

شناسایی عوامل مؤثر بر طراحی فرآیندهای مدیریتی مرکز عملیات امنیت

علیرضا کرامتی پور^{*} ۱

حسین مسلمی ۲

چکیده

پژوهش حاضر با هدف تبیین عوامل مؤثر بر طراحی فرآیندهای مدیریتی مرکز عملیات امنیت، به دنبال پاسخ‌گویی به این سؤال اساسی است که «میزان تأثیر عوامل مؤثر بر فرآیندهای مدیریتی مرکز عملیات امنیت چگونه است؟» به‌منظور جمع‌آوری اطلاعات از ابزارهایی مانند مصاحبه، پرسش‌نامه و مطالعه اسناد و مدارک استفاده به‌عمل آمده است. جهت تجزیه و تحلیل اطلاعات و داده‌ها در بخش اسنادی روش تجزیه و تحلیل اطلاعات کیفی بوده و با کمک تحلیل محتوی انجام شده است و برای تحلیل داده‌های حاصل از پرسش‌نامه‌هایی که در بین ۶۵ نفر از جامعه آماری توزیع گردیده بود، با استفاده از آمار توصیفی و استنباطی با کمک نرم‌افزارهای اکسل و اس پی اس اس تحلیل‌های آماری لازم صورت گرفته و اطلاعات به‌دست‌آمده از جامعه نمونه به تعداد ۱۵۰ نفر جامعه آماری تعمیم داده شده است؛ و درنهایت به‌صورت آمیخته تحلیل گردیده است. طبق نتایج پژوهش، مدیریت پروژه، مدیریت دانش و تداوم فعالیت در بین عوامل مؤثر در طراحی فرآیندهای مدیریتی مرکز عملیات امنیت، از اهمیت زیادی برخوردارند. محقق بر اساس نتایج و یافته‌های تحقیق، پیشنهادهای خود را در دو دسته پیشنهادها اجرای و تحقیقی ارائه نموده است.

واژه‌های کلیدی:

طراحی فرآیند، مرکز عملیات امنیت، فرآیندگرایی

۱ کارشناس ارشد مدیریت دفاعی

۲ استادیار و عضو هیئت علمی دانشگاه فرماندهی و ستاد آجا

* نویسنده مسئول Email: alirezakp00@gmail.com

مقدمه

برخی تهدیدها مثل اختلالات ارتباطی و ویروس‌های اینترنتی مشکلاتی را در فضای تبادل داده ایجاد نموده و مانع از جابجایی بهینه‌ی اطلاعات گشته‌اند. با تأکید بر لزوم توجه به استانداردها و روش‌های امنیتی روز دنیا، یکی از راه‌کارهای مقابله با تهدیدها علیه این فضا، راه‌اندازی مراکزی چون مرکز عملیات امنیت^۱ است. یک مرکز عملیات امنیت متشکل از سه رکن: فناوری، افراد و فرآیندها است؛ که نظارت و تجزیه و تحلیل و همچنین واکنش به تهدیدات امنیت اطلاعاتی را متمرکز می‌سازد. هر مرکز عملیات امنیت از سه لایه اصلی به شرح زیر تشکیل شده است:

لایه اول (مرکز تماس): نقطه تماس کاربران و مسئول پاسخ‌گویی به اخطارهای دریافتی از کاربران است. در این سطح به کلیه اخطارهایی که از پیچیدگی پایین‌تری برخوردارند، پاسخ داده می‌شود.

لایه دوم (تحلیل اولیه): این سطح در حقیقت مکمل سطح یکم است و مسئول پاسخ‌گویی به مشکلات پیچیده‌تر در سامانه‌های امنیتی شبکه است. برای اخطارهایی که از اهمیت بالایی برخوردارند، سامانه‌های سطح دوم به‌طور کامل درگیر می‌شوند.

لایه سوم (تحلیل تخصصی): در این سطح کارشناسان ارشد و مشاوران امنیتی شبکه قرار دارند. این سطح در حقیقت پشتیبان دو سطح پایین‌تر است. کلیه تدابیر امنیتی و مدیریت امنیت شبکه، در این سطح اندیشیده می‌شود.

در هر یک از لایه‌های مطرح‌شده، ابزارهایی برای مدیریت سامانه‌های امنیتی در نظر گرفته می‌شود. این ابزارها، امنیت شبکه را از دو دیدگاه درون‌سازمانی و برون‌سازمانی موردبررسی قرار می‌دهند. برای این منظور، هر مرکز عملیات امنیت دارای تجهیزاتی در داخل شبکه و تجهیزات دیگری در داخل مرکز عملیات امنیت است و تمامی خدماتی که ارائه می‌شوند، پایش و مدیریت می‌شوند (جنگجو، ۱۳۹۴). طراحی فرآیندهای مدیریتی مرکز عملیات امنیت، این اطمینان را حاصل می‌کند که کارشناسان این مرکز، وظایف محوله را به‌درستی انجام داده و بررسی و برخورد با رخدادها، امنیتی به‌خوبی انجام شود. برای طراحی این فرآیندها استفاده از الگوهایی مانند چارچوب طبقه‌بندی فرآیندها^۲ منتشرشده توسط مرکز بهره‌وری و کیفیت آمریکا^۳ به‌عنوان الگویی باز که به کار گرفته می‌شود تا بهبود سازمان‌ها را از طریق مدیریت

^۱.SOC: Security Operation Center

^۲. PCFSM

^۳. APQ: American Productivity & Quality Center

فرآیندها و الگوبرداری از بهترین‌ها صرف‌نظر از صنعت، اندازه و موقعیت جغرافیایی آن تسهیل نماید، راهگشا خواهد بود (جعفری و همکاران (مترجم)، ۱۳۹۳).

با نگرش به اینکه هدف حمله‌کنندگان، تحت‌الشعاع قرار دادن یک یا چند ضلع از اضلاع مثلث امنیت، شامل: محرمانگی^۱، صحت^۲ و دسترس‌پذیری^۳ است و با توجه به اینکه روش‌ها و فناوری‌های مورد استفاده در حمله به زیرساخت‌های داده‌ای، روزبه‌روز پیچیده‌تر می‌شوند، طراحی و پیاده‌سازی یک مرکز عملیات امنیت کارا، می‌تواند تا حد قابل قبولی، آسودگی خاطر را برای فرماندهان و مدیران فناوری اطلاعات و ارتباطات، در حوزه امنیت به ارمغان آورد. ایجاد مرکز عملیات امنیت به‌منظور تحلیل و پایش مستمر تهدیدها و مقابله با حمله‌ها به زیرساخت‌های داده‌ای ج.ا.ایران می‌تواند متضمن پایداری سامانه‌های مأموریتی و عملیاتی و افزایش سطح امنیت و دسترس‌پذیری سامانه‌های حیاتی سازمان‌های دولتی و نظامی شود. در معماری و طراحی ساختار این مرکز، توجه به طراحی و پیاده‌سازی فرایندهای مدیریتی می‌تواند نقش بسزایی در شکل‌گیری این مرکز حیاتی ایفا کند.

معرفی مرکز عملیات امنیت

با توجه به هدف تحقیق، سعی شده است که در خصوص طراحی مرکز عملیات امنیت، با نگرش به رویکرد فرآیندی و دیدگاه فرآیند‌گرایی و بر اساس چارچوب‌های طبقه‌بندی فرآیند و استانداردهای طراحی فرآیند و بهبود فرآیند، ابعاد فرآیندی این مرکز، مورد توجه قرار گرفته و مؤلفه‌ها و عوامل تأثیرگذار بر طراحی فرآیند مدیریتی مرکز، شناسایی و معرفی شوند.

