دانشگاه پیام نور

دانشکده فنی و مهندسی

پایان نامه

جهت دریافت درجه کارشناسی ارشد در رشته مدیریت فناوری اطلاعات

گروه مهندسی کامپیوتر و فناوری اطلاعات

ارائه چارچوبی برای توسعه بیمه های الکترونیک در ایران با بکارگیری مدل تلفیقی ISMS

فرزانه صباحی فاخر

استاد راهنما

دکتر سید علی رضوی ابراهیمی

استاد مشاور

دکتر رضا عسگری مقدم

شهریور 1390

دانشگاه پیام نور

دانشکده فنی و مهندسی

دانشگاه پیام نور مرکز تهران

پایان نامه

جهت دریافت درجه کارشناسی ارشد در رشته مدیریت فناوری اطلاعات

ارائه چارچوبی برای توسعه بیمه های الکترونیک در ایران با بکارگیری مدل تلفیقی ISMS

فرزانه صباحی فاخر

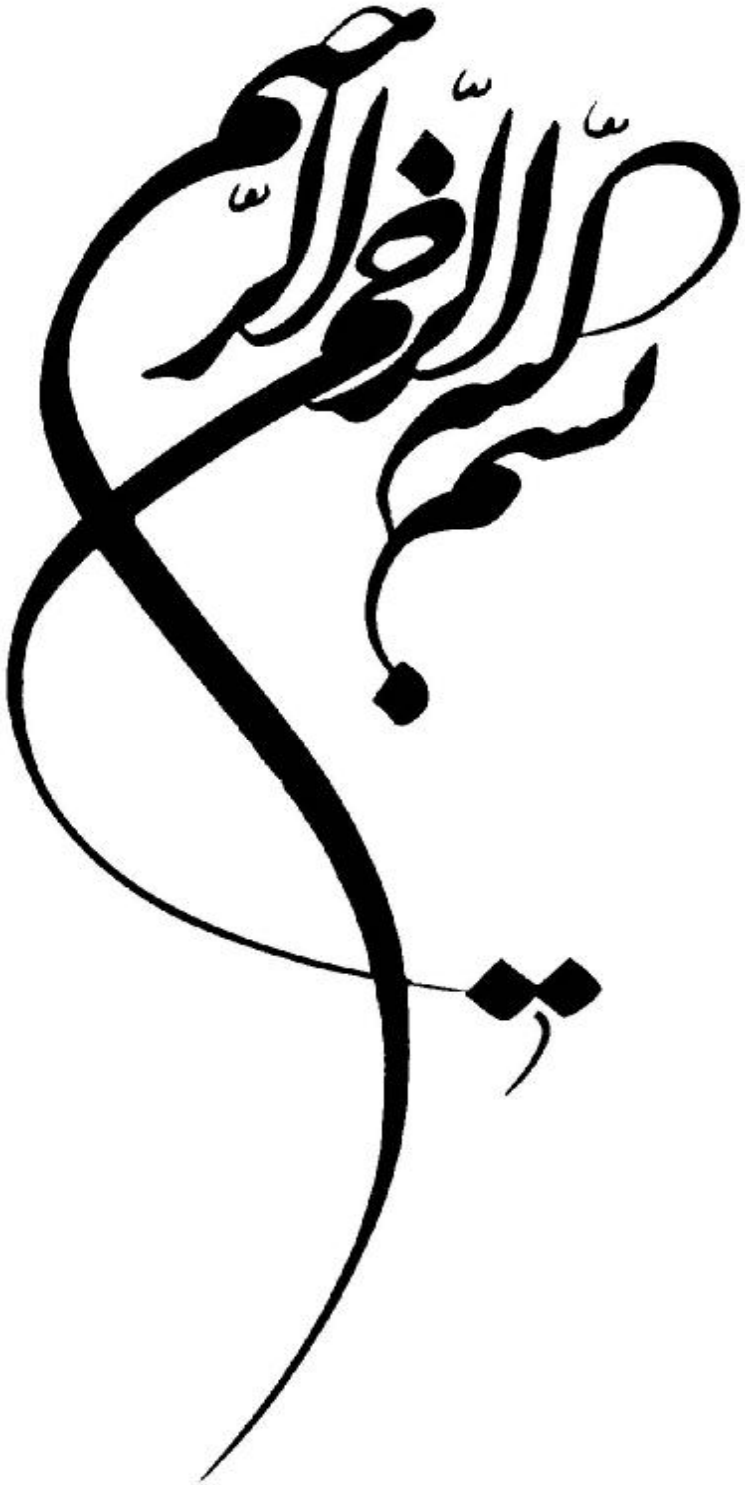
استاد راهنما

دکتر سید علی رضوی ابراهیمی

استاد مشاور

دکتر رضا عسگری مقدم

شهریور 1390


بسم الله الرحمن الرحیم

پیوست .....

دانشگاه پیام نور
دانشگاه پیام نور استان تهران
واحد علمی کاربردی فنی و مهندسی

تصویب نامه

پایان نامه کارشناسی ارشد رشته مدیریت فناوری اطلاعات

تحت عنوان:

"ارائه چار چوبی برای توسعه بیمه های الکترونیک در ایران با به کارگیری مدل تلفیقیISMS "

تاریخ دفاع :۱۳۹۰/۶/۳۰ ساعت۱۰-۸

نمره:۱۹ **درجه ارزشیابی:** عالی

هیات داوران:

داوران	نام و نام خانوادگی	مرتبه علمی	امضاء
استاد راهنما	دکتوسیدعلی رضوی	استادیار	
استاد مشاور	دکتررضا عسگری مقدم	استادیار	
استاد داور داخلی	دکتراحمد فراهی	استادیار	
