

ریسک های در کانون توجه سال

۲۰۲۱

موضوعات داغ برای حسابرسان داخلی

قسمت اول

دپارتمان حسابرسی داخلی



موسسه حسابرسی آزمون پرداز

(حسابداران رسمی)



این گزارش توسط کنسرسیومی از موسسات حسابرسی داخلی شامل موسسات زیر منتشر شده است:
 The Chartered Institute of Internal Auditors (UK & Ireland), Deutsches Institut für Interne Revision (DIIR), IIA Belgium, IIA Nederland, IIA Luxembourg, IIA Austria, Instituto de Auditores Internos de España, IIA Sweden, Institut Français De L'audit Et Du Contrôle Interne (IFACI) and the Italian Association of Internal Auditors.
 و به منظور بهره‌برداری در ایران توسط موسسه حسابرسی آزمون‌پرداز (حسابداران رسمی) ترجمه شده است.
 تولید مجدد این گزارش به طور کامل یا جزئی بدون ذکر کامل ممنوع است.

©2020. All rights reserved.

حسابرسی داخلی لازمه حاکمیت و عملکرد خوب یک مجموعه است. حسابرسی داخلی در مورد اداره ریسک‌های اصلی ایجاد اطمینان می‌کند، اطلاعات لازم برای تصمیم‌گیری مدیران را فراهم می‌کند و عملکرد سازمان را بهبود می‌بخشد.
 ما با استفاده از افراد آگاه و به روز، رویکرد هوشمند و تکنولوژی هوشمند، دپارتمان حسابرسی داخلی شما را پشتیبانی می‌کنیم. این ترکیب، یک ارزش افزوده واقعی را برای مشتریان ما به ارمغان می‌آورد و به بهبود عملکرد آن‌ها کمک می‌کند.

راهکارهای آزمون‌پرداز برای شما در حوزه حسابرسی داخلی و ریسک

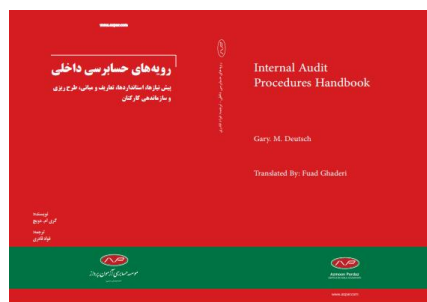
برای:

- اجرای انواع حسابرسی داخلی مبتنی بر ریسک در چارچوب‌های متنوع (کوزو، کوبیت، بلوغ و ...)
- واپایش حسابرسی داخلی توانگرا (ارزیابی اثربخشی و کیفیت فعالیت حسابرسی داخلی بر اساس مدل بلوغ با ارائه تأییدیه معتبر)
- استقرار حسابرسی داخلی، تدوین نظامنامه حسابرسی داخلی و استقرار نظام ارزیابی کیفیت آموزش حسابرسی داخلی
- طراحی سیستم کنترل‌های داخلی
- تحلیل داده‌ها و تحلیل علل ریشه‌ای – انتخاب بهترین رویکرد برای تغییر
- ارزیابی اثربخشی فرآیندهای مدیریت ریسک، کمیته ریسک و کمیته حسابرسی
- استقرار مکانیزم مدیریت ریسک
- شش سیگما و مدیریت ناب – بهبود کارایی عملیاتی
- محک زنی و حسابرسی عملیاتی

با ما در آزمون‌پرداز در تماس باشید.

در هر یک از موارد، ما از سه طریق برون‌سپاری، هم‌سپاری و آموزش و پژوهش در کنار شما هستیم.

انتشارات در حوزه حسابرسی داخلی



فهرست

۴	پیش‌گفتار (ریسک‌های در کانون توجه سال ۲۰۲۱)
۵	مقدمه
۶	متدولوژی (روش‌شناسی)
۷	تجزیه داده‌ها: نتایج نظرسنجی
۱۰	اولویت ریسک در برابر تمرکز حسابرسی
۱۱	ریسک‌های امروز و فردا
۱۲	تمرکز حسابرسی در طول زمان
۱۳	امنیت اطلاعات در محیط کار گسترش یافته

ادامه دارد...



ریسک‌های در کانون توجه سال ۲۰۲۱ در نوشتار

بدون شک، سال ۲۰۲۰ توسط ویروس همه‌گیر جهانی کرونا (GCP) تعریف شد. در ماه مارس، همزمان با شروع تحقیق برای "Risk in Focus"، تبدیل اروپا به مرکز بزرگترین بحران عمومی سلامت در حافظه بشر باقی خواهند ماند. علیرغم این واقعیت که مجمع اقتصاد جهانی و سایر کشورها زنگ خطر را برای امنیت سلامت جهانی و احتمال وقوع یک رویداد همه‌گیر به صدا درآورده بودند، بسیاری از کشورها و کسب و کارها غافلگیرانه گرفتار شدند.

این ویروس نه تنها پیامدهای عظیمی در سلامت عمومی داشته است، بلکه اقدامات فاصله‌گذاری اجتماعی و قرنطینه‌گذاری نیز تأثیرات اقتصادی عمیقی داشته است. حداقل پس از بحران مالی جهانی سال ۲۰۰۸، GCP مهمترین و گسترده‌ترین رویداد برای کسب و کارها است و انتظار می‌رود منجر به رکود عمیق‌تر، نرخ بالاتر بیکاری و افزایش بیشتر بدهی‌های عمومی شود.

مشاغل و پروفایل ریسک آن‌ها به طور قابل توجهی تحت تأثیر ویروس کرونا قرار گرفته است. دستور دولت‌ها و کارفرمایان مبنی بر فرستادن کارکنان به منزل برای دورکاری در نیمه اول سال ۲۰۲۰ نشان دهنده‌ی این است که اولویت اصلی، ایمنی کارکنان بوده است.

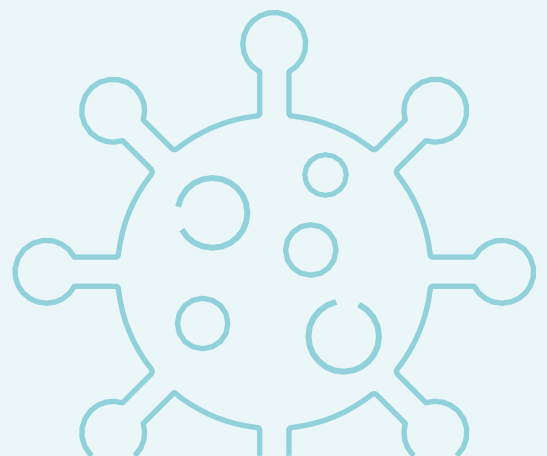
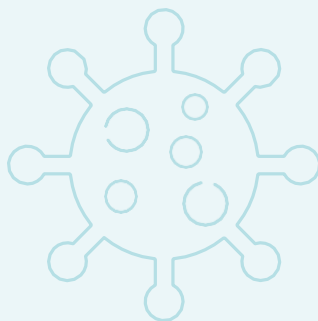
تعطیلی و قرنطینه‌ها به طور حتم سبب اختلال عملیاتی شدیدی شد، به طوری که شرکت‌ها ناگزیر به اعمال تعدیلات سریع شدند و بخش‌هایی از جمله تولید، ساخت و ساز و صنایع به منظور حفظ اقدامات فاصله‌گذاری در کسب و کار اصلی خود، مجبور به کاهش تولید شدند.

ابتدای تابستان ۲۰۲۰ با کاهش محدودیت‌ها مشخص شد، طوری که دولت‌ها تعادل ظریف و شکننده شروع اقتصادشان را با تجدید فعالیت این سربازها مدیریت کردند. انتظار می‌رود که در سال ۲۰۲۱ این چالش مدیریت شود. اگرچه دوره پیشروی دقیق این بیماری همه‌گیر نامشخص است، اما در نیمه دوم سال ۲۰۲۰ روند شتاب آن ادامه دارد.

