ارایه متدولوژی SUPبر اساس استاندارد ISO 27001
و
متدولوژی RUP
در جهت استقرار حاکمیت فناوری اطلاعات درسازمان هوافضا

علیرضا منیری ابیانه
علی‌محمد احمدوند
مهدی الیاسی
اسد محمدی

تاریخ دریافت: ۹۰/۱۲/۱۶
تاریخ پذیرش: ۹۱/۲/۲۸

چکیده:

فناوری اطلاعات و ارتباطات، از جمله مهمترین فناوری‌هایی است که در شکل‌گیری و ایجاد توانمندی‌های مختلف دفاعی بروز شده سازمان هوافضا، تاثیرگذار است. سازمان هوافضا بعنوان یک مجموعه راهبردی در بخش دفاعی کشور، بواسطه اتخاذ راهبردهای محصولی با توجه به راهبردهای عملیاتی اتخاذ شده در دکترین دفاعی مجموعه وزارت، نیازمند یک سیستم دقیق و منظم برای راهبری و کنترل اثربخش فناوری، خصوصا فناوری اطلاعات می‌باشد. بر این اساس هماهنگی و همسویی فناوری اطلاعات در تمامی ابعاد با سازمان، جزء مهمترین مسئله برای اثربخشی این حوزه می‌باشد. طی بررسی تیم خبرگان دو حوزه، یکی از مهمترین چالش‌ها در سازمان‌های نظامی مقوله امنیت اطلاعات در حوزه فناوری اطلاعات و حوزه کسب و کار می‌باشد. نگاه تک‌بعدی به امنیت در یکی از این حوزه‌ها باعث به جا ماندن ریسک‌های بالقوه در حوزه دیگر خواهد بود. در این مقاله ضمن معرفی مفاهیم پایه همسویی، ایزو ۲۷۰۰۱ به عنوان یکی از رهیافت‌های حاکمیتی در جهت همسویی و آر.یو.پی به عنوان یکی از قدرتمندترین متدولوژی‌های تولید و طراحی سیستم‌های اطلاعاتی معرفی شده است. به لحاظ راهبردی کردن اجرای یک سیستم دقیق مدیریتی در خصوص امنیت و برطرف‌کردن یکی از بزرگترین موانع همسویی در سازمان هوافضا، در دو حوزه فناوری اطلاعات و کسب و کار، یک متدولوژی کاملا بومی با عنوان فرآیندهای یکپارچه امنیت ارائه شده است. این متدولوژی بر پایه یکی از اصلی‌ترین رهیافت‌های حاکمیت فناوری اطلاعات(ایزو۲۷۰۰۱)، و متدولوژی تولید و طراحی سیستم‌های اطلاعاتی شرکت آی.بی.ام بنا شده است. تلفیق روش حاکمیتی ذکر شده و متدولوژی آر.یو.پی باعث گردیده است تا بتوان به یک متدولوژی کاملا راهبردی در حوزه مدیریت امنیت فناوری اطلاعات و کسب و کار رسید.

واژه های کلیدی:

همسویی راهبردی، حاکمیت فناوری اطلاعات، استاندارد ایزو ۱۰۰۷۲، متدولوژی، فرآیندهای یکپارچه رشنال. اس.یو.پی.

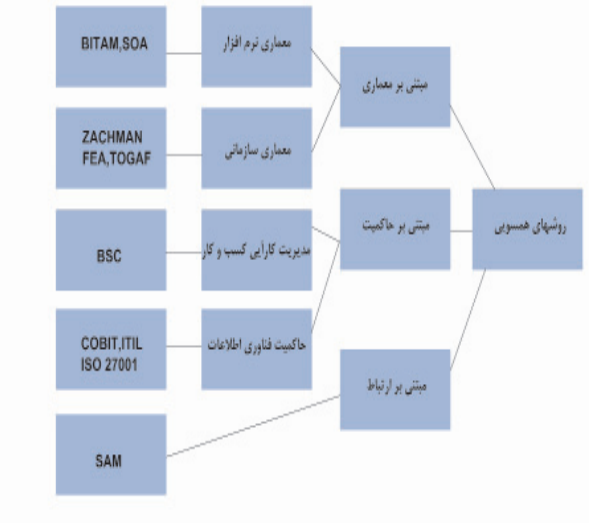
۱- مقدمه

در محیط پرتلاطم و رو به رشد امروزی، جهت موفقیت و پیشرفت سازمان‌ها باید تمامی بخش‌های سازمان با اهداف و مسیر راهبردی کسب وکار آن سازمان همسو گردند. با توجه به نفوذ عمیق فناوری اطلاعات در حوزه‌های مختلف کسب و کار و لایه‌های مختلف سازمان، واحد فناوری اطلاعات در بین سایر واحدهای سازمان و همچنین از بعد همسویی راهبردهای مربوطه با راهبرد کسب وکار از

اهمیت ویژه‌ای برخوردار می‌باشد.

همسویی راهبردی فناوری اطلاعات و کسب وکار، مفهومی است که از سال ۱۹۷۰ مطرح گردیده است و درطی سالیان متمادی و همچنین در حال حاضر بعنوان یکی از دغدغه‌های اصلی مدیران فاوا و مدیران ارشد سازمان‌ها می‌باشد.[۲] به عبارتی دیگر همسویی راهبردی فناوری اطلاعات به سازمان‌ها امکان می‌دهد اثربخشی توانمندی‌ها و قابلیت‌های مورد نیاز فناوری اطلاعات، جهت انجام و رسیدن به اهداف سازمانی را تعریف و تعیین کنند. براساس تحقیقات صورت گرفته تاکنون رهیافت‌های همسویی در سه دسته کلی تقسیم‌بندی شده‌اند که در شکل ۱-۱ به آن اشاره گردیده است.

