به نام خدا

ترجمه: دنا گلناریان

پاییز ۹۷

درباره رهنمودهای تکمیلی

رهنمودهای تکمیلی بخشی از چارچوب اجرای حرفه‌ای بین المللی (IPPF) انجمن حسابرسان داخلی (IIA) هستند و توصیه‌های اضافی را ارائه می‌دهد، رهنمودهای غیر اجباری برای اداره کردن فعالیت‌های حسابرسی داخلی. در حالی که حمایت از *استانداردهای بین المللی برای اجرای حرفه‌ای حسابرسی داخلی است*، رهنمودهای تکمیلی در نظر گرفته شده است تا از مناطق موضعی، و همچنین مسائل مربوط به بخش خاص، در جزئیات رویه‌ای بیشتر از استانداردها یا رهنمودهای پیاده سازی استفاده کنند. رهنمودهای تکمیلی توسط انجمن حسابرسان داخلی از طریق مراحل رسمی و فرآیندهای تصویب صحه گذاشته شده است.

رهنمودهای اجرا

رهنمودهای اجرا نوعی از رهنمودهای تکمیلی هستند که روش‌های دقیق گام به گام، شامل فرآیندها، روش‌ها، ابزار و برنامه‌ها و همچنین نمونه‌هایی از نتایج قابل ارائه تهیه می‌کنند.

رهنمودهای اجرا برای حمایت از حسابرسان داخلی در نظر گرفته شده است. رهنمودهای اجرا همچنین برای حمایت از موارد زیر وجود دارند:

- خدمات مالی
- بخش عمومی
- فناوری اطلاعات

برای یک مرور کلی از موارد راهنمایی معتبر ارائه شده توسط انجمن حسابرسان داخلی لطفا www.globaliia.org/standards-guidance را بازدید کنید.

فهرست مندرجات

خلاصه اجرایی

پیاده سازی یک رویکرد استراتژیک برای راهبری فناوری اطلاعات کمک می کند تا سازمان ها به سرعت به پیشرفت های تکنولوژیکی، گسترش خدمات فناوری اطلاعات، و وابستگی بیشتر به فناوری اطلاعات برای رسیدن به اهداف سازمان پاسخ دهند. راهبری مؤثر فناوری اطلاعات به کنترل بهره‌وری و اثربخشی کمک می‌کند، و به سرمایه‌گذاری سازمان‌ها در فناوری اطلاعات برای تحقق یافتن هر دو مزایای مالی و غیرمالی اجازه می‌دهد. اغلب زمانی که کنترل‌ها ضعیف یا ناکارا طراحی شده‌اند، دلیل اصلی آن راهبری ضعیف یا غیر مؤثر فناوری اطلاعات است.

هم‌ترازی اهداف سازمانی و فناوری اطلاعات بیشتر در مورد راهبری و کمتر در مورد تکنولوژی است. راهبری اطمینان می‌دهد که جایگزین‌ها ارزیابی می‌شوند، اجرا به درستی هدایت می‌شود و ریسک و عملکرد مورد نظارت قرار می‌گیرند.

راهبری فناوری اطلاعات مستقیماً به نظارت سازمانی دارایی‌ها و ریسک‌های فناوری اطلاعات مرتبط است، و این مسئولیت مشترک مدیریت ارشد[1] و هیئت مدیره است. مدیریت ارشد روز به روز مسیر هم‌ترازی ماهرانه با هدایت کلی استراتژیک هیئت مدیره برای مطمئن ساختن از استفاده مؤثر، کارآمد و قابل قبول از منابع فناوری اطلاعات را به پیش می‌برد. نتایج اولیه راهبری مؤثر فناوری اطلاعات شامل موارد زیر است:

- استراتژی‌های فناوری اطلاعات با اهداف سازمانی هماهنگ می شوند.
- ریسک‌ها به طور صحیح شناسایی و مدیریت می‌شوند.
- سرمایه گذاری‌های فناوری اطلاعات برای به دست آوردن ارزش برای سازمان بهینه سازی شده‌اند.
- عملکرد فناوری اطلاعات با استفاده از معیارهای پرمعنی تعریف، اندازه گیری و گزارش شده است.
- منابع فناوری اطلاعات به طور مؤثر مدیریت می‌شوند.

[1] مدیریت ارشد معمولاً شامل مدیر ارشد اجرایی (CEO)، مدیر ارشد مالی (CFO)، مدیر ارشد عملیاتی (COO)، و مدیر بازاریابی می‌باشد.

