فصلنامه چشم انداز حسابداری و مدیریت
دوره ۹، شماره ۱۱۸، پاییز ۱۴۰۵ (جلد اول)

www.jamv.ir
ISSN: 2645-4572

عوامل حرفه‌ای و حاکمیتی مؤثر بر اثربخشی حسابرسی سایبری؛ نقش شایستگی حسابرسان، شایستگی و حمایت هیئت‌مدیره و همکاری با خطوط دفاعی

پریناز اسکندری
دانشجوی دکتری حسابداری، دانشگاه الزهرا، تهران، ایران. (نویسنده مسئول).
parinazskandary9697@gmail.com
غلامرضا سلیمانی امیری
استاد تمام گروه حسابداری، دانشگاه الزهرا، تهران، ایران.
gh.soleymani@alzahra.ac.ir

چشم انداز حسابداری و مدیریت (دوره نهم)
شماره ۱۱۸/ پاییز ۱۴۰۵ (جلد اول)/ صص ۶۶-۸۵

چکیده

هدف پژوهش حاضر بررسی اثر شایستگی حسابرسان سایبری، شایستگی هیئت‌مدیره، حمایت هیئت‌مدیره و همکاری با خطوط دفاعی بر اثربخشی حسابرسی سایبری است. داده‌های پژوهش از ۱۵۳ پاسخ کامل به پرسشنامه‌ای ۴۰ گویه‌ای با طیف پنج‌درجه‌ای لیکرت گردآوری و با استفاده از مدل‌سازی معادلات ساختاری مبتنی بر حداقل مربعات جزئی (PLS-SEM) تحلیل شد. در ارزیابی مدل اندازه‌گیری، بارهای عاملی، آلفای کرونباخ، پایایی ترکیبی، روایی همگرا و روایی واگرا بررسی شد و در مدل ساختاری نیز هم‌خطی، قدرت تبیین، قدرت پیش‌بینی، اندازه اثر و آزمون بوت‌استرپ با ۵۰۰۰ بازنمونه ارزیابی گردید. آلفای کرونباخ سازه‌ها بین ۰٫۸۵۱ تا ۰٫۹۲۱، پایایی ترکیبی بین ۰٫۸۹۰ تا ۰٫۹۳۲ و میانگین واریانس استخراج‌شده بین ۰٫۵۱۶ تا ۰٫۶۱۵ بود و بیشترین مقدار HTMT برابر ۰٫۶۰۴ به دست آمد. نتایج مدل ساختاری نشان داد شایستگی حسابرسان سایبری، حمایت هیئت‌مدیره و همکاری با خطوط دفاعی اثر مثبت و معناداری بر اثربخشی حسابرسی سایبری دارند، در حالی که اثر مستقیم شایستگی هیئت‌مدیره معنادار نبود. مقدار R^2 برابر ۰٫۳۵۷ و Q^2 برابر ۰٫۳۲۶ به دست آمد. یافته‌ها نشان می‌دهد اثربخشی حسابرسی سایبری بیش از اتکای صرف بر دانش هیئت‌مدیره، به شایستگی حرفه‌ای حسابرسان، حمایت عملی ارکان حاکمیتی و همکاری میان خطوط دفاعی وابسته است.

واژگان کلیدی: حسابرسی سایبری، شایستگی حسابرسان، هیئت‌مدیره، حمایت هیئت‌مدیره، خطوط دفاعی.

مقدمه

تحول دیجیتال، گسترش رایانش ابری، استفاده فزاینده از هوش مصنوعی و افزایش وابستگی زنجیره‌های تأمین به زیرساخت‌های دیجیتال، وابستگی سازمان‌ها به دارایی‌ها و فرایندهای فناورانه را به‌طور قابل توجهی افزایش داده است (مجمع جهانی اقتصاد، ۲۰۲۵). در نتیجه، ریسک‌های سایبری دیگر صرفاً در محدوده واحد فناوری اطلاعات قرار نمی‌گیرند و به موضوعی مرتبط با مدیریت ریسک، حاکمیت سازمانی و پاسخگویی مدیران تبدیل شده‌اند (مؤسسه ملی استانداردها و

www.jamv.ir
ISSN: 2645-4572

فناوری آمریکا، ۲۰۲۴). رخدادهای سایبری می‌توانند علاوه بر ایجاد اختلال عملیاتی و هزینه‌های بازیابی، پیامدهایی برای اعتبار و ارزش اقتصادی سازمان داشته باشند (گاتزرت و شوبرت، ۲۰۲۲؛ فلوراکیس و همکاران، ۲۰۲۳). همچنین، وابستگی متقابل سازمان‌ها موجب شده است که آسیب‌پذیری‌های سایبری از طریق روابط تجاری و زنجیره‌های تأمین به سایر بنگاه‌ها نیز منتقل شوند (کراسیگنانی و همکاران، ۲۰۲۳).

در چنین محیطی، سازمان‌ها به سازوکارهای اطمینان‌بخشی نیاز دارند که بتوانند نه‌تنها وجود کنترل‌های امنیتی، بلکه کفایت طراحی و عملکرد آن‌ها و نحوه پاسخ سازمان به ریسک‌های سایبری را ارزیابی کنند (مؤسسه حسابرسان داخلی، ۲۰۲۴). حسابرسی سایبری از این منظر بخشی از سازوکار اطمینان‌بخشی سازمان است که می‌تواند از طریق ارزیابی ریسک‌ها و کنترل‌های سایبری، گزارش یافته‌های حسابرسی و ارائه توصیه‌های اصلاحی، به بهبود مدیریت ریسک کمک کند (اسالپنیچار و همکاران، ۲۰۲۲). با این حال، صرف انجام حسابرسی سایبری لزوماً به اثربخشی آن منجر نمی‌شود و میزان اثرگذاری آن می‌تواند به ظرفیت حرفه‌ای حسابرسان و شرایط حاکمیتی و سازمانی پیرامون فعالیت حسابرسی وابسته باشد (اسلام و همکاران، ۲۰۱۸).

یکی از این ظرفیت‌ها، شایستگی حرفه‌ای حسابرسان است. حسابرسی سایبری مستلزم آن است که حسابرس بتواند دانش حسابرسی را با درک فناوری اطلاعات، کنترل‌های داخلی، مدیریت ریسک و شواهد فنی ترکیب کند. شواهد موجود نیز نشان می‌دهد ویژگی‌های حرفه‌ای فعالیت حسابرسی داخلی و میزان دسترسی آن به دانش فناوری اطلاعات با مشارکت بیشتر در فعالیت‌های مرتبط با امنیت و فناوری ارتباط دارد (اسلام و همکاران، ۲۰۱۸؛ کالوین و همکاران، ۲۰۲۵). از سوی دیگر، اثربخشی حسابرسی سایبری صرفاً به توانایی حسابرس محدود نیست و محیط حاکمیتی سازمان نیز می‌تواند بر میزان استفاده از یافته‌های حسابرسی و تبدیل آن‌ها به اقدامات اصلاحی اثرگذار باشد.

در سطح حاکمیت سازمانی، هیئت‌مدیره در نظارت بر ریسک‌های سایبری و ارزیابی پاسخ سازمان به این ریسک‌ها نقش مهمی دارد. پیچیدگی موضوعات سایبری، عدم تقارن اطلاعاتی و دشواری تبدیل ریسک‌های فنی به پیامدهای کسب‌وکار، نظارت هیئت‌مدیره را با چالش مواجه کرده است (گیل و همکاران، ۲۰۲۲). شواهد موجود نشان می‌دهد دانش و تخصص فناوری اطلاعات اعضای هیئت‌مدیره یا کمیته حسابرسی و همچنین مشارکت فعال آنان می‌تواند به تقویت نظارت بر ریسک سایبری کمک کند (پرادفوت و همکاران، ۲۰۲۳؛ ژنگ و همکاران، ۲۰۲۵). با این حال، برخورداری از دانش به تنهایی لزوماً به اقدام سازمانی منجر نمی‌شود و حمایت عملی، تخصیص منابع، دسترسی به اطلاعات و پیگیری یافته‌های حسابرسی نیز اهمیت دارد.

افزون بر عوامل فردی و حاکمیتی، اثربخشی حسابرسی سایبری به کیفیت تعامل میان واحدهای مختلف سازمان نیز وابسته است. اطلاعات لازم برای ارزیابی ریسک‌های سایبری معمولاً در یک واحد متمرکز نیست و میان واحدهای عملیاتی، امنیت اطلاعات، مدیریت ریسک و حسابرسی داخلی توزیع شده است. بنابراین، همکاری و تبادل اطلاعات میان این نقش‌ها می تواند بر کیفیت ارزیابی ریسک و اطمینان‌بخشی سایبری اثرگذار باشد (استاینبارت و همکاران، ۲۰۱۸؛ مؤسسه حسابرسان داخلی، ۲۰۲۰). در این چارچوب، همکاری میان خطوط دفاعی به معنای ادغام نقش‌ها یا تضعیف استقلال حسابرسی نیست، بلکه بر هماهنگی، تبادل اطلاعات و کاهش شکاف‌های پوشش ریسک تأکید دارد.

با وجود اهمیت این عوامل، ادبیات داخلی هنوز شواهد تجربی محدودی درباره عوامل تعیین‌کننده مستقیم اثربخشی حسابرسی سایبری ارائه می‌کند. بخش مهمی از پژوهش‌های داخلی بر حسابرسی فناوری اطلاعات، کنترل داخلی، مدیریت ریسک سایبری یا موانع اجرای حسابرسی فناوری اطلاعات متمرکز بوده است (پرندین و همکاران، ۱۴۰۲؛ شکرخواه و موسوی‌بصیر، ۱۴۰۳). برخی مطالعات داخلی نیز اهمیت حاکمیت فناوری اطلاعات، حمایت و شایستگی را در حوزه‌های

www.jamv.ir
ISSN: 2645-4572

مرتبط با ریسک و امنیت سایبری مطرح کرده‌اند (حیدری و همکاران، ۱۴۰۲؛ جعفریان و سلیمی، ۱۴۰۴)، اما بررسی همزمان شایستگی حسابرسان، شایستگی هیئت‌مدیره، حمایت هیئت‌مدیره و همکاری با خطوط دفاعی به‌عنوان عوامل مؤثر بر اثربخشی حسابرسی سایبری کمتر مورد توجه قرار گرفته است.

در سطح بین‌المللی نیز مطالعه ووکو و همکاران (۲۰۲۵)، مجموعه‌ای از عوامل حرفه‌ای و حاکمیتی مؤثر ب ر اثربخشی حسابرسی سایبری را مورد توجه قرار داده است. با این حال، آزمون این روابط در زمینه‌های نهادی متفاوت می‌تواند به ارزیابی قابلیت تعمیم یافته‌ها و شناسایی اهمیت نسبی عوامل در محیط‌های حرفه‌ای مختلف کمک کند. از این منظر، بررسی تجربی این روابط در ایران می‌تواند شکاف موجود میان ادبیات حسابرسی داخلی، حاکمیت سایبری و همکاری میان خطوط دفاعی را تا حدی پوشش دهد.