حاکمیت فناوری به عنوان یکی از مطرح‌ترین رهیافت‌های همسویی راهبردی می‌باشد که در این خصوص از استانداردهایی مبتنی بر تکنیک‌های فناوری و اصول مدیریت بنا گردیده است. همچنین به لحاظ حساسیت امنیت اطلاعات در سازمان این مقوله به عنوان یکی از مهمترین مباحث در حوزه زیرساخت فناوری اطلاعات و همچنین سایر حوزه‌های اطلاعاتی مطرح بوده است. از اینرو، در این مقاله سعی در ارایه یک مدل بومی در خصوص استاندارد ایزو ۲۷۰۰۱ بر پایه متدولوژی آر.یو.پی بوده است.



(شکل ۱-۱): رهیافت‌های همسویی[۱]

۲- حاکمیت فناوری اطلاعات

امروزه راهبری فناوری اطلاعات و ارتباطات از ابعاد مختلف در سازمان از اهمیت بسزایی برخوردار می‌باشد و در این خصوص سازمان‌ها سعی دارند قوانین و مسئولیت‌ها در این حوزه را شفاف‌سازی نمایند. به عبارتی دیگر، سازمان‌ها سعی در برقراری حاکمیت در این حوزه مانند حوزه مالی، منابع انسانی و سایر حوزه‌های تعریف شده یا جاافتاده را دارند. به عنوان یک تعریف کلی، حاکمیت فناوری اطلاعات، مسئولیت‌ها و اختیارات تصمیم‌گیری را برای تعیین رفتار مطلوب در کاربری فناوری اطلاعات مشخص می‌سازد. مطابق با تعریفی دیگر، حاکمیت فناوری اطلاعات به عنوان یک سری قوانین و فرآیندهای کلان مدیریتی می‌باشد که بر پایه بهترین تجارب، کسب وکار را قادر می‌سازد تا کاربردهای فناوری اطلاعات در خصوص موارد ذیل را برای رسیدن به شفافیت در زمینه فناوری اطلاعات، هدایت نماید:[۳]

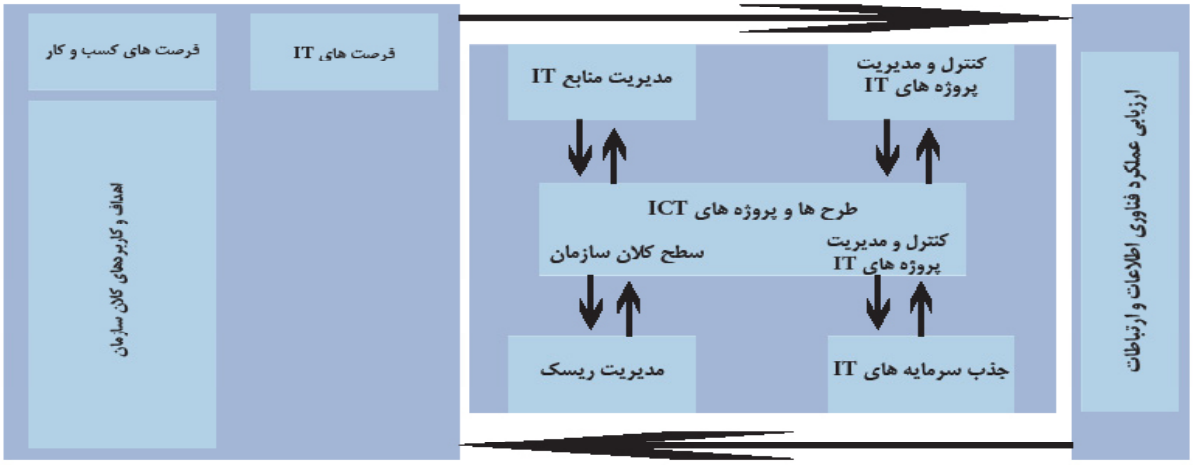
- پشتیبانی اهداف از طریق ایجاد ارزش برای کسب وکار
- افزایش کارایی و اثربخشی فناوری اطلاعات و جلب رضایت مشتریان
- توسعه راه‌حل‌ها و کاربردهای خاص فناوری اطلاعات
- ایجاد اطمینان از مدیریت ریسک‌های فناوری اطلاعات

۲-۱- فرآیندهای حاکمیت فناوری اطلاعات

فرآیندهای عمده حاکمیت فناوری اطلاعات از ابعاد مختلف در خصوص تعاریف ذکر شده موارد ذیل را شامل می‌شود:[۳]

- جهت‌دهی و هدایت راهبردی، مدیریت ریسک، جذب سرمایه‌گذاری، مدیریت پروژه و طرح‌ها، مدیریت منابع، ارزیابی عملکرد

بطور کلی فرآیندهای ذکر شده در سه دسته برنامه‌ریزی، اجرا و نظارت دسته‌بندی می‌گردند که در شکل ۲-۱ به آن اشاره گردیده است.



(شکل ۲-۱): فرآیندهای حاکمیت فناوری اطلاعات[۳]

۳- معرفی ایزو ۲۷۰۰۱

تا به امروز، برای پیشگیری از تهدیدهای امنیتی متدها و استانداردهای مختلفی ارایه شده است اما کامل ترین و معروف‌ترین آن‌ها استاندارد BS7799 می‌باشد. نام کامل این استاندارد British Standard17799 است که به زمان تاسیس موسسه Commercial Computer Security Center (CCSC) و بخش UK Department of Trade and Industry در سال ۱۹۸۷ برمی‌گردد.

