مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال پنجم، شماره ۲، تابستان ۱۳۹۳؛ ص ۱۳۱-۱۲۱

مدل تحلیل شکاف سازمان برای پیاده‌سازی الزامات تداوم و مقاوم‌سازی عملیات‌ها مطابق استاندارد BS 25999

محمدرضا تقوا [۱*]، میلاد یداللهی [۲]

۱- استادیار ۲- کارشناس ارشد دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبایی

(دریافت: ۹۲/۱۲/۲۱، پذیرش: ۹۳/۰۴/۰۴)

چکیده

روند بی‌وقفه و فراهم بودن اطلاعات و فرآیندهای کلیدی مرتبط با خدمات زیرساختی فناوری اطلاعات از طریق مقاوم‌سازی سامانه‌ها در مقابل حملات به عنوان یکی از اصول پدافند غیرعامل، همواره یکی از مهم‌ترین دغدغه‌های سازمان‌ها در پدافندهای غیرعامل الکترونیکی و دفاع سایبری بوده که معمولاً از طریق استقرار استانداردهای امنیتی مدیریت می‌شوند. در این پژوهش پس از مطالعه گسترده ادبیات موضوع، مهم‌ترین عوامل حیاتی موفقیت در پیاده‌سازی سامانه مدیریت تداوم کسب و کار استخراج گردید. این عوامل در پرسش‌نامه‌ای برای ۸۳ نفر از خبرگان ارسال شد که پس از جمع‌آوری اطلاعات از ۶۴ خبره، ۳۶ شاخص شناسایی‌شده، با استفاده از تحلیل عاملی اکتشافی و آزمون دوجمله‌ای در ۹ دسته عامل قرار گرفته و تأیید شدند. توسط روش میانگین موزون، وزن هر یک از گویه‌ها و عوامل محاسبه شد و مدل پیشنهادی شامل عوامل مؤثر به همراه میزان اهمیت هر یک در تعیین میزان فاصله برای پیاده‌سازی سامانه مذکور ایجاد گردید. مدل پیشنهادی در دو شرکت ارائه دهنده خدمات فناوری اطلاعات اجرا و آزمایش شد.

کلید واژه‌ها: تداوم عملیات‌ها، تحلیل فاصله، پدافند غیرعامل، امنیت اطلاعات، بازیابی از حادثه، تداوم کسب و کار.

Organizational Gap Analysis Model to Implement the Requirements for Continuity and Hardening of Operations Based on BS 25999

M. R. Taghva[*], M. Yadollahi
Allameh Tabataba'i University
(Received: 12/03/2014; Accepted: 25/06/2014)

Abstract

Availability and continuity of information and key processes that support the core IT services by hardening the computer systems against the attacks as a passive defence principle, has been one of the most important issues facing companies in electronic passive defences and cyber defence that are generally managed by implementing the relevant security standards. In this research, 36 critical success factors for implementing business continuity management were extracted from the comprehensive study of literature. These indicators were sent to 83 experts, among which 64 were collected, analyzed and categorized in 9 factors after exploratory factorial analysis and also they were all approved by binomial test. Harmonic mean was used to calculate the weight of factors and components and finally a model including the effective factors and weight of their importance for organizational gap analysis to implement business continuity management system, was proposed. The proposed model was implemented and tested in two IT service provider companies.

Keywords: Continuous Operations, Gap Analysis, Passive Defence, Information Security, Disaster Recovery, Business Continuity.

[*] *Corresponding Author E-mail: Taghva@gmail.com*

۱. مقدمه

محیط رقابتی تجارت در قرن بیست و یک از یک‌سو و چالش‌ها و تهدیدهای این محیط از سوی دیگر، کسب و کار سازمان‌های امروزی را در معرض مخاطره‌های مختلفی قرار داده است. این مخاطره‌ها در گستره‌های وسیعی اتفاق می‌افتند و از جمله آن‌ها می‌توان به بلایای طبیعی، حمله‌های تروریستی و اشتباه‌های سهوی یا عمدی کارکنان اشاره کرد. همچنین مخاطره می‌تواند در پی تغییرات درونی سازمان، متوجه آن شود. مواردی مانند تغییر راهبردهای سازمان، کوچک‌سازی شرکت، مهندسی مجدد یا برون‌سپاری کردن فرآیندها و خدمات که هرکدام تبعات خاص خود را دارد [۱]. وقوع این رخدادها ممکن است سبب اختلال در عملیات روزانه کسب و کار، ناراضی شدن مشتریان و به خطر افتادن اعتبار سازمان و ایجاد وقفه در جریان درآمدی گردد [۲ و ۳]. کمتر از ۶۰ ثانیه لازم است تا کل اعتبار یک سازمان از بین به رود و کسب و کار آن نابود شود. خرابی سرویس دهنده به مدت یک دقیقه یا حمله هکرها ممکن است تبعاتی برای کسب و کار داشته باشد که جبران آن ماه‌ها و سال‌ها به طول بینجامد و شاید هرگز نتوان آن را جبران نمود [۴] به طوری که آن دسته از حوادث فناوری اطلاعات و سایبری که موجب عدم دسترسی به اطلاعات می‌شوند، ممکن است کسب و کارها را با مشکلاتی از قبیل از دست دادن مشتریان، اعتبار و سهم بازار مواجه سازد [۵].

از اصول پدافند غیرعامل، حفاظت از مراکز حیاتی و مهم و مقاوم‌سازی آن‌ها در برابر حملات احتمالی است و همچنین تأمین امنیت و حصول اطمینان از عدم دسترسی‌های غیرمجاز به اسرار و اطلاعات کشور و ایمن‌سازی و حصول اطمینان از پایداری و خلل‌ناپذیری در فعالیت‌های شبکه‌های الکترونیکی مدیریت و کنترل کشور را می‌توان از اهداف پدافند غیرعامل در حوزه فناوری اطلاعات دانست [۶]. تحقیقات مؤسسه BSI [۷] نشان می‌دهد که ۶۳ درصد از شرکت‌ها در زمینه فناوری اطلاعات کاملاً آسیب‌پذیر هستند. با وجود محیط مخاطره‌ای و همراه با تهدیدهای فناوری اطلاعات، معمولاً مدیران سازمان‌ها به دنبال تضمین تداوم سرویس‌ها و فعالیت‌های سازمانی خود با بهره‌گیری از طرح‌های تداوم کسب و کار و بازیابی از حادثه برای حفظ حالت دفاعی خود می‌باشند. توانایی وفق‌پذیری و پاسخگویی به بحران‌ها و همچنین موقعیت‌ها و فرصت‌ها به منظور حفظ تداوم عملیات‌های کسب و کار با قابلیت اطمینان بالاتر و همچنین ایجاد بستر رشد و توسعه را تداوم کسب و کار گویند [۸].

واژه پدافند غیرعامل، به کلیه تدابیر، عملیات و روش‌های مختلف که موجب جلوگیری و کاهش از خسارات در ابعاد متفاوتی می‌شود، اطلاق می‌گردد که کشورها، دستگاه‌های اجرایی کشور در شرایط بحران ناشی از تهاجم دشمن به این مجموعه اقدامات غیر مسلحانه نیازمند می‌باشند تا منجر به استمرار تولید و تداوم خدمات، کاهش آسیب‌پذیری، پایداری ملی و تسهیل مدیریت بحران برای ادامه حیات حداقلی مردم باشد [۹].

مدیریت تداوم کسب و کار، فرآیندی را در اختیار سازمان قرار می‌دهد که توسط آن بتواند مأموریت‌های اساسی کسب و کاری خویش را در زمان و پس از شناسایی وقایع، همراه با مخاطره انقطاع، ادامه دهد [۱۰].

از سویی، همان‌گونه که متخصصان حوزه تغییر بیان می‌کنند، تحلیل شکاف و آمادگی سازمانی برای تغییر، یک پیش‌نیاز مهم برای پیاده‌سازی و اجرای موفقیت‌آمیز تغییر است [۱۱]. به گفته دیگر، سازمان‌هایی که برای هدایت و ناوبری تغییر، آمادگی بیشتری نشان می‌دهند، دوره گذار را اثربخش‌تر و موفق‌تر پشت سر خواهند گذاشت [۱۲]. با توجه به اهمیت تداوم کسب و کار و همچنین نیاز به یک چارچوب مناسب برای پیاده‌سازی آن در قالب سامانه مدیریت تداوم کسب و کار، برای تضمین تداوم فعالیت‌های کلیدی و محوری سازمان می‌بایست تمامی ابعاد امنیت و تداوم کسب و کار را مورد نظر قرار داد. سازمان‌های مختلف بنا به نیاز و اصول کسب و کار خود، شروع به برنامه‌ریزی جهت مدیریت تداوم کسب و کار و بازیابی حوادث می‌کنند. اما همان‌گونه که گفته شد، جهانی شدن کسب و کارها و شبکه‌های ارتباطی مانند اینترنت و ارتباط کسب و کارهای مختلف با یکدیگر، نیاز به داشتن برنامه‌ای با اصول یکسان و بر پایه استانداردی جهانی و فراگیر که بتواند تمامی انواع کسب و کار را تحت پوشش قرار دهد را بیش از پیش نمایان و گریزناپذیر می‌سازد. در این راستا مؤسسه‌های معتبر بین‌المللی، استانداردهایی را تدوین کرده‌اند تا تمامیت و یکپارچگی این موضوع را پوشش دهند. مهم‌ترین و معتبرترین استاندارد جهانی در این زمینه از ابعاد امنیت داده‌ها و پدافند، استاندارد جهانی BS 25999 می‌باشد که در دو بخش و در سال‌های ۲۰۰۶ و ۲۰۰۷ توسط مؤسسه استاندارد انگلستان و بر پایه استاندارد PAS56 تدوین شده است و به عنوان یک نقطه آغاز قابل اعتماد در این مقوله به کار می‌رود [۱۳]. در سال ۲۰۱۲ نیز استاندارد جهانی مؤسسه استاندارد، ISO 22301 به عنوان نسخه معادل BS 25999-2 انتشار یافت. این استاندارد نیاز سازمان در تدوین، پیاده‌سازی، اجرا، نظارت، بازنگری، نگهداری و بهبود یک سامانه مستند شده مدیریت تداوم کسب و کار را مشخص می‌سازد [۱۴].

