

نقش آینده‌ی حسابرسة داخلی در مدیریت ریسک

جان شورترید، جان فریزر، گرانت پاردي، آرنولد شان‌فیلد
ترجمه: مرتضی اسدی، نیلوفر اصغری

راهنمای عملی و به‌روزشده‌ای را برای کلیه‌ی سازمان‌ها، اعم از خصوصی و عمومی، به منظور بهبود و افزایش توانایی سازمان‌ها در مدیریت ریسک فراهم می‌کند. تدوین استانداردهای فوق براساس استانداردهای اولیه‌ی مدیریت ریسک و نیز موفقیت‌های عملی سازمان‌هایی چون گروه صنعتی هایدرو وان^۲ و بی. ایچ. پی. بیلیتون^۳ که از روش‌های فوق بهره گرفتند، صورت پذیرفته است. گروه صنعتی هایدرو وان برای اجرای مدیریت ریسک سازمانی (ERM)^۴، نسخه‌ی قدیمی ایزو ۳۱۰۰۰ را در سال ۲۰۰۰ با به‌کارگیری استاندارد مدیریت ریسک ۴۳۶۰ AS/NZS به عنوان الگو شروع کرد. موفقیت‌ها و چالش‌های مدیریت ریسک آن‌ها به خوبی مستندسازی شده است.^۵ مدل آن‌ها که عمدتاً بر پایه‌ی استفاده از کارگاه‌های آموزشی ریسک، اولویت‌بندی ریسک‌ها و تخصیص منابع قرار دارد، بر اساس مدلی آسان اما کارآمد عمل می‌کند. رییس اجرایی حسابرسة (داخلی)، کارکنان واحدهای حسابرسة (داخلی) و مدیریت ریسک را از یکدیگر تفکیک کرده و برای انطباق با روش‌های پذیرفته‌شده‌ی مشارکت حسابرسة داخلی در اجرای مدیریت ریسک سازمانی توسط انجمن حسابرسة داخلی دو رویه‌ی متفاوت را در پیش می‌گیرد (IIA، ۲۰۰۴ و ۲۰۱۱). مدل گروه

حسابرسة داخلی در مسیری قرار دارد که به‌منظور رویارویی با الزامات قانونی جدید برای راهبری شرکتی و استانداردهای جدید مدیریت ریسک، در چند سال آینده نیاز خواهد داشت در روش‌ها، ابزار و تکنیک‌های سنتی خود تغییراتی ایجاد کند. این الزامات جدید به‌گونه‌ای طراحی شده‌اند تا اطمینان بیش‌تری از توانایی سازمان در مدیریت ریسک فراهم شود، از این‌رو، تغییرات عمده‌ای در عملکرد حسابرسة داخلی و حمایت هیأت مدیره از آن را می‌طلبد.

رویدادهای ناگوار اقتصادی و اجتماعی همچون رسوایی انرون، بحران بانکی سال ۲۰۰۸، توفان کاترینا، بحران ناشی از زباله‌های نفتی بریتیش پترولیوم در اقیانوس، رسوایی شرکت الیمپوس، بحران مالی یونان و غیره، بارها رخ داده است. چنین روایدهایی ناشی از فقر راهبری در سازمان‌های خصوصی و دولتی است. بخش عمده‌ی شکست راهبری ناشی از مدیریت نامناسب ریسک است. (برای مثال، نظارت ناکارآمد حسابرسة داخلی).

رهنمودهای بین‌المللی مدیریت ریسک در ایزو ۳۱۰۰۰ سال ۲۰۰۹،^۱ با عنوان "مدیریت ریسک: اصول و رهنمودها"، به صورت استاندارد تدوین شد. این استاندارد

1-International Organization for Standardization (ISO) 31000,2009

2-Hydro One

3-BHP Billiton

4-Enterprise Risk Management (ERM)

5-Simkins 2004, Mikes 2008 and 2009

بهبود اثربخشی هر دوی مدیریت ریسک و راهبری سازمان تکنیک‌های جدیدی را توسعه بخشند؛

۴. به منظور رویارویی با نوآوری، چالش‌های مهم و گسترده با همکاران خود در سراسر جهان برای تغییر در الزامات، آموزش و عملکرد حسابرسان داخلی همکاری کنند. تردیدی نیست که نقش‌های جدید برای حسابرسی داخلی همانند نقش‌های سنتی باید مورد نظارت قرار گیرد تا از همخوانی عملکرد با انتظارات اطمینان حاصل شود. همچنین به منظور اطمینان بخشی به سهامداران، الزام کلیدی ایزو ۳۱۰۰۰، داشتن رویکردهای صریح و روشن برای ارتباطات داخلی و خارجی لازم و ضروری خواهد بود. ایزو ۳۱۰۰۰ راهنمایی مورد نیاز در این زمینه را فراهم می‌کند.

در این مقاله الزامات راهبری جدید، آخرین استانداردهای مدیریت ریسک و مفاهیم حسابرسی داخلی بررسی می‌شود. در ادامه، نتیجه‌گیری‌های اصلی مقاله با (قلم) ایتالیک در متن، نشان داده شده است.

