نشریه علمی مطالعات مدیریت کسب و کار هوشمند- سال هفتم ـ شماره ۳۰ـ زمستان ۱۳۹۸
صفحات ۵۴- ۳۳

نقش پیاده‌سازی چارچوب‌های مدیریت خدمات و امنیت (ITIL و ISMS) در تداوم خدمات فناوری اطلاعات

سهیلا جعفرنژاد
محمدرضا تقوا

چکیده

محیط رقابتی کسب‌وکار و وابستگی به خدمات، باعث شده است که سازمان‌ها بر پایه میزان توانایی در ارائه مستمر خدمات، مورد ارزیابی قرار گیرند. مدیریت تداوم خدمات فناوری اطلاعات، 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. مدیریت امنیت اطلاعات، با حداقل کردن آسیب‌های کسب‌وکار و کتابخانه زیرساخت خدمات فناوری اطلاعات، ساختاری مناسب برای سازمان‌هایی است که با هدف پشتیبانی از فرایندهای کسب‌وکار، خدمات فناوری اطلاعات را به مشتریانش تحویل می‌دهند. این تحقیق، با هدف شناسایی عوامل تأثیرگذار در تداوم خدمات فناوری اطلاعات انجام شده است. پس از مطالعه ادبیات موضوع، مجموعه سؤالاتی در قالب پرسشنامه و با استفاده از طیف لیکرت پنج بخشی تهیه شد و در اختیار خبرگان قرار گرفت. پس از تأیید سؤالات توسط خبرگان این حوزه، پرسشنامه اصلاح شده برای ۶۰ نفر از کارشناسان سازمان‌ها و شرکت‌های مورد مطالعه ارسال شد. پس از تجزیه‌وتحلیل نتایج، شاخص‌های شناسایی‌شده تائید و فرضیه اصلی تحقیق که تأثیرگذاری پیاده‌سازی کتابخانه زیرساخت خدمات فناوری اطلاعات و سیستم مدیریت امنیت اطلاعات در تداوم خدمات فناوری اطلاعات است تائید شد.

کلید واژگان: چارچوب کتابخانه زیرساخت خدمات فناوری اطلاعات، سیستم مدیریت امنیت اطلاعات، مدیریت تداوم خدمات فناوری اطلاعات.

دانشجوی دکتری، مدیریت فناوری اطلاعات، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی، تهران.(نویسنده مسئول)؛ jafarnezhad.sany@gmail.com

* عضو هیئت‌علمی، گروه مدیریت صنعتی، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی، تهران.

تاریخ دریافت:۱۳۹۷/۰۱/۲۱ تاریخ
پذیرش:۱۳۹۸/۰۷/۲۲

مقدمه

امروزه، فناوری اطلاعات در تمام سازمان‌ها و شرکت‌ها از اهمیت بالایی برخوردار است و نحوه به‌کارگیری و مدیریت آن نیز نیازمند دارا بودن تخصص و دانش است. همچنین، امروزه در سازمان‌ها همه‌چیز به‌عنوان یک خدمت در نظر گرفته می‌شود که می‌تواند در ارتباط مستقیم یا غیرمستقیم با مشتری باشد. به‌کارگیری فناوری اطلاعات نیز، به مدیریت خدمات در جهت کاهش هزینه‌های ارائه‌ی خدمات و بهبود کیفیت خدمات و در نتیجه به موفقیت سازمان در جلب رضایت مشتریان کمک می‌کند. جهت حداکثر کردن تأثیر مثبت مدیریت خدمات، از تجربیات سازمان‌های موفق در این زمینه که به‌صورت استانداردها و چارچوب‌هایی به کار گرفته می‌شوند، استفاده می‌شود. مقبول‌ترین این چارچوب‌ها در میان سازمان‌ها، کتابخانه زیرساخت خدمات فناوری اطلاعات ۱ (ITIL) است. کتابخانه‌ای از وسیع‌ترین مجموعه تجربیات برتر و الگوهای موفق[1] در حوزه مدیریت خدمات فناوری اطلاعات[2] است. این کتابخانه، در حال حاضر به‌عنوان یک چارچوب راهنما برای مدیران فناوری اطلاعات است تا بتوانند زیرساخت‌های فناوری اطلاعات را در سازمان مدیریت و در راستای اهداف، الزامات و نیازمندی‌های کسب‌وکار مطلوب سازی کنند (کتابخانه زیرساخت خدمات فناوری اطلاعات، ۲۰۱۱).

مدیریت امنیت اطلاعات، رویکردی برای پیاده‌سازی و نگهداری امنیت اطلاعات است که توسط سازمان‌ها انتخاب می‌شود. مدیریت امنیت اطلاعات، تضمین تداوم کسب‌وکار و حداقل کردن آسیب‌های کسب‌وکار به‌وسیله جلوگیری از حوادث امنیتی است که دارایی‌های اطلاعاتی سازمان را تهدید می‌کند.

استانداردهایی چون ایزو ۲۷۰۰۱[3] برای امنیت اطلاعات استفاده می‌شود و تنها مسائل فناوری اطلاعات را شامل نمی‌شود. با چنین اهداف گسترده‌ای، بدیهی است که چنین استانداردهایی مطابق با کتابخانه زیرساخت خدمات فناوری اطلاعات نیستند. مدیریت مسئله و

1. Best Practices
2. Information Technology Service Management
3. ISO27001

مدیریت پیکربندی در کتابخانه زیرساخت خدمات فناوری اطلاعات، هیچ معادلی در ایزو ۲۷۰۰۱ ندارد. درحالی‌که مدیریت پیکربندی تأثیر بزرگی در محیط فناوری اطلاعات دارد و باید به شیوه‌ای امن اداره شود. علاوه بر این استانداردهای امنیتی به‌عنوان محافظت از محرمانگی، یکپارچگی و در دسترس بودن شناخته شده‌اند، درحالی‌که در کتابخانه زیرساخت خدمات فناوری اطلاعات، در دسترس بودن در مورد جنبه‌های کیفیتی همچون قابلیت اطمینان، نگهداری، قابلیت سرویس‌دهی و انعطاف‌پذیری است. همچنین، به مسائل مالی در استانداردهای امنیتی رسیدگی نشده است و تنها در مورد مدیریت ریسک است. به‌عنوان‌مثال، اجراکننده‌ها باید جهت کاهش هزینه، ریسک را کاهش دهند. از طرف دیگر، کتابخانه زیرساخت خدمات فناوری اطلاعات، در مورد بودجه و تخصیص هزینه برای هر تحویل خدمات فناوری اطلاعات است (ساهیبودین و همکاران[1]، ۲۰۰۸).