باید توجه داشت که مطابق با تعاریف پایه‌ای امنیت اطلاعات و داده‌ها مطابق با الگوهای جهانی نظیر نسخه سال ۲۰۱۳ استاندارد سامانه مدیریت امنیت اطلاعات ISMS[1] که با عنوان ISO 27001 شناخته می‌شود، امنیت اطلاعات گرداگرد ۳ مفهوم دردسترس بودن، صحت و محرمانگی اطلاعات تعریف می‌گردد که تداوم عملیات‌ها و به طور مشخص تداوم کسب و کار، بعد اول آن، یعنی دردسترس بودن و فراهم بودن داده‌ها، اطلاعات و خدمات را پوشش می‌دهد. با توجه به اهمیت این بعد از امنیت اطلاعات، مدیریت تداوم کسب و کار یکی از ۱۴ حوزه کنترل‌های استاندارد ISMS را با ۴ الزام کنترلی به خود اختصاص داده است. همان‌گونه که گفته شد، با توجه به اهمیت این مقوله در فضای مخاطره‌ای امروزی، این حوزه آنقدر گسترش

[1] Information Security Management System

یافت تا استاندارد جدید و مجزایی با عنوان BS 25999 و در ادامه ISO 22301 را به نام خود ثبت کرد. با پیاده‌سازی این استاندارد می‌توان آسیب‌پذیری‌های کلیه دارایی‌های سازمانی نظیر خدمات بنیادین، نیروی انسانی، ساختمان‌ها، تأسیسات، تجهیزات، اسناد و شریان‌ها را در سطح سازمانی و حتی ملی، در مقابل مخاطرات غیر عمدی و یا موارد عمدی نظیر عملیات‌های خصمانه و مخرب مدیریت نمود و آمادگی خود را حفظ کرد. بدین ترتیب با عنایت به مفهوم پدافند غیرعامل، می‌توان این استاندارد را اصلی‌ترین و معتبرترین استاندارد جهانی در حوزه آمادگی برای تداوم عملیات‌ها، مقاومت پایدار و پدافند غیرعامل در نظر گرفت.

با توجه به شروع حرکت بسیاری از سازمان‌ها به سوی پیاده‌سازی سامانه مدیریت تداوم کسب و کار و اهمیت یافتن موضوعاتی همچون پدافند غیرعامل و حفظ و تداوم کسب و کار سازمان‌ها، این پژوهش به دنبال یافتن معیارهایی برای اندازه‌گیری سطح تداوم فعالیت‌های سازمان‌ها جهت پیاده‌سازی سامانه مدیریت تداوم کسب و کار و همچنین تعیین میزان فاصله و بلوغ سازمان‌هایی که قصد پیاده‌سازی این سامانه را بر مبنای استاندارد جهانی BS 25999 و یا استانداردهای معتبر معادل آن نظیر ISO 22301 را دارند، می‌باشد. بنابراین سؤال‌های پژوهش به شرح زیر مطرح شد:

۱.مقیاس و شاخص‌های ارزیابی تحلیل شکاف برای پیاده‌سازی سامانه مدیریت تداوم کسب و کار در سازمان چیست و هر یک به چه میزان تأثیرگذار می‌باشند؟

۲.وضعیت تداوم فعالیت‌ها شرکت‌های ماموت فناوری اطلاعات و توسعه و نوآوری شهر با توجه به شاخص‌های شناسایی شده، چگونه است و آیا آمادگی لازم برای پیاده‌سازی سامانه مدیریت تداوم کسب و کار را دارند؟

در رابطه با تحلیل شکاف و ارزیابی آمادگی سازمان‌ها در زمینه‌های مختلف، مطالعات مختلفی در سطوح متفاوت صورت پذیرفته است. در حقیقت ارزیابی آمادگی کسب و کار، فعالیتی است که در ابتدای پروژه پیاده‌سازی و به عنوان عاملی برای ادامه و یا عدم ادامه فعالیت در نظر گرفته می‌شود [۱۵]. در مجموعه پژوهش‌های انجام شده توسط [۱۶]، دسته‌بندی مناسبی از مدل‌ها و روش‌های معروف در این زمینه مطرح شده است. هرکدام از این مدل‌ها، با توجه به روش مورد استفاده، ابعاد خاصی از سازمان شامل فرآیندها، فناوری، سازمانی و اطلاعاتی را مورد مطالعه خود قرار می‌دهند. از طرفی هر گونه پیاده‌سازی و استقرار سامانه مدیریتی نیز خود، یک تغییر سازمانی محسوب می‌شود که می‌بایست با توجه به ماهیت سامانه مورد نظر، قابلیت سازمان برای پذیرش آن را اندازه‌گیری کرد. در حقیقت آمادگی همواره با خود مفهوم تغییر را به همراه دارد. آمادگی از یک احساس موضوعی و یا یک توانایی قابل قبول نشئت می‌گیرد. بدین ترتیب آمادگی می‌بایست به نحوی مفهوم‌سازی گردد که یک سازمان را به صورت آماده و یا غیر آماده دسته‌بندی نماید [۱۷]. در تحقیق انجام شده توسط [۱۸] دسته‌بندی مناسبی از عوامل مؤثر و نحوه اندازه‌گیری آن‌ها در ارزیابی آمادگی سازمان در برابر تغییرات عنوان شده‌اند که عبارتند از: عوامل انگیزشی برای تغییر، تناسب منابع به‌کار گرفته شده، ویژگی کارکنان و بلوغ و شرایط سازمان.

در حوزه مدیریت تداوم کسب و کار نیز مؤسسه IBM [۱۹ و ۲۰] مطالعاتی گسترده همراه با ارائه فناوری‌های نوین و تجهیزات خاص را انجام داده است که مشهودترین ثمره آن‌ها ارائه چارچوب‌ها و سطح‌بندی‌های تداوم کسب و کار با عنوان ۷ لایه[1] تداوم کسب و کار، به ویژه در حوزه فناوری‌های مربوط به ذخیره‌سازی داده‌ها و چگونگی بازیابی آن‌ها پس از حادثه می‌باشد. هر کدام از این لایه‌ها، دارای مقادیر مختلفی برای مشخصه‌های زمان بازیابی، هزینه و میزان از بین رفتن و یا صدمه دیدن داده‌ها هستند که در بهترین حالت، یعنی سطح هفتم، زمان بازیابی داده‌ها آنی، هزینه حداکثر و میزان صدمه دیدن داده‌ها صفر و یا نزدیک به صفر است [۸]. همچنین مؤسسه استاندارد انگلستان، به عنوان متولی استاندارد این سامانه به همراه انتشارات IT Governance [۲۳-۲۱] روش‌های پیاده‌سازی بهینه را برای درک بهتر مدیریت تداوم کسب و کار و پوشش الزامات استاندارد، در مجموعه کتب خود مورد بررسی قرار می‌دهند. با این وجود با توجه به نوظهور بودن مفاهیم مذکور، تا به حال پژوهشی در رابطه با تحلیل شکاف یا سنجش میزان آمادگی سازمان‌ها برای پیاده‌سازی استانداردهای این حوزه و به طور کلی نگاه سامانه‌ای به این مقوله صورت نپذیرفته است و بیش‌تر مطالعات، جنبه فناوری و تجهیزات را در بر می‌گیرند. بنابراین پژوهش پیش‌رو سعی در بررسی میزان آمادگی سازمان‌ها برای پیاده‌سازی نظام‌مند تداوم کسب و کار را دارد، تا بدین وسیله سازمان‌ها را برای پیاده‌سازی بهینه این سامانه و بیش‌تر کردن شانس موفقیت اجرا، یاری نماید.