مرکز عملیات امنیت واحدی متمرکز برای رسیدگی به حوادث امنیتی، کشف و اولویت‌دهی حوادث، تشخیص و واکنش سریع در برابر حوادث، مدیریت و مانیتورینگ زوایای امنیتی سازمان و تعیین سطح ریسک و دارایی‌ها می‌باشد. این مرکز از طریق یک کنسول مرکزی وضعیت آنچه را که در حال حاضر در شبکه در حال اتفاق است را نشان می‌دهد و تمامی زوایای امنیتی را به‌صورت بلادرنگ از یک نقطه مرکزی مدیریت و مانیتور می‌کند و راهکارهای مناسبی را متناسب با هر رویداد، اجرا یا پیشنهاد می‌نماید. سامانه‌هایی که در مرکز عملیات امنیت جهت مدیریت امنیت شبکه نصب و راه‌اندازی می‌گردند، دارای مکانیسم‌های بررسی تجهیزات شبکه به‌صورت خودکار می‌باشند. تجهیزاتی که توسط این سیستم مورد بررسی قرار

^۱. Confidentiality

^۲. Integrity

^۳. Availability

می‌گیرند، محدود به سامانه‌های امنیتی نیستند، بلکه کلیه تجهیزات زیرساختی شبکه نیز توسط این سیستم مدیریت امنیت یکپارچه مورد بررسی قرار می‌گیرند. این مرکز در حقیقت الگوهای ترافیکی ارسالی از کلیه تجهیزات شبکه از جمله سرورها، مسیریاب‌ها، دیواره آتش‌ها و سامانه‌های امنیتی فیزیکی را مورد بررسی قرار داده و هرکدام از آن‌ها که توان ایجاد یک ریسک امنیتی را دارند مشخص می‌سازد و راه نفوذ به آن سیستم را می‌بندد. هر الگوی ترافیکی غیرعادی مشاهده شده، توسط زیرسیستم‌های آنالیز کننده مورد بررسی قرار می‌گیرد و متناسب با نوع خطای تشخیص داده شده، اخطارهای لازم در شبکه برای هر یک از تجهیزات مربوطه ارسال می‌گردد.

دلایل نیاز به مرکز عملیات امنیت

با وجود تجهیزات و نرم‌افزارهای امنیتی مانند دیواره آتش‌ها، سامانه‌های تشخیص نفوذ و آنتی‌ویروس‌ها بازهم نیاز به مرکزی یکپارچه که تمام فعالیت‌های امنیتی یک سازمان را مدیریت کند، دیده می‌شود. مشکلاتی که این تجهیزات و نرم‌افزارها می‌توانند در حین فعالیت خود داشته باشند شامل موارد ذیل می‌باشد:

- امکان حمله به تجهیزات و نرم‌افزارهای امنیتی مورد استفاده در سازمان
- تأخیر در گرفتن رویدادهای جدید از تجهیزات و نرم‌افزارهای امنیتی مورد استفاده در سازمان
- عدم یکپارچگی رویدادها و تحلیل و پاسخ‌دهی مناسب
- تولید رویدادهای بسیار زیاد که تحلیل آن‌ها برای نیروی انسانی امکان‌پذیر نیست.
- پیچیدگی بعضی حملات سایبری که درک مراحل مختلف آن‌ها برای نیروی انسانی امکان‌پذیر نیست.

اهداف پیاده‌سازی مرکز عملیات امنیت

- برخورد مناسب و مؤثر با رویدادهای امنیتی و تأمین امنیت شبکه در مقابل تهدیدهای احتمالی در درون و بیرون سازمان
- ارتقاء امنیت و پایداری داده‌ها و خدمات به‌وسیله حفاظت از زیرساخت‌های اطلاعاتی، ترافیک، سرویس‌ها و داده‌های مشتریان
- کاهش زمان اختلال در ارائه خدمات به مشتری
- بهبود و تسریع در پاسخ‌ها و واکنش‌ها امنیتی
- بهبود کارایی شبکه

- کاهش هزینه‌های ناشی از تهدیدها و حملات امنیتی (همان)

ویژگی‌های ساختاری در طراحی مرکز عملیات امنیت

مرکز عملیات امنیت باید ویژگی‌های عمومی زیر را داشته باشد:

- مقیاس‌پذیری: مرکز عملیات امنیت باید به نحوی طراحی گردد که با افزایش میزان ترافیک و رخدادهای تولیدی، بتواند با کارایی بالا وظیفه خود را انجام دهد.
- ماژولار بودن: منابع جمع‌آوری رخدادهای در یک مرکز عملیات امنیت در دوره‌های زمانی مختلف دچار تغییر و تحول می‌گردند. پس مرکز باید به نحوی طراحی شود که به راحتی بتوان منابع و الگوریتم‌های تحلیل و همبستگی جدید را به سامانه اضافه کرد و یا تغییر داد. به‌طور کلی باید طراحی ماژولار در کلیه بخش‌ها و زیرسامانه‌های مرکز عملیات امنیت مورد توجه قرار گیرد.
- کارایی بالا: مرکز عملیات امنیت باید تمام اجزای شبکه شامل کلیه کارگزارها، نرم‌افزارها، تجهیزات و ترافیک شبکه را رصد و همچنین الگوریتم‌های تحلیل، همبستگی و همچنین اطلاعات مربوط به آسیب‌پذیری‌ها، الگوی حملات، سیاست‌های امنیتی و وضعیت سامانه را به‌روز کند.
- امنیت: از آنجاکه هدف مرکز عملیات امنیت تأمین و تضمین امنیت و پایداری داده و خدمات است، پیاده‌سازی آن نباید خود منجر به بروز مخاطرات امنیتی جدید در بستر اطلاعاتی گردد. با توجه به دسترسی این مرکز به کلیه تجهیزات امنیتی، ترافیک و سیاست‌های شبکه و اجزای آن، استفاده از دانش و سامانه‌های بومی و مطمئن در طراحی و پیاده‌سازی آن در زیرساخت‌های کشور از اهمیت قابل توجهی برخوردار است (مردانی، ۱۳۹۴).

الزام‌های مهم در طراحی و پیاده‌سازی مرکز عملیات امنیت

- جمع‌آوری رخدادهای از منابع مختلف باید از طریق کانال‌های امن صورت گیرد.
- حتی‌المقدور باید از نصب عامل‌ها بر روی سامانه‌ها جهت جمع‌آوری رخدادهای اجتناب کرد. چراکه خود عامل‌ها می‌توانند باعث به وجود آمدن شکاف‌های امنیتی در سامانه گردند.
- نگهداری رخدادهای، رویدادهای، پیکربندی سامانه‌ها، سیاست‌های امنیتی و دسترسی به آن‌ها باید کاملاً امن باشد.
- دسترسی کاربران به پورتال باید بر اساس نقش آن‌ها بوده و تمامی فعالیت‌های انجام‌گرفته توسط هر کاربری باید ثبت گردد.

• ارتباط با گروه‌های واکنش هماهنگ رویدادهای رایانه‌ای از دیگر ویژگی‌های حائز اهمیت، ارتباط و همبستگی مرکز عملیات امنیت و مراکز امداد و نجات رایانه‌ای و گروه‌های واکنش هماهنگ رویدادهای رایانه‌ای است. به‌گونه‌ای که مراکز عملیات امنیت جهت به‌روزرسانی و جامع کردن پایگاه دانش خود از خروجی‌های حاصل از اقدامات مراکز امداد و نجات رایانه‌ای استفاده می‌کنند (همان، ۳۳۹).

