بسمه‌تعالی

نقشه راه صنعت بیمه در مواجهه با ریسک فناوری اطلاعات

علی کمندی[۱]، وحیده نورانی[۳]

[۱] دانشکده علوم مهندسی، پردیس دانشکده‌های فنی دانشگاه تهران،
kamandi@ut.ac.ir

[۲] مسئول میز تخصصی نوآوری، پژوهشکده بیمه.
va.nourani@gmail.com

چکیده

شرکتهای مالی امروزه بیشترین وابستگی را به تکنولوژی دارند و از منظر تکنولوژی پیچیده ترین ساختار را دارند. این صنعت که وظیفه اصلی آن شناسایی و انتقال ریسک است، بیش از هر صنعت دیگری تحت تاثیر تکنولوژی قرار دارد. ریسک‌های فناوری اطلاعات و عملیات شامل تکنولوژی، فرایندهایی است که موسسات مالی و بیمه‌ها برای شناسایی، پایش و پیشگیری از ریسک به کار می‌گیرند. این طبقه از ریسک‌ها از زمان بحران مالی اخیر مورد توجه شدید نهادهای ناظر قرار گرفته است. نهادهای ناظر حتی تا بازبینی دقیق سیستم‌ها پیش رفته‌اند. استاندارد بازل ۲ در صنعت بانکداری وجود یک موتور محاسبات پیشرفته را با استفاده از متدولوژی‌های جدید ریسک الزام کرده است. همچنین نهادهای ناظر آزمون فشار و بالا به پایین را در برنامه‌ریزی ریسک شرکت‌ها الزام کرده‌اند.

کلمات کلیدی

ریسک، فناوری اطلاعات، بیمه، استاندارد.

۱- مقدمه

صنعت بیمه، خود پذیرای ریسک سایر شرکت‌ها است. ریسک‌های مالی یکی از مهم‌ترین نوع از ریسک‌هایی است که به شرکت‌های بیمه انتقال داده می‌شود. در دهه پس از بحران مالی ۲۰۰۹، مدیران ارشد شرکت‌های بیمه توجه بسیار زیادی را به مدیریت بهتر ریسک‌های مالی معطوف داشتند. با این حال، ریسک‌های غیر مالی، که معمولا به عنوان ریسک‌های عملیاتی[1] نیز شناخته می‌شوند، در درجه دوم اهمیت قرار داشته و اغلب به شایستگی مورد توجه قرار نگرفته‌اند.

ریسک‌های غیر مالی اغلب تنوع زیادی دارند و بر کارکرد روزمره شرکت‌های بیمه اثر می‌گذارند. ریسک‌های اجرایی، ریسک‌های منابع انسانی (به ویژه مشاغل حساس)، تقلب و سوء استفاده، اختلال در خدمات فناوری اطلاعات، حملات سایبری و لو رفتن داده‌ها، نمونه‌هایی از این ریسک‌ها به شمار می‌آیند. مدیران بیمه‌ها به نیکی می‌دانند که هر یک از این ریسک‌ها چه تبعاتی را برای شرکت به دنبال خواهند داشت. گزارش مکنزی نشان می‌دهد این ریسک می‌تواند تا ٦٪ از کل درآمد خالص شرکت، هزینه ایجاد کند. در صنعتی که درآمد سالانه آن ۵ تریلیون دلار است، این مبلغ در جهان به چند ده میلیارد دلار خواهد رسید.

صنعت بیمه در سال‌های اخیر با ریسک‌های بیشتری مواجه بوده است و اکنون ریسک‌های عملیاتی به اولویت اول مدیران ارشد تبدیل شده است. مطالعه‌ای که توسط مکنزی انجام شده است نشان می‌دهد که بیش از نیمی از شرکت‌های بیمه بودجه مدیریت ریسک‌های عملیاتی خود را افزایش داده و افراد متخصصی را برای این منظور جذب کرده‌اند (۱).

یکی از مهم‌ترین ریسک‌های غیر مالی در شرکت‌های بیمه به دلیل وابستگی شدید به سامانه‌ها و زیرساخت‌های فناوری اطلاعات، ریسک‌های این حوزه است. ریسک‌های فناوری اطلاعات، خود گستره وسیعی از ریسک‌های راهبردی، ریسک‌های سرویس‌ها و خدمات فناوری اطلاعات، ریسک‌های زیرساختی و .. را شامل می‌شود. در این مقاله، با فرض اینکه ضرورت پرداختن به ریسک‌های فناوری اطلاعات برای مدیران ارشد صنعت بیمه آشکار شده است، سعی داریم چگونگی پرداختن به این ریسک‌ها در شرکت‌های بیمه را مورد توجه قرار داده و به سوالات زیر پاسخ دهیم:

- ریسک‌های فناوری اطلاعات در چه جایگاهی نسبت به ریسک‌های سازمان قرار می‌گیرند و چگونه طبقه‌بندی می‌شوند؟
- چارچوب‌های استاندارد مدیریت ریسک‌های فناوری اطلاعات کدامند؟
- شرکت‌های بیمه چگونه می‌توانند از تجربیات موجود در این چارچوب‌ها استفاده کنند و شرح وظایف کلان هر یک از واحدها چیست؟
- وظیفه نهاد ناظر در فرایند مدیریت ریسک‌های فناوری اطلاعات چیست؟

همچنین ضمن معرفی استانداردها و منابع لازم سعی خواهیم کرد تا نقطه شروع ورود به بحث مدیریت ریسک‌های فناوری اطلاعات را برای شرکت‌های بیمه فراهم آوریم.