عدم وجود راهبری فناوری اطلاعات یا ضعیف بودن آن می‌تواند اثرات منفی قابل توجهی بر سازمان هم از لحاظ مالی و هم از لحاظ اعتباری داشته باشد. جبران چنین اثراتی مستلزم زمان، انرژی و پول می‌باشد. در بسیاری از سازمان‌ها، یک عدم ارتباط بین مدیریت ارشد و فناوری اطلاعات به دلیل یک باور قدیمی که فناوری اطلاعات منحصراً برای ارائه خدمات روزانه فناوری اطلاعات است، وجود دارد. در حقیقت فناوری اطلاعات در توسعه مزیت رقابتی و برای حمایت از دستیابی به اهداف سازمان و اهداف استراتژیک حیاتی است.

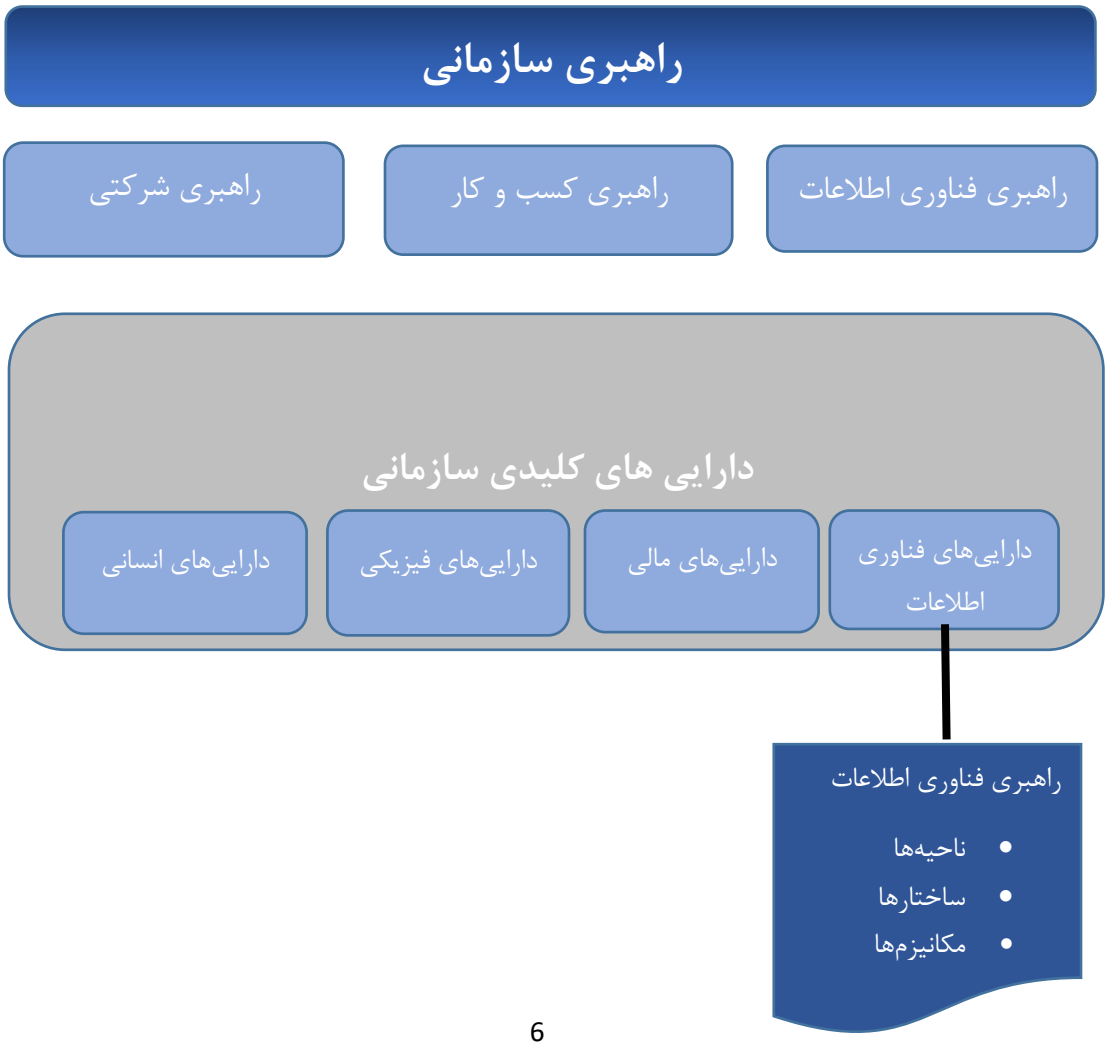
حسابرسی داخلی به طور منحصر به فرد در یک سازمان فعالیت می‌کند تا ارزیابی کند که راهبری فناوری اطلاعات آن استراتژی‌ها و اهداف سازمان را پشتیبانی می‌کند و در صورت نیاز توصیه‌های لازم را ارائه کند. (استاندارد پیاده سازی 2110.A2)