بخش‌های اصلی مرکز عملیات امنیت

- تولیدکننده وقایع^۱: این ماژول، شامل تمامی تجهیزات امنیتی به‌صورت سخت‌افزاری و نرم‌افزاری می‌باشد که در بخش‌های مختلف شبکه قرار گرفته‌اند و وقایع امنیتی را شناسایی و برای تجهیزات مربوط به ماژول جمع‌کننده وقایع ارسال می‌نمایند.
- جمع‌کننده وقایع^۲: این ماژول، شامل تجهیزاتی است که مسئول دریافت وقایع از تجهیزات داخل شبکه یا تولیدکننده‌های وقایع می‌باشند. تمامی وقایع برای جمع‌کننده وقایع ارسال شده و بعد از دسته‌بندی وقایع، آن‌ها را برای ماژول‌های دیگر ارسال می‌کنند.
- پایگاه داده وقایع^۳: این ماژول شامل پایگاه داده‌هایی می‌باشد که بعد از دریافت اطلاعات از جمع‌کننده وقایع، آن‌ها را ذخیره کرده و در اختیار ماژول‌های دیگر قرار می‌دهد.
- تحلیلگر وقایع^۴: این ماژول شامل تجهیزاتی می‌باشد که بعد از ثبت وقایع در پایگاه داده، آن‌ها را آنالیز و بررسی کرده و نتیجه آن را در اختیار ماژول‌های دیگر قرار می‌دهد. این تحلیل می‌تواند منجر به شناسایی رخداد در شبکه شده که با ارائه آن به ماژول واکنش‌دهنده از بروز رخداد جلوگیری نماید.
- واکنش‌دهنده وقایع^۵: این ماژول در صورت تشخیص رخداد توسط تحلیلگر وقایع، می‌تواند به تجهیزات امنیتی فرمان داده و از عبور ترافیک مخرب در شبکه جلوگیری نماید.
- گزارش‌دهنده وقایع^۶: این ماژول به‌منظور ارائه گزارش رخدادهای صورت گرفته در شبکه به مدیران شبکه و یا اپراتورهای بخش مرکز عملیات امنیت می‌باشد. اطلاعات رخدادها توسط ماژول تحلیلگر، شناسایی گشته و توسط ماژول گزارش، اعلام خواهند شد.

^۱ -Event Generator

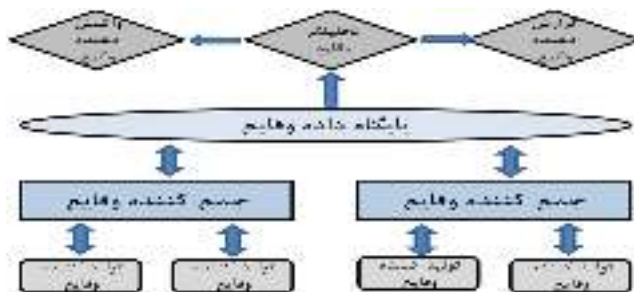
^۲ -Event Collector

^۳ -Event Database

^۴ -Event Analysis

^۵ -Event Reaction

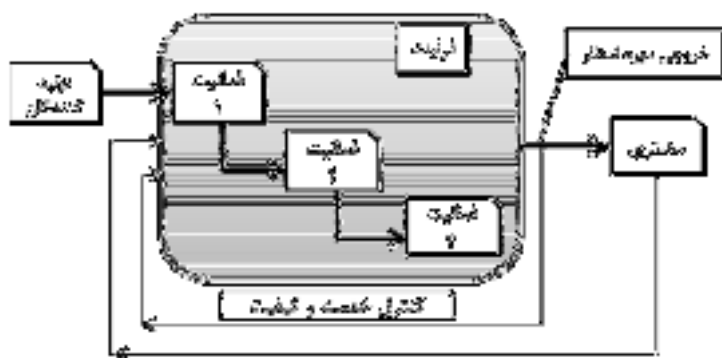
^۶ -Event Reporting



شکل (۱) بخش‌های اصلی مرکز عملیات امنیت

فرآیند

فرآیندها، نمونه‌ای از سامانه‌های بسته هستند که در راستای نیل به هدف، تغییر یافته و دگرگون شده و برای خود تقویتی و خود اصلاحی از بازخوردها بهره می‌گیرند. در نظر گرفتن کل یک فرآیند یا چگونگی تناسب یک فرآیند با فرآیندهای دیگر، اهمیت زیادی دارد (شارن، ۱۳۹۰).



شکل (۲) چرخه فرآیند (شارن، ۱۳۹۰)

تعریف فرآیند، توصیف‌کننده اقدامات، وابستگی‌ها و توالی است. فرآیندها دارای ویژگی‌های زیر هستند:

- قابلیت اندازه‌گیری: می‌توان فرآیندها را با روش مناسبی اندازه‌گیری نمود. این اقدام یک فرآیند عملگراست. مدیران، خواهان ارزیابی هزینه، کیفیت و سایر متغیرها هستند، درحالی‌که افراد حرفه‌ای اغلب به دنبال اندازه‌گیری بهره‌وری و مدت‌زمان انجام فرآیندها هستند.

- نتایج خاص: دلیل وجودی یک فرآیند، تحویل نتایجی خاص است. این نتایج، بایستی به صورت مجزا، قابل شناسایی و شمارش باشند. درحالی که می توانیم تغییرات را شمارش کنیم، شمارش تعداد تغییرات تکمیل شده از طریق میز خدمات غیرممکن است.
 - مشتریان: هر فرآیند، نتایج اولیه خود را به مشتریان یا ذی نفعان ارائه می دهد. مشتریان ممکن است در داخل یا خارج سازمان باشند اما فرآیندها باید انتظارات آنها را برآورده سازند.
 - پاسخ به یک حادثه خاص: درحالی که ممکن است یک فرآیند در حال انجام و یا به صورت تعاملی باشد، بایستی از طریق یک محرک خاص، قابل ردیابی باشد.
- معمولاً کارکردها، فرآیندها، نقش ها و فعالیت ها با یکدیگر ادغام می شوند. کارکردها و فرآیندها نیز معمولاً با یکدیگر اشتباه گرفته می شوند (همان).

انواع فرآیندها

فرآیندهای اصلی:

فرآیندی است که فلسفه وجودی واحد مربوطه را تشکیل داده و در ارتباط مستقیم با مشتری نهایی قرار دارد. به گام های اصلی فرآیندهای اصلی، فرآیند فرعی گفته می شود.

فرآیندهای پشتیبانی:

فرآیندی است که به طور غیرمستقیم و با تأمین منابع مورد نیاز فرآیندهای اصلی در جهت تأمین نیازها و انتظارات مشتری های نهایی عمل می کند.

فرآیندهای مدیریت:

فرآیندهایی هستند که وظیفه هدایت و رهبری نیروی انسانی در دستیابی به اهداف سازمانی را دنبال می کنند (وزارت بهداشت، درمان و آموزش پزشکی، ۱۳۸۷).

رویکرد فرآیندی

بکار گرفتن سیستمی از مجموعه فرآیندها، در درون یک سازمان همراه با مشخص کردن ارتباطات و تعاملات این فرآیندها و مدیریت آنها برای ایجاد خروجی مطلوب، به عنوان رویکرد فرآیندی نامیده می شود. در تمامی سازمان ها، نتایج دلخواه با کارایی بهتر و اثربخشی بیشتر زمانی حاصل می شود که فعالیت ها و منابع مرتبط باهم به عنوان یک فرآیند مدیریت شوند. البته معیارهایی از جنس کارایی و اثربخشی، نمایانگر استفاده حداقل از رویکرد فرآیندی می باشد که برای تکمیل آنها بایستی معیارهای مناسبی نیز از جنس بهره وری و سودآوری را به آن اضافه کرد. بدون تردید طراحی و پیاده سازی رویکرد فرآیندی بسیار سخت تر از طراحی

و پیاده‌سازی رویکرد وظیفه‌ای است. این امر حتی در اجرای اولیه رویکرد فرآیندی نیز صادق است. بیشتر سازمان‌ها در سال اول اجرای رویکرد فرآیندی مشکلات زیادی دارند؛ اما با گذشت زمان کم‌کم، سازمان بهبودهای بیشتری در فرآیندهای خود به وجود می‌آورد. با گذشت زمان به همان نسبت نیز مهارت مدیران و کارکنان در رابطه با فرآیندها بیشتر می‌شود که منجر به مدیریت ساده‌تر و سهل‌تر فرآیندها می‌شود.

