پالس حسابرسی داخلی

توصیف هم ترازی در یک فضای ریسک پویا

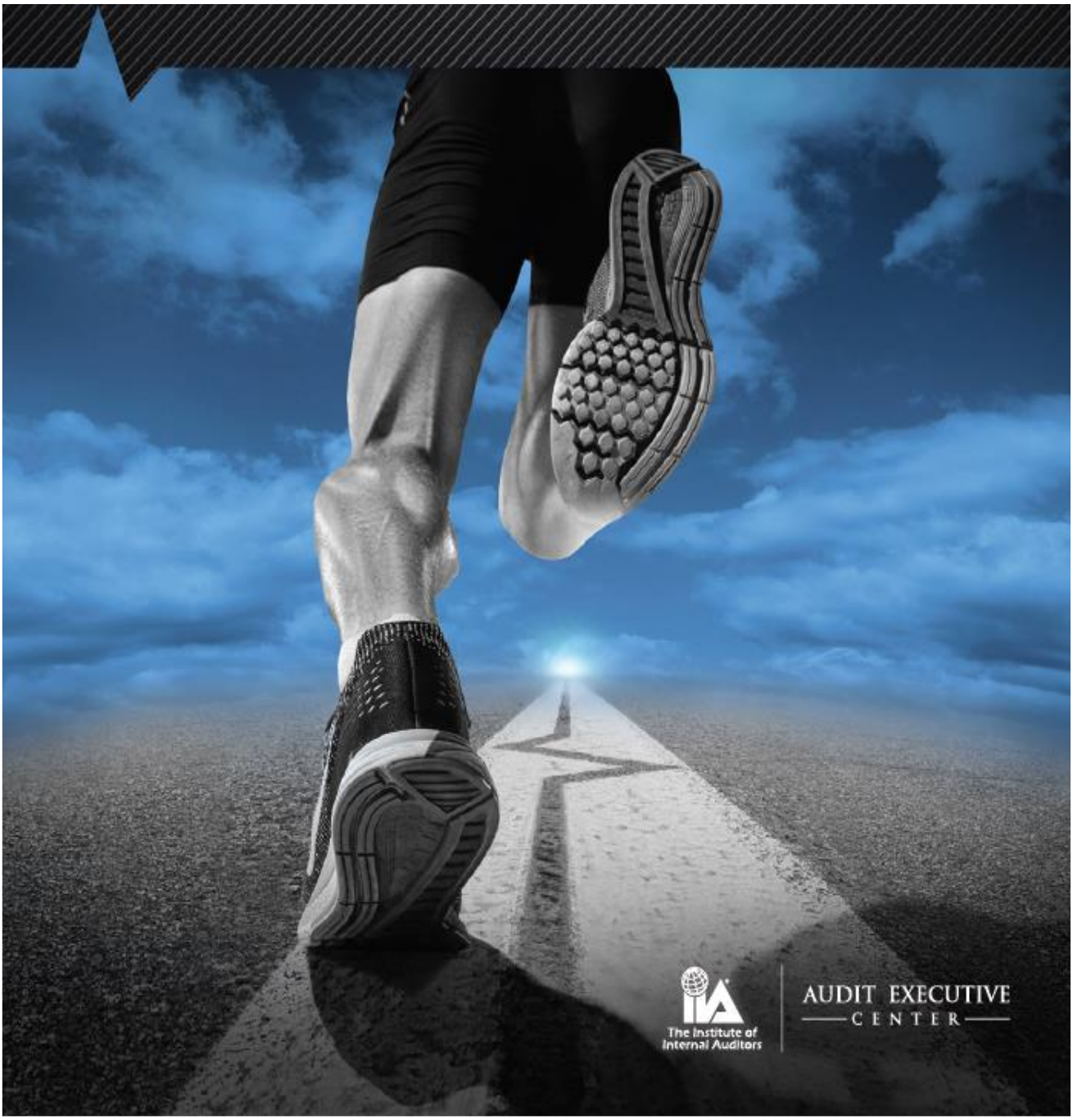
PULSE OF INTERNAL AUDIT

Defining Alignment in a Dynamic Risk Landscape

Audit Executive Center –Institute of Internal Auditors(IIA)

دکتر حسین کثیری

مترجمان: مریم لیلی دوست، مسعود بابائی، محسن مشیر

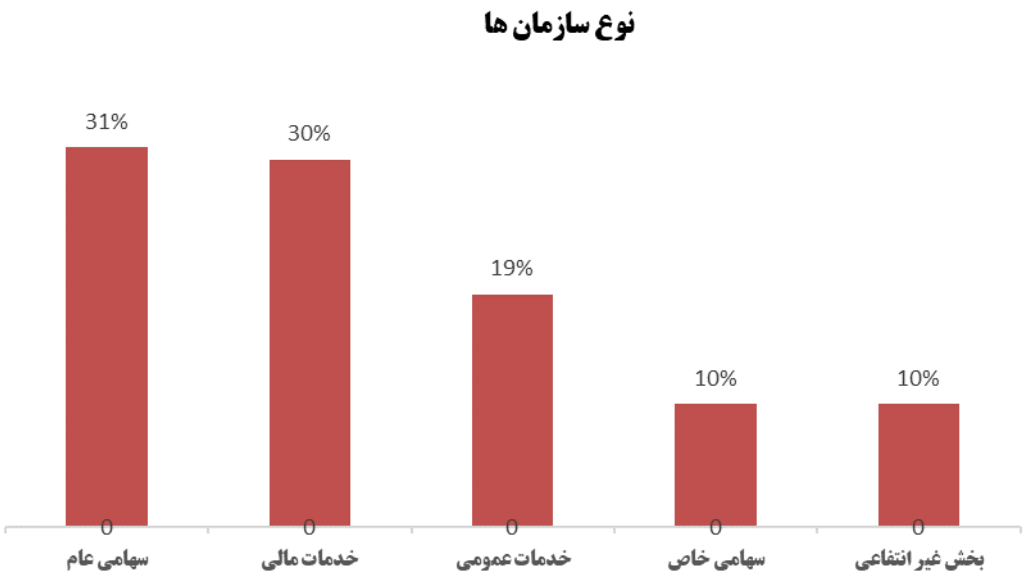


مرکز اجرایی حسابرسی IIA، نظرات صاحب نظران این حرفه را بوسیله "پرسش نامه سالیانه پالس حسابرسی داخلی" درسال 2011، تجمیع نموده است. پرسش نامه حاوی اطلاعاتی در خصوص مشکلات موجود و یا نوظهور بوده و به مسایلی که در این حرفه بسیار مهم هستند و همچنین به موضوعات مربوط به حوزه مدیریت حسابرسی داخلی (مثل تخصیص برنامه‌ها و تغییرات سطح کارمندان) می پردازد.

پرسش نامه آنلاین گزارش پالس آمریکای شمالی در سال 2019، از 5 سپتامبر تا 4 اکتبر 2018، جمع آوری شده است.

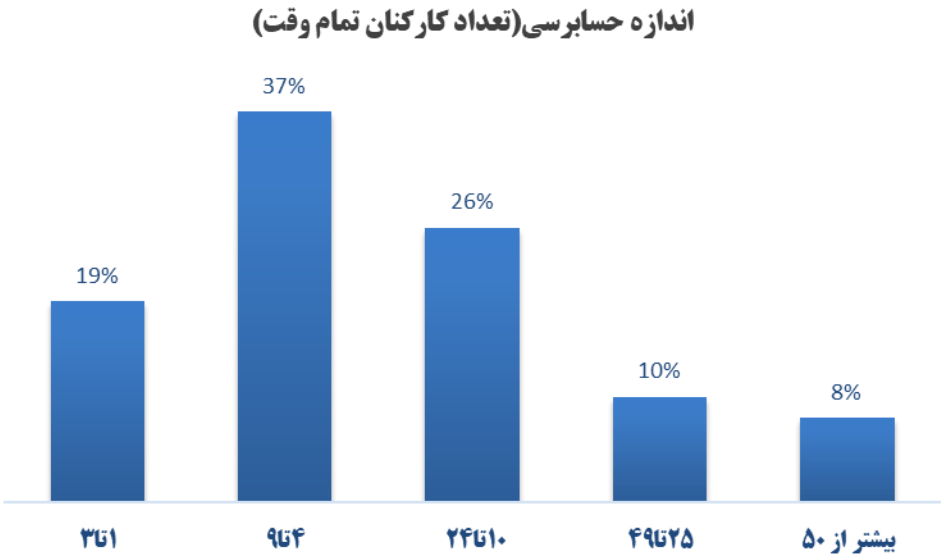
512 نفر در این بررسی شرکت کردند که 447 نفر آنها مدیران اجرایی حسابرسی بوده و الباقی سایر مدیران می باشند. 85درصد پاسخ دهندگان از آمریکا، 10 در صد از کانادا و مابقی از سایر کشورها می‌باشند.

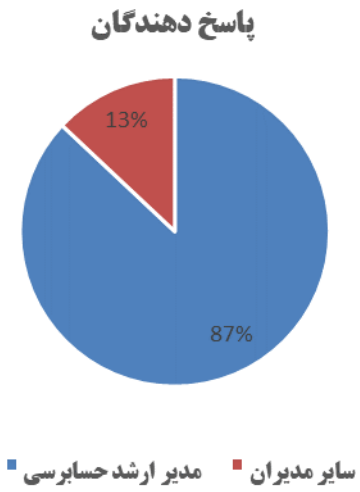
برای تجزیه و تحلیل، پاسخ دهندگان بخش مالی از سایر بخش‌ها جدا شده‌اند.

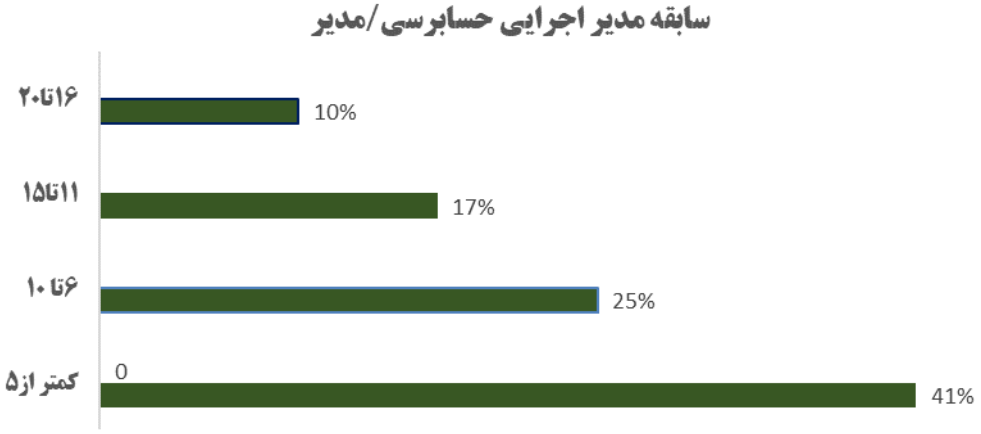


نتایج پرسش نامه در گزارشات مختلفی طرح و مورد تحلیل قرار گرفته است، بعضی از نتایج در سایت پالس حسابرسی داخلی IIA (www.theiia.org) در دسترس عموم قرار گرفته است.

گزارشات تخصصی تر نیز برای اعضای مرکز اجرایی حسابرسی (AEC) در دسترس می‌باشد. برای اطلاعات بیشتر در خصوص عضویت در AEC، صفحه (www.theiia/AEC) را ببینید.


اندازه حسابرسی(تعداد کارکنان تمام وقت)
37%
26%
19%
10%
8%
۳تا۱
۹تا۴
۲۴تا۱۰
۴۹تا۲۵
بیشتر از ۵۰


پاسخ دهندگان
13%
87%
مدیر ارشد حسابرسی
سایر مدیران


سابقه مدیر اجرایی حسابرسی/مدیر
۲۰تا۱۶
10%
۱۵تا۱۱
17%
۱۰تا۶
25%
کمتر از۵
0
41%

فهرست:

درباره مرکز اجرایی حسابرسیAEC: مرکز اجرایی حسابرسی بخش مهمی است که مدیران اجرایی حسابرسی (CAEs) را قادر می سازد موفق‌تر عمل کنند. واحد اطلاعات و خدمات مرکز، به مدیران اجرایی حسابرسی کمک می کند تا به چالش‌ها و ریسک‌های نوظهور پاسخ دهند. (اطلاعات بیشتر در www.theiia.org/AEC)

درباره IIA (انجمن حسابرسان داخلی): حسابرسان انجمن، وکلای شناخته شده در حرفه حسابرسی داخلی و تعریف کننده استانداردهای حسابرسی و نویسنده دفاتر راهنما و گواهینامه‌ها هستند. این سازمان در سال 1941 تأسیس شده و در حال حاضر 190.000 عضو از 170 کشور داشته و دفتر موسسه در لِیک ماری فلوریدا واقع شده است.

رفع مسئولیت:AEC و IIA، این سند به منظور اهداف آموزشی و اطلاعاتی چاپ شده است. از این کتابچه نباید به منظور رفع شرایط و بحران‌های خاص استفاده کرد و تنها جنبه راهنمایی دارد.AEC و IIA موکد توصیه می‌کنند به منظور حل مشکلات خاص از تجارب و دانش متخصصین استفاده گردد.AEC و IIA هیچگونه مسئولیتی در خصوص استفاده نابجا از این کتابچه ندارند.

خلاصه اجرایی

در اواخرسال سال 2019 تحقیقی بشکل پرسش نامه آنلاین ،توسط مرکز اجرایی حسابرسی (AEC)انجمن حسابرسان داخلی (IIA) با عنوان ،پالس حسابرسی:توصیف هم ترازی در یک فضای ریسک پویا ،حاوی اطلاعاتی در خصوص مشکلات موجود و یا نوظهور در حرفه حسابرسی داخلی انجام شد . 512 نفر در این بررسی شرکت کردند که 447 نفر آنها مدیران اجرایی حسابرسی داخلی(CEAs) و الباقی سایر مدیران و 85درصد پاسخ دهندگان از آمریکا، 10 در صد از کانادا و مابقی از سایر کشورها بودند. نتیجه این بررسی بشرح زیر می باشد.

در طول دهه گذشته، سرعت ظهور ریسک‌های جدید به صورت عجیبی افزایش یافته است و شرکت‌ها و سازمانها را مجبور کرده تا با استراتژی‌های جدید، خود را سازگار و اولویت‌های خود را دوباره تعریف کنند ،تا قادر به ادامه فعالیت و رشد در محیطی پر از ریسک‌های پیچیده و فزاینده باشند.

رشد فزاینده چالش‌هایی از قبیل تکنولو ژی‌های مخرب، عدم قطعیت‌های ژئوپلتیکی و شرایط اقتصاد جهانی، اهداف سازمانها را تهدید می‌کنند و کلیه بازیگران در مدیریت ریسک را مجبور می‌کند تا همواره آگاه و آماده باشند. اعضای هیئت مدیره، کارمندان سایبری حرفه‌ای را به تیمشان اضافه می‌کنند و از مدیریت اجرایی‌شان اطلاعات بهتری در خصوص مدیریت ریسک ،خصوصاً در ارتباط با امنیت سایبری (فضای مجازی) درخواست می‌کنند. آن‌ها همچنین آگاه هستند که باید دانش خود را در خصوص تبعات و اثرات ریسک‌ها و فرصت‌ها، ارتقاء دهند. تقویت نظارت بر اجرای استراتژی‌ها و مدیریت ریسک از اولویت‌های اولیه هیات مدیره هامی‌باشد. بر اساس بررسی که توسط انجمن ملی مدیران شرکتها در سال 2018-2019 انجام گردید ،هیئت مدیره و مدیران اجرایی، به حمایت از حسابرسی داخلی برای همکاری در بخش مدیریت ریسک ادامه داده‌اند و این امر از رشد همکاران در بخش حسابرسی داخلی پیداست. تعداد مدیران اجرایی حسابرسی (CEAs)که افزایش تعداد کارکنان را گزارش کرده اند دو برابر تعداد مدیرانی بوده است که کاهش اعلام کرده اند.همراستایی دیدگاه‌های مدیریت اجرایی و هیئت مدیره و حسابرسان داخلی در خصوص ریسک، به منظور خدمت رسانی موفق حسابرسی داخلی و این که به عنوان منبعی ضروری و با ارزش افزوده محسوب گردد،بسیار حائز اهمیت است.حسابرسی داخلی می‌بایست هم راستا با هیئت مدیره و مدیریت اجرایی فعالیت کند، همچنین ضروریست که انها شناختی از دیدگاه ذینفعان نسبت به ریسک‌ها و فرصت‌ها داشته باشند. شروع و خاتمه این امر اطمینان از این موضوع است که هیئت مدیره، اطلاعات کامل و صحیحی از اینکه پایه تصمیمات خود را کجا بنا کند. مدیران حسابرسی داخلی می‌بایست برای مباحث رهنمون گر آماده باشند، چرا که ممکن است مدیریت در شناخت ریسکهای خاصی تأخیر داشته باشد . همچنین در صورتی که مدیریت به نحو مناسبی بر موضوع متمرکز نباشد، انها می‌بایست قدرت بیان مطالب و اظهار نظر داشته باشد.

اهدف این گزارش ،فراهم کردن دانش و راه و روشی جهت کمک به حسابرسان داخلی است که بتوانند مدیران اجرایی و هیئت مدیره را درخصوص 4 ریسک مهم آگاه کنند: این 4 ریسک مهم عبارتست از: 1)اطلاعات و امنیت سایبری، 2)ریسک‌های شخص ثالث، 3)ریسک‌های نوظهور و غیرمعمول و 4)فعالیت مدیریت و هیئت مدیره.

اطلاعات پرسشنامه نشان دهنده عدم توازن در فضای ریسک‌ها ی فوق بوده و نیاز است که مدیران اجرایی حسابرسی این نگرانی‌ها را با کمیته حسابرسی‌شان مطرح و برطرف کنند.

1)امنیت فضای مجازی و محافظت دیتا: امنیت سایبری

حسابرسی داخلی باید تلاش‌های خود را برای ارائه خدمات اطمینان بخشی و مشورتی در این زمینه بهبود بخشد. این نیازمند ایجاد روابط محکم با CIOها و CISOها و سرعت بخشیدن به تلاش در زمینه ساخت تیم‌های سایبری زیرک ازطریق آموزش و استخدام‌های جدید یا همکاری خارج سازمانی می باشد. مدیران اجرایی حسابرسی باید در مورد داشتن برنامه حسابرسی مناسب که منعکس کننده اهمیت خدمات اطمینان بخشی سایبر ی و فناوری اطلاعات باشد ، اگاه باشند و در مورد هر حوزه ای که مدیر اجرایی حسابرسی احساس می‌کند که حسابرسی داخلی باید خود را در آن زمینه تقویت کند به گفتگو بپردازد.