پیامدهای طولانی مدت این سناریوی استثنایی واضح نیست. دولت‌ها و کسب و کارها درس‌های زیادی را در طول ماه‌ها و سال‌های آینده فرا خواهند گرفت. حسابرسی داخلی می‌تواند و باید در این زمینه کمک کند. دیدگاه منحصر به فرد و ۳۶۰ درجه آن در مورد کسب و کار و نگرش کنترل ریسک می‌تواند به سازمان‌ها در شناسایی نقاط کور و فرصت‌ها برای بهبود عملکردشان کمک کند.

با نگاهی به سال ۲۰۲۱ درمی‌یابیم، چشم‌انداز اقدامات گسترده حسابرسی داخلی هیچگاه به این اندازه ضروری نبوده است. هیئت مدیره و تیم‌های مدیریت اجرایی برای پیش در کسب و کار و ریسک‌های آن در طی یک دوره چالش برانگیز قابل ملاحظه، به این دیدگاه مستقل از بالا به پایین بستگی خواهند داشت.

این پس زمینه استثنایی است که Risk in Focus امسال با آن تنظیم شده است.



مقدمه

در پنج سال گذشته *Risk in Focus* تلاش کرده تا زمینه‌های اصلی ریسک را که توسط مدیران ارشد حسابرسی (CAE) شناسایی شده‌اند، برجسته کند. هدف از این کار کمک به حرفه حسابرسی داخلی برای تهیه ارزیابی ریسک مستقل، برنامه ریزی سالانه و حتی تعیین دامنه حسابرسی از طریق به اشتراک گذاشتن بینش‌ها و آموخته‌های حاصل از تحقیق است.

برخلاف سال‌های گذشته، شرایط بی سابقه ناشی از ویروس همه‌گیر کرونا، بزرگترین رویداد ریسک جهانی اخیر، بدون شک چشم انداز ۲۰۲۱ را شکل داده است. با این حال، خود ویروس کرونا ریسک اصلی نیست. ویروس کرونا به جای تهدیدهای جدید، ریسک‌های موجود را تشدید کرده و آن‌ها را در معرض دید جدید قرار داده و سازمان‌ها را مجبور کرده است که از زوایای مختلف درباره آن‌ها فکر کنند یا اولویت‌های جدیدی را به آن‌ها اختصاص دهند. به عنوان یک قضیه، امنیت سایبری و داده‌ها یک ریسک دائمی برای اعضای هیئت مدیره، اعضای کمیته حسابرسی و مدیران ارشد حسابرسی است. تکالیف گسترده به این معنی است که امنیت سایبری بعد جدیدی به خود گرفته است، زیرا زیرساخت‌های فناوری اطلاعات و دیوار محیطی کسب و کار باید در زمان رکورد سازگار شود. ناگزیر، تلاش‌های فیشینگ یا تله‌گذاری^۱ و حوادث مهندسی اجتماعی^۲ در حالی افزایش یافته است که بازیگران بد، تلاش می‌کنند از نقاط ضعف امنیتی بدنبال هزیمت کارکنان در خانه‌های خود (ناشی از دورکاری) استفاده کنند.

سیستم‌های مدیریت ریسک و کنترل داخلی معتبر در میان اختلالات عملیاتی در مقیاس وسیع ارتقا یافته‌اند. حسابرسی داخلی ناگزیر به پرسش در خصوص چگونگی سیاست‌ها، فرآیندها و حمایت‌های ریشه‌ای جاسازی شده در DNA شرکت - به طور خواسته یا ناخواسته - تغییر کرده‌اند تا عملکرد مستمر سازمان را تضمین کنند. محل کار به تدریج در اواسط سال بازگشایی شدند، اما انتظار می‌رود که درجه قابل توجهی دورکاری برای مدت نامعلومی باقی بماند. این امر تأثیراتی در قدرت و یکپارچگی و درستی محیط کنترل داخلی دارد.

برای این امر، حسابرسی داخلی خود مجبور به ارزیابی سریع آن‌چه که در سال ۲۰۲۰ - ۲۰۲۱ می‌تواند ارائه کند، شده است. برنامه‌های حسابرسی پذیرفته شده (مورد توافق) مجدداً مورد بررسی قرار گرفته است تا مشخص کند چه چیزی در اولویت است و کدام کارها می‌توانند، در صورت لزوم، از راه دور انجام شود. تجزیه و تحلیل داده‌ها برای حسابرسی داخلی در مرحله اولیه دورکاری، سود زیادی کسب کرده است و بعضی از آن‌ها از زمان از کار افتادگی (ناشی از کرونا) هوشمندانه استفاده کرده‌اند تا در نهایت قابلیت‌های حسابرسی دیجیتال و مستمر با برنامه‌ریزی طولانی را در خود جای دهند. با عنایت بر دسترسی محدود به کسب و کار و محدودیت‌های سفرهای بین‌المللی، تجزیه و تحلیل و حسابرسی مستمر هرگز به این اندازه موضوعیت نداشته است.

برخی از مدیران حسابرسی، با علم به اینکه پیشنهادات سالانه به زودی منسوخ می‌شوند، پروژه‌های شش‌ماهه یا سه‌ماهه تنظیم کرده‌اند یا به طور کلی خارج از برنامه کار می‌کنند. در برخی موارد پشتیبانی حسابرسی داخلی کوتاه، تیز و به موقع (در زمان واقعی) ارائه شده است و مدیران اجرایی حسابرسی داخلی پیش بینی می‌کنند که این رویه‌ی چالاکانه، برای مدتی نامعلوم حفظ شود. همچنین خط سوم فراخوانده شده است تا نقش مشاور معتمد را با ضرورت و فوریتی که در سال‌های اخیر، هرگز موردی از آن نبوده، اتخاذ کند.

حسابرسی داخلی باید آینده نگر و کنش‌گرا^۳ (پیش‌قدم در شناسایی و پیشگیری از مشکلات احتمالی) باشد، و به نزدیکی خود به کسب و کار تا آن‌جا که ممکن است، ادامه دهد تا هر دوی ریسک‌ها و نیازهای آن را درک کند. به طور فزاینده‌ای، این نه تنها شامل ملاحظات عملیاتی، بلکه شامل ریسک‌ها و عوامل استراتژیک در محیط خارجی است که بر سازمان تأثیر می‌گذارد.

اکنون، زمان اثبات ارزشمندی حسابرسی داخلی است.

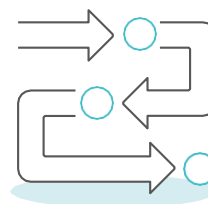
^۱ (ارتباطات از راه دور) روش استفاده از ایمیل‌های جعلی و کپی از وبسایت‌های قانونی برای استخراج داده‌های مالی از کاربران رایانه برای اهداف سرقت هویت

^۲ استفاده از برنامه ریزی متمرکز در تلاش برای مدیریت تغییرات اجتماعی و تنظیم توسعه و رفتار آینده یک جامعه.

^۳ (از طرف شخص، خط مشی یا عملی) ایجاد موقعیت یا کنترل اوضاع با ایجاد اتفاقی به جای پاسخ دادن به آن پس از وقوع.



روش شناسی



تحقیق *Risk in Focus* ۲۰۲۱ بار دیگر ترکیبی از هر دو روش نظرسنجی کمی و مصاحبه کیفی با مدیران ارشد حسابرسی، این بار از ۱۱ کشور اروپایی و ۱۰ موسسه حسابرسی داخلی در کشورهای اتریش، بلژیک، فرانسه، آلمان، ایتالیا، لوکزامبورگ، هلند، اسپانیا، سوئد و انگلیس و ایرلند انجام گرفت.