به‌طور کلی رویکرد فرآیندی بر اهمیت موارد زیر تأکید دارد:

- (۱) در نظر گرفتن فرآیند برحسب ارزش‌افزوده
- (۲) درک و برآورده کردن الزامات
- (۳) نائل شدن به نتایج مربوط به کارایی، اثربخشی، بهره‌وری و سودآوری فرآیند
- (۴) بهبود مستمر فرآیندها بر پایه اندازه‌گیری‌های مبتنی بر واقعیت (خوش‌دهان، ۱۳۹۰)

فعالیت‌های موردنیاز جهت فرآیند گرایی

در تعریف فرآیند گرایی چنین گفته می‌شود که روشی است که با محور قرار دادن فرآیندهای کسب و کار و حذف فعالیت‌های بدون ارزش‌افزوده، برای سازمان مزیت رقابتی به ارمغان می‌آورد. برای اینکه یک سازمان در راه فرآیندگرایی گام بردارد می‌بایست تمامی تلاش خود را جهت پیاده‌سازی موارد زیر به کار گیرد:

- الف) تشخیص فرآیندها: ابتدا باید فرآیندها را شناسایی کرده و برای آن‌ها نام و عنوان برگزید. شناسایی و نام‌گذاری فرآیندها گامی بسیار حساس و بنیادین است. پاره‌ای از سازمان‌ها به اشتباه، فعالیت‌های وظیفه‌ای کنونی را فرایند به حساب می‌آورند.
- ب) شناساندن اهمیت فرآیندها به همه دست‌اندرکاران: گام دوم شناساندن فرآیندها و اهمیت آن‌ها به همه مدیران، کارکنان و نمایندگان دور و نزدیک است به‌نحوی که باید فرآیندها، نام آن‌ها، ورودی‌ها و خروجی‌ها و ارتباطات آن‌ها برای همه افراد ملموس باشد.
- ج) انتخاب معیار ارزیابی: برای اطمینان از کارکرد درست فرآیندها، باید بتوان پیشرفت آن‌ها را اندازه گرفت و در آن صورت به معیارهایی نیاز است. این معیارها می‌توانند برحسب ضرورت بر پایه خواسته مشتری یا بر پایه نیازهای خود سازمان مانند هزینه فرایند و به‌کارگیری درست منابع واقع شوند.
- د) به‌کارگیری مدیریت فرآیند گرا: سازمان فرایند محور بایستی همواره در بهسازی فرآیندهای خود بکوشد زیرا این رویکرد کاری پیوسته و مداوم است. بنابراین، عمده فعالیت مدیریتی

این‌گونه سازمان‌ها اداره و پیشبرد درست فرآیندها در بالاترین توان آن‌ها، بهره‌گیری از فرصت‌ها در بهسازی فرآیندها و پیگیری در کاربرد فرصت‌ها است. فرایند محوری یک طرح موقتی نبوده، بلکه راه و روشی دائمی و فراگیر است (وزارت بهداشت، درمان و آموزش پزشکی، ۱۳۸۷).

استانداردهای مدیریت خدمات فناوری اطلاعات

مهم‌ترین استانداردهایی که در مدیریت خدمات فناوری اطلاعات مورد استفاده قرار می‌گیرند، عبارتند از:

ایزو/آی ای سی ۲۰۰۵:۲۰۰۰:

این استاندارد رویکرد فرآیند یکپارچه را برای اثربخشی در ارائه خدمات مدیریت‌شده به‌منظور دستیابی به نیازمندی‌های کسب و کار و مشتری، ترویج می‌دهد. همچنین برای یک سازمان با وظایف اثرگذار، تعدادی فعالیت به‌هم پیوسته را شناسایی و مدیریت می‌کند. ادغام و پیاده‌سازی هماهنگ شده فرآیندهای مدیریت خدمات، کنترل مداوم، کارایی و فرصت‌هایی بیشتر را برای بهبود مستمر فراهم می‌کند.

ایزو/آی ای سی ۱۵۵۰۴:

چارچوبی برای ارزیابی قابلیت فرآیند است که می‌تواند توسط سازمان‌ها و در زمینه‌هایی مانند برنامه‌ریزی، مدیریت، نظارت، کنترل و بهبود، یادگیری، تدارک و توسعه، عملیاتی‌سازی، تکامل و پشتیبانی از محصولات و خدمات مورد استفاده قرار گیرد.

این استاندارد برای استفاده توسط ارزیابان در فرآیند ارزیابی عملکرد و نیز توسط سازمان‌ها در توسعه مدل‌های مرجع فرآیندی، مدل‌های ارزیابی فرآیند و فرآیندهای ارزیابی فرآیند، در نظر گرفته شده است (شارن، ۱۳۹۱).

چارچوب‌های فرآیندی و بهبود مستمر خدمات

کتابخانه زیرساخت فناوری اطلاعات^۱

در سال ۱۹۸۹ ایجاد گردیده و به تفصیل راهنمایی‌هایی را در مورد ساختار، ادغام و بهبود در فرآیندها و خدمات فناوری اطلاعات فراهم نموده است که البته به روز رسانی و اصلاح گردیده است و توسط دفتر بلزرگانی دولت انگلستان اداره می‌شود (همان، ۱۸۸).

^۱. ITIL

کویت یا همان اهداف کنترلی برای اطلاعات و فناوریهای مربوطه^۱

ابتدا در سال ۱۹۹۵ به عنوان چارچوب ممیزی برای سامانه‌های اطلاعاتی ایجاد گردید و پس از بلوغ، به چارچوب مدیریت فناوری اطلاعات کامل تبدیل شد.

پیکره دانش مدیریت پروژه^۲

مجموعه دانش کسب‌شده در حرفه مدیریت پروژه است. حاوی شیوه‌های سنتی ثابت شده می‌باشد که به طور گسترده به کار می‌روند، همچنین شامل شیوه‌های ابتکاری که در این حرفه پدیدار گشته‌اند و نیز موضوعات منتشر شده و منتشر نشده می‌باشد و به‌طور مداوم در حال تحول است.

چارچوب طبقه‌بندی فرآیندها^۳

چارچوب طبقه‌بندی فرآیندها منتشرشده توسط مرکز بهره‌وری و کیفیت آمریکا^۴ طبقه‌بندی مشتمل بر فرآیندهای کسب‌وکار با کارکردهای متنوع است این طبقه‌بندی بر آن است که امکان مقایسه عینی عملکردهای درون‌سازمانی و بین‌سازمانی را با یک الگوی مبنا ایجاد نماید. این چارچوب توسط مرکز بهره‌وری و کیفیت آمریکا و شرکت‌های عضو آن توسعه‌یافته است و به‌عنوان الگویی باز، به کار گرفته می‌شود تا بهبود سازمان‌ها را از طریق مدیریت فرآیندها و الگوبرداری از بهترین‌ها صرف‌نظر از صنعت، اندازه و موقعیت جغرافیایی آن تسهیل نماید چارچوب طبقه‌بندی فرآیندها، فرآیندهای عملیاتی و مدیریتی را در سطح سازمانی، در ۱۲ گروه یکپارچه طبقه‌بندی کرده است و شامل گروه‌های فرایندی و بیش از ۱۰۰۰ فرایند و فعالیت‌های مرتبط با آن است (جعفری و همکاران (مترجم)، ۱۳۹۳).

