فصلنامه چشم انداز حسابداری و مدیریت
دوره ۹، شماره ۱۱۷، تابستان ۱۴۰۵ (جلد سوم)

www.jamv.ir
ISSN: 2645-4572

چشم انداز حسابداری و مدیریت (دوره نهم)
شماره ۱۱۷/ تابستان ۱۴۰۵ (جلد سوم)/ صص ۱۶۸-۱۸۲

بررسی عوامل مؤثر بر مشارکت حسابرسی داخلی در حسابرسی فناوری اطلاعات و امنیت سایبری

غلامرضا سلیمانی امیری
استاد گروه حسابداری، دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا (س)، تهران، ایران.
gh.soleymani@alzahra.ac.ir
مهدیس ناصری
دانشجوی دکتری حسابداری، گروه حسابداری، دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا (س)، تهران، ایران.
(نویسنده مسئول).
Mahdisnaseri901@gmail.com

چکیده
پژوهش حاضر با هدف بررسی عوامل مؤثر بر مشارکت حسابرسی داخلی در حسابرسی فناوری اطلاعات و امنیت سایبری می باشد. روش پژوهش از نظر هدف کاربردی و از حیث روش، توصیفی- همبستگی است. جامعه آماری شامل کلیه حسابرسان داخلی شاغل در شرکت‌های ایرانی (بورسی، دولتی، خصوصی بزرگ و موسسات مستقل) با حداقل سه سال سابقه فعالیت و آشنایی با مفاهیم فناوری اطلاعات و امنیت سایبری است. به دلیل تخصصی بودن جامعه و محدودیت دسترسی، نمونه گیری غیرتصادفی هدفمند (قضاوتی) همراه با نمونه گیری در دسترس انجام شد و حجم نمونه ۱۵۰ نفر تعیین گردید که برای مدلسازی معادلات ساختاری با نرم افزار SMARTPLS3 کفایت آماری دارد. ابزار گردآوری داده‌ها پرسشنامه ای استاندارد با مقیاس ۵ درجه لیکرت بود که روایی محتوایی و سازه (همگرا و واگرا) آن تایید و پایایی آن از طریق آلفای کرونباخ و پایایی ترکیبی (CR) مورد سنجش و تایید قرار گرفت. نتایج نشان داد که بلوغ حسابرسی داخلی، دسترسی به دانش تخصصی فناوری اطلاعات و حمایت مدیریت ارشد تاثیر مثبت و معناداری بر مشارکت حسابرسی داخلی در حوزه فناوری اطلاعات و امنیت سایبری دارند. فرضیه مربوط به تاثیر شایستگی فناوری اطلاعات حسابرسان داخلی رد شد که حاکی از آن است که مهارت فردی به تنهایی بدون پشتیبانی سازمانی و دسترسی به منابع دانشی منجر به مشارکت موثر نمی شود.

واژگان کلیدی: حسابرسی داخلی، امنیت سایبری، فناوری اطلاعات، مشارکت حسابرسی.

مقدمه
در دهه اخیر، مفهوم امنیت سایبری از یک دغدغه فنی صرف، به یکی از ارکان حیاتی مدیریت راهبردی سازمان‌ها تبدیل شده است. امروزه ریسک‌های سایبری به عنوان برجسته ترین دسته از ریسک‌های کسب وکار شناخته می شوند که نه تنها تداوم عملیات را تهدید می کنند، بلکه سلامت مالی و اعتبار سازمان را نیز به مخاطره می اندازند (والتون[1] و

[1] Walton

www.jamv.ir
ISSN: 2645-4572

همکاران، ۲۰۲۱). حملات سایبری می توانند منجر به توقف کامل فعالیت‌های تجاری شوند و آسیب‌های جبران ناپذیری به ساختار اقتصادی شرکت وارد کنند (سیایا[1] و همکاران، ۲۰۲۵). علاوه بر این، نقض حریم خصوصی داده‌هایی که در اختیار سازمان هستند، لزوما متعلق به خود سازمان نبوده و می توانند مشکلات امانتی و اخلاقی شدیدی ایجاد کنند که مدل کسب وکار را زیر سوال می برد (هپورس[2] و همکاران، ۲۰۲۲). با توجه به کمبود متخصصان فناوری اطلاعات در هیئت مدیره‌ها، شوراها و کمیته‌های حسابرسی ناچارند برای حاکمیت سیستم‌های فناوری اطلاعات و مدیریت ریسک‌های سایبری، به شرکای دیگر تکیه کنند. در این میان، واحد حسابرسی داخلی با ارائه خدمات اطمینان بخشی مستقل و عینی، نقش کلیدی در بهبود حاکمیت، مدیریت ریسک و کنترل‌های داخلی ایفا می کند (اولریچ[3]، ۲۰۲۱). دامنه فعالیت این واحد طیف وسیعی از فعالیت‌های سازمانی را پوشش می دهد و حسابرسان داخلی می توانند منبع ارزشمندی برای ارائه خدمات اطمینان بخشی مرتبط با فناوری اطلاعات، از جمله امنیت اطلاعات، امنیت سایبری و اطمینان بخشی مستمر فناوری اطلاعات باشند (استینبارت[4] و همکاران، ۲۰۱۸).

ارزش افزوده ای که واحد حسابرسی داخلی ایجاد می کند، در توانایی اعضای این حرفه برای کمک به هیئت مدیره و مدیریت ارشد جهت دستیابی به اهداف سازمانی از طریق ارائه اطمینان بخشی مستقل درباره فرآیندهای مدیریت ریسک، کنترل و حاکمیت نهفته است. اگرچه نقش سنتی حسابرسی داخلی بیشتر بر گزارش دهی مالی متمرکز بوده و تاثیر مثبت آن بر این حوزه ثابت شده است (اگ[5]، ۲۰۱۵) و همچنین توانایی کاهش سطح ریسک شرکت مورد تایید قرار گرفته است (کارسلو[6] و همکاران، ۲۰۱۸)، اما بحث‌های جدیدی پیرامون نقش واحد حسابرسی داخلی در امنیت سایبری و حفاظت از سیستم‌های اطلاعاتی سازمان شکل گرفته است (اسلپنیکار[7] و همکاران، ۲۰۲۲ و ۲۰۲۳). نهادهای تعیین استاندارد توصیه می کنند که واحدهای حسابرسی داخلی باید همانند پیاده سازی سایر راهبردهای کاهش ریسک، در این حوزه مشارکت فعال داشته باشند. برای مثال، مؤسسه حسابرسان داخلی (IIA) ادبیات گسترده ای منتشر کرده است که نشان دهنده ضرورت مشارکت بیشتر حسابرسان داخلی در سیستم‌های فناوری اطلاعات و اطمینان بخشی به کنترل‌های امنیت سایبری و فناوری اطلاعات (ITCSA) است (IIA, 2022, 2016). همزمان با این فشار نهادی، دلایل اقتصادی نیز بر مشارکت بیشتر واحد حسابرسی داخلی در ITCSA تاکید دارند؛ چرا که نقض‌ها و شکست‌ها می توانند هزینه‌های مالی و شهرتی سنگینی به همراه داشته باشند. (کالوین[8] و همکاران، ۲۰۲۵).