استاد داور مدعو	دکترغلامرضا شاه محمدی	دانشیار	
نماینده گروه	دکتر احمد فراهی	استادیار	

تهران، خیابان استاد نجات اللهی
تقاطع خیابان سپند، کوچه هشتم
پلاک ۱۱
تلفن: ۸۸۹۰۴۱۲۷
دورنگار: ۸۸۹۰۳۳۱۰
WWW.FANI.TPNU.AC.IR
fani@ tpnu.ac.ir

تقدیم به

پدر مهربان و مادر فداکارم

همسرم او که بهترین است

برادرانم که از صمیم قلب دوستشان دارم

و

اساتید و معلمین گرانقدری که پژوهش را به من آموختند

تشکر و قدردانی

در اینجا لازم می دانم که از زحمات و راهنمایی های اساتید ارجمند، جناب آقای دکتر سید علی رضوی ابراهیمی و دکتر عسگری مقدم کمال تشکر و قدردانی را داشته باشم و از خداوند متعال، موفقیت و پیروزی ایشان را در تمام مراحل زندگی خواهانم.

چکیده

ارائه چارچوبی برای توسعه بیمه های الکترونیک در ایران با بکارگیری مدل تلفیقی ISMS[1]

در سازمانهای امروزی اطلاعات معادل سرمایه است و به همان میزان نیز نیازمند نگهداری مناسب می باشد. اطمینان از صحت ، محرمانگی و در دسترس بودن سرمایه های اطلاعاتی و تجهیزات زیر ساختی کشور گذشته از ابعاد گسترده امنیت ملی ، کلید قفل فرصتهای بی شمار تجاری و غیر تجاری جدید اینترنتی است . صنعت بیمه الکترونیکی در سالهای اخیر توجه زیادی را به امنیت الکترونیکی داشته است زیرا مطابق تحقیقات که در دانشگاه نبراسکالینکولن و کنتاکی شمال آمریکا انجام شده است یکی از ۹ عامل موثر بر موفقیت بیمه های الکترونیکی امنیت و دسترسی پذیری وب سایت شرکتهای بیمه می باشد .