فرآیندهای طراحی

وجود یک مدل فرآیندی به درک ویژگی‌های فرآیند کمک می‌کند. منظور از فرآیند، طراحی مجموعه‌ای ساختاریافته از فعالیت‌ها برای تأمین هدفی خاص می‌باشد. این فرآیند می‌تواند یک یا چند ورودی داشته باشد و آن‌ها را به خروجی‌های تعریف‌شده تبدیل نماید. علاوه بر این، شامل تمامی نقش‌ها و مسئولیت‌ها، ابزارها و کنترل‌های مدیریتی لازم برای ارائه خروجی‌های قابل‌اعتماد می‌باشد. همچنین، یک فرآیند ممکن است در مواقع لزوم سیاست‌ها، استانداردها،

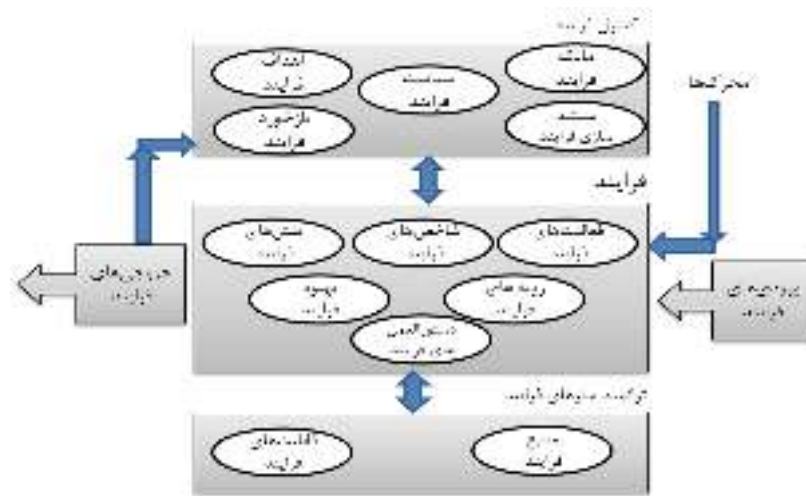
1. COBIT: Control Objectives For Information And Related Technology

2. PMBOK: Project Management Body of Knowledge

3. PCFSM

4. APQ: American Productivity & Quality Center

خطوط راهنما، فعالیت‌ها، فرآیندها، روش‌های اجرا و دستورالعمل‌های کاری را تعریف یا اصلاح نماید.



شکل (۳) چارچوب یک مدل فرآیندی (شارن، ۱۳۹۰)

فعالیت برنامه‌ریزی و تنظیم یک فرآیند، باهدف انجام آن از روشی مؤثر، کارآمد و پایدار را کنترل فرآیند می‌نامند. هنگامی‌که یک فرآیند تعریف شد، مستندسازی و کنترل آن ضرورت می‌یابد. فرآیند تحت کنترل، تکرارپذیر و قابل مدیریت می‌باشد. اجزای کلی یک فرآیند، شامل فرآیند ورود داده، پردازش آن، خروجی و نتایج اندازه‌گیری و بازنگری است. همیشه سازمان‌دهی فرآیند حول محور مجموعه‌ای از اهداف انجام می‌شود. خروجی‌های مهم فرآیند باید توسط اهداف آن هدایت‌شده و همیشه شامل شاخص‌های اندازه‌گیری فرآیند، گزارش‌ها و بهبود فرآیند باشند. هر فرآیند باید مالکی داشته باشد که مسئولیت فرآیند و بهبود آن را به عهده گرفته و دستیابی به اهداف آن را تضمین نماید. اهداف هر فرآیند باید از منظر منافع سازمانی و بر اساس راهبرد و اهداف کسب‌وکار، به شکلی قابل اندازه‌گیری تعریف شوند. طراحی خدمات باید در طراحی فرآیندها به مالک هر فرآیند کمک کند تا قالب استاندارد فرآیندها و یکپارچگی آن‌ها در تمامی حوزه‌های سازمان تضمین شود. خروجی تولیدشده توسط یک فرآیند باید با اصول و معیارهای عملیاتی منتج از اهداف کسب‌وکار تطابق داشته باشد. در صورت وجود این انطباق، اثربخشی فرآیند تأیید می‌گردد. اگر فعالیت‌های لازم، با استفاده از حداقل منابع انجام شود، آنگاه می‌توان فرآیند را کارآمد تلقی نمود. برای تحلیل فرآیند، نتایج و شاخص‌های آن باید در گزارش‌های منظم مدیریتی و بهبود فرآیند لحاظ شود (شارن، ۱۳۹۰).

فرآیندهای مرکز عملیات امنیت

تعداد فرآیندها و رویه‌ها برای یک مرکز عملیات امنیت متناسب با زاویه دید و بر اساس موارد زیر تعیین می‌شود:

- تعداد سرویس‌های قابل ارائه
 - تعداد مشتریانی که قرار است پشتیبانی شوند
 - تعداد و تنوع فناوری‌های بکار گرفته شده
- برای ایجاد کردن یک مرکز عملیات امنیت گسترده، ممکن است ده‌ها و یا حتی صدها فرآیند داشته باشیم. حداقل فرآیندها و رویه‌های پایه‌ای که برای نگهداری یک مرکز عملیات امنیت بکار می‌رود به شرح زیر است:

- فرآیند مانیتورینگ
 - فرآیندهای اطلاع‌رسانی
 - فرآیند سرویس‌دهی روزانه مرکز
 - رویه‌های نوبت‌بندی
 - فرآیندهای لاگ‌گیری از رخدادها
 - رویه‌های تولید گزارش‌ها
 - رویه‌های ایجاد داشبورد
 - رویه‌های رسیدگی به رخداد
- تعدادی از رویه‌ها بر پایه نوع فناوری به‌کارگیری شده در مرکز سفارش‌سازی می‌شوند. برای مثال فرآیند مانیتورینگ برای سامانه مدیریت اطلاعات و رخدادهای امنیتی مک آفی بسیار متفاوت خواهد بود با فرآیند مانیتورینگ در سایر محصولات تولیدکنندگان دیگر اگرچه بسیاری از ویژگی‌های این سامانه‌ها مشترک می‌باشد^۱.
- کارکنان مرکز عملیات امنیت کارمند یابی برای یک مرکز می‌تواند خیلی مشکل باشند. در این زمینه دو سؤال ویژه مطرح است:

- چه تعداد کارمند موردنیاز است؟
- چه مهارت‌هایی موردنیاز است؟

¹. White Paper Creating and Maintaining a SOC Copyright © 2013 McAfee

تعداد کارمندان بستگی دارد به میزان ساعت کاری مرکز. اگر ساعت کاری مرکز ۷*۲۴ باشد نه تنها باید نوبت را در نظر گرفت بلکه برای تعطیلات هم فکر کرد^۱.

فرآیندهای مدیریت پروژه

این فرآیندها در پنج گروه به شرح زیر تحت عنوان گروه‌های فرآیندی مدیریت پروژه تقسیم‌بندی می‌شوند:

- گروه فرآیندی آغازین^۲: فرآیندهایی که در راستای تعریف یک پروژه جدید یا یک فاز جدید از یک پروژه موجود انجام می‌شود.
- گروه فرآیندی برنامه‌ریزی^۳: فرآیندهای موردنیاز جهت تدوین محدوده‌ی پروژه، اصلاح اهداف و تعریف اقدامات لازم برای دستیابی به اهداف پروژه
- گروه فرآیندی اجرا^۴: فرآیندهایی که در راستای تکمیل کار تعریف‌شده در برنامه‌ی مدیریت پروژه برای تأمین مشخصه‌های پروژه انجام می‌شوند.
- گروه فرآیندی نظارت و کنترل^۵: فرآیندهایی که برای پیگیری، بازنگری و کنترل پیشرفت و عملکرد پروژه موردنیازند.
- گروه فرآیندی خاتمه^۶: فرآیندهایی که جهت پایان دادن همه فعالیت‌ها در کلیه گروه‌های فرآیندی انجام‌شده و به پروژه یا فاز خاتمه دهند (حمیدی فر، ۱۳۸۹).