به عنوان ویرایش دوم "حسابرسی راهبری فناوری اطلاعات،" راهنمای حسابرسی جهانی فناوری (GTAG) برای انعکاس چارچوب بین‌المللی اجرای حرفه‌ای ۲۰۱۷ (IPPF) به روز رسانی شده است تا بیشتر و به طور مستقیم برای حسابرسان داخلی عملی باشد.

معرفی

بالاترین سطح راهبری، راهبری سازمانی است که توسط *استانداردهای بین‌المللی برای اجرای حرفه‌ای حسابرسی داخلی* به عنوان "ترکیبی از فرآیندها و ساختارهای اجرا شده توسط هیئت رئیسه برای اطلاع رسانی، هدایت، مدیریت و نظارت بر فعالیت‌های سازمان در جهت به دستیابی به اهداف آن،" تعریف شده است.

راهبری فناوری اطلاعات زیر شاخه‌ای از راهبری سازمانی است که متشکل از رهبری، ساختارهای سازمانی، سیاست‌ها و فرآیندهایی است که اطمینان حاصل می‌کند که فناوری اطلاعات شرکت استراتژی‌ها و اهداف سازمان را پشتیبانی می‌کند. راهبری فناوری اطلاعات از مقررات نظارتی، قانونی، محیطی و نیازمندی‌های عملیاتی سازمان پشتیبانی می‌کند تا امکان دستیابی به برنامه‌های استراتژیک و آرمان‌ها را فراهم سازد. زیرشاخه‌های دیگر شامل حاکمیت شرکتی مسئول فرآیندهای انطباق و مدیریت کسب و کار مسئول فرآیندهای اجرایی می‌باشد. شکل ۱ رابطه بین حاکمیت سازمانی و راهبری فناوری اطلاعات را نشان می‌دهد.



هدف این رهنمود کمک به حسابرسان داخلی در تهیه خدمات اطمینان بخش در مورد راهبری فناوری اطلاعات است. این رهنمود یک توصیف سطح بالا از فرآیندها، شیوه‌ها و اصطلاحات علمی راهبری فناوری اطلاعات را فراهم می‌کند تا به حسابرسان داخلی در دستیابی به درک مفهوم راهبری و مشخصه‌های آن در فرآیندهای راهبری خوب کمک کند.

این ویرایش ابزار و تکنیک‌هایی برای کمک به حسابرسان داخلی در مورد ایجاد یک برنامه کاری و انجام وظایف مربوط به فناوری اطلاعات فراهم می‌کند.

بررسی اجمالی راهبری فناوری اطلاعات

پیاده سازی راهبری فناوری اطلاعات بخشی الزامی در استراتژی‌های سازمان است زیرا اساساً مربوط به اهدافی است که از اینکه فناوری اطلاعات ارزش را به کسب و کار در یک روش کنترل شده و مؤثر ارائه می‌دهد، اطمینان حاصل می‌کند. چارچوب راهبری فناوری اطلاعات به طور معمول بر پنج حوزه کلیدی متمرکز است:

- **هم‌ترازی استراتژیک** – راهبری فناوری اطلاعات مسیر استراتژیک فناوری اطلاعات و هم‌ترازی فناوری اطلاعات و کسب و کار را با توجه به خدمات و پروژه‌ها، اهداف کسب و کار، استراتژی به روز فناوری اطلاعات، پیوند بین اهداف کسب و کار و ابتکارات عمل فناوری اطلاعات ارائه می‌دهد.
- **مدیریت ریسک** - راهبری فناوری اطلاعات می‌تواند به تعیین این که چه فرآیندهایی جهت اطمینان اینکه ریسک‌ها به اندازه کافی مورد توجه قرار گرفته‌اند، کمک کند. علاوه بر این، می توان اطمینان حاصل کرد که مدیریت ریسک بنگاه شامل جنبه‌های ریسک سرمایه‌گذاری فناوری اطلاعات، مسئولیت‌های تعریف شده برای مدیریت ریسک، تعریف یک روش شناسی آنالیز ریسک عمومی، و تعریف استراتژی‌ها برای پرداختن به ریسک‌ها، نظارت مستمر تهدیدات، وقوع، و تأثیر به یک روش جامع است.
- **تحویل ارزش** – راهبری فناوری اطلاعات به فناوری اطلاعات و کسب و کار کمک می‌کند تا یک مشارکت طراحی شود تا بیش‌ترین ارزش کسب و کار را از فناوری اطلاعات کسب کند. این کسب و کار قادر به نظارت بر تحویل ارزش توسط فناوری اطلاعات و اندازه‌گیری بازده سرمایه (ROI)، اجرای برنامه تاکتیکی فناوری اطلاعات و مزایای واضح برای هر سطح از سازمان است. برای مثال، زمان بیداری سیستم (استراتژی زیرساخت)، درجه اتوماسیون در استراتژی توسعه نرم‌افزار (SDLC) ، بهره‌وری (استراتژی عملیاتی) ، و در نهایت درآمد (استراتژی مالی فناوری اطلاعات).
- **اندازه‌گیری عملکرد** – راهبری فناوری اطلاعات مکانیزم‌های تأیید انطباق استراتژیک (یعنی دستیابی به اهداف استراتژیک فناوری اطلاعات، اندازه‌گیری عملکرد فناوری اطلاعات و سهم آن در خط پایین (یعنی،

تحویل عملکرد کسب و کار وعده داده شده) را فراهم می‌کند. معیارهای بیشتر شامل نظارت مستمر و گزارش دهی، سیاست‌های پی‌گیری، آنالیز علت ریشه‌ای و مدیریت مشکل، معیار سنجش در برابر شیوه‌های صنعت، و استانداردهای ثابت شده یا چارچوب‌ها است.

- **مدیریت منبع** – راهبری فناوری اطلاعات مسیر سطح بالایی برای تأمین منابع و استفاده از منابع تهیه می‌کند تا: بر تأمین مالی جمع شده فناوری اطلاعات در سطح بنگاه نظارت کند؛ و اطمینان حاصل کند که توانایی و زیرساخت فناوری اطلاعات کافی برای پشتیبانی از الزامات کسب و کار فعلی و مورد انتظار در آینده، استراتژی‌های تأمین منابع، روش‌های مدیریت انسانی، راهنمای کاربر، تفکیک وظایف، گزارش زمان، مدیریت چرخه عمر زیر ساخت‌ها، توافقات سطح خدمات (SLA ها)، و سیاست‌های مورد استفاده قابل قبول وجود دارد.

برخی از چالش‌هایی که راهبری فناوری اطلاعات می‌تواند به سازمان‌ها در اداره کردن کمک کند عبارتند از:

- پیچیدگی فزاینده محیط‌های فناوری اطلاعات.
- وابستگی رو به رشد به داده‌ها برای تصمیم‌گیری درباره کسب و کار.
- ازدیاد دستگاه‌های تلفن همراه.
- نیاز به تبادل اطلاعات با مشتریان، ارائه دهندگان خدمات و شرکای تجاری.
- ریسک فزاینده حملات سایبری.
- افزایش قوانین و مقررات مربوط به حفاظت از داده‌ها.

در چارچوب مفهومی راهبری فناوری اطلاعات، مدیریت ارشد و هیئت مدیره مسئول ایجاد اهداف فناوری اطلاعات سازمان در هم‌ترازی با استراتژی کلی کسب و کار؛ تعریف استراتژی‌های فناوری اطلاعات برای رسیدن به اهداف کسب و کار؛ و ایجاد سیاست‌های اداره فناوری اطلاعات، ساختارهای سازمانی، و فرآیندهایی برای مدیریت ریسک‌ها برای رسیدن به این اهداف هستند.

مدیریت فناوری اطلاعات مسئول فعالیت‌های روز به روز یک سازمان است: برنامه‌ریزی، اجرا و نظارت بر استفاده از منابع فناوری اطلاعات برای تضمین موفقیت استراتژی‌ها و سیاست‌های تعیین‌شده توسط هیئت مدیره.