مدیریت تداوم خدمات فناوری اطلاعات[2]، رویکرد اصلی میان سازمان‌هایی است که می‌توانند پاسخگویی به خطرات را انتخاب کنند. مزیت اصلی مدیریت تداوم خدمات فناوری اطلاعات، آن است که سازمان می‌تواند فرایندهای اصلی خود را در سطحی از پیش تعیین‌شده در طول دوره اختلال ادامه دهد. این موضوع، می‌تواند به حفظ شهرت سازمان‌ها کمک کرده و هزینه‌های شکست را کاهش دهد.

در تحقیقات قبلی، چارچوب‌ها به‌تنهایی مورد بحث قرار گرفته و به‌طور مشخص تحقیقی که شاخص‌هایی را جهت تداوم خدمات فناوری اطلاعات در نظر گیرد انجام نشده و میزان تأثیرگذاری این شاخص‌های استخراج‌شده از چارچوب‌ها، بررسی نشده است. در تحقیق حاضر، به بسط و توضیح چارچوب‌های حاضر در این زمینه پرداخته می‌شود و شاخص‌ها و عواملی که بر اساس پیاده‌سازی کتابخانه زیرساخت خدمات فناوری اطلاعات و سیستم مدیریت امنیت اطلاعات[3] در تداوم خدمات فناوری اطلاعات نقش دارند، شناسایی می‌شود.

1. Sahibudin et al.
2. IT Service Continuity Management (ITSCM)
3. Information Security Management System (ISMS)

در ادامه این مقاله، در بخش دوم، مرور کلی در مورد کتابخانه زیرساخت خدمات فناوری اطلاعات، سیستم مدیریت امنیت اطلاعات و مدیریت تداوم کسب‌وکار خدمات فناوری اطلاعات و پژوهش‌های انجام شده در این زمینه پرداخته شده است. در بخش سوم و چهارم، روش تحقیق و نتایج و یافته‌های حاصل از پژوهش ارائه شده و بخش پنجم به نتیجه‌گیری از مطالب عنوان شده و پیشنهادهای آتی پرداخته است.

مبانی نظری و پیشینه تحقیق

تداوم فرایندهای کلیدی سازمان پس از وقوع حادثه، نقش بسیار مهمی در کسب‌وکارهای مختلف ایفا می‌کنند (ربانی و همکاران[1]، ۲۰۱۶). بیشتر مطالعات صورت گرفته، در حوزه تداوم کسب‌وکار است و در بررسی‌های صورت گرفته در مورد پیشینه تحقیق، موارد کمی در زمینه تداوم خدمات فناوری اطلاعات است که به آن‌ها اشاره می‌شود. ترابی و همکاران (۲۰۱۶)، چارچوبی توسعه‌یافته جهت ارزیابی ریسک برای سیستم‌های مدیریت تداوم کسب‌وکار ارائه کردند. مدل پیشنهادی، از مجموعه‌ای از تکنیک‌های تحلیلی برای بهبود و تسهیل مدیریت و ارزیابی ریسک بهره می‌برد. یوسفی و همکاران (۱۳۹۶)، در پژوهشی به بررسی تأثیر پیاده‌سازی کتابخانه زیرساخت خدمات فناوری اطلاعات بر بهبود مدیریت خدمات فناوری اطلاعات در یکی از بانک‌ها پرداخته‌اند. همچنین، ترابی و همکاران (۲۰۱۴)، چارچوبی جدید برای تجزیه‌وتحلیل تأثیر کسب‌وکار بر مدیریت تداوم کسب‌وکار با مطالعه موردی ارائه کردند. مقاله‌ای از کریمی بلان در سال ۱۳۸۸ با عنوان "الگوی نظام مدیریت استمرار خدمات فناوری اطلاعات بر اساس کتابخانه زیرساخت خدمات فناوری اطلاعات" ارائه شده که به موضوع استمرار خدمات فناوری اطلاعات به‌عنوان بخشی از طرح تداوم کسب‌وکار پرداخته است.

مطالعات پیشین، چارچوبی برای مدیریت تداوم کسب‌وکار را شناسایی کرده‌اند و آن را در بستر سیستم‌های اطلاعاتی گسترش داده‌اند (جارولاینن[2]، ۲۰۱۳). مقاله‌ای با عنوان

1. Rabbani et al.
2 Järveläinen

"استانداردهای مدیریت امنیت اطلاعات: پذیرش، نظارت و مدیریت ریسک " نیز که توسط هامفریس[1] در سال ۲۰۰۸ به چاپ رسیده است و در مورد اینکه استانداردهای سیستم مدیریت امنیت اطلاعات چه چیزی برای ارائه و پیشنهاد به سازمان‌ها دارند، اینکه این استانداردها، چه منافعی برای سازمان‌ها به ارمغان می‌آورند و چگونه این استانداردها اهداف امنیتی و اطلاعاتی سازمان را با اهداف استراتژیک سازمان همسو می‌کنند، مطالبی ارائه کرده است. به‌طور خاص، این مقاله 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 این استانداردهای بین‌المللی در حل این مشکلات و تهدیدات، مفید واقع می‌شوند (هومفریز[2]، ۲۰۰۸). تنها یک مطالعه در حوزه تداوم خدمات فناوری اطلاعات وجود دارد که آن هم سیستم پشتیبانی تصمیم‌گیری فازی فوریا را به‌عنوان یک نمونه اولیه برای تسهیل همسویی و تنظیم ترجیحات و توافقات گروه در نظر می‌گیرد (وان دِ والی و روتکفوسکی[3]، ۲۰۰۶).

زدسیدیسین و همکاران[4] (۲۰۰۵) پژوهشی ارائه دادند و مشخص کردند چطور و چرا، شرکت‌ها برنامه‌های تداوم کسب‌وکار را ایجاد می‌کنند تا خطرات و تهدیدهای مرتبط با سازمان را مدیریت نمایند. گیب و بوچانان[5] (۲۰۰۶)، چارچوبی برای طراحی، پیاده‌سازی و نظارت بر برنامه مدیریت تداوم با قالب و زمینه استراتژی اطلاعاتی ارائه کردند.

ون‌سولمز[6] نیز در مقاله‌ای کوتاه با عنوان "حرکت از امنیت اطلاعات به سمت امنیت کسب‌وکار " که در سال ۲۰۰۵ انتشار یافت به این موضوع اشاره کردند که امنیت اطلاعات که مسئول حفاظت از سرمایه‌های اطلاعاتی سازمان در مقابل خطرات کسب‌وکار هست، در حال حاضر قسمتی حیاتی از اداره مناسب یک سازمان[7] است؛ بنابراین، آن‌ها بیان کردند که

1. Humphreys
2. Humphreys
3. Van de Walle & Rutkowski
4. Zsidisin
5. Gibb and Buchanan
6. Von Solms
7. Good corporate governance

بهتر است به این مبحث به‌جای امنیت اطلاعات از دید کلان‌تر، امنیت کسب‌وکار گفته شود (ون سولمز و ون سولمز[1]، ۲۰۰۵).