پیاده سازی امنیت اطلاعات فرایندی پیچیده ، زمانبر ، پرهزینه و در ماهیت بین رشته ای است و طیف وسیعی را از جمله امنیت پرسنلی ،کنترل دسترسی کاربر ، امنیت شبکه و مباحث قانونی ، فرهنگ و ... را شامل می شود بنابراین محققان سعی در ارائه چارچوبها و مدل های گوناگون برای اداره مطلوب امنیت اطلاعات را داشتند اما به طور معمول این مدل ها از جامعیت کافی در محتوا و روش برخوردار نبوده و قابلیت تعمیم به تمام سازمانها را دارا نمی باشند که به تفصیل به آنها اشاره خواهد شد. بنابراین این تحقیق سعی در تدوین چارچوبی جامع و تلفیقی برای مدیریت امنیت اطلاعات، متناسب با شرایط فعلی صنعت بیمه کشور دارد. بدین منظور از دو پرسشنامه مجزا برای گردآوری و تحلیل نظرات خبرگان صنعت در این موضوع و مدیران و کارشناسان امنیت اطلاعات ۱۰ شرکت بیمه کشور استفاده شده است.این چارچوب سه رویکرد رایج مدیریت امنیت اطلاعات، یعنی رویکرد فرآیندی (چرخه دمینگ) ، رویکرد سلسله مراتبی (جایگاه سازمانی)و کارویژه ای (مسائل فنی ،انسانی و کسب و کار) را ترکیب نموده است.این چارچوب به دلیل همراستایی با استانداردهای معتبر جهانی ISMS ، قابل پیاده سازی و سازگاری با صنایع دیگر نیز می باشد .

کلید واژه : بیمه ، بیمه الکترونیکی ، سیستم مدیریت امنیت اطلاعات، سلسله مراتب سازمانی، چرخه دمینگ، کارویژه، استاندارد امنیت اطلاعات

[1] Information security management system

فهرست مطالب

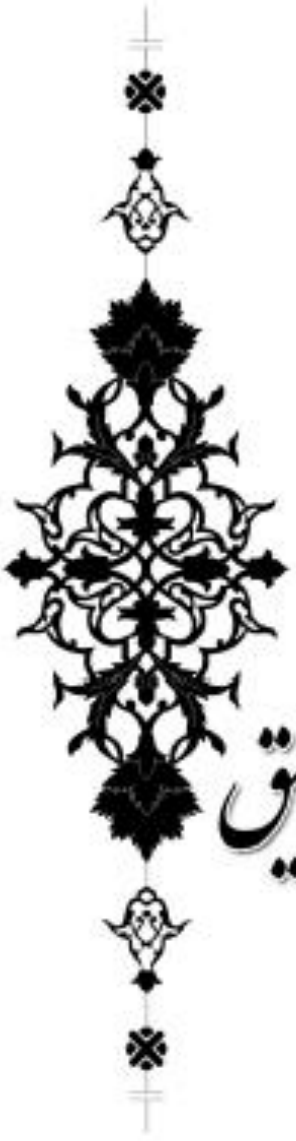
صفحه

فهرست مطالب

صفحه

فهرست جداول و اشکال

صفحه



فصل اول

کلیات تحقیق

۱- ۱ مقدمه

در این فصل به کلیات و مفاهیم تحقیق که شامل موارد ذیل می باشد می پردازیم : تعریف موضوع و اهمیت تحقیق، پیشینه تحقیق، بیان مساله و سوالات تحقیق، فرضیات تحقیق، اهداف تحقیق، کاربرد نتایج و مخاطبان تحقیق، روش انجام تحقیق، و واژگان تخصصی.