نقش حسابرس داخلی در راهبری فناوری اطلاعات در پی برخاستن بحران‌های مالی جهانی و شکاف‌های امنیت اطلاعات مشخصات سطح بالا، به طور فزاینده‌ای مهم شده است. براساس نتایج نظرسنجی منتشر شده در گزارش CBOK انجمن حسابرسان داخلی (IIA)، ارتقا و حمایت از حاکمیت سازمانی مؤثر، حسابرس داخلی به خوبی

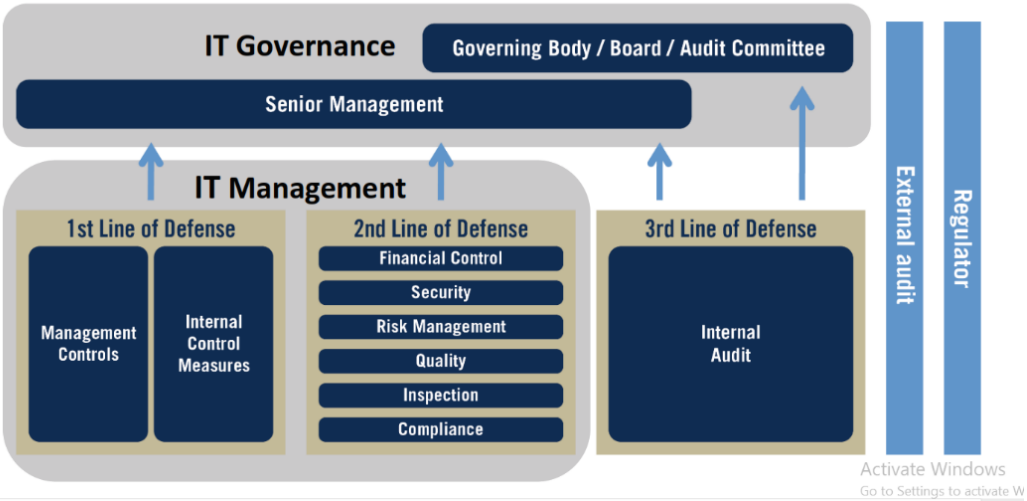
برای ارتقا و حمایت از حاکمیت سازمانی قرار دارد و در نتیجه به دستیابی به تعادلی میان خلق ارزش و حفظ ارزش کمک می‌کند.

نقش حسابرس داخلی شامل مسئولیت ارزیابی و ارائه توصیه‌هایی برای بهبود فرآیندهای حاکمیت سازمان (استاندارد ۲۱۱۰ – حاکمیت) برای کمک به جلوگیری از شکست حاکمیت و بهبود عملکرد استراتژیک به عنوان بخشی از خط سوم دفاع است.

در مدل سه خط دفاعی، مدیریت عملیاتی (شامل فناوری اطلاعات) اولین خط دفاعی را ارائه می‌دهد و مسئول پیاده سازی و نگهداری فرآیندها و کنترل‌ها برای مدیریت ریسک‌ها است. انطباق وظایف و مدیریت ریسک نشان‌دهنده خط دوم دفاع بوده و مسئول نظارت بر خطرات در سراسر سازمان می‌باشند. حسابرس داخلی سومین خط دفاعی را ارائه می‌دهد و مسئول ارائه تضمین مستقل است که مدیریت ریسک و کنترل‌ها به طور مؤثر عمل می‌کنند، و به مدیریت ارشد و هیئت مدیره زمانی که نقص‌ها شناسایی می‌شوند، توصیه می‌کنند.

شکل ۲ مسئولیت‌های مدل سه خط دفاعی را نشان می‌دهد که با راهبری فناوری اطلاعات مرتبط است.

Figure 2: Three Lines of Defense in Reference to IT Governance



چارچوب‌های راهبری فناوری اطلاعات شناخته شده بین‌المللی بسیاری وجود دارند که می‌توانند برای تکمیل این رهنمود استفاده شوند. چارچوب‌هایی مانند ITIL، COBIT، ISO / IEC ۳۸۵۰۰، III King ، و IV King به طور دقیق‌تر فرایندها و مکانیزم‌های مورد نیاز برای توسعه، پیاده سازی، ارزیابی ، و بهبود یک برنامه راهبری فناوری اطلاعات را گزارش می‌دهند. این راهنما بر فرآیندها و مکانیزم‌هایی تمرکز دارد که حسابرس داخلی می‌تواند

برای ارزیابی اینکه آیا برنامه راهبری فناوری اطلاعات از استراتژی‌ها و اهداف سازمان در انطباق با استاندارد پیاده سازی A2.۲۱۱۰ پشتیبانی می‌کند یا خیر، استفاده کند.