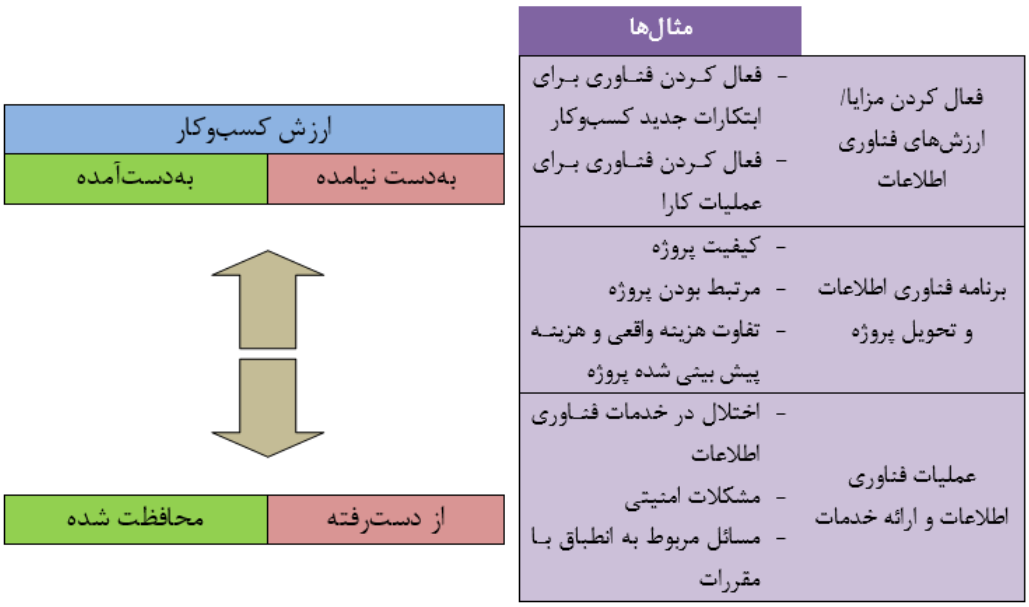
[1] Operational

۱- جایگاه ریسک‌های فناوری اطلاعات

ریسک فناوری اطلاعات، نوعی از ریسک کسب‌وکار است که مشخصا با به کارگیری، مالکیت، عملیاتی‌سازی، تاثیرپذیری یا در ارتباط با فناوری اطلاعات معنی پیدا می‌کند. این نوع از ریسک‌ها شامل رخدادهای مرتبط با فناوری اطلاعات است که می‌تواند به نحوی بر کسب‌وکار تاثیر بگذارد. هم احتمال رخداد این نوع از ریسک‌ها و هم میزان تبعات ناشی از آن، با عدم قطعیت مواجه است، اما به هر حال می‌تواند بر رسیدن سازمان به اهداف راهبردی و نیز بر امور روزمره سازمان تاثیر بگذارد. ریسک‌های فناوری اطلاعات را می‌توان به گونه‌های مختلف طبقه بندی کرد (شکل ۱) (۲).

فرایندهای فناوری اطلاعات از تدوین استراتژی‌ها و مشخص کردن سبد پروژه‌ها، اجرای پروژه‌ها، نگهداشت زیرساخت‌های نرم‌افزاری و سخت‌افزاری و پشتیبانی نرم‌افزارها، در هر یک از مراحل می‌تواند در معرض ریسک‌های مختلف قرار گیرد که باید به نحو مناسب مورد توجه قرار گیرند.

شکل ۱- طبقه‌بندی ریسک‌های فناوری اطلاعات



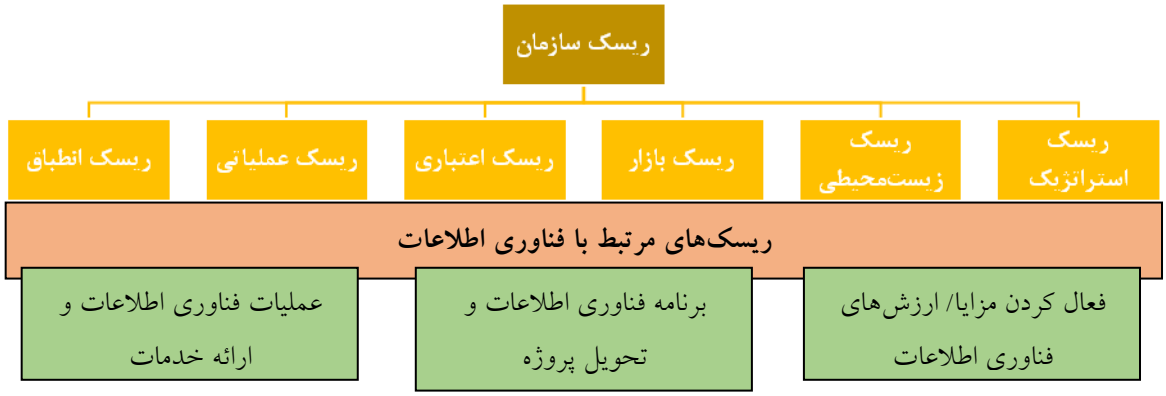
همانگونه که در این شکل ۱ ملاحظه می‌شود، ریسک‌های فناوری اطلاعات در سه سطح می‌تواند بر سازمان تاثیر بگذارد:

- لایه راهبردی: ریسک‌های فناوری اطلاعات در این سطح می‌تواند منجر به از دست رفتن فرصت‌های استفاده از تکنولوژی برای بهبود و ارتقای بهره‌وری و اثربخشی در فرایندهای سازمانی و ایجاد نوآوری در سازمان شوند.
- لایه طرح و پروژه: در این سطح ریسک‌های فناوری اطلاعات بر تعریف و اجرای پروژه‌های بهبود راهکارهای کسب‌وکار که معمولا در قالب تعدادی طرح و پروژه در سازمان تعریف می‌شود، اثر می‌گذارد.
- ریسک‌های لایه عملیاتی و پشتیبانی: در این سطح برقرار و عملیاتی بودن سامانه‌های اطلاعاتی شرکت مد نظر قرار دارد. بنابراین هر گونه اختلال در این سرویس‌ها باعث ایجاد اختلال در عملیات روزمره سازمان و کاهش بهره‌وری می‌شود.