CCSC در سال ۱۹۸۹ اقدام به انتشار کدهایی برای سنجش میزان امنیت کرد که به Users Code of Practice معروف شد. مدتی بعد کیفیت و کمیت این کدها از سوی مرکز محاسبات بین المللی NCC و یک کنسرسیوم از کاربران مورد بررسی قرار گرفت و در نهایت به صورت نخستین نسخه استاندارد امنیت با عنوان "مستندات راهبری PD 003" در انگلستان منتشر شد. نسخه بازنگری شده این استاندارد در سال ۱۹۹۵ با عنوان استاندارد ISO ثبت شد.

با توجه به تجارب گذشته این گروه، در گردآوری اسناد و قوانین و مستندات، استاندارد امنیتی BS7799 توسط این گروه منتشر گردید و در فوریه ۱۹۹۸ قسمت دوم این استاندارد با عنوان سیستم مدیریت امنیت اطلاعات یا Information Security Management System که در حال حاضر آن را به اختصار ISMS می‌نامند منتشر شد. استاندارد ISO/IEC 27001 و ISO/IEC 17799 جدیدترین ویرایش از سری استانداردهای امنیت اطلاعات می‌باشند. در این استانداردها کلیه نکات لازم برای پیاده‌سازی امنیت اطلاعات بیان شده است. البته ذکر این نکته نیز ضروری است که استاندارد ISO/IEC 27001 و ISO/IEC 17799 یک روش جامع و کامل برای کلیه سازمان‌ها با هر ماهیت کاری می‌باشد. بنابراین، بومی کردن آن متناسب با سازمان‌ها ضروری می‌باشد.[۴]

۳-۱- کنترل‌های استاندارد

این استاندارد حفاظت از اطلاعات را در سه مفهوم خاص، محرمانگی، صحت و در دسترس بودن اطلاعات تعریف می‌کند.

- Confidentiality تنها افراد مجاز به اطلاعات دسترسی خواهند یافت.
- Integrity کامل بودن و صحت اطلاعات و روش‌های پردازش اطلاعات مورد نظر هستند.
- Availability اطلاعات در صورت نیاز بطور صحیح در دسترس باید باشد.

با توجه به شکل ۱-۳ این استاندارد دارای یازده گروه کنترلی شامل خط مشی امنیتی، سازمان‌دهی امنیت

اطلاعات، مدیریت دارایی‌ها، امنیت منابع انسانی، امنیت فیزیکی و محیطی، مدیریت ارتباطات و عملیات، کنترل دسترسی، تهیه و توسعه سیستم‌های اطلاعاتی، مدیریت

(شکل ۱-۳): کنترل‌های امنیتی استاندارد[۷]

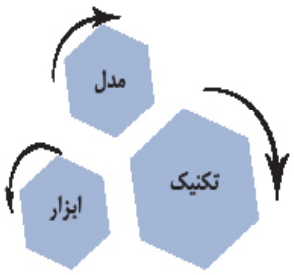
• مفاهیم مدل سازی که جهت ذخیره‌سازی اطلاعات برنامه و راه‌حل‌های آن نیاز است. بطور مثال متدولوژی‌های شی‌گراء از مفاهیمی چون شی، کلاس، توارث، تکنیک و غیره استفاده می‌کند.

• نمادها که مفاهیم مدل‌سازی را به منظور فهم افراد و امکان تغییر و اصلاح آن‌ها ارائه می‌دهند. اکثر اوقات نمادها بصورت گرافیکی نمایش داده می‌شوند. بطور مثال می‌توان به زبان مدل‌سازی یکپارچه اشاره کرد که دارای نمادها و نمودارهای مختلفی است، همچون نمودار فعالیت، کلاس و غیره.

• فرآیند توسعه که راهنمایی در جهت توسعه مدل‌ها می‌باشد. فرآیند توسعه بیان می‌کند که کدام مدل‌ها باید ساخته شوند و چگونه ساخته می‌شوند. به عنوان مثال می‌توان به فرآیند یکپارچه نرم‌افزار اشاره کرد.

• اشارات و ایماها که در طول فرآیند توسعه مورد استفاده قرار می‌گیرند. در حقیقت به راه‌حل‌های ساده‌ای که در جهت اجتناب از مشکلات استفاده می‌شوند، دلالت دارد.

بطور کل متدولوژی را متشکل از سه جزء مدل، تکنیک و ابزار بر می‌شمارند.



(شکل ۱-۴): اجزای اصلی یک متدولوژی

- معرفی متدولوژی آر.یو.پی

ر.یو.پی، متدولوژی ارایه شده توسط شرکت رشنال، کاربردترین فرآیند تولید و توسعه سیستم‌های نرم‌افزاری دنیای کنونی می‌باشد و به عنوان یک استاندارد صنعتی عمل در دنیای فناوری اطلاعات پذیرفته شده است. این ـولوژی برای انواع پروژه‌های نرم‌افزاری در دامنه‌های ختلف مانند سیستم‌های اطلاعاتی، سیستم‌های صنعتی، ستم‌های بلادرنگ، سیستم‌های تعبیه شده، ارتباطات راه دور، سیستم‌های نظامی و در اندازه‌های متفاوت از پروژه‌های بسیار کوچک تا پروژه‌های بسیار بزرگ کاربرد دارد.