اهمیت کسب و کار

اطلاعات و اجزای تکنولوژیکی یک سازمان در بین مهم‌ترین دارایی‌های آن می‌باشند. فقدان حاکمیت مناسب بر اطلاعات ذخیره شده، پردازش شده و یا تولید شده توسط سیستم‌های فناوری اطلاعات می‌تواند تأثیر منفی قابل توجهی بر سازمان داشته باشد، اعم از جریمه‌ها و مجازات‌ها تا اعتبار آسیب دیده که می‌تواند زمان، انرژی و پول را صرف بازسازی کند. به بیان ساده، راهبری فناوری اطلاعات می‌تواند کل سازمان را تحت تأثیر قرار دهد، و نه تنها بر روی فناوری اطلاعات تأثیر بگذارد.

وابستگی بیشتر به سیستم‌ها و اطلاعات به این معنی است که سازمان‌ها باید منابع بیشتری را برای بهبود و حفظ محیط فناوری اطلاعات خود سرمایه‌گذاری کنند. انتظار می‌رود که این‌ها به مدیریت ریسک، بهبود عملیات‌ها، و خلق ارزش از طریق تحویل خدمات کمک کنند که به دستیابی به اهداف سازمانی مالی و غیرمالی کمک می‌کنند.

تمرکز اصلی راهبری فناوری اطلاعات بر ایجاد هم‌ترازی بین اولویت‌های سازمانی و اهداف فناوری اطلاعات است تا اطمینان حاصل شود که تلاش‌های فناوری اطلاعات بر فرآیندها یا پروژه‌هایی متمرکز می‌شوند که اهداف استراتژیک را پشتیبانی می‌کنند. هم‌ترازی موفقیت آمیز بین سازمان و فناوری اطلاعات زمانی رخ می‌دهد که مدیریت ارشد و هیئت مدیره ارزش فناوری اطلاعات را به عنوان یک شریک استراتژیک درک کرده و نقش فناوری اطلاعات را در حمایت از خط پایین بشناسند.

یک چارچوب راهبری فناوری اطلاعات قدرتمند مزایای متعددی را فراهم می‌کند، شامل:

- مزیت رقابتی.
- سرعت بهبود یافته به بازار.
- رعایت و امنیت اطلاعات مؤثر.
- اتوماسیون فرآیند و نوآوری.
- تصمیم‌گیری آگاهانه بیشتر.

هم ترازی مناسب بین سازمان و فناوری اطلاعات یعنی:

- مدیریت ارشد و هیئت‌مدیره پتانسیل و محدودیت‌های فناوری اطلاعات را درک کنند.
- مدیریت ارشد فناوری اطلاعات اهداف و نیازهای مربوط به سازمان را درک کند.
- این درک در سرار سازمان توسط یک حاکمیت مناسب و ساختار پاسخگویی نظارت و اعمال می‌شود.

- درک بهتر علل ریشه‌ای مرتبط با مشکلات که منجر به بهبود مستمر فرآیند می‌شود.

فعالیت‌هایی که در محدوده راهبری فناوری اطلاعات قرار دارند عبارتند از:

- هم‌ترازی سرمایه‌گذاری‌ها و اولویت‌های فناوری اطلاعات با اهداف کسب و کار.
- مدیریت، ارزیابی، اولویت بندی، تأمین مالی، اندازه گیری، و نظارت بر درخواست‌ها برای خدمات فناوری اطلاعات، و کار حاصل شده و قابل تحویل، در یک شیوه استوار و قابل تکرار که بازده‌ها را برای کسب و کار بهینه سازی می‌کند.
- حفظ بهره برداری مسئولانه از منابع و دارایی‌ها.
- تعیین و روشن کردن مسئولیت‌پذیری و حقوق تصمیم – نقش‌ها و اختیارات به وضوح تعریف شده.
- اطمینان از اینکه فناوری اطلاعات برنامه‌ها، بودجه‌ها و تعهدات خود را ارائه می‌دهد.
- مدیریت ریسک‌های بزرگ، تهدیدات، تغییر، و احتمالات فعالانه.
- بهبود عملکرد سازمانی فناوری اطلاعات، انطباق، بلوغ، توسعه کارکنان، و ابتکارات برون سپاری.
- حمایت کردن از نوآوری در فناوری اطلاعات و کل سازمان.