با وجود اینکه مزایای پیوند دادن فعالیت‌های حسابرسی داخلی با حسابرسی فناوری اطلاعات و امنیت سایبری آشکار به نظر می رسد و نهادهای استانداردگذار چارچوب‌های لازم را ترسیم کرده اند (IIA, 2017, 2020, 2022)، اما همسویی در عمل هنوز بسیار دور از مسیر مطلوب است (بوزکوس[9] و همکاران، ۲۰۱۸). با دیجیتالی شدن فرآیندهای شرکتی، مطالعات حرفه ای فعلی، امنیت سایبری را به عنوان ریسک شماره یک شرکت‌ها رتبه بندی کرده است (ECIIA, 2022). طراحی ضعیف کنترل‌های سیستم اطلاعاتی می تواند منجر به سیستم‌های غیرقابل اعتماد شود که حتی بدون سوءنیت نیز به سازمان آسیب می رسانند. همچنین حملات سایبری مخرب همچنان در حال افزایش است (World

[1] Siyaya
[2] Hepworth
[3] Eulerich
[4] Steinbart
[5] Ege
[6] Carcello
[7] Slapničar
[8] Calvin
[9] Bozkus

www.jamv.ir
ISSN: 2645-4572

Economic Forum, 2022). بنابراین، سازمان‌ها باید پروفایل ریسک کلی فناوری اطلاعات و امنیت سایبری خود را به طور مداوم ارزیابی کنند تا در برابر حملات و سایر ریسک‌های ذاتی آماده باشند. واحد حسابرسی داخلی نیز با درک انتظارات سازمان برای خلق ارزش، می تواند از طریق کاهش فراوانی و پیامدهای حوادث مرتبط با فناوری اطلاعات و امنیت سایبری، به این هدف کمک کند (بنتلیون[1] و همکاران، ۲۰۲۱). به عبارت دیگر، تمام ریسک‌های مرتبط با فناوری اطلاعات یک سازمان می تواند در دامنه واحد حسابرسی داخلی باشد، از جمله سیستم‌های فناوری اطلاعات، حاکمیت فناوری اطلاعات و حسابرسی‌های امنیت سایبری (دزورنانین و مالائسکو[2]، ۲۰۱۶).

برای اینکه واحد حسابرسی داخلی بتواند در ITCSA مشارکت کند، نیاز به حمایت مناسب از سوی سازمان دارد. شرکت‌هایی که برای واحد حسابرسی داخلی ارزش قائل شده و رشد و پیشرفت آن را حمایت می کنند، تمایل دارند واحدهای حسابرسی داخلی با بلوغ بالاتری داشته باشند که قابلیت مشارکت در حوزه‌های جدیدتری مانند ITCSA را دارا باشند (کالوین و همکاران، ۲۰۲۵). علاوه بر رسیدن به سطح مشخصی از بلوغ، دانش یک بعد کلیدی دیگر است که برای مشارکت واحدهای حسابرسی داخلی در ITCSA مورد نیاز است. ابوت[3] و همکاران (۲۰۱۶)، شایستگی را جزء لاینفک اثربخشی واحد حسابرسی داخلی میدانند و این پرسش وجود دارد که آیا واحدهای حسابرسی داخلی مهارت‌های لازم را دارند یا می توانند آنها را کسب کنند. حتی اگر یک واحد حسابرسی داخلی به اندازه کافی بالغ باشد، اگر کارکنان با مهارت‌های لازم فناوری اطلاعات و امنیت سایبری نداشته باشد و نتواند این مهارت‌ها را برون سپاری کند (به دلیل تقاضای بالا)، قادر به مشارکت در ITCSA نخواهد بود. از سوی دیگر، نهادهای حاکمیتی مانند کمیته‌های حسابرسی اغلب به دلیل فقدان تخصص داخلی و خارج بودن اطمینان بخشی از دامنه هیئت مدیره، برای کمک به حاکمیت فناوری اطلاعات و امنیت سایبری به واحدهای حسابرسی داخلی تکیه می کنند (سیایا و همکاران، ۲۰۲۵).

علیرغم تاکیدات مکرر نهادهای حرفه ای بر نقش حیاتی حسابرسی داخلی در مقابله با ریسک‌های سایبری، شواهد حاکی از آن است که میزان مشارکت واقعی واحدهای حسابرسی داخلی در ایران و به طور خاص در شرکت‌های ایرانی، همسو با این انتظارات نیست. درحالیکه ادبیات موجود (کالوین و همکاران، ۲۰۲۵) ویژگی‌هایی مانند بلوغ واحد حسابرسی، شایستگی‌های فناوری اطلاعات و دسترسی به دانش تخصصی را به عنوان عوامل موثر شناسایی کرده است، اما بومی سازی این مدل در بافت فرهنگی و ساختاری شرکت‌های ایرانی ضروری به نظر می رسد. بنابراین، این پژوهش با هدف پر کردن این خلأ دانشی به بررسی عوامل مؤثر بر مشارکت حسابرسی داخلی در حسابرسی فناوری اطلاعات و امنیت سایبری می پردازد. براین اساس، فرضیه‌های زیر مطرح شده و مدل پژوهشی به شکل ۱ ارائه می گردد:

فرضیه اول: بلوغ حسابرسی داخلی تاثیر مثبت و معناداری بر مشارکت حسابرسی داخلی در حسابرسی فناوری اطلاعات و امنیت سایبری دارد.

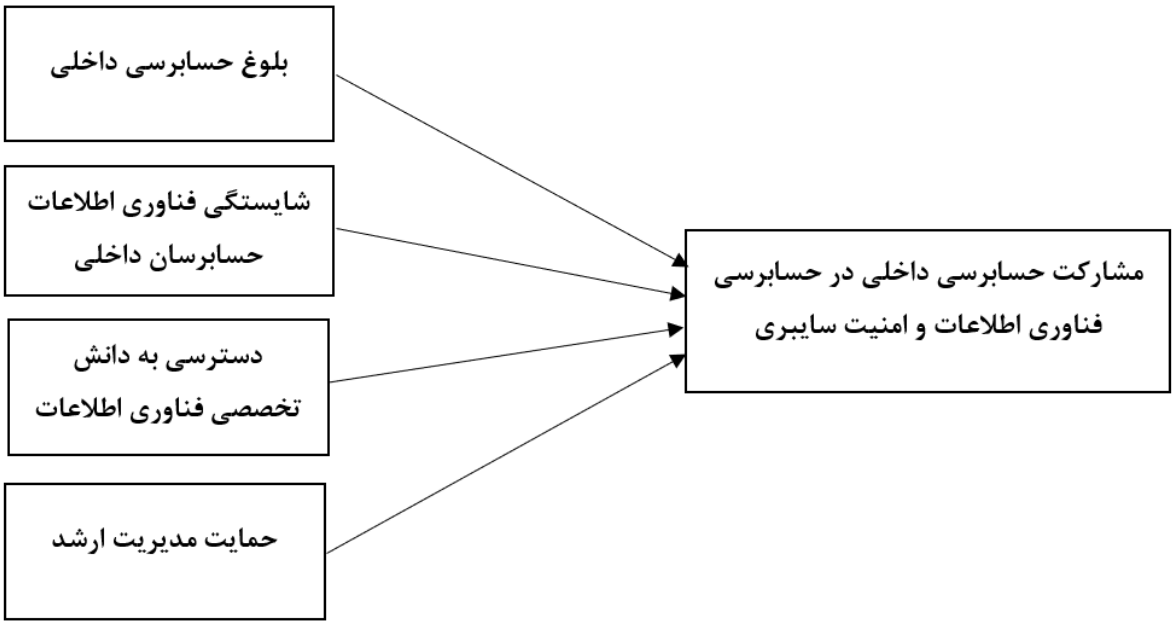
فرضیه دوم: شایستگی فناوری اطلاعات حسابرسان داخلی تاثیر مثبت و معناداری بر مشارکت حسابرسی داخلی در حسابرسی فناوری اطلاعات و امنیت سایبری دارد.

فرضیه سوم: دسترسی به دانش تخصصی فناوری اطلاعات تاثیر مثبت و معناداری بر مشارکت حسابرسی داخلی در حسابرسی فناوری اطلاعات و امنیت سایبری دارد.