یکی از مزایای قابل توجه این متدولوژی استفاده از روش تکرار در تولید و مدیریت تولید نرم‌افزار است که این امکان، تولید مبنی بر کاهش ریسک و مواجهه با مشکلات اصلی در ابتدای کار و در نتیجه احتمال موفقیت بیشتر را فراهم می‌کند. از محاسن دیگر این متدولوژی مبنا قرار دادن نرم‌افزار و تولید یک معماری پایدار در ابتدای کار است که در نتیجه امکان کشف مشکلات عمده، تست و مجتمع‌سازی ممتد را از ابتدای کار فراهم می‌کند و باعث ارتقای افراد تیم همزمان با پیشرفت پروژه و کیفیت فرآیند تولید می باشد.[۸]

۱-۵- اصول اساسی روش آر.یو.پی

- حمله سریع و مداوم به ریسک‌های اصلی
- تضمین تولید محصولی با ارزش به مشتری

- تمرکز روی محصول اصلی
- اعمال سریع تغییرات در پروژه
- تولید سیستم بصورت مولفه‌ای
- کارکردن به صورت گروهی
- توجه به کیفیت محصول به عنوان یک اصل

آر.یو.پی از یک روش تکراری استفاده می‌کند، در هر تکرار مقداری از نیازمندی‌ها و کار تحلیل، طراحی، پیاده‌سازی و تست انجام می‌شود. هر تکرار به منظور تولید یک برنامه قابل اجرا می باشد که یک گام به محصول نهایی نزدیک‌تر است و براساس نتایج تکرارهای قبلی ساخته می‌شود.[۲۱]

۲-۵- دلایل برتری روش تکراری بر روش آبشاری

- روش تکراری با نیازمندی‌های متغیر سازگار است.
- در روش تکراری، مجتمع‌سازی یک اتفاق بزرگ در آخر پروژه نیست.
- در روش تکراری، ریسک‌ها معمولا در مجتمع‌سازی‌های اولیه کشف می‌شوند.
- در روش تکراری با مدیریت می‌توان در محصول تغییرات تاکتیکی ایجاد کرد.
- در روش تکراری، استفاده مجدد آسان می‌شود.
- در روش تکراری، نقص‌ها در طی چندین تکرار کشف و تصحیح می‌شوند.
- در روش تکراری، از پرسنل پروژه بهتر استفاده می‌شود.
- در روش تکراری، اعضای تیم در ضمن انجام کار، مطالب جدیدی را فرا می‌گیرند.
- در روش تکراری، فرآیند تولید همراه با انجام کار، اصلاح شده و بهبود می‌یابد.[۹]

۳-۵- جنبه‌های سازمان‌دهی شده آر.یو.پی

جنبهٔ پویا (افقی) که چرخه‌ها، فازها، تکرارها و مراحل مهم را نشان می‌دهد.

جنبه ایستا (عمودی) فعالیت‌ها، دیسیپلین‌ها، خروجی‌ها و نقش‌ها را نشان می‌دهد.

۱-۳-۵- جنبه پویا

ساختار پویا با چرخه حیات و بعد زمان پروژه سر و کار دارد.

۲-۳-۵- جنبه ایستا

ساختار ایستا با عناصر فرآیند مانند فعالیت‌ها، دیسیپلین‌ها، خروجی‌ها و نقش‌ها بطور منطقی و بصورت دیسیپلین‌های اصلی فرآیند دسته بندی شده‌اند سر و کار دارد. یک فرآیند نشانگر این است که چه کسی، چه کاری را چگونه و در چه وقت انجام می‌دهد.

٦- ایجاد متدولوژی اس.یو.پی براساس استاندارد ایزو۲۷۰۰۱ و بر پایه متدولوژی آر.یو.پی

بی‌شک یکی از مباحث مهم سند جامع فنآوری اطلاعات و ارتباطات، طرح جامع امنیتی یک سازمان می‌باشد. امروزه بحث امنیت دیگر به عنوان یک بخش فرعی در فناوری اطلاعات و ارتباطات مطرح نمی‌باشد؛ بلکه امنیت به عنوان یک دانش جدید و یک شعبه اصلی برای فنآوری اطلاعات و ارتباطات محسوب می‌شود، لذا ضرورت دارد به این دانش به صورت عمیق‌تر و اساسی‌تر نگریسته شود. امنیت باید به چرخه حیات سازمان تزریق شود و به عنوان یک اصل جداناپذیر از چرخه حیات سازمان پذیرفته شود. با پذیرش این حقیقت، مهندسی امنیت در فناوری اطلاعات و ارتباطات شکل گرفته و در چرخه حیات سازمان صاحب جایگاه می‌شود.[۱۰]

به منظور ایجاد امنیت در سازمان‌ها روش‌های بسیاری وجود دارد، اما درتمامی این روش‌ها یک موضوع یکسان است و این موضوع آن است که همیشه باید وضعیت موجود را به یک وضعیت مطلوب و امن تبدیل کرد. برای این‌کار نیز باید وضعیت موجود به لحاظ نقاط ضعف، قوت، تهدیدها و فرصت‌ها شناسایی شود و با تحلیل این ریسک‌های بدست آمده یک وضعیت مطلوب معرفی و پیاده‌سازی گردد. با توجه به این‌که متدولوژی اجرای امنیت بسیار متفاوت می‌باشد، استانداردی در این زمینه تدوین شده است تا اسکلت و چارچوب امنیت را در تمامی سازمان‌ها یکسان کند.