برای اولین بار در سال جاری، این فرآیند شامل مصاحبه با روسای کمیته‌های حسابرسی برای ارائه دیدگاه گسترده‌تری در خصوص اینکه ریسک‌های کلیدی کسب و کار در کجا نهفته است. این گروه مصاحبه شامل ۴۲ نفر از مدیران ارشد حسابرسی و روسای کمیته حسابرسی (۲۹ مدیر ارشد حسابرسی و ۱۳ رئیس کمیته حسابرسی) بود. این نظرسنجی‌ها شامل ۵۷۹ پاسخ دهنده، با ده درصد افزایش سالانه، و همچنین بالاترین میزان پاسخگویی از زمان شروع این مطالعه تحقیقاتی از پنج سال پیش تاکنون می‌باشد.

همچنین برای اولین بار، امسال شامل سه دور مصاحبه با صاحب‌نظران این موضوع با استفاده از روش دلفی بود. این امر سبب ایجاد یک بعد جدید و بینش به‌روز، در مورد چگونگی ایجاد ریسک‌های کلیدی و چگونگی رسیدگی و بررسی حسابرسی داخلی در این حوزه‌ها شد. در مجموع ۵۱ متخصص شرکت کردند که تعداد متخصصان در هر حوزه ریسک از دو تا هفت نفر متفاوت بود.

این فرآیند تحقیق در فصل اول سال ۲۰۲۰ آغاز شد و در فصل دوم، اواسط گسترش ویروس در اروپا، تکمیل شد. زمان این تحقیقات بر چگونگی درک مدیران ارشد حسابرسی و روسای کمیته حسابرسی که با آن‌ها مصاحبه کرده‌ایم، از ریسک‌های کوتاه مدت و میان مدت کسب و کار آن‌ها، به ویژه با توجه به سلامت، ایمنی و نقدینگی مالی تاثیرگذار بوده است. علاوه، این زمان‌بندی احتمالاً روی امتیازدهی به ریسک‌های کلیدی توسط پاسخ دهنندگان نظرسنجی ما تأثیر گذاشته است، همانطوری که در صفحات بعدی، تجزیه و تحلیل نتایج کمی بیان شده است.

نتایج این رویکرد تحقیقاتی سه طبقه‌ای، برای ارائه مباحث انتخاب شده در این گزارش ترکیب شد. یک بار دیگر، ما بی نهایت از همه کسانی که در *Risk in Focus* امسال شرکت کردند، به ویژه در آن زمان چالش برانگیز و نامشخص، سپاسگزاریم.

۴۲



مدیران ارشد حسابرسی و
روسای کمیته حسابرسی
مصاحبه شده



۵۷۹

پاسخ دهندگان نظرسنجی
افزایش سالانه ۱۰ +

۵۱



متخصصان مصاحبه شده



موسسه حسابرسی آزمون پرداز

(حسابداران رسمی)



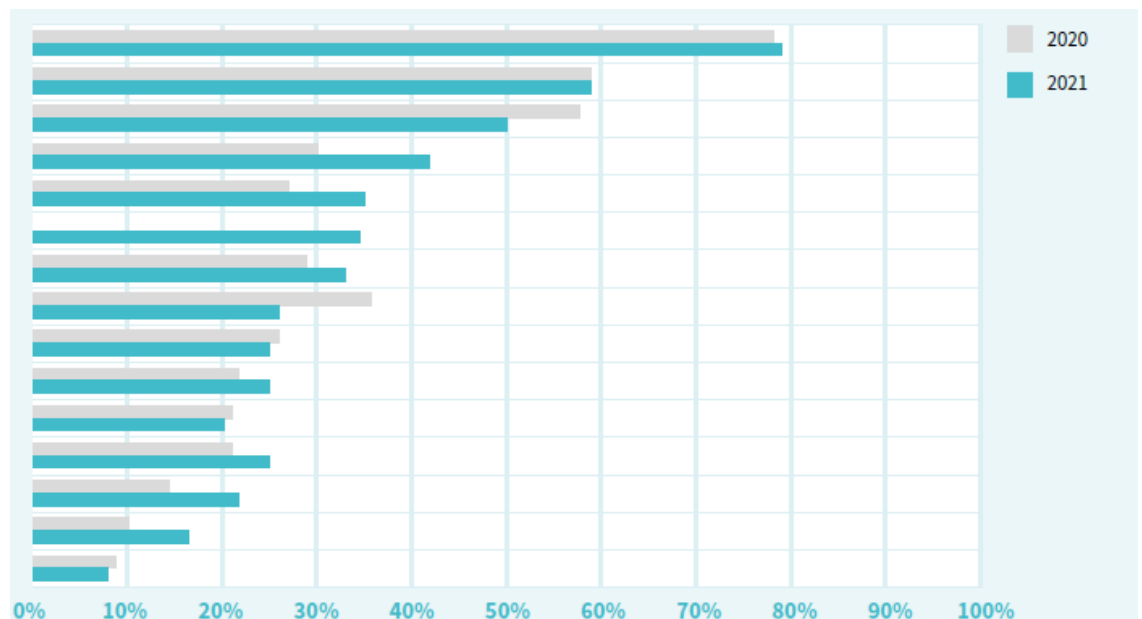
تجزیه داده ها: نتایج نظرسنجی

با مقایسه داده‌های نظرسنجی سال گذشته با داده‌های امسال، می‌توان فهمید که کدام ریسک‌ها از نظر مدیران ارشد حسابرسی داخلی در سراسر اروپا از اهمیت بیشتر یا کمتری برخوردار هستند. به نظر می‌رسد تعدادی از حوزه‌های ریسک تحت تأثیر اپیدمی ویروس کرونا قرار گرفته‌اند، از جمله سلامت و ایمنی، مالی، سرمایه و نقدینگی و سرمایه انسانی و مدیریت استعدادها، که هر سه مورد افزایش سالانه قابل توجهی را نشان داده‌اند. ریسک‌های زنجیره‌های تأمین، برون سپاری و حزب نهم به میزان قابل توجهی کاهش یافته است. یکی از دلایل این ممکن است این باشد که آنچه در آغاز سال ۲۰۲۰ به عنوان یک نگرانی از طرف عرضه آغاز شد، به زودی به یک مشکل تقاضا تبدیل شد، و با ورود جهان به رکود و بحران اقتصادی تأکید بر توانایی شرکت‌ها برای تداوم فعالیت و تسویه بدهی‌ها تداوم می‌یابد.

با این حال، تجدید فعالیت ویروس کرونا همچنان تهدیدی برای شرکت‌ها و تأمین‌کنندگان

۲۰۲۱ در مقابل سال ۲۰۲۰

پنج خطر اصلی که سازمان شما با آن روبرو است، چیست؟



در همین حال، تغییرات آب و هوایی و پایداری محیط زیست نسبت به نظرسنجی سال گذشته افزایش قابل توجهی نشان داده است و روند مثبتی در سال گذشته ادامه دارد. در نظرسنجی ابتدایی ما برای *Risk in Focus 2019*، فقط ۸٪ مدیران ارشد حسابرسی این مهم را در میان پنج ریسک اصلی اول مرتبط با کسب و کار خود می‌دانستند. این عدد در سال جاری به ۱۴ درصد، و هم‌اکنون به ۲۲ درصد رسیده است.

مباحث مربوط به تغییرات آب و هوایی و پایداری بخشی از بحث عمومی برای سال‌های متعددی بوده است، و بطور پیوسته، اگر نه به سرعت، به مناطق تمرکز استراتژیک عملیاتی و کاهش ریسک برای شرکت‌ها تبدیل می‌شود.

مباحث مربوط به تغییرات اقلیمی و پایداری بخشی از بحث عمومی بوده است و بطور پیوسته، اگر نه به سرعت، به حوزه‌های تمرکز استراتژیک عملیاتی و کاهش ریسک برای شرکت‌ها تبدیل می‌شود.