۲. مدیریت ریسک و سازمان‌ها - گرایش‌های جدید

در زمینه‌ی مفاهیم ریسک و تمهیدات کلی مدیریت ریسک در سازمان‌ها اخیراً پیشرفت‌ها و جهت‌گیری‌هایی صورت گرفته است که تأثیر بسیار بر فعالیت حسابرسی داخلی می‌گذارد.

۱.۲ فواید ریسک کردن

در حال حاضر ریسک به عنوان "تأثیر عدم اطمینان در دستیابی به اهداف" در نظر گرفته می‌شود (ایزو ۲۰۰۹). ریسک می‌تواند با هر یک از پیامدهای مثبت یا منفی یا هر دوی آن‌ها مشخص شود و این پیامدها را باید با اهداف سازمان مرتبط ساخت. به عنوان مثال، نتایج سودمند

صنعتی هایدرو وان بالاترین منابع ریسک را مشخص کرده و برای بازنگری و چاره‌اندیشی آن را به مدیریت ارشد و هیأت مدیره ارائه می‌دهد. معیارهای ریسک در سطح هیأت مدیره به عنوان مبنایی برای تشخیص، تحلیل و ارزیابی ریسک تعیین شده و بر سر آن توافق شده است. حسابرسی داخلی از این ریسک مدون شده به عنوان مبنایی حائز اهمیت برای برنامه‌ریزی حسابرسی داخلی بهره می‌گیرد. به‌تازگی، بسیاری از کشورهای بزرگ، مقررات و آیین‌نامه‌هایی برای راهبری شرکتی تعریف کرده‌اند (برای مثال کینگ III^۱ در آفریقای جنوبی، مقررات ترکیبی^۲ در بریتانیا و بورس اوراق بهادار در استرالیا). همه‌ی این موارد نیازمند آن است که اطلاعات کافی برای هیأت مدیره‌ی سازمان فراهم شده باشد تا بتواند برای سهام‌داران به صورت مستند اجرای مؤثر مدیریت ریسک را بیان کند و یا در غیر این صورت (در صورت عدم اجرای اثربخش مدیریت ریسک) ضعف‌های آن را افشا سازد. عموماً هیأت مدیره ملزم به افشای موارد زیر هستند (مدیران بورس اوراق بهادار کانادا^۳، ۲۰۱۰):

- اطلاعات درباره‌ی ریسک‌های ناشر و اشاره به مهم‌ترین آن‌ها؛
- مشاوره در مورد چگونگی یکپارچه‌شدن مدیریت ریسک با دیگر فرایندهای تجاری مهم سازمان به‌ویژه مدیریت راهبردی؛^۴
- سیاست سازمان در برخورد با مدیریت ریسک؛ و
- ارزیابی هیأت مدیره از اثر بخشی سیاست‌ها و روش‌های مدیریت ریسک، شامل چارچوب و فرایند مدیریت ریسک.

این تغییرات به پاسخ مناسب حرفه‌ی حسابرسی داخلی در این زمینه‌ها نیاز دارد:

۱. ایفا کننده‌ی نقشی در مدیریت ریسک باشند، نه این‌که به صورت مستقل تلاش‌های مدیریت را نظاره کنند؛
۲. با اطمینان بخشی از اعمال کنترل‌های مربوط به نقاط بحرانی از مدیریت ریسک پشتیبانی کنند؛
۳. به منظور نظارت، بررسی و ارتباطات با هدف

1-King III

2-Combined Code

3-Canadian Securities Administrators

4-Strategic Management



می‌تواند سبب افزایش رضایت مشتری از محصولات یا خدمات به عنوان نتیجه‌ی 'کنترل' ("میزان تعدیل ریسک") باشد، همانند گروه‌های متمرکز در زمینه‌ی کالا و یا خدمات جدید. این کنترل‌ها احتمال دستیابی به نتایج بهتر را افزایش می‌دهد.

نتیجه‌گیری یک: مدیریت ریسک در زمینه‌ی کاهش دامنه و احتمال پیامدهای زیان‌بار و در عین حال بهبود و افزایش احتمال پیامدهای مفید که ممکن است از تصمیمات برخاسته باشد، عمل می‌کند.

۲.۲. تمرکز حسابرسی داخلی باید روی توانایی سازمان برای مدیریت ریسک و نه صرفاً روی کنترل‌ها باشد.

پیشنهاد بازنگری در قانون ساربینز اکسلی در ایالات متحده آمریکا با تغییر تمرکز حسابرسی از کنترل‌ها به مدیریت ریسک مطرح شده است (لیچ،^۱ ۲۰۱۱). علت ارائه‌ی این پیشنهاد شکست سازمان‌ها در بحران بانکی سال ۲۰۰۸ و دیگر شکست‌های مالی اخیر است که دلیل آن نه شکست کنترل‌های موجود که ناشی از ضعف کنترل‌های مناسب در نتیجه‌ی عدم تشخیص، تجزیه و تحلیل، ارزیابی و بهبود ریسک‌ها به صورت مؤثر بود.

نتیجه‌گیری دو: تمرکز حسابرسی داخلی و دیگر واحدهای نظارتی و بررسی‌کننده باید نه تنها بر اثربخشی کنترل‌ها، که بر ایجاد اطمینان در اثربخشی مدیریت ریسک باشد. مدیریت ریسک باید همواره در زمینه‌ی دستیابی به اهداف سازمانی قابل درک باشد و بنابراین کنترل‌ها عامل دستیابی به این اهداف هستند. حسابرسی‌های داخلی مدیریت ریسک باید مبنایی برای ارزیابی کلی سازمان از مدیریت ریسک خود ایجاد کند تا به‌نوبه‌ی خود نقطه‌ی آغاز هرگونه بررسی برون‌سازمانی مدیریت ریسک و ارتباطات بیرونی مرتبط با ریسک باشد.