۱-۲ سابقه و ضرورت تحقیق

در جهان امروز اتکای هر سازمانی، چه دولتی و چه خصوصی، بر مبنای تکنولوژی اطلاعات است که بطور فزاینده ای در حال افزایش می‌باشد. در طول دو دهه گذشته، ماهیت سیستم‌های اطلاعاتی بطور عمده‌ای تغییر یافته و تبدیل به بخش بزرگی از فرآیندهای کسب و کار شده است. اطلاعات، به یک دارایی راهبردیی توسعه یافته و سیستم های اطلاعاتی به یک ابزار راهبردیی برای سازمان‌ها و دولت تبدیل شده است. اطلاعات، مهمترین دارایی است و در شرایط کنونی برای فعالیت‌های کسب و کار و تصمیم‌گیری حیاتی شده است و به سازمان‌ها اجازه بقا و رشد در محیط‌های اقتصادی رقابتی و خشن می‌دهد. همچنین به دولت‌ها این امکان را می‌دهد که خدمات و زیرساخت را برای اجزاء سازنده خود فراهم آورند. (Woodhouse, ۲۰۰۸) .

اما فراهم شدن امکانات فنی جدید تنها باعث پیدایش محصولات نوین و راه هـای بهتـر و کارآمـدتر برای انجام امور نشده ، بلکه در کنار آن امکـان سـوء اسـتفاده از فنـاوری را نیـز افـزایش داده اسـت فناوری اطلاعات و ارتباطات نیز همانند سایر فناوریها حالت ابزاری دارد و می توان آن را به گونه ای مورد استفاده قرار داد که برای همگان مفید باشد و یا به نحوی از آن استفاده کرد که نتایج خطرنـاکی به بار آورد . عامل سرعت در فناوری اطلاعات و ارتباطات چیزی در حدود میکـرو ثانیـه اسـت کـه باعث می شود اطلاعات غیرقابل مشاهده با چشم غیر مسلح ، تحت کنترل نرم افزار تهیه شده توسط افراد جابجا گردد . در چنین فضایی اعمال غیر قانونی و مخرب آنقدر سریع صورت می گیرد که مـی تواند غیر قابل شناسایی باشد . در نتیجه امروزه امنیت فن آوری اطلاعات به عنوان مهمتـرین چـالش بر سر راه توسعه فن آوری محسوب می شود. امنیت فن آوری خصوصـاً در کاربردهـای اقتصـادی و تجاری بیشترین اهمیت را دارد. در این راستا، با پیشرفت روزافزون تجارت الکترونیکی، سازمان‌ها به سیستم‌های اطلاعاتی برای انجام عملیات روزانه کسب و کارشان بیشتر وابسته شده‌اند. این وابستگی،

خود ضرورت مدیریت امنیت این سیستم‌ها را برجسته ساخته است (Zuccato, ۲۰۰۷). به این ترتیب، اطلاعات معادل سرمایه است و به همان مقدار نیازمند نگهداری مناسب می باشد (Kwon, et al., ۲۰۰۷).

محرمانگی، صحت و در دسترس بودن اطلاعات، صفاتی است که هدف از پیاده سازی امنیت اطلاعات را تشکیل می دهند(Farn, et al., ۲۰۰٤).