بر این اساس، مسئله اصلی پژوهش حاضر آن است که شایستگی حسابرسان سایبری، شایستگی هیئت‌مدیره، حمایت هیئت‌مدیره و همکاری با خطوط دفاعی تا چه اندازه می‌توانند اثربخشی حسابرسی سایبری را تبیین کنند. تمرکز هم‌زمان بر عوامل فردی، حاکمیتی و بین‌واحدی، امکان مشاهده سازوکارهای مکمل اثربخشی را فراهم می‌کند (آرنا و آزونه، ۲۰۰۹). سنجش اثربخشی حسابرسی سایبری به‌صورت یک سازه چندگویه‌ای نیز با نگاه چندبعدی به کیفیت برنامه‌ریزی، اجرا، گزارشگری و پیامدهای حسابرسی سازگار است (اسلاپنیچار و همکاران، ۲۰۲۲). افزون بر این، استفاده از یک چارچوب تلفیقی می‌تواند شکاف میان ادبیات حسابرسی داخلی و ادبیات حاکمیت سایبری را کاهش دهد (اسلاپنیچار و همکاران، ۲۰۲۳).

مبانی نظری و پیشینه پژوهش

اثربخشی حسابرسی سایبری

اثربخشی حسابرسی داخلی مفهومی فراتر از انجام برنامه حسابرسی و ارائه گزارش است و به میزان توانایی فعالیت حسابرسی در ایجاد ارزش، بهبود کنترل‌ها و کمک به مدیریت ریسک سازمان مربوط می‌شود (آرنا و آزونه، ۲۰۰۹). شواهد پژوهشی نیز نشان می‌دهد اثربخشی حسابرسی داخلی تحت تأثیر مجموعه‌ای از عوامل شامل ویژگی‌های واحد حسابرسی، منابع در دسترس، جایگاه سازمانی و کیفیت تعامل آن با مدیریت قرار دارد (الزبان و گویلیام، ۲۰۱۴؛ لنز و هان، ۲۰۱۵).

در حوزه سایبری، دامنه و پیچیدگی موضوعات مورد بررسی حسابرس افزایش می‌یابد؛ زیرا ارزیابی ریسک و کنترل‌های سایبری مستلزم درک فناوری اطلاعات، دسترسی‌ها، آسیب‌پذیری‌ها، کنترل‌های امنیتی و فرایند پاسخ به رخدادهای سایبری است (کاهیااوغلو و چالیورت، ۲۰۱۸). از این رو، اثربخشی حسابرسی سایبری را نمی‌توان صرفاً بر اساس کیفیت فنی اجرای مأموریت ارزیابی کرد، بلکه میزان اثرگذاری یافته‌ها بر مدیریت ریسک و بهبود وضعیت سازمان نیز اهمیت دارد.

اسلپنیچار و همکاران (۲۰۲۲)، اثربخشی حسابرسی سایبری را مفهومی قابل سنجش در ارتباط با کیفیت فعالیت‌های اطمینان‌بخشی و مدیریت ریسک سایبری مورد توجه قرار داده‌اند. بر این مبنا، در پژوهش حاضر اثربخشی حسابرسی سایبری به‌عنوان پیامد نهایی فعالیت حسابرسی در نظر گرفته شده و ابعادی همچون کیفیت برنامه‌ریزی و اجرای حسابرسی، گزارشگری یافته‌ها، ارائه توصیه‌های قابل اجرا و کمک به بهبود مدیریت ریسک سایبری را دربرمی‌گیرد. این رویکرد با تأکید استانداردهای حرفه‌ای بر شایستگی، ارتباط مؤثر، کیفیت خدمات اطمینان‌بخشی و پیگیری نتایج نیز سازگار است (مؤسسه حسابرسان داخلی، ۲۰۲۴).

www.jamv.ir
ISSN: 2645-4572

نظریه نهادی و حاکمیت حسابرسی سایبری

نظریه نهادی بر این دیدگاه استوار است که ساختارها و رویه‌های سازمانی تنها حاصل محاسبات اقتصادی نیستند، بلکه قواعد، هنجارها و انتظارات محیطی نیز بر شکل‌گیری آن‌ها تأثیر می‌گذارند (اسکات، ۲۰۱۴). دیماجیو و پاول (۱۹۸۳)، سه نوع فشار نهادی شامل فشار اجباری، هنجاری و تقلیدی را مطرح کردند که می‌تواند سازمان‌ها را به سمت پذیرش ساختارها و رویه‌های مشابه سوق دهد.

در حوزه حسابرسی، محیط نهادی و الزامات حرفه‌ای می‌توانند بر توسعه و جایگاه فعالیت حسابرسی داخلی اثرگذار باشند (التویجری و همکاران، ۲۰۰۳). در حوزه سایبری نیز افزایش توجه نهادهای حاکمیتی و حرفه‌ای به مسئولیت هیئت‌مدیره، افشای ریسک و پاسخگویی سایبری موجب شده است حاکمیت سایبری به یکی از اجزای مهم ساختار سازمانی تبدیل شود (گیل و همکاران، ۲۰۲۲). همچنین، توزیع مسئولیت میان نقش‌های مختلف سازمان در مدیریت و اطمینان‌بخشی سایبری، بخشی از سازوکار پاسخگویی سازمانی محسوب می‌شود (اسلپنیچار و همکاران، ۲۰۲۳).

با این حال، فشارهای نهادی به‌تنهایی نمی‌توانند تفاوت در سطح اثربخشی حسابرسی سایبری میان سازمان‌ها را توضیح دهند. وجود الزامات و ساختارهای رسمی، لزوماً به معنای برخورداری از حسابرسی اثربخش نیست؛ بلکه ظرفیت‌های حرفه‌ای، حاکمیتی و سازمانی لازم برای اجرای مؤثر این ساختارها نیز باید مورد توجه قرار گیرد. از این منظر، نظریه نهادی در پژوهش حاضر نقش زمینه‌ای دارد و توضیح می‌دهد چرا سازمان‌ها به سمت ایجاد سازوکارهای حاکمیت و اطمینان‌بخشی سایبری حرکت می‌کنند، در حالی که سایر مبانی نظری به توضیح تفاوت در ظرفیت اجرای مؤثر این سازوکارها کمک می کنند.

شایستگی حسابرسان سایبری و نظریه سرمایه انسانی

نظریه سرمایه انسانی، دانش، مهارت و تجربه افراد را نوعی سرمایه مولد می‌داند که می‌تواند بهره‌وری و کیفیت عملکرد را افزایش دهد (بکر، ۱۹۶۴). در فعالیت حسابرسی سایبری، این دیدگاه اهمیت ویژه‌ای دارد؛ زیرا حسابرس باید بتواند دانش حسابرسی را با شناخت فناوری اطلاعات، کنترل‌های داخلی، مدیریت ریسک و تهدیدهای سایبری ترکیب کند.

کاهیااوغلو و چالیورت (۲۰۱۸)، بر ضرورت پیوند میان ارزیابی فنی و اهداف کسب‌وکار در فعالیت‌های مرتبط با حسابرسی سایبری تأکید کرده‌اند. همچنین، اسلام و همکاران (۲۰۱۸)، نشان داده‌اند که ویژگی‌های حرفه‌ای فعالیت حسابرسی داخلی با میزان درگیری آن در فعالیت‌های مرتبط با امنیت و فناوری ارتباط دارد. شواهد جدیدتر نیز نشان می‌دهد بلوغ فعالیت حسابرسی داخلی و دسترسی آن به دانش فناوری اطلاعات با مشارکت بیشتر در فعالیت‌های اطمینان‌بخشی فناوری و سایبری همراه است (کالوین و همکاران، ۲۰۲۵).

در محیط ایران نیز محدودیت‌های مهارتی و حرفه‌ای به‌عنوان یکی از موانع اجرای حسابرسی فناوری اطلاعات گزارش شده است (پرندین و همکاران، ۱۴۰۲). بنابراین، در پژوهش حاضر شایستگی حسابرسان سایبری مفهومی فراتر از برخورداری از مدرک یا گواهینامه حرفه‌ای است و دانش، تجربه، توانایی تحلیل و قابلیت به‌کارگیری دانش فنی در فرایند قضاوت و اجرای مأموریت حسابرسی ر ا دربرمی‌گیرد.

شایستگی هیئت‌مدیره و نظریه وابستگی به منابع

www.jamv.ir
ISSN: 2645-4572

نظریه وابستگی به منابع، هیئت‌مدیره را علاوه بر یک نهاد نظارتی، منبعی برای دانش، تجربه و دسترسی سازمان به منابع راهبردی می‌داند (پففر و سالانچیک، ۱۹۷۸). بر اساس این دیدگاه، سرمایه انسانی اعضای هیئت‌مدیره می‌تواند توان نظارتی و ظرفیت سازمان برای دسترسی و استفاده از منابع مورد نیاز را افزایش دهد (هیلمن و دالزیل، ۲۰۰۳).

در حوزه سایبری، پیچیدگی فناوری و سرعت تغییر تهدیدها موجب شده است دانش و سواد فناوری اطلاعات در سطح هیئت‌مدیره اهمیت بیشتری پیدا کند (گیل و همکاران، ۲۰۲۲). تخصص فناوری اطلاعات اعضای کمیته حسابرسی نیز با کیفیت توجه به ریسک و افشای ریسک سایبری مرتبط گزارش شده است (ژنگ و همکاران، ۲۰۲۵). افزون بر این، کیفیت حاکمیت سایبری به میزان استقرار واقعی سازوکارهای نظارتی و پاسخگویی وابسته است و صرف وجود ساختارهای رسمی نمی‌تواند تضمین‌کننده پیامدهای بهتر باشد (گائو و کالدرون، ۲۰۲۵).

از سوی دیگر، برخورداری از تخصص فناوری به‌تنهایی لزوماً به عملکرد بهتر منجر نمی‌شود. بناروچ و فینک (۲۰۲۱)، نشان داده‌اند که پیامدهای مرتبط با شایستگی فناوری هیئت‌مدیره به نحوه استفاده از این ظرفیت نیز وابسته است. بنابراین، در این پژوهش شایستگی هیئت‌مدیره به ظرفیت دانشی و تخصصی اعضای هیئت‌مدیره برای درک، ارزیابی و نظارت بر موضوعات فناوری و سایبری اشاره دارد و از حمایت عملی هیئت‌مدیره به‌عنوان سازه‌ای متمایز در نظر گرفته می‌شود.

حمایت هیئت‌مدیره و نظریه حمایت سازمانی

دانش و تخصص ارکان حاکمیتی زمانی می‌تواند به پیامدهای سازمانی منجر شود که با حمایت عملی، تخصیص منابع و پیگیری همراه باشد. نظریه حمایت سازمانی بر این فرض استوار است که ادراک حمایت از سوی سازمان می‌تواند ظرفیت و انگیزش لازم برای انجام مؤثر فعالیت‌ها را تقویت کند (آیزنبرگر و همکاران، ۱۹۸۶).

