مجله اقتصادی - ماهنامه بررسی مسائل و سیاست‌های اقتصادی
شماره ۱۱، بهمن ۱۳۹۰، صفحات ۱۳۸ - ۱۳۵

ارزیابی ریسک و حسابرسی مبتنی بر ریسک

مرتضی اسدی[۱]
مهدی ناظمی‌اردکانی

یک برنامه حسابرسی مبتنی بر ریسک مؤثر تمام فعالیت‌های اصلی یک مؤسسه را پوشش خواهد داد. فراوانی و عمق حسابرسی هر قسمت بر مبنای ارزیابی ریسک هر قسمت متفاوت خواهد بود. بررسی‌کنندگان می‌بایست تعیین کنند که آیا عملکرد حسابرسی به تناسب اندازه و پیچیدگی مؤسسه مناسب است یا خیر؟

واژه‌های کلیدی: ارزیابی ریسک، پوشش حسابرسی، امتیازبندی ریسک، ریسک تجاری.

۱. عناصر برنامه

برنامه‌های طراحی شده حسابرسی مبتنی بر ریسک احتمالاً کارایی و اثربخشی حسابرسی را افزایش می‌دهند. قابلیت اتکا و رسمیت حسابرسی‌های مبتنی بر ریسک ممکن است بسته به اندازه و پیچیدگی مؤسسه با یکدیگر متفاوت باشند. به منظور تعیین سطح مناسب پوشش حسابرسی برای محیط IT سازمان، مدیریت می‌بایست شیوه مؤثر ارزیابی ریسک را مشخص نماید. این شیوه ارزیابی می‌بایست برای حسابرس و هیأت مدیره اطلاعاتی بی‌طرفانه در جهت تعیین اولویت تخصیص برنامه‌های حسابرسی به درستی فراهم نماید. به منظور اجرای برنامه‌های حسابرسی IT مبتنی بر ریسک می‌بایست این موارد رعایت شوند:

- شناسایی اطلاعات مؤسسه از قبیل پرسنل، امکانات، تکنولوژی، سیستم‌های عملیاتی و اجرایی
- شناسایی فعالیت‌ها و فرایندهای تجاری در هریک از آن طبقات
- لحاظ کردن پرونده‌های واحدهای تجاری مهم، بخش‌ها و خطوط تولید یا سیستم‌ها، ریسک‌های تجاری مرتبط و مشخصه‌های کنترل
- بکارگیری یک سیستم امتیازبندی یا اندازه‌گیری ریسک‌های کنترل و تجاری را برای واحدهای تجاری، بخش‌ها و محصولات

۱. عضو هیأت علمی دانشگاه علوم اقتصادی. asadi@ses.ac.ir

- لحاظ نمودن تأیید کمیته حسابرسی یا هیأت مدیره از ارزیابی‌های ریسک و برنامه‌های سالانه حسابرسی مبتنی بر ریسک که جداول زمانی حسابرسی، چرخه‌های حسابرسی، حوزه برنامه‌کاری و تخصیص منبع برای هر قسمت حسابرسی شده
- اجرای برنامه حسابرسی از طریق برنامه‌ریزی، اجرا، گزارشگری و پیگیری.
- لحاظ نمودن فرایندی که به طور منظم ارزیابی ریسک را تنظیم می‌کند و آن را حداقل به صورت سالانه برای تمام واحدهای تجاری مهم، قسمت‌ها و محصولات یا سیستم‌ها به روز می‌کند.

۲. سیستم امتیازبندی ریسک

یک برنامه حسابرسی IT مبتنی بر ریسک موفق می‌تواند بر مبنای یک سیستم مؤثر امتیازبندی باشد. در وضع یک سیستم امتیازبندی، هیأت مدیره و مدیریت می‌بایست اطمینان حاصل کنند که سیستم قابل فهم است، تمام عوامل مربوط به ریسک را در نظر می‌گیرد و تا حد ممکن از ذهنیت‌گرایی اجتناب می‌کند. عوامل اصلی ریسک که معمولاً در سیستم‌های امتیازبندی بکار گرفته می‌شوند شامل موارد زیر می‌شود:

- ماهیت مبادلات و رویدادها (به عنوان مثال، تعداد و حجم پولی و پیچیدگی)
- ماهیت محیط عملیاتی (به عنوان مثال، تغییرات در حجم، درجه سیستم و تمرکز (استقرار) گزارشگری، حساسیت اطلاعات رسیدگی شده، تأثیرگذاری بر فرایندهای بحرانی مؤسسه تجاری، تأثیر بالقوه مالی، تغییرات برنامه‌ریزی شده و محیط قانونی و اقتصادی
- امنیت فیزیکی و معقول اطلاعات، تجهیزات و ساختمان‌ها
- کفایت غفلت[1] مدیریت عملیاتی و تنظیم و کنترل
- نتایج حسابرسی و قانونی (منظم) قبلی و پاسخگویی مدیریت در موضوعات موردنظر
- منابع انسانی شامل تجربه مدیریت و کارکنان، گردش، رقابت تکنیکی، طرح جانشینی مدیریت و درجه هیأت نمایندگی
- غفلت مدیریت ارشد