[1] Bantleon
[2] Dzuranin & Mălăescu
[3] Abbott

www.jamv.ir
ISSN: 2645-4572

فرضیه چهارم: حمایت مدیریت ارشد تاثیر مثبت و معناداری بر مشارکت حسابرسی داخلی در حسابرسی فناوری اطلاعات و امنیت سایبری دارد.



شکل (۱): مدل مفهومی پژوهش

پیشینهٔ پژوهش

واحد حسابرسی داخلی (IAF[1]) به عنوان بازوی نظارتی مستقل، نقشی حیاتی در تضمین اثربخشی فرآیندهای مدیریت ریسک و حاکمیت ایفا می کند (عبدالرئوف[2] و همکاران، ۲۰۲۵). با اینحال، ادبیات موجود نشان می دهد که واحدهای حسابرسی داخلی کم تجربه یا دارای بلوغ پایین، معمولا بر وظایف سنتی و هسته ای خود متمرکز بوده و پیش از افزودن مسئولیت‌های اضافی مانند حسابرسی فناوری اطلاعات ، نیاز دارند که پایه‌های اصلی فعالیت خود را مستحکم کنند. شرکت‌هایی که برای واحد حسابرسی داخلی ارزش قائل بوده و رشد آن را حمایت میکنند، تمایل دارند واحدهایی با بلوغ بالاتر داشته باشند که آمادگی بیشتری برای ورود به حوزه‌های نوپدید مانند امنیت سایبری دارند (کالوین و همکاران، ۲۰۲۵). این دیدگاه نظری توسط مطالعات تجربی تایید می شود؛ بطوریکه وو[3] و همکاران (۲۰۲۴)، در پژوهش خود نشان دادند که ساختارمند بودن فرآیندهای حاکمیت فناوری اطلاعات در داخل واحد حسابرسی، رابطه مثبتی با اثربخشی کنترل‌های عمومی دارد. بنابراین، انتظار میرود هرچه بلوغ ساختاری و فرآیندی واحد حسابرسی داخلی بالاتر باشد، توانایی و تمایل آن برای مشارکت فعال در حسابرسی‌های پیچیده فناوری اطلاعات و امنیت سایبری افزایش یابد.

H1: بلوغ حسابرسی داخلی تاثیر مثبت و معناداری بر مشارکت حسابرسی داخلی در حسابرسی فناوری اطلاعات و امنیت سایبری دارد.

[1] internal audit function
[2] Abdelraouf
[3] Wu

www.jamv.ir
ISSN: 2645-4572

شایستگی و دانش تخصصی، جزء لاینفک اثربخشی واحد حسابرسی داخلی محسوب می شود (ابوت و همکاران، ۲۰۱۶). حتی اگر یک واحد از نظر ساختاری بالغ باشد، اما فاقد کارکنانی با مهارت‌های فنی باشد، قادر به ارائه اطمینان بخشی عمیق در حوزه ITCSA[1] نخواهد بود (کالوین و همکاران، ۲۰۲۵). شکاف مهارتی بین حسابرسی سنتی و نیازهای نوظهور سایبری، نیازمند پر کردن خلأ دانشی است. پژوهش ابراهیمی کردلر و همکاران (۱۴۰۳)، نشان داد که صلاحیت‌های حسابرسی فناوری اطلاعات رابطه مثبت و معناداری با عملکردهای حسابرسی داخلی در زمینه حاکمیت فناوری اطلاعات دارد. همچنین، الزبان[2] و همکاران (۲۰۲۶)، در مطالعه ای دریافتند که تخصص فناوری اطلاعات مدیر ارشد حسابرسی (CAE[3]) به طور معناداری کیفیت امنیت سایبری سازمان را بهبود می بخشد، بطوریکه هر سال اضافه شدن بر تخصص حسابرسی فناوری اطلاعات ، کیفیت ادراک شده امنیت سایبری را افزایش میدهد. این یافته‌ها حاکی از آن است که شایستگی فنی حسابرسان، پیش شرط لازم برای پوشش پیچیدگی‌های تکنولوژیک و مشارکت موثر در این حوزه است.

H2: شایستگی فناوری اطلاعات حسابرسان داخلی تاثیر مثبت و معناداری بر مشارکت حسابرسی داخلی در حسابرسی فناوری اطلاعات و امنیت سایبری دارد.

علاوه بر شایستگی فردی، دسترسی به دانش تخصصی نیز به عنوان یک منبع سازمانی، نقش تعیین کننده ای در توانایی واحد حسابرسی ایفا می کند. این دانش می تواند از طریق آموزش داخلی کارکنان یا برون سپاری تخصص‌های مورد نیاز فراهم شود (کالوین و همکاران، ۲۰۲۵). تحقیقات نشان میدهد که وقتی دانش فناوری اطلاعات در اختیار حسابرسان قرار گیرد، می تواند نقش‌های متمایز حسابرسی داخلی را تقویت کرده و مشارکت آنها را در حاکمیت فناوری اطلاعات افزایش دهد (ابراهیمی کردلر و همکاران، ۱۴۰۳). وو و همکاران (۲۰۲۴)، نیز گزارش کردند که دانش فناوری اطلاعات رابطه مثبت و معناداری با کیفیت رابطه بین واحد حسابرسی داخلی و توابع فناوری اطلاعاتدارد. بنابراین، دسترسی سیستماتیک به دانش تخصصی، نه تنها ابزاری برای رفع نقص‌های آموزشی است، بلکه بستری را فراهم می کند که حسابرسان بتوانند با اطمینان بیشتری در ارزیابی ریسک‌های سایبری و انطباق مقرراتی مشارکت کنند.

H3: دسترسی به دانش تخصصی فناوری اطلاعات تاثیر مثبت و معناداری بر مشارکت حسابرسی داخلی در حسابرسی فناوری اطلاعات و امنیت سایبری دارد.

حمایت مدیریت ارشد و کمیته حسابرسی، کاتالیزگری کلیدی برای جهت دهی به اولویت‌های واحد حسابرسی داخلی است. از آنجا که استانداردهای IIA مستلزم گزارش دهی به هیئت مدیره است، حمایت مدیریتی باعث میشود نیازهای اطمینان بخشی حاکمیت فناوری اطلاعاتدر اولویت برنامه ریزی قرار گیرد (کالوین و همکاران، ۲۰۲۵). با توجه به کمبود متخصصان فناوری اطلاعاتدر سطوح عالی مدیریتی، شوراهای شرکتی اغلب به واحد حسابرسی داخلی تکیه می کنند (بهم[4] و همکاران، ۲۰۱۹). استینبارت و همکاران (۲۰۱۸)، در پژوهش خود دریافتند که سطوح بالاتری از حمایت مدیریت برای امنیت اطلاعات، تاثیر مثبتی بر کیفیت رابطه بین توابع حسابرسی داخلی و امنیت اطلاعات دارد. علاوه براین، کارگرشورکی و مکوندی (۱۴۰۰)، تاکید می کنند که حسابرسی داخلی به عنوان ابزار نظارتی، امکان مدیریت بهتر فعالیت‌ها و تصمیم گیری در شرایط بحرانی را فراهم می کند. بنابراین، زمانیکه مدیریت ارشد منابع لازم (برای آموزش و

[1] information technology systems and cybersecurity controls assurance
[2] Alzeban
[3] Chief Audit Executive
[4] Bhme

www.jamv.ir
ISSN: 2645-4572

جذب نیرو) و انگیزه سازمانی را برای مشارکت در حوزه‌های راهبردی مانند امنیت سایبری ایجاد کند، احتمال مشارکت واحد حسابرسی داخلی در این حوزه‌ها به شدت افزایش می یابد.

