Store image as a risk reducer. journal of retailing and Consumer Services, 16(4), pp. 281- 290.
19-De Barros, M. D., Alberto Leite Salles, C., Francisco Simões, C., Alexandre da Silva, R. & Gomes Costa., H. (2015). Mapping of the Scientific Production on the ITIL Application. Procedia Computer Science, 55,pp.102-111.
20-Mehrabiyon Mohammadi, M., Shahryari, G. R & Zare Ravasan, A., (2014). Identifying and categorizing critical success factors Implementing the Information Technology Infrastructure Library in Iran. Quarterly Journal of Information Technology Management, 5,pp. 41-71
21-NIST. April 2013 .Security and Privacy Controls for Federal Information Systems and Organizations .53-800.< https://www.nist.gov/ >.[25/02/2017]
22-Norita, A., Noha, T., Faten, Q., & Faten, A. (2013). Technology adoption model and a road map to successful implementation of ITIL. Journal of Enterprise Information Management, 26(5),pp.553-576.
23-obrien, J. (2006). Introduction to Management information Systems. (A. Maniyan, M. Fatahi, & B. Vasegh, Trans.) Tehran: Negah danesh. (In Persian)
24-Office of the Information Security Management System(Nama). (2015). Collection of information security security and data encoding in executive agencies. Tehran: Iran Information Technology Organization. (In Persian)
25-Omidifar, M. (Feb.2015). A Survey and Prioritizing of Information Security Management System Elements in the Telecommunication

Company of Khorasan. The Dissertation of M.Sc. in Information technology management, The University of Sistan & Baluchestan. (In Persian)

26-Sarika, S., Pravin, A., Vijayakumar, A., & Selvamani, K. (2016). Security Issues In Mobile Ad Hoc Networks. Conference Organized by Interscience Institute of Management and Technology(92),pp. 329 – 335.

27-Siyadat, S., & Saghafi, N. (2015). Identify the Challenges of Implementing Information Security Management System (ISMS) in the organization. First International Information Technology Conference.Tehran. (In Persian)

28-Siyadat, S., Salehi pour, S., & Athari fard, A. (2017). The Challenges of Implementing Information Security Management System in the Banking System. Fourth International Conference on Knowledge Based Research in Computer Engineering and Information Technology.Tehran. (In Persian)

29-Steinberg, R. (2014). Operation of ITIL service. (B. Taheri, & F. Narimani, Trans.) Tehran: Tehran University Publisher. (In Persian)

30-Songyang, W., Yong, Z., & Wei, C. (2017). Network security assessment using a semantic reasoning and graph based approach. Computers and Electrical Engineering,000, pp.1–14.

31-Taj Far, A., Mahmoudi, M., Reza Soltani, F., & Reza Soltani, P. (2014). Ranking barriers to implementation of information security management system and exploring readiness of exploration management. Information Technology Management - Faculty of Management, University of Tehran, 4(6), 551-566. (In Persian)

32-Wen,& Wu, S. (2010). Linking Bayesian networks and PLS path modeling for causal analysis. Export Systems with Applications(37), pp.134-139.

33-Whitman, M& Mattord, H .(2011) .Principles of Information Security . Course Technology.

34-Wixom, B.&, Watson, H. (2001). A empirical investigation of the factors affecting data warehousing success. MIS Quarterly, 25(1), pp. 17-41.

35-Yaghoubi, N., shokouhi, J., & Salavati, A. (2015). Management information systems with strategic integration and alignment approach. mashhad: Marandiz Publisher. (In Persian)