ریسک‌های کلیدی

همان طور که منافع راهبری فناوری اطلاعات می‌تواند به سازمان برای دستیابی به اهداف مالی و غیرمالی کمک کند، عملیات‌ها را بهبود بخشد و ریسک را کنترل کند، اثرات منفی می‌تواند برای کل سازمان مضر باشد.

تأکید بر جنبه‌های فنی یا مالی فناوری اطلاعات به جای تأکید بر زمینه سازمانی استفاده از فناوری اطلاعات به عنوان یک توانمند ساز کسب و کار، معمولاً منجر به پیامدهای منفی، بازده ضعیف سرمایه‌گذاری فناوری اطلاعات، یا شکست برای نشان دادن مزایای ایجاد شده از طریق سرمایه‌گذاری فناوری اطلاعات می‌شود.

مثال‌های دیگر از تأثیرات منفی عبارتند از:

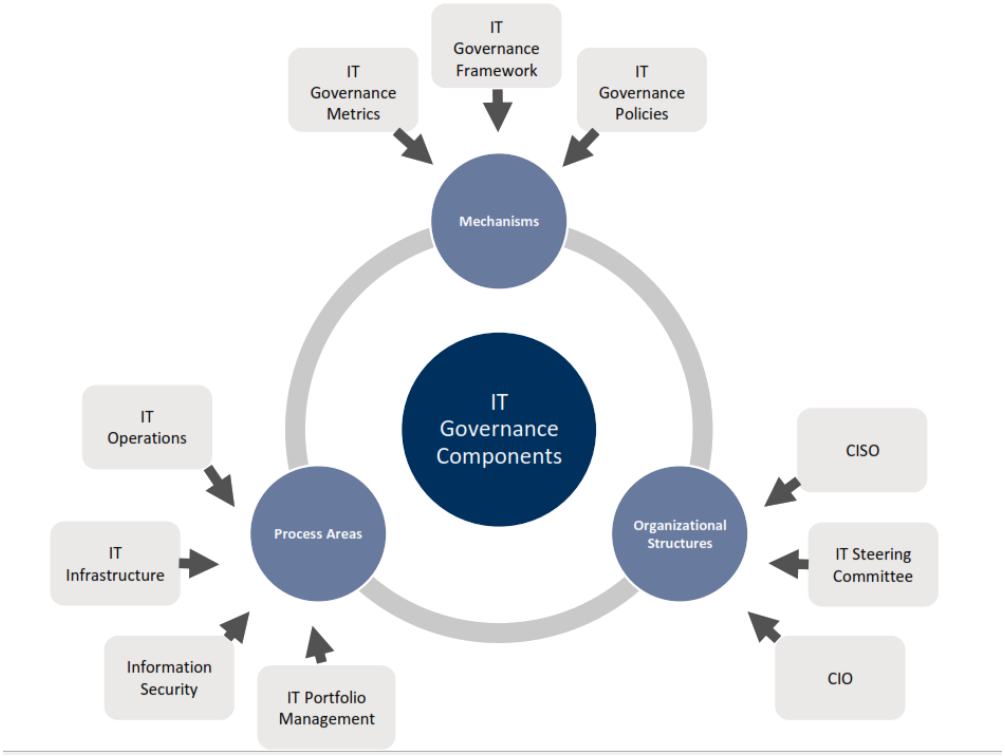
- زیان‌های مالی ناشی از اختلال در کسب و کار.
- هزینه‌های بالاتر برای اجرای عملیات‌های کسب‌وکار.
- کیفیت ضعیف یا شکست در مواجه شدن با انتظارات مشتری جدید و مشتریان ناراضی.
- فرآیندهای کسب و کار اصلی توسط تحویل ضعیف خدمات فناوری اطلاعات تحت تأثیر منفی قرار می‌گیرند.
- خطرات و تهدیدهای ناشناس کل سازمان را در معرض شکاف‌های امنیتی قرار می‌دهد.
- مجازات ناشی از شکست در مواجه شدن با الزامات قانونی.