۳.۲. مدیریت ریسک نیاز به تصمیم‌گیری مشخص و پایدار مدیریت دارد.

مدیریت ریسک باید با برنامه‌ریزی راهبردی و دیگر فرایندهای مدیریت به طور کامل یکپارچه شود. از آنجا که ریسک تأثیر عدم اطمینان در دستیابی به اهداف است، تعیین اهداف وابسته (به عنوان مثال برای طرح‌های تجاری، برنامه‌ها و پروژه‌ها) نیز باید با مدیریت ریسک درآمیخته شود. زیرا (شبکه‌ی بین‌المللی راهبری شرکتی،^۲ ۲۰۱۰):

"ریسک‌پذیری عنصری جدایی‌ناپذیر از راهبرد، محرک حیاتی در دستیابی به اهداف و همچنین بخشی از تصمیم‌گیری هر شرکت است. راهبرد و ریسک مفاهیم نوینی نیستند، هرچند مشخص شده ریسک موضوعی است که نهادهای نظارتی و قانونی در بسیاری از مراجع صلاحیتدار، بسیار به آن توجه می‌کنند. ... توانایی ارزیابی و پاسخ‌گویی به چگونگی مدیریت ریسک یک شرکت، ارتباطی فراتر از سهام‌داران و هیأت مدیره ایجاد می‌کند که خود برگرفته از اثرگذاری شرکت بر تمامی ذی‌نفعان شامل کارکنان و جوامعی که شرکت در آن به تجارت می‌پردازد و در موارد خاص، بازارهای ملی یا بین‌المللی است."

به عقیده‌ی نویسنده پرداختن به موضوع "اثرگذاری بر همه‌ی ذی‌نفعان" الزام کلیدی برای موفقیت در جهان امروزی است که دارای ارتباطات اجتماعی لحظه‌ای است و بر سازمان‌ها تأثیرگذار است. در بررسی بحران بانکی سال ۲۰۰۸، شکست‌های مدیریت ریسک مشخص شد. آنچه اتفاق افتاد برای بسیاری از سازمان‌های دیگر نیز قابل اعمال است و شامل موارد زیر است (هیأت ثبات مالی^۳، ۲۰۰۹):

- عدم تمایل یا ناتوانی اعضای هیأت مدیره و مدیران ارشد در ادراک، اندازه‌گیری و پای‌بندی به سطح ریسک

ریسک‌پذیری عنصری جدایی‌ناپذیر از راهبرد، محرک حیاتی در دستیابی به اهداف و همچنین بخشی از تصمیم‌گیری هر شرکت است

1-Leech

2-International Corporate Governance Network

3-Financial Stability Board, 2009

قابل پذیرش سازمان،... در اغلب موارد ریسک‌های به وقوع پیوسته‌ی درون‌سازمانی با ریسک‌های قابل ادراک هیأت مدیره متفاوت بود.

• تمهیدات داخلی از جمله پاداش مدیریت که در تضاد یا تعارض با اهداف سازمانی است.

• زیرساخت‌های نامناسب و اغلب پراکنده که مانع از تشخیص، تحلیل، ارزیابی و ارتقای اثربخشی ریسک می‌شود.

نتیجه‌گیری ۳: فرایندهای مدیریت ریسک باید با سیستم‌های مدیریت سازمان یکپارچه شود تا مؤثر واقع گردد. از آنجایی که رویه‌های اخیر معطوف به فعالیت‌های

مدیریت ریسک به منظور تهیه‌ی گزارش‌های راهبردی معنادار و قابل اطمینان است، این امر مستلزم به‌کارگیری مدیریت ریسکی سازگار و جامع و نیز استفاده‌ی مناسب از خدمات اطمینان‌بخشی حساب‌رسان داخلی در سرتاسر سازمان است. در پاسخ به شکست‌های اخیر، تمرکز بر بهبود راهبری سازمان‌ها بوده است که حاصل آن "اثربخشی بیش‌تر مدیریت ریسک" است.

۳. ایزو ۳۱۰۰۰ سال ۲۰۰۹، مدیریت ریسک - اصول و رهنمودها

ایزو ۳۱۰۰۰ منعکس‌کننده‌ی بهترین رویه‌ی اخیر است و تکامل آن از طریق فرایندی چهارساله و با حضور هزاران کارشناس مدیریت ریسک از سراسر جهان برای دستیابی به

استانداردی مورد توافق حاصل شد. این استاندارد شامل راهکارهایی در زمینه‌ی چگونگی پیاده‌سازی و بهبود چارچوب مدیریت ریسک است. استاندارد یادشده در دوره‌ای توسعه یافت که چارچوب‌های رقیب بسیاری چون کوزو ۲۰۰۴، استانداردهای مدیریت پروژه^۱، اهداف کنترلی اطلاعات و فناوری مرتبط با آن (کوبیت)^۲ و جز آن وجود داشت. برخلاف سایر استانداردها، استاندارد ایزو مختص هیچ کشور، کاربرد یا نوع خاصی از ریسک نیست. این استاندارد