در زمینه تحلیل شکاف برای پیاده‌سازی نظام‌های مدیریتی بر اساس استانداردها، سامانه‌های اطلاعاتی، فناوری و به طور کلی آمادگی برای تغییر، پژوهش‌های مختلفی انجام پذیرفته است. در تحقیق انجام شده برای سنجش میزان آمادگی سازمان به منظور پیاده‌سازی سامانه مدیریت امنیت اطلاعات [۲۴]، پس از بررسی مجموعه‌ای از عوامل مؤثر در میزان آمادگی سازمان در پیاده‌سازی ISMS و استفاده از استاندارد ISO/IEC 27001 به عنوان مرجع این سامانه مدیریتی، به ارائه عوامل مؤثر در سنجش میزان آمادگی و بلوغ سازمان جهت پیاده‌سازی ISMS پرداخته شده است. همچنین در پژوهش [۱۴] که با هدف ارزیابی وضعیت مدیریت تداوم کسب و کار در پایانه‌های فروش فروشگاه‌های زنجیره‌ای انجام شده است، به بررسی وضعیت مدیریت تداوم کسب و کار و میزان تطابق آن با استاندارد مرجع این حوزه در ۶ حوزه محدوده و پشتیبانی از سامانه مدیریت، شناسایی کسب و کار، مشخص نمودن راهبرد تداوم کسب و کار، تمرین، بازبینی و نگهداری سامانه، نهادینه‌سازی مدیریت تداوم کسب و کار در فرهنگ سازمانی و گواهینامه تطابق با استاندارد

[1] Tier

پرداخته شده است. اما در یک سطح بالاتر و در حوزه ارزیابی آمادگی فناوری‌های مختلف کـه ارتبـاط تنگـاتنگی بـا اسـتقرار سـامانه‌هـای مدیریتی دارند، تحقیقات صورت گرفته گسترده و متنوع‌تر هستند. با نگاه به سیر تاریخی و جمع‌بندی ارزیـابی آمـادگی در حـوزه فنـاوری مطابق با پژوهش انجام شده توسط منکینـز [۲۵] کـه در آن سـطوح مختلف مرتبط با آمادگی فناوری مورد بررسی قرار مـی‌گیـرد و سـیر تاریخی آن بحث می‌شود، برای آمـادگی حـوزه فنـاوری، ۷ سـطح در نظر گرفته شده است که شامل مواردی چون: اسـتقرار اصـول اولیـه، قاعده‌مند شدن مفاهیم یا کاربرد فنـاوری، انجـام شـدن تحلیـل‌هـا و پژوهش‌ها برای اثبات مفاهیم، تأیید نمونه‌ها در محیط آزمایشـگاهی، تأییـد نمونـه‌هـا در محـیط‌هـای مربوطـه، اثبـات الگـوی سـامانه در محیط‌های مربوطه، اثبات الگوی سامانه در محیط‌هـای برنامـه‌ریـزی شده و عملیاتی، تکمیل شدن سـامانه واقعـی و تأییـد شـدن سـامانه واقعی از طریق انجام موفقیت‌آمیز مأموریت‌ها، می‌شوند. همچنـین بـا بررسی پژوهش انجام شده توسط کواک و لی [۲۶] می‌توان بـه درک خوبی در اصول تئوریک و اثبات عملی در آمادگی برای تغییـر دسـت یافت. در پژوهش انجام شده، آمادگی برای تغییر و همچنین تأثیر آن بر ارزش ایجاد شده از طریق کاربرد سامانه‌هـای ERP بررسـی شـده است. ابتدا مدل پژوهش با اسـتفاده از TAM[1] و TPB[2] ایجـاد شـد و سپس با استفاده از داده‌های گردآوری شـده از یـک سـامانه ERP در کره جنوبی، مورد آزمون قـرار گرفتـه و در نهایـت تحلیـل معـادلات ساختاری با استفاده از ابـزار لیـزرل[3] انجـام شـده اسـت. نتـایج ایـن پژوهش، تأثیر غیر مستقیم آمادگی برای تغییر بر روی رفتار کـاربران برای استفاده از سامانه را نشان می‌دهد و از طرفی تأکید می‌کند کـه آمادگی بـرای تغییـر توسـط دو عامـل تعهـد سـازمانی و شایسـتگی کارکنان افزایش می‌یابد. در زمینه آمادگی فنـاوری، تحقیقـات انجـام شده توسط آهونن [۲۷] و رعنایی و قهرمانی‌فرد [۲۸] نیز در زمینـه موضوعی اینترانت اجتماعی، همسو با استقرار سـامانه‌هـای مـدیریتی می‌باشند. در پژوهش اول، مدل آمـادگی سـازمان بـرای تغییـر وینـر [۱۱] شامل عوامل زمینه‌ای، ارزش‌گذاری تغییر و ارزیـابی اطلاعـاتی مورد استفاده قرار گرفته که پس از تحلیل داده‌ها از طریق رگرسـیون خطی چند متغیره، هیچ‌گونه ارتباط معنی‌داری بین متغیرهای اشـاره شده وجود نداشت، از طرفی در پژوهش دوم، ویژگـی‌هـای سـازمانی مورد نیاز جهت آمادگی برای پیاده‌سازی اینترانت اجتمـاعی، شـامل فرهنگ سازمانی، سیاست‌ها و رویه‌ها، تجربه شخصی، منابع سازمانی، ساختار سازمانی مشخص و ابزاری شامل ۴۸ گویه برای اندازه‌گیـری ویژگی‌های سازمانی طراحی و در نهایت ۴۳ گویـه پایـا و معتبـر بـه دست آمد و این یافته در شرکت برق منطقه‌ای فـارس مـورد آزمـون قرار گرفت.

همان‌طور که پیشینه پژوهش نشان می‌دهـد، پـژوهش‌هـای اول و دوم، اختصاص به دو اسـتاندارد اصـلی و جهـانی امنیـت اطلاعـات و تداوم کسب و کار، یعنی ISO/IEC 27001 و BS 25999 دارند که بـا توجه به جدید بودن دید نظـام‌منـد و اسـتانداردی بـه حـوزه تـداوم عملیات‌ها و سـنجش آن، محـدودیت پـژوهش در ایـن حـوزه بسـیار مشهود است.

۲. روش تحقیق

پژوهش حاضر از منظر هدف، کاربردی است و روش آن نیز توصیفی-پیمایشی به شمار می‌رود. مشخصات دیگر این پژوهش در جدول (۱) آورده شده‌اند.

جدول ۱. خلاصه اطلاعات مربوط به روش پژوهش

روش	فلسفه	نوع مدل	رویکرد	هدف
توصیفی پیمایشی	اثبات گرایی	سنجش انعکاسی	قیاسی تطبیقی	بنیادی کاربردی

جامعه آماری این پژوهش جهت تعیین شاخص‌های مطلوب وزن‌ها مربوط به ابعاد سطح آمادگی برای پیاده‌سازی سامانه مدیریت تـداوم کسـب و کـار شامل اساتید، خبرگان و محققین با زمینه فعالیت یا پژوهش در حوزه امنیت اطلاعات، کارشناسان حوزه تداوم کسـب و کـار و بخـش سـامانه‌ای امنیـت اطلاعات در شرکت‌های مشاور امنیتی و برخی از مدیران امنیت در سازمان‌ها و شرکت‌های بزرگ تهران می‌باشند. برای ۸۳ نفـر از ایـن خبرگـان جهـت استخراج نظر آن‌ها جهت میزان موافقت با اجزای مـدل، پرسـش‌نامـه‌ای بـا بهره‌گیری از طیف لیکرت ارسال شد که ۶۴ پرسش‌نامه برگشت داده شده، به عنوان نمونه آماری به صورت تصادفی مورد پیمایش قرار گرفتند. پرسش‌نامه مـذکور از دو قسـمت اصـلی شـامل مشخصـات فـردی پاسـخ‌دهنـده و شاخص‌های مرتبط با تداوم کسب و کار تشکیل شده است. در قسـمت اول پرسش‌نامه، اطلاعاتی همچون نوع سازمان محل خـدمت (شـامل دانشـگاه، مرکز تحقیقاتی، سازمان دولتی یا خصوصی)، جایگاه سازمانی (شـامل مـدیر ارشد، مدیر میانی و کارشناس اجرایی)، میزان تحصـیلات (شـامل دکتـری، کارشناسی ارشد، کارشناسی و سایر موارد)، میزان آشنایی با مفاهیم و الزامات استاندارد هدف (شامل آشنایی خیلی کم، کم، متوسط، زیاد و خیلی زیـاد) و همچنین مدت زمان فعالیت در حوزه امنیت اطلاعات و یا تداوم کسب و کار و پدافند غیرعامل، دریافت گردید. در قسمت دوم پرسش‌نامـه، ۳۶ شـاخص نهایی برای ارزیابی که از ادبیات موضوع و اسـتاندارد هـدف مسـتخرج شـده بودند، مورد سوال قرار گرفتند.

تحلیل جمعیت شناختی نمونه از منظر میزان تحصیلات، نوع سازمان محل خدمت، جایگاه سازمانی و سابقه فعالیت در حوزه امنیت اطلاعات یـا تـداوم کسب و کار، در جدول‌های (۵-۲) نشان داده شده است. همان‌طـور کـه در جداول مرتبط با تحلیل جمعیت شناختی نمونه دیده می‌شود، پاسخ‌دهندگان از سطح تجربه قابل توجهی در حوزه امنیت اطلاعات و تـداوم کسـب و کـار برخوردار هستند (حدود ۷۲ درصد آن‌ها دارای سابقه بیش از ۳ سال در این حوزه هستند) و از طرفی میزان تحصیلات و جایگاه سـازمانی ایـن افـراد در سطح مناسبی برای پاسخگویی به سؤالات پرسش‌نامه قرار می‌گیرد.

[1] Technology Acceptance Model
[2] Theory of Planned Behavior
[3] Lisrel

از طرفی باید توجه داشت که تعداد ۶۴ نفر، حجم مطلوبی برای تحلیل عاملی به نظر نمی‌رسد و با توجه به تعداد عامل‌ها، این تعداد می‌بایست حداقل ۱۰۸ باشد. ولی با توجه به عدم دسترسی به افراد خبره این حوزه و نوظهور بودن موضوع، محقق به این ضعف در اندازه نمونه اشعار می‌دارد. در این پژوهش برای تجزیه تحلیل داده‌ها از نرم‌افزار SPSS استفاده شده است.

