نقش حسابرس در تعیین نظام راهبردی فناوری اطلاعات

احمد عدالت

مقدمه

در اوایل دهه ۹۰ میلادی و با پررنگ شـدن سیستمهای الکترونیکی در چرخه فعالیت سازمانها، مدیران این مجموعه‌ها با طیف وسـیعی از فرایندهای جدید، متناسب با شـرایط توسعه جامعه مواجه شدند؛ فرایندهایی که حجم انبوهی از اطلاعات را در چرخه فعالیت سـازمان وارد کرده و موجب شـدند تا سـازوکارهای قدیمی نتوانند نقش مؤثری در پیشـبرد هدفهای سـازمانی ایفا کنند. هرچند که اجرای مهندسـی مجدد فرایندها در کسـب‌وکارها، موجب شد تا نتایج تغییرات ایجادشـده باعث افزایش بهره‌وری و کارامدی سازمان شود، اما با گذشـت زمان به دلیل اسـتفاده بدون برنامه از ابزار فناوری اطلاعات و صرف‌نظر از تعیین نظامی کارامد (به دلیل نبود ارزیابی مناسـب از به‌کارگیری این ابزار در فرایندهای سازمانی)، شرایط عدم هماهنگی مابین رشد فرایندهای سازمانی و استفاده راهبردی از فناوری اطلاعات فراهم گردید.

از آنجـاکـه حسابرسـی، مهم‌ترین ابزار به‌منظـور کنترل اجرای صحیـح چرخه‌های سـازمانی و منطبق با استانداردهای تدوین‌شده در حوزه‌های مختلف هر کسب‌وکاری است، نتایج این کنترل‌ها در سازمان می‌تواند نیـاز مدیران کسـب‌وکارها را در تدوین یک نظام جامع راهبردی فناوری اطلاعات و ارتباطات مرتفع سـازد. همچنین حسابرسـان فناوری اطلاعات، خواه داخلی یا مستقل، می‌توانند فعالیت مدیریت فناوری اطلاعات و متخصصان این حوزه را کنترل کرده و با اسـتفاده از فراهم آوردن تأییدیه‌ای مسـتقل از دقت نشـانگرهای مدیریتی و به‌کمک ارزیابی خود از فعالیت‌ها و دستاوردهای فناوری اطلاعات، نقاط ضعف استقرار و به‌کارگیری این ابزار را در راسـتای پیشبرد هدفهای سـازمانی تعیین کنند. در حقیقت این ارزیابی‌ها موجب نمایان شدن چالش‌های موجود در سازمان شده و طراحی یک معماری فناوری اطلاعات، متناسب با نیازمندی‌های به‌روز آن سـازمان را فراهم می‌کند. در ادامه به نقش حسابرسان در تدوین نظام راهبردی فناوری اطلاعات و تأثیر آن در پیشبرد هدفهای سازمانی خواهیم پرداخت.

نقش حسابرس در راهبری فناوری اطلاعات

راهبـری فنـاوری اطلاعات طبق تعاریف ارائه‌شـده در این حوزه عبارت اسـت از «تدوین برنامه‌ای از سـوی متخصصان امر به‌منظور همسـوکردن برنامه راهبردی فناوری اطلاعات با برنامه راهبردی عمومی سـازمان یا بنگاه اقتصادی، همچنین مدیریت خطرهای مداوم ایجادشـده در اجرای سیسـتمهای فناوری اطلاعات»

(ISACA, 2002). این وظیفه، مسـئولیتی وسـیع و سـطح بالا بوده و در جریـان فرایندهای کاری و برای به‌کارگیری فناوری اطلاعات کارامد و کنترل‌شده است که برعهده هیئت مدیره و مدیران اجرایی قرار دارد.

یکـی دیگـر از ارکانی که در این امر نقش مهمی را بازی کرده و اقدام بـه ارزیابی و کنترل اجرای فرایندهای سـازمانی و انطباق آن با برنامه‌های راهبردی و اسـتانداردهای تدوین‌شده در هر صنعتی می‌نماید، حسابرس فناوری اطلاعات است.