حوزه‌های دانش مدیریت پروژه

- استاندارد پم باک، ۹ حوزه دانشی به شرح زیر برای مدیریت مؤثر پروژه معرفی نموده است:
- مدیریت یکپارچگی پروژه^۷: مجموعه فرآیندها و فعالیت‌های موردنیاز برای شناسایی، تعریف، ترکیب، جمع‌آوری و هماهنگی کلیه فرآیندها و فعالیت‌های مدیریت پروژه، درون گروه‌های فرآیندی می‌باشد. این حوزه دارای ۶ فرآیند است.
 - مدیریت محدوده پروژه^۸: شامل فرآیندهای موردنیاز جهت اطمینان از اینکه پروژه فقط شامل کارهای موردنیاز برای تکمیل پروژه است. این حوزه دارای ۵ فرآیند است.

¹. White Paper Creating and Maintaining a SOC Copyright © 2013 McAfee

². Initiating Process Group

³. Planning Process Group

⁴. Executing Process Group

⁵. Monitoring Process Group

⁶. Closing Process Group

⁷. Project Integration Management

⁸. Project Scope Management

- مدیریت زمان پروژه^۱: شامل فرایندهای موردنیاز برای مدیریت تکمیل به موقع فعالیت‌های پروژه است و شامل ۶ فرآیند است.
- مدیریت هزینه پروژه^۲: شامل فرایندهای مرتبط با تخمین، بودجه‌بندی و کنترل هزینه‌ها است تا پروژه بتواند مصوب و تکمیل شود. این حوزه دارای ۳ فرآیند است.
- مدیریت کیفیت پروژه^۳: شامل فرایندهای و فعالیت‌هایی در سازمان اجرایی پروژه می‌باشد که مشخص‌کننده مسئولیت‌ها، اهداف و سیاست‌های کیفی هستند که رد جهت تأمین نیازهایی که پروژه آن‌ها را برعهده گرفته است، قرار دارند. این حوزه دارای ۳ فرآیند است.
- مدیریت منابع انسانی پروژه^۴: شامل فرایندهای سازمان‌دهی، مدیریت و رهبری گروه پروژه می‌باشد و شامل ۴ فرآیند است.
- مدیریت ارتباطات پروژه^۵: شامل فرایندهای موردنیاز جهت اطمینان از این که اطلاعات پروژه به موقع و مناسب، تولید، جمع‌آوری، توزیع، ذخیره، بازیابی و درنهایت جمع‌بندی می‌شوند؛ و دارای ۵ فرآیند است.
- مدیریت مخاطره پروژه^۶: شامل فرایندهای برنامه‌ریزی، شناسایی، تحلیل، برنامه‌ریزی پاسخ و نظارت و کنترل ریسک پروژه می‌باشد؛ و دارای ۶ فرآیند است.
- مدیریت تأمین پروژه^۷: شامل فرایندهای خرید یا دریافت محصولات، خدمات یا نتایج موردنیاز از خارج از تیم پروژه بوده و شامل ۴ فرآیند است.

مدیریت تداوم فعالیت^۸

فرآیند مدیریت استمرار فعالیت شامل کاهش مخاطره تا یک سطح قابل قبول است و برنامه‌ریزی برای بازیابی فرایندهای فعالیت در صورتی که یک اختلال برای فعالیت رخ دهد. این مدیریت به سازمان امکان می‌دهد که مخاطره‌هایش را شناسایی و ارزیابی کرده و از این رو آن را قادر می‌سازد که درک بهتری از محیطی که در آن عمل می‌کند داشته باشد و تصمیم بگیرد که می‌خواهد با کدام خطر مقابله کند (شارن، ۱۳۹۱).

1. Project Time Management
 2. Project Cost Management
 3. Project Quality Management
 4. Project Human Resource Management
 5. Project Communication Management
 6. Project Risk Management
 7. Project Procurement Management
 8. BCM: Business continuity Management

مدیریت دانش

دانش مخلوط سیالی از تجربیات، ارزش‌ها، اطلاعات موجود و نگرش‌های کارشناسی نظام‌یافته است که چارچوبی برای ارزشیابی و بهره‌گیری از تجربیات و اطلاعات جدید به دست می‌دهد. دانش، در ذهن دانشور به وجود آمده و به کار می‌رود. دانش در سازمان‌ها نه تنها در مدارک و ذخایر دانش، بلکه در رویه‌های کاری، فرآیندهای سازمانی، اعمال و هنجارها مجسم می‌شود. این تعریف، از اول مشخص می‌کند که دانش ساده و روشن نیست، مخلوطی از چند عامل متفاوت است؛ سیالی است که درعین حال ساختارهای مشخصی دارد و نهایت اینکه، ابهامی و شهودی است و به همین علت، به راحتی نمی‌توان آن را در قالب کلمات گنجانده و به صورت تعریفی منطقی عرضه کرد. دانش در خود مردم وجود دارد و بخشی از پیچیدگی ندانسته‌های انسانی است. ما گرچه به‌طور سنتی، سرمایه‌ها را مشخص و ملموس می‌دانیم، اما سرمایه‌ی دانش را نمی‌توان به راحتی تعریف کرد. درست مشابه ذره اتمی که می‌تواند موج یا ذره باشد، بسته به اینکه دانشمندان چگونه وجود آن را دنبال کنند. دانش به شکل‌های پویا و نیز انباشته و ایستا قابل تصور است (دانپورت و پروساک، دانش، ۱۳۷۹).

دانش از اطلاعات و اطلاعات از داده‌ها ریشه می‌گیرند. تبدیل اطلاعات به دانش در عمل برعهده خود بشر است. با نگرش فراتری به این موضوع، آشکار می‌شود که معمولاً «دانش پایه» عامل تمایز بین داده، اطلاعات و دانش است. این یکی از دلایلی است که در محیط و فضای متکی به دانش، برخی مؤسسات یا شرکت‌ها می‌توانند همچنان برتری‌های اقتصادی و رقابتی خود را حفظ کنند. «کوهن» و «لونیتال» در مباحث خود، این حقیقت را تشریح می‌کنند که گسترش دانش منوط به شور و هیجان یادگیری و دانش پیشین است؛ به عبارت دیگر، دانش اندوخته شده عامل مؤثری در افزایش واکنش و فراگیری سهل‌تر مفاهیم است؛ بنابراین، دانش ترکیب سازمان‌یافته‌ای است از «داده‌ها» که از طریق قوانین، فرآیندها و عملکردها و تجربه حاصل آمده است؛ به عبارت دیگر، «دانش» معنا و مفهومی است که از فکر پدید آمده است و بدون آن اطلاعات و داده تلقی می‌شود. تنها از طریق این مفهوم است که «اطلاعات» حیات یافته و به دانش تبدیل می‌شوند (Wesley & Leviathan، 1990).

مدیریت دانش، مدیریت صریح و سامان‌مند دانش حیاتی و فرآیندهای مربوط به ایجاد، سازمان‌دهی، انتشار و استفاده و اکتشاف دانش است (Wickramasinghe, & Lubitz، 2007). مدیریت دانش، شامل همه‌ی روش‌هایی است که سازمان، دارایی‌های دانش خود را اداره می‌کند که شامل چگونگی جمع‌آوری، ذخیره‌سازی، انتقال، به‌کارگیری، به‌روز سازی و ایجاد دانش است (Grover, R & Madhavm. R.، 1998).