جدول ۲. ویژگی‌های جمعیت شناختی نمونه - میزان تحصیلات

میزان تحصیلات	درصد فراوانی	فراوانی (n=۶۴)
دیپلم	۳	۲
فوق دیپلم	۱۱	۷
کارشناسی	۴۴	۲۸
کارشناسی ارشد	۳۴	۲۲
دکتری	۸	۵

جدول ۳: ویژگی‌های جمعیت شناختی نمونه - نوع سازمان محل خدمت

نوع سازمان محل خدمت	درصد فراوانی	فراوانی (n=۶۴)
دانشگاه	۱۱	۷
مرکز تحقیقاتی	۶	۴
سازمان دولتی	۳۳	۲۱
شرکت خصوصی	۵۰	۳۲

جدول ۴: ویژگی‌های جمعیت شناختی نمونه - جایگاه سازمانی

جایگاه سازمانی	درصد فراوانی	فراوانی (n=۶۴)
کارشناس اجرایی	۵۵	۳۵
مدیر میانی	۳۳	۲۱
مدیر ارشد	۱۲	۸

جدول ۵: ویژگی‌های جمعیت شناختی نمونه – سابقه در حوزه امنیت

سابقه و تجربه در حوزه امنیت اطلاعات	درصد فراوانی	فراوانی (n=۶۴)
کمتر از ۳ سال	۲۸	۱۸
بین ۳ و ۶ سال	۵۰	۳۲
بزرگ‌تر مساوی ۶ سال	۲۲	۱۴

تعیین پایایی پرسش‌نامه با استفاده از آلفای کرونباخ انجام شد و برای اندازه‌گیری روایی ظاهری و محتوایی پرسش‌نامه، از نظر خبرگان و اساتید مربوطه استفاده شد و اشکالات ساختاری آن شناسایی و اصلاحات لازم جهت برآورده ساختن روایی محتوا انجام شد. برای اندازه‌گیری روایی سازه از تحلیل عاملی اکتشافی و تأییدی استفاده شده است. پس از آن برای آزمون فرضیه‌ها از آزمون دوجمله‌ای استفاده می‌شود و جهت تعیین وزن و اهمیت هر شاخص و همچنین وزن عوامل نهایی نیز از روش میانگین موزون استفاده شده است. در پایان، دو شرکت ماموت فناوری اطلاعات و توسعه و نوآوری شهر که قصد پیاده‌سازی سامانه مدیریت تداوم کسب و کار را دارند، به عنوان نمونه انتخاب شدند. وضعیت موجود این شرکت‌ها به منظور مقداردهی شاخص‌های به دست آمده با به‌کارگیری مدل ۵ سطحی مهندسی امنیتی بلوغ قابلیت‌های امنیتی (SSE-CMM[1]) [۲۹] و استفاده از مصاحبه ساخت‌یافته با مدیران این مجموعه‌ها، استخراج شده و میزان فاصله برای پیاده‌سازی این سامانه در آن شرکت‌ها تعیین گردید.

۳. نتایج و بحث

با توجه به دریافت ۶۴ پرسش‌نامه از پاسخ‌دهندگان، پایایی پرسش‌نامه با استفاده از ضریب آلفای کرونباخ، ۰/۹۵۰ به دست آمد که با توجه به بیشتر بودن از ۰/۷ و اختلاف زیاد آن، رقمی بسیار قابل قبول است. بر روی داده‌های جمع‌آوری شده با استفاده از روش مؤلفه‌های اصلی تحلیل عاملی صورت گرفت و نتیجه آزمون KMO، ۰/۷۸۶ محاسبه شد که با توجه به اینکه بیشتر از ۰/۵ است، نمایانگر کفایت نمونه‌گیری و درجه تناسب داده‌ها برای اجرای تحلیل عاملی می‌باشد. همچنین آزمون کرویت بارتلت که نشان دهنده همبستگی داده‌های ماتریس می‌باشد نیز با ضریب اهمیت ۰/۰۰۰۱ مورد تأیید قرار گرفت. به علاوه، مقدار آزمون بارتلت برابر با ۱۴۶۲ است و معنی‌داری آن در سطح ۹۹ درصد، نشان می‌دهد از یک سو بین گویه‌های داخل هر عامل همبستگی بالایی وجود دارد و از سوی دیگر، بین گویه‌های یک عامل با گویه‌های عامل دیگر، هیچ‌گونه همبستگی مشاهده نمی‌شود.

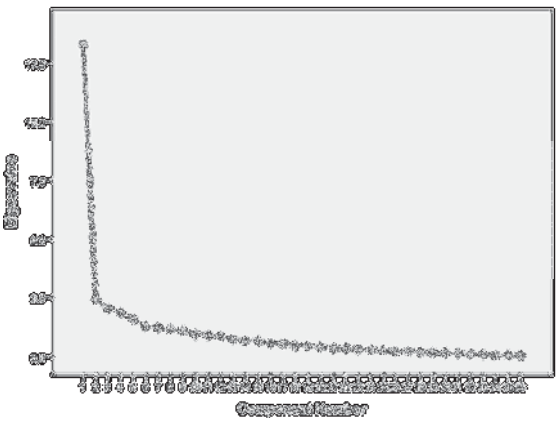
با توجه به جدول (۶)، ماتریس همبستگی داده‌ها که با روش مؤلفه‌های اصلی به دست آمده است، نشان می‌دهد که از مجموع ۳۶ گویه پرسش‌نامه، ۹ گویه دارای مقدار ویژه بالاتر از ۱ می‌باشند و این ۹ عامل می‌توانند حدود ۷۱ درصد از واریانس متغیر کمی را تبیین کنند و در واقع نشان‌دهنده روایی سؤالات می‌باشد.

تحلیل سنگریزه که در شکل (۱) نشان داده شده است، نشان دهنده مقدار ویژه عوامل شناسایی‌شده می‌باشد. این نمودار نشان می‌دهد که ۹ عامل از گویه‌ها استخراج شده است. در نهایت برای دسته‌بندی عوامل از چرخش پروماکس استفاده شد که در ماتریس چرخش‌یافته برای متغیرهای سامانه مدیریت تداوم کسب و کار (BCMS[2])، در مجموع ۹ عامل کلی شناسایی و با توجه به ادبیات پژوهش نام‌گذاری شد. این عوامل عبارتند از: ۱. شناخت سازمان، ۲. بهبود مستمر، ۳. ایجاد و مدیریت سامانه، ۴. ایجاد واکنش و طرح تداوم، ۵. بازبینی و کنترل سامانه، ۶. تعبیه سامانه در فرهنگ سازمانی، ۷. مستندسازی سامانه، ۸. تعیین راهبردهای تداوم و ۹. تمرین، نگهداشت و بازنگری سامانه.

[1] Systems Security Engineering Capability Maturity Model (SSE-CMM)
[2] Business Continuty Management System

جدول ۶. ماتریس همبستگی داده‌ها و اطلاعات توصیفی

عامل	مقادیر اولیه			مجموع مربعات چرخش یافته
	مجموع	واریانس (٪)	تجمعی (٪)	
۱	۳۹/۲۹۶	۳۶/۹۳۴	۳۶/۹۳۴	۹/۹۸۷
۲	۲/۴۰۸	۶/۶۸۹	۴۳/۶۲۳	۰/۱۰۹
۳	۲/۰۴۵	۵/۶۸۲	۴۹/۳۰۵	۷/۷۰۶
۴	۱/۸۴۰	۵/۱۱۰	۵۴/۴۱۵	۶/۵۵۴
۵	۱/۵۷۴	۴/۳۷۲	۵۸/۷۸۷	۳/۴۸۴
۶	۱/۲۷۱	۳/۵۳۰	۶۲/۳۱۷	۵/۳۷۳
۷	۱/۲۲۰	۳/۳۸۹	۶۵/۷۰۷	۴/۴۴۷
۸	۱/۱۴۵	۳/۱۸۱	۶۸/۸۸۸	۱/۷۲۸
۹	۱/۰۹۰	۳/۰۲۹	۷۱/۹۱۶	۲/۰۱۰



شکل ۱. تحلیل سنگریزه

پس از تحلیل عاملی بر روی متغیرها و تعیین متغیرهای نهایی و عامل‌های شناسایی‌شده، فرضیه‌های پژوهش که نظر موافق پاسخ دهندگان در مورد تأثیر عوامل کشف شده بر روی آمادگی سازمان برای پیاده‌سازی سامانه مدیریت تداوم کسب و کار را مورد آزمون قرار می‌دهد، با استفاده از توزیع دوجمله‌ای مورد بررسی قرار گرفتند. همان‌طور که در جدول (۷) نشان داده شده است، کلیه عوامل اصلی و همچنین کلیه گویه‌ها، با نسبت بالاتر از ۰/۶ درصد و سطح معناداری ۰/۰۰۰ مورد تأیید قرار گرفتند. در این آزمون، میزان خطا ۰/۰۵و تعداد نمونه ۶۴ در نظر گرفته شد که افراد در آن به ۳ گروه موافق (منتخبین گزینه ۴ و ۵ طیف لیکرت)، مخالف (منتخبین گزینه ۱ و ۲ طیف لیکرت) و حذف شده (منتخبین گزینه ۳ طیف لیکرت) تقسیم شدند.

برای محاسبه وزن هر یک از شاخص‌ها از روش میانگین موزون استفاده می‌شود. بدین منظور، ارزش هر گویه که بر اساس طیف لیکرت، عددی بین ۱ تا ۵ است، در فراوانی نسبی هر یک از گویه‌ها ضرب می‌شود. مجموع این حاصل‌ضرب‌ها، ارزش هر شاخص را تشکیل می‌دهد. از آنجایی که برای تحلیل ارزش هر عامل لازم است تا این اعداد بین صفر و ۱ باشند، این ارزش‌ها باید نرمال‌سازی شوند. بدین منظور، مجموع ارزش همه شاخص‌های هر عامل، جمع شده و عددی به دست می‌آید که ارزش هر شاخص بر این عدد تقسیم می‌شود. بدین ترتیب، ارزش هر یک از شاخص‌ها نرمال شده و می‌توان از آن‌ها برای محاسبه ارزش هر عامل استفاده نمود. نتایج حاصل‌شده در جدول (۸) نشان داده شده‌اند.