حسابرسان می‌بایست دستورالعمل‌های کتبی در مورد استفاده از ابزارهای ارزیابی ریسک ایجاد و گسترش دهند و این دستورالعمل‌ها را با کمیته حسابرسی یا هیأت مدیره مورد بازنگری قرار دهند، قابلیت اتکا و رسمیت دستورالعمل‌ها برای مؤسسات (به صورت جداگانه) بسته به اندازه، پیچیدگی، حوزه فعالیت‌ها، تنوع جغرافیایی، تکنولوژی‌های مختلف بکار گرفته شده متفاوت خواهد بود. مؤسسه می‌تواند بر شیوه عمل استاندارد صنعت یا بر تجربه‌های خود در جهت امتیازبندی ریسک اتکا کند. حسابرسان

1. Oversight

می‌بایست دستورالعمل‌ها را برای درجه‌بندی یا ارزیابی حوزه‌های اصلی ریسک و مشخص کردن دامنه امتیازات یا ارزیابی‌ها بکار برند. به عنوان مثال، طبقه‌بندی مانند ریسک‌پایین، ریسک متوسط و ریسک بالا یا به صورت یک زنجیره عددی مانند ۵-۱. دستورالعمل‌های کتبی ارزیابی ریسک می‌بایست عناصر زیر را مشخص سازند:

- یک حداکثر طول دوره زمانی برای چرخه‌های حسابرسی براساس امتیازات ریسک (به عنوان مثال، برخی مؤسسات چرخه‌های حسابرسی خود را ۱۲ ماهه یا کمتر برای قسمت‌های با ریسک بالا، ۲۴ ماهه یا کمتر برای قسمت‌های با ریسک متوسط و بیش از ۳۶ ماه برای حوزه‌های با ریسک پایین، چرخه‌های حسابرسی نمی‌بایست نامحدود باشد).
- زمان‌بندی ارزیابی‌های ریسک برای هر قسمت یا هر فعالیت (معمولاً ریسک‌ها به صورت سالانه ارزیابی می‌شوند، اما ارزیابی‌هایی با تکرار بیشتر ممکن است لازم باشد، اگر مؤسسه رشد سریع یا تغییری با اهمیت در عملیات یا فعالیت‌هایش تجربه می‌کند.
- مستندسازی الزامات و نیازها در جهت حمایت از تصمیمات امتیازبندی
- رهنمودهایی برای لغو ارزیابی‌های ریسک در شرایط خاص براساس آنچه می‌توانند لغو و باطل شوند (به عنوان مثال، رهنمود می‌بایست مشخص کند چه کسی می‌تواند ارزیابی‌ها را لغو کند و چگونه لغوکردن تأیید می‌شود، گزارش می‌شود و مستند می‌شود).

بسیاری از گروه‌های صنعتی منابعی که مؤسسات می‌توانند به دست آورند ماتریس‌ها، مدل‌ها یا اطلاعات اضافی را پیشنهاد می‌کنند. در مورد ارزیابی‌های ریسک از جمله این گروه‌ها می‌توان به گروه‌های زیر اشاره نمود: ISACA، انجمن بانکداران امریکا (ABA)، انجمن حسابداران خبره آمریکا (AICPA) و IIA.

مدیریت روزانه برنامه حسابرسی مبتنی بر ریسک برعهده مدیر حسابرسی داخلی می‌باشد که حوزه حسابرسی و ارزیابی‌های ریسک در جهت اطمینان از اینکه پوشش حسابرسی درحد کفایت باقی بماند تنظیم و کنترل می‌کند. همچنین مدیر حسابرسی داخلی گزارش‌هایی که رتبه‌بندی ریسک، حوزه برنامه‌ریزی شده و چرخه حسابرسی برای هر حوزه نشان می‌دهد، آماده می‌کند.

مدیرداخلی می‌بایست قابلیت اتکاء سیستم ارزیابی ریسک حداقل به صورت سالانه یا هرگاه که تغییرات مهمی در یک بخش یا عملکرد حادث می‌شود را تأیید کند.

مدیران بخش عملیاتی و حسابرسان می‌بایست با همدیگر در ارزیابی ریسک در تمام بخش‌ها و عملکردها با بازنگری در ارزیابی‌های ریسک درجهت تعیین معقول بودنشان همکاری کنند. حسابرسان می‌بایست به طور ادواری نتایج پردازش‌های کنترل داخلی را مورد بازنگری قرار دهند و داده‌های عملیاتی و مالی را برای هرتأثیر بر ارزیابی ریسک یا امتیازبندی تحلیل کنند.

بنابراین، مدیریت عملیاتی می‌بایست ملزم باشد تا حسابرسان را درباره تمام تغییرات اصلی در بخش‌ها و وظایف بروز نگهدارد از جمله معرفی یک محصول جدید، اجرای یک سیستم جدید، تغییرات استعمال یا تغییرات مهم در سازمان‌ها یا کارکنان.