H4: حمایت مدیریت ارشد تاثیر مثبت و معناداری بر مشارکت حسابرسی داخلی در حسابرسی فناوری اطلاعات و امنیت سایبری دارد.

روش‌شناسی پژوهش

تحقیق حاضر از نظر هدف، کاربردی و از حیث روش، توصیفی–همبستگی محسوب می‌شود. جامعه آماری این پژوهش را کلیه حسابرسان داخلی شاغل در شرکت‌های ایرانی (اعم از شرکت‌های پذیرفته‌شده در بورس اوراق بهادار تهران، شرکت‌های دولتی، شرکت‌های خصوصی بزرگ و نیز مؤسسات حسابرسی داخلی مستقل) تشکیل می دهند که حداقل دارای سه سال سابقه فعالیت در حوزه حسابرسی داخلی بوده و با مفاهیم حسابرسی فناوری اطلاعات و امنیت سایبری آشنایی دارند. با توجه به تخصصی بودن جامعه آماری و محدودیت‌های دسترسی به تمامی اعضای آن، در این پژوهش از روش نمونه‌گیری غیرتصادفی هدفمند (قضاوتی) همراه با نمونه‌گیری در دسترس استفاده شده است. بدین صورت که پژوهشگر با شناسایی حسابرسان داخلی شاغل در شرکت‌های مختلف از جمله شرکت سحر و سایر شرکت‌های همکار، اقدام به توزیع پرسشنامه نموده است. انتخاب شرکت سحر به عنوان یکی از منابع اصلی نمونه، به دلیل دسترسی مستقیم پژوهشگر به حسابرسان داخلی این شرکت صورت گرفته است و مابقی نمونه از طریق ارتباط با سایر شرکت‌های ایرانی تکمیل گردیده است. برای تعیین حجم نمونه، با توجه به نامعلوم بودن حجم دقیق جامعه و با استناد به رویکردهای رایج در پژوهش‌های مدیریت و حسابداری که از مدلسازی معادلات ساختاری استفاده مینمایند، تعداد ۱۵۰ پرسشنامه به عنوان حجم نمونه مطلوب در نظر گرفته شده است. این تعداد ضمن آنکه از لحاظ آماری برای انجام مدلسازی معادلات ساختاری با نرمافزار SMART PLS3 کفایت لازم را دارد (نیاز به حداقل ۵ تا ۱۰ برابر تعداد گویه‌های پرسشنامه)، امکان تعمیم‌پذیری نسبی نتایج را نیز فراهم می‌آورد. پرسشنامه‌ها به صورت حضوری و الکترونیکی توزیع و پس از تکمیل، جمع‌آوری گردیده است. برای جمع‌آوری داده‌ها از پرسشنامه‌ای استفاده گردید که گویه‌های آن از مقیاس‌های معتبر پژوهش‌های پیشین اقتباس شده است. در این پرسشنامه از مقیاس ۵ درجه لیکرت جهت سنجش متغیرهای مدل مفهومی استفاده گردیده است. این پژوهش با استفاده از نرم‌افزار SMART PLS3 و با روش مدل یابی معادلات ساختاری به بررسی روابط بین متغیرها پرداخته است. عدم نیاز به نرمال بودن توزیع نسبت به سایر نرم‌افزارهای موجود می‌باشد (کلاین، ۲۰۱۵). روایی پرسش‌نامه از طریق روایی محتوایی و سازه مورد ارزیابی و تائید قرار گرفته است. برای سنجش روایی محتوایی[1] ابزار از نظرات اساتید و صاحب‌نظران آگاه به موضوع استفاده شده است و برای سنجش روایی سازه از الگوی معادلات ساختاری[2] از روایی همگرا و واگرا استفاده شده است. به منظور تعیین روایی همگرا[3] از شاخص میانگین انحراف معیار استخراج شده[4] (AVE) و برای سنجش واگرا از شاخص جذر میانگین واریانس استخراج شده استفاده شده است (حسینی و همکاران، ۲۰۲۴). برای سنجش پایایی از آلفای کرونباخ و پایایی ترکیبی استفاده شده است. ضریب آلفای کرونباخ عاملی است که مقدار آن از ۰ تا ۱ متغیر است، مقدار آلفای کرونباخ بالاتر از ۰/۷ (کرونباخ، ۱۹۵۱)،

[1] Content Validity
[2] Structural Equation Modeling(SEM)
[3] Convergent Validity
[4] Average Variance Extracted(AVE)

www.jamv.ir
ISSN: 2645-4572

نشانگر پایایی قابل‌قبول است. پایایی ترکیبی مرکب (CR) توسط ورتس[1] و همکاران (۱۹۷۴) معرفی شد و برتری آن نسبت به آلفای کرونباخ در این است که پایایی سازه‌ها نه به‌صورت مطلق بلکه با توجه به همبستگی سازه‌هایشان با یکدیگر محاسبه می‌گردد. درصورتی‌که مقدار پایایی ترکیبی برای هر سازه بالای ۰/۷ شود، نشان از پایایی درونی مناسب برای مدل‌های اندازه‌گیری دارد و مقدار کمتر از ۰/۶ عدم وجود پایایی را نشان می‌دهد. فورنل و لارکر[2] (۱۹۸۱) معیار میانگین واریانس استخراج شده (AVE) را برای سنجش روایی همگرا معرفی کرده و اظهار داشتند که مقدار عدد بحرانی ۰/۵ است.

یافته‌های پژوهش

بررسی مدل پژوهش طی دو مرحله انجام می‌شود. در مرحله اول، مدل بیرونی پژوهش، در مرحله دوم، مدل درونی پژوهش بررسی شده است.

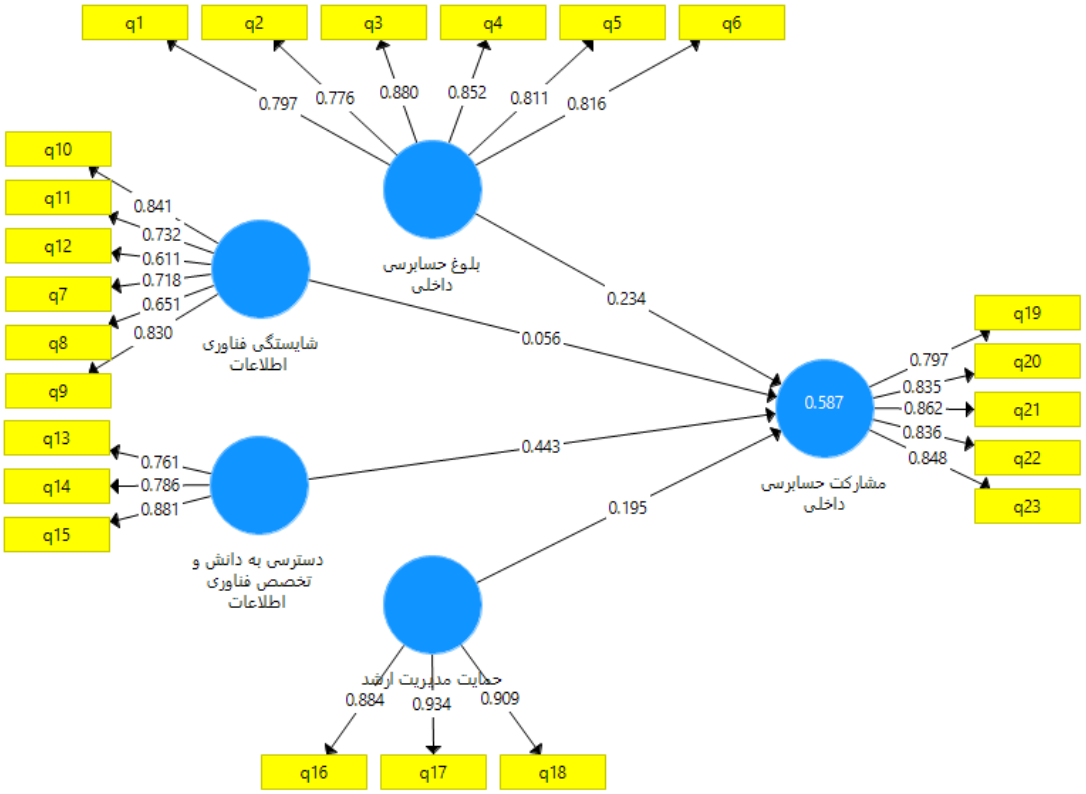
در مرحله اول، بار عاملی مربوط به شاخص‌های سنجیده‌شده هر متغیر، بررسی شد بارهای عاملی بالاتر از ۰/۴ مطلوب هستند. مدل در حالت ضریب مسیر و بارهای عاملی اولیه در جدول و نمودار ۱، نشان داده شده است.