ابزارها و چارچوب‌های مهم پیاده‌سازی حاکمیت فناوری اطلاعات

حاکمیت فناوری اطلاعات، بر اجرایی کردن و تبدیل فناوری اطلاعات در مواجهه با نیازهای فعلی و آتی کسب‌وکار تمرکز دارد (سیریسومبونساک و همکاران[2]، ۲۰۱۸). چارچوب‌های متعددی برای راهبری و مدیریت خدمات فناوری اطلاعات در صنایع ارتباطات و فناوری اطلاعات، توسعه یافته‌اند. استانداردها و چارچوب‌های بهترین تجارب، راهنماهایی را برای سازمان‌هایی که به دنبال تعالی عملیاتی[3] در راهبری و مدیریت خدمات فناوری اطلاعات می‌باشند، ارائه می‌دهند تا سازمان‌ها بر اساس نیاز خود، به انتخاب آن‌ها اقدام نمایند (جمشیدی، ۱۳۹۰).

به‌منظور پیاده‌سازی حاکمیت فناوری اطلاعات در سازمان، مکانیسم‌های مختلفی وجود دارد؛ برخی از چارچوب‌ها برای انطباق با قواعد و قوانین و برخی برای مؤثرتر کردن و بازمهندسی رویه‌های عملیاتی توسعه یافته‌اند و برخی دیگر از این چارچوب‌ها نیز ریشه در صنایع تولیدی و مالی دارند.

کتابخانه زیرساخت خدمات فناوری اطلاعات (ITIL)

ITIL، یکی از چارچوب‌های حاکمیت فناوری اطلاعات در سازمان است که از سازمان جهت ارائه خدمات اثربخش پشتیبانی می‌کند (گروالا و همکاران، ۲۰۱۸). کتابخانه‌ای از وسیع‌ترین مجموعه تجربیات برتر و الگوهای موفق[4] در حوزه مدیریت خدمت فناوری اطلاعات است که در حال حاضر به‌عنوان یک چارچوب راهنما برای مدیران فناوری اطلاعات است تا بتوانند زیرساخت‌های فناوری اطلاعات را در سازمان مدیریت و در راستای

1. Von Solms & Von Solms
2. Sirisomboonsuk et al.
3. Operational Excellence
4. Best Practices

اهداف، الزامات و نیازمندی‌های کسب‌وکار مطلوب سازی کنند (کتابخانه زیرساخت خدمات فناوری اطلاعات، ۲۰۱۱).

امروزه، چارچوب ITIL به‌طور وسیعی مورد پذیرش قرار گرفته است تا جایی که به‌عنوان استاندارد مدیریت فناوری اطلاعات پذیرفته شده است. در واقع ITIL، به مدیران این امکان را می‌دهد تا از سطح خدمت ارائه شده در سازمان اطمینان حاصل نموده و بتوانند زیرساخت‌های مورد نیاز را بر طبق یک برنامه از پیش تعیین شده تهیه کنند (کتابخانه زیرساخت خدمات فناوری اطلاعات، ۲۰۱۱).

سیستم مدیریت امنیت اطلاعات[1] (ISMS)

امنیت اطلاعات، دربرگیرنده روش‌ها، اقدامات فنی و مدیریتی برای حفاظت از سرمایه‌های اطلاعاتی در مقابل جمع‌آوری‌های غیرمجاز، آسیب، افشاء، دست‌کاری، تغییر و ازدست‌رفتن و سوءاستفاده است (ایلاف و ایلاف[2]، ۲۰۰۳). مدیریت امنیت اطلاعات، یک رویکرد مدیریت سازمانی جهت جلوگیری از نقض امنیت اطلاعات مخرب فراهم می‌کند و برای تضمین سطح قابل قبولی از محرمانه بودن اطلاعات طراحی شده است (هو و همکاران[3]، ۲۰۱۸). هدف مدیریت امنیت اطلاعات، تضمین تداوم کسب‌وکار، اطمینان مشتری، حفاظت از فرصت‌ها و سرمایه‌گذاری‌های کسب‌وکار به‌وسیله جلوگیری و کمینه کردن اثرات حوادث امنیتی است (ما[4]، ۲۰۰۵).

سیستم مدیریت امنیت اطلاعات، ابزاری است برای شناسایی، مدیریت و به حداقل رساندن احتمال وقوع تهدیداتی که امروزه سازمان‌ها به‌واسطه از دست دادن اطلاعات خود با آن‌ها مواجه می‌باشند (محمدنژاد و صبوحی، ۱۳۹۵).

در حال حاضر، مجموعه‌ای از استانداردهای مدیریتی و فنی امنیت اطلاعات و ارتباطات، ارائه شده‌اند. استاندارد BS7799، اولین استاندارد مدیریت امنیت اطلاعات است. آخرین

1. Information Security Management System
2. Eloff & Eloff
3. Hou et al.
4. Ma

نسخه این استاندارد،(BS7799:2002) در سال ۲۰۰۲ و در دو بخش منتشر شد. استاندارد ISO/IEC17799، نسخه‌ای که بیشتر موردتوجه قرار گرفته، استاندارد BS7799 است که توسط سازمان ISO در سال ۲۰۰۰ انتشار یافت.

هدف این استاندارد، ارائه توصیه‌هایی برای مدیریت امنیت اطلاعات است که مسئول آغاز، پیاده‌سازی و نگهداری امنیت در سازمان خود هستند. این استاندارد شامل یازده بخش اصلی، خط‌مشی امنیت سازمانی، اهداف زیرساخت امنیت، طبقه‌بندی و کنترل دارایی، اهداف امنیتی فیزیکی و محیطی، اهداف مدیریت عملیات و ارتباطات، کنترل دسترسی سیستم، توسعه و نگهداری سیستم، مدیریت حوادث امنیت، برنامه‌ریزی تداوم کسب‌وکار و اهداف مقبولیت است که خود به ۱۳۳ کنترل تقسیم می‌شود (کاراباکاک و سوگوکپینار[1]، ۲۰۰۶).

در سال ۲۰۰۱، بخش دوم استاندارد BS 7799 مورد بازبینی قرار گرفت و در سال ۲۰۰۲، نسخه اصلاح شده آن انتشار یافت و در سال ۲۰۰۵ با پذیرش در سازمان بین‌المللی استانداردسازی (ISO) تحت عنوان ایزو ۲۰۰۵۲۷۰۰۱: انتشار یافت. در حال حاضر، استاندارد بین‌المللی امنیت اطلاعات استانداردهای سری ISO/IEC27000 را می‌توان به‌عنوان معتبرترین استاندارد بین‌المللی امنیت اطلاعات برشمرد.