نگاهی رو به جلو دارد و منعکس‌کننده‌ی ویژگی‌های بهترین تجربه در سازمان‌های پیشرو است. صنعت معدن و بخش‌های مرتبط با منابع مثال‌هایی است که به‌طور کلی نیازمند مدیریت ریسک بسیار مؤثر برای ایجاد بازده سرمایه‌گذاری است، تا از «مجوز فعالیت» خود محافظت کند و استانداردهای مناسب ایمنی را برای کارمندان خود و محیط مجاور فراهم کند. بزرگ‌ترین شرکت استخراج معدن جهان شرکت بی. اچ. پی. بیلیتون^۳ است و سیاست‌های مدیریت ریسک آن (حول و حوش ۲۰۰۷) در نگاره‌ی یک نشان داده شده است. نگاره‌ی یادشده کم‌وبیش تمامی الزامات کلیدی عملکرد مدیریت ریسک گنجانده شده در ایزو ۳۱۰۰۰ را نمایش می‌دهد. در این بخش

نوآوری‌های کلیدی موجود در ایزو ۳۱۰۰۰ همراه با مفاهیم حسابرسی داخلی ارائه شده است.

۱،۳. یکپارچه کردن مدیریت ریسک با سیستم‌های مدیریت و تصمیم‌گیری سازمانی «سازمان‌ها به صورت مداوم در حال توسعه، پیاده‌سازی و بهبود مستمر چارچوبی هستند که هدف آن یکپارچه کردن فرایند مدیریت ریسک با راهبری کلی سازمان، راهبرد و برنامه‌ریزی، مدیریت، فرایندهای گزارشگری، سیاست‌ها، ارزش‌ها و فرهنگ سازمانی است» (ایزو ۲۰۰۹).

هر ریسکی باید دارای یک مالک تعیین‌کننده باشد، منظور کسی است که ریسک را عنوان و تصمیم‌گیری در خصوص آن را راهبری می‌کند. به عبارت دیگر، ریسک‌ها از آن یک تصمیم‌گیرنده است، نه گروهی جداگانه مانند حساب‌رسان داخلی یا بخش مدیریت ریسک و این یکی از مهم‌ترین نوآوری‌ها در ایزو ۳۱۰۰۰ است. مدیریت ریسک با فرماندهی، کنترل و ساختار گزارشگری سازمان کاملاً یکپارچه می‌شود و فعالیت‌ی مستقل نیست.

هر سازمان با توجه به مأموریت، چشم‌انداز و اهداف خود، ساختار سازمانی را برای دستیابی به رسالت و اهداف

فرایندهای مدیریت ریسک باید با سیستم‌های مدیریت سازمان یکپارچه شود تا مؤثر واقع گردد

1-Project Management Standards
2-COBIT (Control Objective For Information and Related Technologies)
3-BHP Billiton

زیر می‌شود:

- دلایل انتخاب راهکارهای بهبود شامل دستیابی به مزایای موردانتظار؛
- افرادی که مسئول تصویب و اجرای طرح هستند؛
- اقدامات پیشنهادی؛
- منابع مورد نیاز شامل پیشامدهای احتمالی؛
- اندازه‌گیری عملکرد و محدودیت‌ها؛
- الزامات گزارشگری و نظارت؛ و
- جدول زمان‌بندی.

بنابراین فرایند مدیریت ریسکی که تصمیم‌گیرنده از آن استفاده می‌کند تمامی ورودی‌های اساسی مورد نیاز برای برنامه‌ریزی حسابرسی‌های داخلی^۲ را دربرمی‌گیرد. بنیاد تحقیقاتی انجمن حسابرسان داخلی، به‌صراحت راهنمای به‌کارگیری استانداردهای استرالیا در زمینه‌ی «خدمات اطمینان‌بخشی» را به رسمیت می‌شناسد.

نتیجه‌گیری ۵: حسابرسی داخلی اطلاعات موردنیاز برای برنامه‌ریزی حسابرسی (و نیز برنامه‌های حسابرسی سالانه) را از فرایند مدیریت ریسک انجام شده به دست تصمیم‌گیرندگان که متصدی و پاسخ‌گوی ریسک‌ها هستند، به دست می‌آورد.

این‌که طی چه مدت زمانی حسابرسی داخلی خود را

خود تشکیل می‌دهد. نمودارهای سازمانی نمونه‌ی بارز این ساختار سازمانی است. در ایزو ۳۱۰۰۰ این باور هست که مدیریت ریسک تنها یکی از موارد مهم در میان انبوه مواردی است که هر یک از مدیران سازمانی در زمان تصمیم‌گیری از آن استفاده می‌کنند. برای حمایت از تصمیم‌گیری، مدیریت ریسک با سایر ملزومات تصمیم‌گیری مانند منابع انسانی، بودجه‌بندی، اجرای وظایف تخصیص یافته و سیاست‌های اخلاقی رایج پیوند می‌خورد. مدیریت ریسک به منظور اطمینان‌بخشی از تشخیص، تحلیل، ارزیابی، بهبود و بازبینی عدم قطعیت‌های مرتبط با تصمیم‌گیری‌ها اجرا و پیاده‌سازی می‌شود تا از این طریق نظارتی حاصل شود که نتیجه‌ی آن کنترل پایدار است.