آن‌ها محسوب می‌شود و نباید فراموش کرد که ریسک‌های مالی و نقدینگی که با یک بازار پایین افزایش می‌یابد، برای تأمین‌کنندگان اصلی نیز اعمال می‌شود. کسب و کارها و حسابرسی داخلی باید به توانایی پرداخت بدهی‌های تأمین‌کنندگان اصلی و شرکای برون سپاری و توانایی مداوم در تهیه سطح مناسب موجودی کالا متناسب با تقاضا توجه داشته باشند.

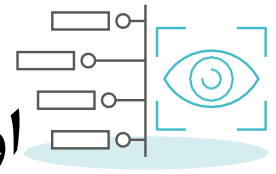
این جدیدترین نسخه از این مطالعه، برای اولین بار شامل حوادث و واکنش در برابر بحران‌ها می‌باشد، که ۳۴ درصد از مدیران ارشد حسابرسی از آن‌ها به عنوان پنج ریسک اول خود نام برده‌اند. این پنج ریسک، درست قبل از سرمایه‌انسانی و مدیریت استعداد قرار دارند. حسابرسی پاسخ کسب‌وکارها به اپیدمی ویروس کرونا به وضوح از اولویت برخوردار است.

در ماه‌های اخیر و بیشتر، اگر نه همه، سازمان‌ها باید تمرین‌های آموخته شده را انجام دهند و پروتکل‌های تداوم بحران خود را به روز کنند.



"با تغییرات اقلیمی به طور فزاینده ای برای سرانجام کسب و کار مورد توجه قرار می گیرد، به ویژه هنگامی که بزرگترین سرمایه گذاران جهان خواستار اقدام فوری هستند ، توجه قابل توجهی از خط سوم در مورد این حوزه ریسک وجود ندارد."





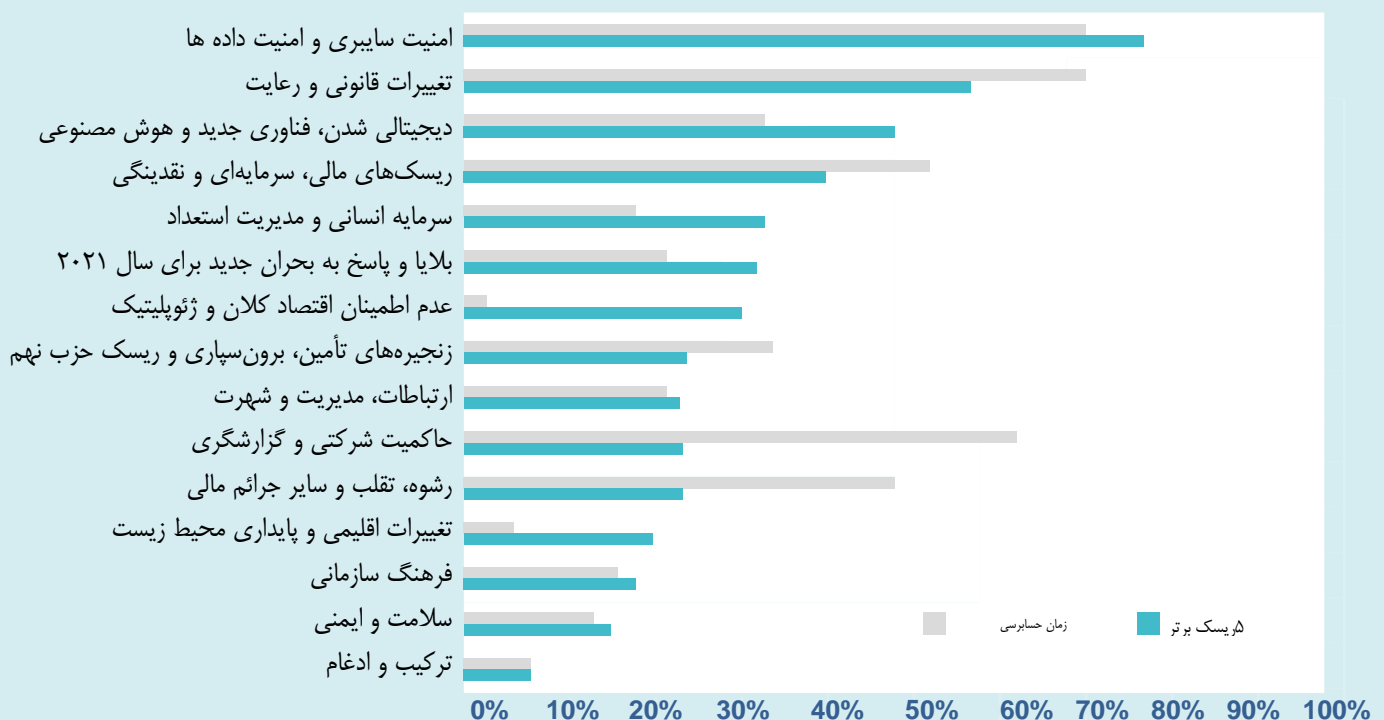
اولویت ریسک در برابر تمرکز حسابرسی

با این حال، این نتایج دلیلی برای تأمل و گفتگو با هیئت مدیره یا کمیته حسابرسی، در مورد اینکه آیا زمان و منابع حسابرسی داخلی هوشمندانه صرف می‌شود و آیا در صورت نیاز به تخصیص، تخصیص مجدد در حوزه‌های ریسک نادیده گرفته شده وجود دارد، است.

با تغییر شرایط اقلیمی که به یک موضوع فزاینده برای کسب و کار تبدیل می‌شود تا در نهایت به آن پردازند؛ به ویژه هنگامی که بزرگترین سرمایه‌گذاران جهان خواستار اقدام فوری هستند، فقدان توجه قابل ملاحظه‌ای از خط سوم در این حوزه ریسک وجود دارد. عدم اطمینان اقتصاد کلان و ژئوپلیتیک و دیجیتالی شدن، فناوری جدید و هوش مصنوعی نیز در مقایسه با سطح اولویت ریسک خود، حداقل حسابرسی را مورد توجه قرار می‌دهند. اگر این مسئله در سازمان شما صادق است، آیا توجهی وجود دارد که چرا این حوزه‌ها، حوزه‌های تمرکز خط سوم نیستند؟

با پرسش از مدیران ارشد حسابرسی در مورد این که، آن‌ها در حال حاضر چه چیزهایی را به عنوان بزرگترین ریسک‌ها برای سازمان خود می‌بینند و بیشترین وقت و تلاش حسابرسی را برای چه حوزه‌های ریسکی صرف می‌کنند، ما تصویری از چگونگی همسویی و هم‌ترازی خط سوم اطمینان‌بخشی ایجاد می‌کنیم. هرگونه عدم تطابق لزوماً به این معنی نیست که حسابرسی داخلی رویکردی کاملاً مبتنی بر ریسک اتخاذ نمی‌کند. به عنوان مثال، در شرکت‌های تحت نظارت، حسابرسی داخلی موظف است منابع خود را به وظایف حسابرسی رعایت اختصاص دهد، حتی اگر ریسک‌های مربوط به رعایت را بزرگ‌ترین تهدیدهای جهانی برای سازمان نبیند. همچنین، مناطقی که بیشتر با حسابرسی سروکار دارند، ممکن است از اولویت ریسک کمتری در نتیجه تلاش‌های حسابرسی داخلی برای کاهش ریسک برخوردار باشند، یعنی خط سوم تأثیر مطلوب خود را دارد.

پنج ریسک اصلی که سازمان شما در حال حاضر با آن روبرو است در مقابل پنج ریسک برتر که در حال حاضر حسابرسی داخلی بیشترین وقت و تلاش را روی آن‌ها می‌گذارد.