در حالیکه فضای مجازی و فناوری اطلاعات (IT) حدود 20٪ متوسط تصمیمات حسابرسی را پوشش می‌دهند، این مشکلات کلیدی به طور مداوم توسط هیئت مدیره به عنوان فاکتورهایی با ریسک پایین و همانند موضوعات گزارش گری عملیاتی، مالی و تطبیق با قوانین در نظر گرفته می‌شود. به علاوه ،مدیران اجرایی حسابرسی گزارشی مبنی بر رشد آهسته در دانش فناوری اطلاعات (IT) و مهارت‌های دنیای مجازی کارمندان را تهیه می‌کنند و شکاف بین تلاش حوزه حسابرسی داخلی در زمینه امنیت فضای مجازی و سطحی که مدیران اجرایی حسابرسی باور دارند که آن‌ها باید در خصوص امنیت فضای مجازی بایدبطورگسترده فراهم سازند، مشخص نمایند

یک مورد اقدام بالقوه مدیران اجرایی حسابرسی داخلی، متوازن نمودن علاقه روبه افزایش هیئت مدیره و وارد شدن به مشکلات امنیت فضای مجازی به منظور بروزرسانی و تطبیق روش‌های حسابرسی و همچنین برداشتن گام‌هایی در جهت رفع چنین شکاف‌هایی در حوزه چنین ریسک کلیدی می‌باشد. ضمناً مدیران اجرایی حسابرسی داخلی می‌بایست کلیه انتخاب‌ها را مدنظرقرار دهد، به عنوان مثال ،هم سپاری به منظور افزایش مهارت سایبری کارمندان را میتوان نام برد. بحث‌های صادقانه با کمیته حسابرسی در خصوص موانع حوزه ی حسابرسی داخلی، این اطمینان را می‌دهد که مشکلات آتی سایبری موردتوجه قرار گرفته‌اند.

2)ریسک‌های شخص ثالث

ارتباط شخص ثالث ،بخشی از اکوسیستم ریسک های هر سازمانی است و سازمانهایی که نتوانند به طور صحیح به ریسک‌های شخص ثالث رسیدگی کنند در معرض مخاطره هستند. حسابرسی داخلی باید به هیئت مدیره و مدیریت اجرایی در زمینه ریسک های ضعف یا عدم وجود کنترل در روابط شخص ثالث آموزش دهد و با کمیته حسابرسی و مدیریت برای تعریف نقشی که حسابرسی داخلی بایستی برای اطمینان بخشی در این حوزه مهم ایفا نماید همکاری نزدیک داشته باشد.

نظارت سازمانی بر روابط شخص ثالث، توسط نیمی ازمدیران اجرایی حسابرسی به عنوان ضعف دیده می‌شود. پاسخ‌های نظر سنجی به طور واضحی نگرانی مدیران اجرایی حسابرسی داخلی در خصوص نحوه انتخاب و نظارت شخص ثالث را نشان می‌دهد و اینکه اگر

سازمانها حوزه فروشندگان را به درستی مدیریت نکنند ،چگونه آسیب خواهند دید. یک مورد توصیه شده برای مدیران اجرایی حسابرسی این است که به ذینفعان آموزش دهند که روابط شخص ثالث جزئی از اکوسیستم ریسک سازمان است و نباید آن را به صورت جداگانه در نظر گرفت. همچنین مدیران اجرایی حسابرسی باید حساسیت در خصوص کنترل‌های ضعیف بر روی ریسک‌های شخص ثالث را در کمیته حسابرسی افزایش دهند. این روابط، نیازمند همان سطحی از مدیریت ریسک است که سایر ریسک‌هایی که بر سازمان به طور مستقیم تأثیر می‌گذارند، نیاز به مدیریت دارند

3)ریسک‌های نوظهور و غیر عادی

تهدیدات ناشی از ریسک‌های نوظهور و غیرعادی با توجه به این که فناوری سرعت بلوغ و امکان آسیب رسانی آنان را افزایش داده است در حال رشد می باشند. مدیران اجرایی حسابرسی‌ها باید در مورد ریسکهای نوظهور و غیر عادی که می‌توانند روی سازمانها تأثیربالقوه بگذارند، آموزش دریافت نمایند. مدیران اجرایی حسابرسی باید هنگامی که سازمان فقط به اطمینان بخشی مدیریتی در مورد کاهش ریسک های نوظهور و غیرعادی متکی می باشد سخن بگویند. مدیران اجرایی حسابرسی باید شاخص‌های ریسک های کلیدی قوی‌تری را برای اطمینان بخشی از فرایند هایی که به منظور شناسایی، نظارت و کاهش ریسک های نوظهور و غیرعادی در نظر بگیرند.

گزارشات مدیران اجرایی حسابرسی نشان می‌دهد که هیئت مدیره در خصوص شناسایی و ارزیابی ریسک‌های نوظهور و غیر عادی بیشتر به مدیریت متوسل می‌شوند تا حسابرسی داخلی ، در حالیکه اکثرمدیران اجرایی حسابرسی ادعا می‌کنند که سازمان‌ها، قدرت شناسایی و ارزیابی چنین ریسک‌هایی را دارند. تقریباً نیمی از آنها می گویند که این تقریباً عادی است که ظهور چنین ریسک‌هایی مدیریت را در طی یک سال متعجب و شگفت زده نماید . هشدار به هیئت مدیره در خصوص سوء استفاده احتمالی، در زمان بروز ریسک‌های نوظهور و غیرمعمول اولین گام برای بازکردن درب به سوی حسابرسی داخلی در جهت ایفای نقش بزرگتری (در زمان بروز چنین ریسک‌هایی) می‌باشد. مدیران اجرایی حسابرسی می‌بایست از نظارت شاخص‌های کلیدی ریسک (KRI) که شامل پیش زمینه‌های ظهور ریسک‌های نوظهور هستند، حمایت کنند.

4)هیئت مدیره و فعالیت مدیریتی

امروز بیشتر از گذشته برای تأمین نظارت پیشبینانه صحیح، قانون گذاران و سهامداران بر هیات مدیره فشاروارد می‌کنند. آن‌ها در صورتی می‌توانند به بهترین شکل ممکن این کار را انجام دهند که اطلاعاتی که تصمیمات خود را بر آن پایه گذاری می‌کنند دقیق و کامل باشد. مدیران اجرایی حسابرسی باید در مورد کلیه اطلاعاتی که به هیئت مدیره می‌رود اطمینان فراهم کنند و هیئت مدیره و مدیریت اجرایی را در مورد مزایایی که اطمینان بخشی مستقل می‌تواند فراهم آورد، آگاه سازند.

امروزه مدیریت چالش‌های پیش روی حسابرسان داخلی– که پیچیده، شتاب یافته و جهانی می باشند– به چابکی، نوآوری و گفتگوی مؤثر با هیئت مدیره و مدیریت اجرایی نیاز دارد. این امر به یک الزام اساسی نیاز خواهد داشت تا این اطمینان حاصل شود که اطلاعاتی که هیات مدیره در اختیار دارد دقیق، کامل، به موقع، شفاف و قابل اعتماد است. برای اینکه حسابرسی داخلی بتواند جایگاه خود را در این دنیای جدید پیدا کند، باید با شهامت صدای خود را بلند کنند.

بیش از نیمی از پاسخ دهندگان می گویند که حسابرسی داخلی هرگز و یا به ندرت، در مورد اطلاعاتی که توسط مدیریت به هیئت مدیره ارائه می‌گردد اطمینان و اطمینان بخشی را فراهم نمی‌آورد. همزمان اعضای هیئت مدیره می گویند که کیفیت اطلاعات ارائه شده توسط مدیریت می‌بایست بهبود یابد ضمناً گوناگونی وظایف و مسئولیت‌های کمیته ممکن است مانع دسترسی هیئت مدیره به یافته‌ها و دیدگاه‌های حسابرسی داخلی در خصوص حوزه‌های ریسکی کلیدی همانند امنیت سایبری گردد.

مدیران اجرایی حسابرسی باید آمادگی اطمینان بخشی به اطلاعاتی که به هیئت مدیره می‌رود را داشته باشند، همچنین تلاش کنند تا در کمیته‌های کلیدی دیگر هیئت مدیره ،همانند فناوری اطلاعات، ریسک و کمیته‌های جبران خدمات حضور یابند تا اطمینان حاصل کنند که دیدگاه‌های حسابرسی داخلی به وضوح به هیئت مدیره اعلام شده‌اند.

استفاده از این گزارش

با استفاده از افزایش بینش فراهم شده توسط این گزارش ، مدیران اجرایی حسابرسی می‌توانند ذینفعان را از عدم توانایی بالقوه در این حوزه‌های کلیدی ریسک آگاه کنند و از راه‌های توصیه شده برای شناسایی و رسیدگی به هر گونه ضعف یا سوء استفاده که ممکن است در سازمانشان وجود داشته باشد، بهره مند سازند. با بحث و گفتگو با کمیته حسابرسی، نگرانی‌های موجود جهت اقدام و رسیدگی ثبت خواهند شد. همانند سال‌های گذشته، نتایج پرسشنامه، اطلاعات با ارزشی در خصوص برنامه‌های حسابرسی، کارمندان و برون سپاری ارائه می‌دهد . این گزارش حاوی روند سه ساله برنامه حسابرسی بر اساس نوع سازمان می‌باشد. هر حوزه‌ای از ریسک سوء استفاده، نه تنها ریسک‌های واضح سازمان را نمایش می‌دهد، بلکه اطمینان به اینکه حسابرسی داخلی نیز تضعیف شده باشد را نیز نمایان می‌سازد. همانند اغلب موارد بحرانی، حسابرسی داخلی در مقابل سؤال اجتناب ناپذیر "حسابرسی داخلی کجا بود؟" قربانی خواهد شد. مدیران اجرایی حسابرسی می‌توانند در مواقعی که ضعف کنترلی یا سوء استفاده‌ای شناخته نمی‌شود و یا زمانیکه ریسک‌ها به درستی شناسایی نمی‌شوند در مقابل چنین انتقاداتی صدای خود را بلند کرده و ازخود محافظت کنند. از این گذشته، ریسکی که به گفتگو گذاشته نشود تنها یک ریسک مفروض است

معرفی

هم ترازی: جایگاه توافق یا اتحاد

بحث در خصوص هماهنگی کار حسابرسی داخلی با نیازهای هیئت مدیره، عموماً به توان درک نیازهای هیئت مدیره و مدیران اجرایی توسط مدیران اجرایی حسابرسی تمرکز دارد.

آنچه سهامداران را از خواب شب بازمی‌دارد یا آنچه که باید آنها را نگران کند، هدایت می کند رهبران حسابرسی داخلی را برای اینکه بدانند چه چیزی در اتاق‌های هیئت مدیره و مدیران ارشد اهمیت دارند.

این شامل درک درجه و راستای مورد نظر سهامداران در مورد تعادل بین فرصت‌ها و تهدیدهای ناشی از ریسک می‌باشد.

برای دستیابی به این اهداف، مدیران اجرایی حسابرسی می‌بایست بیشتر در خصوص صنایع سازمانی خود اطلاعات کسب کنند، فعالیت‌های اقتصادی خود را بشناسند و رابطه قوی‌تری با هیئت مدیره و کمیته حسابرسی، مدیران اجرایی و دیگر متخصصان ریسک در سازمان برقرار کنند.

این امر به ناچار نیازمند مکالمات شجاعانه توسط مدیران اجرایی حسابرسی می‌باشد. منابع بی شماری برای کمک به مدیران اجرایی حسابرسی وجود دارد تا به تفکر هیئت مدیره دست پیدا کنند که از آن جمله پرسش نامه سالانه NACD (The National Association of Corporate Directors(انجمن ملی مدیران شرکتها)) برای هیئت مدیره می‌باشد. به عنوان مثال پرسشنامه 2018-2019 طبق نظر اعضاء هیئت مدیره در سال 2019، تغییرات در شرایط نظارتی، چشم انداز کندی نزول اقتصادی، رشد تهدیدهای امنیت سایبری، اختلال در مدل کسب و کار و بدتر شدن نوسانات ژئوپلتیکی را به عنوان ریسک‌های مهم معرفی کرده است. مدیران اجرایی حسابرسی باید از مطالبی که هیئت مدیره و مدیریت اجرایی مطالعه می‌کنند، آگاه بوده و همان مطالب را مطالعه کنند تا از آنها جلوتر باشند.

در حالی که چالش هیئت مدیره در جهت شناسایی، درک و نشان دادن عکس العمل در مقابل ریسک دشوار است، هیئت مدیره می‌داند که ریسک‌ها فرصت هایی را نیز پیشنهاد می دهند.

مطابق یافته‌های کلیدی پرسش نامه NACD در سال 2019-2019، مدیران، هوش مصنوعی (AI) را به عنوان بزرگ‌ترین مزاحم تکنولوژِی می‌دانند، اما همچنین آن را به عنوان بزرگترین توانمند ساز که احتمالاً در 12 ماه آینده به نفع سازمانشان خواهد بود نیز شناسایی می‌کنند.

مدیران اجرایی حسابرسی بیشتر از گذشته باید نسبت به تکنولوژی آگاه باشند و بتوانند راحت در مورد تکنولوژی و تکنولوژی مشکل آفرین صحبت کنند. مطمئناً تکنولوژِی به طور کلی سرعت رشد پیشرفت تجارت را افزایش داده و همچنین سرعت ظهور و بلوغ ریسک‌ها را نیز افزایش داده است.

اینترنت دری به سوی انقلاب صنعتی چهارم باز کرده و همچنین جهان را با حملات سایبری آشنا ساخته است.

در واقع چالش‌های روبه رشد امنیت سایبری و حفاظت اطلاعات به طرز چشم گیری اولویت‌های ریسک را تغییر داده است و ریسک‌های تطبیق جدیدی ایجاد کرده است؛ همانند ایجاد قوانین سایبری جدید در اروپا، آمریکا و چین، جنبش حریم خصوصی داده‌ها، وعده پیچیده‌تر کردن مشخصات ریسک فناوری را می‌دهد و نیازمند مشارکت و اطمینان بیشتری از سوی حسابرس داخلی است.

این تحولات نشان دهنده اهمیت و ضرورت بیشتر این امر است که هیئت مدیره می‌بایست به اطلاعات کامل و صحیح که بر اساس آنها تصمیم گیری می‌کند، دسترسی داشته باشد.

حسابرسی داخلی می‌تواند به پر کردن این نقش کمک کند، دقیقاً همان گونه که نقش حسابرس داخلی در سازمان استنتاج از واکنش‌های ارائه شده و اطمینان بخشی ادراک منفعل به یکی از بینش‌ها و بصیرت‌های تحریک کننده است، بنابراین می‌بایست دیدگاه خود را نیز در خصوص تغییرات لازم در هیئت مدیره بسط دهد.

در محیط ریسک پویای امروزمدیران اجرایی حسابرسی باید نقش بیشتری از فهم و رعایت قواعد توسط هیئت مدیره داشته باشند، این چشم انداز جدید می‌بایست بر این اساس باشد که هیئت مدیره درک کامل و بدون ابهامی از ریسک‌های جهانی سازمان دارد. این تغییر چشم انداز، در عین ظرافت، نقش بسیار مهمی را در توانایی حسابرسی داخلی در تأمین اطمینان بخشی، اضافه کردن ارزش به سازمان و افزایش استفاده از مشاورین قابل اعتماد، بازی می‌کند.

هماهنگی با هیئت مدیره و مدیریت اجرایی

مدیران اجرایی حسابرسی باید از هر فرصتی برای ارتقا اگاهی خود، در خصوص دیدگاه‌های هیئت مدیره و مدیریت اجرایی در مورد ریسکها برای هماهنگی بیشتر با آنها، استفاده کند. این کار با مکالمات مداوم بین مدیران اجرایی حسابرسی و ذینفعان کلیدی حسابرسی داخلی امکان پذیر است. (ایجاد) ارتباطات، به منظور کسب هماهنگی بسیار مهم است.

این امر همچنین شامل داده های پرسش نامه و سایر منابعی است که بینش بیشتری در خصوص هیئت مدیره و مدیریت اجرایی و نیز هر آنچه که بر دیدگاه هیئت مدیره و مدیریت اجرایی اثر می‌گذارد فراهم میکند.

درک چشم انداز هیات مدیره و مدیران اجرایی سایر سازمان‌ها نیز اهمیت زیادی دارد، با این حال هر ذینفعی متفاوت است؛ بنابراین مدیران اجرایی حسابرسی باید بادیدگاه های ویژه هیئت مدیره و مدیریت اجرایی در مورد ریسک منطبق باشند.