نتیجه‌گیری ۴: حسابرس داخلی نباید به نمایندگی از سازمان به ارزیابی ریسک بپردازد. نقش این حسابرسان یاری رساندن به تصمیم‌گیرندگان در دستیابی به مناسب‌ترین راهکارهای بهبود ریسک و سپس، نظارت و بررسی ریسک‌ها و کنترل آن است. اصطلاح «ارزیابی ریسک‌ها»^۱ در این مقاله به معنای اجرای معیارها و رهنمودهایی برای ارزیابی ریسک است که در ایزو ۳۱۰۰۰ بیان شده است. چراکه ارزیابی بخشی از وظیفه‌ی مدیریت است و از جمله وظایف حسابرسی داخلی نیست.

نتیجه‌گیری ۲ و ۴ بدین معناست که به عملکرد سنتی حسابرسی داخلی در ارزیابی ریسک دیگر نیازی نیست و درواقع از آن رو که مسئولیت‌پذیری و پاسخ‌گویی مدیریت را کاهش می‌دهد، مطلوب نیست. ارزیابی ریسک توسط حسابرس داخلی به صورت سنتی روی طراحی برنامه‌ی حسابرسی و نه حمایت از تصمیم‌گیری متمرکز انجام شده است. نگره‌ی دو فرایند مدیریت ریسک ایزو را برای استفاده‌ی تمامی تصمیم‌گیرندگان نشان می‌دهد (ایزو ۳۱۰۰۰، سال ۲۰۰۹). در نگره‌ی دو خروجی فرایند ارزیابی ریسک توسط مالک ریسک می‌تواند به طور مستقیم به عنوان نقطه‌ی شروع برای حسابرسی داخلی و نیز توسعه‌ی برنامه‌ی حسابرسی داخلی سالانه مورد استفاده قرار گیرد. همچنین در نگره‌ی دو خروجی دیگر فرایند مدیریت ریسک، برنامه‌ی بهبود ریسک است که با توجه به ایزو ۳۱۰۰۰ شامل موارد



1-Assess Risks

2-The Joint Institute of Internal Auditors Research Foundation

با تغییرات از نقش‌های سنتی به نقش جدید «حمایت از متصدی ریسک/تصمیم‌گیرنده» تطبیق دهد، نامشخص است. با این حال، روشن است که اساس عملکرد آن‌ها در ارائه‌ی نظارت و بررسی بی‌طرفانه، مستقل و اطمینان‌بخش ریسک‌ها، مدیریت ریسک و کنترل‌ها بدون تغییر باقی می‌ماند. بسیاری از تکنیک‌های جدید نیازمند آزمون مجدد و بازبینی هستند.

۲.۳. چارچوب مدیریت ریسک

در ایزو ۳۱۰۰۰ پیشنهاد می‌شود سازمان‌ها نیاز به چارچوب و سیستم مشخص مدیریتی دارند تا قابلیت تطبیق مناسب اهداف سازمانی با مدیریت ریسک فراهم شود. فرایند کلیدی مدیریت ریسک در نگاره‌ی دو نشان داده شده است (ایزو ۲۰۰۹). هر تصمیم‌گیرنده از این فرایند برای تصمیم‌گیری استفاده می‌کند. چارچوب مدیریت ریسک ایزو ۳۱۰۰۰ عمدتاً به منظور اطمینان‌دهی در این مورد است که فرایند مورد استفاده قرار می‌گیرد و اثربخش است.

چارچوب مدیریت ریسک بیان شده در ایزو ۳۱۰۰۰ برپایه‌ی بهبود مستمر با استفاده از روش سنتی (PDCA)^۱ است (دیمینگ^۲، ۱۹۸۶). پرفروش‌ترین کتاب دانشگاهی اخیر در مورد مدیریت ریسک واحد اقتصادی (فریزر^۳، ۲۰۱۰) به توصیف عناصر کاربردی ERM پرداخته است. روشن است که ERM و چارچوب مدیریت ریسک ایزو ۳۱۰۰۰ پیش از این به‌صورت کاربردهای عملی و پس از این به شکل اصول و دستورالعمل‌ها، مشابه یکدیگرند. انتظار می‌رود که اجرای رهنمودهای ایزو برای چارچوب مدیریت ریسک در تعامل با طرح‌های در حال اجرای ERM تکامل یابد. نتیجه‌گیری ۶: ERM و استاندارد مدیریت ریسک ISO ۳۱۰۰۰ در تعامل مشترک با هم هستند و پایه و اساس مدیریت ریسک در سازمان‌ها خواهند بود.

نگاره‌ی سه (CSA، ۲۰۱۱) نشان‌دهنده‌ی نمونه‌ای از چارچوب مدیریت ریسک برای یک سازمان است و شامل کارگروه‌ها و فعالیت‌های درگیر در اجرای چارچوب و نیز بهبود مستمر آن است. این نگاره برگرفته از اثر برودلیف^۴ و استانداردهای مدیریت ریسک انجمن استانداردهای

کانادا^۵ با افزودن ارتباط راهبری شرکتی است. در نگاره‌ی سه مربع «بررسی و بهبود»^۶ در قسمت انتهایی سمت راست، مربوط به عملکرد سنتی حسابرسی داخلی در «اطمینان‌بخشی کنترل»^۷ همراه با دیگر بررسی‌های صورت گرفته از راهبری، تکامل مدیریت ریسک و پیشرفت در اجرای چارچوب است. این بررسی‌ها ورودی مربع بالایی سمت راست با عنوان «مأموریت و تعهد»^۸ است که به بهبود مستمر چرخه منجر می‌شود.