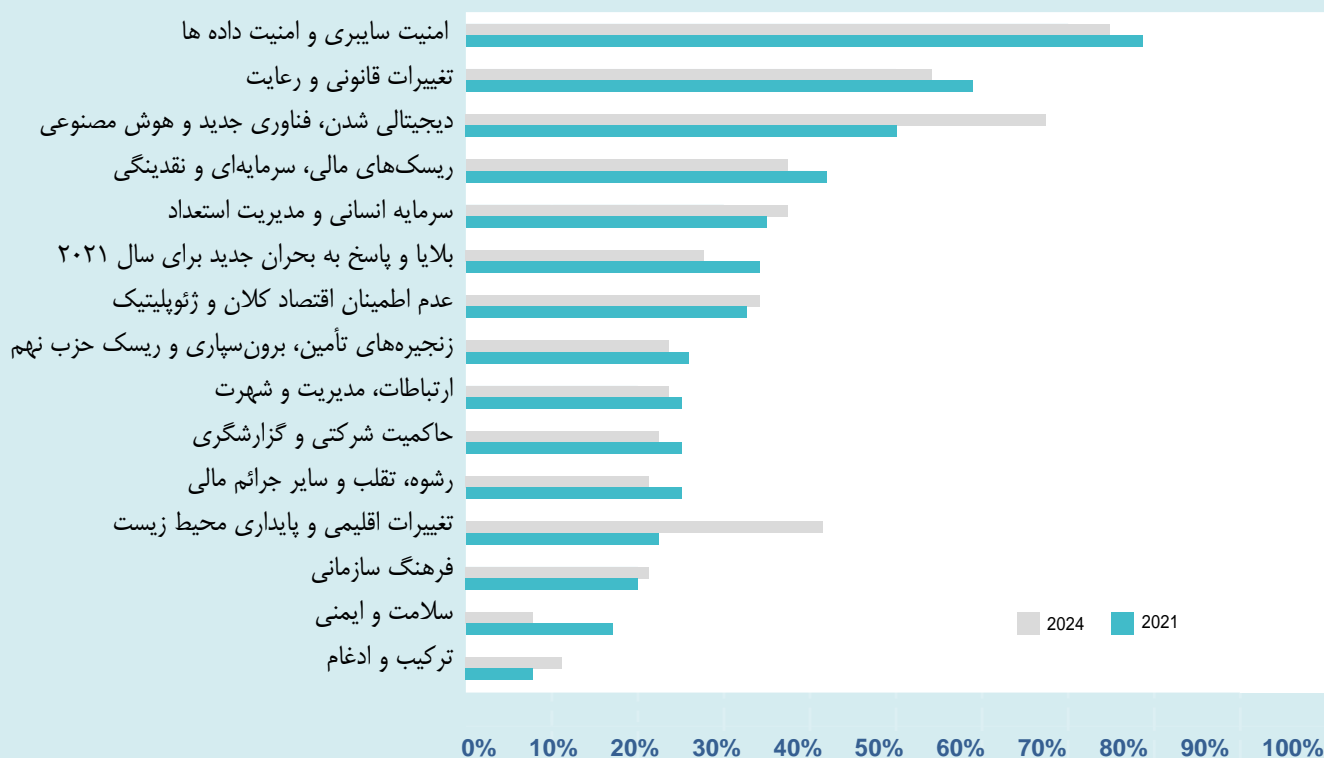
ریسک‌های امروز و فردا

فناوری و نوآوری ذاتاً با پایداری ارتباط دارد. کاربرد سخت افزارها و نرم افزارهای پیشرفته به کاهش تأثیرات تغییرات آب و هوایی و بهبود پایداری کمک می‌کند. شرکت‌ها به ایجاد نوآوری در محصولات اصلی خود و تحت کنترل قرار دادن فناوری‌های جدید و نوظهور مانند ذخیره سازی طولانی مدت باتری و اندازه‌گیری هوشمند پیشرفته برای به حداقل رساندن انتشار گازهای گلخانه‌ای و همچنین تجزیه و تحلیل داده‌های بزرگ برای کشف شکاف‌های بهره‌وری عملیاتی دارند که می‌تواند بهبود یابد، در میان رویکردهای بشماروی دیگر برای دستیابی به اهداف پایدار بلند پروازانه خود استفاده شود، نیاز دارند...

علاوه بر این که از مدیران ارشد حسابرسی داخلی پرسیدیم که بزرگترین ریسک‌های سازمان شما چیست، پرسیدیم که آن‌چه آن‌ها انتظار دارند بزرگترین ریسک سازمان در مدت سه سال آتی باشد، کدامند؟ این نشان می‌دهد که چگونه رهبران حسابرسی پروفایل ریسک سازمان‌های خود را که در طول زمان در حال ایجاد است، پیش بینی می‌کنند. به طور برجسته مشهود است که انتظار می‌رود در آینده نزدیک هر سه مورد دیجیتال سازی، فناوری جدید و هوش مصنوعی و تغییرات آب و هوایی و پایداری محیط زیست به طور قابل توجهی در اولویت خود افزایش دهند.

“به طور برجسته مشهود است که انتظار می‌رود در آینده نزدیک هر سه مورد دیجیتال سازی، فناوری جدید و هوش مصنوعی و تغییرات آب و هوایی و پایداری محیط زیست به طور قابل توجهی در اولویت خود افزایش دهند.”

پنج خطر اصلی که سازمان شما در حال حاضر با آن روبرو است در مقابل خطراتی که فکر می‌کنید سازمان شما ظرف سه سال آتی با آن روبرو خواهد شد.





تمرکز حسابرسی در طول زمان

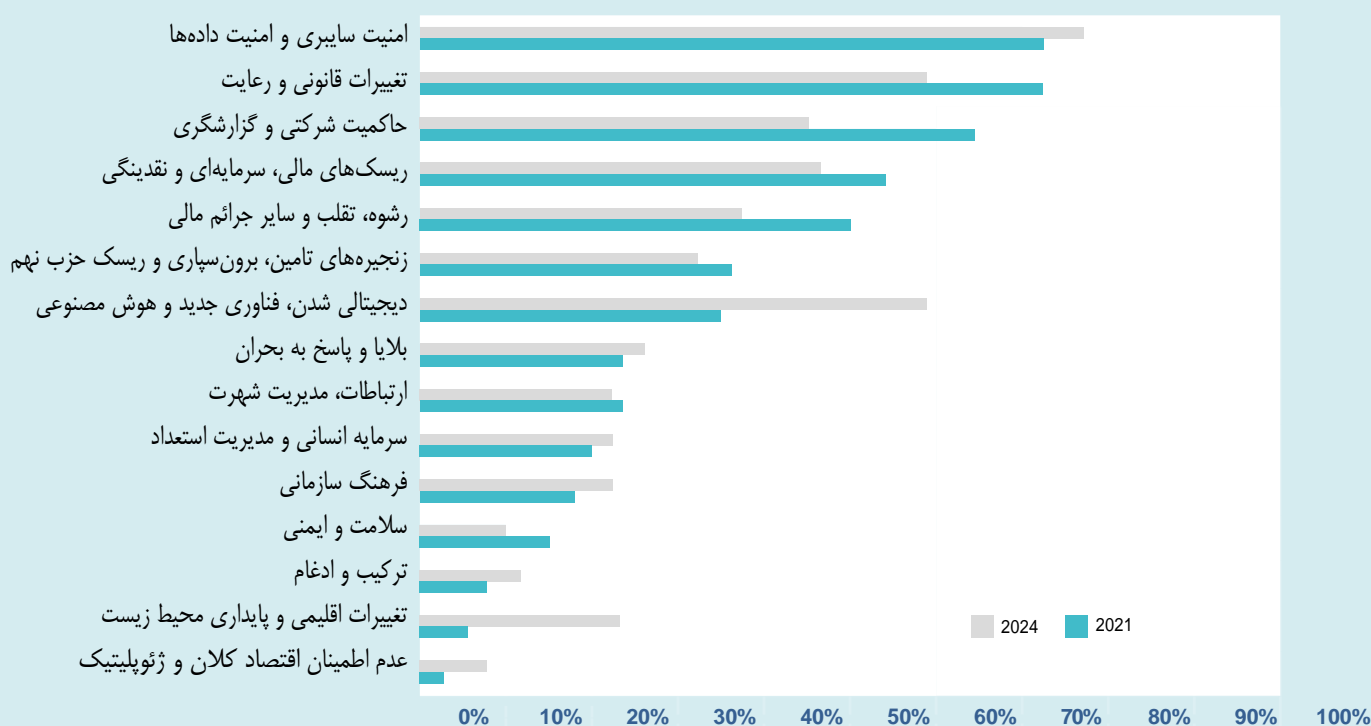
در مقابل، در حالی که انتظار می‌رود در آینده نزدیک حسابرسی داخلی به حوزه‌های نظارتی (شامل حاکمیت شرکتی و گزارش‌گری، رشوه، تقلب و سایر جرایم مالی و تغییرات قانونی و رعایت) توجه کمتری نماید، پیش‌بینی می‌شود زمان و تلاش صرف شده برای این ریسک‌ها طی سه سال به میزان قابل توجهی از اولویت آن ریسک فراتر رود. این ممکن است ارتباط سازنده‌ای را با کمیته حسابرسی در مورد چگونگی تأمین منابع خط سوم طی سال‌های آینده، و اینکه آیا باید توجه را از مناطق دارای ریسک کنترل شده دور کرد تا خط سوم بتواند رویکرد مبتنی بر ریسک موثرتری را بپذیرد، بطلبد.