ریسک‌های فناوری اطلاعات بخشی از دنیای ریسک‌ها در سازمان به شمار می‌آیند. سایر ریسک‌ها در سازمان شامل ریسک‌های راهبردی، ریسک‌های محیطی، ریسک بازار، ریسک‌های اعتباری، ریسک‌های عملیاتی و ریسک‌های انطباق (با مقررات) هستند. در برخی از چارچوب‌ها نظیر Basel II برای موسسات مالی، ریسک‌های فناوری اطلاعات زیر مجموعه ریسک‌های عملیاتی طبقه‌بندی شده است؛ اما نگاهی دقیق‌تر، نشان می‌دهد که فناوری اطلاعات حتی می‌تواند به عنوان بخشی از ریسک‌های استراتژیک نیز طبقه‌بندی شود، به ویژه در سازمان‌هایی نظیر شرکت‌های بیمه که وابستگی شدیدی به فناوری اطلاعات و سامانه‌ها و زیرساخت‌های فناوری اطلاعات دارند. این ریسک‌ها حتی می‌توانند به عنوان بخشی از ریسک‌های اعتباری نیز تلقی شوند، از آنجا که ضعف در سامانه‌های اطلاعاتی و به ویژه امنیت این سامانه‌ها، معمولا باعث کاهش رتبه اعتباری شرکت‌ها می‌شود.

با توجه به همپوشانی ریسک‌های فناوری اطلاعات در چارچوبی نظیر ISACA، ریسک‌های مرتبط با فاوا به عنوان یک جزء در ساختار سلسله مراتبی در کنار سایر موارد قرار نگرفته است، بلکه به عنوان یک لایه مجزا که با همه موارد می تواند همپوشانی داشته باشد، دیده شده است (شکل ۲).

شکل ۲- ریسک فناوری اطلاعات در سلسله مراتب ریسک



۲- چارچوب‌های موجود برای مدیریت ریسک فناوری اطلاعات

۲-۱- چارچوب ISACA

انجمن ISACA چارچوبی را به عنوان راهنمای حکمرانی فناوری اطلاعات[۲] ارائه داده است تا به سازمان‌ها کمک کند که ساختار و فرایندهای فناوری اطلاعات خود را به نحو مطلوب سازماندهی کنند. همچنین راهنمای جامعی در خصوص ریسک‌های فناوری اطلاعات ارائه کرده است.

چارچوب Risk IT بر مبنای چارچوبها و استانداردهای مدیریت ریسک‌های سازمانی[۳] نظیر COSO ERM و AS/NZS 4360 (جایگزین ایزو ۳۱۰۰۰) طراحی شده است. این چارچوب علاوه بر ارائه مفاهیم پایه مدیریت ریسک‌های فناوری اطلاعات، روش‌ها و تکنیک هایی برای مدیریت این ریسک‌ها ارائه داده است. اجزای مدل فرایند جامع این چارچوب

[2] IT Governance
[3] Enterprise Risk Management (ERM)

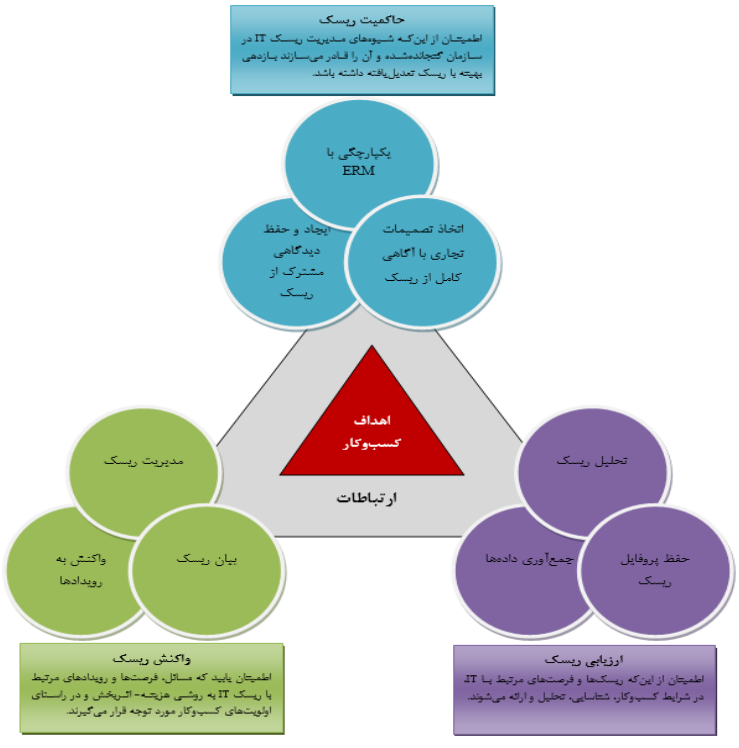
مشابه COBIT و Val IT طراحی شده است تا برای افرادی که با این چارچوب‌ها آشنایی دارند، قابل فهم تر باشد. مدل فرایندی به سه حوزه حاکمیت ریسک، ارزیابی ریسک و پاسخ ریسک تقسیم می‌شود (جدول ۱).