منابع برای درک و ارتباط برقرار کردن با هیئت مدیره و مدیران ارشد

<u>هیئت مدیره چه می‌گوید:</u>

1- پرسش نامه جهانی سالیانه **CED**
2- پرسش نامه مدیران شرکت‌ها
3- چشم اندازهای اجرایی بر ریسک‌های مهم (دانشگاه کارو لینای شمالی **ERM**)
4- پرسش نامه مدیریت شرکت‌های عمومی **NACD**(انجمن ملی مدیران شرکتها)

<u>هیئت مدیره چه می‌خوانند:</u>

1- گزارشات ریسک‌های جهانی و فرم اقتصاد جهانی
2- گزارش کمیسیون روبان آبی **NACD** (انجمن ملی مدیران شرکتها)
3- گزارش چشم انداز دولت **NACD** (انجمن ملی مدیران شرکتها)

<u>آنچه که حسابرس داخلی می‌بایست به اشتراک بگذارد:</u>

1- پالس حسابرس داخلی **(IIA)**
2- فضای اخلاقی در راس سازمان(**tone at the top**) **(IIA)**
3- ریسک تمرکز: موضوعات مهم برای حسابرسین داخلی (مؤسسات حسابرس داخلی کنفدراسیون اروپا)

بخش اول

امنیت سایبری و حفاظت از داده

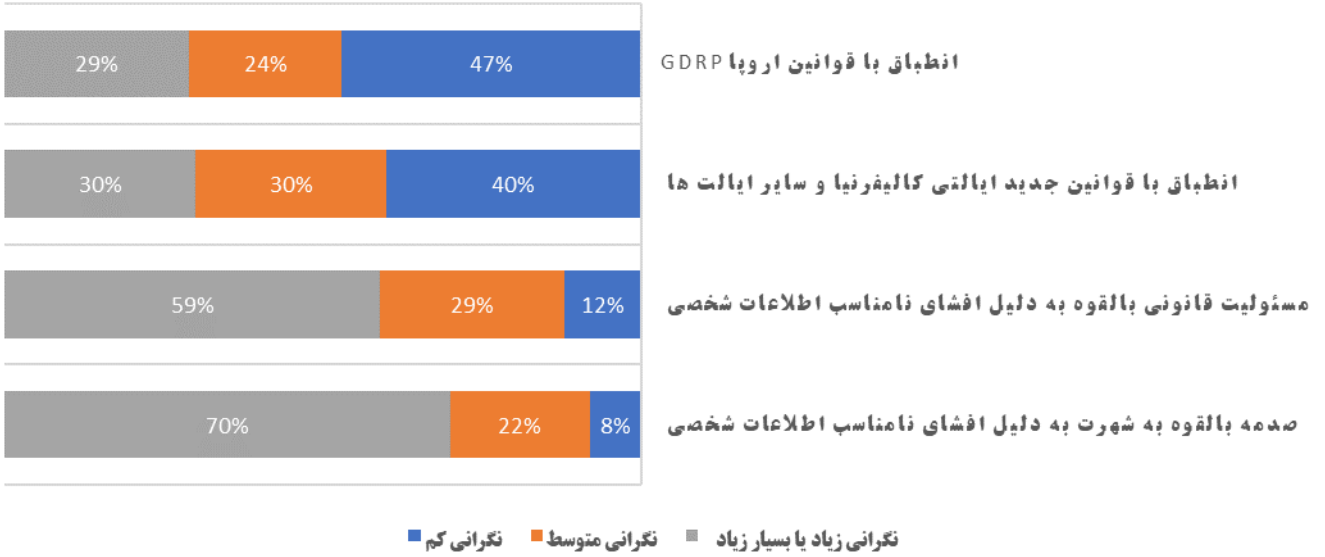
پرسشنامه پالس متوجه شده که فضای سایبری و تکنولوژی اطلاعات از مهم‌ترین ریسک‌ها توسط پاسخ دهندگان معرفی شده‌اند.

بزرگ‌ترین نگرانی مدیران اجرایی حسابرسی، آسیب بالقوه به شهرت سازمان است، که ناشی از افشای نامناسب اطلاعات خصوصی بوده است، حدود 7 نفر از 10 نفر، این مسئله را فضای نگرانی بزرگی در سازمان خود شناسایی کرده‌اند. (شکل 2) این نگرانی نشان دهنده هماهنگی با هیئت مدیره است، که به طور مداوم تهدیدات امنیت سایبری را به عنوان 5 عامل مهم که به سازمانشان ضربه می زند معرفی کرده‌اند. (مطابق با نظرسنجی NACD در سال 19-2018)

با این حال، نگرانی در خصوص انطباق با قوانین جدید حفاظت اطلاعات، همانند قوانین آمریکا درایالت های کالیفرنیا و نیویورک و یا قوانین عمومی حفاظت اطلاعات اتحادیه اروپا (GDPR) به عنوان ریسک‌های پایین‌تر شناسایی شده است و 47 درصد از پاسخ دهندگان ادعا کرده‌اند سازمانشان در این خصوص نگرانی کمی داشته و یا هیچ نگرانی ندارند. (شکل 1)

70٪ ازمدیران اجرایی حسابرسی ریسک صدمه به شهرت شرکت را ناشی از رخنه اطلاعات خصوصی به بیرون می‌دانند و آن را به عنوان نگرانی بسیار مهم سازمان شناسایی می‌کنند.

شکل 2. نگرانی‌های سازمانی در خصوص ریسک‌های حریم شخصی



یادداشت: (سوال 9) Q9 : میزان نگرانی سازمان خود را در مورد حریم شخصی داده های کارمندان یا شخص ثالث که توسط سازمان شما نگهداری می شود، بیان کنید. آن‌ها که پاسخ " قابل استفاده نیست " را انتخاب کرده‌اند در تجزیه و تحلیل این متغیر در نظر گرفته نشده‌اند.

این مسئله برخی سوء تفاهم‌ها در مورد چگونگی و زمان محافظت از اطلاعات و قوانین حریم شخصی را نشان می‌دهد. به عنوان مثال، برخی ازمدیران اجرایی حسابرسی در آمریکا ممکن است متوجه نشوند که سازمانشان به همان اندازه مسئول پیروی از قوانین GDPR هستند که همتایان اروپایی‌شان می‌باشند. این مسئله بدین خاطر است که قوانین ارتباطی به محل قرارگیری سازمان ندارند، بلکه به مکانی بستگی دارد که اطلاعات مشتری در آن جمع شده است. هر سازمانی که مشتریانی در سطح اروپا دارد ملزم است که مقررات مربوط به حریم خصوصی و محافظت از داده‌های مندرج در GDPR را رعایت کند.

چه بسا، به این نکته باید توجه کرد که نگرانی در خصوص انطباق قوانین GDPR همانگونه که اندازه سازمان بزرگ‌تر می‌شود، افزایش می‌یابد.

به عنوان مثال، در سازمانی با بیش از 50/000 کارمند،62 درصد، انطباق با قوانین GDPR را بسیار مهم ارزیابی کرده‌اند.

این مسئله نشان می‌دهد که سازمان‌های بزرگتر به احتمال قوی‌تر؛ عملیات بین المللی بیشتری دارند و لذا می‌بایست بیشتر به قوانین GDPR عمل کنند.

شکاف تلاش، محدوده‌ای از نگرانی

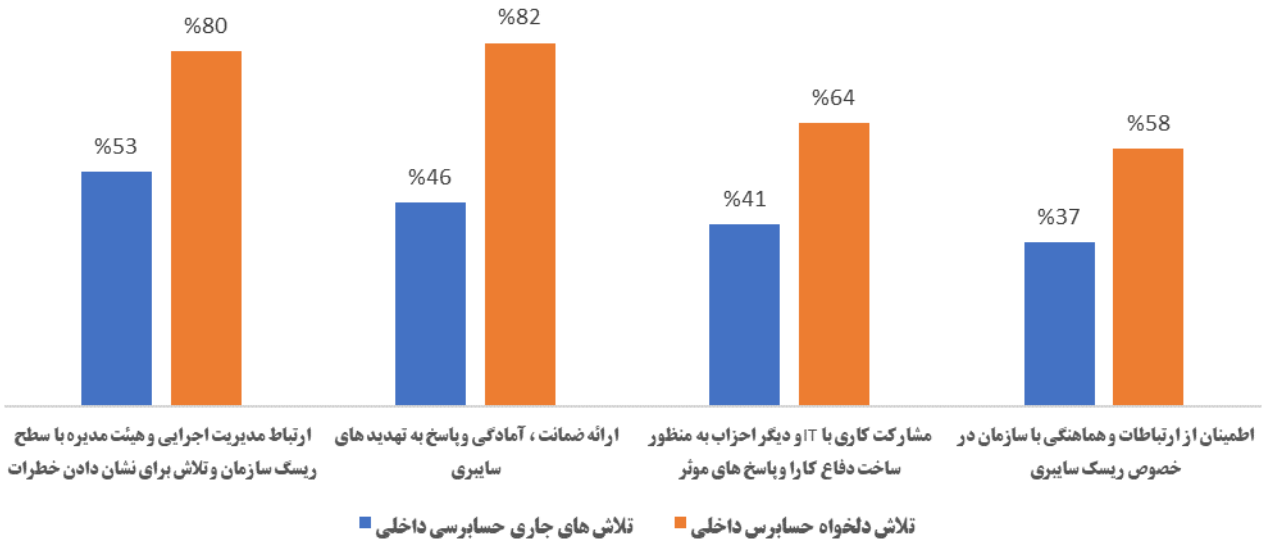
داده‌های پالس در خصوص اطمینان بخشی بخشی و اطمینان در مورد مناطق کلیدی امنیت سایبری نشان دهنده " شکاف تلاش " معناداری است. این شکاف نشان دهنده تفاوت بین حوزه حسابرسی داخلی که در حال حاضر انجام می‌گردد با سیاستی که درواقع باید اتخاذ شود می‌باشد (همانگونه که توسط پاسخ دهندگان مشخص شده است).

به عنوان مثال، 46 درصد پاسخ دهندگان گفته اند که آنها تلاش "زیاد یا قابل توجهی" را برای آمادگی و پاسخ به تهدیدهای سایبری انجام می‌دهند، در حالیکه 82 درصد گفته‌اند، آن‌ها باید " تلاش زیاد یا قابل توجهی " را فراهم کنند (شکل 3).

شکاف تلاش ممکن است بیانگر این باشد که حسابرسی داخلی موفق نشده است که خود را سریع با تغییرات سازگار کند و قادر نیست که اطمینان بخشی و اطمینان لازم را ارائه دهد. این مفهوم همچنین می‌تواند نشان دهنده سوء تفاهم بالقوه بین الویت های ریسک و برنامه حسابرسی باشد.

در حالیکه مسائل سایبری و فناوری اطلاعات (IT) تقریباً با روند رو به رشدی 20٪ تصمیمات حسابرسی را نشان می‌دهند، این دو حوزه ریسک برای هیئت مدیره به عنوان ریسک‌هایی کم اهمیت همانند گزارشگری مالی، عملیاتی و انطباق / مقررات (شکل B در ضمیمه) تلقی می‌شوند.

شکل 3: تلاش‌های امنیت سایبری حسابرسی داخلی واقعی در برابر تلاش‌های مطلوب



یادداشت: سوال های 6و 7 Q6 و Q7: سطح تلاش حوزه حسابرسی داخلی را"در سطح موجود" (Q6) یا "در سطح مورد انتظار" (Q7) در هر یک از زمینه های مرتبط با امنیت سایبری بیان کنید.

کشمکش بین حسابرسی داخلی و موضوعات سایبری

علیرغم اینکه سازمانها به طور یکسان امنیت سایبری و آگاهی سایبری را به عنوان الویت های کلیدی شناسایی می‌کنند مدیران اجرایی حسابرسی در خصوص سایبر و تکنولوژی اطلاعات IT نگرانی زیادی دارند. تقریباً 7 نفر از 10 نفر (68٪) ریسک های سایبری

را بالا و بسیار بالا ارزیابی کرده‌اند و نیز 53 ٪ ریسک IT را بالا و بسیار بالا ارزیابی نموده‌اند.هر CAE باید مکث کرده و از خود بپرسد هرچند وقت یکبار با کمیته حسابرسی درباره این نگرانی‌ها بحث می‌کند و آیا حسابرس داخلی توانایی/منابع حل این مسائل را دارد.

رتبه بالای ریسک در این حوزه باعث تلاش مداوم حسابرسی داخلی برای تقویت مهارت های خود در این حوزه شده است. بیش از نیمی ازمدیران اجرایی حسابرسی عدم تخصص حسابرسی داخلی در امنیت سایبری را به عنوان نقصی مهم در توانایی حسابرسی داخلی در شناسایی ریسک‌های امنیت سایبری ارزیابی کرده‌اند.

علاوه بر این بیش از 4 نفر از 10 نفر ازمدیران اجرایی حسابرسی، کمبود همکاری یا ارتباطات از طریق تیم IT و همچنین کمبود حمایت توسط مدیریت اجرایی را به را دارای اثرمهم و قابل ملاحظه ارزیابی کردند. (شکل 4)

مدیران اجرایی حسابرسی به وضوح ریسکی را که مسائل سایبری و IT در سازمانهایشان ایجاد می‌کنند می‌دانند. با این حال پاسخ‌های نظرسنجی نشان دهنده پیشرفت آهسته حسابرسی داخلی در استخدام/بهره گیری از کارکنان کارآزموده و یا آموزش به کارکنانی که بتوانند اطمینان بخشی مستقل در این حوزه‌های ریسکی فراهم کنند می‌باشد. رشد روزافزون و پیچیدگی‌های حملات سایبری این شکاف را به طرز نگران کننده‌ای رشد می‌دهد. این موضوعات می‌بایست با کمیته حسابرسی مورد بحث قرار گیرد. از جمله گفتگوی صادقانه در خصوص منابع مورد نیاز در دستیابی به اطمینان کافی در خصوص فضای سایبری و IT.

شکل 4 – موانع پرداختی به ریسک امنیت سایبری

بی اهمیت	تقریباً مهم	بسیار مهم	توضیحات
٪23	٪26	٪51	عدم وجود تخصص بین کارمندان حسابرسی داخلی
٪43	٪14	٪43	عدم وجود همکاری و ارتباط از بخش IT سازمان
٪44	٪13	٪45	عدم وجود حمایت توسط مدیریت اجرایی در شناسایی ریسک امنیت سایبری

یادداشت: Q8: هر کدام از موانع فوق چه تاثیری بر توانایی حسابرس داخلی برای مقابله با ریسک امنیت سایبری دارند؟

موارد عملی

1- مدیران اجرایی حسابرسی باید هرگونه پیشرفت یا کمبود در ایجاد مهارت‌های سایبری و دلایل چرایی آن را به کمیته حسابرسی گزارش دهند. مباحث صادقانه با کمیته حسابرسی در خصوص کافی بودن پوشش حسابرسی و یا اینکه مجموعه مهارت‌هایی که در حال حاضر وجود ندارد، تنها راه حل پاسخ به تغییرات مدام در آن شرایط است.

2- مدیران اجرایی حسابرسی باید هرگونه شکاف امنیت سایبری را به مدیریت و کمیته حسابرسی اعلام کنند. این بدین معنی است که مدیران اجرایی حسابرسی باید دلایل شکاف‌های موجود منجمله منابع مهم در برون سپاری را مستند کنند، همچنین می‌بایست اولویت‌های برنامه حسابرسی و هر نوع عدم ارتباط حقیقی با IT را نیز ثبت کنند.

3- مدیران اجرایی حسابرسی باید وقت بیشتری در ساخت رابطه /همکاری با CISO ها و CIO ها صرف کنند. عدم همکاری توسط بخش IT ممکن است منجر به ضعف ارتباط یا نگرانی در خصوص عدم کفایت حسابرسی داخلی در خصوص حوزه سایبری گردد.

4- مدیران اجرایی حسابرسی می‌بایست وقت بیشتری در آموزش تیم‌هایشان درباره امنیت سایبری صرف کنند که این امر می‌تواند شامل بسط دادن ادراکی عمیق از چهارچوب‌هایی باشد که غالباً در امنیت سایبری استفاده می‌شوند مثل NIST CFT، NIST 800-53، ISO/IEC 2700.

5- مدیران اجرایی حسابرسی باید هنگامی که مهارت‌ها در سازمان کافی نیستند می بایست همسپاری(cosourcing) را به عنوان یک عامل مهم در نظر بگیرند.

6- مدیران اجرایی حسابرسی باید به دنبال فرصت‌هایی برای کارمندانشان باشند تا حسابرسی‌های امنیت سایبری را با کمک تیم IT انجام دهند. به عنوان مثال شناسایی دارایی‌های مهم سازمان که نیازمند محافظت هستند، بررسی کنترل‌های تهدید داخلی و ارزیابی فرایندها و ساختارهایی که به منظور افشاء عمدی یا سهوی اطلاعات سازمان طراحی شده‌اند.

منابع

- **Artificial Intelligence: The Data Below (Internal Audit Foundation)**
- **Approaches to Upskilling for Internal Auditors (IIA Global Knowledge Brief)**
- **The Future of Cybersecurity in Internal Audit (Internal Audit Foundation and Crowe)**
- **Auditing Cyber Security: Evaluating Risk and Auditing Controls (ISACA)**
- **Cybersecurity Framework (National Institute of Standards and Technology {NIST})**
- **Global Information Security Survey (EY)**
- **ISO/IEC 27001:2013: Information Security Management Systems — Requirements (International Organization for**
- **Standardization/International Electrotechnical Commission {ISO/IEC})**
- **Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53 Rev. 4)**

نکات کلیدی

- **آسیب به شهرت در ارتباط یا نفوذهای سایبری برای سازمان‌های شمال آمریکا، نگران بزرگی محسوب می‌گردد. 70٪ ازمدیران اجرایی حسابرسی می گویند سازمانشان نگرانی‌های زیاد یا بسیار زیادی در خصوص آسیب بالقوه شهرت که ناشی از افشای نامناسب اطلاعات شخصی است دارند.**
- **حسابرسی داخلی در توسعه مهارت‌ها و تجاربی به منظور تأمین امنیت سایبری نقص دارد. 51٪ ازمدیران اجرایی حسابرسی گفته‌اند عدم مهارت کارکنان در سایبر مشکلی است که باعث می‌شود متوجه ریسک امنیت سایبری نشوند.**
- **شکاف تلاشی، بین سطحی از تلاش که در حال حاضر توسط حسابرس در حوزه‌های کلیدی سایبری انجام می گردد و آن سطحی که مدیران اجرایی حسابرسی معتقدند که باید انجام گردد وجود دارد. 36٪ ازمدیران اجرایی حسابرسی شکاف بین واقعی و مورد دلخواه را در خصوص آمادگی و پاسخ به تهدیدهای سایبری گزارش کرده‌اند.**
- **شکاف تلاش ممکن است بیانگر این باشد که حسابرسی داخلی نتوانسته به اندازه کافی سریع با تغییر ریسک ها و نیازهای ذینفعان سازگار شود ، و عدم هماهنگی بالقوه بین ریسک های و اولویت های برنامه حسابرسی وجود دارد.**

بخش دوم

ریسک‌های اشخاص ثالث

پرسشنامه پالس، اطلاعاتی ارزشمندی در خصوص نحوه مدیریت ریسک شخص ثالث در سازمانها را گردآوری کرده است. داده‌ها نشان می‌دهد سازمان‌ها قویاً بر تأمین کنندگان شخص ثالث در حوزه‌های کلیدی ریسک متکی هستند که شامل IT و سرویس‌های کسب و کار می‌باشد.

طبق نظرمدیران اجرایی حسابرسی 8 مورد از 10 سازمان، قراردادهای شخص ثالث برای خدمات IT دارند و 7 از 10 تای آن‌ها برای سایر خدمات کسب و کار همانند زنجیره عرضه یا حسابداری نیز قراردادهای شخص ثالث دارند.

پاسخ‌های مدیران اجرایی حسابرسی به وضوح نشان دهنده نگرانی بالا در خصوص نحوه انتخاب و بازرسی اشخاص ثالث است و این نگرانی ها ناشی از این است که سازمانها چقدر آمادگی مدیریت فروشندگان ضعیف را دارند نیز می‌باشد.