مدیریت دانش در بهبود مستمر خدمات، نقش کلیدی بازی می‌کند. در هر مرحله از چرخه حیات خدمت، داده‌ها باید تحصیل دانش به تسخیر درآیند و ادراک موجود در خصوص آنچه در واقع اتفاق می‌افتد، خرد را ایجاد می‌نماید. این‌ها اغلب به صورت مدل: داده، اطلاعات، دانش و خرد^۱ نشان داده می‌شوند. با توجه به مطالب عنوان‌شده در ادبیات تحقیق، می‌توان بیان نمود که مرکز عملیات امنیت یک مجموعه کاملاً مکانیزه و پیشرفته است که جهت ارائه ۲۴ ساعته خدمات طراحی می‌شود. یک مرکز عملیات امنیت باید بتواند بدون وقفه سرویس‌های اصلی و حیاتی خود را ارائه داده و گزارش‌های خود را در قالب‌های گوناگون و بر اساس ویژگی‌هایی مانند پایش امنیت جهت مدیریت مخاطره، تحلیل مخاطره، مانیتورینگ و ... ارائه نماید. استقرار رویکرد فرآیند محوری در این مرکز الزامی بوده و تدوین سلسله‌مراتب فرآیندی در راستای طراحی فرآیند کلی مرکز و با نگاه به چارچوب‌های طبقه‌بندی فرآیندها و سایر چارچوب‌ها و استانداردهای مرتبط با موضوع صورت می‌پذیرد.

تجزیه و تحلیل یافته‌ها

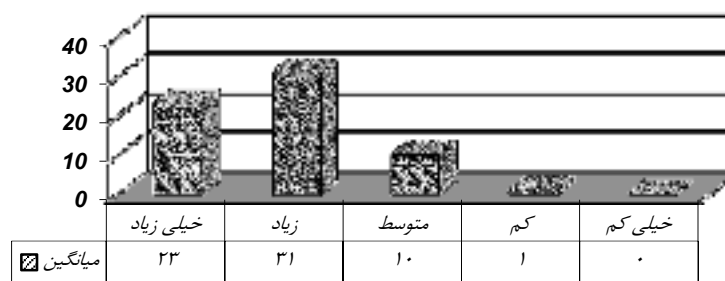
در خصوص هدف پژوهش ۱۲ سؤال بین جامعه نمونه مطرح گردید که به منظور تجزیه و تحلیل و مشخص ساختن اطلاعات به دست آمده، میانگین و واریانس پاسخ‌های پرسش‌شوندگان به سؤال‌های مطرح‌شده به شرح جداول زیر می‌باشد:

جدول (۱) نظر پاسخ‌دهندگان به سؤال‌های مطرح شده

ردیف	مؤلفه	به نظر شما در طراحی فرایندهای مدیریتی مرکز عملیات امنیت تأثیر شاخص زیر به چه میزان می‌باشد						
		خیلی زیاد	زیاد	متوسط	کم	خیلی کم	جمع	میانگین
۱	مدیریت پروژه	۲۴	۳۱	۹	۰	۱	۲۷۲	۴,۱۸
۲		۲۵	۲۸	۱۱	۰	۱	۲۷۱	۴,۱۶
۳		۱۷	۲۹	۱۶	۲	۱	۲۵۴	۳,۹
۴		۲۵	۳۰	۸	۲	۰	۲۷۳	۴,۲
۵	مدیریت دانش	۱۸	۳۴	۱۲	۰	۱	۲۶۳	۴,۰۴
۶		۲۴	۳۵	۵	۱	۰	۲۷۷	۴,۲۶
۷		۳۱	۲۳	۱۰	۱	۰	۲۷۹	۴,۲۹

^۱. DIKW: Data, Information, Knowledge and Wisdom

۴,۳۲	۲۸۱	۶۵	۰	۰	۷	۳۰	۲۸	ایجاد و به‌روزرسانی بانک اطلاعات آسیب‌پذیری‌های شبکه و سامانه‌ها و سیاست‌های امنیتی تعریف شده	تداوم فعالیت:	۸
۴,۲۸	۲۷۸	۶۵	۰	۰	۶	۳۵	۲۴	فرآیند جریان کاری مرکز		۹
۴,۲	۲۷۳	۶۵	۰	۱	۶	۳۷	۲۱	برنامه‌ریزی برای بازیابی فرآیندهای فعالیت‌ها، در صورت بروز اختلال		۱۰
۴,۱۵	۲۷۰	۶۵	۰	۱	۱۰	۳۲	۲۲	شناسایی دارایی‌های سازمان در ابر ترکیبی و تحلیل و ارزیابی ریسک‌های آن		۱۱
۳,۹۸	۲۵۹	۶۵	۰	۰	۱۶	۳۴	۱۵	پیاده‌سازی و نگهداری کنترل‌ها و سامانه‌های حفاظت فیزیکی شامل: اعلام و اطفای حریق، و ... CCTV برق اضطراری، اکسس کنترل،		۱۲
۴,۱۶	۲۷۱	۶۵	۰	۱	۱۰	۳۱	۲۳	میانگین		



نمودار (۱) نظر پاسخ‌دهندگان به سؤال‌های مطرح شده

واریانس:

$$\sigma^2 = \frac{\sum_{i=1}^N f_i (x_i - \bar{x})^2}{n - 1} = 0.55$$

جدول (۲) تجزیه و تحلیل آمیخته داده‌های به دست آمده

اسناد و مدارک	مصاحبه‌ها	آمیخته
<p>برای مدیریت صحیح پروژه طراحی و راه‌اندازی مرکز عملیات امنیت، توجه به ابعاد مختلف آن اهمیت دارد. ابعادی نظیر مدیریت یکپارچگی پروژه، مدیریت محدوده پروژه، مدیریت زمان پروژه، مدیریت هزینه پروژه، مدیریت کیفیت پروژه، مدیریت منابع انسانی پروژه، مدیریت ارتباطات پروژه، مدیریت مخاطره پروژه و مدیریت تأمین پروژه</p>	<p>این فرآیندها باید به‌گونه‌ای طراحی شوند که موارد قبل، هنگام و بعد از ایجاد و راه‌اندازی مرکز به لحاظ مختلف از جمله موارد اعتباری، تأمین و تدارکات، منابع انسانی، امنیت، کیفیت و ... به صلاح و صرفه باشد.</p> <p>هدف از این فرایندها به نظر به عملکرد صحیح و مدیریت‌شده مرکز در راستای اجرای وظایف و مأموریت‌های تعیین‌شده‌اش می‌باشد.</p> <p>فرآیندهای مدیریتی به دنبال به‌کارگیری حداقل منابع جهت کسب حداکثر نتیجه می‌باشد و در این راستا باید به‌گونه‌ای برنامه‌ریزی صورت پذیرد که پروژه اجرایی با داشتن منابع دانشی مناسب در زمان مشخص‌شده پاسخگوی نیازهای سازمان باشد.</p>	<p>با نگرش به اسناد و مدارک بررسی شده و نظر صاحب‌نظران و همچنین بررسی پرسش‌نامه‌های توزیع شده در بین جامعه نمونه به نظر می‌رسد برای طراحی فرآیندهای مدیریتی مرکز عملیات امنیت ابر ترکیبی ن.م بایستی راه‌اندازی این مرکز را به‌عنوان ایجاد یک خدمت فناوری اطلاعات در نظر گرفته و فرآیندهای مدیریت پروژه، تداوم فعالیت و مدیریت دانش را برای این امر تدوین نمود. توجه به شاخص‌های زیر برای طراحی فرایندهای یاد شده راهگشا خواهد بود:</p> <p>مدیریت امنیت اطلاعات پروژه</p> <p>هزینه پروژه و ارائه چارت زمانی و هزینه‌ای</p> <p>منابع انسانی پروژه و ارائه چارت سازمانی</p> <p>یکپارچه‌سازی محدوده پروژه</p> <p>ایجاد و به‌روزرسانی بانک اطلاعات آسیب‌پذیری‌های شبکه و سامانه‌ها و سیاست‌های امنیتی تعریف‌شده</p> <p>به‌روزرسانی بانک اطلاعات قوانین و روال‌های تشخیص و تحلیل تهدیدها</p> <p>تأمین دانش موردنیاز برای همبسته‌سازی هشدارها و شناسایی تهدیدها</p> <p>تسهیم دانش</p> <p>فرآیند جریان کاری مرکز</p> <p>برنامه‌ریزی برای بازیابی فرایندهای فعالیت‌ها، در صورت بروز اختلال</p> <p>شناسایی دارایی‌های سازمان در ابر ترکیبی و تحلیل و ارزیابی ریسک‌های آن</p> <p>پیاده‌سازی و نگهداری کنترل‌ها و سامانه‌های حفاظت فیزیکی شامل: اعلام و اطفای حریق، برق اضطراری، اکسس کنترل و ...</p>