جدول ۱- مدل فرایند جامع چارچوب ریسک Risk IT

حوزه	فرایند
حاکمیت ریسک[۴]	تدوین و پشتیبانی از یک دید مشترک از ریسک
	یکپارچگی با ERM
	تصمیم گیری‌های سازمانی مبتنی بر ریسک
ارزیابی ریسک	جمع آوری داده ها
	تحلیل ریسک
	نگهداری پروفایل ریسک
مواجهه با ریسک	تفصیل ریسک
	مدیریت ریسک
	پاسخ مناسب به رخدادها

مدل فرایندی جامع چارچوب Risk IT در شکل ۳ نشان داده شده است. همانگونه که در این شکل مشخص است، فعالیت‌های اصلی در قالب تعدادی فرایند مشخص شده که این فرایندها به سه حوزه اصلی تقسیم می‌شوند. برای هر فرایند، راهنمای انجام، مسئولیت‌ها، گردش اطلاعات بین فرایندها و مدیریت کارآیی فرایندها در چارچوب ذکر شده است.

شکل ۳- مدل فرایندی جامع چارچوب Risk IT



[4] Risk Governance

سه حوزه اصلی در این چارچوب شامل حاکمیت ریسک، ارزیابی ریسک و مواجهه با ریسک است که هر یک از سه فرایند تشکیل می‌شوند.

نقش‌های مدیریت ریسک	دید مشترک ریسک	یکپارچگی با ERM	تصمیم گیری مبتنی بر ریسک	جمع آوری داده ها	آنالیز ریسک	نگهداشت پروفایل ریسک	ریسک	مدیریت ریسک	مواجهه با ریسک
هیات مدیره و مدیرعامل									
مدیریت ریسک									
مدیریت فناوری اطلاعات									
مدیریت مالی									
کمیته ریسک سازمان									
مدیریت کسب و کار									
مالک فرایندهای کسب و کار									
حوزه‌های تخصصی (امنیت شبکه، ...)									
منابع انسانی									

	نقشی که مسئولیت آن بخش را به عهده دارد و پاسخگوی بخشی از امور مربوطه است.
	نقشی که پاسخگوی اصلی ان بخش است.

۲-۲- ایزو ۳۱۰۰۰

در سال ۲۰۰۹، سازمان بین‌المللی استانداردها، ایزوی مدیریت ریسک را با شماره ۳۱۰۰۰ منتشر کرد که بر مبنای رویکردهای ملی استرالیا و نیوزیلند (یعنی AS/NZS 4360:2004) و نیز اتریش (یعنی ONR 49000:2004) بود. این استاندارد به سطح جهانی تکامل یافت و تا امروز گسترده‌ترین پذیرش را داشته است. ایزو ۳۱۰۰۰، به سبب رویکرد عمومی و صریحش، صرف نظر از نوع، منظر و اندازه سازمان، می‌تواند برای هر نوع سازمانی به کار گرفته شود. ایزو ۳۱۰۰۰ به عنوان یک خانواده استاندارد سازماندهی شده و متشکل از هفت عنصر است که بر جنبه‌های مختلفی تمرکز دارند:

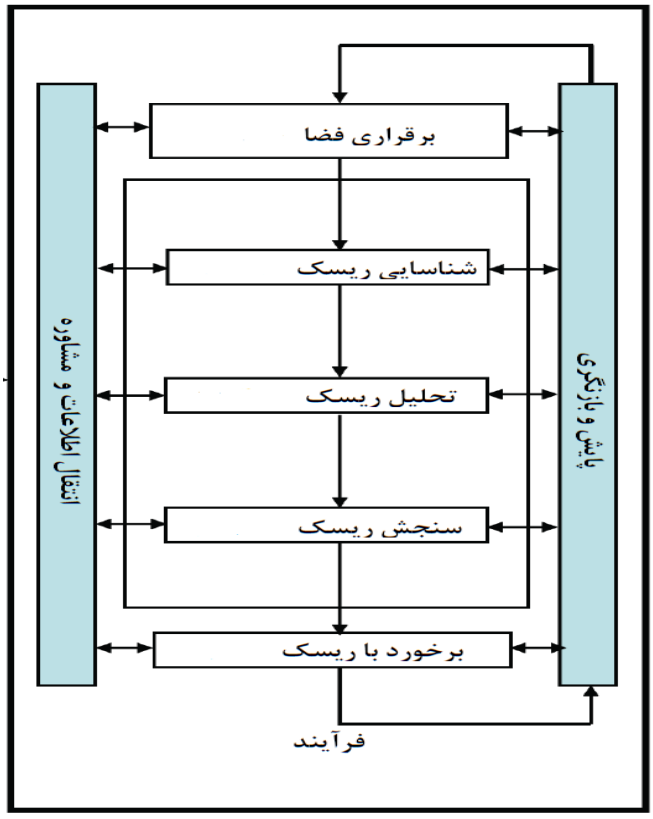
- راهنمای ایزوی ۵۷۳: لغت‌نامه مدیریت ریسک (۲۰۰۹)- همه تعاریف و اصطلاحات در آن رده‌بندی شده است.
- ایزو ۳۱۰۰۰: اصول و رهنمودها- این استاندارد، اصول بنیادی و رهنمودهای کلی برای مدیریت ریسک را ارائه می‌کند.
- ایزو ۳۱۰۰٤: راهنمای اجرای ایزو ۳۱۰۰۰- درباره مفاهیم و اصول، با جزییات بحث می‌کند.
- ایزو ۳۱۰۱۰: تکنیک‌های ارزیابی ریسک- رویه‌های منتخب برای ارزیابی ریسک را معرفی و درباره احتمالات به‌کارگیری آن‌ها بحث می‌کند.
- ایزو ۳۱۰۲۰- مدیریت ریسک‌های مرتبط با عدم‌النفع (توقف کسب‌وکار).

[5] ISO Guide 73

- ایزو ۳۱۰۲۱- مدیریت ریسک زنجیره تامین.

نمایی از چارچوب ایزو ۳۱۰۰۰، در شکل ٤ قابل مشاهده است.