فرایندهای نظارت، انتخاب

زنگ ریسک

تقریباً آنچه از پرسشنامه‌های پاسخ داده شده، نتیجه گرفته شده این است که:

1- سازمان‌ها در انتخاب شخص ثالث ضعیف عمل کرده‌اند و یا اصلاً فرایندی جهت انتخابشان نداشته‌اند. (21٪)

2- فرایندی قوی برای انتخاب آنها توسط سازمان به کار گرفته شده. (22٪)

3- 57٪ باقیمانده، فرایند انتخاب را کافی و نه خوب توصیف کرده‌اند.

همین اعداد نگران کننده در بحث تأمین کنندگان شخص ثالث شرکت‌ها وجود دارند. تنها 9٪ ازمدیران اجرایی حسابرسی نظارت را قوی توصیف کرده‌اند، 43٪ آن را کافی و 48٪ آن را ضعیف دانسته‌اند و یا اعتقاد دارند اصلاً نظارتی وجود ندارد. (شکل 5)

شکل5-تلاش سازمان در انتخاب و بررسی تأمین کنندگان شخص ثالث

	قوی	کافی	ضعیف	وجود ندارد
انتخاب	٪22	٪57	٪19	٪2
نظارت	٪9	٪43	٪36	٪12

یادداشت: سوالات 28 و 29 Q28 و Q29: تلاشهای سازمان خود را برای حسن انتخاب و انجام نظارت بر ارائه دهندگان خدمات شخص ثالث چگونه توصیف می کنید؟

برنامه‌های بازیابی، یک مسئله لوکس و نادر

میزان برنامه های بازیابی که برای رفع عملکرد ضعیف یک ارائه دهنده خدمات شخص ثالث طراحی شده است نیز نگران کننده است. برنامه‌های بازیابی برای محافظت سازمانها بوسیله شناسایی فرایندی برای پایان دادن قراردادهایی که اختلال در خدمات دارند و محدود کردن بدهی‌های قانونی و محافظت از دارایی‌ها و شهرت سازمان طراحی شده‌اند. با این وجود بیش از نیمی ازمدیران اجرایی حسابرسی گزارش داده‌اند که سازمانشان چنین برنامه‌های بازیابی را بر پایه‌های ضعیف بنا کرده‌اند. به طور کلی تنها 42٪ ازمدیران اجرایی حسابرسی سازمانشان را طوری توصیف کرده‌اند که گویا برنامه‌های بازیابی برای تمام قراردادهای شخص ثالث و یا آنها که ریسک‌های بالا به موسسه تحمیل می‌کنند، دارند. (شکل 6)

شکل 6: فراوانی برنامه‌های بازیابی به منظور نشان دادن حوزه ضعیف شخص‌های ثالث

برای کلیه قراردادهای شخص ثالث	٪3
برای شخص‌های ثالث با ریسک بالا	٪39
برای برخی اشخاص ثالث خاص، نه برمبنای ریسکشان	٪53
بدون برنامه	٪5

یادداشت: Q30: میزان برنامه های بهبود سازمان شما برای رفع عملکرد ضعیف ارائه دهنده خدمات شخص ثالث چقدر است؟

کمتر ازیک سوم مدیران اجرایی حسابرسی میزان رضایت خود را از مدیریت ریسک شخص ثالث سازمانشان را عمدتاً راضی کننده توصیف کرده‌اند. (شکل 7)

شکل 7: رضایت از مدیریت ریسک شخص ثالث

خیلی راضی	٪2
تقریباً راضی	28
کمی راضی	٪32
بسیارکم راضی	٪25
ناراضی	٪13

یادداشت: Q31: به طور کلی میؤان رضایت شما از مدیریت ریسک مربوط به فروشندگان شخص ثالث چقدر است؟

اطمینان بخشی شخص ثالث و اکوسیستم ریسک

برخلاف نگرانی‌های مهم که توسط مدیران اجرایی حسابرسی بیان شده‌اند، پاسخ‌های پرسشنامه نشان دهنده حداقل متخصصین برنامه حسابرسی برای بررسی روابط شخص ثالث است.

به طور متوسط حسابرسی 4 درصد از منابع خود را به اطمینان بخشی در خصوص ریسک شخص ثالث اختصاص می‌دهد (برمبنای اطلاعات پرسشنامه پالس سال 2013). تناوب حملات سایبری به واسطه آسیب پذیری های شخص ثالث تسهیل می‌گردد و می‌بایست این موضوع مورد بررسی قرار بگیرد تا مشخص گردد که این ریسک باید به عنوان اولویت برنامه حسابرسی ارزیابی شود.

هشت سازمان بلند پایه به دلیل افشای اطلاعات شخص ثالث درنیمه اول سال 2018، درمعرض ریسک قرارگرفتند. (همانگونه که دراین مطلب توسط مشاور امنیت سایبری GRX سایبر نیزمورد توجه قرار گرفته است.)

هکرها از نقاط ضعف سیستم های فروش ، چت و سیستم عامل های خدمات مشتری و سیستم های اتوماسیون و برنامه ریزی گردش کار که به طور محافظه کارانه بیش از 250 میلیون پرونده مشتری را در معرض دید خود قرار داده است سوءاستفاده کردند. قوانین جدید نگهداری و محافظت از اطلاعات دراروپا، آمریکا و چین، ریسک های مالی و تطبیق بیشتری را مطرح می‌کند. دقت کنید که ریسک‌های شخص ثالث فقط مختص سایبر نیست، روابط شخص ثالث، دارای فساد بالقوه، ریسک‌های شهرت وعملیاتی می‌باشد.

سازمان‌ها نمی‌توانند ریسک‌های مرتبط با روابط شخص ثالث را جدای از ریسک‌های سازمان خود در نظر بگیرند. همه ریسک‌های مستقیم، ثانویه، ثالث و ... بخشی از اکو سیستم ریسکی هستند که در آن سازمان‌ها فعالیت می‌کنند.

درست همان طور که سازمان‌ها درک کرده‌اند که ریسک‌های زنجیره تأمین می‌تواند ناشی از اتفاقات نامربوط در آن سوی دنیا باشند، باید بدانید که ضعف کنترل نیز می‌تواند ارمغان روابط شخص ثالث باشد.

موارد عملی:

1-مدیران اجرایی حسابرسی می‌بایست کمیته حسابرسی را از کمبود در فرآیندهای انتخاب، نظارت و برنامه بازیابی (recovery plan) شخص ثالث آگاه سازند.

2-مدیران اجرایی حسابرسی به طور فعالانه می‌بایست کلیه روابط شخص ثالث و نرخ ریسک را براساس اندازه، پیچیدگی و اثر برروی سازمانشان ارزیابی و مشخص کنند.

3-مدیران اجرایی حسابرسی باید در خصوص هر یک از صاحبان روابط -احتمالاً از طریق نظرسنجی- کنترل های کلیدی، نظارت و عملیات حسابرسی موجود را تعیین کنند و کمیته حسابرسی را از نتایج مطلع سازند.

4--مدیران اجرایی حسابرسی می‌بایست مشخص کنند کدام رابطه باید حسابرسی شود و حسابرسی را انجام دهند.

منابع:

- **Auditing Third-party Risk Management (IIA Practice Guide)**
- **Auditing Outsourced Functions: Risk Management in an Outsourced World (Internal Audit Foundation)**
- **Oversight of Third-party Risks: Insights From the Audit Committee Leadership Networks (EY)**

نکات کلیدی:

- **بیش از نیمی ازمدیران اجرایی حسابرسی گزارش داده‌اند که برنامه‌های بازیابی برای شناسایی فروشندگان ضعیف، ریسک را درنظر نگرفته اند.53٪ ازمدیران اجرایی حسابرسی گزارش داده‌اند برنامه‌های بازیابی برای روابط خاص شخص ثالث ایجاد شده‌اند اما براساس ریسک نیستند.**
- **تعداد کمی ازمدیران اجرایی حسابرسی ازمدیریت سازمانشان در خصوص ریسک فروش شخص ثالث راضی هستند. 30٪ ازمدیران اجرایی حسابرسی می گویند که از نحوه مدیریت ریسک اشخاص ثالث سازمانشان بسیار راضی هستند.**
- **مدیران اجرایی حسابرسی باید بیشتر به این موضوع بپردازند تا اطمینان حاصل شود که مدیریت و هیئت مدیره درک کنند که روابط شخص ثالث در اکوسیستم کلی ریسک ها نقش دارند و از سازمان جدا نیستند.**

بخش 3ریسک‌های نوظهور و غیر عادی

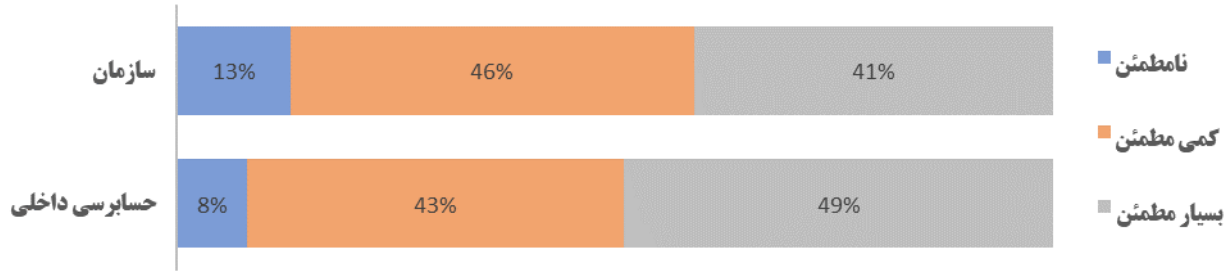
محیط‌های پویای ژئوپلتیک، شرایط اقتصاد جهانی را تغییر داده‌اند و اختلالات تکنولوژی باعث بروز ریسک‌های نوظهور و غیر عادی درخط مقدم هیئت مدیره و مدیریت ارشد، شده‌اند.

فن آوری های جدید و مفاهیم کسب و کار، از هوش مصنوعی گرفته تا ارزهای رمز گذاری شده، موبایل‌های نسل پنجم، وعده بازنویسی قوانین ریسک های غیر متعارف و پتانسیل آنها در ضربه زدن به سازمان را می‌دهند.

برخلاف گذشته، هم ترازی و هماهنگی بین تمامی حوزه های ریسک بسیارحیاتی است، درحالی که سازمان (می‌بایست) ریسک‌های نوظهورو غیر عادی را شناسایی، رمز گشایی و بررسی کند.

پاسخ دهندگان به پرسشنامه پالس ادعا کرده‌اند که مدیران اجرایی حسابرسی به طرز قابل ملاحظه‌ای به توان سازمان و حوزه حسابرسی در ارزیابی و شناسایی ریسک‌های نوظهور، ایمان دارند. 92٪ ازمدیران اجرایی حسابرسی این اطمینان را از متوسط تا بسیار بالا عنوان کرده‌اند. (شکل 8)

شکل 8: اطمینان از شناسایی و ارزیابی ریسک‌های نوظهور*



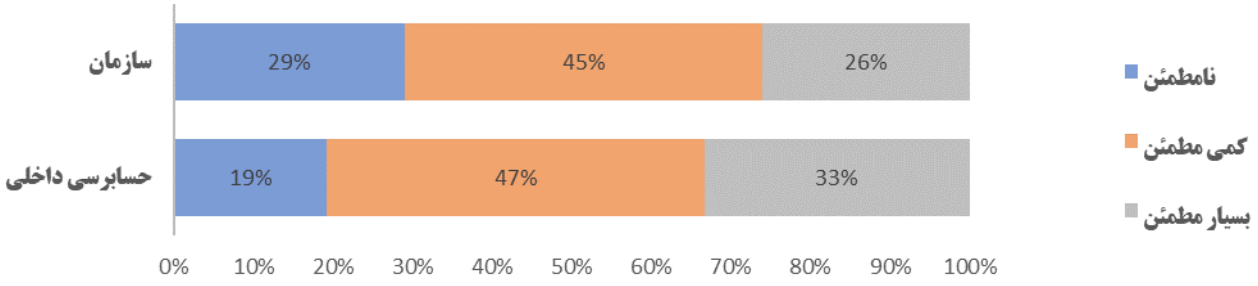
یادداشت: Q18: لطفا میزان اعتمادتان به توانایی های سازمان و حسابرسی داخلی برای شناسایی و ارزیابی ریسک های نوظهور بیان کنید.

* ریسک های نوظهور ریسکهای جدیدی هستند که در گذشته هیچ پیامدی نداشته اند.

این اطمینان فقط درزمان شناسایی ریسک‌های غیر عادی که به "ریسک‌هایی که سخت شناسایی و ارزیابی می‌شوند یا آنهایی که بسیار نادر هستند" تعریف می‌شوند، کمی کاهش می‌یابد. 8 نفر از 10 نفر ازمدیران اجرایی حسابرسی می گویند، آن‌ها بسیار به توان حوزه حسابرسی در شناخت و ارزیابی ریسک‌های غیر عادی، اطمینان دارند. در زمانیکه بحث شناسایی و ارزیابی ریسک‌های غیر عادی مطرح می‌شود اطمینان آنها کمی کاهش می‌یابد و به 7 نفر از 10 نفر کاهش می‌یابد. (شکل 9)

فقط 3 نفر از 10 نفر ازمدیران اجرایی حسابرسی گزارش کرده‌اند که برای شناسایی و ارزیابی ریسک‌های نوظهور و غیر عادی از تکنیک‌های پیشرفته اطلاعات استفاده می‌کنند.

شکل 9 اطمینان از شناسایی و ارزیابی ریسک غیر عادی*



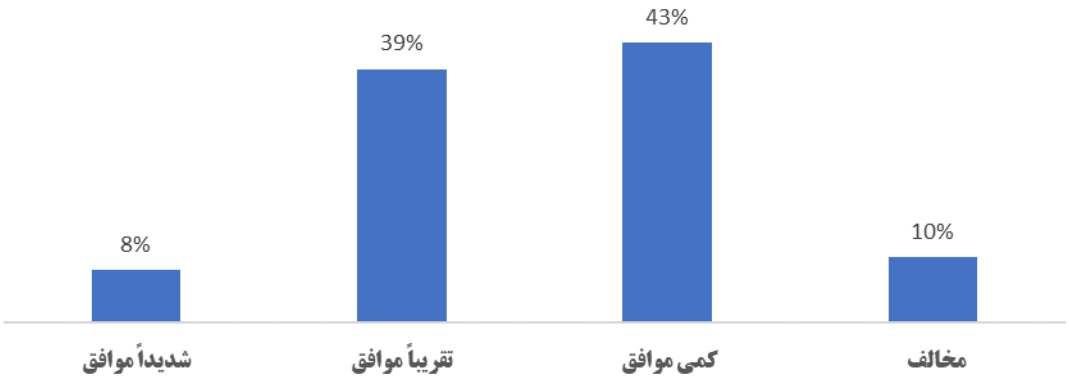
یادااشت: Q19: لطفا میزان اعتمادتان به توانایی های سازمان و حسابرسی داخلی برای شناسایی و ارزیابی ریسک های غیر عادی بیان کنید.

* ریسک های غیر عادی به ریسک هایی اطلاق می شود که شناسایی و ارزیابی آنها بسیار دشوار است و یا رخداد انها بسیار نادر است.

اعتماد شگفت انگیز

چه بسا، این اعتماد با پاسخ مدیران اجرایی حسابرسی به دو سؤال زیر، مغایرت دارد. اول 47٪ ازمدیران اجرایی حسابرسی با این مطلب که "عادی است که ریسک‌های نوظهور و غیر عادی مدیریت را شگفت زده کند" موافق هستند. (شکل 10) دوم، 24٪ گزارش داده‌اند که "ریسک شگفت انگیزی" در 12 ماه گذشته رخ داده است.

شکل 10: عادی است که ریسک نوظهور یا غیر عادی مدیریت را شگفت زده کند



یادداشت: Q24: میزان توافق شما با این جمله چقدر است؟ یک ریسک نوظهور یا غیرعادی کاملاً عادی است که باعث تعجب مدیریت شود.

حاشیه مشارکت حسابرسی داخلی:

این ناسازگاری را می‌توان با مراجعه به منابعی که هیئت مدیره برای کسب اطلاعات درخصوص ریسک‌های نوظهور و غیر عادی به آنها اعتماد می‌کند، مورد بررسی بیشتر قرارداد. حدود سه چهارم ازمدیران اجرایی حسابرسی گفته‌اند، هیئت مدیره غالباً به مدیریت اجرایی تکیه می‌کند، اما کمتر از نصف آنها همین مطلب را درخصوص حسابرسی داخلی یا حوزه مدیریت ریسک گفته‌اند. (شکل 11)

شکل 11: اتکا هئیت مدیره به گروه‌های مختلف به منظور شناسایی و بررسی ریسک‌های نوظهور و غیر عادی

	بسیار محتمل	محتمل	کمی محتمل	نامحتمل
مدیریت اجرایی	٪78	٪15	٪6	٪1
حسابرسی داخلی	٪49	٪35	٪14	٪2
حوزه مدیریت ریسک	٪48	٪29	٪15	٪8

یادداشت: Q23: میزان احتمال اتکا هیئت مدیره به طرفهای فوق برای شناسایی و ارزیابی ریسک های نوظهور و غیر عادی چقدر است؟

این که پاسخ‌های مدیران اجرایی حسابرسی ممکن است نشان دهنده اعتماد نادرست در توان سازمانشان در شناسایی و کاهش ریسک‌های نوظهور و غیر عادی باشد نگران کننده است.

به عنوان مثال، درحالیکه بیشترمدیران اجرایی حسابرسی، مصاحبه‌های مدیریتی و بـه روزرسـانی هـای دوره‌ای ارزیـابی ریسـک و برنامه‌های حسابرسی را روش‌هایی برای ارزیابی ریسک گزارش کرده‌اند، کمی کمتر از نصف آنها، شاخص‌های کلیدی ریسک از جملـه ریسک‌های نوظهور یا ریسکهای در حال رشد را، شناسایی و ارزیابی می‌کنند. (شکل 12)

این مسئله باعث می‌شود که هیئت مدیره به جای آن که مستقلاً و با ابزارهای کنترلی، ریسک‌های کلیدی را اندازه گیری کنند تکیه و اتکا بیشتری برآن چیزی از مدیریت شنیده است داشته باشد.

این مسئله همچنین تفاوت بین سطح اطمینان CAE و تفاوت گزارش ریسک‌های شگفت آور را نیز نشان می‌دهد.