در نگاره‌ی سه، چارچوب از کاربرد فرایند مدیریت ریسک «مرکزی» حمایت می‌کند. این نگاره مشخص‌کننده‌ی نیاز به آموزش برای اجرای چارچوب، کمیته‌ی مدیریت ریسک متشکل از اعضای هیأت مدیره و سایر فعالیت‌ها و کمیته‌ها به منظور پیاده‌سازی و بهبود مستمر چارچوب است. همچنین نگاره‌ی سه نشان‌دهنده‌ی یکی از عناصر کلیدی ERM یعنی مأموریت و تعهد برای مدیریت ریسک از واحدهای راهبری سازمان است.

نتیجه‌گیری ۷: مدیریت ریسک اثربخش نیازمند بیان واضح و روشن اهداف و اختیارات هیأت‌مدیره و مدیران ارشد است. در استانداردهای مدیریت ریسک کانادا بر این الزام تأکید شده است و به‌عنوان یک اصل اساسی نشان‌دهنده‌ی رویه‌ی عملی برای بیان این تعهد است (CSA، ۲۰۱۱). نگاره‌ی یک، همچنین نشان‌دهنده‌ی چگونگی بیان مأموریت و تعهد به مدد سیاست‌های مدیریت ریسک سازمان است.

۳.۳. ایزو ۳۱۰۰۰ بیان مفهوم «ایجاد زمینه» در

زمینه‌ی طراحی چارچوب مدیریت ریسک

زمینه‌ی مورد بحث با «تعریف پارامترهای بیرونی و داخلی و مدنظر قرار دادن آن‌ها در مدیریت ریسک و تعیین اهداف و معیارهای ریسک برای سیاست‌گذاری مدیریت ریسک» ایجاد می‌شود. این مرحله در طراحی چارچوب به منظور اطمینان‌بخشی از تطابق چارچوب (که برای هر سازمان متفاوت خواهد بود)، با محیط سازمانی، مشخصات ریسک و گذشته‌ی آن است. به عنوان مثال، یک سازمان دولتی مشمول نظارت سیاسی که تغییرات سریع در جهت‌گیری‌های سیاسی را تجربه کرده است

1-Plan-Do-Check-Act 2-Deeming
3-Frase 4-Broadleaf, 2008 (Broadleaf Capital International)
5-CSA (Canadian Standard Association)
6-Review and Improve 7-Control Assurance
8-Mandate and Commitment

خواستار چارچوب مدیریت ریسک شفاف بوده که در زمان تصمیم‌گیری‌ها نیز برای آن‌ها ایجاد محدودیت نکند. برخلاف سایر استانداردهای ایزو، (ایزو ۳۱۰۰۰) به‌صراحت منع استفاده از این استاندارد را به منظور تایید بیان کرده است. زیرا چارچوب مدیریت ریسک باید متناسب با زمینه‌ی سازمان طراحی شود تا اثربخش باشد. اگرچه عناصر اصلی چارچوب در سازمان‌های گوناگون قابل تشخیص است، این عناصر در تعامل با سیستم مدیریتی مشخص هر سازمان متفاوت با یکدیگر خواهد بود.

سازمان‌ها در حال حاضر از موارد بسیاری از فرایندهای مدیریت ریسک در زمینه‌های مقررات بهداشت و ایمنی، استانداردهای استخدام، اولویت‌های قانونی و... برخوردارند. در حال حاضر تمامی سازمان‌ها به مدیریت ریسک می‌پردازند و در نتیجه دارای چارچوب مدیریت ریسک اما به صورت موردی هستند. با این حال، اثربخش بودن آن بعید به نظر می‌رسد و ایزو ۳۱۰۰۰ امکان بررسی این رویکردهای موجود را تا زمان ارتقا و بهبود آن‌ها فراهم می‌کند. یکی از اهداف ایزو ۳۱۰۰۰، تهیه‌ی استانداردی به منظور ایجاد توازن با سایر استانداردهایی است که در تعامل با مدیریت ریسک هستند که در نتیجه‌ی آن با ایزو ۳۱۰۰۰ همسو و سازگار می‌شوند.

نتیجه‌گیری ۸: اصلاحات تکمیلی در نقش و عملکرد حسابرسی داخلی به عنوان بخشی از بهبود مستمر چارچوب در مدیریت ریسک به وقوع خواهد پیوست. پیاده‌سازی مدیریت ریسک اثربخش در یک سازمان در حدود سه الی پنج سال به طول می‌انجامد و در این مدت فرایند بهبود مستمر به‌روزرسانی می‌شود و حاصل آن تکامل چارچوب است. این تغییرات شامل بهبود و تغییر نقش حسابرسی داخلی و عملکرد سایر کارکنان در سازمان است که سبب تغییرات منظم و مؤثر در مدیریت ریسک می‌شود.