حسـابرس، همیشـه درنقش پشتیبان و تسـریع‌کننده کنترل و ارزیابی فرایندها، مشـاور مدیران در راهبری برنامه‌های سازمانی است؛ کنترل مواردی مانند مدیریت مالی، رعایت تکالیف قانونی و مدیریت عملیات و در چنددهه اخیر کنترل مکانیزم فناوری اطلاعات. به دلیل زیادبودن سـرعت تغییرات و میزان منابعی که سالانه صرف فناوری اطلاعات و ارتباطات می‌شود، برنامه‌ریزی و مدیریت ابزار این صنعت در هر کسب‌وکاری، نیاز به داشـتن اطلاعاتی دقیق از مشـکلات و انحرافات به‌وجود آمده در اجرای برنامه‌های راهبردی هر سـازمان دارد. اکنون بیش از همیشـه لازم اسـت که حسـابرس برای حمایت و کمک به مدیران ارشد کسب‌وکارها، در اسـتقرار سیسـتم راهبری فناوری اطلاعات و مدیریت آن تلاش کند. بنابراین، باید بررسـی شود که بهترین روش استقرار سیستم راهبری فناوری اطلاعات کدام است.

بیان همسوسازی طرح‌های راهبردی فناوری اطلاعات با برنامه راهبردی عمومی کسب‌وکار، بسیار ساده‌تر از عملی کردن آن اسـت. در دهه گذشـته، بسـیاری از انواع برنامه‌هـای راهبردی جدید در حـوزه بازرگانی و فنـاوری اطلاعات به‌وجود آمده اسـت که از پایه با روش‌های قدیمی و انعطاف‌ناپذیـر قبلی، تفاوت دارد. این نوع برنامه‌های راهبردی، توجه اصلی بر استراتژی‌های متنوعی دارند که پویا بوده و به‌طور مداوم اندازه‌گیری و ارزیابی می‌شـوند. حسابرسـان فناوری اطلاعات با کنترل و ارزیابی اجرای فرایندهای سـازمانی و این نوع برنامه‌هـای راهبردی، و نیز با اسـتفاده از علامت‌ها و مکانیزم‌های بازخور بـازار، در تصمیم‌گیری چرخه‌های کاری و سمت و سوی امور و تولیدات، به مدیران کمک می‌کنند.

نقش نظام راهبری در بهبود عملکرد کسب‌وکار

تحقیقات اخیر نشان داده است که دو جنبه «انجام کار درست (محرک عملکرد) و انجام کارها به روشی درست (حصول اطمینان از **تطابق**[1])» در نظام راهبری از اهمیت برابر برخوردار هسـتند. سازمان‌ها از طریق مطابقت فرایندهای خود با قوانین و شیوه‌های مناسب کسب‌وکار، نمی‌توانند در عصر فناوری اطلاعات به فعالیت خود ادامه دهند، اما بدون این تطبیق هم، شکسـت بسـیار محتمل اسـت. این موضوع در **تصویر ۱** نشـان داده می‌شود.

ارزش‌های زیادی در استفاده از این مدل، برای بازآفرینی تفکر نقش فناوری اطلاعات در پیشبرد برنامه‌های راهبردی یک سازمان وجود دارد. فناوری اطلاعات می‌تواند در هر دو جنبه نظام راهبری، مشارکت داشته باشد. ابزار فناوری اطلاعات و ارتباطات می‌تواند عملکرد را بهبود داده و به تطبیق فرایندها با برنامه راهبردی سازمان کمک کند.

سازمان‌هایی که به خوبی راهبری شده‌اند، چرخه‌های کاری خود را برای دستیابی به مقصودی که سازمان برای آن تأسیس شده (مأموریت سازمان)، و همچنین احتیاجات قانون و مقرراتی، ایجاد می‌کنند.

چارچوب‌های کنترلی و تطبیق قانونی

چارچوب‌های کنترلی به‌وجودآمده همانند **کمیته سازمان‌های حامی**[۲] و **مدیریت ریسک کسب‌وکار**[۳]، ساختاری را که در آن نظام راهبری مناسب بتواند اجرا شود، فراهم می‌آورد. محیط کنترلی یک سازمان با استفاده از نگرشی که در رأس آن سازمان در رابطه با مطالبات عملکردی و الزامات تطبیقی وجود دارد، هدایت می‌شود. سازمان‌هایی که برحسب هزینه تطبیق (هم به لحاظ قانونی و هم اخلاقی) به عملکرد اهمیت می‌دهند، منشاء بسیاری از رسوایی‌ها بوده‌اند. هرچند که این نوع سازمان‌ها که بر حسب هزینه عملکرد به تطبیق اهمیت می‌دهند، ممکن است سست و غیرقابل انعطاف شوند.