شکل ٤- چارچوب ایزو ۳۱۰۰۰



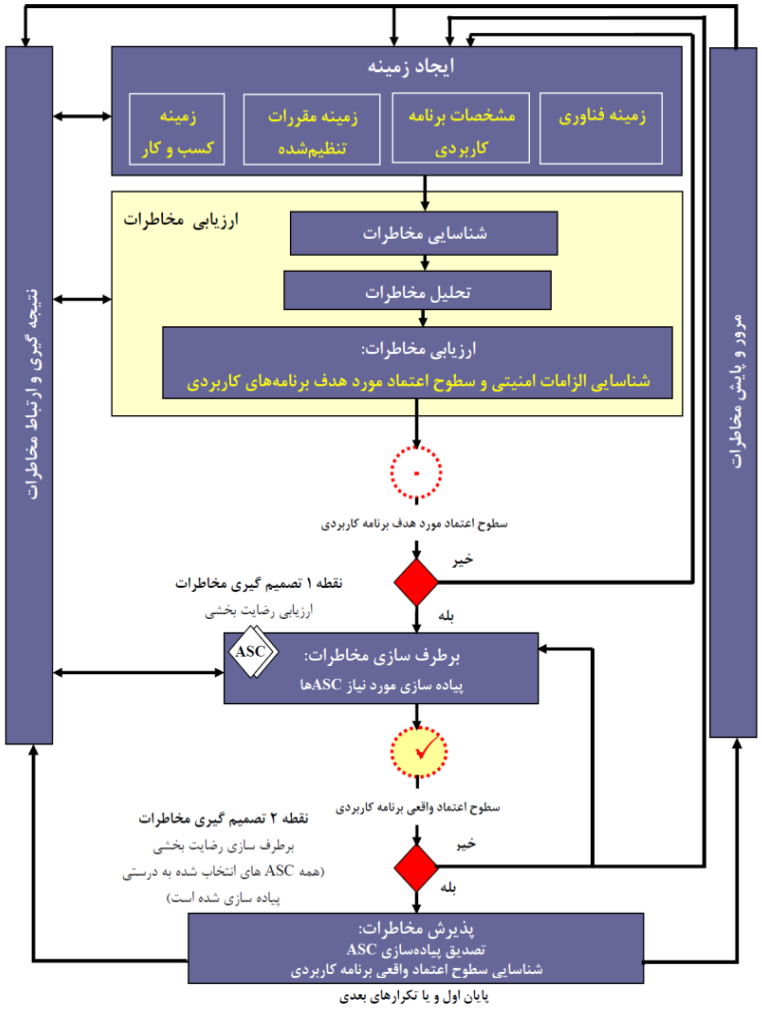
منبع: (۳)

۲-۳- مدل ایزو ۲۷۰۰۵: مدیریت ریسک امنیت اطلاعات

ایزو ۲۷۰۰۵ بخشی از خانواده استاندارد ایزو ۲۷۰۰۰ است که به حوزه امنیت اطلاعات و اجرای سیستم‌های مدیریت مرتبط با این حوزه در سازمان‌های مختلف می‌پردازد. این استاندارد، یک فرایند مبسوط مدیریت ریسک را ارائه می‌کند که به‌طور خاص با الزامات امنیت اطلاعات انطباق دارند. بنابراین، پنج گام اصلی که قبلا در ایزو ۳۱۰۰۰ آمده است را برای امنیت اطلاعات اجرا می‌کند. البته، علاوه بر پنج گام عمومی ایزو ۳۱۰۰۰، یک گام دیگر هم به نام «پذیرش ریسک» و دو نقطه تصمیم (رضایت‌بخشی ارزیابی و رضایت‌بخشی برطرف‌سازی[6]) نیز در آن وجود دارند (٤). نمای کلی ایزو ۲۷۰۰۵ در شکل ۵ نمایش داده شده است.

[6] treatment

شکل۵- چارچوب ایزو ۲۷۰۰۵



منبع: (۵)

۲-٤- مدل COSO

مدل کوزو[7] برای مدیریت یکپارچه ریسک‌های سازمان، اهداف سازمان را در ٤ سطح راهبردی، عملیاتی، گزارش‌گری و تطابق با مقررات لحاظ می‌کند که هر یک در سطوح سازمان، شعبه، بخش (واحد) و زیرواحد تقسیم‌بندی می‌شوند. فعالیت‌های مدیریت ریسک نیز از ۸ مرحله کلیدی محیط داخلی (آماده کردن فرهنگ سازمانی ریسک)، مشخص کردن اهداف، شناسایی وقایع، ارزیابی ریسک، پاسخ به ریسک، فعالیت‌های کنترلی، ارتباطات و اطلاع رسانی و پایش تشکیل می‌شود.

[7] COSO

شکل ۵- مدل کوزو

نقش‌های اصلی متولی مدیریت ریسک در این مدل شامل هیات مدیره، مدیران، دفتر (مدیریت) ریسک و حسابرسی داخلی است. اگر چه حسابرسی داخلی در این مدل مسئولیت مستقیم به عهده ندارد اما از طریق ارزیابی، پایش، آزمون، گزارش گری می‌تواند به هیئت مدیره شرکت کمک قابل توجهی کند. مدل کوزو تاکید زیادی روی حسابرسی داخلی دارد و مستندات تکمیلی در این خصوص ارائه داده است.