شکل 12: استفاده از متدهای ارزیابی ریسک

	بسیاراستفاده شده	متوسط استفاده شده	کم استفاده شده	استفاده نشده
مصاحبه دوره‌ای مدیریت در طول سال به منظور شناسایی تغییرات ریسک سازمان	٪63	٪25	٪9	٪3
به روز رسانی رسمی ارزیابی ریسک و برنامه حسابرسی	٪53	٪33	٪12	٪2
معرفی و نظارت شاخص‌های کلیدی ریسک	٪14	٪34	٪29	٪23
استفاده از روش‌های تحلیل پیشرفته اطلاعات در شناسایی و ارزیابی تغییرات ریسک‌هایی که قابل مشاهده نیستند	٪6	٪24	٪39	٪31

یادداشت: سوال Q20 20: لطفاً میزان استفاده حسابرسی داخلی در سازمان خود را از روشهای فوق الذکر برای ارزیابی ریسک را مشخص کنید.

موارد عملی

1- مدیران اجرایی حسابرسی باید بر موارد زیر نظارت داشته و در خصوص آنها به روز شوند:

- پیش بینی‌های اقتصادی.
- ابتکارات جدید که در حال برنامه ریزی است.
- دیدگاه‌های قانونگذاری و نظارتی.
- تهدیدها و فرصتهای پیش روی صنعت.
- رقبای اولیه و چالش‌های آن‌ها.
- ریسک های پدیدار شده در عناوین از طریق رسانه‌های سنتی یا اجتماعی.

2- مدیران اجرایی حسابرسی باید به همراه مدیریت و کمیته حسابرسی/ هیات مدیره به گسترش نقش حسابرسی داخلی در شناسایی و ارزیابی ریسکهای نوظهور یا غیرمعمول بپردازد.

3- مدیران اجرایی حسابرسی باید شیوه‌های مدیریت ریسک را که فقط به مصاحبه‌های مدیریتی درمورد آنچه که برای نظارت بر ریسک های نوظهور و غیرعادی انجام می‌شود متکی هستند، به چالش بکشند و به تنها به پرسش از چرایی و چگـونگی آن اکتفا نکنند.

4- مدیران اجرایی حسابرسی باید بر بهبود چگونگی استفاده سازمانهایشان از KRI، تجزیه و تحلیل داده‌ها و سایر ابزارها برای شناسایی و نظارت بر پیش سازهای ریسک های در حال رشد و نوظهور تمرکز کنند.

منابع

- **Internal Audit and Emerging Risks: From Hilltops to Desktops (Chambers on the Profession**)
- **Auditing and Disruptive Technologies (Internal Audit Foundation**)
- **International Risk Governance Council (Website**)

نکات کلیدی:

- مدیران اجرایی حسابرسی به توانایی سازمان‌های خود و حوزه حسابرسی برای شناسایی و ارزیابی ریسک‌های درحال ظهور و غیر عادی بسیار اطمینان دارند. 87 درصد از مدیران اجرایی حسابرسی به شدت یا بطور متوسط به توانایی سازمانهای خود برای شناسایی و ارزیابی ریسک‌های نو ظهور و غیر عادی اطمینان دارند.
- تقریباً نیمی از مدیران اجرایی حسابرسی گفتند مدیریت بارها بوسیله ریسک‌های درحال ظهور و غیر عادی شگفت زده شده است. 47 درصد از مدیران اجرایی حسابرسی گفتند، نسبتا متداول است که ریسک‌های درحال ظهور و غیر عادی موجب تعجب مدیریت شود.
- مدیران اجرایی گزارش می دهند حسابرسی داخلی در خصوص داشتن اطلاعات در مورد ریسک‌های نوظهور و غیر عادی در بالای لیست قرار ندارد. 78 درصد از مدیران اجرایی حسابرسی می‌گوید هیئت مدیره به مدیریت (نه حسابرسان داخلی)برای شناسایی و ارزیابی ریسک‌های درحال ظهور و غیر عادی متوسل خواهد شد.
- مدیران اجرایی حسابرسی گزارش می‌دهند که هیئت مدیره برای شناسایی و ارزیابی ریسک‌های درحال ظهور و غیر عادی به احتمال زیاد به مدیریت متوسل می‌شوند.

بخش 4

فعالیت هیئت مدیره مدیریت

فشارهای نظارتی، به ویژه در زمینه گزارشگری مالی و امنیت سایبری در حال رشد است؛ و این نظـارت هیئـت مـدیره و مـدیریت را درکانون توجه قرار می‌دهد. شکست های اخیر در نظارت و محافظت از داده‌ها در بانکداری و رسانه‌های اجتماعی منجر به ایـن شـده است که مدیران ارشد برای توضیح اقدامات خود به کمیته های کنگره فراخوانده شوند و همچنین برخی از اعضای هیئت مـدیره نیـز مجبور به استعفا شوند.

هیئت مدیره با دقت بیشتری اطلاعاتی را که از مدیریت دریافت می‌کنند بررسی می‌کند. به عنوان مثال، بر طبق نظر سنجی سال NACD 2019-2018، اعضای هیئت مدیره گزارش می‌دهند که زمانی که آنها برای مرور اطلاعاتی که از مدیریت دریافت می نمایند تقریبا دوبرابر زمانی است که صرف مرور اطلاعات دریافتی از منابع خارجی می نمایند. علاوه بر این، " با توجه به یافته‌ها، پنجاه و سه درصد مدیران اظهار داشتند که کیفیت گزارش مدیریت به هیئت مدیره باید بهبود یابد، که این نشان می دهد هیات مدیره نیاز به اطلاعا بهتر و نه بیشتر دارد "

نظرسنجی پالس 2019، قصد دارد این را مورد سنجش قرار بدهد که آیا از دید CAE، هیات مدیره تصویر کاملی از ریسک دریافت می نماید و آیا حسابرسی داخلی، نقشی در اطمینان بخشی درباره اطلاعات دریافت شده از هیئت مدیره دارد.

اطلاع رسانی به هیات مدیره

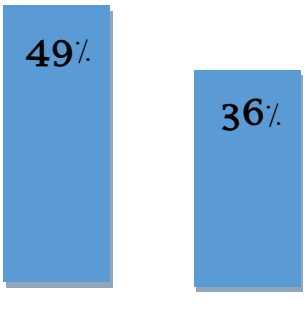
به طور کلی، مدیران اجرایی حسابرسی معتقدند که هیات مدیره اطلاعات مورد نیاز خود را در محدوده‌های حیاتی ریسک دریافت می‌کنند. اکثریت قریب به اتفاق به شدت یا تا حدودی معتقدند که اطلاعاتی که مدیریت درمورد ریسک های بالقوه قابل توجه ارائه می نماید دقیق، مداوم، کامل، بیانگر، به موقع و شفاف هستند.

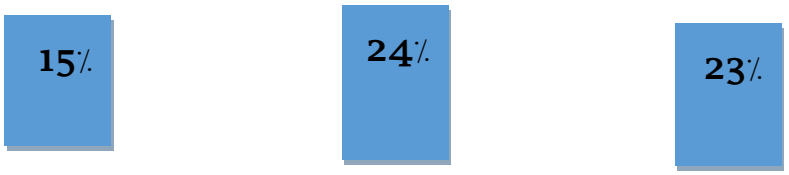
به عنوان مثال، پاسخ‌های CAE نشان می‌دهد که 85 درصد به شدت یا تا اندازه‌ای با این موضوع که تمام اطلاعاتی که مربوط به هیئت مدیره می‌شود و نه فقط اطلاعات که از دیدگاه‌های مدیریت پشتیبانی می‌کند، به هیات مدیره می رسد. (شکل 13)

با این حال، یک حوزه از نگرانی بالقوه ، تأثیر کوتاه مدت اطلاعاتی است که از طرف مدیریت به هیئت مدیره می‌روند. در حالی که 24 درصد مدیران اجرایی حسابرسی کاملاً موافق هستند که مدیریت در درجه اول مسائل را بر اساس تأثیر طولانی مدت آن ها بر سازمان ارزیابی می‌کند و 53 درصد تا حدودی موافق هستند، تقریباً یک چهارم (23 درصد) تا حدودی یا به شدت مخالف این موضوع هستند. (شکل 14)

شکل 14: مدیریت مسائل مربوطه را بر اساس تاثیر بلند مدت آن ارزیابی می‌کند.

شکل 13: مدیریت همه اطلاعات ریسک مرتبط را برای هیات مدیره فراهم می‌کند.





Q10: میزان توافق یا عدم توافق خود را با هر یک از گفته‌های فوق در مورد وضعیت جاری سازمانتان بیان کنید. مدیریت در درجه اول موضوعات را بر اساس تأثیر طولانی مدت آن بر سازمان ارزیابی می‌کند

Q11: میزان توافق یا عدم توافق خود را در مورد ویژگی‌های اطلاعاتی که مدیریت به هیات مدیره (یا مشابه) ارائه می‌دهد مشخص کنید. همه اطلاعات مرتبط ارائه می‌شود و نه فقط آنهایی که از نظرات مدیریت پشتیبانی می‌کند**o**

مشارکت پیرامونی حسابرسی داخلی

داده‌ها تصویری دلگرم کننده را درباره اینکه حسابرسی داخلی اطمینان لازم را در مورد اطلاعاتی که به هیئت مدیره می رسد فراهم می آورد، نمایان نمی کند.

نزدیک به 6 نفر از 10 نفرمدیران اجرایی حسابرسی گزارش داده‌اند که حسابرسی داخلی به ندرت یا هرگز اطمینانی از کیفیت اطلاعات داده شده، ایجاد نمی‌کند و همچنین حسابرسی داخلی در مورد اطلاعات مربوط به هیات مدیره و مدیریت به طور رسمی به گفتگو نمی پردازد (شکل 15).

نکته مهم دیگر این است که هیئت مدیره غالباً دارای کمیته‌های متعددی هستند (مثلاً کمیته جبران خسارت، کمیته ریسک، کمیته فناوری اطلاعات) که شامل حسابرسی داخلی نمی‌شوند. حسابرسی داخلی توانایی محدودی در ارزیابی و تامین اطمینان در کیفیت اطلاعاتی که هیات مدیره از این کمیته‌ها دریافت می‌کند، دارد.

همچنان که انتظارات قانونگذاردر مورد خطاهای هیئت مدیره رشد می‌کند، ممکن است درخواست از حسابرسی داخلی به منظور اطمینان بخشی اطلاعاتی که هیئت مدیره دریافت می‌کند افزایش یابد. مدیران اجرایی حسابرسی باید فرایندهای مربوط به رسیدن اطلاعات به هیات مدیره را مورد بررسی قرار دهند و آماده حسابرسی هرگونه اطلاعاتی که هیئت مدیره به دنبال اطمینان یافتن از انهاست، باشند. آن‌ها می‌توانند با رسیدگی کردن به کنترل های مربوطهیا هشدار به هیئت مدیره درمورد عدم وجود چنین کنترل‌هایی شروع کنند. در نهایت، هدف این است که هیئت مدیره را آگاه ساخت که حسابرسی داخلی می‌تواند خدمات اطمینان دهی یا مشاوره‌ای در مورد اطلاعاتی که هیئت مدیره دریافت می نماید ارائه بدهد.

شکل 15: فعالیت حسابرسی داخلی درخصوص اطلاعات دریافتی هیات مدیره از مدیریت

هرگز	تنها برای وضعیت‌های غیر عادی	برای برخی موضوعات	برای همه موضوعات با اهمیت

حسابرسی داخلی اطمینان می دهد که اطلاعات ارائه شده به هیات مدیره کامل، به موقع و ... است.	27٪	13٪	31٪	29٪
حسابرسی داخلی بطور رسمی در مورد کامل بودن، به موقع بودن و ... اطلاعات با هیئت مدیره و مدیریت گفتگو می‌کند.	30٪	13٪	34٪	23٪

یادداشت: **Q13** : میزان مشارکت حسابرسی داخلی را در خصوص اطلاعات ارائه شده توسط مدیریت به هیات مدیره (در مورد موضوعات مهم) مشخص کنید.

شنواندن صدای حسابرسی داخلی

تجزیه و تحلیل پاسخ‌های مدیریت اجرایی حسابرسی در مورد هیئت مدیره و فعالیت‌های مدیریتی به طور غیرمستقیم یک سؤال اساسی را مطرح می‌کند که آیا خطوط گزارشگری سنتی برای اطمینان از شنیده شدن یافته‌ها و توصیه‌های حسابرسی داخلی کافی است یا خیر. **IIA** از یک ساختار دوگانه خط گزارش که در آن حسابرسی داخلی به صورت اداری(**administratively**) به **CEO** و به صورت عملکردی(**functionally**) به هیئت مدیره گزارش می‌دهد پشتیبانی می‌کند. در عمل، بیشتر سازمان‌ها دارای خطوط گزارشگری عملکردی هستند که در آن مدیر اجرایی حسابرسی به کمیته حسابرسی هیئت مدیره گزارش می‌دهد.

با این حال، پراکنش در ساختار و مسئولیت کمیته حسابرسی (همانطور که قبلاً اشاره شد) این امکان را در واقعیت ایجاد می کند که در برخی از سازمان ها، حسابرسی داخلی با کمیته‌هایی که به موضوعات مهمی مانند امنیت سایبری و نظارت به ریسک کلی رسیدگی می کنند، برهمکنش ندارند. به عنوان مثال، در بسیاری از سازمان‌ها، کمیته‌های ریسک و فناوری اطلاعات، و نه کمیته‌های حسابرسی، وظیفه سرپرستی آمادگی و امنیت سایبری را دارند. چنین شرایطی می‌تواند توانایی حسابرسی داخلی را برای ارائه دیدگاه در مورد آن حوزه‌های ریسک، با نقصان مواجه سازد.

علاوه بر این، خط گزارشگری اداری در بسیاری از سازمان‌ها می‌تواند توانایی ارتباط حسابرسی داخلی را با مدیر اجرایی حسابرسی محدودتر کند. به عنوان مثال، بسیاری از سازمانها گزارشگری اداری مدیر اجرایی حسابرسی را به رئیس ارشد مالی ادامه می‌دهند، که این موضوع یک لایه گزارش اضافی بین **CAE** و **CEO** ایجاد می‌کند.

در میان مجموع پاسخ دهندگان نظرسنجی پالس، **4** نفر از **10** نفر ابراز نموده اند که به صورت اداری به **CFO** گزارش می‌دهند این در حالی است که **3** نفر از **10** نفربه **CEO** گزارش می دهند و افراد باقیمانده به سایر مراجع درون سازمانی گزارش می‌دهند. تفکیک سازمان ها بر اساس نوع آن ها نشان می دهد که در شرکت های سهامی عام و سهامی خاص مدیران اجرایی حسابرسی به احتمال بسیار بیشتری به **CFO** گزارش می‌دهند حدود **7** نفر از **10** نفر (شکل **16**).

شکل 16: خطوط گزارشگری اداری*

	مدیر ارشد مالی یا موارد مشابه	CEO، رئیس، رئیس آژانس	سایر مدیران اجرایی	کمیته حسابرسی، هیئت مدیره یا معادل آن	سایر
سهامی عام	75٪	9٪	10٪	6٪	0
سهامی خاص	64٪	9٪	19٪	8٪	0
غیر انتفاعی	25٪	25٪	42٪	8٪	0
خدمات مالی	19٪	47٪	22٪	12٪	0
بخش عمومی	10٪	55٪	15٪	17٪	3٪
کل	40٪	31٪	18٪	10٪	1٪

یادداشت:Q3: خط گزارشگری اداری برای مدیر اجرایی حسابرسی (CAE) یا رئیس حسابرسی داخلی در سازمان شما چگونه است؟

* گزارش اداری به نظارت بر امور روزمره، تأیید هزینه، مدیریت منابع انسانی، ارتباطات، سیاست‌های داخلی و رویه‌ها اشاره دارد.

موارد عملی:

1- مدیران اجرایی حسابرسی بایستی بطور فعال با مدیر کمیته حسابرسی در مورد تمایل حسابرسی داخلی برای فراهم کردن اطمینان در مورد صحت، کامل بودن، به موقع بودن، شفافیت داده‌های ارائه شده به هیئت مدیره گفتگو کنند.

2- باید از مدیر اجرایی حسابرسی خواسته شود که مطالبی را که به هیات مدیره می‌رود بررسی نماید و در کمترین حالت اطمینانی سلبی از صحت، کامل بودن، به موقع بودن، شفافیت آن ارائه دهند. به عنوان مثال می توان اطمینان سلبی را به عنوان تأیید صحت، کامل بودن، به موقع بودن، شفافیت و قابلیت اطمینان موارد یاد شده از جانب حسابرسی داخلی در مورد موضوعاتی که به هیئت مدیره راه می یابد توصیف کرد در شرایطی که هیچ شواهدی بر خلاف آن وجود نداشته باشد.

3- باید ازمدیر اجرایی حسابرسی خواسته شودکه در جلسات دیگر کمیته‌ها، از جمله IT، ریسک و جبران خسارت حضور یابند، و این جایی است که حسابرسی داخلی ممکن است اطلاعات و بینش‌های مرتبط با هیئت مدیره را به اشتراک بگذارد.

4- به منظور ایجاد اطمینان بخشی اثربخش، مستقل و بی طرفانه، مدیران اجرایی حسابرسی باید تحقیقات مربوط به خطوط گزارشگری ترجیحی را با رئیس کمیته حسابرسی به اشتراک بگذارند.

منابع

- The Audit Committee and the CAE: Sustaining a Strategic Partnership (Internal Audit Foundation)

- **CAE Strategic Relationships: Building Rapport With The Executive Suite (Internal Audit Foundation)**
- **Interaction With the Board (IIA Practice Guide)**
- **Internal Auditing's Role in Corporate Governance (IIA Position Paper)**
- **Why Conformance Matters (IIA Position Paper)**

نکات کلیدی

- **معمولاً مدیران اجرایی حسابرسی معتقدند مدیریت اجرایی اطلاعات مربوط به ریسک را که هیات مدیره به آن نیاز دارند، در اختیار ایشان قرار می دهد. 85 درصد مدیران اجرایی حسابرسی موافق هستند که اطلاعاتی که به هیات مدیره می‌رسد، فقط مواردی هست که از دیدگاه مدیریت پشتیبانی می‌کند.**
- **ممکن است مدیریت همیشه دیدگاه بلند مدت را به کار نبندد. 23 درصد مدیران اجرایی حسابرسی می گویند مدیریت اجرایی به تأثیر بلند مدت موضوعات نگاه نمی‌کند.**
- **به ندرت از حسابرسی داخلی خواسته می شود که در مورد اطلاعاتی که به هیئت مدیره میرسد تامین اطمینان نماید. 57 درصد مدیران اجرایی حسابرسی گزارش می‌دهند که آن ها به ندرت یا هرگز در موردکامل بودن، به موقع بودن، راستگویی و شفافیت اطلاعات که به هیات مدیره داده می رسد با هیات مدیره یا مدیریت گفتگو نمی‌کنند.**
- **از آنجا که حسابرسی داخلی به طور معمول به کمیته حسابرسی گزارش می‌دهد، ممکن است به اندازه کافی با سایر کمیته های مدیریتی که به مسائل مهمی مانند فناوری اطلاعات یا مدیریت ریسک رسیدگی می‌کنند تعامل کافی نداشته باشند.**

حسابرسی داخلی برای تعیین جایگاه خود در دنیایی که به سرعت در حال تغییر است، در حال مسابقه است.