فرآیند بومی کردن استاندارد ایزو۲۷۰۰۱ و متدولوژی آر.یو.پی در قالب طرحی به نام اس.یو.پی انجام پذیرفته که هدف از آن داشتن یک رویکرد و روشی برای مدیریت

همه جانبه امنیت اطلاعات و ارتباطات می‌باشد. این رویکرد دارای ویژگی‌های برجسته‌ایی مانند تکرار پذیری و افزایشی می‌باشد. اس.یو.پی یک فرآیند سازماندهی شده می‌باشد که نقش‌ها ، فعالیت‌ها ، دستاوردها و جریان‌های کار تعریف شده در آن، عناصر اصلی یک فرآیند (یعنی چه کسی ، چه کاری ، چگونه و چه موقع) را تعریف و تبیین می‌کند.

۶-۱- اس.یو.پی

اس.یو.پی یک فرآیند مهندسی امنیت ساختارمند است که به طور روشن و واضح مشخص می‌کند که چه کسی مسئول چه چیزی است و چگونه و چه موقع هر چیزی انجام شود. اس.یو.پی همچنین یک ساختار مناسب را برای چرخه حیات یک پروژه فراهم می‌کند که به طور روشن مراحل مهم و نقاط تصمیم‌گیری را بیان می‌کند و همچنین یک محصول فرآیندی است که چارچوب فرآیند با قابلیت سفارشی شدن را برای مهندسی امنیت فراهم می‌نماید.

پیکربندی اس.ی.پی را می‌توان برای پشتیبانی از تیم‌های کوچک و بزرگ انجام داد. محصول اس.یو.پی شامل چندین نوع پیکربندی فرآیند و نماهای مختلف از فرآیند می‌باشد که تحلیل‌گران، متخصصین امنیت، مدیران پروژه، مدیران پیکربندی و دیگر اعضاء تیم را در نحوه استقرار سیستم مدیریت امنیت اطلاعات هدایت می‌کند.

۶-۲- روش اس.یو.پی

هسته اس.یو.پی از چندین اصل اساسی تشکیل شده است که از استقرار تکراری پشتیبانی کرده و معرف ماهیت آن می‌باشد که در ذیل به آن اشاره گردیده است:

- شناسایی دارایی‌های سازمان بر اساس مکعب امنیتی
- حمله سریع و مدام به ریسک‌های اصلی
- تضمین می‌کند که استقرارISMS به نحو عالی انجام شده و سازمان قادر به ادامه اثربخش آن خواهد بود
- پیاده‌سازی به صورت مولفه‌ای خواهد بود
- در قالب یک تیم کار انجام می‌شود
- کیفیت را به عنوان یک اصل قرار می‌دهد نه یک فرع.

۶-۳- اس.یو.پی و تولید تکراری

اکثر تیم‌های امنیتی هنوز از فرآیند آبشاری برای پروژه‌های ISMS استفاده می‌کنند که در آن‌ها هر فاز را در یک مرحله کامل می‌کنند. در این توالی ابتدا شناخت مدل کسب و کار و شناخت دارایی‌ها انجام می‌شود و سپس شناسایی تهدیدات و مدیریت ریسک انجام می‌گردد. بعد از آن نیز پیاده‌سازی و تست انجام خواهد شد. چنین روشی اعضای کلیدی تیم را برای مدت طولانی بیکار می‌کند و تست را تا پایان چرخه حیات پروژه، یعنی زمانی که حل کردن مشکلات سخت و پرهزینه است و تهدیدهای جدی وجود دارد، به تاخیر می‌اندازد.

بر خلاف روش آبشاری، اس.یو.پی از یک روش تکراری استفاده می‌کند، یعنی یک توالی از گام‌های افزایشی یا تکرار ها وجود دارد. هر تکرار چنانچه در شکل ۱-۶مشاهده می‌کنید شامل تعداد زیادی دیسیپلین است (مدل کسب و کار، دارایی، سیاست امنیتی، پیاده سازی، مدیریت پیکربندی و تغییرات و مدیریت پروژه). هر تکرار مجموعه‌ای تعریف شده از اهداف است و بخشی از پیاده‌سازیISMS را تولید می‌کند. هر یک از این تکرارهای متوالی برای تکمیل و اصلاح سیستم تا زمان کامل شدن محصول نهایی، بر مبنای کار تکرارهای قبلی ساخته می‌شود.

(شکل ۱-۶): چرخه فرایند اس.یو.پی

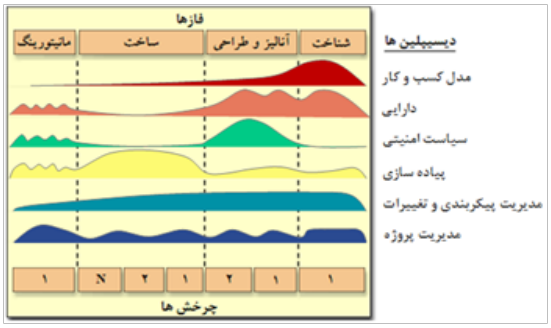
تکرارهای اولیه بر شناخت سازمان و دارایی‌هایش و تکرارهای بعدی بر تجزیه و تحلیل و طراحی (مدیریت ریسک)، نوشتن سیاست‌های امنیتی، پیاده‌سازی و پایش تاکید دارد.