همچنین، این چارچوب‌ها، ارزیابی ریسک یا مدیریت ریسک را در موقعیتی مرکزی قرار می‌دهند. ریسک‌ها باید در رابطه با هر دو جنبه چارچوب نظام راهبری و سیستمهای کنترلی مناسب (برای نمایش آن ریسک‌ها) در جای مناسب قرار داده شوند. براساس کوزو، این ریسک‌ها، در رابطه با هدفهای عملیاتی، زیرمجموعه عملیاتی هیئت‌مدیره در خصوص موارد زیر هستند:

- صرفه‌جویی و کارایی عملیات، شامل دستیابی به هدفهای کلان عملکردی و حراست از دارایی‌ها در برابر خسارت،
- داده‌ها و گزارشهای مالی و عملیاتی اطمینان‌پذیر،
- تطبیق با قوانین و مقررات،

همان‌طور که در **تصویر ۲** نشان داده شده، فرایندهایی که برای اطمینان‌بخشی در سازمان برقرار شده‌اند، برای آزمون سیستمهای کنترلی در رابطه با ریسک‌ها و دستاوردهای سازمان و به‌منظور حصول اطمینان از وجود آن کنترل‌ها، مسئولیتی سه‌لایه دارند که عبارتند از:

- متناسب با ریسک‌ها،
- اثربخش در عملیات،

- کارا.

محدودیت‌های قانونی اعمال‌شده در سازمان‌ها از سوی چنین قوانینی همچون قانون ساربنز-آکسلی ایالات متحد یا **قانون قابلیت حمل و پاسخگویی بیمه سلامتی**[۴]، هیچ چیزی را فراتر از نمایش این ریسک‌ها به فرایندهای سازمانی نمی‌افزاید. به صورت اولیه، چارچوب قانونی برای حمایت از ذینفعان سازمان وجود دارد، که بیشتر اوقات دستکم سطوح عملکردی را در رابطه با ریسک‌هایی که معمولا در مسیر راه‌اندازی کسب‌وکار به وجود خواهند آمد، فراهم می‌کند.

نقش حسابرس در چارچوب‌های کنترلی نظام راهبری فناوری اطلاعات

یکی از گام‌های تدوین برنامه راهبردی فناوری اطلاعات در کسب‌وکارها، تعیین نقاط ضعف و چالش‌های موجود در اجرای فرایندهای سازمان و به‌تبع آن فناوری اطلاعات و استقرار ابزار این حوزه مطابق با برنامه‌های کلان راهبردی کسب‌وکارها است.

نقش حسابرس بیشتر متمایل به نقش یک مشاور در تدوین نظام راهبری فناوری اطلاعات در کسب‌وکارها است. هنوز هم حسابرس مسئول بررسی و اظهارنظر مستقل در مورد عملیات و کنترلهای شرکت است و باید این کار را در مجموعه برنامه‌های حسابرسی و در پی توافق با هیئت‌مدیره انجام دهد. اما، حسابرس می‌تواند در موارد زیر هم با مدیریت همکاری کند:

- تدوین و اجرای برنامه‌های ارتباطی و آگاه‌سازی،
- توصیه نکات کنترلی مناسب برای فرایندهای جدید کاری،
- تشخیص خطرها و نقاط ضعف در طرح‌ها، سیستمهای دردست ایجاد و نحوه به‌کارگیری فناوری اطلاعات مناسب با سیاست‌های سازمان.

مدیران بخش فناوری اطلاعات همچون دیگر رهبران شرکت، نگران درستی شناسایی فرایندها و کنترل‌ها هستند؛ مواردی همچون کنترل‌های داخلی و فرایندهایی که برای مدیریت خطر، کسب اطمینان از رعایت مقررات قانونی و انجام امور به روشی که همسو با هدف‌ها و ارزش‌های کسب‌وکارها باشد. با توجه به نقش حسابرس در تنظیم چارچوب راهبری فناوری اطلاعات کسب‌وکار یا بنگاه اقتصادی، گام‌های زیر در ایفای صحیح این نقش باید مدنظر قرار گیرد:

گام اول: در جریان قرار گرفتن حسابرس از روند تدوین برنامه‌های سازمان موجب می‌شود تا او بر روند تغییرات برنامه‌ریزی فناوری اطلاعات نظارت داشته باشد. با توجه به اینکه تغییرات انجام‌شده باعث به‌روزشدن فرایند برنامه‌ریزی استراتژیک و تدوین برنامه‌های کاری شود، کاملاً لازم است که حسابرس در بخشی از فرایند

مزبور دخالت داشته باشد و برنامه‌های کاری فناوری اطلاعات به او اطلاع داده شود.