هدف مدیریت امنیت اطلاعات، تضمین تداوم کسب و کار، اطمینان مشتری، حفاظت از فرصت‌ها و سرمایه‌گذاری‌های کسب و کار و کاهش آسیب‌های کسب و کار بوسیله جلوگیری و کمینه کردن اثرات حوادث امنیتی است (Vermeulen and von Solms, ۲۰۰۲; Ma, ۲۰۰۵). همچنین می‌توان گفت مقصود اصلی از طراحی نظام مدیریت امنیت اطلاعات، ایجاد اطمینان برای مدیریت سطح عالی است که امنیت اطلاعات شرکت همانگونه که مورد نیاز مدیریت عالی و یا نیازهای تنظیمی[۱]بوده به خوبی مدیریت می‌شود و شواهدی وجود دارد که آنها در قبال مسئولیت خود پرتلاش[۲] و امین[۳] می‌باشند (Broderick, ۲۰۰٦). علاوه بر آن مدیریت امنیت بنگاه موجب کاهش مصرف منابع و بهبود کارایی مدیریت می‌شود (Kim et al., ۲۰۰٦)، ریسک را کاهش داده و از اطلاعات ارزشمند حفاظت می‌نماید (Knapp, ۲۰۰۵). عامل دیگر در اهمیت یافتن مدیریت امنیت اطلاعات، شبکه‌های جهانی و تجارت الکترونیکی می‌باشند. با اشاعه اینترنت و جهانی شدن زندگی روزمره ما دچار تغییر شده است و سازمان‌های مدرن از اینترنت برای عملیات کسب و کار خود استفاده نموده و در نتیجه به آن وابسته شده‌اند. این امر تجارت الکترونیکی را به دنبال داشته است که موجبات تغییر فرآیندهای کسب و کار سازمان‌ها را فراهم نموده است. این وابستگی به کسب و کار الکترونیکی نیز ضرورت حفاظت از اطلاعات را مطرح نموده و رویکردهای گوناگونی را برای مدیریت امنیت اطلاعات به وجود آورده است (Zuccato, ۲۰۰۷). یکی از مشکلات عمده در رویکرد مدیران در برقراری امنیت اطلاعات این است که چندپارگی در اداره آن به چشم می‌خورد. لذا برای پیاده‌سازی اثربخش امنیت اطلاعات نیاز به رویکردی یکپارچه است. البته انتخاب این

---

[۱] regulatory
[۲] diligence
[۳] fiduciary

رویکرد باید با توجه به ویژگی‌های مدیریت عالی باشد. (Vermeulen and Von Solms,۲۰۰۲) از طرفی دیگر، یکپارچه شدن سیستم‌های اطلاعاتی به پیچیده‌تر شدن امنیت اطلاعات کمک می‌کند (Korzyk, ۲۰۰۲). این پیچیدگی مدیریت امنیت اطلاعات، خود نیاز برای یک راهنما را برای اداره آن به‌وجود آورده است (Vermeulen and Von Solms, ۲۰۰۲).

یکی از حوزه هایی که در آن بحث امنیت اطلاعات اهمیت بسیار می یابد، صنعت بیمه و به ویژه بیمه الکترونیکی می باشد. بیمه الکترونیکی که در ۱۵ سال اخیر و با توسعه فناوری اطلاعات مطرح شده است، استفاده از فناوری رایانه برای گذار از جنبه های زمانبر و فیزیکی شرکتهای بیمه سنتی می باشد. بیمه الکترونیکی از فناوری استفاده می کند تا به مشتریان و دیگر ذینفعانش اجازه دهد تا با شرکتهای بیمه به صورت الکترونیکی از طریق کانالهای متنوعی نظیر اینترنت، وسایل بی سیم[٤] و شعبات فیزیکی تعامل داشته باشند. امروزه صنعت بیمه (و به طور گسترده تر بخش مالی)، با اشیایی سروکار دارند که به راحتی کد گذاری می شوند (نظیر داده های الکترونیکی) بنابراین طبیعی است که این صنعت هدایتگر راه در توسعه راه حل های فناوری اطلاعات باشد. سیستم های اطلاعاتی جامع و دربرگیرنده، برای وجود موسسات مالی، اصلی ضروری می شوند. طبق تحقیقات صورت گرفته روند رشد سیستمهای اطلاعاتی و وابستگی بیش از پیش به اطلاعات، ایجاد سیستم مدیریت امنیت اطلاعات را در کشور ما نیز همانند سایر کشورهای جهان ضروری می نماید.