مدیریت تداوم خدمات فناوری اطلاعات

محیط رقابتی کسب‌وکار و وابستگی شدید به خدمات، باعث شده است که سازمان‌ها بر پایه میزان توانایی در ارائه مستمر و دائمی خدمات، مورد ارزیابی قرار گیرند. مدیریت تداوم خدمات فناوری اطلاعات (ITSCM)[2]، به مدیریت قابلیت‌های سازمان در تداوم ارائه سطحی توافقی و از پیش تعیین شده 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 در برمی‌گیرند. مدیریت تداوم خدمات فناوری اطلاعات، چارچوبی برای توسعه طرح‌های

1. Karabacak & Sogukpinar
2. IT Service Continuity Management (ITSCM)

بازیابی ساختار فناوری اطلاعات در پشتیبانی از طرح‌های مدیریت تداوم کسب‌وکار ارائه می-دهد؛ بنابراین، مدیریت تداوم خدمات فناوری اطلاعات را به‌عنوان بخشی درونی از فرایند مدیریت تداوم کسب‌وکار برای اطمینان از امکان ارائه خدمات فناوری اطلاعات می‌توان قلمداد نمود (کریمی بلان، ۱۳۸۸).

مدیریت تداوم خدمات فناوری اطلاعات، به دنبال پشتیبانی از مدیریت تداوم کسب‌وکار از طریق تأمین زیرساخت‌های مورد نیاز فناوری اطلاعات و خدمات آن است که توانایی بازگرداندن این خدمات را در زمان کوتاهی پس از وقوع حادثه ایجاد می‌کند.

مدیریت تداوم خدمات فناوری اطلاعات، رابطه تنگاتنگی با مدیریت تداوم کسب‌وکار (BCM[1]) دارد. مدیریت تداوم کسب‌وکار توسعه، استقرار و نگهداری خط‌مشی‌ها، چارچوب‌ها و طرح‌هایی است که به یک سازمان در مدیریت اختلالات کسب‌وکار و نیز ایجاد بازگشت‌پذیری یاری می‌رساند(بی سی آی[2]، ۲۰۰۱).

مدیریت تداوم کسب‌وکار، به‌عنوان یک طرح مادر تحلیل و مدیریت مخاطرات را به شکل کلی بر عهده دارد. این طرح، دو هدف عمده را دنبال می‌کند؛ کاهش مخاطرات تا حد قابل‌قبول و تهیه و توسعه طرح‌های احیای[3] فعالیت‌های کسب‌وکار در صورت وقوع حادثه. اما طرح تداوم خدمات فناوری اطلاعات 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. مدیریت تداوم خدمات فناوری اطلاعات، نقش ارزشمندی در پشتیبانی فرایند برنامه‌ریزی تداوم کسب‌وکار فراهم می‌کند. در بسیاری سازمان‌ها، مدیریت تداوم خدمات فناوری اطلاعات به‌منظور بالا بردن آگاهی از تداوم و نیازهای بازیابی استفاده می‌شود و اغلب به توجیه و پیاده‌سازی فرایند برنامه‌ریزی تداوم کسب‌وکار و طرح تداوم کسب‌وکار استفاده می‌شود.

---

[1] Bussiness Continuity Management
2 BCI
[3] Recovery Plan

روش تحقیق

روش تحقیق این مقاله از نظر هدف، کاربردی و از نظر ماهیت و روش، توصیفی- پیمایشی است. در این مقاله، جهت تعیین شاخص‌ها و معیارهای مربوط به تداوم خدمات فناوری اطلاعات شامل اساتید، خبرگان، محققین با زمینه فعالیت یا پژوهش در حوزه امنیت اطلاعات، کارشناسان حوزه ITIL و بخش سامانمند امنیت شرکت‌های مشاوره امنیتی و مدیران امنیت در سازمان‌های شهر تهران می‌باشند. به‌طورکلی، در این پژوهش، پیمایش داده‌ها به روش پرسشنامه انجام شده است، با توجه به دسترسی محدود به کارشناسان و خبرگان حوزه در مرحله اولیه پرسشنامه طراحی شده به ۸ تن از خبرگان ارائه شد و پس از تائید پرسشنامه از سوی خبرگان و متخصصان و بررسی نتایج آن، پرسشنامه در میان ۶۰ نفر که از شرکت‌های خصوصی و سازمان‌های دولتی انتخاب شده بودند، توزیع و به شناسایی عوامل مؤثر در شناسایی عوامل تأثیرگذار بر تداوم خدمات فناوری اطلاعات منتهی شد.

روش یافتن افراد نمونه، به این طریق بوده که با استفاده از لیست شرکت‌های اعلام‌شده در سایت سازمان فناوری اطلاعات که در حوزه مشاوره پیاده‌سازی، ممیزی و آموزش سیستم مدیریت امنیت اطلاعات و ITIL فعال بودند، اساتید دانشگاه و خبرگان شناسایی شدند. برای کسانی که در این زمینه فعال بودند، پرسشنامه فرستاده شد. به‌منظور شناخت بهتر ماهیت جامعه‌ای که در پژوهش مورد مطالعه قرار گرفته است، باید گفت ۶ درصد پاسخ‌دهندگان در دانشگاه، ۴۲ درصد در سازمان دولتی و ۵۲ درصد در سازمان خصوصی فعالیت دارند. از لحاظ سابقه فعالیت در این حوزه، ۶۶ درصد پاسخ‌دهندگان تا ۵ سال، ۲۴ درصد بین ۶ تا ۱۰ سال و ۱۰ درصد نیز بالای ۱۰ سال سابقه دارند. در تحقیق حاضر، نقش پیاده‌سازی ITIL و ISMS در تداوم خدمات فناوری اطلاعات برای اولین بار در سازمان‌ها سنجیده می‌شود و شاخص‌های تأثیرگذار با استفاده از تحلیل عاملی تائید شدند.جهت شناسایی معیارهای مناسب ،ابتدا ادبیات و منابع داخلی و خارجی مورد بررسی قرار گرفت که درمجموع، در این مرحله ۳۳ شاخص شناسایی گردید. پس از تائید شاخص‌ها در مرحله اولیه توسط خبرگان، در مرحله

بعدی تعدادی بیشتری از خبرگان به پرسشنامه پاسخ داده و از نتایج حاصله از آن برای انجام تحلیل‌های بعدی استفاده شد.