گام دوم: کنترل فرایند تولید و توسعه سیستمهای کاربردی و نرم‌افزارها؛ یکی دیگر از مواردی است که به مشـارکت حسابرس نیاز دارد. حسابرس در این مشـارکت باید به‌منظور استقرار کنترل‌های داخلی مناسب و کمینه‌سـازی خطر، توصیه‌های لازم را به تیم تحلیل و طراحی سیسـتم بکند. مشارکت فعال حسابرس در گروه پروژه‌های ایجاد سیسـتمهای کاربردی، برای فرایند راهبری فناوری اطلاعات بسیار مفید است. راهبران شـرکت به گروه پروژه کمک می‌کنند تا هدف‌ها را تأمین و سیستمهای با کیفیت مناسب را مستقر کنند. حسابرس به اطمینان یافتن از کیفیت تولیدات، استانداردها و تأمین هدف‌های راهبران کمک می‌کند. مشارکت حسابرس در پروژه‌های ایجاد سیستمهای کاربردی در نقش مشاور راهبران و کنترل‌های داخلی شرکت است.

گام سـوم: حسـابرس باید فرایندهای بازرگانی فناوری اطلاعات را مورد رسیدگی قرار دهد تا مطمئن شود که فرایندهای مزبور:

- با ساختار و فرهنگ تشکیلات هماهنگ است،
- با خطرهای فناوری اطلاعات برخورد مناسبی دارد، و
- امکان تأمین هدف‌های بازرگانی را برای بخش فناوری اطلاعات ایجاد کرده است.

حسـابرس، با ابزارهای مناسـبی چون اسـتانداردها، قوانین و مقررات، هدف‌های کنترلی برای فناوری اطلاعات، رشـته‌های پیوسته و کسب مهارت در چاره‌سـازی و تحلیل خطرها می‌تواند منبع مهمی برای شناسـایی نقاط ضعف فرایندها و ارائه پیشنهادهای اصلاحی، برگرفته از بهترین روش‌های معمول در آن رشته از کار باشد.

گام چهـارم: حسـابرس می‌تواند با مسـاعدت در آمـوزش و آگاهی‌دادن درباره مدیریـت خطر، کنترل‌ها و بهترین روش‌های موجود، سهم خود را در راهبری فناوری اطلاعات، ایفا کند.

گام پنجم: حسـابرس باید با واحدهای ایمن‌سـازی اطلاعات، منابع انسانی، حقوقی و مدیریت خطر برای هماهنگ‌کـردن برنامه‌های حسابرسـی، همکاری کند تـا بتواند برخوردی هماهنگ و نقشـی حمایتی در ارزیابی خطرها، ایجاد طرح کنترل‌های مناسب و فرایندهای آزمون رعایت کنترل‌ها داشته باشد.

گام ششم: حسابرس باید از تمام دارایی‌های مربوط به کاربرد فناوری اطلاعات در شرکت، صورت‌برداری کرده و برای تشخیص اهمیت و خطرهای مربوط به هر یک از پروژه‌ها، سیستمهای کاربردی و زیرساخت‌ها و فرایندهای بازرگانی فناوری اطلاعات، همه آن‌ها را بررسی، ارزیابی و درجه‌بندی کند.

داراییهای مزبور باید به‌طور مرتب روزامد شـود و برای برنامه‌ریزی حسابرسی، تحلیل خطرها و ارزیابی رهبری فناوری اطلاعات مورد اسـتفاده قرارگیرد. دانش مفید، در اختیار داشتن اطلاعات درست در موقع مناسـب اسـت. با افزایش سطح مسئولیت حسـابرس در نظام جدید تجارت، توانایی حسابرس در تدوین

و تلفیـق اطلاعـات و آگاهـی از انواع جدید خطرها و کنترلها، اهمیت بیشـتری پیدا کرده اسـت. اسـاس این تواناییهای جدید، روشهای برگزیده عملیاتی، تولیدات ویژه و مجموعه‌ای از عملیات است که در هنگام ایجاد سیستمهای کاربردی جدید یا ارزیابی کاربردهای بازرگانی موجود می‌تواند مورد استفاده قرارگیرد. یکی از ابزار باارزش مدیریت خطر و حسابرسی در دسترس داشتن سیستم پشتیبانی است که بتواند وسایل و دانش لازم را در شرایط جدید، برای حسابرس تأمین کند.