نتیجه گیری

این مکان جایی است که نوید انقلاب صنعتی چهارم (که در آن ارتباطات و داده ها با پیشرفت‌های فناوری در روباتیک و هوش مصنوعی با هم پیوند می خورند) تصویری قدرتمند از رهبران سازمانها به نمایش می‌گذارد. کسانی که می‌توانند بر این تحولات دگرگون کننده جهان تسلط داشته باشند، سازمانهای خود را به سمت رسیدن به موفقیت هدایت خواهند کرد.

با این وجود، موفقیت فقط به کسانی خواهد رسید که می‌توانند فرصتها و ریسک های ایجاد شده توسط این پیشرفتهای فناوری را تعدیل کنند و حسابرسی داخلی باید نقش مرکزی در کمک به آنها برای یافتن این تعادل باشد. این کار نیازمند این است که حسابرسی داخلی، اعضای تیم را به گونه ای توسعه بدهد که ایشان مهارت‌های لازم را برای ارائه خدمات اطمینان بخش مستقل در مورد مسائل ریسکی پیچیده داشته باشند و این که رهبران این شجاعت را داشته باشند که کاری کنند که صداهای آنان در اتاق هیات مدیره شنیده شود.

پالس حسابرسی داخلی 2019 آمریکای شمالی چهار حوزه ریسک را مشخص می‌کند که صدای حسابرسی داخلی می تواند در آن شنیده شود:

امنیت سایبری

حسابرسی داخلی باید تلاش‌های خود را برای ارائه خدمات اطمینان بخشی و مشورتی در این زمینه بهبود بخشد. این نیازمند ایجاد روابط محکم با CIOها و CISOها و سرعت بخشیدن به تلاش در زمینه ساخت تیم‌های سایبری زیرک ازطریق آموزش، استخدام‌های جدید یا همکاری خارج سازمانی می باشد. مدیران اجرایی حسابرسی باید در مورد داشتن برنامه حسابرسی مناسب که منعکس کننده اهمیت خدمات اطمینان بخشی سایبر و فناوری اطلاعات باشد ابراز نمایند و در مورد هر حوزه ای که مدیر اجرایی حسابرسی احساس می‌کند که حسابرسی داخلی باید خود را در آن زمینه تقویت کند به گفتگو بپردازد.

ریسک های شخص ثالث

ارتباط شخص ثالث بخشی از اکوسیستم ریسک های هر سازمانی است و سازمانهایی که نتوانند به طور صحیح به ریسک‌های شخص ثالث رسیدگی کنند در معرض مخاطره هستند. حسابرسی داخلی باید به هیئت مدیره و مدیریت اجرایی در زمینه ریسک های ضعف یا عدم وجود کنترل در روابط شخص ثالث آموزش دهد و با کمیته حسابرسی و مدیریت برای تعریف نقشی که حسابرسی داخلی بایستی برای اطمینان بخشی در این حوزه مهم ایفا نماید همکاری نزدیک داشته باشد.

ریسک های نوظهور و غیرعادی

تهدیدات ناشی از ریسک‌های نوظهور و غیرعادی با توجه به این که فناوری سرعت بلوغ و امکان آسیب رسانی آنان را افزایش داده است در حال رشد می باشند. مدیران اجرایی حسابرسی‌ها باید در مورد ریسکهای نوظهور و غیر عادی که می‌توانند روی سازمانها تأثیربالقوه بگذارند، آموزش دریافت نمایند. مدیران اجرایی حسابرسی باید هنگامی که سازمان فقط به اطمینان بخشی مدیریتی در مورد کاهش ریسک های نوظهور و غیرعادی متکی می باشد سخن بگویند. مدیران اجرایی حسابرسی باید شاخص‌های ریسک های کلیدی قوی‌تری را برای اطمینان بخشی از فرایند هایی که به منظور شناسایی، نظارت و کاهش ریسک های نوظهور و غیرعادی در نظر بگیرند.

هیئت مدیره و فعالیت مدیریتی

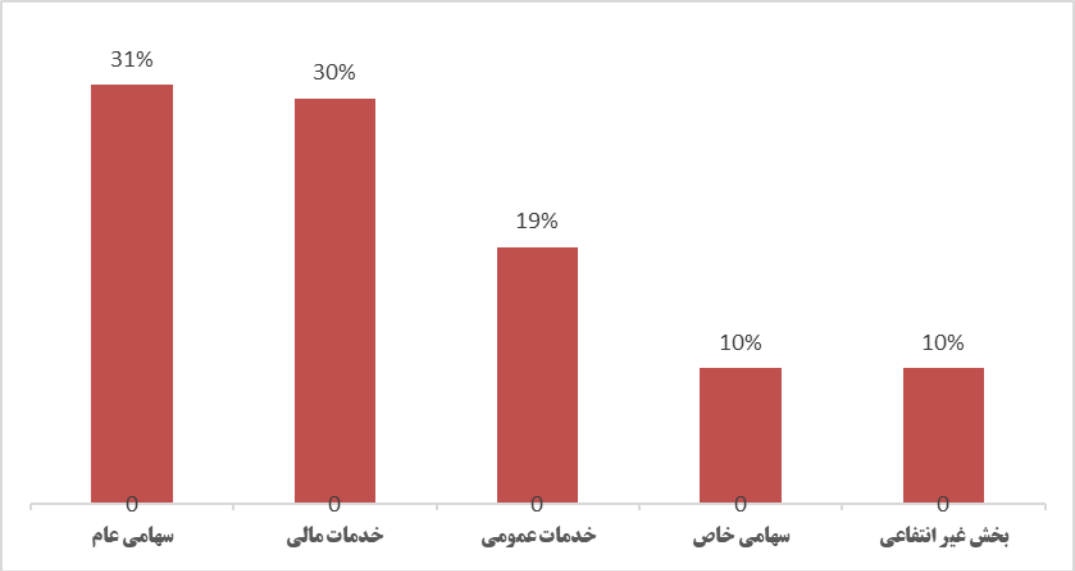
امروز بیشتر از گذشته برای تأمین نظارت پیشبینانه صحیح، قانون گذاران و سهامداران بر هیات مدیره فشاروارد می‌کنند. آن‌ها در صورتی می‌توانند به بهترین شکل ممکن این کار را انجام دهند که اطلاعاتی که تصمیمات خود را بر آن پایه گذاری می‌کنند دقیق و کامل باشد. مدیران اجرایی حسابرسی باید در مورد کلیه اطلاعاتی که به هیئت مدیره می‌رود اطمینان فراهم کنند و هیئت مدیره و مدیریت اجرایی را در مورد مزایایی که اطمینان بخشی مستقل می‌تواند فراهم آورد، آگاه سازند.

امروزه مدیریت چالش‌های پیش روی حسابرسان داخلی- که پیچیده، شتاب یافته و جهانی می باشند- به چابکی، نوآوری و گفتگوی مؤثر با هیئت مدیره و مدیریت اجرایی نیاز دارد. این امر به یک الزام اساسی نیاز خواهد داشت تا این اطمینان حاصل شود که اطلاعاتی که هیات مدیره در اختیار دارد دقیق، کامل، به موقع، شفاف و قابل اعتماد است. برای اینکه حسابرسی داخلی بتواند جایگاه خود را در این دنیای جدید پیدا کند، باید با شهامت صدای خود را بلند کنند.

به منظور دستیابی به اهداف حسابرسی داخلی، مدیران اجرایی حسابرسی باید مهارت‌های مدیریتی قوی وتوانایی استفاده بهینه از منابع را داشته باشند. در پالس سالیانه حسابرسی داخلی،IIA اطلاعات مربوط به معیار های کلیدی مدیریت حسابرسی داخلی را جمع آوری می‌کند. برخی از آنها در این بخش ارائه خواهد شد. گزارش‌های دقیق‌تر برای اعضای AEC در www.theiia.org/AEC در دسترس خواهد بود.

معیارهای مدیریت حسابرسی داخلی به پنج نوع سازمان – سهامی عام، سهامی خاص، سهامی خاص، خدمات عمومی، بخش غیرانتفاعی و خدمات مالی دسته بندی شده است (شکل A).

شکل A: نوع سازمان



یادداشت: Q80: در حال حاضر برای چه نوع سازمانی فعالیت می‌کنید؟ برای سهامی عام، 151 برای خدمات مالی، 96 برای خدمات عمومی، 53 برای سهامی خاص، 48 برای بخش غیرانتفاعی.

متداول ترین صنایعی که در هر یک از این طبقه ها قرار می گیرند عبارت اند از:

سهامی عام

- تولید (30٪)
- معادن و استخراج نفت و گاز (10٪)
- خدمات رفاهی (9٪)
- خرده فروشی (6٪)
- مراقبت‌های بهداشتی و کمک‌های اجتماعی (6٪)
- اطلاعات (به عنوان مثال، نشریات، صدا و سیما، پردازش داده‌ها) (6٪)

- سایر خدمات (به جز مدیریت دولتی) (6٪)

خدمات مالی

- موسسه مالی (55٪)
- بیمه (28٪)
- مدیریت دارایی (7٪)
- دلالی (3٪)
- سایر (7٪)

خدمات عمومی

- مدیریت عمومی (40٪)
- خدمات آموزشی (28٪)
- خدمات رفاهی (8٪)
- مراقبت‌های بهداشتی و کمک‌های اجتماعی (5٪)

سهامی خاص

- تولید (25٪)
- مراقبت‌های بهداشتی و کمک‌های اجتماعی (13٪)
- خدمات حرفه‌ای، علمی و فنی (11٪)
- سایر خدمات (به جز مدیریت دولتی) (9٪)
- خدمات آموزشی (8٪)

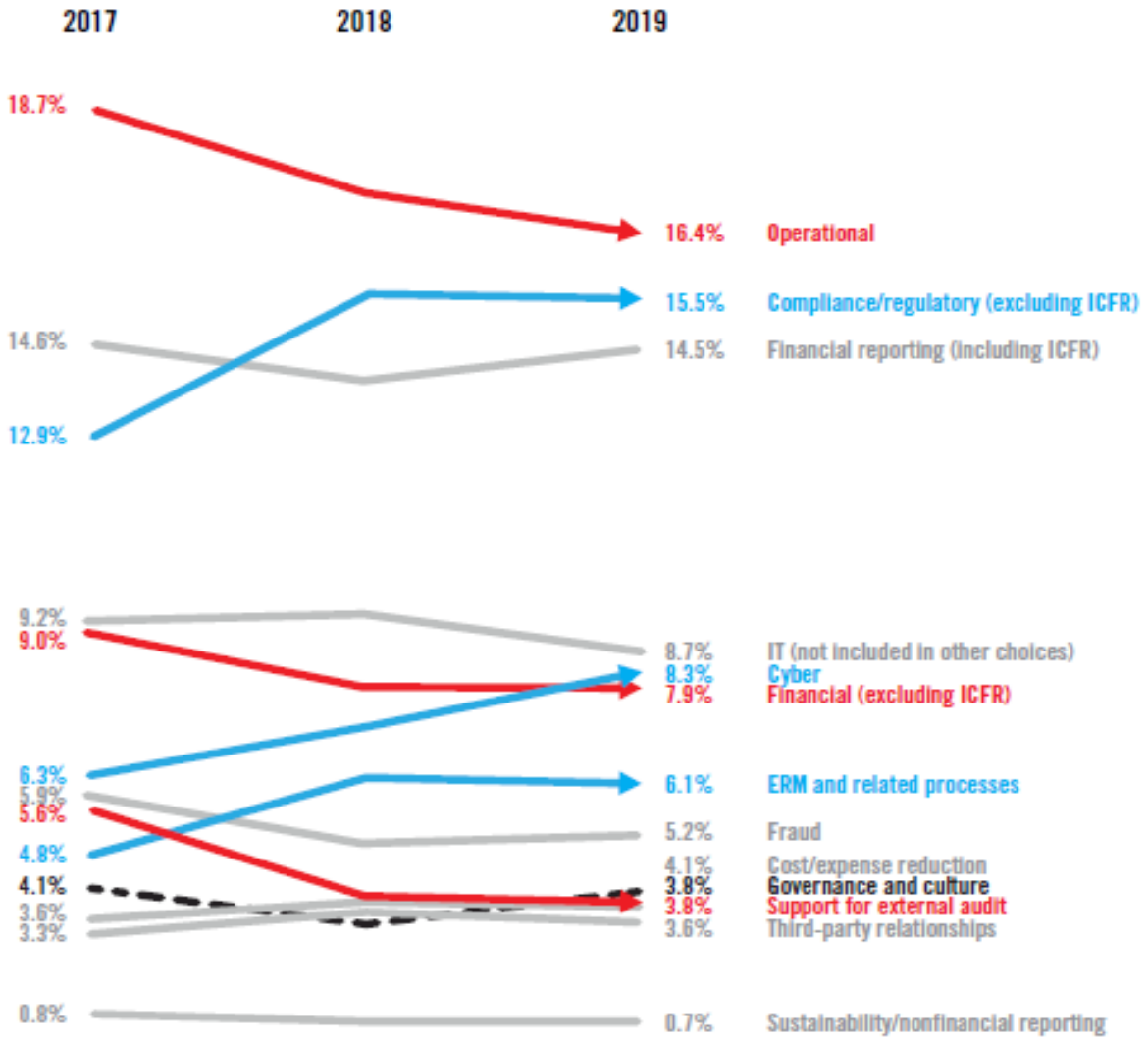
بخش بخش غیرانتفاعی

- مراقبت‌های بهداشتی و کمک‌های اجتماعی (58٪)
- خدمات آموزشی (15٪)
- سایر خدمات (به جز مدیریت دولتی) (15٪)

برنامه حسابرسی – کلیه پاسخ دهندگان

در بخش زیر به تفصیل روندهای برنامه‌های حسابرسی بر اساس طبقه بندی در طی یک دوره سه ساله ارائه شده است. میانگین همه پاسخ دهندگان نقطه شروع خوبی را ارائه می‌دهند و چشم انداز بزرگی را در مورد اقدامات برنامه حسابرسی ارائه می‌دهند. اما مفیدترین اطلاعات بعد از تفکیک نوع سازمان ها حاصل می‌شود. لازم به ذکر است که سهامی عام و خدمات مالی هر کدام، تقریباً یک سوم از پاسخ دهندگان را در بر می گیرد و بنابراین نتایج میانگین کلی را هدایت می‌کنند (شکل B).

شکل B: تخصیص برنامه حسابرسی – کلیه پاسخ دهندگان (2017 تا 2019)



یادداشت: تخصیص تلاش حسابرسی با توجه به بررسی سالانه پالس از سال 2017 تا 2019. ICFR = کنترل های داخلی حاکم بر گزارشگری مالی. درصد اختصاص داده شده به "سایر" در این نمودار موجود نیست.

- روند صعودی (1 درصد افزایش یا بیشتر)
- خنثی (خط توپر) (کمتر از 1 درصد تغییر)

■ روند نزولی (1 درصد کاهش یا بیشتر)

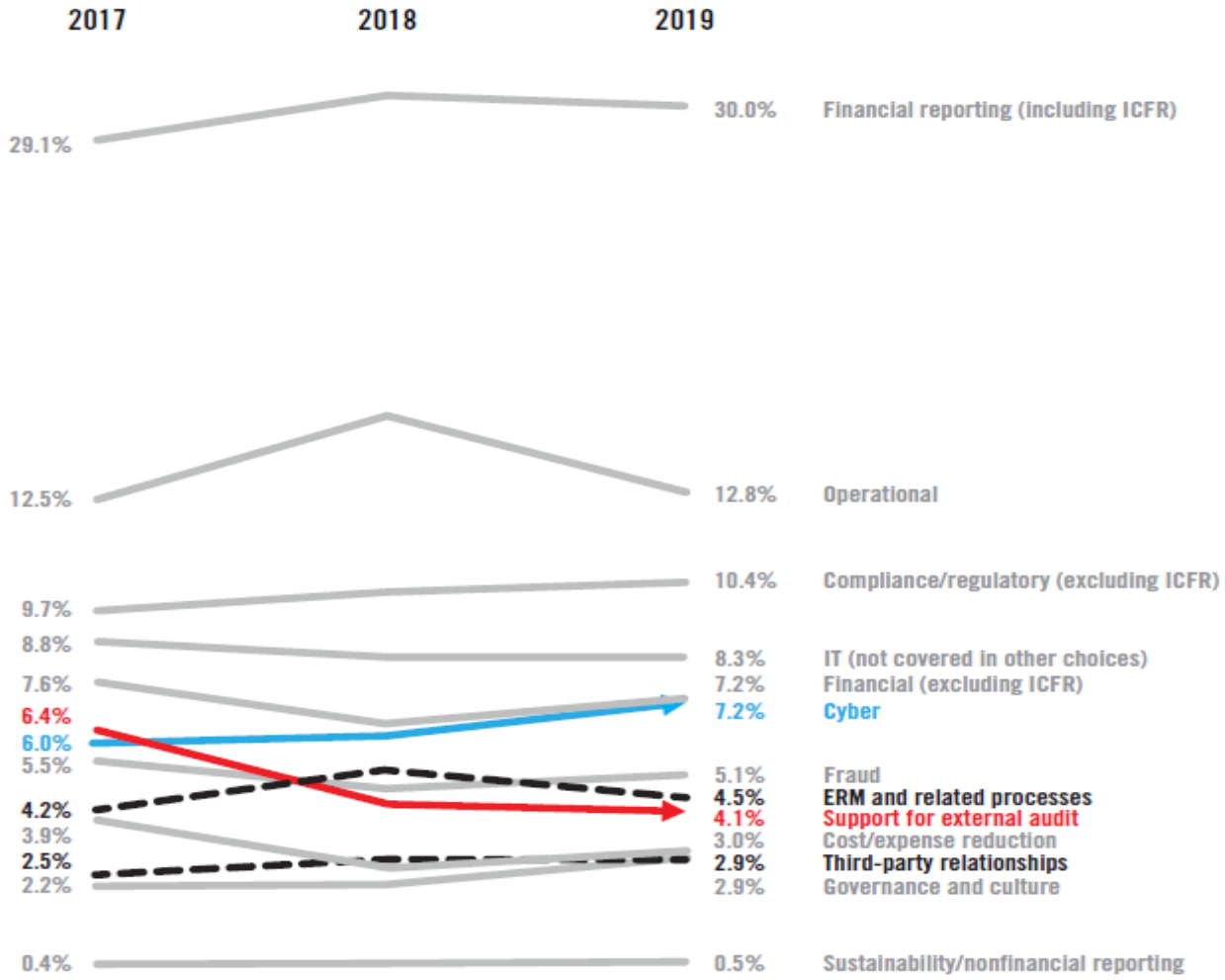
■ سیاه (خط چین) * (کمتر از 1 درصد تغییر)

* خط نقطه چین برای کمک به تمایز خطوط استفاده می‌شود.