در حوزه حسابرسی داخلی، رابطه مناسب میان کمیته حسابرسی و واحد حسابرسی داخلی با جایگاه و اثربخشی این فعالیت ارتباط دارد (گودوین، ۲۰۰۳). همچنین، مشارکت هیئت‌مدیره و کمیته حسابرسی با میزان درگیری حسابرسی داخلی در فعالیت‌های امنیت و فناوری اطلاعات ارتباط نشان داده است (اسلام و همکاران، ۲۰۱۸). پژوهش‌های جدیدتر نیز نشان می‌دهند تعامل میان مدیر ارشد حسابرسی، کمیته حسابرسی و سازوکارهای حاکمیت فناوری اطلاعات می‌تواند با کیفیت بالاتر حسابرسی سایبری همراه باشد (الزبان و همکاران، ۲۰۲۶).

بر این اساس، حمایت هیئت‌مدیره در پژوهش حاضر به حمایت عملی از فعالیت حسابرسی سایبری اشاره دارد؛ از جمله تأمین منابع، پشتیبانی از استقلال حسابرسی، فراهم‌کردن دسترسی مناسب به اطلاعات، توجه به یافته‌های حسابرسی و پیگیری توصیه‌های اصلاحی. تمایز این مفهوم از شایستگی هیئت‌مدیره از نظر نظری اهمیت دارد؛ زیرا شایستگی ناظر بر «توانایی فهم و نظارت» است، در حالی که حمایت هیئت‌مدیره بر «اقدام و پشتیبانی سازمانی» دلالت دارد.

همکاری با خطوط دفاعی و نظریه هماهنگی سازمانی

مدیریت ریسک سایبری ماهیتی بین‌واحدی دارد و اطلاعات مورد نیاز برای ارزیابی ریسک معمولاً میان واحدهای عملیاتی، امنیت اطلاعات، مدیریت ریسک و حسابرسی داخلی توزیع شده است. بنابراین، مدیریت مؤثر این ریسک‌ها مستلزم توزیع روشن مسئولیت و در عین حال هماهنگی میان نقش‌های مختلف است (مؤسسه حسابرسان داخلی، ۲۰۲۰).

نظریه هماهنگی سازمانی، هماهنگی را فرایند مدیریت وابستگی‌های میان فعالیت‌ها و نقش‌ها می‌داند و بر جریان اطلاعات و سازوکارهای ارتباطی تأکید دارد (مالون و کروستون، ۱۹۹۴). در محیط سایبری، این موضوع اهمیت بیشتری دارد؛ زیرا

www.jamv.ir
ISSN: 2645-4572

حسابرس داخلی برای ارزیابی کنترل‌ها و ریسک‌های سایبری به اطلاعاتی نیاز دارد که بخشی از آن در اختیار خطوط اول و دوم دفاع قرار دارد.

شواهد تجربی نیز نشان می‌دهد کیفیت رابطه میان حسابرسی داخلی و واحد امنیت اطلاعات با پیامدهای بهتر امنیت اطلاعات همراه است (استاینبارت و همکاران، ۲۰۱۸). همچنین، چارچوب سه خط بر هماهنگی میان نقش‌های مدیریتی و اطمینان‌بخشی، در عین حفظ استقلال و تمایز مسئولیت‌ها، تأکید می‌کند (مؤسسه حسابرسان داخلی، ۲۰۲۰). اسلپنیچار و همکاران (۲۰۲۳)، نیز بر توزیع مسئولیت و هماهنگی میان نقش‌های مختلف در حاکمیت سایبری تأکید کرده‌اند.

در این پژوهش، همکاری با خطوط دفاعی به معنای ادغام مسئولیت‌ها یا انتقال مسئولیت حسابرسی به واحدهای مدیریتی نیست؛ بلکه به تبادل اطلاعات، هماهنگی ارزیابی‌ها، دسترسی مناسب به یافته‌ها، وضوح مرز مسئولیت‌ها و کاهش شکاف‌های نظارتی اشاره دارد.

جمع‌بندی مبانی نظری

چارچوب نظری پژوهش حاضر بر این فرض استوار است که فشارهای نهادی می‌توانند زمینه توجه سازمان به حسابرسی سایبری را ایجاد کنند، اما سطح اثربخشی به ظرفیت‌های درونی سازمان وابسته است (اسکات، ۲۰۱۴). شایستگی حسابرسان از طریق کیفیت قضاوت و اجرای مأموریت بر فرایند حسابرسی اثر می‌گذارد (کالوین و همکاران، ۲۰۲۵). شایستگی هیئت‌مدیره ظرفیت نظارت آگاهانه بر ریسک فناوری را افزایش می‌دهد (ژنگ و همکاران، ۲۰۲۵). حمایت هیئت‌مدیره منابع و مشروعیت لازم برای تبدیل یافته‌ها به اقدام را فراهم می‌کند (گودوین، ۲۰۰۳). همکاری میان خطوط دفاعی نیز از طریق بهبود جریان اطلاعات و هماهنگی نقش‌ها، پوشش ریسک را تقویت می‌کند (استاینبارت و همکاران، ۲۰۱۸). تلفیق این چهار ظرفیت، مبنای توسعه فرضیه‌های پژوهش را تشکیل می‌دهد.

مرور مطالعات تجربی مرتبط

مطالعات تجربی در حوزه حسابرسی داخلی نشان داده‌اند که اثربخشی این فعالیت تحت تأثیر مجموعه‌ای از عوامل قرار دارد. آرنا و آزونه (۲۰۰۹)، نقش کیفیت تیم، ویژگی‌های سازمانی و روابط حسابرسی داخلی با مدیریت را در اثربخشی حسابرسی مورد توجه قرار دادند. کوهن و سایگ (۲۰۱۰)، نیز حمایت مدیریت و جایگاه سازمانی حسابرسی داخلی را از عوامل مرتبط با اثربخشی این فعالیت گزارش کردند. در بخش عمومی، الزبان و گویلیام (۲۰۱۴)، نشان دادند که منابع، شایستگی و حمایت مدیریت می‌توانند عملکرد حسابرسی داخلی را تحت تأثیر قرار دهند. لنز و هان (۲۰۱۵)، نیز با مرور ادبیات تأکید کردند که اثربخشی حسابرسی داخلی حاصل یک عامل منفرد نیست و به ترکیبی از عوامل حرفه‌ای و سازمانی وابسته است.

در حوزه حسابرسی و امنیت سایبری، اسلام و همکاران (۲۰۱۸)، نشان دادند ویژگی‌های فعالیت حسابرسی داخلی و محیط سازمانی با میزان مشارکت آن در فعالیت‌های امنیت و فناوری اطلاعات ارتباط دارد. کاهیااوغلو و چالیورت (۲۰۱۸)، بر ضرورت پیوند میان دانش فنی و اهداف کسب‌وکار در فعالیت‌های مرتبط با حسابرسی سایبری تأکید کردند. استاینبارت و همکاران (۲۰۱۸)، نیز ارتباط میان کیفیت رابطه حسابرسی داخلی و امنیت اطلاعات و پیامدهای امنیت اطلاعات را بررسی کردند.

در زمینه حاکمیت سایبری، گیل و همکاران (۲۰۲۲)، چالش‌های نظارت هیئت‌مدیره بر امنیت سایبری را بررسی و بر اهمیت دانش و ظرفیت اعضای هیئت‌مدیره تأکید کردند. پرادفوت و همکاران (۲۰۲۳)، نیز نقش اقدام فعال هیئت‌مدیره در حاکمیت

www.jamv.ir
ISSN: 2645-4572

و مدیریت ریسک سایبری را مورد توجه قرار دادند. ژنگ و همکاران (۲۰۲۵)، رابطه تخصص فناوری اطلاعات کمیته حسابرسی با کیفیت افشای ریسک سایبری را بررسی کردند و گائو و کالدرون (۲۰۲۵)، بر اهمیت سازوکارهای واقعی حاکمیت در گزارشگری ریسک سایبری تأکید داشتند. این مطالعات نشان می‌دهند که ظرفیت دانشی و حاکمیتی هیئت‌مدیره می‌تواند اهمیت داشته باشد، اما نحوه تبدیل این ظرفیت به اقدام سازمانی نیز باید مورد توجه قرار گیرد.

در پژوهش‌های جدیدتر، کالوین و همکاران (۲۰۲۵)، نشان دادند بلوغ فعالیت حسابرسی داخلی و دسترسی به دانش فناوری اطلاعات با مشارکت بیشتر این فعالیت در اطمینان‌بخشی فناوری و سایبری همراه است. ووکو و همکاران (۲۰۲۵)، نیز مجموعه‌ای از عوامل حرفه‌ای و حاکمیتی، از جمله حرفه‌ای‌سازی حسابرسی داخلی، شایستگی هیئت‌مدیره، حمایت هیئت‌مدیره و همکاری با خطوط دفاعی را در ارتباط با اثربخشی حسابرسی سایبری مورد بررسی قرار دادند. همچنین، الزبان و همکاران (۲۰۲۶)، بر اهمیت هم‌افزایی میان مدیر ارشد حسابرسی، حاکمیت فناوری اطلاعات و فعالیت حسابرسی داخلی در کیفیت حسابرسی سایبری تأکید کردند.

در ایران، مطالعات موجود بیشتر بر چالش‌های اجرای حسابرسی فناوری اطلاعات، کنترل داخلی، حاکمیت فناوری اطلاعات و عوامل مرتبط با فرهنگ و آگاهی امنیت سایبری متمرکز بوده‌اند. پرندین و همکاران (۱۴۰۲)، محدودیت‌های مهارتی و حرفه‌ای را از موانع اجرای حسابرسی فناوری اطلاعات در ایران معرفی کردند. حیدری و همکاران (۱۴۰۲)، نیز بر اهمیت شایستگی، حمایت و حکمرانی امنیتی در شکل‌گیری فرهنگ و آگاهی امنیت سایبری تأکید کردند. شکرخواه و موسوی بصیر (۱۴۰۳)، بر ضرورت توجه به حسابرسی ریسک سایبری در طراحی کنترل‌های داخلی تأکید داشتند و جعفریان و سلیمی (۱۴۰۴)، نقش حسابرسی داخلی الکترونیک مبتنی بر حاکمیت فناوری اطلاعات را در کاهش ریسک‌های حسابرسی بررسی کردند.

در مجموع، مرور مطالعات نشان می‌دهد اگرچه هر یک از عوامل حرفه‌ای، حاکمیتی و هماهنگی سازمانی در ادبیات پیشین مورد توجه قرار گرفته‌اند، شواهد تجربی درباره بررسی همزمان آن‌ها در تبیین اثربخشی حسابرسی سایبری، به‌ویژه در بستر ایران، محدود است. بنابراین، پژوهش حاضر با قرار دادن این چهار عامل در یک مدل واحد، به دنبال بررسی نقش نسبی شایستگی حسابرسان، شایستگی هیئت‌مدیره، حمایت هیئت‌مدیره و همکاری با خطوط دفاعی در اثربخشی حسابرسی سایبری است.