گام هفتم: ارائه مسـتندات تهیه‌شـده از فرایندهای کنترلی و ارزیابی، به‌وسـیله حسـابرس به مدیران ارشـد سـازمان و مدیران فناوری اطلاعات اسـت تا در تدوین نظام برنامه راهبردی فناوری اطلاعات از آن بهره‌مند شوند.

نمونه‌ای از مدل نظام راهبری یکپارچه

یکی از مهم‌ترین وظایف هیئت‌مدیره هر سازمانی، پذیرش مسئولیت در برقراری مکانیزم‌ها و پایش عملیات اجرایی آن سـازمان به کمک حسابرسـان اسـت تا اطمینان حاصل کنند که سازمانها به هدفهای عملیاتی‌شان دسـت می‌یابنـد و اجـرای برنامه‌های مصوب سـازمان با قوانین تطابـق دارند. این موضـوع پایش عملیات، سیستمهای کنترلی و دقت گزارش‌دهی را پوشش می‌دهد.

منظور از پایش عملیات، کنترل و ارزیابی مداوم عملیات اجرایی بخش‌های مهم فرایندهای سـازمانی است که این مهم به کمیته حسابرسـی محول می‌شـود. کمیته حسابرسی سـه منبع دارد و می‌تواند به‌منظور کسب اطمینانـی که نیاز دارد، از آن‌ها اسـتفاده کند. ایـن کمیته می‌تواند از مدیریت هر فرایند، که مسـئولیت اصلی بـرای تحویـل نتایج بـه رهبران سـازمان را دارد، پرس‌وجو کرده یا می‌تواند از حسابرسـان داخلی و مسـتقل پرس‌وجو کند. این سه گروه هر یک، بخشی از اطلاعات چرخه کنترلی را فراهم می‌کنند، هرچند که اطلاعات جمع‌آوری‌شده از سوی هریک، از منظرهای متفاوتی و براساس نیازهای گوناگون، تهیه شده است. بنابراین، کمیته حسابرسی ممکن است تصویر کاملی از اطلاعات منبع‌یابی شده و مستقل از آن گروه‌ها را ایجاد کند.

سـازمان‌ها، فضای بسـیاری از فعالیت‌های اطمینان‌بخشی همچون اطمینان‌بخشـی کیفیت، سیستمهای شـکایات، گروه‌های مدیریت ریسک و حسابرسـان داخلی را در محیط کسب‌وکار خود مهیا می‌کنند، اما دیگر موارد اطمینان‌بخشی و ارزیابی چرخه‌های کاری جهت ارزیابی مستقل و به دور از روابط کاری به آنها تحمیل می‌شـوند (به‌طور مثال، حسابرسـان مسـتقل، بازرسـان انتظام‌بخشی). کمیته حسابرسـی برای رسیدگی به گزارشهای هریک از آنها، نتیجه جمع‌آوری اطلاعات و تحقیقاتشان را مورد مطالعه قرار می‌دهد.

ارزیابی و مدیریت ریسـک، در قسـمت میانی مدل نظام راهبری کلان سـازمان اسـت. ریسکها به‌واسطه هدفهای عملیاتی شـرکت، افزایش می‌یابند. این ریسـکها باید تا سـطوح درخور پذیرش، از طریق روشهای بهبودبخشـی، فرایندها را در حالت کنترلی نگهدارند. فرایندهای اطمینان‌بخش به‌گونه‌ای برقرار می‌شوند که

هیئت‌مدیره بتواند بدون شبهه، مدیریت ریسکها و دستیابی به هدفهای عملیات سازمانی را پایش کند (**تصویر ۳**).

نظام راهبردی فناوری اطلاعات

نظام راهبردی فناوری اطلاعات به‌طور منطقی یکی از زیرمجموعه‌های نظام راهبردی کسب‌وکار می‌باشد. این نظام، ملاحظات عملکردی و تطبیقی را پوشش می‌دهد. از آنجایی که فناوری اطلاعات، از ابزار توانمندسازی برای هر کسب‌وکاری است، بهترین تعبیر آن است که بگوییم، نظام راهبردی فناوری اطلاعات باید به‌منظور کمک به سازمان‌ها تدوین شده تا بیش از هر برنامه‌ای بتواند ساختار فناوری اطلاعات سازمان را به‌وجود آورد. این برنامه راهبردی در صدد کسب اطمینان از عملکرد فناوری اطلاعات سازمان است تا از آن به‌عنوان نقشه راه استقرار فناوری‌های نوین اطلاعاتی استفاده شده و راهبردها و هدفهای عملیاتی سازمان را حمایت کرده و بسط دهد.