برنامه حسابرسی – سهامی عام

مقررات گزارشگری مالی و تطبیق به وضوح بر عملکردهای حسابرسی در شرکتهای سهامی عام تاکید دارد. حدود 40 درصد از برنامه‌های حسابرسی در این نوع سازمانها به این دو حوزه اختصاص دارد. با افزودن سه حوزه پر ریسک دیگر (عملیاتی، سایبر و فناوری اطلاعات) نزدیک به 69 درصد از برنامه حسابرسی به این پنج حوزه ریسک اختصاص داده شده است. این باعث می‌شود 31 درصد باقیمانده بین سایر مناطق در معرض ریسک از جمله مدیریت ریسک سازمانی، کشف کلاهبرداری، روابط شخص ثالث و حاکمیت و فرهنگ تقسیم شود.

شکل C: تخصیص برنامه حسابرسی – سهامی عام (2017 تا 2019)



یادداشت: تخصیص تلاش حسابرسی با توجه به بررسی سالانه پالس از سال 2017 تا 2019. ICFR = کنترل داخلی حاکم بر گزارشگری مالی. درصد اختصاص داده شده به "سایر" در این نمودار موجود نیست. فقط پاسخ دهندگان سهامی عام(به استثنای خدمات مالی)

■ روند صعودی (1 درصد افزایش یا بیشتر)

■ خنثی (خط توپر) (کمتر از 1 درصد تغییر)

■ روند نزولی (1 درصد کاهش یا بیشتر)

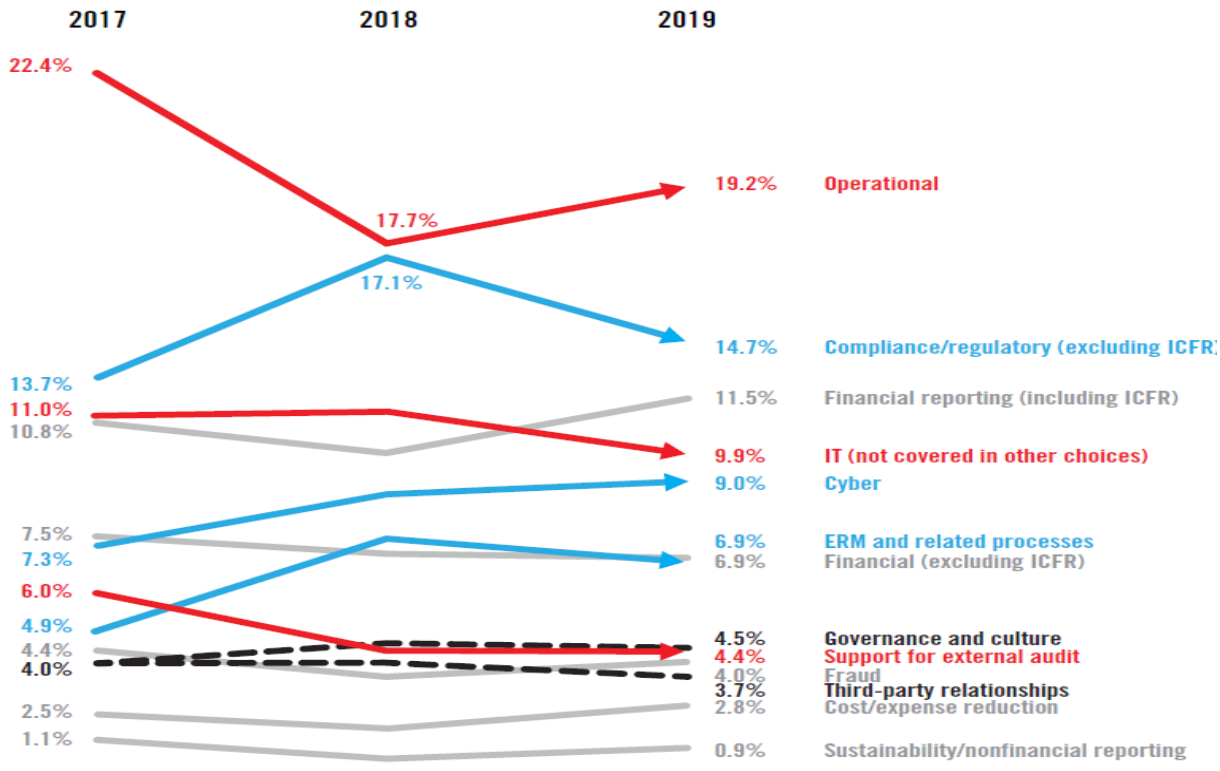
■ سیاه (خط چین) * (کمتر از 1 درصد تغییر)

* خط نقطه چین برای کمک به تمایز خطوط استفاده می‌شود.

برنامه حسابرسی – خدمات مالی

با وجود شرایط نظارتی سنگین در خدمات مالی، این تنها نوع سازمانی است که در برنامه حسابرسی تلاش عملیاتی فراتر از میزان مقبول انجام می‌دهد. در مقایسه با شرکت‌های سهامی عام، خدمات مالی فقط حدود یک چهارم (26 درصد) برنامه حسابرسی خود را به انطباق و گزارشگری مالی اختصاص می دهد (Sarbanes-Oxley). در واقع، خدمات مالی در مقایسه با سهامی عام قادر است که درصد بالاتری از برنامه حسابرسی خود را به بخش عملیاتی، cyber / IT، ERM، ریسک های شخص ثالث و ریسک های حاکمیتی و فرهنگی اختصاص بدهد. لازم به ذکر است که برخی سازمانها الزامات انطباق، مانند تست استرس را به عنوان بخشی از عملیات می‌دانند، که می‌تواندکژی تخصیص عملیات را بالاتر ببرد. (شکل D).

شکل D: تخصیص برنامه حسابرسی - خدمات مالی (2017 تا 2019)



یادداشت: تخصیص تلاش حسابرسی با توجه به بررسی سالانه پالس از 2017 تا 2019. ICFR = کنترل داخلی حاکم بر گزارشگری مالی. درصد اختصاص داده شده به "سایر" در این نمودار درج نشده است. فقط پاسخ دهندگان خدمات مالی.

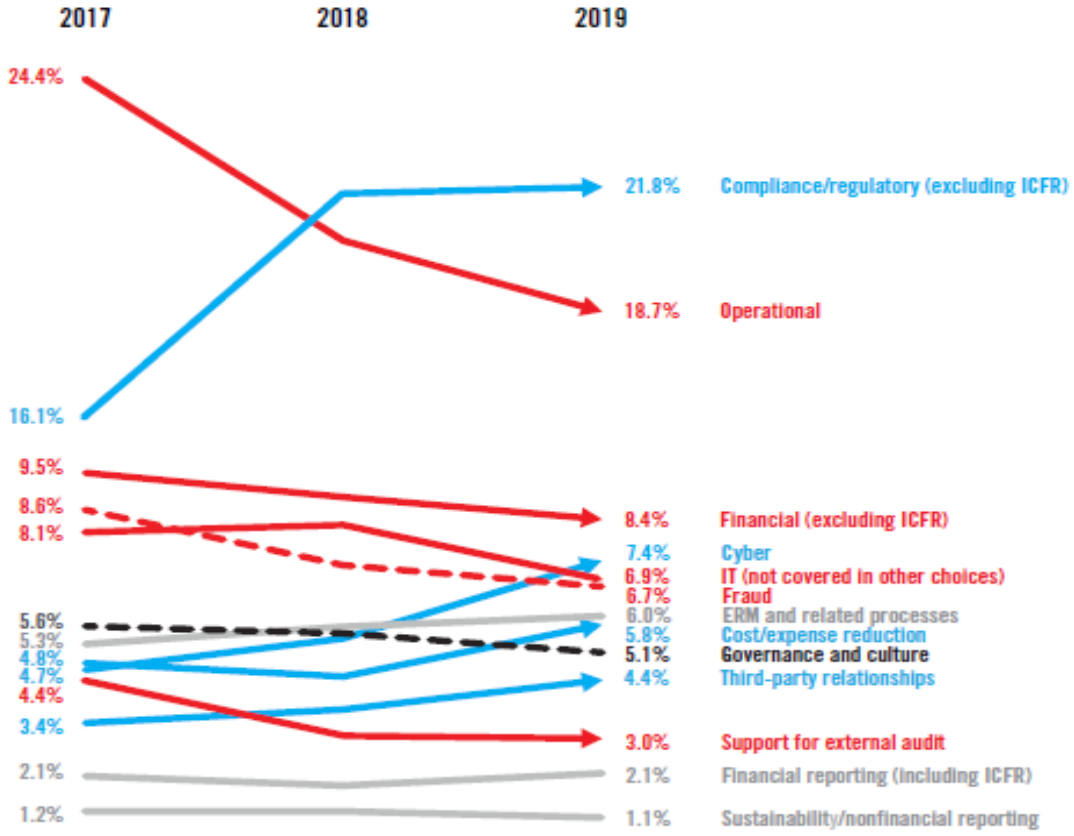
- روند صعودی (1 درصد افزایش یا بیشتر)
- خنثی (خط توپر) (کمتر از 1 درصد تغییر)
- روند نزولی (1 درصد کاهش یا بیشتر)
- سیاه (خط چین) * (کمتر از 1 درصد تغییر)

* خط نقطه چین برای کمک به تمایز خطوط استفاده می‌شود.

برنامه حسابرسی – خدمات عمومی

تطبیق عمومی بزرگترین بخش برنامه حسابرسی برای بخش خدمات دولتی است، که عمدتا توسط حسابرسی های اجباری از قوه مقننه یا سایر دستگاه های حاکمیتی هدایت می شود. به همین ترتیب، حسابرسی‌های عملیاتی با بررسی عملکرد اقتصاد سازمان های دولتی و کارآیی و استفاده مؤثر از منابع موجود صورت می پذیرد. اگر چه سهم حسابرسی عملیاتی به میزان قابل توجهی در برنامه حسابرسی کاهش یافته ولی همچنان رتبه دوم را دارد. خدمات عمومی 14 درصد را برای ترکیب IT / سایبر اختصاص می دهد، که فقط 1 درصد پایین‌تر از میانگین همه پاسخ دهندگان است (شکل E).

شکل E: تخصیص برنامه حسابرسی - خدمات عمومی (2017 تا 2019)



یادداشت: تخصیص تلاش حسابرسی با توجه به بررسی سالانه پالس از 2017 تا 2019. ICFR = کنترلهای داخلی حاکم بر گزارشگری مالی. درصداختصاص داده شده به "سایر" در این نمودار موجود نیست. فقط پاسخ دهندگان خدمات عمومی (به استثنای خدمات مالی).

■ روند صعودی (1 درصد افزایش یا بیشتر)

■ خنثی (خط توپر) (کمتر از 1 درصد تغییر)

■ روند نزولی (1 درصد کاهش یا بیشتر)

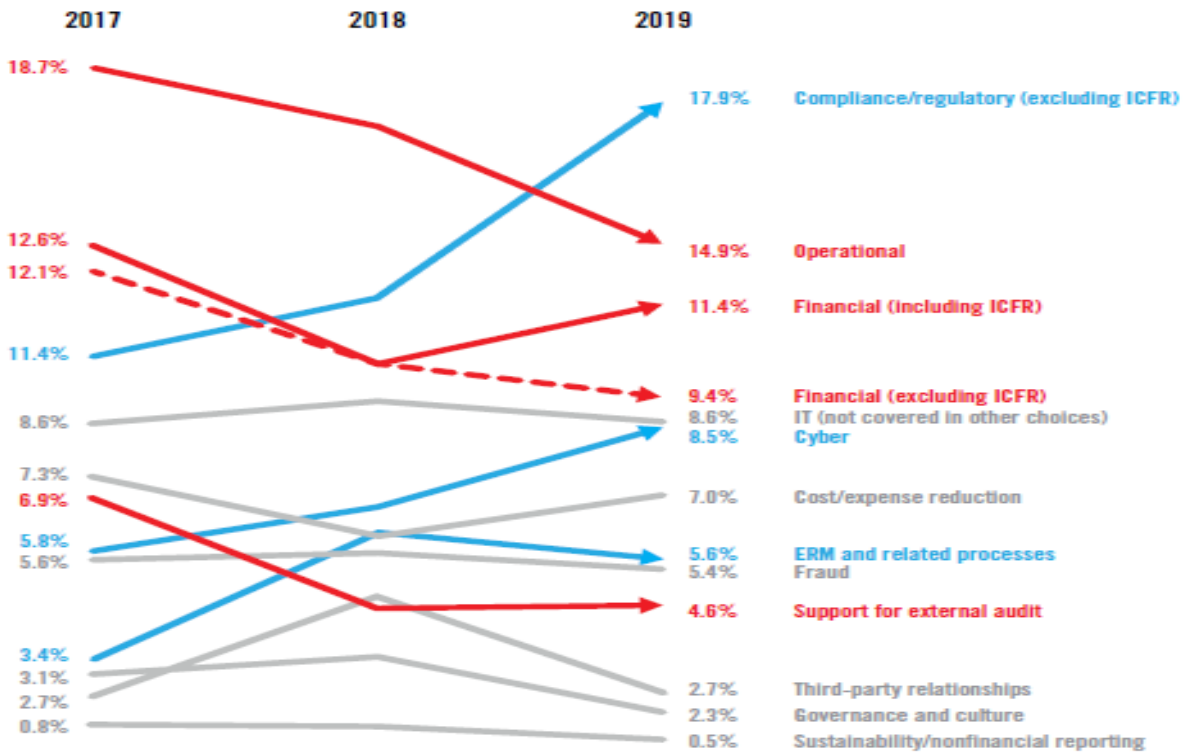
■ سیاه (خط چین) * (کمتر از 1 درصد تغییر)

* خط نقطه چین برای کمک به تمایز خطوط استفاده می‌شود.

برنامه حسابرسی – سهامی خاص

تولید، خدمات درمانی و خدمات علمی، بخش عمده از فعالیت سازمانهای سهامی خاص را به خود اختصاص داده است که تمرکز آن بیشتر بر روی موضوعات غیر مالی و تلاش های نظارتی است. ریسک های این صنایع بیشتر بر نگرانی‌های زیست محیطی، بهداشتی و ایمنی متمرکز است. این نوع سازمان ها تلاش بیشتری را برای موضوعات سایبری و مسائل مربوط به فناوری اطلاعات اختصاص می دهد، که ممکن است ناشی از نگرانی‌های بیشتری در مورد حفاظت از داده‌ها باشد و یا میتواند به دلیل تطبیق بیشتر با GDPR و سایر قوانین محافظت از داده ها و حریم خصوصی که در سال 2018 به اجرا در آمد، باشد. (شکل F)

شکل F: تخصیص برنامه حسابرسی -سهامی خاص (2017 برای 2019)



یادداشت : تخصیص تلاش حسابرسی با توجه به بررسی سالانه پالس از 2017 تا 2019. ICFR = کنترل داخلی حاکم بر گزارشگری مالی. درصد اختصاص داده شده به "سایر" در این نمودار درج نشده است. فقط پاسخ دهندگان خصوصی (به استثنای خدمات مالی).

■ روند صعودی (1 درصد افزایش یا بیشتر)

■ خنثی (خط توپر) (کمتر از 1 درصد تغییر)

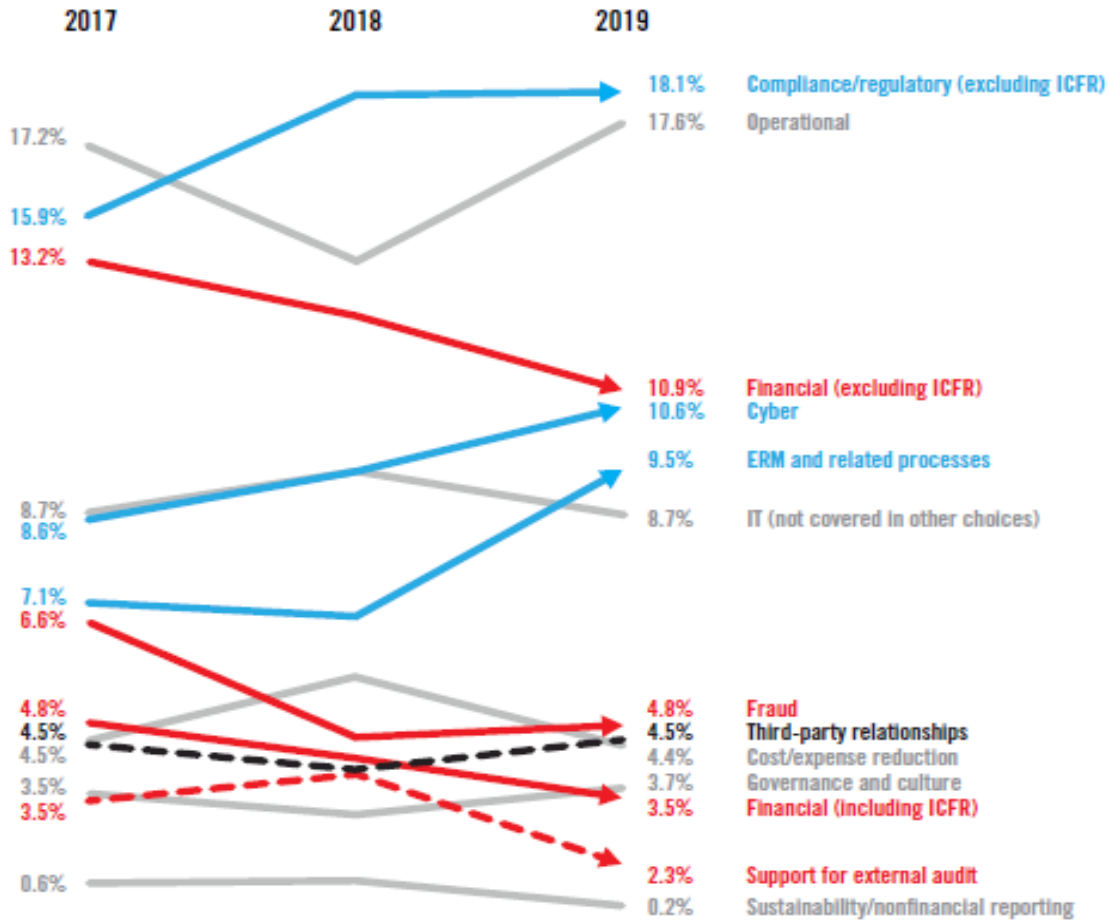
■ روند نزولی (1 درصد کاهش یا بیشتر)

■ سیاه (خط چین) * (کمتر از 1 درصد تغییر)

* خط نقطه چین برای کمک به تمایز خطوط استفاده می‌شود.