علیرغم تلاش های بسیار در ارتقای سطح مدیریت اطلاعات در سازمان های سنتی به نظر می رسد نظریات گذشته قابلیت تعمیم به سازمان های امروزی با ویژگی های نوین را دارا نمی باشند(Raval, and Fichadia, ۲۰۰۷) از نظر تئوریک معمولا سازمانها از چارچوب ها و سبک های گوناگونی برای مدیریت امنیت اطلاعات استفاده می نمایند که بر این اساس تقسیم بندی هایی صورت گرفته است و تلاش شده است تا مدل یا سبکی خاص را برای اداره بهینه امنیت اطلاعات در سازمان ها مشخص نمایند اما همانطور که Hong نیز معتقد است تمام این نظرات قطعاتی جدا افتاده از یکدیگرند که به تنهایی کاربرد نخواهند داشت و باید راهکاری برای تلفیق آنها یافت (Hong, ۲۰۰۳). از آن گذشته در سال های اخیر امواج جدید مدیریت امنیت اطلاعات نظیر دانش

[٤] Wireless

محور شدن(Belsis, et al, ۲۰۰۵)، استاندارد ها و مسائل حقوقی مطـرح گشـته انـد کـه بـه دلیـل گستردگی تعاملات شرکتهای بیمه و اثرات گسترده نتایج این تعاملات از نظر امنیتی، باید در هر طرح مدیریتی منعکس شوند.

با توجه به موارد مطرح شده ، نیاز برای تدوین و طراحی یک چارچوب جامع، تلفیق شده و مطابق با مباحث روز در زمینه مدیریت امنیت اطلاعات برای شرکتهای بیمه ضـروری و حیـاتی بـه نظـر مـی رسد(Von solms, ۱۹۹۹; Von solms, ۲۰۰٦) . مدل های موجود معمولا تک بعدی هسـتند و در محتوی یا رویکرد، ویژگی های جامع بودن و تلفیق ابعاد مختلـف را در بـر نمـی گیرنـد. معایـب مدلها به صورت موردی در جدول شماره ۲-۳ نام برده شده اند . دراین تحقیق سعی بر آن است کـه ضمن ارائه جامع ترین و کامل ترین نگرش به مقوله مدیریت امنیت اطلاعـات، سـه رویکـرد مهـم و مرسوم مدیریت امنیت اطلاعات به عنوان چرخه دمینگ (بـه منظـور نگـرش فرآینـدی و انطبـاق بـا استاندارد های معتبر) ، سلسه مراتب سازمانی (به منظور درک جایگاه اقدامات در سطوح سازمانی)، و کارویژه ای (به منظور سهولت درک و به کارگیری و افزایش کارایی) را بـا یکـدیگر در قالـب مـدلی تلفیق نموده و چارچوب جامع مـدیریت امنیـت اطلاعـات در بیمـه الکترونیکـی را ارائـه مـی دهـد. مدلهایی که در این زمینه ارائه شده اند عبارتند از : راهنمـای مـدیریت امنیـت فنـاوری اطلاعـات یـا GMITS که توسط وان سولمز۵ در سال ۱۹۹۸ ارائه گردیده است که در آن روشها و الزامات پیـاده سازی سیستم مدیریت امنیت اطلاعات در سازمانها به تشریح بیان گردیده است ، مدل بعدی طراحی روال های مدیریت امنیت اطلاعات است که چارچوبی برای تعیـین گـام هـا و روال هـای مـدیریت امنیت اطلاعات است کـه توسـط سـولمز و ورمـولن٦ در سـال ۲۰۰۲ ارائـه شـده اسـت، سـولمز و پوستامس۷ نیز در سال ۲۰۰٤ چارچوبی برای راهبری امنیت اطلاعات در سازمان ها بیان کردند . در سال ۲۰۰٤، استو پرسر۸ مدلی فرایندگرا برای مدیریت امنیت اطلاعات در نظر گرفتـه اسـت کـه بـر اساس توسعه از طریق درک شرایط جاری سازمان بنا شده است ، اسمیت۹ نیز مدلی بـرای مـدیریت