جدول (۱): بارهای عاملی

متغیر	شاخص	ضریب بار عاملی	متغیر	شاخص	ضریب بار عاملی
بلوغ حسابرسی داخلی	q1	۰.۷۹۷	دسترسی به دانش و تخصص فناوری اطلاعات	q13	۰.۷۶۱
	q2	۰.۷۷۶		q14	۰.۷۸۶
	q3	۰.۸۸۰		q15	۰.۸۸۱
	q4	۰.۸۵۲	حمایت مدیریت ارشد	q16	۰.۸۸۴
	q5	۰.۸۱۱		q17	۰.۹۳۴
	q6	۰.۸۱۶		q18	۰.۹۰۹
شایستگی فناوری اطلاعات	q7	۰.۷۱۸	مشارکت حسابرسی داخلی	q19	۰.۷۹۷
	q8	۰.۶۵۱		q20	۰.۸۳۵
	q9	۰.۸۳۰		q21	۰.۸۶۲
	q10	۰.۸۴۱		q22	۰.۸۳۶
	q11	۰.۷۳۲		q23	۰.۸۴۸
	q12	۰.۶۱۱			

[1] Werts
[2] Fornell and Larcker

www.jamv.ir
ISSN: 2645-4572



شکل (۲): مدل معادلات ساختاری حالت تخمین ضرایب استاندارد (بارهای عاملی)

در نرم‌افزار smart pls برای برازش مدل‌های اندازه‌گیری از نظر پایایی معیارهای ضرایب بار عاملی، پایایی مرکب (CR) و برای بررسی روایی همگرای مدل‌های اندازه‌گیری از معیار متوسط اشتراک (AVE) و برای بررسی روایی واگرای این مدل‌ها جدول فورنل و لارکر را ارائه می‌دهد.

در جدول ۲ مقدار ضریب آلفای کرونباخ، پایایی مرکب و معیار متوسط اشتراک برای هر یک از سازه‌ها ارائه شده است.

جدول (۲): کرونباخ آلفا، پایایی ترکیبی و روایی همگرا

AVE	Composite Reliability	Cronbachs Alpha	متغیر
۰.۶۷۷	۰.۹۲۶	۰.۹۰۴	بلوغ حسابرسی داخلی
۰.۸۲۷	۰.۹۳۵	۰.۸۹۵	حمایت مدیریت ارشد
۰.۶۵۸	۰.۸۵۲	۰.۷۴۰	دسترسی به دانش و تخصص فناوری اطلاعات
۰.۵۴۱	۰.۸۷۴	۰.۸۳۷	شایستگی فناوری اطلاعات
۰.۶۹۹	۰.۹۲۱	۰.۸۹۲	مشارکت حسابرسی داخلی

مطابق با جدول ۲ ضریب آلفای کرونباخ برای تمام سازه‌های موردنظر بالاتر از ۰/۷ است که حاکی از پایایی مناسب مدل می‌باشد. همین‌طور مقادیر پایایی ترکیبی برای تمام سازه‌های موردنظر بالاتر از ۰/۷ است که حاکی از پایایی مناسب مدل دارد. مقدار تمام مقادیر AVE بالاتر از ۰/۵ است، پس برازش مدل مناسب است.

همان‌گونه که در جدول ۳ قابل مشاهده است مقدار جذر AVE متغیرهای مکنون در پژوهش حاضر که در خانه‌های موجود در قطر اصلی ماتریس قرار گرفته‌اند از مقدار همبستگی میان آنها که در خانه‌های زیرین و راست قطر بیشتر است که این مطلب بیانگر برازش مناسب مدل‌های اندازه‌گیری از نظر روایی واگرا است.

www.jamv.ir
ISSN: 2645-4572

جدول (۳): جدول فورنل و لاکر

	بلوغ حسابرسی داخلی	حمایت مدیریت ارشد	دسترسی به دانش و تخصص فناوری اطلاعات	شایستگی فناوری اطلاعات	مشارکت حسابرسی داخلی
بلوغ حسابرسی داخلی	۰.۸۲۳				
حمایت مدیریت ارشد	۰.۵۲۶	۰.۹۰۹			
دسترسی به دانش و تخصص فناوری اطلاعات	۰.۵۵۶	۰.۴۸۲	۰.۸۱۱		
شایستگی فناوری اطلاعات	۰.۴۸۵	۰.۴۸۶	۰.۵۰۳	۰.۷۳۵	
مشارکت حسابرسی داخلی	۰.۶۱۰	۰.۵۵۹	۰.۶۹۵	۰.۴۸۷	۰.۸۳۶

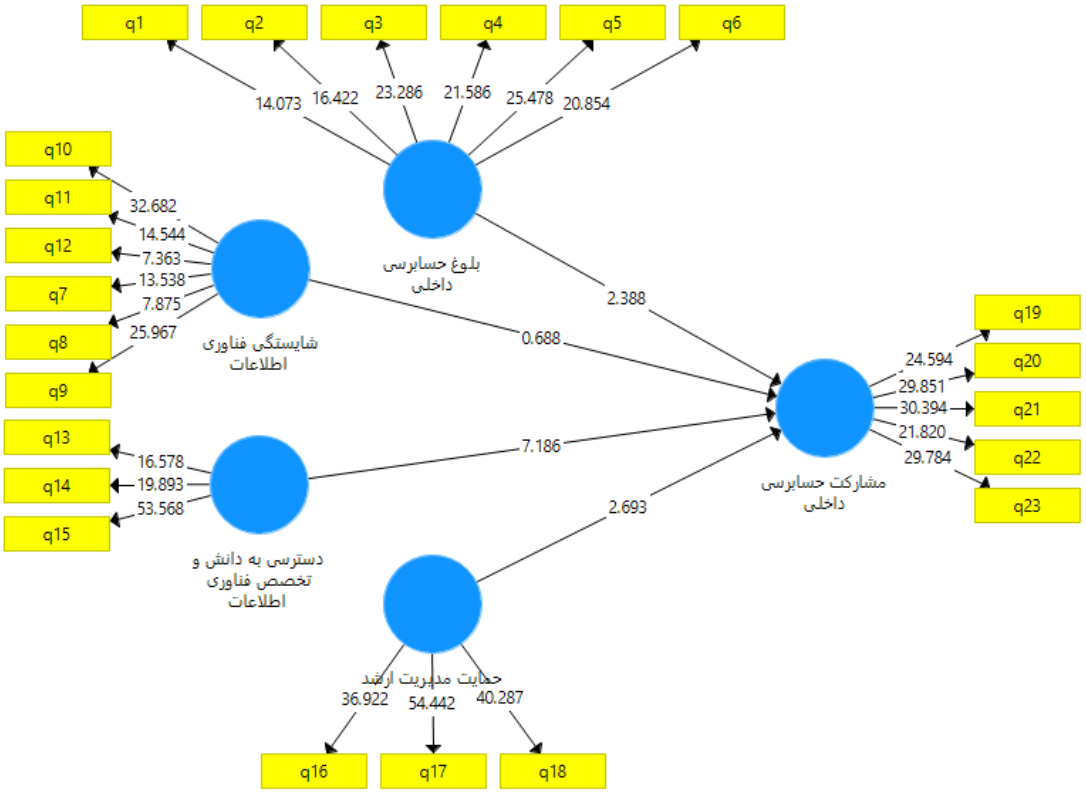
مطابق با جدول ۳، تمام مقادیر قطر اصلی از مقادیر زیرین و راست خود بزرگ‌تر می‌باشد؛ بنابراین برازش مدل مناسب می‌باشد.