توسعه فرضیه‌ها و مدل مفهومی

شایستگی حسابرسان و اثربخشی حسابرسی سایبری

شواهد پژوهشی نشان می‌دهد ویژگی‌های حرفه‌ای و سطح دانش حسابرسان داخلی با میزان مشارکت آنان در فعالیت‌های مرتبط با امنیت اطلاعات و فناوری ارتباط دارد و برخورداری از دانش فناوری اطلاعات می‌تواند مشارکت حسابرسی داخلی در فعالیت‌های اطمینان‌بخشی فناوری و سایبری را تقویت کند (اسلام و همکاران، ۲۰۱۸؛ کالوین و همکاران، ۲۰۲۵). بر این اساس، انتظار می‌رود حسابرسان برخوردار از شایستگی بالاتر، توانایی بیشتری در شناسایی و ارزیابی ریسک‌های سایبری، اجرای مناسب رویه‌های حسابرسی و ارائه یافته‌های قابل استفاده داشته باشند. بنابراین:

فرضیه ۱: شایستگی حسابرسان سایبری تأثیر مثبت و معناداری بر اثربخشی حسابرسی سایبری دارد.

شایستگی هیئت‌مدیره و اثربخشی حسابرسی سایبری

www.jamv.ir
ISSN: 2645-4572

مطالعات پیشین نشان داده‌اند که دانش و تخصص فناوری اطلاعات در سطح هیئت‌مدیره و کمیته حسابرسی با کیفیت توجه به ریسک‌های سایبری و افشای اطلاعات مرتبط با آن ارتباط دارد. همچنین، مشارکت فعال اعضای هیئت‌مدیره در نظارت بر مسائل فناوری و امنیت اطلاعات می‌تواند فرایند نظارت بر ریسک‌های سایبری را تقویت کند (گِیل و همکاران، ۲۰۲۲؛ پرادفوت و همکاران، ۲۰۲۳؛ ژنگ و همکاران، ۲۰۲۵). بر این اساس، انتظار می‌رود شایستگی بالاتر هیئت‌مدیره در حوزه فناوری و سایبری، ارزیابی و استفاده از یافته‌های حسابرسی سایبری را در فرایند نظارت اثربخش‌تر کند. بنابراین:

فرضیه ۲: شایستگی هیئت‌مدیره تأثیر مثبت و معناداری بر اثربخشی حسابرسی سایبری دارد.

حمایت هیئت‌مدیره و اثربخشی حسابرسی سایبری

شواهد موجود بر اهمیت رابطه میان ارکان حاکمیتی و حسابرسی داخلی در اثربخشی فعالیت حسابرسی تأکید دارد و نشان می‌دهد تعامل مناسب هیئت‌مدیره و کمیته حسابرسی با فعالیت‌های حسابرسی امنیت و فناوری اطلاعات می‌تواند به تقویت این فعالیت‌ها منجر شود (گودوین، ۲۰۰۳؛ اسلام و همکاران، ۲۰۱۸). همچنین، تعامل مدیر ارشد حسابرسی با کمیته حسابرسی و سازوکارهای حاکمیت فناوری اطلاعات با کیفیت بهتر حسابرسی سایبری مرتبط گزارش شده است (الزبان و همکاران، ۲۰۲۶). بنابراین، انتظار می‌رود حمایت عملی هیئت‌مدیره از حسابرسی سایبری، زمینه دسترسی به منابع، پیگیری یافته‌ها و اجرای اقدامات اصلاحی را فراهم کرده و در نتیجه اثربخشی حسابرسی سایبری را افزایش دهد. بنابراین:

فرضیه ۳: حمایت هیئت‌مدیره تأثیر مثبت و معناداری بر اثربخشی حسابرسی سایبری دارد.

همکاری با خطوط دفاعی و اثربخشی حسابرسی سایبری

شواهد پژوهشی نشان می‌دهد کیفیت رابطه میان حسابرسی داخلی و واحدهای مسئول امنیت اطلاعات با پیامدهای بهتر در حوزه امنیت اطلاعات همراه است (استاینبارت و همکاران، ۲۰۱۸). همچنین، چارچوب سه خط بر هماهنگی و ارتباط میان نقش‌های مختلف در مدیریت ریسک و ارائه اطمینان، در عین حفظ استقلال هر یک از نقش‌ها، تأکید دارد (مؤسسه حسابرسان داخلی، ۲۰۲۰). بر این اساس، انتظار می‌رود همکاری مؤثرتر میان خطوط دفاعی، دسترسی حسابرسان به اطلاعات مرتبط با ریسک و کیفیت فرایند اطمینان‌بخشی را بهبود بخشیده و در نهایت اثربخشی حسابرسی سایبری را افزایش دهد. بنابراین:

فرضیه ۴: همکاری با خطوط دفاعی تأثیر مثبت و معناداری بر اثربخشی حسابرسی سایبری دارد.

مدل مفهومی پژوهش

بر اساس فرضیه‌های مطرح‌شده، مدل مفهومی پژوهش رابطه چهار متغیر برون‌زا شامل شایستگی حسابرسان سایبری، شایستگی هیئت‌مدیره، حمایت هیئت‌مدیره و همکاری با خطوط دفاعی را با متغیر درون‌زای اثربخشی حسابرسی سایبری نشان می‌دهد. جهت روابط مورد انتظار در هر چهار مسیر مثبت است. بر مبنای فرضیه‌های فوق، مدل مفهومی پژوهش شامل چهار سازه برون‌زا یعنی شایستگی حسابرسان سایبری، شایستگی هیئت‌مدیره، حمایت هیئت‌مدیره و همکاری با خطوط دفاعی و یک سازه درون‌زا یعنی اثربخشی حسابرسی سایبری است. جهت همه مسیرهای نظری، مثبت در نظر گرفته شده است.

روش شناسی پژوهش

www.jamv.ir
ISSN: 2645-4572

پژوهش حاضر از نظر فلسفه پژوهش در چارچوب رویکرد اثبات‌گرایی، از نظر هدف کاربردی و از نظر رویکرد، کمی و از نوع مطالعات مقطعی است. داده‌های پژوهش با استفاده از پرسشنامه محقق‌ساخته گردآوری شد. طراحی ابزار اندازه‌گیری با اتکا به مبانی نظری و مطالعات پیشین در زمینه اثربخشی حسابرسی سایبری انجام گرفت. به‌طور مشخص، ساختار مفهومی سازه‌های پژوهش از مطالعه ووکو و همکاران (۲۰۲۵)، و برای سازه اثربخشی حسابرسی سایبری از شاخص توسعه‌یافته توسط اسلاپنیچار و همکاران (۲۰۲۲)، استفاده شد. ووکو و همکاران (۲۰۲۵)، عوامل حرفه‌ای و حاکمیتی از جمله شایستگی حسابرسان، شایستگی هیئت‌مدیره، حمایت هیئت‌مدیره و همکاری حسابرسی داخلی با خطوط اول و دوم دفاع را از عوامل مؤثر بر اثربخشی حسابرسی سایبری معرفی کرده‌اند.

جامعه مورد مطالعه شامل افراد دارای دانش و تجربه مرتبط با حسابداری و حسابرسی، از جمله حسابرسان داخلی و حسابرسان شاغل در مؤسسات حسابرسی بود. داده‌های پژوهش از طریق پرسشنامه گردآوری شد و پس از بررسی اولیه پاسخ‌ها، موارد ناقص از تحلیل حذف شدند.پرسشنامه پژوهش شامل ۴۰ گویه و در قالب طیف پنج‌درجه‌ای لیکرت تنظیم شد. این ابزار پنج سازه شامل شایستگی حسابرسان سایبری (۸ گویه)، شایستگی هیئت‌مدیره (۶ گویه)، حمایت هیئت‌مدیره (۷ گویه)، همکاری با خطوط دفاعی (۶ گویه) و اثربخشی حسابرسی سایبری (۱۳ گویه) را اندازه‌گیری کرد. در تدوین گویه‌های سازه‌های شایستگی و حاکمیتی، چارچوب ووکو و همکاران (۲۰۲۵)، مبنا قرار گرفت. این مطالعه شایستگی هیئت‌مدیره را با تأکید بر پیشینه دانشگاهی، آموزش و تجربه سایبری تعریف کرده و حمایت هیئت‌مدیره را به‌عنوان سطح حمایت از حسابرسی داخلی در زمینه حسابرسی سایبری سنجیده است. همچنین همکاری، شدت همکاری حسابرسی داخلی با خط اول و خط دوم دفاع را نشان می‌دهد.

برای اندازه‌گیری اثربخشی حسابرسی سایبری، رویکرد فرایندی اسلاپنیچار و همکاران (۲۰۲۲)، که در مطالعه ووکو و همکاران (۲۰۲۵)، نیز مورد استفاده قرار گرفته است، مبنا قرار گرفت. این رویکرد اثربخشی حسابرسی سایبری را در سه مرحله اصلی برنامه‌ریزی، اجرای عملیات حسابرسی و گزارش‌دهی در نظر می‌گیرد و بر ویژگی‌هایی مانند ریسک‌محور بودن، جامعیت، استفاده از چارچوب‌های امنیت سایبری و ارائه گزارش مستقل و جامع به هیئت‌مدیره تأکید دارد.

برای بررسی پایایی و روایی سازه‌ها، مدل اندازه‌گیری با استفاده از مدل‌سازی معادلات ساختاری مبتنی بر حداقل مربعات جزئی (PLS-SEM) ارزیابی شد. در این مرحله، بارهای عاملی، آلفای کرونباخ و پایایی ترکیبی (CR) برای بررسی پایایی درونی سازه‌ها و میانگین واریانس استخراج‌شده (AVE) برای ارزیابی روایی همگرا مورد استفاده قرار گرفتند. روایی واگرا نیز با استفاده از شاخص HTMT بررسی شد. (هیر و همکاران، ۲۰۲۲؛ هنسلر و همکاران، ۲۰۱۵) .

در ارزیابی مدل ساختاری، هم‌خطی متغیرهای پیش‌بین با استفاده از VIF بررسی شد. همچنین قدرت تبیین مدل با استفاده از R^2، قدرت پیش‌بینی با استفاده از Q^2 و اندازه اثر روابط با استفاده از f^2 ارزیابی شد. برای آزمون معناداری ضرایب مسیر نیز از روش بوت‌استرپ با ۵۰۰۰ بازنمونه استفاده شد.