جدول ۷. نتایج آزمون دوجمله ای بر روی عوامل و شاخص‌ها

عامل	گویه	تعداد (n)	نسبت مشاهده شده
شناخت سازمان	۱- تحلیل اثرات کسب و کار	۵۷	۰/۹۴
	۲- پارامترهای تداوم	۵۲	۰/۹۸
	۳- شناسایی فعالیت‌های کلیدی	۵۱	۰/۹۶
	۴- تعیین الزامات استمرار	۵۸	۰/۹۸
	۵- ارزیابی مخاطره	۵۶	۰/۹۸
	۶- تعیین گزینه‌های انتخاب	۵۸	۰/۹۴
بهبود مستمر	۷- اقدامات پیشگیرانه	۵۶	۰/۹۶
	۸- اقدامات اصلاحی	۵۸	۰/۹۴
	۹- توسعه مستمر	۵۱	۰/۹۲
ایجاد و مدیریت سامانه	۱۰- تعیین محدوده پیاده‌سازی	۵۸	۰/۹۴
	۱۱- خط مشی	۵۴	۰/۹۶
	۱۲- تدارک منابع	۵۸	۰/۹۴
	۱۳- شایستگی کارکنان	۵۳	۰/۹۴
ایجاد واکنش و طرح تداوم	۱۴- ساختار واکنش به حادثه	۵۸	۰/۹۴
	۱۵- نقش‌ها و وظایف در طرح	۵۷	۰/۹۸
	۱۶- فراخوانی طرح	۵۵	۱/۰۰
	۱۷- مالک سند مربوط به طرح	۵۷	۰/۹۸
	۱۸- اطلاعات مخاطبین در طرح	۵۴	۰/۹۸
	۱۹- فهرست فعالیت‌ها در طرح	۵۵	۰/۹۸
	۲۰- محل استقرار تیم حادثه	۵۴	۰/۸۹
بازبینی سامانه	۲۱- ممیزی داخلی	۵۶	۰/۹۶
	۲۲- بازنگری مدیریت	۵۴	۰/۹۴
تعمیم فرهنگ	۲۳- آگاهی عمومی	۶۰	۰/۹۳
	۲۴- آگاهی از مسئولیت‌ها	۵۲	۰/۹۸
مستند سازی	۲۵- کنترل سابقه‌ها	۶۱	۰/۹۵
	۲۶- کنترل مستندات	۵۷	۰/۹۲
تعیین راهبردهای تداوم	۲۷- راهبرد تداوم برای افراد	۵۸	۰/۹۳
	۲۸- راهبرد تداوم برای سایت	۵۹	۰/۹۴
	۲۹- راهبرد تداوم برای فناوری	۵۷	۰/۹۲
	۳۰- راهبرد تداوم برای اطلاعات	۵۶	۰/۹۸
	۳۱- راهبرد تداوم برای بودجه	۵۷	۰/۹۲
	۳۲- ذینفعان در راهبرد تداوم	۵۹	۰/۹۳
نگهداشت، تمرین و بازنگری	۳۳- تمرین طرح‌های تداوم	۵۶	۰/۹۲
	۳۴- نگهداشت ترتیبات تداوم	۵۶	۰/۹۲
	۳۵- بازنگری ترتیبات تداوم	۵۷	۰/۹۶
	۳۶- ممیزی ترتیبات تداوم	۵۱	۰/۹۴

جدول ۸. وزن عوامل و گویه‌های استخراج شده

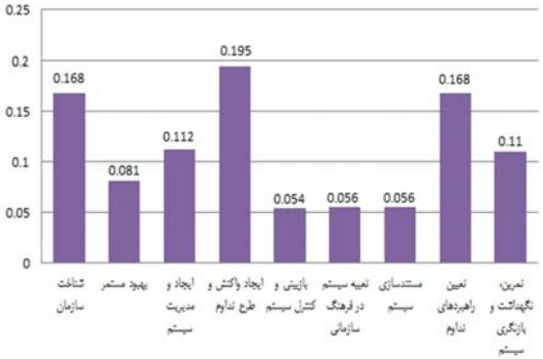
عامل	گویه	فراوانی نسبی طیف لیکرت					ارزش گویه	وزن گویه	امتیاز عامل	وزن عامل
		۱	۲	۳	۴	۵				
شناخت سازمان	۱- تحلیل اثرات کسب و کار	۰/۰	۳/۱	۱۲/۵	۳۲/۸	۵۱/۶	۴۳۲/۸	۰/۱۶۹	۲۵۶۵/۶	۰/۱۶۸
	۲- پارامترهای تداوم	۰/۰	۱/۶	۱۷/۲	۴۳/۸	۳۷/۵	۴۱۷/۲	۰/۱۶۳		
	۳- شناسایی فعالیت‌های کلیدی	۱/۶	۱/۶	۲۰/۳	۳۷/۵	۳۹/۱	۴۱۰/۹	۰/۱۶۰		
	۴- تعیین الزامات استمرار	۰/۰	۱/۶	۹/۴	۳۷/۵	۵۱/۶	۴۳۹/۱	۰/۱۷۱		
	۵- ارزیابی مخاطره	۰/۰	۱/۶	۱۲/۵	۳۷/۵	۴۸/۴	۴۳۲/۸	۰/۱۶۹		
	۶- تعیین گزینه‌های انتخاب	۱/۶	۳/۱	۹/۴	۳۲/۸	۵۳/۱	۴۳۲/۸	۰/۱۶۹		
بهبود مستمر	۷- اقدامات پیشگیرانه	۳/۱	۰/۰	۱۲/۵	۴۲/۲	۴۲/۲	۴۲۰/۳	۰/۳۳۹	۱۲۴۰/۶	۰/۰۸۱
	۸- اقدامات اصلاحی	۱/۶	۳/۱	۹/۴	۴۰/۶	۴۵/۳	۴۲۵/۰	۰/۳۴۳		
	۹- توسعه مستمر	۱/۶	۴/۷	۲۰/۳	۴۳/۸	۲۹/۷	۳۹۵/۳	۰/۳۱۹		
ایجاد و مدیریت سامانه	۱۰- تعیین محدوده	۱/۶	۳/۱	۹/۴	۳۷/۵	۴۸/۴	۴۲۸/۱	۰/۲۵۲	۱۷۰۰/۰	۰/۱۱۲
	۱۱- خط مشی	۰/۰	۳/۱	۱۵/۶	۳۴/۴	۴۶/۹	۴۲۵/۰	۰/۲۵۲		
	۱۲- تدارک منابع	۳/۱	۱/۶	۹/۴	۲۹/۷	۵۶/۳	۴۳۴/۴	۰/۲۵۶		
	۱۳- شایستگی کارکنان	۰/۰	۴/۷	۱۷/۲	۳۹/۱	۳۹/۱	۴۱۲/۵	۰/۲۴۳		
ایجاد واکنش و طرح تداوم	۱۴- ساختار واکنش به حادثه	۱/۶	۳/۱	۹/۴	۵۱/۶	۳۴/۴	۴۱۴/۱	۰/۱۳۹	۲۹۶۸/۸	۰/۱۹۵
	۱۵- نقش‌ها و وظایف در طرح	۰/۰	۱/۶	۱۰/۹	۴۲/۲	۴۵/۳	۴۳۱/۳	۰/۱۴۵		
	۱۶- فراخوانی طرح	۰/۰	۰/۰	۱۴/۱	۳۹/۱	۴۶/۹	۴۳۲/۸	۰/۱۴۶		
	۱۷- مالک سند طرح	۰/۰	۱/۶	۱۰/۹	۴۶/۹	۴۰/۶	۴۲۶/۶	۰/۱۴۴		
	۱۸- اطلاعات مخاطبین	۰/۰	۱/۶	۱۵/۶	۴۸/۴	۳۴/۴	۴۱۵/۶	۰/۱۴۰		
	۱۹- فهرست فعالیت‌ها	۰/۰	۰/۰	۱۴/۱	۲۶/۶	۵۷/۸	۴۴۰/۶	۰/۱۴۸		
	۲۰- محل استقرار تیم	۰/۰	۷/۸	۱۵/۶	۳۷/۵	۳۹/۱	۴۰۷/۸	۰/۱۳۷		
بازبینی سامانه	۲۱- ممیزی داخلی	۰/۰	۳/۱	۱۲/۵	۴۲/۲	۴۲/۲	۴۲۳/۴	۰/۵۱۱	۸۲۸/۱	۰/۰۵۴
	۲۲- بازنگری مدیریت	۱/۶	۳/۱	۱۵/۶	۴۸/۴	۳۱/۳	۴۰۴/۷	۰/۴۸۹		
تعبیه فرهنگ	۲۳- آگاهی عمومی	۰/۰	۶/۳	۶/۳	۴۲/۲	۴۵/۳	۴۲۶/۶	۰/۵۰۴	۸۴۶/۹	۰/۰۵۶
	۲۴- آگاهی از مسئولیت‌ها	۰/۰	۱/۶	۱۸/۸	۳۷/۵	۴۲/۲	۴۲۰/۳	۰/۴۹۶		
مستند سازی	۲۵- کنترل سابقه‌ها	۰/۰	۴/۷	۴/۷	۴۵/۳	۴۵/۳	۴۳۱/۳	۰/۵۰۵	۸۵۳/۱	۰/۰۵۶
	۲۶- کنترل مستندات	۰/۰	۴/۷	۱۲/۵	۳۹/۱	۴۳/۸	۴۲۱/۹	۰/۴۹۵		
تعیین راهبردهای تداوم	۲۷- راهبرد تداوم برای افراد	۳/۱	۳/۱	۹/۴	۳۹/۱	۴۵/۳	۴۲۰/۳	۰/۱۶۷	۲۵۵۶/۳	۰/۱۶۸
	۲۸- راهبرد تداوم برای سایت	۰/۰	۴/۷	۷/۸	۴۶/۹	۴۰/۶	۴۲۳/۴	۰/۱۶۹		
	۲۹- راهبرد تداوم برای فناوری	۳/۱	۳/۱	۱۰/۹	۳۷/۵	۴۵/۳	۴۱۸/۸	۰/۱۶۷		
	۳۰- راهبرد تداوم برای اطلاعات	۰/۰	۱/۶	۱۲/۵	۵۱/۶	۳۴/۴	۴۱۸/۸	۰/۱۶۷		
	۳۱- راهبرد تداوم برای بودجه	۱/۶	۴/۷	۱۰/۹	۵۰/۰	۳۲/۸	۴۰۷/۸	۰/۱۶۲		
	۳۲- ذینفعان در راهبرد تداوم	۱/۶	۴/۷	۷/۸	۴۲/۲	۴۳/۸	۴۲۱/۹	۰/۱۶۸		
نگهداشت، تمرین و بازنگری	۳۳- تمرین طرح‌های تداوم	۰/۰	۶/۳	۱۲/۵	۴۵/۳	۳۵/۹	۴۱۰/۹	۰/۲۴۶	۱۶۷۳/۴	۰/۱۱۰
	۳۴- نگه‌داشت ترتیبات تداوم	۰/۰	۴/۷	۱۴/۱	۴۲/۲	۳۹/۱	۴۱۵/۶	۰/۲۴۸		
	۳۵- بازنگری ترتیبات تداوم	۰/۰	۳/۱	۱۰/۹	۲۸/۱	۵۷/۸	۴۴۰/۶	۰/۲۶۳		
	۳۶- ممیزی ترتیبات تداوم	۰/۰	۴/۷	۲۰/۳	۳۹/۱	۳۵/۹	۴۰۶/۳	۰/۲۴۳		