برای بررسی برازش مدل ساختاری پژوهش از چندین معیار استفاده می‌شود که اولین و اساسی‌ترین معیار، ضرایب معناداری Z است. برازش مدل ساختاری با استفاده از ضرایب t به این صورت است که این ضرایب باید از ۱/۹۶ بیشتر باشند تا بتوان در سطح اطمینان ۹۵ درصد معنادار بودن آن‌ها را تأیید کرد. در صورتی که مقدار آماره t بیشتر از ۱/۹۶ گردد، ضریب مسیر در سطح اطمینان ۹۵ درصد و درصورتی‌که مقدار آماره t بیشتر از ۲/۵۸ گردد، ضریب مسیر در سطح اطمینان ۹۹ درصد معنادار است (داوری و رضازاده،۱۳۹۲).

جدول (۴): ضریب معناداری Z فرضیه (مقادیر T-value)

مسیر	مقدار T
بلوغ حسابرسی داخلی -> مشارکت حسابرسی داخلی	۲.۳۸۸
حمایت مدیریت ارشد -> مشارکت حسابرسی داخلی	۲.۶۹۳
دسترسی به دانش و تخصص فناوری اطلاعات -> مشارکت حسابرسی داخلی	۷.۱۸۶
شایستگی فناوری اطلاعات -> مشارکت حسابرسی داخلی	۰.۶۸۸

www.jamv.ir
ISSN: 2645-4572



شکل (۳): مدل معادلات ساختاری در حالت ضریب معنادار

ضریب تعیین R^2 (R Squars)

R^2 معیاری است که برای متصل کردن بخش اندازه‌گیری و بخش ساختاری مدل‌سازی معادلات ساختاری به‌کار می‌رود و نشان از تأثیری دارد که یک متغیر برون‌زا بر یک متغیر درون‌زا می‌گذارد. نکته ضروری این است که مقدار R^2 تنها برای سازه‌های وابسته (درون‌زا) مدل محاسبه می‌گردد و در مورد سازه‌های برون‌زا، مقدار این معیار صفر است. هرچه مقدار R^2 مربوط به سازه‌های درون‌زای یک مدل بیشتر باشد، نشان از برازش بهتر مدل است. چاین[1] (۱۹۹۸)، سه مقدار ۰/۱۹، ۰/۳۳ و ۰/۶۷را به‌عنوان مقدار ملاک برای مقادیر ضعیف، متوسط و قوی بودن برازش بخش ساختاری مدل به‌وسیله معیار R^2 در نظر می‌گیرد.

جدول (۵): مقادیر R Square

متغیر	R Square
مشارکت حسابرسی داخلی	۰.۵۸۷

مقدار ضریب تعیین در جدول ۵، نشان‌دهنده مناسب بودن برازش مدل است.

کیفیت پیش‌بینی‌کنندگی (Q^2)

این معیار قدرت پیش‌بینی مدل را مشخص می‌سازد. مدل‌هایی که دارای برازش بخش ساختاری قابل‌قبول هستند باید قابلیت پیش‌بینی شاخص‌های مربوط به سازه‌های درون‌زای مدل را داشته باشند. هنسلر و همکاران (۲۰۰۹)، سه مقدار

[1] Chine

www.jamv.ir
ISSN: 2645-4572

۰/۰۲، ۰/۱۵ و ۰/۳۵را برای نشان دادن قدرت پیش‌بینی ضعیف، متوسط و قوی سازه یا سازه‌های برون‌زای مربوط به آن تعریف کرده‌اند. ذکر این نکته ضروری است که این مقدار تنها برای سازه‌های درون‌زای مدل که شاخص‌های آن‌ها از نوع انعکاسی است، محاسبه می‌گردد (داوری و رضازاده،۱۳۹۲).

جدول (۶): کیفیت پیش‌بینی‌کنندگی (Q^2)

متغیر	Q^2
مشارکت حسابرسی داخلی	۰.۳۷۷

مقادیر کیفیت پیش‌بینی‌کنندگی در جدول۶ نشان از مناسب بودن این معیار می‌باشد.

آزمون مدل کلی

معیار نیکویی برازش

معیاری برای سنجش تمام مدل وجود ندارد. با این وجود یک معیار کلی برای نیکویی برازش به‌وسیله تنتهاوس و همکاران پیشنهاد شده بود به نام شاخص GOF.

که مدل کلی شامل هر دو بخش مدل اندازه‌گیری و ساختاری شد و با تایید برازش آن، بررسی برازش در یک مدل کامل شد. برای بررسی برازش مدل کلی تنها کافی بود یک معیار به نام GOF سنجیده شود:

$$GOF = \sqrt{\text{مدل درونی} \times \text{مدل بیرونی}}$$

$$GOF = \sqrt{\overline{Communalities} \times \overline{R^2}}$$

میزان$\overline{Communalities}$ از میانگین مقادیر اشتراکی که در جدول بالا آمده است، به‌دست می‌آید.

میزان میانگین مقادیر اشتراکی برابر بود با: ۰/۶۸۰

میزان میانگین مقدار$\overline{R^2}$ برابر بود با: ۰/۵۸۷

لذا مقدار معیار GOF برابر بود با:۰/۶۳۱

با توجه به سه مقدار ۰/۰۱، ۰/۲۵ و ۰/۳۶ که به‌عنوان مقادیر ضعیف، متوسط و قوی برای GOF معرفی‌شده است. حصول مقدار به‌دست آمده برای این معیار نشان از برازش قوی مدل کلی تحقیق دارد.

با توجه به گفته رینگل در سال ۲۰۱۳ اگر مقدار GOF>۰/۳۵ یعنی کیفیت مدل به ۹۷ درصد کووراینس‌ها می‌رسد.

با توجه به بررسی فرضیه‌های تحقیق برازش ساختاری با استفاده از ضرایب t به این صورت است که این ضرایب باید از ۱/۹۶ بیشتر باشند تا بتوان در سطح اطمینان ۰/.۹۵ معنادار بودن آنها را تأیید کرد. البته باید توجه داشت که اعداد t فقط صحت رابطه‌ها را نشان می‌دهند و شدت رابطه بین سازه‌ها را نمی‌توان با آنها سنجید و ضرایب مسیر نیز نشان‌دهنده تأثیر مثبت یا منفی یک متغیر بر متغیر دیگر می‌باشد (داوری و رضازاده،۱۳۹۲).