ارزیابی ریسک فناوری اطلاعات

آسیب‌پذیری یک دارایی یا گروهی از دارایی‌ها می‌تواند به‌عنوان تهدیدی برای دیگر دارایی‌های سازمان تلقی شود. تأثیر یا شدت نسبی ریسک حاصل از میزان آسیب‌پذیری آن دارایی، متناسب با ارزش کسب‌وکار از خسارت/آسیب و فراوانی تخمینی تهدید مربوط به آن است. به همین منظور روش‌هایی برای ارزیابی ریسک در حوزه فناوری اطلاعات به‌عنوان دارایی وجود دارد که این روشها، مکانیزمهایی هستند برای شناسایی حوادثی که ممکن است هدفهایی عملیاتی، پیامدهای بالقوه آن حوادث و احتمال متناظر آن وقایع را تحت تأثیر قرار دهد. نتایج ارزیابی ریسک به‌وسیله حسابرس در حوزه فناوری اطلاعات، شامل فهرستی اولویت‌بندی‌شده از حوادث ممکن است که می‌تواند پایه‌ای را برای اقدام بیشتر در راستای آن ریسک تشکیل دهد. **تصویر ۴**، روش رتبه‌بندی را در فرایندهای کلی سازمان نشان می‌دهد. ریسک‌های با اولویت بالاتر نزدیک به گوشه راست بالای نمودار هستند.

ارزیابی ریسک فناوری اطلاعات، به دانش آسیب‌پذیری‌های فناوری، عیب‌های احتمالی در اجرای سیستمهای کامپیوتری و استنباط‌های متناظر فناوری از کسب‌وکار نیاز دارد، که این ریسک‌ها در حیطه وظایف حسابرس فناوری اطلاعات به سه نوع زیر تقسیم‌بندی می‌شود:

- ریسک‌های ذاتی- ریسکهای موجود در دوره عادی تحلیل یک فرایند از کسب‌وکار،
- ریسک کنترل- ریسکی که کنترلها از یک حادثه مضر، جلوگیری نکرده و یا آن را کشف یا اصلاح نخواهند

کرد.

- **ریسک‌های باقیمانده**[5] - ریسکهای بعد از اینکه کنترل‌ها در تحلیل فرایند در نظر گرفته می‌شوند.

منافع اصلی اعضای هیئت‌مدیره در مورد این ریسکها عبارتند از اینکه یک روش سیستماتیک برای شناسایی و ارزیابی آن‌ها وجود دارد؛ دامنه نوسان ریسک سازمان در تعیین روش بهبود مناسب در نظر گرفته شده است و درمان‌های تجویزشده مطابق انتظار در حال کار هستند. برخی ریسک‌ها ممکن است به اندازه‌ای باشند که اعضای هیئت‌مدیره نیاز به گزارش‌دهی روزمره در خصوص آن‌ها داشته باشد. فرایندهای مدیریتی هرروزه، بیشتر ریسک‌ها را اداره خواهند کرد.

سئوالات کلیدی برای پرسش عبارتند از:

- ریسک باقیمانده، همیشه با هر حادثه ممکن نزد سازمان درخور پذیرش است؟
- در آن شرایط، جایی که یک ریسک ذاتی جدی وجود دارد، آیا ریسک کنترل، درخور پذیرش است؟

اطمینان‌بخشی فناوری اطلاعات

اطمینان‌بخشی فناوری اطلاعات یکی از دغدغه‌های اصلی مدیران فناوری اطلاعات است که باید با استفاده از پاسخ دادن به چند سوال کلیدی، اطمینان لازم را به اعضای هیئت‌مدیره در خصوص صحت و کارایی نظام راهبردی فناوری اطلاعات بدهند. پاسخ به این سئوالها به‌گونه‌ای باید باشد که مدیران ارشد بتوانند تعهدات نظام راهبردی فناوری اطلاعات را به‌عنوان یکی از زیرمجموعه‌های برنامه راهبردی کلان سازمان پذیرفته و نسبت به تکمیل آن اقدام کنند. اطمینان‌بخشی مبتنی بر اطلاعات جمع‌آوری‌شده و یکپارچه است.