۲-۵- بازل ۲

کمیته بازل از مهم‌ترین ارکان تدوین مقررات نظارتی در حوزه بانکداری و هولدینگ‌های مالی است که قوانین و استانداردهای آن، بانک‌ها و شرکت‌های زیرمجموعه گروه‌های مالی را هدف قرار داده است. مقررات بازل در جهت فراهم آوردن شرایطی است که چنین موسساتی بتوانند به سلامت بحران‌های مالی را پشت سر بگذارند و از تضمین کافی برای بقا برخوردار باشند. مقررات آکورد بازل ۲۸ شامل ۳ محور کلیدی است: الزامات کفایت سرمایه، نظارت موثر و ضوابط بازار (شفافیت برای مشتریان). محور ۱ بازل شامل ریسک‌های اعتباری، عملیاتی و بازار می‌شود که خود ریسک‌های عملیاتی شامل ریسک‌های فناوری اطلاعات نیز هستند. طبق مقررات بازل ۲، ۷ گروه از رخدادها برشمرده شده که همگی در حوزه فناوری اطلاعات نیز مورد توجه هستند:

- تقلب داخلی: سوء استفاده از موقعیت یا دارایی‌ها، رشوه، فرار مالیاتی
- تقلب بیرونی: سرقت اطلاعات، خسارت‌های ناشی از رخنه در سیستم‌ها
- کارکنان و ایمنی محیط کار: تبعیض، سلامت و ایمنی کارکنان
- مشتریان، محصولات و امور تجاری: دستکاری در بازار، اقدامات انحصارگرایانه، تجارت نادرست، نقص محصول، نقض امانتداری
- خسارت به دارایی‌های فیزیکی: بلایای طبیعی، تروریسم و خرابکاری
- خرابی سیستم‌ها و اختلال در امور جاری: ایجاد اختلال در سرویس، خرابی نرم‌افزار، خرابی سخت‌افزار
- اجرا، تحویل و مدیریت فرآیند: خطاهای ورود اطلاعات، خطاهای حسابداری، اشکال در گزارش‌های اجباری، سهل انگاری در حفظ دارایی‌های مشتری

[8] Basel III Accord

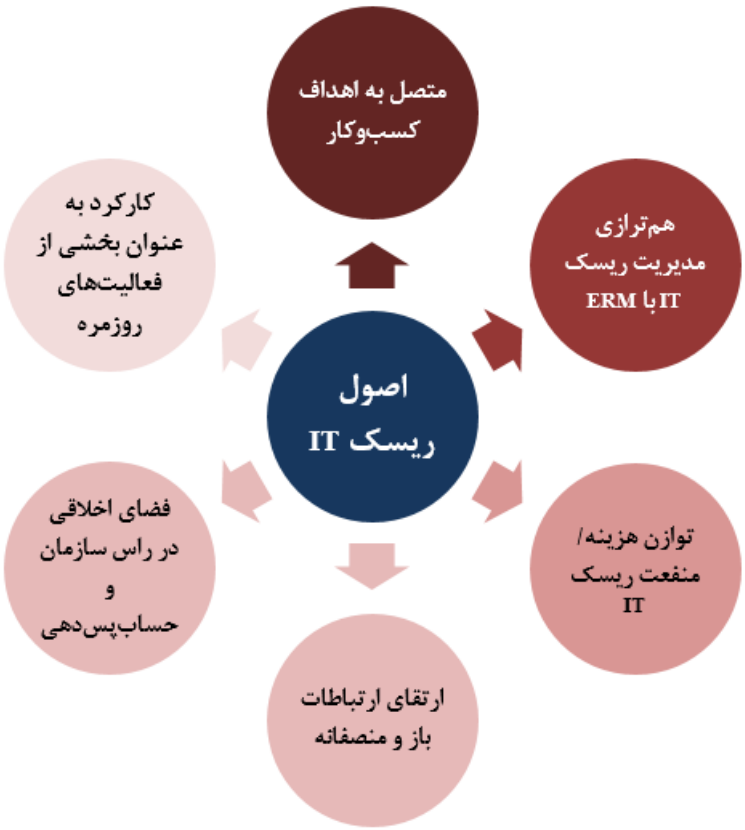
از آنجا که کمیته بازل اصولا از نهادهای نظارتی تشکیل شده است، لذا تمرکز آن به وضوح بر وظایف نهادهای ناظر قرار دارد و تکالیف متعددی را جهت ارزیابی مستمر ریسک‌های موسسات بر عهده نهادهای نظارتی قرار می‌دهد. به عنوان مثال در اولین بند از وظایف نهاد ناظر تاکید دارد که نهاد ناظر باید به صورت مستقیم و غیرمستقیم و به‌طور منظم، ارزیابی مستقل از سیاست‌ها، فرایندها و سیستم‌های بانک‌ها در خصوص ریسک‌های عملیاتی انجام دهد. همچنین نهاد ناظر باید اطمینان حاصل نماید که سازوکارهای لازم جهت اطلاع از هرگونه تحولی در موسسات (بانک‌ها) وجود داشته باشد. از آنجا که عموما بانک‌ها عضوی از یک گروه مالی هستند و دارای شرکت‌های مرتبط نظیر شرکت‌های بیمه هستند، این استاندارد شرکت‌های مرتبط با بانک‌ها را نیز شامل می‌شود.

۳- مدل پیشنهادی برای شرکت‌های بیمه

۳-۱- اصول مدیریت ریسک فناوری اطلاعات در شرکت‌های بیمه

اصول مدیریت ریسک فناوری اطلاعات، بر مبنای اصول رایج پذیرفته‌شده مدیریت ریسک سازمانی است که برای دامنه فناوری اطلاعات هم به کار می‌رفته‌اند. این مدل طراحی و ساختاربندی شده است تا سازمان‌ها را قادر سازد این اصول را در عمل به کار گیرند و عملکرد خود را بهینه‌کاوی کنند.