در این رابطه، با چندین مسابقه یکسان، هماهنگی و هم‌ترازی زیادی وجود دارد. این را می‌توان با خوش‌بینی در بین مدیران حسابرسی توضیح داد که منابع حسابرسی داخلی به بیشتر موارد مورد نیاز تخصیص یافته و هدایت می‌شوند. عدم تناسب قابل ملاحظه‌ای شامل دیجیتالی شدن، فناوری جدید و هوش مصنوعی مشاهده می‌شود، در حالی که ۶۷٪ می‌گویند پنج خطر اصلی خواهد بود اما تنها ۵۹٪ پیش‌بینی می‌کنند که یک حوزه حسابرسی دارای اولویت باشد. این ممکن است حاکی از آن باشد که حسابرسی داخلی باید مهارت‌های خود را بهبود ببخشد، روش‌های خود را نوآوری کند و تخصص بیشتری کسب کند تا با موفقیت این حوزه خطر را در آینده مورد توجه و تمرکز قرار دهد.

همچنین می‌توانیم ببینیم که زمان و تلاش‌های حسابرسی داخلی به مرور زمان در کجا سپری و هدایت می‌شود. آنجایی که مدیریت ریسک در حوزه‌هایی مانند حاکمیت شرکتی و گزارش‌گری، و تغییرات قانونی و رعایت به بلوغ می‌رسد، نشانه‌های پدیدار می‌شود که حسابرسی داخلی بیشتر بر روی حوزه‌های کمتر سنتی مانند عدم اطمینان اقتصاد کلان و ژئوپلیتیک، تغییرات اقلیمی و پایداری محیط زیست، دیجیتالی شدن، فناوری جدید و هوش مصنوعی و سرمایه انسانی و مدیریت استعداد تمرکز خواهد کرد.

ما همچنین می‌توانیم این مورد را با آنچه مدیران ارشد حسابرسی اولویت‌های ریسک کسب و کار در سه سال آینده می‌دانند، مقایسه کنیم.

پنج حوزه ریسک برتر که در حال حاضر حسابرسی داخلی بیشترین وقت و تلاش خود را در آن‌ها صرف می‌کند در مقابل پنج حوزه ریسکی برتر که فکر می‌کنید حسابرسی داخلی در سه سال آتی بیشترین وقت و تلاش را صرف آن‌ها خواهد کرد.



“تهدید امنیت سایبری به ضعیف‌ترین حلقه سازمان بستگی دارد و ضعیف‌ترین پیوندها همیشه مردم هستند. تا زمانی که در محیط امن سازمان خود کار می‌کنید، می‌دانید که افراد امنیتی می‌توانند با شرایط کنار بیایند و احتمالاً نزدیک به ۱۰۰٪ امنیت دارند. با دورکاری همه در خانه، اوضاع کاملاً متفاوت است. بنابراین چگونه می‌توانیم از یک طرف دیوار آتش را باز کنیم تا افراد بتوانند از راه دور کار کنند، اما از طرف دیگر مطمئن باشید که هرکدام از شرایط فعلی سو استفاده نمی‌کنند؟ این یک چالش است.”

رئیس کمیته حسابرسی، دولت محلی فلاندر، بلژیک



امنیت سایبری و امنیت داده در نظرسنجی
امسال در رتبه اول قرار گرفت، ۷۹٪ مدیران ارشد حسابرسی گفتند که این مورد جزء پنج ریسک اصلی است.

در سراسر جهان

بیش از ۴,۵ میلیارد

مردم در اوج اولین موج همه‌گیری در اروپا تحت اقدامات فاصله اجتماعی زندگی می‌کردند.

* تخمین زده

Source: BBC

“ارتباطات دیجیتال و توانایی هدایت شرکت از راه دور با استفاده از ابزارهای دیجیتال افزایش می‌یابد. تبادل اطلاعات در مواقع بحران و محیط جدید و قابلیت اطمینان این رسانه‌ها برای برقراری ارتباط، یکی از ریسک‌های اصلی و عمده خواهد بود.

یکی از دروس اصلی این خواهد بود که در صورت بروز یک فاجعه چگونه می‌توانیم ارتباطات موثر و ایمن را حفظ کنیم؟ آن کانال‌های ارتباطی چقدر پایدار هستند؟ اگر اینترنت خراب باشد،

چه کاری انجام می‌دهیم؟

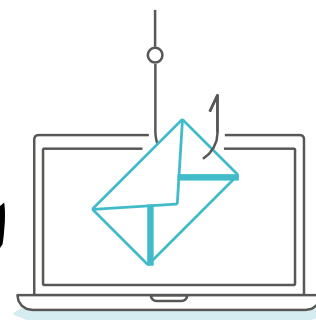
از واکی تاکی استفاده می‌کنید؟”

مدیر حسابرسی داخلی، شرکت مواد شیمیایی DAX، آلمان



موسسه حسابرسی آزمون پرداز

(حسابداران رسمی)



امنیت اطلاعات در محیط کار گسترش یافته

داده‌ها و اطلاعات - اعم از اعتبار مشتری یا مالکیت معنوی - سرمایه اقتصادی هستند که همه سازمان‌ها به آن‌ها وابسته هستند. تا زمانی که چنین تغییراتی رخ دهد، امنیت داده یکی از مهمترین اولویت‌ها در دستور کار شرکت‌ها خواهد بود. یک بار دیگر، امنیت سایبری و امنیت داده‌ها در نظرسنجی امسال در رتبه اول قرار گرفتند، با گفته ۷۹٪ مدیران ارشد حسابرسی، ریسک امنیت سایبری و امنیت داده‌ها از پنج ریسک اصلی است و ۲۷٪ آن را به عنوان ریسک شماره یک سازمان خود انتخاب می‌کنند.