برای تائید رابطه میان پیاده‌سازی سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات در تداوم خدمات فناوری اطلاعات از ضریب همبستگی استفاده شد، که این فرضیه تائید شد. نتایج حاصله در جدول مشاهده می‌شود.

جدول ۳: ماتریس همبستگی بین متغیرهای تحقیق

متغیرهای پژوهش	۱	۲	۳
ISMS	۱/۰۰		
ITIL	۰/۷۲۱**	۱/۰۰	
تداوم خدمات فناوری اطلاعات	۰/۷۵۲**	۰/۶۹۸**	۱/۰۰

سطح معنی‌داری ضرایب همبستگی متغیرهای پژوهش $p<0.05$* $p<0.01$**

برای اثبات تأثیر پیاده‌سازی سیستم مدیریت امنیت اطلاعات و کتابخانه زیرساخت فناوری اطلاعات در تداوم خدمات فناوری اطلاعات، از روش حداقل مربعات جزئی استفاده شد که در تمامی موارد فرضیات تائید و مشخص شد که این دو عامل با تداوم خدمات فناوری اطلاعات در ارتباط بوده و پیاده‌سازی آن‌ها علاوه بر مزایای بسیاری که بر سازمان‌ها داشته و به‌تنهایی می‌توانند بر عملکرد و کارایی سازمان‌ها تأثیر بگذارند و می‌توانند بر تداوم خدمات فناوری اطلاعات نیز تأثیر بسزایی داشته باشند. نتایج حاصله در جدول مشاهده می‌شود.

جدول ٤: ضرایب مسیر، آماره‌ی t و ضریب تعیین (متغیر وابسته: تداوم خدمات فناوری اطلاعات)

متغیر مستقل	ضریب مسیر ( )	آماره t	R^2
ITIL	۰/۳۲۵	۳/۱۳۹**	۰/۶۱۷
ISMS	۰/۵۱۸	۵/۱۶۳**	

با توجه به ضریب مسیر ۰/۳۲۵ و همچنین آماره t به مقدار ۳/۱۳۹ می‌توان گفت: ITIL در سطح اطمینان ۹۹ درصد در یک سازمان باعث تداوم خدمات فناوری اطلاعات می‌شود.

با توجه به ضریب مسیر ۰/۵۱۸ و همچنین آماره t به مقدار ۵/۱۶۳ ، می‌توان گفت: ISMS در سطح اطمینان ۹۹ درصد در یک سازمان باعث تداوم خدمات فناوری اطلاعات می‌شود.

مقدار ضریب تعیین چندگانه (R^2) برابر ۰/۶۱۷ شده است. این ضریب توانایی پیش‌بینی متغیر وابسته توسط متغیرهای مستقل را بررسی می‌کند. بر این اساس متغیرهای ITIL ,ISMS روی‌هم‌رفته توانسته ۶۱ درصد از متغیر تداوم خدمات فناوری اطلاعات را پیش‌بینی کند. ۳۹ درصد باقیمانده، خطای پیش‌بینی است.

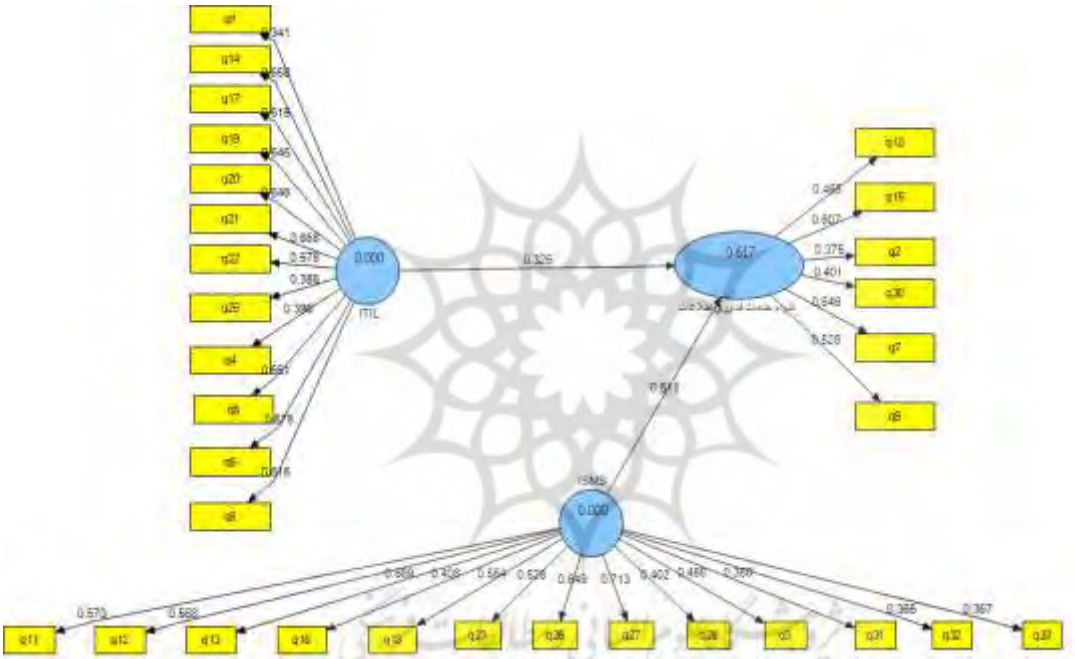
جهت تعیین شاخص‌ها و معیارهای مؤثر در ارتقاء سطح خدمات فناوری اطلاعات، به مقایسه میانگین متغیرهای تحقیق با مقدار حد وسط عدد ۳ پرداخته شد. چون مقدار میانگین یک جامعه با یک عدد مقایسه می‌شود از آزمون تی تک نمونه‌ای[1] استفاده شد و میزان تأثیرگذاری هر شاخص مشخص گردید.

با توجه به نتایج آزمون تی تک نمونه‌ای، می‌توان گفت شاخص‌هایی که دارای میانگین بیشتر از ۳ و آماره تی بیشتر از ۱/۹۶ و سطح معناداری کمتر از ۰/۰۵ باشد به‌عنوان عوامل کلیدی مؤثر در اجرا و پیاده‌سازی موفق سیستم تداوم خدمات فناوری اطلاعات می‌باشند.