شکل ٦- اصول مدیریت ریسک فناوری اطلاعات



۳-۲- ساختار ریسک‌های فناوری اطلاعات

بر اساس دیدگاه معماری سازمانی و با الگو گرفتن از چارچوب‌های متداول آن نظیر زکمن و توگف و نیز با نیم نگاهی به چارچوب مدیریت خدمات فناوری اطلاعات نظیر ITIL و ITSM، می‌توان بخش‌های ساختاری ریسک‌های فناوری اطلاعات را مطابق جدول ۲ مد نظر قرار داد:

جدول ۲- بخش‌های ساختاری ریسک‌های فناوری اطلاعات

طبقه بندی ریسک‌های فناوری اطلاعات	توضیح
ریسک‌های لایه استراتژی	ریسک‌های ناشی از ناتوانی فناوری اطلاعات در برآورده ساختن نیازهای استراتژیک شرکت و تحقق استراتژی‌های کلان شرکت.
ریسک‌های مبتنی بر افراد	ریسک‌های ناشی از افراد، نظیر استعفای کارکنان کلیدی یا خرابکاری‌های عمدی یا سهوی توسط کارکنان.
ریسک‌های مبتنی بر فرایندها	ریسک‌های ناشی از مشکلات فرایندی در حوزه فناوری اطلاعات نظیر تحلیل ناقص سیستم‌ها، فرایندهای ناکارآمد پشتیبانی و نظایر آن.
ریسک‌های تکنولوژی	ریسک‌های ناشی از به‌کارگیری تکنولوژی‌های خاص (نظیر تکنولوژی خیلی جدید یا خیلی قدیمی).
ریسک‌های زیرساخت	ریسک‌های مربوط به زیرساخت نظیر زیرساخت فیزیکی مرکز داده یا زیرساخت ارتباطی شرکت. ریسک‌های ناشی از بلایای طبیعی نیز در این رده تقسیم بندی می‌شود.
ریسک‌های پروژه محور	ریسک‌های مبتنی بر پروژه نظیر عدم اتمام به موقع پروژه‌ها (این ریسک‌ها را می‌توان بر مبنای PMBOK مورد بررسی قرار داد).
ریسک‌های ناشی از حکمرانی داده	ریسک‌های مرتبط با داده تنوع زیادی داشته و خود به گونه‌های مختلف تقسیم می‌شود، نظیر ریسک لورفتن اطلاعات مشتریان یا اطلاعات حساس شرکت که به عنوان نمونه در اتحادیه اروپا قوانین مشخصی در این خصوص تحت عنوان GDPR وضع شده است. ریسک‌های ناشی از کیفیت پایین داده‌ها، داده‌های مخدوش، تکراری یا نامعتبر و نظایر آن. این ریسک‌ها را می‌توان به کمک DMBOK به طور دقیق مورد ارزیابی قرار داد.
ریسک‌های امنیتی	این ریسک‌ها به امنیت سیستم‌ها و نفوذناپذیری سامانه‌های شرکت‌های بیمه بر می‌گردد. استانداردهای امنیت اطلاعات نظیر ISMS و ایزو ۲۷۰۰۱ در این خصوص می‌تواند مد نظر قرار گیرد.
ریسک‌های مرتبط با زمان	عدم رعایت محدودیت‌های زمانی در سامانه‌های شرکت نظیر آماده نشدن اطلاعات یا گزارش‌ها در زمان مقرر یا عدم ارائه سرویس‌ها مطابق زمانبندی یا عدم پاسخگویی در زمان منطقی.
ریسک‌های کیفی	ریسک‌های کیفی به کیفیت پایین خدمات و سامانه‌های فناوری اطلاعات باز می‌گردد. مشخصه‌های کیفی سیستم‌ها مواردی نظیر سرعت، در دسترس بودن (عدم قطعی سیستم)، قابل اتکا بودن و نظایر آن را شامل می‌شود.

لازم به ذکر است جدول فوق به منظور تفکیک بهتر ریسک‌های فناوری اطلاعات تنظیم شده است و ممکن است تا حدی بین برخی از طبقات همپوشانی نیز وجود داشته باشد.

۳-۳- وظایف

جدول ۳- وظایف هر یک از نقش‌های مدیریت ریسک

نقش‌های مدیریت ریسک	دید مشترک ریسک
نهاد ناظر (بیمه مرکزی ج. ا. ا.)	تدوین استاندارد مدیریت ریسک شرکت‌های بیمه، الزام ملزومات (ساختار، فرایند) مدیریت ریسک‌های فناوری اطلاعات، ممیزی منظم ادواری ریسک‌های فناوری اطلاعات.
هیات مدیره و مدیرعامل	تهیه و ابلاغ سیاست‌های مدیریت ریسک‌های فناوری اطلاعات، حصول اطمینان از رعایت کلیه مقررات در حوزه مدیریت ریسک، ارزیابی و نظارت مستمر.
مدیریت ریسک	تهیه برنامه جامع مدیریت ریسک‌های فناوری اطلاعات، ممیزی ادواری و گزارش به هیئت مدیره.
مدیریت فناوری اطلاعات	شناسایی، طبقه بندی، و ارزیابی ریسک‌های فناوری اطلاعات در هر یک از طبقات مذکور در جدول ... و برنامه ریزی مناسب جهت مدیریت و مواجهه هر یک از ریسک ها. تشکیل کارگروه‌های تخصصی برای هر یک از انواع ریسک و پیش بینی نفرات و ساختار لازم به عنوان مثال در خصوص ریسک‌های امنیت اطلاعات.
مدیریت مالی	
مالک فرایندهای کسب و کار	همکاری در شناسایی و طبقه بندی ریسک‌های فناوری اطلاعات در هر یک از مدیریت‌ها و بخش‌های سازمان نظیر بیمه‌های زندگی. شناسایی تبعات احتمالی هر یک از ریسک‌ها بر آن واحد.
حوزه‌های تخصصی(امنیت شبکه، ...)	برنامه ریزی دقیق برای مدیریت ریسک در حوزه‌های تخصصی نظیر مدیریت داده، امنیت اطلاعات، امنیت شبکه، تداوم کسب و کار و ... .
منابع انسانی	برنامه ریزی جهت کاهش ریسک‌های مرتبط با منابع انسانی، ارزیابی مستمر وضعیت.