با توجه به نتایج حاصل شده مطابق با جدول (۸)، در مورد عامل شناخت سازمان، شاخص تعیین الزامات استمرار، بیشترین امتیاز را به خود اختصاص داده است. همچنین مواردی همچون ارزیابی مخاطره و تحلیل اثرات کسب و کار دارای ارزشی برابر بوده و از درجه اهمیت بالایی در مدل برخوردار می‌باشند. با توجه به اهمیت خاصی که استاندارد برای این دو مبحث در قسمت برنامه‌ریزی سامانه قائل است، به نظر می‌رسد که در این مورد، پاسخ دهندگان نیز نظری یکسان با استاندارد را دارند. در مورد عامل بهبود مستمر، با توجه به مکمل بودن دو شاخص اقدامات اصلاحی و پیشگیرانه، امتیازات نزدیک به هم را از دید خبرگان کسب کرده‌اند. با توجه به نتایج حاصل‌شده برای عامل ایجاد و مدیریت BCMS،

شاخص تدارک منابع بیشترین امتیاز را به خود اختصاص داد. بدین ترتیب پاسخ‌دهندگان بر این باورند که تدارک منابع از ابعاد مختلف می‌تواند نقشی اساسی در شروع پیاده‌سازی را به خود اختصاص دهد. کنترل مستندات و رکوردهای مربوط به سامانه مدیریت تداوم کسب و کار نیز در عامل هفتم قرار می‌گیرند. این دو مبحث به عنوان دو فعالیت مستمر و بنیادین در سامانه در نظر گرفته می‌شوند که با توجه به استاندارد بودن اهداف، مستندسازی بسیار مهم و حیاتی می‌باشد. از این نتایج می‌توان دریافت که پاسخ دهندگان تفاوت محسوسی بین این دو شاخص قائل نگردیده‌اند.

عامل هشتم شامل راهبرد برای استمرار منابع مختلف سازمان نظیر: افراد، محل کار، فناوری، اطلاعات، موجودی و ذینفعان می‌باشد که در بررسی نظر پاسخ دهندگان، تفاوت زیادی بین اهمیت این شاخص‌ها مشاهده نمی‌شود، ولی می‌توان راهبرد تداوم برای سایت کاری را پررنگ‌تر دید که با مقایسه این یافته با اصول پدافند غیرعامل، ساخت و مقاوم‌سازی سازه‌های نظامی، صنعتی، تجاری و مسکونی به عنوان راهکاری مناسب برای کاهش خسارات جانی و مالی در اثر وقوع حوادث و بلایای طبیعی و یا انفجار در داخل یا خارج این سازه‌ها به دلیل حملات تروریستی اهمیت بیشتری پیدا کرده [۳۰] و از طرفی نشان می‌دهد ، اصل وجودی راهبرد مناسب در این حوزه، جدا از نوع راهبرد مورد استفاده دارای اهمیت بیشتری است.

در مجموع با توجه به نتایج حاصل‌شده مطابق با جدول (۸)، همان‌طور که در شکل (۲) نشان داده شده است، عامل ایجاد واکنش و طرح تداوم با اختلاف نسبتاً زیادی به عنوان مهم‌ترین عامل از سوی خبرگان در مدل پیشنهادی برای تحلیل شکاف سازمانی سامانه مدیریت تداوم فعالیت‌ها شناسایی شد. این نتیجه بیانگر این است که تمامی خبرگانی که در این پژوهش مورد سؤال قرار گرفته‌اند، بر عملی و مشهود بودن فعالیت‌های صورت گرفته نگاهی ویژه دارند. همچنین دو عامل شناخت سازمان و تعیین راهبردهای تداوم که جزء مراحل اولیه پیاده‌سازی سامانه می‌باشند در رتبه بعدی قرار گرفتند که باز هم نتیجه‌گیری فوق را تأیید می‌نمایند.



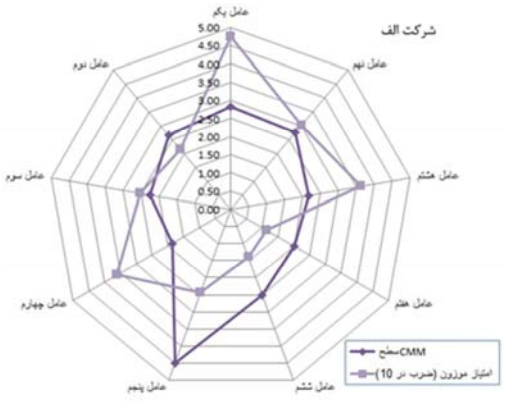
شکل ۲. وزن ها مدل برای عوامل مرتبط با تحلیل شکاف پیاده‌سازی BCMS

۳-۱. نتایج حاصل از اجرای مدل پیشنهادی

برای آزمودن مدل به دست آمده، شرکت ماموت فناوری اطلاعات (شرکت الف) و شرکت توسعه و نوآوری شهر (شرکت ب) به عنوان دو شرکت ارائه دهنده خدمات فناوری اطلاعات که قصد پیاده‌سازی سامانه مدیریت تداوم کسب و کار را دارند، انتخاب شدند. در مورد شرکت الف، با توجه به اینکه ارائه خدمات مشاوره در زمینه استقرار سامانه‌های مدیریتی از جمله سامانه مدیریت امنیت اطلاعات، جزء سبد محصول این شرکت می‌باشد و از طرفی سامانه مذکور در این شرکت پیاده‌سازی شده است، برخی از فعالیت‌های مشترک میان سامانه‌های مدیریتی دیگر و سامانه مدیریت تداوم کسب و کار در این شرکت از پیش پیاده‌سازی شده‌اند، از طرفی شرکت ب نیز با توجه به اینکه در حوزه بانکداری و پرداخت الکترونیکی فعالیت می‌کند و حساسیت خاص این بخش، برخی از نیازمندی‌های این سامانه را پوشش داده است.

با توجه به شاخص‌ها و وزن های که در مدل به دست آمد، جهت سنجش میزان پیاده‌سازی این شاخص‌ها در شرکت‌های مذکور از طریق مصاحبه با مدیران میانی و ارشد، برای هر کدام از شاخص‌ها مطابق با روش CMM سطوح پنج‌گانه‌ای شامل: ۱- اولیه، ۲- تکرارپذیر، ۳- تعریف شده، ۴- مدیریت شده و ۵-ب هبودیافته [۲۹]، در نظر گرفته شد. امتیاز موزون هر شاخص از ضرب سطح CMM در وزن آن مطابق مدل، به دست می‌آید. سطح CMM هر عامل در شرکت از میانگین سطوح CMM شاخص‌های آن عامل به دست می‌آید. از ضرب این سطح در وزن عامل مطابق مدل، امتیاز موزون عامل در شرکت به دست می‌آید. نتایج حاصل شده در جدول (۹) آورده شده‌اند.

برای درک بهتر میزان شکاف و فاصله شرکت‌های مورد بررسی، می‌توان از شکل‌های ۳ و ۴ استفاده نمود. در این نمودار می‌توان سطح CMM هر یک از عامل‌ها در مقایسه با امتیاز موزون آن را در قالب نمودار رادار برای هر یک از شرکت‌ها مقایسه نمود.