1. Iterative
2. Incremental
3. Roles
4. Activities

٤-٦- اس.یو.پی یک فرآیند مهندسی ساختارمند

هسته اصلی اس.یو.پی دارای دو ساختار یا بعد مطابق شکل۲-۶ می باشد:

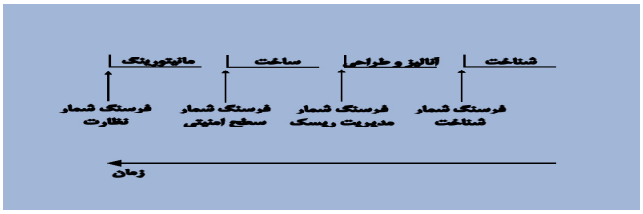
- ساختارپویا: بعد افقی، ساختار دینامیک یا بعد زمانی فرآیند را نشان می‌دهد. این ساختار نشان می‌دهد که فرآیند چگونه در قالب چرخه‌ها، فازها، تکرارها و مراحل مهم موجود در چرخه حیات یک پروژه بیان می‌شود.
- ساختار ا یستا: بعد عمودی، ساختار ایستای فرآیند را نشان می‌دهد. این ساختار توضیح می‌دهد که عناصر فرآیند (فعالیت‌ها، دیسیپلین‌ها، خروجی‌ها و نقش‌ها) چگونه به طور منطقی و به صورت دیسیپلین‌های اصلی فرآیند (یا جریان کارها) دسته‌بندی می‌شوند.



(شکل ۶-۲): معماری فرآیند اس.یو.پی

٥-٦- ساختار دینامیک اس.یو.پی

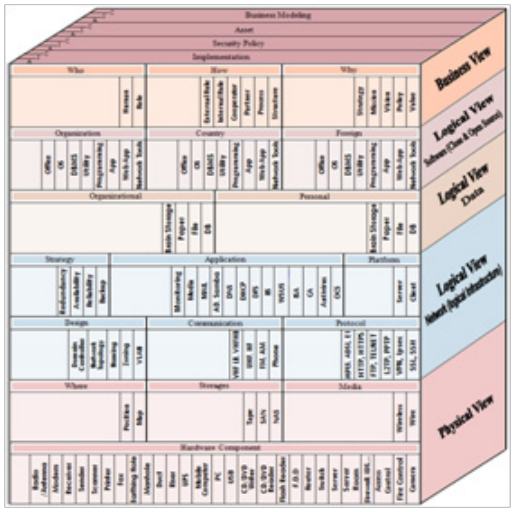
همان‌طور که در شکل ۳-۶ نشان داده شده است ساختار دینامیک با چرخه حیات و بعد زمانی سروکار دارد. اس.یو.پی، یک روش ساختاربندی شده برای تولید تکراری فراهم می‌کند که یک پروژه را به چهار فاز تقسیم می‌کند: شناخت، آنالیز و طراحی، ساخت و مانیتورینگ. هر فاز یک یا چند تکرار است که با تولید خروجی‌های تکنیکی لازم، در نهایت اهداف تجاری آن فاز را برآورده می‌سازد. تعداد تکرارها باید به اندازه مورد نیاز، برای رسیدن به اهداف فاز باشد، نه بیشتر. اگر اهدافی که در فاز طرح‌ریزی شده، مورد توجه قرار نگیرد، یک تکرار دیگر نیز باید به فاز اضافه شود که پروژه را به تاخیر می‌اندازد.



(شکل ۶-۳): ساختار دینامیک اس.یو.پی

فاز شناخت

شناخت سیستم در فاز اول انجام خواهد شد. مواردی که در این فاز مورد شناسایی قرار می گیرند به سه دید کلی دیدگاه کسب وکار، دیدگاه منطقی و دیدگاه فیزیکی با توجه به مکعب امنیتی شکل ۴-۶ تقسیم می شود:



(شکل۶-۴): ساختار دینامیک اس.یو.پی

فاز آنالیز و طراحی

بر اساس اطلاعات حاصل از اجرای مرحله قبل ریسک‌ها و مخاطرات مرتبط با دارایی‌های اطلاعاتی و فرآیندهای موجود در سطح سازمان شناسایی، تحلیل و دسته‌بندی(اولویت‌بندی) خواهند شد. آسیب‌پذیری‌های دارایی‌های اطلاعاتی و فرآیندهای عملیاتی منابع تولید ریسک بوده و لازم است تهدیدهای ناشی از هر یک از آسیب‌پذیری‌ها شناسایی و فهرست گردند. سپس هزینه‌های احتمالی ناشی از وجود هر تهدید محاسبه شده و با توجه به احتمال وقوع هر یک، شاخص‌های ریسک مربوط استخراج و نسبت به اولویت‌بندی و برنامه‌ریزی فرآیندهای ایمن‌سازی اقدام خواهد شد.

با توجه به سیاست‌های گذاشته شده در این مرحله معماری شبکه امن طراحی می‌شود. در این مرحله با توجه به سیاست گذاشته شده یک طرح جامع از شبکه ایجاد می‌شود. این مرحله شامل تجهیزات امنیتی و نحوه چیدمان آن‌ها در شبکه می‌شود.

فاز ساخت

در این مرحله با توجه به نتایج حاصل از تحلیل ریسک، مکانیزم‌های کنترلی لازم برای جلوگیری از ایجاد ریسک یا کاهش و حذف آن ارائه خواهد شد. مکانیزم‌ها بر اساس سند سیاست‌گذاری امنیتی تدوین شده، طبق استانداردهای مذکور ارایه خواهند گردید. مکانیزم‌های کنترلی این فاز در دو حوزه فنی و سازمانی طراحی خواهند شد. هزینه‌های خرید تجهیزات لازم برای اجرای مکانیزم‌ها به عهده کارفرما بوده و نصب و عملیاتی نمودن آن‌ها به عهده مجری می‌باشد.