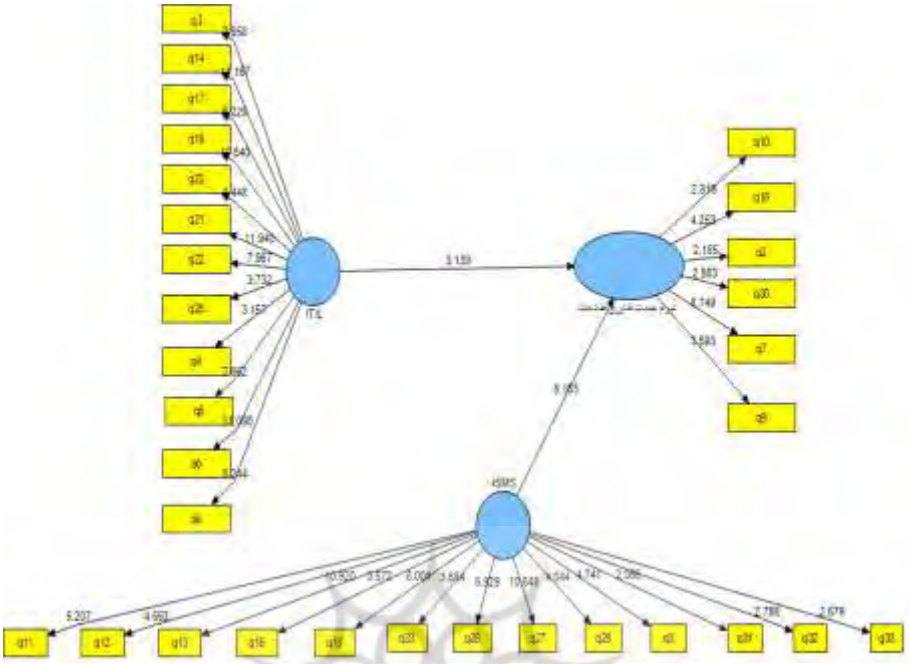
به‌منظور تحلیل ساختار درونی پرسشنامه و کشف عوامل تشکیل‌دهنده هر سازه، از ابزار تحلیل عاملی تأییدی استفاده شد. با استفاده از تحلیل عاملی تأییدی، ۳۳ عامل شناسایی‌شده مورد تحلیل قرار گرفت که از این تعداد ۳۱ عامل دارای بار عاملی مناسب بوده و در مدل باقی ماندند.

1. One- Sample T Test

نتایج تحلیل عاملی در مدل اولیه، نشان دادند که تمامی شاخص‌های مربوط به متغیرهای ISMS و ITIL و تداوم خدمات فناوری اطلاعات به‌جز شاخص‌های Q24, Q29 (شاخص‌های مدیریت میزان در دسترس بودن خدمات سازمان و آگاهی تمامی کارکنان از نقش خود برای دستیابی به تداوم خدمات IT در سازمان) از مقادیر تی (بیشتر از ۱/۹۶) و بار عاملی (بیشتر از۰/۴) مورد قبولی برخوردارند و برای سنجش ISMS و ITIL و تداوم خدمات فناوری اطلاعات شاخص‌های مناسبی محسوب می‌شوند. با حذف شاخص‌های Q24, Q29 مدل اصلاحی به شکل زیر دوباره پردازش شد.



شکل ۳: مدل اصلاحی تحلیل عاملی تائیدی در حالت تخمین ضرایب مسیر



شکل ٤: مدل اصلاحی تحلیل عاملی تائیدی در حالت معناداری ضرایب(t-value)

نتایج تحلیل عاملی مندرج در اشکال (۳و ۴) نشان می‌دهد که تمامی شاخص‌های مربوط به متغیرهای ISMS و ITIL و تداوم خدمات فناوری اطلاعات از مقادیر تی (بیشتر از ۱/۹۶) و بار عاملی (بیشتر از۰/۴) مورد قبولی برخوردارند و برای سنجش ISMS و ITIL و تداوم خدمات فناوری اطلاعات شاخص‌های مناسبی محسوب می‌شوند.

این عوامل در صورت پیاده‌سازی ITIL و ISMS در تداوم خدمات فناوری اطلاعات نقش بسزایی دارند. این ۳۱ عامل نهایی که در قالب ۸ عامل کلی دسته‌بندی شده بودند به شرح زیر در جدول ۶ نشان داده شده است.

جدول ٦: عوامل مؤثر در تداوم خدمات فناوری اطلاعات

اهداف و استراتژی		
Q1	تعریف اهداف برای مدیریت تداوم خدمت IT	ITIL, ؛BMP, 2011 2011
Q2	تعیین استراتژی مناسب به‌منظور تداوم خدمات IT	ITIL, ؛BMP, 2011 2011 BS ISO/IEC 27001:2005 ؛Menken, 2008
Q3	تعریف سیاست‌های امنیتی	BS ISO/IEC 27001:2005 Tipton & Krause, 2008
سازمان و فعالیت‌ها		
Q5	وجود توافقنامه سطح خدمت (SLA) مناسب	ITIL, ؛BMP, 2011 2011
Q6	سنجش و مشخص کردن فرایندها در سازمان	ITIL, ؛BMP, 2011 2011
Q7	مشخص‌سازی فعالیت‌های فرایند جهت تداوم خدمت IT	ITIL, ؛BMP, 2011 2011
Q8	تعیین الزام‌ها و احتیاجاتی که هر فعالیت برای ازسرگیری و استمرار کار خود به آن‌ها نیازمند است	ITIL, ؛BMP, 2011 2011 BS ISO/IEC 27001:2005 ؛Menken, 2008
ممیزی و بازنگری		
Q9	در نظر گرفتن ممیزی‌هایی به‌منظور شناسایی نارسایی‌های موجود و یا بالقوه در سازمان	ITIL, ؛BMP, 2011 2011
Q10	بررسی و پالایش منظم طرح‌های بازیابی برای حصول اطمینان از کارا و مؤثر باقی ماندنشان	ITIL, ؛BMP, 2011 2011 BS ISO/IEC 27001:2005 ؛Menken, 2008
Q11	آزمون و پیاده‌سازی تکنیک‌های بازیابی	

پیکربندی		
Q12	تعیین اجزای پیکربندی (CI) سازمان	BS ISO/IEC 27001:2005 Tipton & Krause, 2008
Q13	جمع‌آوری، ثبت و نگهداری از اطلاعات اجزای پیکربندی	
ریسک		
Q14	مشخص کردن ریسک‌ها	BS ISO/IEC 27001:2005 Tipton & Krause, 2008
Q15	شناسایی دارایی‌ها برای ارزیابی ریسک	ITIL, ؛BMP, 2011 2011
Q16	اولویت‌بندی طرح‌های بازیابی برای مدیریت ریسک	ITIL, ؛BMP, 2011 2011 BS ISO/IEC 27001:2005 ؛Menken, 2008
Q17	تعیین فعالیت‌هایی که از به وقوع پیوستن دوباره حوادث جلوگیری نمایند و مشکل فعلی را نیز حل نمایند	BS ISO/IEC 27001:2005 Tipton & Krause, 2008
حوادث		
Q18	تعیین معیارهای مهم و کلیدی برای مدیریت رویداد	ITIL, ؛BMP, 2011 2011
Q19	اولویت‌بندی مناسبی از رویدادها از نظر تأثیر و فوریت آن‌ها	
Q20	تعریف حوادث	
Q21	تعیین معیارهای مهم و کلیدی برای مدیریت حوادث	
Q22	اولویت‌بندی مناسبی از حوادث از نظر تأثیر و فوریت آن‌ها	
اقدامات اصلاحی و پیشگیرانه و توسعه		
Q23	به‌موقع عمل کردن بخش گزارش دهی فعالیت‌ها	ITIL, ؛BMP, 2011 2011
Q24	حفظ منابع اطلاعاتی،شبکه و برنامه‌های کاربردی از دسترسی غیرمجاز کارکنان	BS ISO/IEC 27001:2005 Tipton & Krause, 2008