یافته‌های پژوهش

آمار توصیفی متغیرهای پژوهش

جدول (۱): آمار توصیفی سازه‌های پژوهش

سازه	میانگین	انحراف معیار	حداقل	حداکثر	چولگی	کشیدگی
شایستگی حسابرسان سایبری (AC)	۳,۴۳۴	۰,۴۵۸	۲,۲۵۰	۴,۵۰۰	۰,۱۷۵	−۰,۵۳۰
شایستگی هیئت‌مدیره (BC)	۳,۲۴۶	۰,۴۸۷	۲,۱۶۷	۴,۳۳۳	−۰,۲۲۷	−۰,۳۷۴

www.jamv.ir
ISSN: 2645-4572

حمایت هیئت‌مدیره (BS)	۳,۳۶۹	۰,۵۳۹	۱,۷۱۴	۴,۷۱۴	−۰,۱۵۸	۰,۴۲۷
همکاری با خطوط دفاعی (LOD)	۳,۲۱۵	۰,۵۵۱	۱,۵۰۰	۴,۶۶۷	−۰,۲۱۹	۰,۵۶۷
اثربخشی حسابرسی سایبری (CAE)	۳,۴۱۹	۰,۴۴۳	۲,۳۸۵	۴,۵۳۸	۰,۱۸۲	−۰,۳۶۲

نتایج آمار توصیفی نشان داد میانگین هر پنج سازه بالاتر از نقطه میانی مقیاس پنج‌درجه‌ای لیکرت است. بیشترین میانگین مربوط به شایستگی حسابرسان سایبری با مقدار ۳,۴۳۴ و کمترین میانگین مربوط به همکاری با خطوط دفاعی با مقدار ۳,۲۱۵ بود. میانگین شایستگی هیئت‌مدیره ۳,۲۴۶، حمایت هیئت‌مدیره ۳,۳۶۹ و اثربخشی حسابرسی سایبری ۳,۴۱۹ به دست آمد. همچنین، مقادیر چولگی و کشیدگی در دامنه مشاهده‌شده، نشانه‌ای از انحراف توصیفی شدید از توزیع متعارف نشان نمی‌دهند.

برازش مدل اندازه‌گیری

برای ارزیابی مدل اندازه‌گیری پژوهش، پایایی و روایی سازه‌ها با استفاده از بارهای عاملی، آلفای کرونباخ، پایایی ترکیبی (CR)، میانگین واریانس استخراج‌شده (AVE) و شاخص هتروتریت–مونوتریت (HTMT) بررسی شد. بارهای عاملی، آلفای کرونباخ و پایایی ترکیبی برای ارزیابی پایایی درونی سازه‌ها و شاخص AVE برای بررسی روایی همگرای سازه‌ها مورد استفاده قرار گرفتند. همچنین، روایی واگرا با استفاده از شاخص HTMT ارزیابی شد (هیر و همکاران، ۲۰۲۲؛ هنسلر و همکاران، ۲۰۱۵).

نتایج مدل اندازه‌گیری نشان می‌دهد که مقدار آلفای کرونباخ سازه‌های پژوهش بین ۰,۸۵۱ تا ۰,۹۲۱ و مقدار پایایی ترکیبی بین ۰,۸۹۰ تا ۰,۹۳۲ قرار دارد. بنابراین، پایایی درونی همه سازه‌ها در سطح مطلوب قرار دارد. همچنین، مقادیر AVE برای سازه‌های شایستگی حسابرسان سایبری، شایستگی هیئت‌مدیره، حمایت هیئت‌مدیره، همکاری با خطوط دفاعی و اثربخشی حسابرسی سایبری به‌ترتیب ۰,۵۶۹، ۰,۵۷۵، ۰,۶۱۵، ۰,۵۸۴ و ۰,۵۱۶ است. از آنجا که مقدار AVE تمامی سازه‌ها از ۰,۵۰ بیشتر است، روایی همگرای مدل اندازه‌گیری تأیید می‌شود.

بارهای عاملی گویه‌ها نیز در مجموع در سطح قابل قبول قرار دارند. بارهای عاملی سازه شایستگی حسابرسان سایبری بین ۰,۶۵۸ تا ۰,۸۱۶، شایستگی هیئت‌مدیره بین ۰,۷۰۸ تا ۰,۸۲۱، حمایت هیئت‌مدیره بین ۰,۶۹۶ تا ۰,۸۲۶، همکاری با خطوط دفاعی بین ۰,۶۴۰ تا ۰,۸۵۳ و اثربخشی حسابرسی سایبری بین ۰,۵۷۷ تا ۰,۷۹۳ قرار گرفته است. کمترین بار عاملی مربوط به CAE9 با مقدار ۰,۵۷۷ است؛ با این حال، با توجه به قابل قبول بودن شاخص‌های پایایی و روایی همگرای سازه اثربخشی حسابرسی سایبری، این گویه در مدل حفظ شده است.

برای بررسی روایی واگرا، شاخص HTMT محاسبه شد. مقادیر این شاخص برای روابط بین سازه‌ها بین ۰,۳۶۰ تا ۰,۶۰۴ قرار دارد و بیشترین مقدار مربوط به رابطه میان حمایت هیئت‌مدیره و همکاری با خطوط دفاعی با مقدار ۰,۶۰۴ است. از آنجا که تمامی مقادیر HTMT پایین‌تر از آستانه ۰,۸۵ قرار دارند، روایی واگرای سازه‌های مدل اندازه‌گیری تأیید می‌شود (هنسلر و همکاران، ۲۰۱۵).

بر این اساس، نتایج ارزیابی مدل اندازه‌گیری نشان می‌دهد که سازه‌های پژوهش از پایایی درونی، روایی همگرا و روایی واگرای قابل قبول برخوردارند و مدل اندازه‌گیری از شرایط لازم برای ورود به مرحله ارزیابی مدل ساختاری برخوردار است.

جدول (۲): بارهای عاملی، پایایی و روایی همگرای سازه‌ها

سازه	گویه‌ها و بارهای عاملی	آلفای کرونباخ	CR	AVE

www.jamv.ir
ISSN: 2645-4572

شایستگی حسابرسان سایبری (AC)	۰,۷۶۱=۱AC ۰,۷۵۶=۲AC ۰,۷۸۳=۳AC ۰,۷۰۹=۴AC ۰,۷۲۴=۵AC ۰,۸۱۴=۶AC ۰,۶۵۸=۷AC ۰,۸۱۶=۸AC	۰,۸۹۱	۰,۹۱۳	۰,۵۶۹
شایستگی هیئت‌مدیره (BC)	۰,۷۷۴=۱BC ۰,۷۰۸=۲BC ۰,۷۳۲=۳BC ۰,۷۴۲=۴BC ۰,۷۶۸=۵BC ۰,۸۲۱=۶BC	۰,۸۵۱	۰,۸۹۰	۰,۵۷۵
حمایت هیئت‌مدیره (BS)	۰,۷۲۸=۱BS ۰,۸۲۴=۲BS ۰,۸۲۶=۳BS ۰,۸۲۶=۴BS ۰,۶۹۶=۵BS ۰,۷۹۲=۶BS ۰,۷۸۶=۷BS	۰,۸۹۴	۰,۹۱۸	۰,۶۱۵
همکاری با خطوط دفاعی (LOD)	۰,۸۰۷=۱LOD ۰,۷۵۴=۲LOD ۰,۶۴۰=۳LOD ۰,۷۶۱=۴LOD ۰,۷۵۳=۵LOD ۰,۸۵۳=۶LOD	۰,۸۵۴	۰,۸۹۳	۰,۵۸۴
اثربخشی حسابرسی سایبری (CAE)	۰,۷۰۴=۱CAE ۰,۷۲۳=۲CAE ۰,۷۰۵=۳CAE ۰,۷۴۶=۴CAE ۰,۷۱۲=۵CAE ۰,۷۶۲=۶CAE ۰,۶۸۹=۷CAE ۰,۷۴۳=۸CAE ۰,۵۷۷=۹CAE ۰,۷۹۳=۱۰CAE ۰,۷۴۲=۱۱CAE	۰,۹۲۱	۰,۹۳۲	۰,۵۱۶

www.jamv.ir
ISSN: 2645-4572

	۰,۶۹۲=۱۲CAE ۰,۷۲۷=۱۳CAE			

کمترین بار عاملی مربوط به گویه شماره ۹ سازه اثربخشی حسابرسی سایبری با مقدار ۰,۵۷۷ است؛ با توجه به کفایت شاخص‌های پایایی و روایی سازه و ضرورت حفظ پوشش محتوایی، این گویه در مدل نهایی حفظ شد (فورنل و لارکر، ۱۹۸۱؛ چئونگ و همکاران، ۲۰۲۴).

جدول (۳): ماتریس HTMT برای ارزیابی روایی واگرا

سازه	AC	BC	BS	LOD	CAE
شایستگی حسابرسان سایبری	۱,۰۰۰	–	–	–	–
شایستگی هیئت‌مدیره	۰,۴۶۰	۱,۰۰۰	–	–	–
حمایت هیئت‌مدیره	۰,۴۳۴	۰,۵۲۴	۱,۰۰۰	–	–
همکاری با خطوط دفاعی	۰,۳۶۰	۰,۴۷۸	۰,۶۰۴	۱,۰۰۰	–
اثربخشی حسابرسی سایبری	۰,۴۵۸	۰,۴۷۱	۰,۵۰۷	۰,۵۴۸	۱,۰۰۰

برای بررسی روایی واگرای سازه‌های پژوهش از معیار نسبت هتروتریت–مونوتریت (HTMT) استفاده شد. این معیار میزان تمایز سازه‌های مختلف از یکدیگر را بررسی می‌کند و در صورتی که مقدار HTMT بین سازه‌ها در محدوده قابل قبول قرار داشته باشد، می‌توان نتیجه گرفت که سازه‌ها از روایی واگرای مناسبی برخوردار هستند.بر اساس نتایج به‌دست‌آمده، بیشترین مقدار HTMT در مدل پژوهش برابر با ۰,۶۰۴ بوده است. با توجه به اینکه این مقدار کمتر از حد آستانه ۸۵/۰ است، می‌توان نتیجه گرفت که بین سازه‌های پژوهش تمایز مناسبی وجود دارد و هر سازه مفهوم متمایزی از سایر سازه‌ها را اندازه‌گیری می‌کند.بنابراین، نتایج معیار HTMT، روایی واگرای مدل اندازه‌گیری را تأیید می‌کند و نشان می‌دهد که سازه‌های پژوهش از یکدیگر قابل تفکیک هستند.

برازش مدل ساختاری

برای ارزیابی برازش مدل ساختاری پژوهش، معیارهای همخطی، قدرت تبیین، قدرت پیش‌بینی و اندازه اثر مورد بررسی قرار گرفت و معناداری ضرایب مسیر نیز با استفاده از روش بوت‌استرپ ۵۰۰۰ بازنمونه ارزیابی شد .نتایج نشان داد مقادیر شاخص عامل تورم واریانس (VIF) متغیرهای پیش‌بین بین ۱,۲۸۰ و ۱,۵۹۸ قرار دارد؛ بنابراین، مشکل قابل‌توجهی از نظر همخطی بین متغیرهای پیش‌بین مشاهده نشد.