۴،۳ تکامل مدیریت ریسک: ایزو ۳۱۰۰۰ اصول اساسی را بیان می‌کند که ERM باید آن‌ها را مدنظر قرار دهد. همچنین ایزو ۳۱۰۰۰، پنج ویژگی مدیریت ریسک «برتر» را ارائه می‌کند که عبارتند از:

۱. بهبود مستمر به واسطه‌ی تنظیم اهداف عملکرد سازمانی، سنجش، بررسی و اصلاح آتی فرایندها، سیستم‌ها، منابع، توانمندی و مهارت‌ها.

۲. پاسخ‌گویی کامل برای ریسک‌ها، وظایف رفتار ریسک و کنترل‌ها. تعیین افراد کاملاً پاسخ‌گو که مهارت‌های مناسب و منابع کافی را برای کنترل‌ها دارند، بر ریسک نظارت کرده کنترل‌ها را بهبود می‌بخشند و با سهام‌داران بیرون و داخل در خصوص ریسک و مدیریت آن ارتباط مؤثر برقرار می‌کنند.

۳. کاربرد مدیریت ریسک در تمام تصمیم‌گیری‌ها، در هر سطحی از اهمیت، باید ریسک‌های موجود و اعمال مدیریت ریسک تا حد مناسب در نظر گرفته شود.

۴. ارتباطات مستمر با سهام‌داران داخلی و بیرونی، از جمله ارائه‌ی گزارش‌های جامع و مکرر از عملکرد مدیریت ریسک، بخشی از راهبری مناسب تلقی می‌شود.

۵. یکپارچگی کامل در ساختار راهبری سازمان به صورت مرکزیت فرایندهای مدیریت سازمانی دیده شده است، به‌گونه‌ای که ریسک به عنوان تأثیر عدم اطمینان در دستیابی به اهداف در نظر گرفته شده است. ساختار راهبری و فرایندها براساس مدیریت ریسک است. مدیریت ریسک اثربخش را مدیران برای دستیابی به اهداف سازمانی ضروری تلقی می‌کنند.»

همچنین ایزو ۳۱۰۰۰ نشان می‌دهد چه‌گونه می‌توان عملکرد مدیریت ریسک را در برابر این اقدامات ارزیابی کرد، که معمولاً حداقل به صورت سالانه تحت عنوان «ارزش‌یابی تکامل مدیریت ریسک» انجام می‌شود. به عنوان مثال فریزر^{۲۹} در کانادا، که اداره‌ی سه بیمارستان را برعهده داشت، به ارزیابی سالانه از ۲۱ ویژگی تکامل مدیریت ریسک برای اطمینان از اجرای مداوم و بهبود ERM می‌پرداخت (پارکینز،^{۲۰} ۲۰۰۹). روش‌های اساسی و الزامات را مؤسسه‌ی اعتبارسنجی کانادا که از مراجع قانون‌گذار دولت فدرال است، ارائه کرده است. این سیستم برای حسابرسی مدیریت ریسک مربوط به مراقبت‌های بهداشتی برای حداقل یک دهه قبل از ایزو ۳۱۰۰۰ وجود داشته است و نمونه‌ای خوب از بهترین تجربه در حوزه‌ی مدیریت ریسک است که پایه و اساس ایزو ۳۱۰۰۰ را فراهم می‌کند.

نتیجه‌گیری ۹: تکامل مدیریت ریسک را باید مورد ارزیابی قرار داد و حداقل به صورت سالانه گزارش کرد. درحالی‌که بهتر است مدیریت این اندازه‌گیری تکامل ریسک را انجام دهد، تا به صورت روشن و شفاف نقشی را برای حسابرسی داخلی نشان دهد.

۴. تحول نقش‌های حسابرسی داخلی

منشور کمیته‌ی حسابرسی هیأت مدیره‌ی بانک رویال کانادا چنین بیان می‌کند «کمیته باید به صورت سالانه به بررسی و ارزیابی کفایت مأموریت‌ها و اثربخشی آن‌ها بپردازد.» علاوه بر این که مفاد دستور کمیته‌ی حسابرسی هیأت مدیره می‌باید مطابق با عملکرد حسابرسی داخلی باشد تا شایستگی اثربخشی و مأموریت آن بازبینی و تعیین شود. پتانسیل لازم برای تکامل حسابرسی داخلی به واحدی با راهبرد بیشتر در مطالعه‌ی موردی که چادا (۲۰۱۱) انجام داده مستند شده است. او معتقد است که پس از ERM حسابرسی داخلی در جهان باید با حرکت از کنترل و نظارت به سوی توسعه‌ی دو نقش جدید ارائه شده در ذیل به نوآوری و شکوفایی برسد:

۱. تهیه‌ی دیدگاه‌های تجاری مرتبط و با کیفیت بالا، و
۲. تبدیل شدن به یک کارشناس در زمینه‌ی مدیریت بر طرح‌های راهبردی، چالش‌ها و تغییرات در سازمان چادا همچنین استدلال می‌کند که حسابرسی داخلی، نیروی انسانی، دانش و تجربه‌ی لازم را برای ایجاد اثربخش دو نقش یادشده داراست.