جدول (۷): نتایج حاصل از آزمون فرضیه‌ها

ردیف	فرضیه‌های تحقیق	ضریب مسیر	آماره t	مقادیر P	سطح معناداری	نتیجه
۱	بلوغ حسابرسی داخلی -> مشارکت حسابرسی داخلی	۰.۲۳۴	۲.۳۸۸	۰.۰۱۷	<۰/۰۵	تائید
۲	حمایت مدیریت ارشد -> مشارکت حسابرسی داخلی	۰.۱۹۵	۲.۶۹۳	۰.۰۰۷	<۰/۰۵	تائید
۳	دسترسی به دانش و تخصص فناوری اطلاعات -> مشارکت	۰.۴۴۳	۷.۱۸۶	۰.۰۰۰	<۰/۰۵	تائید

www.jamv.ir
ISSN: 2645-4572

	حسابرسی داخلی					
۴	شایستگی فناوری اطلاعات -> مشارکت حسابرسی داخلی	۰.۰۵۶	۰.۶۸۸	۰.۴۹۲	<۰/۰۵	رد

با توجه به جدول ۷ فرضیات تحقیق به جز فرضیه اثر شایستگی فناوری اطلاعات بر مشارکت حسابرسی داخلی که رد شد، مابقی فرضیات تأیید شدند.

بحث، نتیجه‌گیری و پیشنهادها

پژوهش حاضر با هدف بررسی عوامل مؤثر بر مشارکت حسابرسی داخلی در حسابرسی فناوری اطلاعات و امنیت سایبری انجام پذیرفته است. نتایج نشان می دهد که بلوغ حسابرسی داخلی به عنوان یک زیرساخت ساختاری و فرآیندی، نقش مهمی در تسهیل مشارکت واحدهای حسابرسی داخلی در حوزه‌های حساس فناوری اطلاعات و امنیت سایبری ایفا می کند. ضریب مسیر مثبت و معنادار (۰/۲۳۴) حاکی از آن است که هرچه چارچوب‌های کاری، استانداردها و روش‌های عملیاتی واحد حسابرسی داخلی بالغ تر و منظم تر باشد، توانایی این واحد برای شناسایی ریسکهای سایبری و انجام وظایف نظارتی مرتبط با آنها افزایش می یابد. این یافته تایید میکند که حسابرسی داخلی نمی تواند تنها براساس تجربه‌های شهودی یا روش‌های سنتی به موضوعات پیچیده فناوری اطلاعاتبپردازد بلکه نیازمند پختگی سازمانی و وجود دستورالعمل‌های مشخص است تا بتواند با اطمینان و دقت بیشتری در این حوزه فعالیت کند.

یکی از یافته‌های کلیدی و قابل توجه این مطالعه، تاثیر مستقیم و قوی دسترسی به دانش تخصصی فناوری اطلاعات بر مشارکت حسابرس داخلی است. با داشتن بزرگترین ضریب مسیر (۰/۴۴۳) و آماره t بسیار بالا (۷/۱۸۶)، مشخص شد که دسترسی به منابع دانشی، ابزارهای تحلیلی پیشرفته و پایگاه‌های داده تخصصی، قدرتمندترین عامل محرک برای ورود فعالانه حسابرس داخلی به مباحث امنیت سایبری است. این نتیجه نشان می دهد که حسابرس داخلی حتی اگر دارای شایستگی‌های فردی اولیه باشد، بدون دسترسی به دانش به روز و تخصصی در مورد تهدیدات نوظهور، معماری شبکه و تکنولوژی‌های امنیتی، قادر به ارائه ارزش افزوده واقعی نخواهد بود. بنابراین، نهادینه سازی دسترسی به دانش تخصصی، پیش شرط اصلی موفقیت در این عرصه است.

نقش حمایت مدیریت ارشد نیز به عنوان یک عامل تسهیلگر راهبردی، تایید شد. اگرچه ضریب اثرگذاری آن (۰/۱۹۵) کمی کمتر از دسترسی به دانش تخصصی است، اما همچنان رابطه مثبت و معناداری دارد. این بدان معناست که وقتی رهبران سازمان اهمیت و اولویت موضوع امنیت سایبری را برجسته کنند، بودجه لازم را اختصاص دهند و فرهنگ امنیت را ترویج نمایند، موانع سیاسی و اجرایی برای حضور حسابرس داخلی در پروژه‌های فناوری اطلاعاتکاهش می یابد. حمایت مدیریت ارشد به حسابرس داخلی قدرت چانه‌زنی و مشروعیت لازم را می دهد تا بتواند بر مقاومت‌های احتمالی بخش‌های فنی غلبه کرده و در فرآیندهای حسابرسی فناوری اطلاعات مشارکت موثری داشته باشد.

در مقابل، رد فرضیه مربوط به شایستگی فناوری اطلاعات حسابرسان داخلی نکته جالبی را آشکار میسازد. این نتیجه نشان می دهد که صرفِ داشتن مهارت‌ها و شایستگی‌های فردی در سطح کارکنان، به تنهایی باعث افزایش مشارکت آنها در حسابرسی فناوری اطلاعاتنمی شود. ممکن است حسابرسان داخلی دانش فنی کافی داشته باشند، اما اگر سیستم‌های پشتیبان (مانند دسترسی به دانش تخصصی سازمانی)، چارچوب‌های بلوغ سازمانی و حمایت مدیریت ارشد فراهم نباشد، این شایستگی‌ها به عملکرد عملیاتی تبدیل نمی شوند. این یافته بیانگر آن است که تمرکز صرف بر آموزش فردی بدون ایجاد اکوسیستم حمایتی و دسترسی به منابع دانشی، راهبرد ناکافی ای برای بهبود مشارکت در حسابرسی سایبری است.

www.jamv.ir
ISSN: 2645-4572

یافته‌ها بر این اصل استوار است که مشارکت موثر حسابرسی داخلی در امنیت سایبری، یک پدیده چندبعدی است که نیازمند ترکیبی از بلوغ سازمانی، دسترسی به دانش تخصصی و حمایت مدیریتی است. از میان متغیرهای مورد بررسی، دسترسی به دانش تخصصی بیشترین سهم را در تبیین تغییرات مشارکت داشت، که نشان دهنده گذار از رویکرد سنتی حسابرسی به رویکرد مبتنی بر دانش و داده است. بنابراین، سازمان‌ها برای ارتقای نقش حسابرسی داخلی در حوزه سایبری نباید تنها بر استخدام افراد با شایستگی فنی تمرکز کنند، بلکه باید زیرساخت‌های دانشی خود را تقویت کرده و محیطی حمایتی از سوی مدیریت ارشد ایجاد نمایند تا پتانسیل‌های موجود در واحد حسابرسی داخلی به شکوفایی کامل برسد.

نتایج همسویی قابل توجهی را در تایید نقش زیرساخت‌های سازمانی و دانشی نشان می دهد، اما تفاوت‌های ظریفی نیز آشکار می سازد. نتایج حاضر مبنی بر تاثیر مثبت بلوغ حسابرسی داخلی و حمایت مدیریت ارشد بر مشارکت، کاملا با دیدگاه کالوین و همکاران (۲۰۲۵)، که بر اهمیت ساختار و حمایت رهبری برای ورود به حوزه‌های نوپدید تاکید دارند، همسو است. همچنین، ضریب مسیر بالای دسترسی به دانش تخصصی در این پژوهش، تداوم یافته‌های وو و همکاران (۲۰۲۴)، و ابراهیمی کردلر و همکاران (۱۴۰۳)، درباره نقش حیاتی منابع دانشی سازمانی در تقویت عملکرد حسابرسی فناوری اطلاعاتاست. با اینحال، برخلاف فرضیه دوم و برخی مطالعات مانند الزبان و همکاران (۲۰۲۶)، که شایستگی فردی حسابرسان را عامل کلیدی بهبود امنیت می دانند، نتیجه رد شدن این فرضیه در پژوهش حاضر نویدبخش یک بینش جدید است، بدین معنا که در بستر شرکت‌های ایرانی، صرفِ داشتن مهارت فردی بدون وجود دسترسی به دانش تخصصی سازمانی، بلوغ فرآیندی و حمایت مدیریتی کافی نیست و ممکن است منجر به مشارکت موثر نشود. این تفاوت نشان می دهد که درحالیکه ادبیات جهانی گاهی بر صلاحیت فردی (مانند تخصص CAE) تمرکز دارد، در محیط‌های با محدودیت دسترسی به منابع یا ساختارهای سنتی تر، عوامل سیستمی و دسترسی به دانش نهادینه شده اولویت بیشتری نسبت به شایستگی‌های پراکنده فردی دارند.