همان‌طور که در جدول ۴ مشاهده می‌شود، مقدار ضریب تعیین برای سازه درون‌زای اثربخشی حسابرسی سایبری برابر با ۰,۳۵۷ و ضریب تعیین تعدیل‌شده برابر با ۰,۳۳۹ است. بنابراین، متغیرهای برون‌زای مدل توانسته‌اند ۳۵,۷ درصد از واریانس اثربخشی حسابرسی سایبری را تبیین کنند. همچنین، مقدار Q^2 برابر با ۰,۳۲۶ به دست آمد که نشان‌دهنده وجود قدرت پیش‌بینی مدل برای سازه درون‌زا است.

از نظر اندازه اثر نیز، نتایج نشان می‌دهد همکاری با خطوط دفاعی با مقدار ۰,۰۷۹ بیشترین اندازه اثر را بر اثربخشی حسابرسی سایبری دارد. پس از آن، شایستگی حسابرسان سایبری با مقدار ۰,۰۵۱، حمایت هیئت‌مدیره با مقدار ۰,۰۲۸ و شایستگی هیئت‌مدیره با مقدار ۰,۰۲۴ قرار دارند. بنابراین، در میان متغیرهای مورد بررسی، همکاری با خطوط دفاعی بیشترین سهم را در اثرگذاری بر سازه درون‌زای پژوهش داشته است.

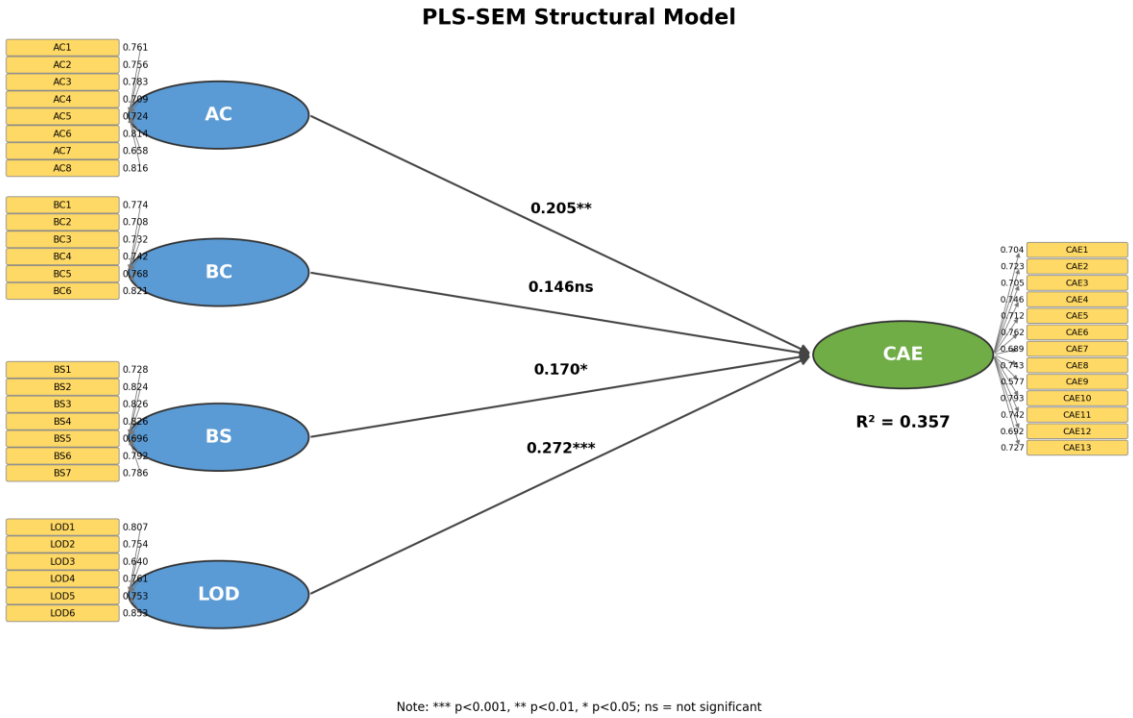
www.jamv.ir
ISSN: 2645-4572

نتایج آزمون ضرایب مسیر نشان داد شایستگی حسابرسان سایبری با ضریب مسیر ۰,۲۰۵ و سطح معناداری ۰,۰۰۲، اثر مثبت و معناداری بر اثربخشی حسابرسی سایبری دارد؛ بنابراین، فرضیه اول تأیید شد. شایستگی هیئت‌مدیره نیز دارای اثر مثبت با ضریب مسیر ۰,۱۴۶ است، اما این اثر در سطح ۵ درصد معنادار نیست (p=۰۰۰۸۴۸) ؛ ازاین‌رو، فرضیه دوم تأیید نشد. حمایت هیئت‌مدیره با ضریب مسیر ۰,۱۷۰ و سطح معناداری ۰,۰۱۸ اثر مثبت و معناداری بر اثربخشی حسابرسی سایبری دارد و فرضیه سوم تأیید می‌شود. همچنین، همکاری با خطوط دفاعی با ضریب مسیر ۰,۲۷۲ و سطح معناداری ۰,۰۰۰۴، قوی‌ترین اثر مستقیم را در میان مسیرهای مدل نشان داد و فرضیه چهارم نیز تأیید شد.

در مجموع، سه فرضیه از چهار فرضیه پژوهش تأیید شد. مقدار R^2 برابر با ۰,۳۵۷ نشان می‌دهد متغیرهای برون‌زای مدل بخش قابل‌توجهی از تغییرات اثربخشی حسابرسی سایبری را تبیین می‌کنند و مقدار Q^2 برابر با ۰,۳۲۶ نیز بیانگر برخورداری مدل از قدرت پیش‌بینی است. در میان روابط بررسی‌شده، همکاری با خطوط دفاعی بیشترین ضریب مسیر و بیشترین اندازه اثر را به خود اختصاص داد، در حالی که شایستگی هیئت‌مدیره تنها مسیر مثبت اما غیرمعنادار مدل بود.

جدول (۴): نتایج آزمون فرضیه‌ها، هم‌خطی و اندازه اثر

فرضیه	β	SE	t	p	VIF	f^2	نتیجه
H1	۰,۲۰۵	۰,۰۷۱	۲,۹۰۵	۰,۰۰۲	۱,۲۸۰	۰,۰۵۱	تأیید
H2	۰,۱۴۶	۰,۰۸۳	۱,۷۶۶	۰,۰۸۴۸	۱,۴۱۸	۰,۰۲۴	تأیید نشد
H3	۰,۱۷۰	۰,۰۷۳	۲,۳۲۳	۰,۰۱۸	۱,۵۹۸	۰,۰۲۸	تأیید
H4	۰,۲۷۲	۰,۰۶۹	۳,۹۴۰	۰,۰۰۰۴	۱,۴۶۸	۰,۰۷۹	تأیید



شکل (۱): نمای گرافیکی خروجی مدل را نشان می‌دهد؛ در آن گره‌های سازه‌ای، گویه‌ها، بارهای عاملی، ضرایب مسیر و مقدار R^2 نمایش داده شده است.

www.jamv.ir
ISSN: 2645-4572

در مجموع، سه فرضیه از چهار فرضیه پژوهش تأیید شد. مقدار R^2=۰,۳۵۷ نشان می‌دهد مدل ۳۵,۷ درصد از واریانس اثربخشی حسابرسی سایبری را تبیین می‌کند. همچنین Q^2=۰,۳۲۶ در چارچوب شاخص مورد استفاده مثبت بود؛ بااین‌حال، این یافته نباید به‌عنوان اثبات رابطه علّی یا تضمین عملکرد مدل در نمونه‌های جدید تفسیر شود. از نظر اندازه اثر، f^2=۰,۰۷۹ برای همکاری با خطوط دفاعی، f^2=۰,۰۲۸ برای حمایت هیئت‌مدیره، f^2=۰,۰۵۱ برای شایستگی حسابرسان و f^2=۰,۰۲۴ برای شایستگی هیئت‌مدیره به دست آمد. بر اساس آستانه‌های متعارف، همه اندازه اثرهای مشاهده‌شده در این مدل در دامنه اثر کوچک قرار دارند؛ بااین‌حال، همکاری با خطوط دفاعی در مقایسه نسبی، بزرگ‌ترین اندازه اثر را نشان می‌دهد.

بحث و نتیجه‌گیری

هدف پژوهش حاضر بررسی عوامل حرفه‌ای و حاکمیتی مؤثر بر اثربخشی حسابرسی سایبری با تمرکز بر شایستگی حسابرسان سایبری، شایستگی هیئت‌مدیره، حمایت هیئت‌مدیره و همکاری با خطوط دفاعی بود. نتایج نشان داد سه مسیر از چهار مسیر پیشنهادی از نظر آماری معنادار بودند. به‌طور مشخص، شایستگی حسابرسان سایبری، حمایت هیئت‌مدیره و همکاری با خطوط دفاعی رابطه مثبت و معناداری با اثربخشی حسابرسی سایبری داشتند؛ در حالی که اثر مستقیم شایستگی هیئت‌مدیره، اگرچه مثبت بود، در سطح معناداری ۵ درصد تأیید نشد. این الگو نشان می‌دهد که اثربخشی حسابرسی سایبری در نمونه مورد بررسی صرفاً به وجود ظرفیت‌های دانشی یا ساختاری وابسته نیست، بلکه به توان تبدیل این ظرفیت‌ها به اقدام حرفه‌ای، حمایت سازمانی و هماهنگی میان واحدهای مرتبط نیز وابسته است.

بحث و مقایسه فرضیه اول: شایستگی حسابرسان سایبری

نتایج نشان داد شایستگی حسابرسان سایبری اثر مثبت و معناداری بر اثربخشی حسابرسی سایبری دارد. این یافته با منطق نظریه سرمایه انسانی سازگار است؛ زیرا حسابرسی سایبری مستلزم ترکیب دانش حسابرسی با درک فناوری اطلاعات، امنیت سایبری، ارزیابی کنترل‌ها، تحلیل ریسک و تفسیر شواهد فنی است. در چنین محیطی، افزایش توانایی حرفه‌ای حسابرس می‌تواند کیفیت شناسایی ریسک، طراحی رویه‌های حسابرسی، ارزیابی شواهد و ارائه توصیه‌های قابل اجرا را بهبود دهد.

این نتیجه با شواهد تجربی ووکو و همکاران (۲۰۲۵)، هم‌راستا است که بر اهمیت حرفه‌ای‌سازی حسابرسی داخلی، آموزش و گواهینامه‌های تخصصی در اثربخشی حسابرسی سایبری تأکید کرده‌اند. همچنین با مطالعات پیشین درباره نقش تخصص و قابلیت‌های حرفه‌ای در اثربخشی حسابرسی داخلی سازگار است. با این حال، پژوهش حاضر این رابطه را در قالب یک سازه نهفته و در چارچوب مدل معادلات ساختاری بررسی کرده و از این طریق شواهدی تکمیلی درباره اهمیت شایستگی حرفه‌ای در بستر حسابرسی سایبری ارائه می‌کند.