فرایند اطمینان‌بخشی، یکی از مواردی است که ابتدا باید به‌وسیله حسابرس فناوری اطلاعات مورد ارزیابی قرار گیرد، تا اطلاعاتِ موردنظر در قالب نشانگرهای مستقیم عملکرد یا تأیید چنین نشانگرهایی را فراهم کند. **تصویر ۵**، دیاگرامی را از کتاب «توجیه اعضای هیئت‌مدیره درباره نظام راهبری فناوری اطلاعات» برای نمایش جایگاه اطمینان‌بخشی فناوری اطلاعات در چارچوب نظام راهبری اقتباس می‌کند.

منابع اطمینان‌بخشی

همان طور که پیش از این پیشنهاد شد، هیئت‌مدیره‌ها یا کمیته‌های حسابرسی، در پی اطمینان‌بخشی از گستره‌ای از منابع هستند. قسمت عمده اطلاعاتی که آنها در تصمیم‌گیریها مورد استفاده قرار می‌دهند، از مدیران سازمان نشأت می‌گیرد. مدیران سازمان، بهترین دسترسی و گسترده‌ترین منابع را در اختیار دارند.

بنابرایـن، آن‌هـا می‌توانند بهترین اطلاعات را فراهم نمایند. اطلاعات مدیریتی، کارشناسـانه بوده و مسـتقل از عملیات نیسـت. اطلاعات مدیریتی مفید اسـت، اما ممکن است متوازن نباشـد. از این رو، اعضای هیئت‌مدیره مجبور می‌شوند نگاهی فراتر از اطلاعات در اختیار، به اظهارنظرهای مستقل که از سوی حسابرسان مستقل تهیه شده داشته باشند. به عبارت دیگر، اظهارنظر گستره‌ای از حسابرسان فناوری اطلاعات (هم داخلی و هم مستقل سازمان) باید به‌عنوان منابع اطمینان‌بخشی به‌وسیله اعضای هیئت‌مدیره کسب شود.

کیفیـت نظـام راهبردی سـازمان به کیفیت اطلاعاتی بسـتگی دارد کـه از اتاق هیئت‌مدیـره و صداقت فکری به کاربرده‌شـده از سوی اعضای هیئت‌مدیره اسـتخراج می‌شـود. اگر هیئت‌مدیره به‌طور کارا در حال فعالیت است، یا به عبارت دیگر سـوار بر کار اسـت، هر دو این اظهارنظرها، مورد نیاز هستند. کسب اطمینان از اینکه اطلاعات از چندین فرد مورد تأیید و از دو طرف مسـتقل دریافت می‌شـود، دلگرمی سـاختاری را برای هیئت‌مدیره‌ها برای کسـب بهترین اطلاعات کیفی فراهم می‌کند. تجربه نشان داده است که هیئت‌مدیره‌ها به‌طور کلی به دستکم سه منبع اطمینان‌بخشی مستقل احتیاج دارند (**تصویر ۶** را نگاه کنید).

حسابرسی فناوری اطلاعات

گزارشهای مدیریتی فناوری اطلاعات در راستای چارچوب نظام راهبردی فناوری اطلاعات سازمان، اطمینان‌بخشی ارزشـمندی را برای هیئت‌مدیره فراهم می‌کند. اطلاعات فراهم‌شده از سوی مدیریت فناوری اطلاعات به کمک اطلاعات تهیه‌شده به‌وسیله فعالیت‌های اطمینان‌بخشی مستقل همچون فعالیت‌های حسابرسان داخلی و مستقل متوازن تهیه می‌شوند.

فعالیت اطمینان‌بخشـی فناوری اطلاعات، عملکرد مدیریت این حوزه و فعالیت‌هایش را (شامل امنیت فناوری اطلاعـات) در مقابـل اسـتانداردهای مناسـب (همچـون **کوبیـت** (COBIT)، **کتابخانه زیرسـاخت فناوری اطلاعات**[۶] (ISO 17799 و BS 7799-2) بررسی خواهد کرد. اطلاعات مستقل فراهم‌شده از سوی گزارشهای اطمینان‌بخشی فناوری اطلاعات، اطمینان به هیئت‌مدیره را فراهم می‌کند.

در مـورد موضوعی مهم (به‌طور مثال، در رابطه با دقت گزارش‌دهی مالی)، دریافت مشـاوره از هر سـه بازوی فرایند اطمینان‌بخشی: مدیریت، حسابرس داخلی و حسابرس مستقل برای هیئت‌مدیره معقولانه است.