نتیجه‌گیری و پیشنهادها

تجزیه و تحلیل توصیفی که از سؤالات پرسشنامه در خصوص مؤلفه مدیریت پروژه به دست آمده، مؤید این واقعیت است که ۹۸٪ افراد جامعه نمونه میزان تأثیر مؤلفه مدیریت پروژه را در سطح متوسط به بالا و مورد تأیید می‌دانند و در ضمن چون میانگین این مؤلفه ۴/۲۹۵ است، تأثیر آن به میزان زیاد به بالا است. در تجزیه و تحلیل توصیفی که از سؤالات پرسشنامه در خصوص مؤلفه تداوم فعالیت به دست آمده مؤید این واقعیت است که ۹۵٫۷٪ افراد جامعه نمونه میزان تأثیر مؤلفه تداوم فعالیت را در سطح متوسط به بالا و مورد تأیید می‌دانند و در ضمن چون میانگین این مؤلفه ۴/۰۱۹ است، تأثیر آن زیاد به بالا است. در تجزیه و تحلیل توصیفی که از سؤالات پرسشنامه در خصوص مؤلفه مدیریت دانش به دست آمده، مؤید این واقعیت است که ۹۲/۵٪ افراد جامعه نمونه میزان تأثیر مؤلفه مدیریت دانش را در سطح متوسط به بالا و

مورد تأیید می‌دانند و در ضمن چون میانگین این مؤلفه ۳/۸۶۶ است، تأثیر آن بین متوسط و زیاد است. با توجه به تجزیه و تحلیل کمی و کیفی اسناد و مدارک، مصاحبه‌ها و پرسش‌نامه، می‌توان نتیجه گرفت که فرآیندهای مدیریتی به دنبال به‌کارگیری حداقل منابع، جهت کسب حداکثر نتیجه می‌باشد و در این راستا باید به‌گونه‌ای برنامه‌ریزی صورت پذیرد که پروژه اجرایی با داشتن منابع دانشی مناسب در زمان مشخص شده پاسخگوی نیازهای سازمان باشد. از فرآیندهای این حوزه می‌توان به مدیریت پروژه، مدیریت دانش یا به‌طور ویژه فرآیندهای مرتبط با تداوم فعالیت اشاره کرد. اگرچه استانداردهای موجود می‌توانند به‌عنوان تجارب قبلی به‌عنوان اساس و مبنای کار قرار گیرند اما باید در این حوزه استانداردسازی شود و به بومی‌سازی نیاز است. در فرآیندهای مدیریتی باید برنامه‌ریزی مشخص و مدونی جهت انجام امور زیر صورت پذیرد:

- شروع و پایان پروژه و تعیین محدوده پروژه
 - تقسیم منابع و توزیع آن‌ها (کسب و در اختیار قرار دادن منابع هر بخش از حوزه‌های کاری مرکز عملیات امنیت ابر ترکیبی)
 - تامین دانش موردنیاز و بهره‌برداری از پایگاه‌های داده دانشی و قرار دادن آن‌ها در چرخه فرآیند
 - برقراری یک خط کنترلی جهت ارتقای کیفیت و حذف خطاها
 - مدیریت امنیت مرکز عملیات امنیت
 - همچنین برای تداوم فعالیت مرکز نیز چند نکته اساسی را باید رعایت نمود:
 - پشتیبانی مستمر و با کیفیت برای تضمین تداوم کار و امیدبخشی
 - تهیه نقشه راه برای هر کار یا فرآیندی که قرار است اعمال شود
 - وجود نیروی انسانی متخصص و مجرب و آموزش‌دیده
 - تعیین نمودن نحوه اجرای کار برای رسیدن به هدف
- فعالیت‌ها و عواملی که در بالا به برخی از آن‌ها اشاره شد، از جمله عوامل تأثیرگذار بر فرآیند کلی مرکز عملیات امنیت هستند که در حوزه فرآیندهای مدیریتی شناسایی شده‌اند؛ و میزان تأثیر این موارد در بررسی انجام شده مشخص گردید.

منابع

- آشنایی با فرآیندگرایی و مدیریت فرآیند در سازمان، وزارت بهداشت، درمان و آموزش پزشکی مرکز مدیریت آمار و فناوری اطلاعات، زمستان ۱۳۸۷
- تامس دانپورت ولارنس پروساک، مدیریت دانش، ترجمه حسین رحمان سرشت، نشر ساپکو، ۱۳۷۹
- تمتاجی، مصطفی، ارائه معماری مرجع امنیتی محیط رایانش ابر خصوصی سازمان، فصلنامه علمی - پژوهشی امنیت پژوهی، شماره ۴۷ پائیز ۱۳۹۳
- جنگجو، مهرداد، عبدالمهدی، علی، پور حسینی، سید ابوالحسن، مصطفایی، علی، مرکز عملیات امنیت (SOC)، انتشارات مهرگان قلم، ۱۳۹۴
- چارچوب طبقه‌بندی فرآیندها، مرکز بهره‌وری و کیفیت آمریکا، مترجمان جعفری، سید مهرداد، عباس نژاد، ندا، قالیبافی، مهدی، صادق زاده، اعظم، انتشارات سپید برگ، ۱۳۹۳
- حمیدی‌فر، حسین، راهنمای کاربردی سامانه‌های اطلاعات پروژه، ناشر نویسنده، چاپ اول، زمستان ۸۹
- شارن، تیلر، مترجم رکوعی، ایمان، مدیریت خدمات فناوری اطلاعات بهبود مستمر خدمات، ناشر موسسه آموزشی تحقیقاتی صنایع دفاعی، چاپ اول، ۱۳۹۱
- شارن، تیلر، مترجم منزوی، طاهره، مدیریت خدمات فناوری اطلاعات طراحی خدمات، ناشر موسسه آموزشی تحقیقاتی صنایع دفاعی، چاپ اول، زمستان ۱۳۹۰
- خوش دهان، علی، مدیریت مبتنی بر فرآیندها، انتشارات مرکز آموزش و تحقیقات صنعتی ایران، ۱۳۹۰
- مردانی، محمد، پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات، ناشر قرارگاه سازندگی خاتم‌الانبیاء (ص)، تهران، چاپ اول، ۱۳۹۴
- Cohen, Wesley & Leviathan. 1990. Absorptive Capacity: A New Perspective on Learning and Innovation. Administrative Science Quarterly, vol.35: 128-152
- Nilmini Wickramasinghe, & Dag von Lubitz (2007). Knowledge-based Enterprise: Theories and Fundamentals. Idea Group Publishing
- Madhavi. R. and Grover. R. 1998. From Embedded Knowledge to Embodied Knowledge: New Product Development as Knowledge Management. Journal of Marketing, 62(4): 1-12
- Madhavi. R. and Grover. R. 1998. From Embedded Knowledge to Embodied Knowledge: New Product Development as Knowledge Management. Journal of Marketing,
- Nilmini Wickramasinghe, & Dag von Lubitz (2007). Knowledge-based Enterprise: Theories and Fundamentals. Idea Group Publishing
- White Paper Creating and Maintaining a SOC Copyright © 2013 McAfee

- Creating and Maintaining a SOC The details behind successful security operations centers Copyright © 2013 McAfee, Inc. 60059wp_creating-soc_0613B_ETMG