---

۵ Rossouw von Solms
٦ Vermeulen
۷ Posthumus
۸ Steve Persur
۹ Smith

امنیت الکترونیکی در سازمان ارائه نمود. سانگو و همکارانش[10] در سال ۲۰۰۷ مدلی را تحت عنوان "مدل خودارزیابی ISMS " ارائـه داده ،وود هـوس[11] نیـز در سـال ۲۰۰۸ مـدل بلـوغی را بـرای ISMS به منظور تشریح مباحث فرهنگی و رسیدن بـه قضـاوت بهتـری از سـطوح بلـوغ ارائـه داد(سولمز ، ۲۰۰۵) .در میان تحقیقاتی که در ایران در زمینه امنیت اطلاعات انجام شده می توان به پایان نامه کارشناسی ارشدی که به مسائل فنی در این زمینه تکیه داشته با عنوان "ارزیابی امنیتی شبکه های کامپیوتری بررسی موضوع و ارائه راه حل" که توسط داوود صرامی فروشانی در سال ۱۳۸۳ نگـارش یافته است. "ارائه مدل مفهومی ارزیابی ریسک امنیت اطلاعات: مورد بانک سـپه" پدیدآورنـده زهـرا کریمی در سال ۱۳۸۵ ، "ارائه مدلی جهت سنجش میزان آمادگی سازمان برای پیـاده سـازی سیسـتم مدیریت امنیت اطلاعات: مورد راه آهن" پدیدآورنده عماد شهیدی در سـال ۱۳۸٦ ، همچنـین پایـان نامه کارشناسی ارشد سحر میرانوری با عنوان "شناسایی عوامـل بحرانـی موفقیـت (CSFs) سیسـتم مدیریت امنیت اطلاعات در سازمان های ایرانی" به دسته بندی عوامل بحرانـی موفقیـت در ISMS می پردازد.

۱-۳ اهداف تحقیق

- ارائه چارچوب جامع و تلفیقی مدیریت امنیت اطلاعات با توجه به ویژگی های سازمان های ایرانی
- در نظر گرفتن ویژگی های خاص شرکتهای بیمه در تدوین چارچوب تحقیق

۱-٤ مخاطبان تحقیق

مخاطبان اصلی تحقیق ، مدیران ارشد فناوری اطلاعات و امنیت اطلاعات شرکتهای بیمه می باشـند، چراکه این تحقیق نگاه جامع و استراتژیک از ابعاد گوناگون مدیریت امنیت اطلاعات در اختیـار آنهـا قرار می دهد ، همچنین امکان تلفیق سه رویکرد مجزا که در پیشینه تحقیقات و همـه اسـتانداردهای معتبر بین المللی امنیت اطلاعات نیز ذکـر گردیـده انـد را بـه ایشـان مـی دهـد . همچنـین اسـاتید، دانشجویان و پژوهشگران مدیریت امنیت اطلاعات نیز می توانند درک جامع از نیازمندی های امنیـت اطلاعات، راهکارهای پاسخگویی به نیازهای کسب و کار و نحوه پیاده سازی آنها به دست آوردند .

[10] Sungho Kwon ،Sangsoo Jang ،Jaeill Lee و Sangkyun Kim
[11] Steven Woodhouse

۱-۵ بیان مسئله و سوال های تحقیق

مهمترین چالش شرکتهای بیمه، کاهش ریسک های آن به ویژه در زمینه امنیت اطلاعات است(Claessens, et al, ۲۰۰۲). تحقیقات نشان داده است که عموم مشتریان شرکتهای بیمه و تقریبا تمام مصرف کنندگان خدمات بیمه الکترونیکی از مسائل امنیت اطلاعاتی هراس دارند و از آنجا که کوچکترین رخنه امنیتی منجر به خسارات سرسام آور مالی و همینطور تخریب وجهه شرکتهای بیمه نزد مشتریان اصلی شرکتهای بیمه (که همانا مردم هستند) می شوند، به نظر می رسد تدوین و پیاده سازی راهکارهای امنیتی برای اطلاعات از دغدغه های اصلی این گونه سازمان ها محسوب می شود(Claessens, et al, ۲۰۰۲).