نتیجه‌گیری

نظـام راهبـردی فناوری اطلاعات زیرمجموعه‌ای از نظام راهبردی سـازمان اسـت و تدوین چارچوب آن نشـان می‌دهد، فناوری اطلاعات از ابزار قدرتمند و مدرن در سازمان‌های امروزی است. نظام راهبردی فناوری اطلاعات باید موضوعهای عملکردی (تولید ارزش) و تطابقی (تطبیق انتظام‌بخشی) را در برنامه راهبردی کلان سازمان به تصویر بکشد. چارچوب نظام راهبردی فناوری اطلاعات، نیاز به کنترل و ارزیابی عملکرد واقعی (اطمینان‌بخشی

از اینکه فرایندها به‌درستی در حوزه فناوری اطلاعات تحلیل و طراحی شده و مستقر شده‌اند و مطابق انتظار در حال کار هستند) دارد.

اقدامات فناوری اطلاعات ممکن است منجر به ایجاد مجموعه‌ای از استانداردها به‌عنوان پایه‌ای برای تحویل خدمات به سازمان شود، اما هدفهای عملیاتی خدمات فناوری اطلاعات به‌طور یکسان (برای ترویج موفقیت سازمان) باقی می‌ماند. مدیران فناوری اطلاعات، باید به‌طور آگاهانه، تطابق و عملکرد برنامه راهبردی فناوری اطلاعات را در نظر بگیرند (بدین معنی که، آن‌ها باید کلیه ریسک‌هایی را که با تحویل خدمات فناوری اطلاعات مرتبط هستند، نشان دهند).

از سوی دیگر حسابرسان فناوری اطلاعات، چه حسابرسان داخلی و چه حسابرسان مستقل، باید فعالیت مدیریت فناوری اطلاعات و متخصصان بخشهای مختلف این حوزه را بدون درنظر گرفتن شاخصهای مدیریتی دیکته شده، از طریق ارزیابی خود نسبت به فعالیتها و دستاوردهای فناوری اطلاعات، مورد ارزیابی قرار دهند.

در نهایت چارچوب نظام راهبردی فناوری اطلاعات باید براساس واقعیت‌های سازمان و با در نظر گرفتن برداشت‌های حسابرسان داخلی و مستقل، تدوین و در ساختار کلی برنامه راهبردی سازمان قرار گیرد.

پانوشتها:

1- Conformance

2- Committee of Sponsoring Organizations (COSO)

3- Enterprise Risk Management (ERM)

4- Health Insurance Portability and Accountability Act (HI PAA)

5- Residual Risks

6- Information Technology Infrastructure Library

منابع:

• Parkinson M. J.A. , and N.J. Baker, **IT and Enterprise Governance**, Information Systems Control Journal, Volume 3, 2005

• **Information Systems Control Journal**, Vol. 2, Information Systems Audit and Control Assocation (ISACA), 2002

• سروش علیرضا، **نظام راهبری بنگاه و فناوری اطلاعات**، ماهنامه عصر فناوری اطلاعات شماره ۹۱، مهر ۱۳۹۲

تصویر ۱- مدل نظام راهبری بنگاه

نظام راهبری برای موفقیت

نظام راهبری بنگاه

نظام راهبری برای محدودیت‌ها

مسئولیت امین ذیحسابی

قابلیت حمایت از خلق ارزش/ ثروت

عملکرد/ نتایج

تطابق/ تطبیق

تصویر ۲- هدفهای عملیاتی، ریسک‌ها، کنترل و اطمینان‌بخشی

هدفهای عملیاتی سازمانی

فرایند فرایندهای سازمانی

دستاوردهای سازمانی

سیستمهای کنترلی

ریسکها

فرایندهای اطمینان‌بخشی

تصویر ۳- چارچوبهای نظام راهبری

هدفهای عملیاتی نظام راهبری
ارزیابی ریسک
اطمینان‌بخشی حسابرسی داخلی
اطمینان‌بخشی مدیریت
نتایج عملکردی
نتایج بنگاه
نتایج تطابقی
اطمینان‌بخشی حسابرسی مستقل

تصویر ۴- مدل ریسک

زیاد
احتمال
تأثیر کنترل
ریسک کنترل
کم

کم
پیامد
زیاد

تصویر ۵- اطمینان‌بخشی فناوری اطلاعات

فعالیت‌های فناوری اطلاعات
تنظیم جهت‌گیری
مقایسه
تنظیم هدفهای عملیاتی
ارزیابی مستقل توسط حسابرس

فرایندهای اطمینان‌بخشی
اندازه‌گیری عملکرد

تصویر ۶- منابع اطلاعاتی نظام راهبری

مدیریت
حسابرسی داخلی
هیئت‌مدیره
حسابرسی مستقل