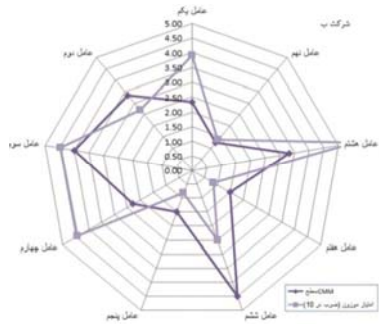
شکل ۳. وضعیت تحلیل شکاف تداوم فعالیت‌ها در شرکت الف

جدول ۹: سطح CMM در شرکت‌های مورد بررسی و نتایج اجرای مدل پیشنهادی

عامل	گویه	سطح CMM اولیه		امتیاز موزون		سطح CMM اولیه		امتیاز موزون	
		الف	ب	الف	ب	الف	ب	الف	ب
شناخت سازمان	۱- تحلیل اثرات کسب و کار	۲	۱	۰/۳۳۸	۰/۱۶۹	۲/۸۳	۲/۳۳	۰/۴۷۵	۰/۳۹۲
	۲- پارامترهای تداوم	۳	۲	۰/۴۸۹	۰/۳۲۶				
	۳- شناسایی فعالیت‌های کلیدی	۳	۵	۰/۴۸۹	۰/۸۰۰				
	۴- تعیین الزامات استمرار	۲	۴	۰/۳۴۲	۰/۶۸۴				
	۵- ارزیابی مخاطره	۴	۱	۰/۶۷۶	۰/۱۶۹				
	۶- تعیین گزینه‌های انتخاب	۳	۱	۰/۵۰۷	۰/۱۶۹				
بهبود مستمر	۷- اقدامات پیشگیرانه	۱	۴	۰/۳۳۹	۱/۳۵۶	۲/۶۶	۳/۳۳	۰/۲۱۵	۰/۲۷۰
	۸- اقدامات اصلاحی	۴	۵	۱/۳۷۲	۱/۷۱۵				
	۹- توسعه مستمر	۳	۱	۰/۹۵۷	۰/۳۱۹				
ایجاد و مدیریت سامانه	۱۰- تعیین محدوده	۲	۴	۰/۵۰۴	۱/۰۰۸	۲/۲۵	۴/۰۰	۰/۲۵۲	۰/۴۴۸
	۱۱- خط مشی	۱	۴	۰/۲۵۰	۱/۰۰۸				
	۱۲- تدارک منابع	۳	۴	۰/۷۶۸	۱/۰۲۴				
	۱۳- شایستگی کارکنان	۳	۴	۰/۷۲۹	۰/۹۷۲				
ایجاد واکنش و طرح تداوم	۱۴- ساختار واکنش به حادثه	۲	۴	۰/۲۷۸	۰/۵۵۶	۱/۸۵	۲/۲۸	۰/۳۶۱	۰/۴۴۵
	۱۵- نقش‌ها و وظایف در طرح	۳	۳	۰/۴۳۵	۰/۴۳۵				
	۱۶- فراخوانی طرح	۱	۱	۰/۱۴۶	۰/۱۴۶				
	۱۷- مالک سند طرح	۱	۲	۰/۱۴۴	۰/۲۸۸				
	۱۸- اطلاعات مخاطبین	۳	۲	۰/۴۲۰	۰/۲۸۰				
	۱۹- فهرست فعالیت‌ها	۲	۱	۰/۲۹۶	۰/۱۴۸				
	۲۰- محل استقرار تیم	۱	۳	۰/۱۳۷	۰/۴۱۱				
بازبینی سامانه	۲۱- ممیزی داخلی	۴	۱	۱/۰۲۲	۰/۵۱۱	۴/۵۰	۱/۵۰	۰/۲۴۳	۰/۰۸۱
	۲۲- بازنگری مدیریت	۵	۲	۰/۴۸۹	۰/۹۷۸				
تعبیه فرهنگ	۲۳- آگاهی عمومی	۳	۴	۱/۵۱۲	۲/۰۱۶	۲/۵۰	۴/۵۰	۰/۱۴۰	۰/۲۵۲
	۲۴- آگاهی از مسئولیت‌ها	۲	۵	۰/۹۹۲	۲/۴۸۰				
مستند سازی	۲۵- کنترل سابقه‌ها	۱	۲	۰/۵۰۵	۱/۰۱۰	۲/۰۰	۱/۵۰	۰/۱۱۲	۰/۰۸۴
	۲۶- کنترل مستندات	۳	۱	۱/۴۸۵	۰/۴۹۵				
تعیین راهبردهای تداوم	۲۷- راهبرد تداوم برای افراد	۴	۱	۰/۶۶۸	۰/۱۶۷	۲/۱۶	۳/۳۳	۰/۳۶۳	۰/۵۶۰
	۲۸- راهبرد تداوم برای سایت	۲	۵	۰/۳۳۴	۰/۸۴۵				
	۲۹- راهبرد تداوم برای فناوری	۳	۴	۰/۵۰۱	۰/۶۶۸				
	۳۰- راهبرد تداوم برای اطلاعات	۲	۵	۰/۳۳۴	۰/۸۳۵				
	۳۱- راهبرد تداوم برای بودجه	۱	۲	۰/۱۶۲	۰/۳۲۴				
	۳۲- ذینفعان در راهبرد تداوم	۱	۳	۰/۱۶۸	۰/۵۰۴				
نگه‌داشت، تمرین و بازنگری	۳۳- تمرین طرح‌های تداوم	۴	۱	۰/۹۸۴	۰/۲۴۶	۲/۷۵	۱/۲۵	۰/۳۰۳	۰/۱۳۷
	۳۴- نگه‌داشت ترتیبات تداوم	۳	۲	۰/۷۴۴	۰/۴۹۶				
	۳۵- بازنگری ترتیبات تداوم	۲	۱	۰/۵۲۶	۰/۲۶۳				
	۳۶- ممیزی ترتیبات تداوم	۲	۱	۰/۴۸۶	۰/۲۴۳				

همان‌طور که در شکل (۳) مشاهده می‌شود، در مورد شرکت الف، سطح CMM اظهار شده برای عامل پنجم که مواردی همچون بازنگری مدیریت و ممیزی داخلی را شامل می‌شود، با توجه به پیاده‌سازی دیگر سامانه‌های مدیریتی در شرکت، امتیاز بالاتری را معادل ۴/۵۰، به خود اختصاص داده است و دیگر عامل‌ها در بازه امتیازیِ ۱/۸۵ تا ۲/۸۳ قرار گرفته‌اند. پس از اعمال مدل پیشنهادی، مشاهده می‌شود که عامل اول- شناخت سازمان، به همراه عوامل چهارم- ایجاد واکنش و طرح‌های تداوم و هشتم- تعیین راهبردهای تداوم، به دلیل برخورداری از وزن ها بالاتر و یا همچنین وضعیت CMM بهتر در شرکت، امتیازات بهتری را کسب کرده‌اند.

از سوی دیگر مطابق با شکل (۴) در مورد شرکت ب، عوامل ایجاد و مدیریت سامانه و همچنین تعبیه سامانه در فرهنگ سازمانی دارای سطح CMM مناسب و بیشتر از ۴ می‌باشند. پس از اعمال مدل، عامل هشتم که به تعیین راهبردهای تداوم اختصاص دارد، توانست بالاترین امتیاز را در این شرکت کسب نماید.



شکل ۴. وضعیت تحلیل شکاف تداوم فعالیت‌ها در شرکت ب

۴. نتیجه‌گیری

در عصر فناوری اطلاعات و محیط رقابتی امروز، در بسیاری از کسب و کارها و به ویژه کسب و کارهای مرتبط با فضای دیجیتال، فرآیندهای کلیدی و محوری سازمان شدیداً به زیرساخت‌های فناوری اطلاعات وابسته می‌باشند و از کارافتادگی سامانه‌های بنیادین و اساسی، سازمان‌ها و حتی در بعضی موارد کشورها را با مشکلات جدی و هزینه‌های بالایی روبرو خواهد کرد. در این بین، بسیاری از مدیران به منظور حصول اطمینان از عدم بروز انقطاع در فرآیندهای سازمانی و به دنبال آن عدم بروز اختلال در ارائه خدمات و محصولات خود، سعی در به‌کارگیری روش‌ها، چارچوب‌ها و استانداردهای مرتبط با امنیت داده‌ها و مدیریت تداوم کسب و کار را دارند. با توجه به لزوم شناخت مناسب از وضعیت فعلی سازمان، قبل از شروع پروژه‌های پیاده‌سازی سامانه مدیریت تداوم کسب و کار، جهت بهینه شدن منابعی همچون هزینه و زمان پیاده‌سازی، نیاز به ابزار اندازه‌گیری مناسب برای سنجش میزان آمادگی سازمان و یا میزان فاصله سازمان با الزامات استاندارد در این حوزه احساس می‌شود. در این راستا، پس از بررسی ادبیات موضوع و استخراج ویژگی‌ها و فرآیندهای مورد نیاز در این سامانه، در نهایت ۳۶ گویه پایا و معتبر حاصل شد که با توجه به محاسبه میزان تأثیرگذاری هر یک در تعیین میزان فاصله سازمان با الزامات استاندارد از طریق اختصاص وزن به آن‌ها، ابزاری جهت میزان آمادگی سازمان برای پیاده‌سازی سامانه مدیریت تداوم کسب و کار بر مبنای استاندارد جهانی BS 25999 تهیه شد. نتایج وزن ها مدل پیشنهادی برای هر عامل در جدول (۱۰) نشان داده شده است.