Q26	وجود برنامه آموزشی برای افزایش آگاهی کارکنان از تداوم خدمات IT	ITIL, ؛BMP, 2011 2011
Q27	بروز رسانی، ارزیابی و بررسی پایگاه داده سازمان	BS ISO/IEC 27001:2005 Tipton & Krause, 2008
Q28	تهیه نسخه پشتیبان بروز از اطلاعات	
Q29	تهیه برنامه‌هایی جهت جلوگیری از گم‌شدن یا از بین رفتن اطلاعات سازمان	
آموزش و آگاهی		
Q31	تعریف نقش‌ها و مسئولیت افرادی که در هنگام وقوع حادثه یا پس‌ازآن وظیفه‌ای را بر عهده دارند	ITIL, ؛BMP, 2011 2011 BS ISO/IEC 27001:2005 ؛Menken, 2008
Q32	رعایت قوانین و آیین‌نامه‌های سازمان به‌وسیله کارکنان هنگام انتقال و انتشار اطلاعات	BS ISO/IEC 27001:2005 Tipton & Krause, 2008
Q33	آموزش کارکنان سازمان	
Q34	توجه سازمان به رویه‌های کنترل دسترسی مجاز برای کاربران	

بحث و نتیجه‌گیری

جهت تائید نقش پیاده‌سازی سیستم مدیریت امنیت اطلاعات(ISMS) و کتابخانه زیرساخت فناوری اطلاعات (ITIL) در تداوم خدمات فناوری اطلاعات که در واقع سؤال اصلی تحقیق است از آزمون‌های آماری استفاده شد که این فرضیه تائید شد.

در مورد سؤال دوم پژوهش، شاخص‌ها و معیارهای مؤثر در ارتقاء سطح تداوم خدمات فناوری اطلاعات است، به کمک آزمون‌های آماری که در بخش ۳ به آن پرداخته شد، عوامل کلیدی مؤثر در اجرا و پیاده‌سازی موفق سیستم تداوم خدمات فناوری اطلاعات مشخص و میزان تأثیر عوامل مشخص شد.

با توجه به نتایج تحلیل‌ها، عواملی چون تعریف اهداف برای مدیریت تداوم خدمت IT، اولویت‌بندی مناسبی از حوادث از نظر تأثیر و فوریت آن‌ها، آگاهی تمامی کارکنان از نقش خود برای دستیابی به تداوم خدماتIT، مشخص کردن ریسک‌ها، حفظ منابع اطلاعاتی شبکه

و برنامه‌های کاربردی از دسترسی غیرمجاز کارکنان، تهیه نسخه پشتیبان بروز از اطلاعات، آموزش کارکنان سازمان، ، رعایت قوانین و آیین‌نامه‌های سازمان به‌وسیله کارکنان هنگام انتقال و انتشار اطلاعات، بروز رسانی، ارزیابی و بررسی پایگاه داده سازمان دارای بیشترین تأثیر بر تداوم خدمات IT در سازمان‌ها است و سایر عوامل نیز دارای تأثیر اما به میزان کمتر از عوامل ذکرشده می‌باشند.

پیشنهادهایی برای تحقیقات آتی

مدیریت تداوم خدمات فناوری اطلاعات رویکردی اصلی میان سازمان‌هایی است که می‌توانند پاسخگویی به خطرات را انتخاب کنند. مزیت اصلی مدیریت تداوم خدمات فناوری اطلاعات آن است که سازمان می‌تواند فرایندهای اصلی خود را در حداقل سطح کاربردی از پیش تعیین شده در طول دوره اختلال ادامه دهد و این موضوع می‌تواند کمک به حفظ شهرت سازمان‌ها نماید و هزینه‌های شکست را کاهش دهد. این تحقیق ابتدا پیاده‌سازی چارچوب‌های مدیریت خدمات فناوری اطلاعات و مدیریت امنیت را نشان داد که می‌توانند تداوم خدمات فناوری اطلاعات را تضمین کنند و سپس نشان داد که کدام عوامل بیشتر در تداوم خدمات فناوری اطلاعات تأثیرگذار هستند.

با توجه به نتایج تحقیق انجام شده، بهتر است در تدوین برنامه‌ها به عواملی که تأثیرگذاری بیشتری در تداوم خدمات فناوری اطلاعات دارند توجه بیشتری صورت گیرد و همه ابعاد شامل استراتژی و اهداف، فرایندها، کارکنان، وجود توافقنامه سطح خدمات(SLA) و ... را در برگیرد تا نتیجه مطلوب‌تری به همراه داشته باشد. در خود چارچوب ITIL ، تمرکز و تأکید زیادی بر مدیریت چرخه عمر خدمت شده است با توجه به اینکه این حیطه به هزینه و زمان زیادی نیاز دارد و تغییرات زیادی را می‌طلبد، لازم است تا سازمان‌ها سرمایه‌گذاری بیشتری را بر روی این مورد انجام دهند.

در برنامه‌ریزی برای بهبود و تداوم خدمات، ارزیابی وضعیت فعلی سازمان و وضعیت هدف، نقطه‌ی شروع فرآیند برنامه‌ریزی محسوب می‌شود، که در این تحقیق بررسی وضعیت

هدف صورت گرفته است، با توجه به نظر محقق و نظرات خبرگان، وظیفه بعدی، ارزیابی وضعیت فعلی برای سازمان‌ها است تا به کمک ارزیابی وضعیت فعلی و هدف، تدوین برنامه عملیاتی برای بهبود وضعیت صورت گیرد.

منابع

باقراسماعیلی، ه.، (۱۳۸۸). *سنجش همسویی استراتژیک کسب‌وکار و فناوری اطلاعات پس از پیاده‌سازی چارچوب ITIL*. پایان‌نامه کارشناسی ارشد، دانشگاه صنعتی شریف.