از منظر عملی، این یافته نشان می‌دهد سرمایه‌گذاری سازمان در آموزش حسابرسان نباید به آموزش‌های عمومی حسابرسی محدود شود. آموزش امنیت سایبری، فناوری اطلاعات، ارزیابی کنترل‌های فناوری، تحلیل شواهد دیجیتال و مدیریت ریسک سایبری می‌تواند بخشی از الزامات توسعه شایستگی حسابرسان سایبری باشد.

بحث و مقایسه فرضیه دوم: شایستگی هیئت‌مدیره

فرضیه دوم تأیید نشد. اگرچه ضریب مسیر شایستگی هیئت‌مدیره مثبت بود، این رابطه در سطح ۵ درصد معنادار نبود. این نتیجه از نظر نظری اهمیت دارد؛ زیرا نشان می‌دهد وجود دانش یا تخصص سایبری در سطح هیئت‌مدیره لزوماً به افزایش مستقیم اثربخشی حسابرسی سایبری منجر نمی‌شود.

www.jamv.ir
ISSN: 2645-4572

این یافته با برخی مطالعات پیشین که بر نقش دانش فناوری و تخصص هیئت‌مدیره در نظارت بر ریسک سایبری تأکید کرده‌اند، تفاوت دارد. مطالعاتی مانند گیل و همکاران (۲۰۲۲)، پرادفوت و همکاران (۲۰۲۳)، و ووکو و همکاران (۲۰۲۵)، بر اهمیت ظرفیت دانشی هیئت‌مدیره در حاکمیت و نظارت سایبری تأکید داشته‌اند. تفاوت نتیجه حاضر با این مطالعات را می‌توان با تمایز میان «دانش» و «اقدام حاکمیتی» توضیح داد.

به بیان دیگر، اعضای هیئت‌مدیره ممکن است از دانش و آگاهی مناسبی درباره ریسک‌های سایبری برخوردار باشند، اما این دانش تنها زمانی می‌تواند بر اثربخشی حسابرسی اثرگذار شود که به تصمیم‌گیری، تخصیص منابع، حمایت از استقلال حسابرسی، مطالبه پاسخگویی و پیگیری اقدامات اصلاحی تبدیل شود. بنابراین، غیرمعنادار بودن اثر مستقیم این متغیر را نباید به معنای بی‌اهمیت بودن شایستگی هیئت‌مدیره تلقی کرد. یافته حاضر بیشتر نشان می‌دهد که نقش این شایستگی ممکن است در تعامل با سایر سازوکارهای حاکمیتی ظاهر شود.

این تفسیر با معنادار بودن همزمان حمایت هیئت‌مدیره در مدل حاضر نیز سازگار است. به عبارت دیگر، ممکن است «دانستن» درباره ریسک سایبری به‌تنهایی کافی نباشد و «حمایت و اقدام» شرط لازم برای تبدیل دانش حاکمیتی به پیامدهای عملی حسابرسی باشد. بررسی این احتمال، به‌ویژه از طریق آزمون اثرهای میانجی یا تعدیلگر در مطالعات آینده، می‌تواند مسیر پژوهشی مهمی باشد.

بحث و مقایسه فرضیه سوم: حمایت هیئت‌مدیره

نتایج نشان داد حمایت هیئت‌مدیره اثر مثبت و معناداری بر اثربخشی حسابرسی سایبری دارد. این یافته با ادبیات اثربخشی حسابرسی داخلی سازگار است؛ زیرا حمایت ارکان حاکمیتی می‌تواند از طریق فراهم کردن منابع، تسهیل دسترسی به اطلاعات، حمایت از استقلال حسابرسی و الزام مدیریت به پیگیری یافته‌های حسابرسی، ظرفیت حرفه‌ای حسابرس را به نتایج عملی تبدیل کند.

یافته حاضر با نتایج ووکو و همکاران (۲۰۲۵)، نیز هم‌راستا است که حمایت حاکمیتی را در زمره عوامل مؤثر بر اثربخشی حسابرسی سایبری قرار داده‌اند. همچنین با مطالعات کلاسیک‌تر درباره اثربخشی حسابرسی داخلی، از جمله گودوین (۲۰۰۳)، و کوهن و سایگ (۲۰۱۰)، هماهنگ است که نقش حمایت مدیریت و ارکان حاکمیتی را در افزایش اثربخشی فعالیت حسابرسی برجسته کرده‌اند.

اهمیت این یافته در محیط سایبری بیشتر است؛ زیرا حسابرسی سایبری ممکن است به دسترسی به اطلاعات فنی، همکاری واحدهای فناوری و امنیت اطلاعات، منابع تخصصی و پیگیری اقدامات اصلاحی نیاز داشته باشد. در نتیجه، حمایت هیئت‌مدیره می‌تواند شرایط سازمانی لازم برای استفاده مؤثر از ظرفیت حسابرسی را فراهم کند.

بحث و مقایسه فرضیه چهارم: همکاری با خطوط دفاعی

قوی‌ترین رابطه مستقیم در مدل مربوط به همکاری با خطوط دفاعی بود و فرضیه چهارم تأیید شد. این یافته با منطق مدل سه خط و نظریه هماهنگی سازمانی سازگار است. ریسک سایبری ماهیتی چندبعدی دارد و اطلاعات مرتبط با آن میان واحدهای عملیاتی، مدیریت ریسک، امنیت اطلاعات، فناوری اطلاعات و حسابرسی توزیع شده است. در چنین شرایطی، اثربخشی حسابرسی به توانایی حسابرس در دسترسی به اطلاعات مناسب و برقراری ارتباط مؤثر با سایر خطوط دفاعی وابسته است.

نتیجه حاضر با یافته‌های استاینبارت و همکاران (۲۰۱۸)، درباره اهمیت رابطه میان حسابرسی داخلی و امنیت اطلاعات و همچنین با تأکید اسالپنیچار و همکاران (۲۰۲۳)، بر هماهنگی و توزیع مسئولیت در حاکمیت سایبری هم‌راستا است.

www.jamv.ir
ISSN: 2645-4572

همچنین، هم‌جهتی با نتایج ووکو و همکاران (۲۰۲۵)، نشان می‌دهد همکاری میان خطوط دفاعی می‌تواند یکی از سازوکارهای مهم برای افزایش اثربخشی حسابرسی سایبری باشد.
البته منظور از همکاری در این پژوهش ادغام نقش‌ها یا تضعیف استقلال حسابرسی نیست. همکاری اثربخش باید همراه با تفکیک مسئولیت‌ها و حفظ استقلال حرفه‌ای حسابرس باشد. تبادل اطلاعات، هماهنگی ارزیابی ریسک، جلوگیری از هم‌پوشانی غیرضروری فعالیت‌های اطمینان‌بخشی و پیگیری یافته‌ها، مهم‌ترین سازوکارهایی هستند که می‌توانند از طریق آنها همکاری میان خطوط دفاعی به اثربخشی بیشتر حسابرسی سایبری منجر شود.

جمع‌بندی و تبیین الگوی کلی یافته‌ها

الگوی کلی نتایج نشان می‌دهد اثربخشی حسابرسی سایبری در نمونه مورد مطالعه حاصل ترکیب سه نوع ظرفیت است: ظرفیت حرفه‌ای حسابرس، حمایت حاکمیتی و هماهنگی سازمانی. شایستگی حسابرسان بیانگر توانایی حرفه‌ای برای انجام مؤثر حسابرسی است؛ حمایت هیئت‌مدیره زمینه سازمانی لازم برای استفاده از این توانایی را فراهم می‌کند؛ و همکاری با خطوط دفاعی دسترسی به اطلاعات و هماهنگی لازم برای پوشش مؤثر ریسک را تقویت می‌کند. در مقابل، غیرمعنادار بودن اثر مستقیم شایستگی هیئت‌مدیره نشان می‌دهد ظرفیت دانشی در سطح حاکمیت ممکن است بدون وجود سازوکارهای حمایتی و اجرایی، اثر مستقیمی بر اثربخشی حسابرسی نداشته باشد. از این منظر، یافته‌های پژوهش میان «ظرفیت بالقوه» و «ظرفیت بالفعل» تمایز ایجاد می‌کند: دانش می‌تواند ظرفیت بالقوه ایجاد کند، اما حمایت و سازوکارهای همکاری ممکن است تعیین کنند که این ظرفیت تا چه اندازه به نتیجه عملی تبدیل شود. این تفسیر با مبانی نظری پژوهش نیز سازگار است. نظریه سرمایه انسانی نقش قابلیت‌های حرفه‌ای را توضیح می‌دهد، نظریه وابستگی به منابع اهمیت ظرفیت حاکمیتی را روشن می‌کند، نظریه حمایت سازمانی نقش حمایت ارکان سازمانی را تبیین می‌کند و نظریه هماهنگی سازمانی اهمیت ارتباط و همکاری میان واحدها را توضیح می‌دهد. بنابراین، استفاده همزمان از این دیدگاه‌ها امکان تبیین چندسطحی اثربخشی حسابرسی سایبری را فراهم می‌کند.

نوآوری و سهم پژوهش

سهم اصلی پژوهش حاضر در سه سطح قابل بیان است. نخست، پژوهش به‌جای تمرکز صرف بر وجود یا میزان اجرای حسابرسی فناوری اطلاعات، اثربخشی حسابرسی سایبری را به‌عنوان پیامد اصلی بررسی می‌کند و آن را در امتداد ادبیات سنجش اثربخشی حسابرسی سایبری توسعه می‌دهد (اسلپنیچار و همکاران، ۲۰۲۲). دوم، چهار ظرفیت حرفه‌ای و حاکمیتی شامل شایستگی حسابرسان، شایستگی هیئت‌مدیره، حمایت هیئت‌مدیره و همکاری با خطوط دفاعی به‌صورت هم‌زمان در یک مدل تجربی بررسی شده‌اند؛ بنابراین پژوهش میان ادبیات حسابرسی داخلی، حاکمیت سایبری و مدل سه خط ارتباط برقرار می‌کند. سوم، پژوهش شواهد تجربی از بستر ایران ارائه می‌دهد و نشان می‌دهد برخی سازوکارهای شناسایی‌شده در مطالعات بین‌المللی، مانند حمایت هیئت‌مدیره و همکاری با خطوط دفاعی، در این محیط نیز اهمیت دارند، در حالی که اثر شایستگی هیئت‌مدیره ممکن است به شرایط نهادی و میزان تبدیل دانش به اقدام وابسته باشد. از این رو، ارزش افزوده پژوهش نه صرفاً در تکرار یک مدل خارجی، بلکه در آزمون و تفسیر مجدد روابط آن در یک زمینه نهادی متفاوت است.