٤- جمع‌بندی

در این مقاله مروری انجام شد بر جایگاه ریسک‌های فناوری اطلاعات در میان ریسک‌های سازمانی شرکت‌های بیمه و سپس مدل‌ها و چارچوب‌های استاندارد را در این زمینه مورد مطالعه اجمالی قرار گرفتند. در نهایت ضمن مقایسه این چارچوب‌ها، تجربیاتی را از میان مدل‌های موجود جهت اجرا در شرکت‌های بیمه پیشنهاد نمودیم. این پیشنهاد هم شامل مدل فرایندی و هم تقسیم وظایف سطح بالا می‌شود. شرکت‌های بیمه می‌توانند این مدل را به کمک مدل‌های مرجع ذکر شده پیاده‌سازی و اجرا نمایند. به عبارتی جزئیات هر یک از گام‌ها در مستندات مذکور موجود بوده و می‌توان به آن رجوع نمود.

با این حال، تجربیات بین‌المللی در خصوص موسسات مالی نشان می‌دهد که نهاد ناظر در موضوع ریسک به طور عام و ریسک‌های فناوری اطلاعات به طور خاص وارد شده و مقرراتی را در این خصوص وضع و بر اجرای آن نظارت می‌کند. این مقررات می‌تواند نظیر بازل ۳، ریسک‌های سیستماتیک را مورد توجه قرار دهد یا نظیر مقررات حفاظت از داده‌ها که

نمونه آن مقررات GDPR اتحادیه اروپا است، بر حوزه خاص اطلاعات محرمانه اشخاص تمرکز نماید. قوانین مشابهی در صنعت بانکداری تحت عنوان PSD II برای حفظ اطلاعات مشتریان وضع شده است. از این رو نهاد ناظر صنعت بیمه می‌تواند به موضوع ریسک‌های فناوری اطلاعات نیز وارد شده و مقررات و تکالیف شفافی را در این خصوص وضع نماید. همچنین سنجش و پایش مستمر و دوره ای میزان پایبندی شرکت‌ها به این برنامه‌ها را نیز در دستور کار خود قرار دهد.

لزوما همه انواع ریسک فناوری اطلاعات که در جدول ۲ ارائه گردید از نظر نهاد ناظر دارای اهمیت نیستند. به عنوان مثال ریسک پروژه، صرفا باعث می‌شود شرکت نتواند به موقع طرح‌های توسعه‌ای خود را اجرا نماید که حوزه آن محدود به خود شرکت می‌باشد. اما برخی از ریسک‌ها دامنه‌ای فراتر داشته و مورد توجه نهاد ناظر صنعت بیمه است. به عنوان نمونه، انجمن نهادهای ناظر بیمه IAIS در دستورالعمل بنیادی ۱۶ موضوع ریسک‌های سازمانی را مورد توجه قرار داده است و از آن میان به طور خاص بند ۱۵ این دستورالعمل به موضوع فناوری اطلاعات گره می‌خورد. بند ۱۵ موضوع برنامه بازیابی است که به عنوان جزئی از برنامه تداوم کسب و کار باید مد نظر قرار گیرد. برنامه تداوم کسب‌وکار سعی می‌کند تضمین نماید که تحت هر شرایطی و با وقوع هر اتفاق پیش بینی نشده، چگونه شرکت بیمه می‌تواند به بقای خود ادامه دهد. این موضوع هم در سطح کلان و هم در حوزه فناوری اطلاعات باید مد نظر قرار گیرد. به عنوان مثال در صورت آتش‌سوزی در ساختمان مرکزی شرکت یا دیتاسنتر اصلی شرکت، با چه برنامه‌ای شرکت خواهد توانست فعالیت‌های خود را ادامه دهد و با بحران جدی مواجه نشود.

علاوه بر ریسک‌های مربوط به تداوم کسب‌وکار، ریسک‌های وابسته به حفظ اطلاعات شخصی افراد نیز معمولا مورد توجه نهاد ناظر قرار می‌گیرد. معمولا قوانین سختگیرانه‌ای در این زمینه وضع می‌شود. برخی از این قوانین عمومیت داشته و مختص یک صنعت خاص نیستند، مانند قانون GDPR اروپا، در حالی که برخی از قوانین دقیقا یک صنعت خاص را مد نظر قرار می‌دهد، مانند قانون حفظ اطلاعات کارت‌های پرداخت بانکی. از این رو نهادهای ناظر به موضوع حفظ حریم شخصی افراد و نحوه نگهداری و طبقه بندی اطلاعات افراد به عنوان بخشی از وظیفه حاکمیتی خود می‌نگرند.

فهرست منابع

۱. Buehler K, Carpineti M, Michel-Kerjan E, Nauck F, Serino L. The value for insurers in better management of nonfinancial risk McKinsey; 2019 [Available from: https://www.mckinsey.com/business-functions/risk/our-insights/the-value-for-insurers-in-better-management-of-nonfinancial-risk.

۲. ISACA. THE RISK IT FRAMEWORK. USA: Information Systems Audit and Control Association; 2009.

۳. سازمان‌ملی‌استانداردایران. مدیریت ریسک- اصول و رهنمودها. ۱۳۸۹,

۴. EuropeanCommission. Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative risk manaGement tools for critical information infrAstrucTrurEs. **European Commission**.۲۰۱۸

۵. سازمان‌ملی‌استانداردایران. ایزو ۲۷۰۰۵. ۱۳۹۲.