همه ابزارهای ارتباط دیجیتال، نه فقط ایمیل، همچنین باید پایدار و از نظر عملیاتی مقاوم باشند و همچنین از دخالت خارجی و جاسوسی احتمالی توسط مجرمان اینترنتی، رقبا و دولت‌های ملی ایمن باشند. موارد متعددی از نفوذ سرکش در سیستم عامل‌های نرم افزار کنفرانس ویدیویی وجود داشته است که با شروع قرنطینه، وسیله اصلی ارتباطات شد. نگرانی دیگر یکپارچگی سیستم‌عامل‌های خاص است. آژانس‌های اطلاعاتی به دولت‌ها هشدار داده‌اند که از استفاده از بزرگ‌نمایی (زوم) به دلیل نگرانی در برابر آسیب‌پذیری این بخش از نظارت دولت پنهانی، که بخش تحقیقات این شرکت در چین مستقر است، خودداری کنند.

داده بسیار مهم و حیاتی است. فاقد تعامل شخصی، کارکنان می‌توانند بیشتر در معرض ترفندهای مهندسی اجتماعی قرار بگیرند، زیرا آن‌ها نمی‌توانند بلافاصله ایمیل‌های خود را با همکاران اطراف بررسی کنند. در فقدان تعامل شخصی، کارکنان می‌توانند بیشتر در معرض ترفندهای مهندسی اجتماعی قرار بگیرند، زیرا آن‌ها نمی‌توانند بلافاصله ایمیل‌های خود را با همکاران اطراف بررسی کنند. همچنین زمانی که کارگران تحت مراقبت قرار نمی‌گیرند، ظرفیت بیشتری برای دور زدن یا تعدیل اقدامات کنترلی و ایمنی وجود دارد، زیرا این کنترل‌ها برای صرفه‌جویی در وقت نادیده گرفته می‌شوند و از آن‌ها چشم‌پوشی می‌شود. یک گزارش نشان می‌دهد که ۵۲٪ از کارمندان ادارات معتقدند که می‌توانند هنگام کار در خانه با رفتارهای پرریسک‌تر، مانند به اشتراک‌گذاری پرونده‌های محرمانه از طریق ایمیل و استفاده از وسایل شخصی برای انجام کارهای شرکت، کنار بیایند. دلایل عدم پیروی از کنترل‌های امنیتی عبارتند از احساس اینکه این پروتکل‌ها مانع بهره‌وری (۵۱٪) هستند و تحت نظارت بخش‌های IT قرار نگرفته‌اند (۴۸٪).^۵

قوانین بازی اما تغییر کرده است. تغییر مقیاس گسترده به ترتیب اجرای کارها در منزل در زمان سریع در هنگام قرنطینه، آسیب‌پذیری سازمان‌ها را در برابر حملات سایبری افزایش داد. تخمین زده می‌شود که در اوج اولین موج همه‌گیری در اروپا، در سراسر جهان حداقل ۴٫۵ میلیارد نفر - بیش از نیمی از جمعیت جهان - تحت اقدامات فاصله‌گذاری اجتماعی زندگی می‌کردند.^۴ کارگران مجبور بودند از طریق دستگاه‌های شخصی یا کانال‌های باز و رو به اینترنت به زیرساخت‌ها و داده‌های مهم دسترسی پیدا کنند. طی یک شبانه روز، لپ‌تاپ‌های کار مجبور شدند شبکه‌های WiFi خانگی را به طور دسته جمعی به اشتراک بگذارند، و باعث می‌شود سطح حمله شرکت‌ها با وضوح کمتری مشخص و نفوذپذیرتر شود. تعداد اندکی از برنامه‌های تداوم تجارت (BCP) چنین آشفتگی گسترده‌ای را در چنین مدت کوتاهی رقم زده است. مراکز عملیات امنیتی شرکت‌ها (SOC) که برای نظارت و تجزیه و تحلیل فعالیت‌های غیرمعمول احتمالی در شبکه‌ها، سرورها و پایگاه‌های داده در شرایط عادی ایجاد شده‌اند، با شناسایی داده‌های خارج از محدوده در یک محیط اصلاح شده فناوری اطلاعات، دچار اختلال می‌شوند.

توابع و کارکردهای امنیت اطلاعات برای اطمینان از کاهش ریسک‌های دسترسی از راه دور به داده‌های حساس با ایمن‌سازی دستگاه‌های دورکاری در خانه با به روزرسانی پیچ، حفظ تقسیم‌بندی شبکه و مدیریت حقوق دسترسی برای اطمینان از سطح قابل قبولی از امنیت لازم است. عنصر رفتاری انسان برای ریسک سایبر و امنیت

⁵ The State of Data Loss Prevention 2020 | Tessian

⁴ coronavirus pandemic: Tracking the global outbreak | BBC

انتظار نمی‌رود تنظیم محیط کار در خانه موقتی باشد. شرکت‌هایی که بهره‌وری خود را از طریق قرنطینه حفظ کرده‌اند و کارکنان آن‌ها با موفقیت خود را با کار از راه دور تطبیق داده‌اند، ممکن است فضای اداری را به طور دائمی دور بیندازند، به ویژه هنگامی که درآمد تحت فشار قرار می‌گیرد و مشاغل به دنبال راه‌هایی برای کاهش پایه هزینه ثابت خود هستند.

یک تخمین نشان می‌دهد که ۷۴٪ شرکت‌ها قصد دارند بعد از اپیدمی ویروس کرونا بیش‌تر از راه دور کار کنند.^۶ این امر به شرکت‌هایی نیاز دارد تا ضمن حفظ بالاترین استانداردهای امنیت اطلاعات، هم در محل کار و هم در محیط کار مستقر در خانه، انعطاف‌پذیر و سازگار شوند.

گروهی از متخصصان مورد بررسی برای *Risk in Focus* چندین تهدید سایبری را به ترتیب احتمال رتبه بندی کرده‌اند. تلاش‌های فیشینگ و بدافزارهای مخرب به عنوان محتمل‌ترین تهدیدهای ایجاد شده دیده می‌شوند که نشان دهنده اهمیت رفتار، آموزش و آگاهی کارکنان در کاهش خطر سایبری است.

تهدید سایبری	به احتمال زیاد در سال آینده با آن روبرو خواهیم شد (ترتیب اهمیت: از بیشتر به احتمال کمتر)	چالش برای سازمان‌ها
فیشینگ یا تله گذاری		کاهش بازه زمانی بین رویدادهای امنیتی و پاسخ‌ها
آلودگی به بدافزار		
ورود به شبکه شرکت		
حملات DoS / DDoS		
نقض امنیت اطلاعات		
فعالیت های جاسوسی سایبری / نرم افزارهای جاسوسی		
آسیب پذیری های نرم افزار		
استخراج اطلاعات و اطلاعات		

دیدگاه حسابرسی داخلی

حسابرسی داخلی می‌تواند نظر خود را در مورد حدی از هرگونه کاهش یا تطبیق با کنترل‌ها و پذیرش آن‌ها که احتمال نشت داده‌ها یا نقض امنیت را افزایش دهد، پیشنهاد نماید. سوال واقعی این است - چه چیزی تغییر کرده است؟ این امر به طور خارجی (به عنوان مثال افزایش در تلاش‌های فیشینگ) و به طور داخلی اعمال می‌شود (به عنوان مثال کمبود آموزش کارکنان در زمینه آگاهی سایبری پس از بحران یا وصله‌های امنیتی دستگاه‌های دورکاری که به اندازه موثر مدیریت نمی‌شوند). حسابرسی داخلی با درک اینکه کجا بیشترین اختلال قرار دارد و کجا بیشترین ارزش دارایی‌های داده بارگذاری شده است می‌تواند تأثیر هرگونه تغییر بر ریسک امنیت اطلاعات سازمان و محیط کنترل موجود برای کاهش آن را تعیین کند.