با استفاده از ابزار ایجاد شده، تحلیل شکاف برای دو شرکت ارائه دهنده خدمات فناوری اطلاعات در مورد الزامات تداوم فعالیت‌ها بر مبنای استاندارد مذکور اندازه‌گیری شد. با توجه به نتایج پژوهش، مبنای بررسی امتیازات و نتیجه‌گیری‌ها در هر عامل، امتیاز موزون کسب شده توسط آن عامل خواهد بود. بدین ترتیب عامل اول- شناخت سازمان با کسب امتیاز ۰/۴۷۵ در شرکت الف و عامل هشتم- تعیین راهبردهای تداوم با کسب امتیاز ۰/۵۵۹ در شرکت ب دارای بالاترین آمادگی می‌باشند. می‌توان نتیجه گرفت دو شرکت در مهم‌ترین عامل شناسایی‌شده با ضریب ۰/۱۹۵، امتیاز نسبتاً بالایی معادل ۰/۳۶۱ و ۰/۴۴۵ را دریافت کرده و در نتیجه در مدل، در سطح خوبی قرار می‌گیرند. از سوی دیگر مواردی همچون عامل ششم-تعبیه سامانه در فرهنگ سازمانی با امتیاز ۰/۱۴۰ و عامل هفتم- مستندسازی سامانه با امتیاز ۰/۱۱۲ در شرکت الف و همچنین عوامل پنجم- بازبینی و کنترل سامانه با امتیاز ۰/۰۸۱ و هفتم- مستندسازی سامانه با امتیاز ۰/۰۸۴ در شرکت ب، برای پیاده سازی موفق‌تر سامانه در این شرکت‌ها باید بیش‌تر مورد توجه قرار گیرند. از حاصل جمع امتیاز موزون ۹ عامل می‌توان به یک عدد واحد دست یافت که میزان آمادگی نهایی سازمان را نشان می‌دهد و قابلیت اندازه گیری مجدد در طول زمان و یا مقایسه وضعیت آمادگی سازمان‌های مختلف را امکان‌پذیر می‌سازد. نتیجتاً دو شرکت ماموت فناوری اطلاعات و توسعه و نوآوری شهر به ترتیب با کسب امتیازات نهایی ۲/۴۶ و ۲/۶۶، مطابق با مدل CMM بین سطوح دوم (تکرار پذیر) و سوم (تعریف شده) قرار گرفتند که در مجموع وضعیت مناسبی برای پیاده‌سازی سامانه را می‌توان برای آن‌ها متصور شد.

جدول ۱۰. وزن‌ها مدل پیشنهادی

عامل	عنوان	وزن
۱	شناخت سازمان	۰/۱۶۸
۲	بهبود مستمر	۰/۰۸۱
۳	ایجاد و مدیریت سامانه	۰/۱۱۲
۴	ایجاد واکنش و طرح تداوم	۰/۱۹۵
۵	بازبینی و کنترل سامانه	۰/۰۵۴
۶	تعبیه سامانه در فرهنگ سازمانی	۰/۰۵۶
۷	مستندسازی سامانه	۰/۰۵۶
۸	تعیین راهبردهای تداوم	۰/۱۶۸
۹	تمرین، نگهداشت و بازنگری سامانه	۰/۱۱۰

در پایان برای پژوهش‌های آتی این حوزه، پیشنهاد می‌شود تا مدل اندازه‌گیری طراحی‌شده در دیگر شرکت‌ها و سازمان‌های متعلق به بخش خصوصی و دولتی مورد اعتباریابی قرار گرفته و نتایج حاصل از سازمان‌های مختلف با یکدیگر مقایسه گردند. همچنین با توجه به نوظهور بودن مفاهیم این حوزه و تعریف پروژه‌های جدید استقرار این سامانه در سازمان‌های مختلف، پیشنهاد می‌شود اثربخشی به‌کارگیری سامانه مدیریت تداوم کسب و کار، ارائه مدلی تلفیقی از ITIL، ISMS و BCMS برای پیاده‌سازی سامانه مدیریت خدمات فن‌آوری اطلاعات در بستری امن و مداوم و همچنین نقش استانداردهای حوزه سامانه مدیریت امنیت اطلاعات در مدیریت و بهینه‌سازی فعالیت‌های مرتبط با پدافند غیرعامل و یا تعمیم مدل پیشنهادی برای استانداردهای

هم‌خانواده نظیر اســتانداردهای ســری ۲۷۰۰۰، ۲۲۳۰۱ و ۲۲۳۰۲ نیــز مورد مطالعه قرار گیرد.

۵. مراجع

[1] Gibb, F.; Buchanan, S. "A Framework for Business Continuity Management"; Int. J. Inf. Manag. 2006, 26, 128-141.

[2] Ernest-Jones, T. "Business Continuity Strategy – The Life Line"; Network Security, 2005, 2005, 5-9.

[3] Gibb, F.; Buchanan, S.; Shah, S. "An Integrated Approach to Process and Service Management"; Int. J. Inf. Manag. 2006, 26, 44-58.

[4] Stanton, R. "Beyond Disaster Recovery: The Benefits of Business Continuity"; Comput. Fraud. Secur. 2005, 18-19.

[5] Jarvelainen, J. "IT Incidents and Business Impacts: Validating a Framework for Continuity Management in Information Systems"; Inf. Manag. 2013, 33, 583-590.

[6] Khosravi, M.; Parsa, S. "Design and Implementation of a Metamorphic Engine Malware with Evaluation of Identifying Techniques Performance Approach"; J. Passive Defence Sci. & Tech. 2013, 3, 145-155 (In Persian).

[7] Pritchard, S. "Continuity in A Disaster"; Infosecurity, 2007, 4, 24-25.

[8] Brooks, C.; Clem, L.; Aslam, M.; Neal, C.; Qiu, Y. L.; Sing, J.; Wong, F. Th.; Wright, I. R. "IBM System Storage Business Continuity: Part 1 Planning Guide"; Int. Business Machines Corporation Press: United States, 2007.

[9] Hosseini, S. A.; Eskandari, M. "Iran's Passive Defence Organization Study of Organizational Commitment Officers"; J. Dev. & Mgmt. Hum. Res. 2011, 20, 103-130 (In Persian).

[10] Smith, C. L.; Brooks, D. J. "Business Continuity Management"; Bus. Cont. Manag. 2013, 2013, 192-223.

[11] Weiner, B. J.; Amick, H.; Lee, S. Y. D. "Review: Conceptualization and Measurement of Organizational Readiness for Change: A Review of the Literature in Health Services Research and Other Fields"; Med. Care. Res. Rev. 2008, 65, 379-436.

[12] Discovery Learning "Research Summary 14-Development of the Change Readiness Gauge"; http://www. discoverylearning. com/images/document/Research%20Summaray14%20CRG.pdf , 2005.

[13] Frankland, J. "IT Security Metrics: Implementation and Standards Compliance"; Network Security 2008, 6-9.

[14] Dehmoubed, B. "Assessing Organizational Readiness in Chain Stores POSes Base on BS 25999"; Master Thesis, Department of Management, Tehran University 2009 (In Persian).

[15] Bottrell, E. G. "Business Rediness Assessment Plan-Project Implementation"; http://www.docstoc.com/docs/37728080/ ERP -Deliverables-Series, 2008.

[16] Khalfan, M. M. A.; Anumba, C. J.; Siemieniuch, C. E.; Sinclair, M. A. "Readiness Assessment of the Construction Supply Chain for Concurrent Engineering"; Eur. J. Purch. Supp. Manage. 2001, 7, 141-153.

[17] Mrayyan, M. T.; Modallal, R.; Awamreh, K.; Atoum, M.; Abdullah, M.; Suliman, S. "Readiness of Organizations for Change, Motivation and Conflict-Handling Intentions: Senior Nursing Students' Perceptions"; Nurs. Educ. Pract. 2008, 8, 120-128.

[18] Lehman, W. E. K.; Greener, J. M.; Simpson, D. D. "Assessing Organizational Readiness for Change"; J. Subt. Abuse. Treat. 2002, 22, 197-209.

[19] Brooks, C.; Clem, L.; Aslam, M.; Neal, C.; Qiu, Y. L.; Sing, J.; Wong, F. Th.; Wright, I. R. "IBM System Storage Business Continuity Solutions Overview"; Int. Business Machines Corporation Press: United States, 2007.

[20] Bedernjak, M. J.; Merryman, J. I. "Disaster Recovery Strategies with Tivoli Storage Management"; Int. Business Machines Corporation Press: United States, 2002.

[21] Drewitt, T. "A Manager's Guide to BS25999 A Practical Guide to Developing and Implementing A Business Continuity Management System"; IT Governance Pub.: London, 2008.

[22] Sharp, J. "The Route Map to Business Continuity Management: Meeting the Requirements of BS 25999"; British Standards Institute BSI: London, 2008.

[23] Calder, A. "Business Continuity and BS25999 A Combined Glossary"; IT Governance Pub: U.K. 2008.

[24] Shahidi, S. E. "A proposed Model for Assessing Organizational Readiness to Implement Information Security Management System"; Master Thesis, Department of Management & Accounting, Allameh Taba Tabaei University 2007 (In Persian).

[25] Mankins, J. C. "Technology Readiness Assessments: A Retrospective"; Acta. Astronaut. 2009, 65, 1216-1223.

[26] Ahonen, J. "Implementing a Social Intranet: A Study of Organizational Readiness for Change"; Master Thesis, Dep. of Management and International Business (Johtamisen ja kansainvälisen liiketoiminnan laitos), Aalto University 2011.

[27] Kwahk, K. Y.; Lee, J. N. "The Role of Readiness for Change in ERP Implementation: Theoretical Bases and Empirical Validation"; Inf. Manag. 2008, 45, 474-481.

[28] Ranaei, H.; Ghahremanifard, M. "Generate and Validating an Scale to Assess Organizational Readiness to Implementing Social Interanet"; J. Inf. Tech. Manag. 2013, 5, 37-60 (In Persian).

[29] Paulk, M. C.; Curtis, B.; Chrissis, M. B.; Weber, C. V. "Capability Maturity Model, Version 1.1"; IEEE Software, 1993, 10, 18-27.

[30] Sadrnejad, S. A.; Ziaei, M. "Behaviour of Bolted Beam-Column Connections Under Blast"; J. Passive Defence Sci. & Tech. 2013, 2, 93-101 (In Persian).