نتیجه‌گیری ۱۰: حسابرسی داخلی برای حمایت از پیشرفت مداوم و پیاده‌سازی اثربخش مدیریت ریسک می‌باید نقش‌ها و مسئولیت خود را به‌روزرسانی کند. چادا (۲۰۱۱) به منظور شروع برنامه‌ریزی راهبردی برای نقش‌های جدید حسابرسی داخلی شش سؤال زیر را پیشنهاد می‌کند:

- ۱) آیا واحد حسابرسی داخلی شما از انتظارات ذی‌نفعان از خود آگاه است؟
- ۲) آیا اهداف واحد حسابرسی داخلی شما با اهداف سازمان هم‌سو است؟

۳) آیا واحد حسابرسی داخلی شما تعادل معقول میان خدمات مشاوره و اطمینان‌بخشی ایجاد کرده است؟

۴) آیا واحد حسابرسی داخلی شما از ترکیب مناسب نیروی انسانی برای ارائه‌ی خدمات مشاوره و تخصص مورد درخواست سازمان برخوردار است؟

۵) آیا تعریف مجدد اختیارات برای واحد حسابرسی داخلی شما مورد نیاز است؟

۶) آیا واحد حسابرسی داخلی شما ارتباط مستقیم با مدیران سازمان دارد؟

ارتباط و هم‌سویی حسابرسان داخلی و مستقل مثال بارز از مسایل بسیاری است که باید در نقش در حال تحول حسابرسی داخلی مورد بررسی قرار گیرد. برای اطمینان‌بخشی به ذی‌نفعان، به حسابرسی مستقل نیاز است. به عقیده‌ی نویسنده، شروع حسابرسی‌های مستقل از نتایج کار حسابرسان داخلی از مدیریت ریسک کلی سازمان است. با این حال، خروجی عملکرد حسابرسی‌های داخلی مانند اطمینان‌بخشی در خصوص یکپارچگی مالی، نظارت و بررسی جداگانه‌ی داخلی و مستقل درون سازمانی است. ایزو ۳۱۰۰۰ نیازمند سازمان‌هایی است که چارچوب مدیریت ریسک سازمان را با زمینه، ساختار و نقش‌ها و مسئولیت‌ها منطبق سازد. هر سازمان منحصر به فرد است و مدیریت ریسک و سیاست‌گذاری نیز چارچوب منحصر به فرد خود را داراست و به مدد سیاست‌های سازمان تمایلات خود را به برقراری ارتباط با ذی‌نفعان بیرونی، بیش از آن‌چه براساس مقررات الزامی است، هدایت می‌کند.

۵. نتیجه‌گیری

الزامات جدید راهبری شرکتی که الزام هیأت مدیره به کسب اطمینان از اثربخشی مدیریت ریسک و همچنین انتشارات ایزو در مورد استاندارد بین‌المللی مورد توافق در زمینه‌ی اصول و رهنمودهای مدیریت ریسک اثربخش است، چالش‌ها و فرصت‌هایی را برای حسابرسی داخلی سنتی ایجاد کرده است. در طول چند سال آینده حسابرسی داخلی ملزم به تغییر در نقش و رویکرد خود به منظور افزایش اثربخشی مدیریت ریسک است.

نتیجه می‌گیریم که:

۱. مدیریت ریسک در زمینه‌ی کاهش دامنه و احتمال پیامدهای زیان‌بار و درعین حال بهبود و افزایش احتمال پیامدهای مفید که ممکن است از تصمیمات برخاسته باشد، عمل می‌کند.
۲. تمرکز حسابرسی داخلی و دیگر واحدهای نظارتی و بررسی‌کننده باید نه تنها بر اثربخشی کنترل‌ها، بلکه ایجاد اطمینان در اثربخشی مدیریت ریسک باشد.
۳. فرایندهای مدیریت ریسک باید با سیستم‌های مدیریت سازمان یکپارچه شود تا مؤثر واقع شود.
۴. حسابرس داخلی نباید به نمایندگی از سازمان به ارزیابی ریسک پردازد. نقش آن‌ها یاری رساندن به تصمیم‌گیرندگان در دستیابی به مناسب‌ترین راهکارهای بهبود ریسک و سپس، نظارت و بررسی ریسک‌ها و کنترل آن است.
۵. حسابرسی داخلی اطلاعات موردنیاز برای برنامه‌ریزی حسابرسی (و نیز برنامه‌های حسابرسی سالانه‌ی خود را) از فرایند مدیریت ریسک انجام‌شده به دست تصمیم‌گیرندگان که مالک و پاسخ‌گوی ریسک‌ها هستند به دست می‌آورد.
۶. ERM و استاندارد مدیریت ریسک ایزو ۳۱۰۰۰ در تعامل مشترک با هم هستند و پایه و اساس مدیریت ریسک در سازمان‌ها خواهند بود.
۷. مدیریت ریسک اثربخش نیازمند بیان واضح و روشن از اهداف و اختیارات هیأت‌مدیره و مدیران ارشد است.
۸. اصلاحات تکمیلی در نقش و عملکرد حسابرسی داخلی به عنوان بخشی از بهبود مستمر چارچوب در مدیریت ریسک به وقوع خواهد پیوست.
۹. تکامل مدیریت ریسک را باید مورد ارزیابی قرار داد و حداقل به صورت سالانه گزارش کرد.
۱۰. حسابرسی داخلی برای حمایت از پیشرفت مداوم و پیاده‌سازی اثربخش مدیریت ریسک می‌باید نقش‌ها و مسئولیت‌های خود را به‌روزرسانی کند.