طراحی و استقرار سیستم اجرایی و مدیریتی با هدف مدیریت یکپارچه امنیت اطلاعات یکی دیگر از مراحل اصلی این پروژه می‌باشد. در این مرحله معماری طراحی شده، پیاده‌سازی می‌شود. این مرحله شامل نصب و راه‌اندازی تجهیزات مختلف امنیتی در شبکه و تنظیم آن‌ها می‌شود.

فاز پایش

این مرحله بر اساس گردش کارهای منظم و از پیش تعریف‌شده‌ایی که در استاندارد اس.یو.پی وجود دارد به تست عملیات پیاده‌سازی و رفع نقایص می‌پردازد. فاز پایش به سه دیسیپلین دارایی، سیاست امنیتی و پیاده‌سازی توجه دارد.

٦-٦-ساختار ایستا اس.یو.پی

ساختار ایستا، با عناصر فرآیند (نقش‌ها، فعالیت‌ها، خروجی‌ها و دیسیپلین‌ها) که به طور منطقی و به صورت دیسیپلین‌های اصلی فرآیند دسته‌بندی شده‌اند، سروکار دارد. یک فرآیند توضیح می‌دهد که چه کسی، چه کاری را چگونه و چه وقت انجام می‌دهد. اس.یو.پی با استفاده از ۴ عنصر کلیدی مدل‌سازی که در جدول ۱-۵ به آن اشاره شده، نشان داده می‌شود.

Who	نقش‌ها – کار را چه کسی انجام می‌دهد
How	فعالیت‌ها – کار چگونه انجام می‌شود
What	خروجی‌ها – حاصل کار چه باید باشد
When	جریان‌های کار – کار در چه زمانی باید انجام شود

(جدول۱-۶): چهار عنصر کلیدی مدل‌سازی فرآیند

نقش‌ها

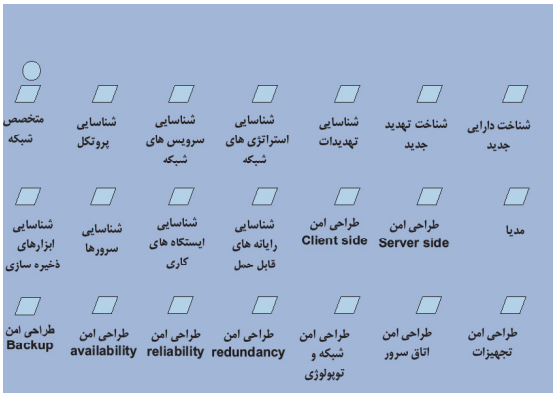
یک نقش مانند یک کلاه است که هر فرد (یا گروه) در طی یک پروژه بر سر می‌گذارد. یک فرد ممکن است کلاه‌های زیادی بر سر بگذارد. در اس.یو.پی، نقش‌ها به سادگی تعریف می‌کنند که افراد چگونه باید کار را انجام دهند و نیز مشخص می‌کند که فرد یا افرادی که آن نقش را ایفا می‌کنند چه توانایی‌ها و مسئولیت‌هایی باید داشته باشند. یک فرد معمولا یک یا چند نقش را انجام می‌دهد و چند نفر ممکن است یک نقش را انجام دهند.

در اس.یو.پی نقش‌های ذیل وجود دارد:

۱- تحلیل‌گر فرآیندهای کسب و کار
۲- تحلیل‌گر نیروی انسانی
۳- تکنیسین کامپیوتر
۴- متخصص شبکه
۵- متخصص امنیت شبکه
۶- متخصص طراح و معمار شبکه
۷- متخصص ارتباطات
۸- متخصص امنیت اطلاعات
۹- متخصص امنیت فیزیکی
۱۰- متخصص نرم‌افزار

فعالیت‌ها

فعالیت یک نقش خاص، یک واحد از کار است که فردی که آن نقش را بر عهده دارد باید آن‌را انجام دهد. این فعالیت، هدف مشخصی دارد که معمولا به صورت ایجاد یا بروز کردن بعضی خروجی‌ها مانند یک مدل، یک مولفه یا یک طرح بیان می‌شود. هر فعالیت به یک نقش خاص اختصاص دارد. یک فعالیت به طور کلی بین چند ساعت تا چند روز طول می کشد. به عنوان مثال در شکل۵-۶ به فعالیت‌های نقش متخصص شبکه اشاره گردیده است.



(شکل ۵-۶): فعالیت‌های متخصص شبکه

خروجی‌ها

یک خروجی، بخشی از اطلاعات است که توسط یک فرآیند تولید می‌شود، تغییر می‌کند یا استفاده می‌شود. خروجی‌ها، عناصر ملموس پروژه هستند؛ چیزهایی که پروژه در حین کار برای محصول نهایی، تولید یا استفاده می‌کند. خروجی‌ها توسط نقش‌ها برای انجام یک فعالیت به عنوان ورودی استفاده می‌شوند و نتیجه یا خروجی سایر فعالیت‌ها هستند. خروجی‌ها ممکن است اشکال یا فرم‌های مختلفی داشته باشند:

۱- یک مستند مانند سند چشم‌انداز سازمان

۲- برنامه‌های قابل اجرا مانند یک نمونه اولیه قابل اجرا

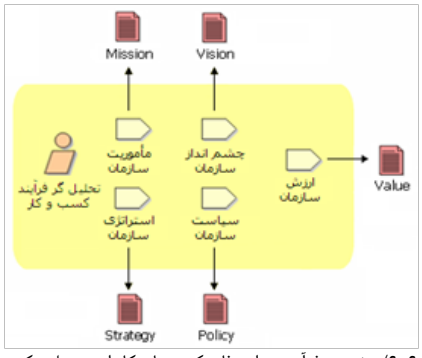
۳- یک مدل مانند سند طراحی

جریان‌های کار

فقط فهرست کردن همه نقش‌ها، فعالیت‌ها و خروجی‌ها تشکیل‌دهنده یک فرآیند نیست. راهی برای توضیح توالی معنادار از فعالیت‌هایی که بعضی نتایج ارزشمند را تولید می‌کنند و نیز برای نشان دادن کنش نقش‌ها، مورد نیاز است. این دقیقا کاریست که جریان‌های کار انجام می‌دهند. [۶]

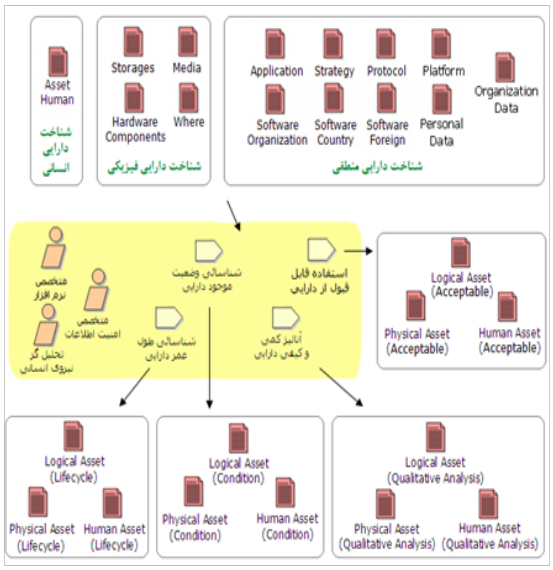
جریان‌های کار به اشکال متفاوتی وجود دارند. دو جریان کار رایج، یکی دیسیپلین‌ها هستند که جریان‌های کار سطح بالا هستند و دیگری جزییات جریان کار که جریان‌های کار موجود در یک دیسیپلین می‌باشند. به عنوان مثال به دو مورد از دیسپلین‌ها در شکل ۶-۶ و ۶-۷ و اشاره شده است.

a. یک جریان کار از دیسیپلین کسب و کار



(شکل ۶-۶): وضعیت فرآیند در این فاز یک جریان کار از دیسیپلین کسب و کار

b. یک جریان کار از دیسیپلین دارایی



(شکل ۷-۶): یک جریان کار از دیسیپلین دارایی

۷- نتیجه‌گیری

در حال حاضر، حاکمیت فناوری اطلاعات به عنوان یکی از ضروری‌ترین اهرم‌ها در خصوص استفاده کارآمد و ارزش‌افزای فناوری اطلاعات، جزء ضروریات یک سازمان می‌باشد. هر کدام از استانداردهای تشریح شده در این تحقیق بیانگر مدیریت ابعاد مختلفی از فناوری اطلاعات و استقرار حاکمیت فناوری اطلاعات با راهکارهای خود می‌باشند. در این تحقیق سعی گردید تا حوزه‌های تحت پوشش هر کدام از این استانداردها در خصوص حاکمیت فناوری اطلاعات ارایه گردد. همچنین با ارایه مدلی جدید در خصوص استاندارد ایزو ۲۷۰۰۱ بر پایه مدل آر.یو.پی سعی شد یک مدل پویا معرفی شود که در تحقیق آینده موارد ذیل محقق گردد:

- عملیاتی نمودن متدولوژی بومی شده؛

- استخراج سطح بلوغ امنیت بر اساس مکعب امنیتی ارایه شده؛
- استخراج سند برنامه‌ریزی امنیت بر اساس مدل با توجه به استخراج سندهایی همچون وضعیت موجود سازمان در فاز شناخت، شاخص‌ها در سطوح مکعب امنیتی، وضعیت مطلوب با توجه به سطوح بلوغ امنیت.

۸- منابع :

[1] Hong-Mei Chen,") 2007"(Enterprise Architecture and Business-IT Alignment", MANAGING ENTERPRISE ARCHITECTURE STRATEGIES & EXPERIENCES, 23.–24. August.

[2] Hong-Mei Chena, Rick Kazmana, Aditya Gargb, (2005) "BITAM: An engineering-principled method for managing misalignments between business and IT architectures", Science of Computer Programming 57 5–26.

[3] Board Briefing on IT Governance, 2nd Edition, Web sites: www.itgi.org and www.isaca.org

[4] ISO/BS7799 , Compliance with best practices in Information security.

[5] Rossouw von Solmsa, S.Hvon Solms, (2009) "Information Security Governance A model based on the Direct–Control Cycle", computers & security 25 408–412.

[6] Haumer, P.,) (2005"IBM Rational Method Composer: Part 1: Key Concepts", December 2005

[7] J. Stuart Broderick, (2006) "ISMS, security standards and security regulations", information security technical report 26 – 31.

[8] Kruchten, P.) 2003(, Rational Unified Process, The: An Introduction, Third Edition, Addison Wesley, December.

[9] Balduino, R., "Basic Unified Process: A Process for Small and Agile Projects", Ricardo Balduino - Rational Unified Process Content Developer, IBM.

[10] Rosslin John Robles, Ji-Yeu Park, Tai-hoon Kim ,"Information Security Control Centralization and IT Governance for Enterprises", International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 3, July, 2008.

[11] Software & Systems Process Engineering Meta-Model Specification", http://www.omg.org/spec/SPEM/2.0/PDF

[12] Rational Unified Process: Best Practices for Software Development Teams, Rational Software White Paper TP026B, Rev 11/01