آگاهی و درک کارکنان از خطر امنیت اطلاعات کاملاً ضروری است. این امر در مورد پروتکل‌های مربوط به استفاده، مدیریت و ذخیره‌سازی داده‌های محرمانه برای جلوگیری از نشت داده‌ها اعمال می‌شود و برای اطمینان از اینکه کارگران می‌دانند چگونه جرایم سایبری را تشخیص دهند تا از تسلیم شدن در معرض فیشینگ و فیشینگ نیزه (هدف یک فرد خاص) و تلاش‌هایی که می‌تواند منجر به حملات مخرب گران بدافزار و باج افزار و کلاهبرداری با فریب شود، جلوگیری کنند. حسابرسی داخلی می‌تواند و باید بررسی کند که آیا آگاهی از امنیت سایبری به اندازه کافی تقویت شده است و آیا آموزش کارکنان با توجه به تغییر در محیط کار و زیرساخت‌های فناوری اطلاعات به روز شده است. همچنین باید تلاش شود تا اطمینان حاصل شود که کارکنان برای صرفه جویی در وقت و تلاش فرایندهایی را دور نمی‌زنند.

حسابرسی داخلی همچنین می‌تواند یک برد صدا^۷ برای تیم‌های امنیت اطلاعات باشد که ممکن است مجبور شوند محیط کنترل فناوری اطلاعات را برای عملیاتی کردن کار و کارایی و بهره‌وری هر چه بیشتر کسب و کار در برابر حوادث شوک وفق دهند. ضروری است هرگونه تغییر کنترل پریسک به مدیران ارشد گزارش شود تا بررسی کند که آیا آن‌ها در اشتباهی ریسک سایبری سازمان قرار دارند یا خیر.

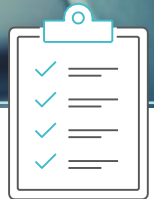
^۱ CFO Actions in Response to COVID-19 | Gartner

^۷ a sounding board شخص یا گروهی که یکی با آن‌ها در مورد ایده، برنامه یا پیشنهادی بحث می‌کند تا نقاط قوت، مقبولیت، امکان سنجی، عملی بودن و غیره را ارزیابی کند.



"گروهی از متخصصان مورد بررسی برای *Risk in Focus* چندین تهدید سایبری را به ترتیب احتمال رتبه بندی کرده اند. تلاش‌های فیشینگ و بدافزارهای مخرب به عنوان محتمل‌ترین تهدیدهای ایجاد شده دیده می‌شوند، که نشان دهنده اهمیت رفتار، آموزش و آگاهی کارکنان در کاهش خطر سایبری است."

سوالات و ملاحظات برای حسابرسی داخلی



- آیا برنامه‌های نرم افزاری جدید (به عنوان مثال نرم افزار کنفرانس ویدئویی) برای اطمینان از این که تداوم عملکرد برای نقص و آسیب-پذیری‌های احتمالی امنیتی به طور مناسب و به اندازه کافی بررسی شده‌اند، به تصویب می‌رسند؟
- آیا آگاهی کارکنان آزمایش خط اول یا دوم با تلاش‌های فیشینگ دوستانه وجود دارد؟
- آیا حسابرسی داخلی باید دفاعیه‌های فناوری اطلاعات را به طور مستقل شاید با کمک هم‌سپاری یک شریک آزمایش کند؟

- آیا وصله‌های امنیتی دستگاه‌های شخصی با همان استاندارد دستگاه‌های پیش فرض به روز می‌شوند و مدیریت می‌شوند؟
- چگونه توانایی نظارت بر مرکز عملیات امنیتی شرکت در ۱۲ ماه گذشته با مانع رو به رو شده یا مختل شده است؟
- آیا خط اول به طور واقعی محیط کسب و کار را درک می‌کند؟
- به عنوان مثال، آیا کاملاً تمام دستگاه‌های دارای اتصال و دسترسی به شبکه (به عنوان مثال دستگاه‌های اینترنت اشیا) ایمن هستند؟

- محیط کار تازه گسترش یافته چه تاثیری بر سیستم کنترل فناوری اطلاعات در بخش‌های مختلف کسب و کار داشته است و این امر چه ریسک‌هایی در بر دارد؟
- آیا شرکت برای ارزیابی نقاط ضعف احتمالی شبکه و دارایی‌های داده که حساسیت آن‌ها در برابر حملات و سرقت در ۱۲ ماه گذشته افزایش یافته، ارزیابی ریسک انجام داده است؟
- آیا خط اول باعث افزایش آگاهی کارکنان در مورد تهدیدهای اصلی سایبری شده و به آن‌ها می‌گوید که باید به دنبال چه چیزی باشند؟





موسسه حسابرسی آزمون پرداز

(حسابداران رسمی)

اعضای جامعه حسابداران رسمی ایران

کارشناسان رسمی دادگستری در رشته حسابداری و حسابرسی

حسابداران خبره رسمی انگلستان (ACCA)

مدیران ریسک مالی (FRM)

کارفرمای مورد تایید انجمن حسابداران خبره رسمی انگلستان (ACCA) در بالاترین سطح (Platinum)



حسابرسان رتبه ۱ معتمد سازمان بورس و اوراق بهادار

موسسه حسابرسی رتبه «الف» کنترل کیفیت از جامعه حسابداران رسمی ایران

دفتر مرکزی:

تهران، خیابان بخارست (احمد قصیر)، خیابان ششم، شماره ۳۶، واحد ۴، کدپستی:

۱۵۱۴۴۳۵۱۵

تلفن: ۲-۸۸۵۴۴۵۹۰

فاکس: ۸۸۵۰۳۵۲۸

دفتر اصفهان:

اصفهان، چهارراه فلسطین، ساختمان حافظ، طبقه ۴، واحدهای ۱۹ و ۲۰

کدپستی: ۸۱۴۳۹۹۵۹۵۱

تلفن: ۲-۸۸۵۴۴۵۹۰

فاکس: ۸۸۵۰۳۵۲۸

همکاران در این ترجمه:

فاطمه مهدی - مدیر حسابرسی داخلی

خلاصه سوابق

فاطمه مهدی، مدیر حسابرسی داخلی است. او در مقطع تحصیلی کارشناسی ارشد رشته حسابداری از دانشگاه آزاد اسلامی واحد تهران شمال فارغ التحصیل شده است. وی حسابدار رسمی عضو جامعه حسابداران رسمی ایران و دارای بیش از ۱۴ سال تجربه حرفه‌ای در زمینه حسابداری، حسابرسی و بازار سرمایه شامل ارزیابی کنترل‌های داخلی، طراحی سیستم، تهیه صورت‌های مالی تلفیقی و انواع گزارشات تحلیلی و مدیریتی است. وی کتاب‌های متعددی در زمینه حسابداری و حسابرسی تألیف و اقتباس نموده که مهم‌ترین آن کاربرد الگوی بکر در حسابرسی داخلی (ارزیابی کنترل‌های داخلی بر اساس مدل ترکیبی بلوغ، کوزو و ریسک) است که بر اساس تجربه اجرایی حسابرسی داخلی در گروه مپنا و شرکت‌های زیرمجموعه آن تدوین شده است.



تلفن: ۲- ۹۸ ۲۱ ۸۸۵۴۴۵۹۰

فکس: ۹۸ ۲۱ ۸۸۵۰۳۵۲۸

موبایل: ۹۸ ۹۱۲ ۲۷۷ ۴۹۷۶

ایمیل: fatemeh.mahdi@azpar.com

امیررضا پورآقاچان - حسابرس داخلی

خلاصه سوابق

امیررضا پورآقاچان، حسابرس داخلی است. او در مقطع تحصیلی کارشناسی رشته حسابداری از دانشگاه مازندران فارغ التحصیل شده است. وی دارای چهار سال سابقه کار حرفه‌ای بوده و هم اکنون در مقطع کارشناسی ارشد دانشگاه علامه طباطبائی در حال تحصیل است.



تلفن: ۲- ۹۸ ۲۱ ۸۸۵۴۴۵۹۰

فکس: ۹۸ ۲۱ ۸۸۵۰۳۵۲۸



موسسه حسابرسی آزمون پروداز

(حسابداران رسمی)