بانشی، ز.، و وزیری، ع.، (۱۳۸۸). استاندارد بین‌المللی مدیریت و راهبری سرویس فناوری اطلاعات ISO 20000/ITIL.. *دومین کنفرانس بین‌المللی شهرداری الکترونیکی*.

خالقی، م.،(۱۳۸۳). *راهنمای پیاده‌سازی سیستم مدیریت امنیت اطلاعات*، مرکز تحقیقات مخابرات ایران.

صادقی، ا.، (۱۳۹۰).*تحلیل فاصله وضعیت مدیریت خدمات فناوری اطلاعات در موسسه تحقیقاتی صنعتی مترا، نسبت به نسخه سوم چارچوب ITIL*، پایان‌نامه کارشناسی ارشد، دانشگاه علامه طباطبائی.

فکری ازگمی، ک.، (۱۳۹۰). *تحلیل فاصله مدیریت امنیت موسسه تحقیقاتی صنعتی مترا نسبت به استاندارد سیستم مدیریت امنیت اطلاعات ایزو ۲۷۰۰۱ با استفاده از رویکرد فازی*، پایان‌نامه کارشناسی ارشد، دانشگاه علامه طباطبائی.

کریمی بلان، زهرا، ۱۳۸۸، الگوی نظام مدیریت استمرار خدمات فناوری اطلاعات بر اساس ITIL، *دومین کنفرانس بین‌المللی شهر الکترونیک*، تهران، پژوهشکده فناوری اطلاعات و ارتباطات جهاد دانشگاهی، شهرداری تهران.

محمدنژاد, م و صبوحی ب، ۱۳۹۵، بررسی اهمیت سیستم مدیریت امنیت اطلاعات و استانداردهای آن، *سومین کنفرانس جهانی مدیریت، اقتصاد حسابداری و علوم انسانی در آغاز هزاره سوم*، شیراز، با همکاری مشترک موسسه آموزش عالی علامه خویی دانشگاه زرقان–واحد پژوهش دانش‌پژوهان همایش آفرین.

یداللهی، م.، (۱۳۹۱). *مدلی جهت سنجش میزان آمادگی سازمان برای پیاده‌سازی سیستم مدیریت تداوم کسب‌وکار بر اساس استاندارد جهانی BS 25999*. پایان‌نامه کارشناسی ارشد، دانشگاه علامه طباطبائی.

یوسفی، ع.، (۱۳۹۶). *بررسی تأثیر پیاده‌سازی ITIL بر بهبود مدیریت خدمات فناوری اطلاعات (مطالعه موردی: بانک توسعه تعاون)*. پایان‌نامه کارشناسی ارشد، دانشگاه پیام نور.

BCI. (2010). *The Business Continuity Institute Good Practice Guidelines, a Management Guide to Implementing Global Good Practice in Business Continuity Management*. Business Continuity Institute, London.

Eloff, J.H.P., and Eloff, M.M. (2005). Information Security Architecture. *Computer Fraud & Security*, 11, 10-16.

Gërvalla, M., Preniqi, N., & Kopacek, P. (2018). IT Infrastructure Library (ITIL) framework approach to IT Governance. *IFAC-PapersOnLine*, *51*(30), 181-185.

Hou, Y., Gao, P., & Nicholson, B. (2018). Understanding organisational responses to regulative pressures in information security management: the case of a Chinese hospital. *Technological Forecasting and Social Change*, *126*, 64-75.

ISO 27000 Directory. (2011). An Introduction to ISO 27001, ISO 27002.ISO 27008 Retrieved June 2011 from : http://www.27000.org

ISO/IEC15504. (2011). In Wikipedia, the free encyclopedia. Retrieved June 10, 2011, from: http://en.wikipedia.org/wiki/ISO/IEC_15504.

ISO/IEC20000-1. (2011). *ISO/IEC 20000-1 Information technology - Service management - Part 1: Service management system requirements*, April 2011.

ISO19770. (2011). *ISO19770 Software Asset Management Processes*. Retrieved jun 10, 2011, from: http://www.iso19770.com/.

ITIL Books. (2011). *The ITIL Toolkit*. Retrieved jun 10, 2011 from: http://www.itil.org.uk/kit.htm

ITIL HELP (2005). *What is BS15000?*, Whitepaper, September 2005. Retrieved from: www.bestpracticehelp.com/Whats_BS15000.pdf

ITIL. (2011). *In Wikipedia, the free encyclopedia*. Retrieved June 10, 2011, from: http://en.wikipedia.org/wiki/ITIL

Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, *33*(3), 583-590.

Karabacak, B., and Sogukpinar, I. (2006). A quantitative method for ISO 17799 gap analysis. *Computers & Security*, 25, 413-419.

Ma, Q. (2004). Theoretical and design issues for a computer assisted vocabulary learning program: WUFUN. *Proceedings from CALL 2004 : the Eleventh International Computer-Assisted Language Learning Conference (pp. 241-251)*. Antwerp, Belgium : University of Antwerp. 2-6 sep 2004.

Menken, I.(2008), *IT Service Continuity Management and Disaster Recovery Best Practice Handbook*, Emereo Pty Ltd,.

OGC. (2007). *The official introduction to the ITIL service lifecycle*. London: TSO.

Rabbani, M., Soufi, H. R., & Torabi, S. A. (2016). Developing a two-step fuzzy cost–benefit analysis for strategies to continuity management and disaster recovery. *Safety Science*, *85*, 9-22.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008, May). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In *2008 Second Asia International Conference on Modelling & Simulation (AMS)* (pp. 749-753). IEEE.

Sirisomboonsuk, P., Gu, V. C., Cao, R. Q., & Burns, J. R. (2018). Relationships between project governance and information technology governance and their impact on project performance. *International journal of project management*, *36*(2), 287-300.

Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety science*, *89*, 201-218.

Torabi, S. A., Soufi, H. R., & Sahebjamnia, N. (2014). A new framework for business impact analysis in business continuity management (with a case study). *Safety Science*, *68*, 309-323.

Van de Walle, B., & Rutkowski, A. F. (2006). A fuzzy decision support system for IT service continuity threat assessment. *Decision support systems*, *42*(3), 1931-1943.

Von solms, R., and Von solms, SH. (2006a). Information Sarurity Governance: A model based on the Direct-Control Cycle. *computers & security*, 25, 408-412.

Von solms, R., and Von Solms, SH. (2006b). Information security governance: Due care. *computers & security*, 25, 494-497.

Zsidisin, G.A., Melnyk, S.A., Ragatz, G.L., 2005. An institutional theory perspective of business continuity planning for purchasing and supply management. *Int. J. Prod. Res*. 43 (16), 3401–3420.