براساس یافته‌های پژوهش، پیشنهاد می شود سازمان‌ها به جای تمرکز صرف بر آموزش‌های عمومی شایستگی فردی، سرمایه گذاری جدی بر روی ایجاد و به روزرسانی پایگاه‌های دانش تخصصی فناوری اطلاعات و بسترهای اشتراک گذاری دانش در داخل واحد حسابرسی داخلی انجام دهند. همچنین، تدوین چارچوب‌های بلوغ حسابرسی داخلی که شامل شاخص‌های مشخصی برای ارزیابی آمادگی در حوزه فناوری اطلاعاتباشد، ضروری است. علاوه براین، برگزاری جلسات منظم گزارش دهی بین مدیریت ارشد و هیئت مدیره حسابرسی داخلی با محوریت نمایش ارزش افزوده خدمات سایبری، میتواند حمایت مدیریتی را تثبیت کرده و موانع ساختاری را برای مشارکت بیشتر حسابرس داخلی برطرف سازد.

یکی از محدودیت‌های اصلی این پژوهش، استفاده از روش نمونه گیری غیرتصادفی و دسترسی محدود به جامعه آماری تخصصی حسابرسان داخلی در ایران بود که ممکن است تعمیم پذیری نتایج را تحت تاثیر قرار دهد. بنابراین پیشنهاد میشود پژوهش‌های آتی با استفاده از نمونه گیری تصادفی و گسترش دامنه جغرافیایی یا مقایسه بین المللی، صحت سنجی بیشتری انجام دهند.

منابع

- ✓ ابراهیمی کردلر، علی، رهنما، مریم، خازن، آتنا، (۱۴۰۳)، بررسی رابطه بین ویژگی‌های حسابرسی داخلی و کنترل فناوری اطلاعات با توجه به نقش میانجی مشارکت حسابرسی داخلی، مدیریت اطلاعات، دوره ۱، شماره ۱۰.

- ✓ داوری، علی، رضازاده، آرش، (۱۳۹۲)، مدل سازی معادلات ساختاری با نرم افزار PLS، انتشارات جهاد دانشگاهی، چاپ اول.
- ✓ کارگرشورکی، امید، مکوندی، مهسا، (۱۴۰۰)، مشارکت حسابرسان داخلی در مدیریت ریسک در حسابداری و راهبری شرکتی، دهمین کنفرانس ملی اقتصاد، مدیریت و حسابداری، شیروان.
- ✓ Abbott, L. J., Daugherty, B., Parker, S., & Peters, G. F. (2016). Internal audit quality and financial reporting quality: The joint importance of independence and competence. Journal of Accounting Research, 54(1), 3-40.
- ✓ Abdelraouf, M., Muharram, F., & Mohamed, A. (2025). The impact of internal audit function characteristics on internal control quality: The moderating role of cyber risk. MSA-Management Sciences Journal, 4(3), 1-27.
- ✓ 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.
- ✓ Bantleon, U., d'Arcy, A., Eulerich, M., Hucke, A., Pedell, B., & Ratzinger- Sakel, N. V. (2021). Coordination challenges in implementing the three lines of defense model. International Journal of Auditing, 25(1), 59-74.
- ✓ Bhme, R., Laube, S., & Riek, M. (2019). A fundamental approach to cyber risk analysis. Variance, 12(2).
- ✓ Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. Managerial auditing journal, 33(4), 360-376.
- ✓ 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.
- ✓ Carcello, J. V., Eulerich, M., Masli, A., & Wood, D. A. (2018). The value to management of using the internal audit function as a management training ground. Accounting Horizons, 32(2), 121-140.
- ✓ Chin, W. W. (1998). Commentary: Issues and Opinion on Structural Equation Modeling. MIS Quarterly, 22(1), vii-xvi.
- ✓ Cronbach LJ. Coefficient alpha and the internal structure of tests. psychometrika. 1951; 16(3): 297-334.
- ✓ Dzuranin, A. C., & Mălăescu, I. (2016). The current state and future direction of IT audit: Challenges and opportunities. Journal of Information Systems, 30(1), 7-20.
- ✓ Ege, M. S. (2015). Does internal audit function quality deter management misconduct?. The Accounting Review, 90(2), 495-527.
- ✓ Eulerich, M. (2021). The new three lines model for structuring corporate governance–A critical discussion of similarities and differences. Available at SSRN 3777392.
- ✓ Eulerich, M., Masli, A., Pickerd, J., & Wood, D. A. (2023). The impact of audit technology on audit task outcomes: Evidence for technology- based audit techniques. Contemporary Accounting Research, 40(2), 981-1012.
- ✓ Eulerich, M., Waddoups, N., Wagener, M., & Wood, D. A. (2024). The dark side of robotic process automation (RPA): Understanding risks and challenges with RPA. Accounting Horizons, 38(2), 143-152.
- ✓ European Confederation of Institutes of Internal Auditors (ECIIA) (2022): Risk in Focus 2023 – Hot topics for internal auditors. Available at: https://www.iia.org.uk/ policy-and-research/research-reports/risk-in-focus (last accessed March 3, 2023).

- ✓ Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research, 18(1), 39-50.
- ✓ Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In New challenges to international marketing. Emerald Group Publishing Limited.
- ✓ Hepworth, L. R., Greenman, C., Esplin, D., & Johnston, R. (2022). Cybersecurity and data privacy: The rising expectations within internal audit. Journal of Forensic and Investigative Accounting, 14(3), 454-465.
- ✓ Institute of Internal Auditors (IIA). 2016. Assessing cybersecurity risk: roles of the three lines of defense. Available at: https://global.theiia.org/standards-guidance/ Member%20Documents/GTAG-Assessing-Cybersecurity-Risk.pdf (last accessed March 3, 2023).
- ✓ Institute of Internal Auditors (IIA). 2017. International Standards for the Professional Practice of Internal Auditing. Available at: https://www.theiia.org/globalassets/ site/standards/mandatory-guidance/ippf/2017/ippf-standards-2017-english.pdf (last accessed March 3, 2023).
- ✓ Institute of Internal Auditors (IIA). 2020. Global Technology Audit Guides (GTAG): Assessing Cybersecurity Risk. Altamonte Springs, FL.
- ✓ Institute of Internal Auditors (IIA). 2022. Global Technology Audit Guides (GTAG): Auditing cybersecurity operations: Prevention and detection. Altamonte Springs, FL
- ✓ Siyaya, M. C., Dubihlela, J., & Sibanda, M. (2025). A literature review of internal auditing involvement in cybersecurity risk management of the organisation. Journal of Contemporary Management, 22(SPE), 89-115.
- ✓ 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.
- ✓ Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548.
- ✓ 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.
- ✓ Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. Journal of Information Systems, 35(1), 155-186.
- ✓ Werts, C. E., Linn, R. L., & Jöreskog, K. G. (1974). Intraclass Reliability Estimates: Testing Structural Assumptions. Educational and Psychological Measurement, 34(1), 25-33.
- ✓ World Economic Forum. 2022. Global cybersecurity outlook 2022: Insight report. Available at: https://www.weforum.org/reports/global-cybersecurity-outlook-2022 (last accessed March 3, 2023).
- ✓ Wu, T. H., Huang, S. Y., Chiu, A. A., & Yen, D. C. (2024). IT governance and IT controls: Analysis from an internal auditing perspective. International Journal of Accounting Information Systems, 52, 100663.