پاسخ ها برای این نوع سازمان در درجه اول مربوط به دو گروه مراقبت‌های بهداشتی و کمک‌های اجتماعی بوده است (58 درصد). برای این دو گروه، دو منطقه در معرض ریسک، تقریباً یکسان است. هر دو گروه همچنین نسبت به میانگین، درصد بالاتری از برنامه‌های حسابرسی خود را به IT / سایبر اختصاص داده اند. سازمان‌های غیر انتفاعی در مقایسه با میانگین کلی 17 ٪، درصد بیشتری از برنامه حسابرسی خود را به IT / سایبر (20٪) اختصاص داده اند. آن ها همچنین در مقایسه با میانگین کلی 6٪ ، درصد بالاتری را به مدیریت ریسک سازمانی اختصاص داده اند(10 ٪) (شکل G).

شکل G: تخصیص برنامه حسابرسی - بخش بخش غیرانتفاعی (2017 برای 2019)



یادداشت: تخصیص تلاش حسابرسی طبق بررسی سالانه پالس از سال 2017 تا 2019. ICFR = کنترل داخلی حاکم بر گزارشگری مالی. درصد اختصاص داده شده به "سایر" در این نمودار درج نشده است. فقط پاسخ دهندگان بخش غیرانتفاعی (به استثنای خدمات مالی).

■ روند صعودی (1 درصد افزایش یا بیشتر)

■ خنثی (خط توپر) (کمتر از 1 درصد تغییر)

■ روند نزولی (1 درصد کاهش یا بیشتر)

■ سیاه (خط چین) * (کمتر از 1 درصد تغییر)

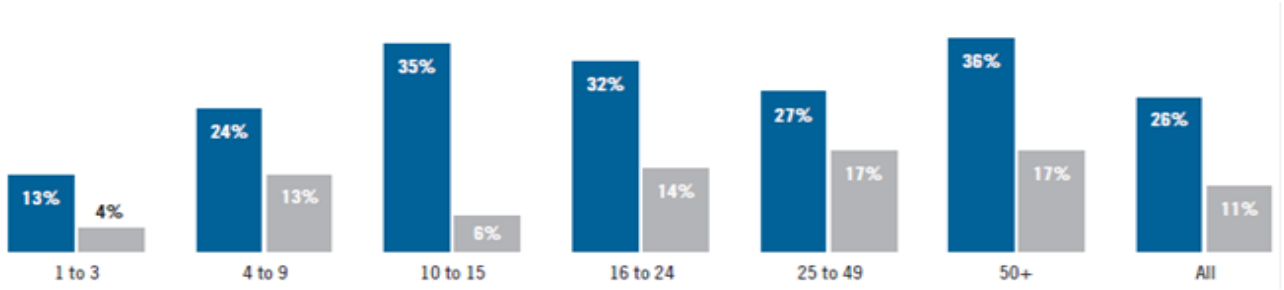
* خط نقطه چین برای کمک به تمایز خطوط استفاده می‌شود.

کارمندان

در سال گذشته تعداد مدیران اجرایی حسابرسی که افزایش تعداد کارکنان را گزارش کرده اند دو برابر تعداد مدیرانی بوده اســت کــه کاهش گزارش کرده اند(26 درصد به 11درصد). شایان ذکر است که کوچکترین حوزه ها (1 تا 3 FTE) در مقایسه با میانگین کلی بــه طور معناداری احتمال پایین تری برای افزایش دارند (13 درصد در مقایسه با 26 درصد). بیشترین رشد در حوزه هــایی بــا 10 تــا 15 FTE رخ داده است، (35 درصد گزارش ها حاکی از افزایش بوده ودر مقابل 16 درصد گزارش کاهش داده اند) (شکل H).

نمودار پایین صفحه تعداد FTE هایی را که در حوزه هایی از حسابرسی داخلی که تغییری را تجربه کرده است (افــزایش یــا کــاهش یافته اند) را نشان می‌دهد. حوزه هایی که تغییر را تجربه کرده اند به طور متوسط 2.7 FTEها افزایش می‌یابد در حالی کــه بــه طــور متوسط 3.2 FTE کاهش می‌یابد. لازم به ذکر است که حوزه هایی با 50 یا بیشتر FTE، نوسانات بیشتری را با افزایش و کاهش قابل توجه FTE گزارش کرده‌اند (نمودار I).

شکل H: افزایش یا کاهش گزارش حوزه حسابرسی داخلی در سال گذشته

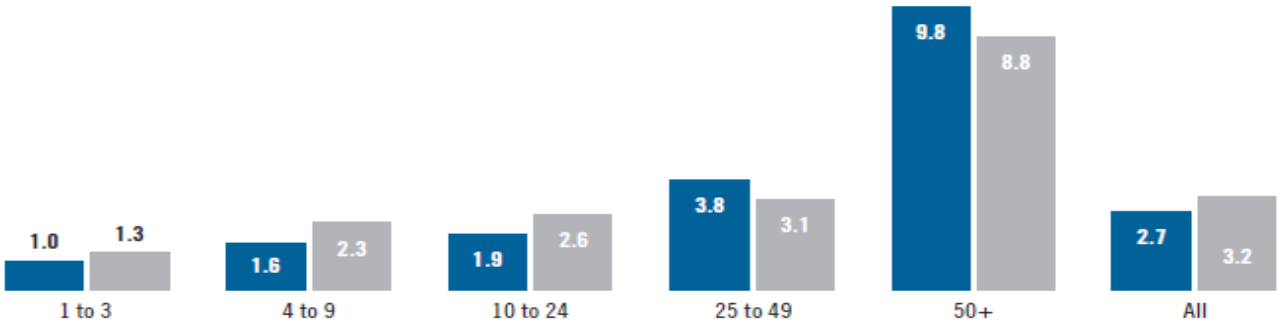


اندازه حوزه حسابرسی داخلی

یادداشت: Q42: با نگاهی به 12 ماه گذشته، تعداد پرسنل معادل تمام وقت (کارمندان، پیمانکاران، کارآموز و برون سپاری) در حــوزه حسابرسی داخلی شما: افزایش، عدم تغییر، یا کاهش را تجربه کرده است. FTE مخفف معادل ساعات کاری کارکنان تمام وقت است.

- افزایش را تجربه کرد
- کاهش را تجربه کرد

شکل I: متوسط افزایش یا کاهش FTE در سال گذشته



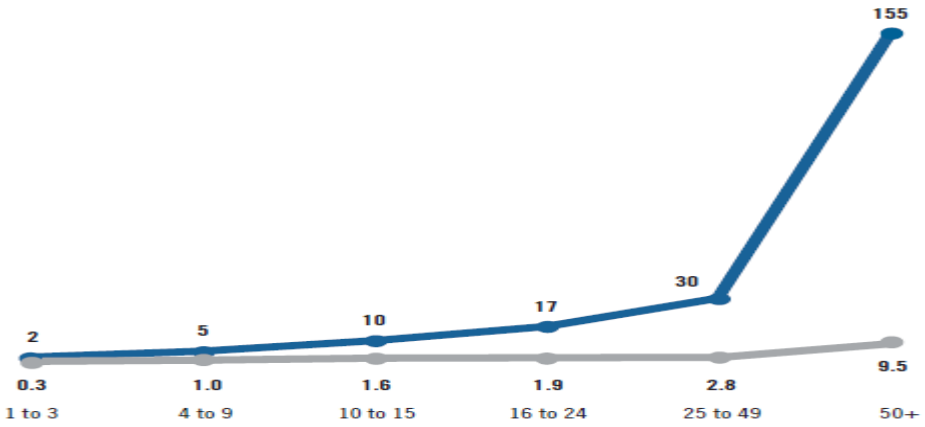
یادداشت:**Q43**: به چه تعدادی کارمندان خود (کارمندان، پیمانکاران، شرکت‌های همکار و برون سپاری) را افزایش داده اید؟در مقایسه با **Q44**: چه تعداد از کارمندان خود را کاهش داده اید (کارمندان، پیمانکاران، تأیید شده، و برون سپاری)؟ **FTE** مخفف معادل ساعات کاری کارکنان تمام وقت است.

- میزان **FTE** ها افزایش یافته است
- میزان **FTE** ها کاهش یافته است

درون سازمانی، برون سپاری، همکار بیرونی و پیمانکاری

برای اولین بار، معیارهای مدیریت پالس، داده‌هایی درمورد تعداد **FTE** های برون سپاری، همکار بیرونی، یا پیمانکاری برای فعالیت حسابرسی داخلی را پوشش داد. همانطور که در شکل **J** نشان داده شده است، تعداد **FTE** های غیر حسابرسان داخلی به طور کلی بین **1** تا **3** می باشد و متناسب با اندازه حوزه حسابرسی داخلی افزایش نمی‌یابد. این نشان می دهد که تأثیر برون سپاری برای حوزه های کوچکتر بیشتر است.

شکل **J**: **FTE** های حسابرسی داخلی درون سازمانی در مقایسه با **FTE** های همکاری خارجی / پیمانکاری/ برون سپاری*



اندازه حوزه حسابرسی داخلی

یادداشت:Q37: تعداد تقریبی FTE های درون سازمانی (شامل CAE، کارمندان و پیمانکاران بلند مدت) را وارد کنید. Q38: تعداد تقریبی سایر FTE های بدست آمده را از طریق قراردادهای کوتاه مدت، همکاری خارجی، برون سپاری یا سایر موارد مشابه وارد نمایید. FTE معادل تعداد ساعات یک کارمند تمام وقت است.

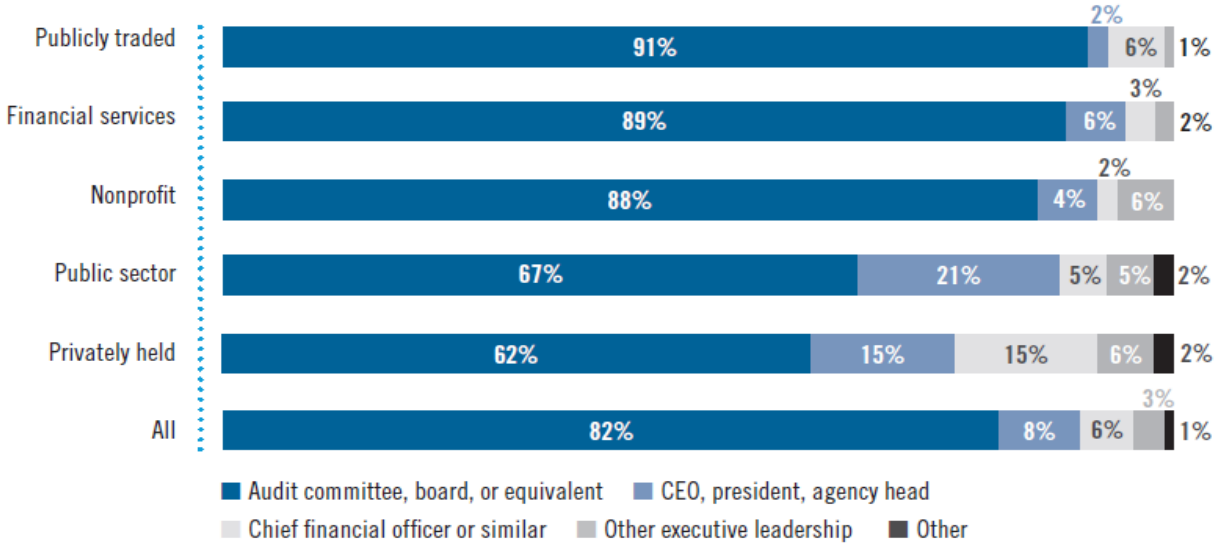
* چندین حوزه حسابرسی داخلی بسیار بزرگ در طبقه +50 باعث شده است که میانگین FTEهای این گروه نسبت به سایر حوزهها بسیار بالا باشد.

درون سازمانی

قراردادهای برون سپاری / همکاری خارجی / قراردادهای پیمانکاری

خطوط گزارشگری:

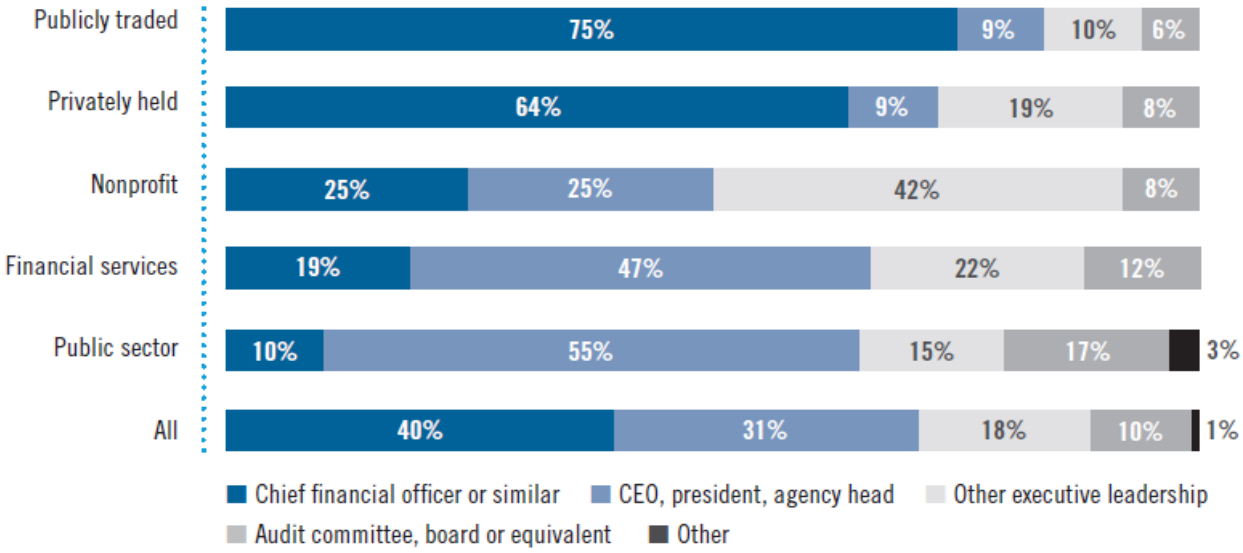
شکل K: خطوط گزارش گری عملکردی*



یادداشت:Q35: خط اصلی گزارش گری عملکردی برای مدیر اجرایی حسابرسی (CAE) یا رئیس حسابرسی داخلی در سازمان شما چیست؟

* به نظارت بر مسئولیت‌های حوزه حسابرسی داخلی، از جمله تصویب منشور حسابرسی داخلی، تصویب برنامه حسابرسی، ارزیابی CAE، جبران خسارات CAE. اشاره دارد.

شکل L: خطوط گزارشگری اداری *



یادداشت:**Q34**: در سازمان شما خط اصلی گزارش اداری برای مدیر اجرایی حسابرسی (CAE) یا رئیس حسابرسی داخلی چیست؟

* گزارشگری اداری به نظارت بر امور روزمره، تأیید هزینه، مدیریت منابع انسانی، ارتباطات، سیاست‌ها و رویه‌های داخلی اشاره دارد.

یاداشت ها

1. 2018–2019 NACD Public Company Governance Survey: Key Findings (Arlington, VA: National Association

of Corporate Directors, Dec. 2018), Key Finding 3, accessed at https://www.nacdonline.org/insights/publications.cfm?ItemNumber=63799.

2. 2018–2019 NACD Public Company Governance Survey: Key Findings (Arlington, VA: National Association of Corporate Directors, Dec. 2018), Key Finding 9, accessed at https://www.nacdonline.org/insights/publications.cfm?ItemNumber=63799.

3. 2018–2019 NACD Public Company Governance Survey: Key Findings (Arlington, VA: National Association of Corporate Directors, Dec. 2018), Key Finding 1, accessed at https://www.nacdonline.org/insights/publications.cfm?ItemNumber=63799.

4. Q52: How would you describe the level of risk in your organization in the following risk areas? $n = 502$.

5. Q27: Which types of third parties are significant in your organization's business model? $n = 509$.

6. Top Third-party Breaches of 2018 (So Far) (Denver, CO: Cyber GRX, 7 June 2018), accessed at https://www.cybergrx.com/resources/blog/top-11-third-party-breaches-of-2018-so-far-data-breach-report/.

7. Q25: Have you experienced such a surprise* in the last 12 months? *An emerging or atypical risk requiring the attention of executive management that was not foreseen. $n = 435$.

8. 2018–2019 NACD Public Company Governance Survey: Key Findings (Arlington, VA: National Association of Corporate Directors, Dec. 2018), Key Finding 9, accessed at https://www.nacdonline.org/insights/publications.cfm?ItemNumber=63799.

9. Interpretation of IIA Standard 1110 — Organizational Independence (Lake Mary, FL: Institute of Internal Auditors, 1 January 2017), accessed at https://global. theiia.org/standards-guidance/attribute-standards/Pages/Attribute-Standards.aspx Also see Implementation Guide 1100: Independence and Objectivity (Lake Mary, FL: Institute of Internal Auditors, 1 January 2017), section titled "Considerations for Implementation," p. 14, accessed at https://na.theiia.org/standards-guidance/ recommended-guidance/Pages/Practice-Advisories.aspx.