نتیجه‌گیری

www.jamv.ir
ISSN: 2645-4572

در مجموع، نتایج این نمونه نشان می‌دهد اثربخشی حسابرسی سایبری با مجموعه‌ای از ظرفیت‌های حرفه‌ای، حمایت حاکمیتی و هماهنگی سازمانی ارتباط دارد. همکاری با خطوط دفاعی بیشترین ضریب مسیر و بزرگ‌ترین اندازه اثر نسبی را در مدل داشت و پس از آن شایستگی حسابرسان و حمایت هیئت‌مدیره قرار گرفتند. عدم معناداری اثر مستقیم شایستگی هیئت‌مدیره نیز نشان می‌دهد که دانش حاکمیتی، در این نمونه، بدون سازوکارهای حمایت و اقدام الزاماً به اثربخشی بالاتر منجر نشده‌است. با توجه به مقطعی و خودگزارشی. بودن داده‌ها، این یافته‌ها باید به‌عنوان روابط آماری در نمونه حاضر تفسیر شوند و نه شواهد قطعی علیت.

دلالت‌های کاربردی و توصیه به مدیران

بر اساس نتایج، سازمان‌ها باید توسعه شایستگی حسابرسان سایبری را در اولویت قرار دهند. آموزش مستمر در زمینه امنیت سایبری، فناوری اطلاعات، ارزیابی کنترل‌های فناوری، تحلیل شواهد دیجیتال و مدیریت ریسک سایبری می‌تواند ظرفیت حرفه‌ای حسابرسان را تقویت کند.

همچنین، حمایت هیئت‌مدیره باید از حمایت نمادین فراتر رود و در قالب تخصیص منابع کافی، تضمین استقلال حسابرسی، فراهم کردن دسترسی مناسب به اطلاعات و مطالبه پیگیری اقدامات اصلاحی نمود پیدا کند.

در خصوص همکاری با خطوط دفاعی نیز پیشنهاد می‌شود سازوکارهای رسمی و مستمر برای تبادل اطلاعات میان خطوط اول و دوم دفاع، واحدهای فناوری و امنیت اطلاعات، مدیریت ریسک و حسابرسی داخلی ایجاد شود. این سازوکارها باید ضمن جلوگیری از موازی‌کاری، استقلال و مسئولیت حرفه‌ای هر یک از خطوط دفاعی را حفظ کنند.

در نهایت، با توجه به غیرمعنادار بودن اثر مستقیم شایستگی هیئت‌مدیره، سازمان‌ها نباید صرف برخورداری اعضای هیئت‌مدیره از دانش سایبری را کافی تلقی کنند. لازم است این دانش به تصمیم‌گیری، تخصیص منابع، نظارت، مطالبه پاسخگویی و پیگیری اقدامات اصلاحی تبدیل شود. به این ترتیب، ظرفیت دانشی هیئت‌مدیره می‌تواند از یک ویژگی بالقوه به یک سازوکار عملی حاکمیت سایبری تبدیل شود.

منابع

- ✓ احمدی، مجتبی، پورابراهیمی، علیرضا، ریاضی، لادن، امین‌موسوی، سید عبدالله، (۱۴۰۳)، چالش‌های اجرای فرآیند حسابرسی فناوری اطلاعات در شبکه بانکی ایران.
- ✓ جعفریان، مرضیه، سلیمی، پیام، (۱۴۰۴)، تأثیر حسابرسی داخلی الکترونیک مبتنی بر حاکمیت فناوری اطلاعات در کاهش ریسک‌های حسابرسی در سازمان‌های بخش عمومی، حسابداری و بودجه‌ریزی بخش عمومی، دوره ۶، شماره ۲، صص ۱-۲۷.
- ✓ حیدری، صدیقه، برزگر، مجید، محمدداودی، امیرحسین، (۱۴۰۲)، شناسایی عوامل مؤثر بر فرهنگ و آگاهی امنیت سایبری با استفاده از تحلیل مضمون، پدافند الکترونیکی و سایبری، دوره ۱۱، شماره ۱، صص ۶۷-۸۰.
- ✓ شکرخواه، جواد، موسوی‌بصیر، سید حمید، (۱۴۰۳)، چارچوب کنترل داخلی یکپارچه در عصر سایبری و حسابرسی ریسک سایبری، پژوهش‌های حسابرسی حرفه‌ای، دوره ۴، شماره ۱۴، صص ۱۵۴-۱۵۸.
- ✓ Al-Twaijry, A. A. M., Brierley, J. A., & Gwilliam, D. R. (2003). The development of internal audit in Saudi Arabia: An institutional theory perspective. Critical Perspectives on Accounting, 14(5), 507–531.

- ✓ Alzeban, A., Al-Hajaya, K., Sawan, N., Chammaa, H., & Foster, S. (2026). The quality of cybersecurity audits: Do synergies among the chief audit executive, IT governance and internal audit functions matter? Managerial Auditing Journal, 41(2), 322–349.
- ✓ Alzeban, A., & Gwilliam, D. (2014). Factors affecting the internal audit effectiveness: A survey of the Saudi public sector. Journal of International Accounting, Auditing and Taxation, 23(2), 74–86.
- ✓ Arena, M., & Azzone, G. (2009). Identifying organizational drivers of internal audit effectiveness. International Journal of Auditing, 13(1), 43–60.
- ✓ Becker, G. S. (1964). Human capital: A theoretical and empirical analysis, with special reference to education. University of Chicago Press.
- ✓ Benaroch, M., & Fink, L. (2021). No rose without a thorn: Board IT competence and market reactions to operational IT failures. Information & Management, 58(8), 103546
- ✓ Calvin, C., Eulerich, M., & Holt, M. (2025). Characteristics of cybersecurity and IT involvement by the IA activity. International Journal of Accounting Information Systems, 56, 100726
- ✓ Cheung, G. W., Cooper-Thomas, H. D., Lau, R. S., & Wang, L. C. (2024). Reporting reliability, convergent and discriminant validity with structural equation modeling: A review and best-practice recommendations. Asia Pacific Journal of Management, 41(2), 745–783. https://doi.org/10.1007/s10490-023-09871-y
- ✓ Cohen, A., & Sayag, G. (2010). The effectiveness of internal auditing: An empirical examination of its determinants in Israeli organisations. Australian Accounting Review, 20(3), 296–307. https://doi.org/10.1111/j.1835-2561.2010.00092.x
- ✓ Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. Journal of Financial Economics, 147(2), 432–448. https://doi.org/10.1016/j.jfineco.2022.12.002
- ✓ DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160. https://doi.org/10.2307/2095101
- ✓ Eisenberger, R., Huntington, R., Hutchison, S., & Sowa, D. (1986). Perceived organizational support. Journal of Applied Psychology, 71(3), 500–507. https://doi.org/10.1037/0021-9010.71.3.500
- ✓ Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. The Review of Financial Studies, 36(1), 351–407. https://doi.org/10.1093/rfs/hhac024
- ✓ Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39–50. https://doi.org/10.1177/002224378101800104
- ✓ Gale, M., Bongiovanni, I., & Slapničar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. Computers & Security, 121, 102840. https://doi.org/10.1016/j.cose.2022.102840
- ✓ Gao, L., & Calderon, T. G. (2025). Cybersecurity risk governance and companies' cybersecurity risk disclosures in their 10-K filings. Journal of Accounting and Public Policy, 54, 107376. https://doi.org/10.1016/j.jaccpubpol.2025.107376
- ✓ Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. Journal of Risk and Insurance, 89(3), 725–763. https://doi.org/10.1111/jori.12381
- ✓ Goodwin, J. (2003). The relationship between the audit committee and the internal audit function: Evidence from Australia and New Zealand. International Journal of Auditing, 7(3), 263–278. https://doi.org/10.1046/j.1099-1123.2003.00074.x

- ✓ Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). A primer on partial least squares structural equation modeling (PLS-SEM) (3rd ed.). SAGE.
- ✓ Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43, 115–135. https://doi.org/10.1007/s11747-014-0403-8
- ✓ Hillman, A. J., & Dalziel, T. (2003). Boards of directors and firm performance: Integrating agency and resource dependence perspectives. Academy of Management Review, 28(3), 383–396. https://doi.org/10.5465/amr.2003.10196729
- ✓ Institute of Internal Auditors. (2020). The IIA's Three Lines Model: An update of the Three Lines of Defense. https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/
- ✓ Institute of Internal Auditors. (2024). Global Internal Audit Standards. https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/
- ✓ Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. Managerial Auditing Journal, 33(4), 377–409. https://doi.org/10.1108/MAJ-07-2017-1595
- ✓ Kahyaoglu, S. B., & Caliyurt, K. T. (2018). Cyber security assurance process from the internal audit perspective. Managerial Auditing Journal, 33(4), 360–376. https://doi.org/10.1108/MAJ-02-2018-1804
- ✓ Lenz, R., & Hahn, U. (2015). A synthesis of empirical internal audit effectiveness literature pointing to new research opportunities. Managerial Auditing Journal, 30(1), 5–33. https://doi.org/10.1108/MAJ-08-2014-1072
- ✓ Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. ACM Computing Surveys, 26(1), 87–119. https://doi.org/10.1145/174666.174668
- ✓ National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
- ✓ Pfeffer, J., & Salancik, G. R. (1978). The external control of organizations: A resource dependence perspective. Harper & Row. https://books.google.com/books?id=iZv79yE--5EC
- ✓ Podsakoff, P. M., Podsakoff, N. P., Williams, L. J., Huang, C., & Yang, J. (2024). Common method bias: It's bad, it's complex, it's widespread, and it's not easy to fix. Annual Review of Organizational Psychology and Organizational Behavior, 11, 17–61. https://doi.org/10.1146/annurev-orgpsych-110721-040030
- ✓ Proudfoot, J. G., Cram, W. A., Madnick, S., & Coden, M. (2023). The importance of board member actions for cybersecurity governance and risk management. MIS Quarterly Executive, 22(4), Article 6. https://aisel.aisnet.org/misqe/vol22/iss4/6/
- ✓ Scott, W. R. (2014). Institutions and organizations: Ideas, interests, and identities (4th ed.). SAGE. https://us.sagepub.com/en-us/nam/institutions-and-organizations/book237665
- ✓ Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. International Journal of Accounting Information Systems, 51, 100642. https://doi.org/10.1016/j.accinf.2023.100642
- ✓ Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548. https://doi.org/10.1016/j.accinf.2021.100548
- ✓ Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. International Journal of Accounting Information Systems, 13(3), 228–243. https://doi.org/10.1016/j.accinf.2012.06.007

- ✓ Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. Accounting, Organizations and Society, 71, 15–29. https://doi.org/10.1016/j.aos.2018.04.005
- ✓ Verizon. (2025). 2025 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
- ✓ Vuko, T., Slapničar, S., Čular, M., & Drašček, M. (2025). Key drivers of cybersecurity audit effectiveness: A neo-institutional perspective. International Journal of Auditing, 29(1), 188–206. https://doi.org/10.1111/ijau.12365
- ✓ World Economic Forum. (2025). Global Cybersecurity Outlook 2025. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
- ✓ Zheng, G., Xia, Z., He, F., & Xiao, Z. (2025). The audit committee's IT expertise and its impact on the disclosure of cybersecurity risk. Research in International Business and Finance, 73, 102542.