در وضعیت کنونی پیاده سازی امنیت اطلاعات فرآیندی پیچیده، زمانبر و پرهزینه و در ماهیت بین رشته ای است(Mitchell, et al., ۱۹۹۹; Von solms, ۲۰۰۵). نکته مهم این است که امنیت اطلاعات ماهیتی میان رشته ای دارد و طیف وسیعی را از جمله امنیت پرسنلی، کنترل دسترسی[۱۲] کاربر، امنیت شبکه و مباحث قانونی، فرهنگ و ... را شامل می شود (Dhillon, ۲۰۰۷; Tsoumas and Tryfonas, ۲۰۰٦). این امر مدیریت آن را مشکل ساخته است (Eloff and Von solms, ۲۰۰۰). در هر حال اداره امنیت اطلاعات امروزه به عنوان بخش پیوسته ای از مدیریت محیط IT در سازمان ها پذیرفته شده است و پستی تحت عنوان مدیر امنیت اطلاعات در تمام سازمان های پیشرو به ویژه شرکتهای بیمه ها ایجاد گشته است(Huang,, et al., ۲۰۰٦).

این تحقیق در صدد تدوین چارچوب مناسب ، بهینه و جامع و با رویکردی تلفیقی و مختص بیمه الکترونیک در ایران می باشد .

سوالات این تحقیق در بعد چرخه دمینگ عبارتند از:

- آیا اقدامات مربوط به طراحی در مدیریت امنیت اطلاعات، اثر مثبت بر بهبود عملکرد مدیریت امنیت اطلاعات شرکتهای بیمه دارد؟
- آیا اقدامات مربوط به اجرا در مدیریت امنیت اطلاعات، اثر مثبت بر بهبود عملکرد مدیریت امنیت اطلاعات شرکتهای بیمه دارد؟

[۱۲] Access Control

- آیا اقدامات مربوط به ارزیابی در مدیریت امنیت اطلاعات، اثر مثبت بر بهبود عملکرد مدیریت امنیت اطلاعات شرکتهای بیمه دارد؟
- آیا اقدامات مربوط به اصلاح و بازنگری در مدیریت امنیت اطلاعات، اثر مثبت بر بهبود عملکرد مدیریت امنیت اطلاعات شرکتهای بیمه دارد؟

سوالات این تحقیق در بعد سلسله مراتب سازمانی عبارتند از:

- آیا عملکرد سطح راهبردی امنیت اطلاعات چارچوب تلفیقی مدیریت امنیت اطلاعات، اثر مثبت بر بهبود عملکرد مدیریت امنیت اطلاعات شرکتهای بیمه دارد؟
- آیا عملکرد سطح تاکتیکی امنیت اطلاعات چارچوب تلفیقی مدیریت امنیت اطلاعات ، اثر مثبت بر بهبود عملکرد مدیریت امنیت اطلاعات شرکتهای بیمه دارد؟
- آیا عملکرد سطح عملیاتی امنیت اطلاعات چارچوب تلفیقی مدیریت امنیت اطلاعات ، اثر مثبت بر بهبود عملکرد مدیریت امنیت اطلاعات شرکتهای بیمه دارد؟

سوالات این تحقیق در بعد کارویژه ها عبارتند از:

- آیا مولفه های مرتبط با مسائل فنی اثر مثبت بر بهبود عملکرد مدیریت امنیت اطلاعات شرکتهای بیمه دارد؟
- آیا مولفه های مرتبط با مسائل انسانی اثر مثبت بر بهبود عملکرد مدیریت امنیت اطلاعات شرکتهای بیمه دارد؟
- آیا مولفه های مرتبط با کسب و کار، اثر مثبت بر بهبود عملکرد مدیریت امنیت اطلاعات شرکتهای بیمه دارد؟

سوال اصلی این تحقیق عبارت است از:

- چارچوب مناسب برای مدیریت امنیت اطلاعات در زمینه بیمه الکترونیکی کدام است؟