اجزای راهبری فناوری اطلاعات

پیاده سازی و نگهداری یک برنامه راهبری فناوری اطلاعات به اجزایی وابسته است که می‌توانند به مدیریت ارشد و هیئت مدیره در هدایت، نظارت و اندازه‌گیری عملکرد فناوری اطلاعات کمک کنند. همانطور که در شکل ۳ نشان داده شده، اجزای کلیدی راهبری فناوری اطلاعات مؤثر در سه دسته گروه بندی شده‌اند:

- *محیط‌های فرآیند* - شامل تمام فرآیندهای فناوری اطلاعات که برای ارائه خدمات به سازمان پیاده سازی می‌شوند (برای مثال، مدیریت تغییر، مدیریت امنیت اطلاعات، توسعه نرم افزار و مدیریت پروژه).
- *ساختارهای سازمانی* – شامل نقش‌های ضروری و روابط گزارش دهی تا به فناوری اطلاعات اجازه مواجه شدن با نیازهای سازمان را بدهد، در حالی که این فرصت را فراهم می‌آورد تا الزامات مشخص شده از طریق ارزیابی و اولویت‌بندی رسمی به دست آورد (شکل ۴).
- *مکانیزم‌ها* – شامل استانداردها، سیاست‌ها، و چارچوب‌های پیاده سازی شده برای هدایت، نظارت و اندازه‌گیری عملکرد فناوری اطلاعات. چارچوب راهبری فناوری اطلاعات باید تعیین کند که کدام فرآیندها باید در جایگاه اطمینان دادن به اینکه رسیک‌ها به طور رضایت بخش شناسایی، ارزیابی و نیز مشخص و پذیرفته شده مطابق با تحمل و اشتهای ریسک سازمان، قرار گیرند.

Figure 3: IT Governance Components



شکل ۴: مثال‌هایی از ساختارهای سازمانی

بدنه حاکمیت	اعضا	محدوده
هیئت مدیره راهبری فناوری اطلاعات	CAE، CIO، CFO، CEO	استراتژی کسب و کار و فناوری اطلاعات و برنامه‌های سرمایه گذاری
کمیته هدایت فناوری اطلاعات	مدیر ارشد فناوری اطلاعات، مالکان واحد کسب و کار	هم‌ترازی استراتژیک فناوری اطلاعات
دفتر پورتفوی فناوری اطلاعات	مدیران برنامه فناوری اطلاعات، برنامه کسب و کار/مدیران پروژه، مدیران پروژه فناوری اطلاعات	معیارهای پروژه فناوری اطلاعات، نظارت، و گزارشگری
دفتر معماری فناوری اطلاعات	، مدیران زیرساخت فناوری COO، CISO، CIO اطلاعات	طراحی معماری فناوری اطلاعات
شورای فناوری اطلاعات	، مالکان واحد کسب و کارCTO، CIO	ارزیابی فرصت‌های فناوری
امنیت سایبری و شورای حفاظت داده	، CAE، COO، CFO، CRO، CISO، CTO، CIO مالکان واحد کسب و کار	ارزیابی ریسک و استراتژی‌های سازمانی برای حفاظت از دارایی‌های اطلاعاتی سازمان

نقش حسابرس داخلی در راهبری فناوری اطلاعات

راهبری فناوری اطلاعات یک مسئولیت مدیریتی است، حسابرس داخلی باید مستقل باقی بماند، اما این می‌تواند موقعیت خوبی را برای تحت تأثیر قرار دادن و توصیه برای تغییر ایجاد کند.

امری ضروری است که حسابرسی فناوری اطلاعات بسته به نیرومندی سیستم راهبری فناوری اطلاعات در محل به هر دو بخش اطمینان بخشی و مشاوره تقسیم شود. استقلال نباید مانع از ارائه توصیه شود، تا زمانی که مدیریت مسئولیت کامل و پاسخگویی برای پیاده سازی و اجرای کنترل‌ها را بر عهده گیرد.

هر نوع حسابرس می‌تواند ارزیابی کند که آیا مالکان کسب و کار به دنبال سیاست‌ها هستند و حفاظت کافی از دارایی‌ها را با کار کردن با فناوری اطلاعات برای شناسایی ریسک و کنترل‌ها نشان می‌دهند.

فرآیندهای راهبری در طول فعالیت ارزیابی ریسک حسابرس داخلی و توسعه برنامه حسابرسی در نظر گرفته می‌شوند. رئیس حسابرسی داخلی (CAE) معمولاً فرآیندهای راهبری ریسک بالاتر سازمان را شناسایی می‌کند که از طریق پروژه‌های اطمینان بخشی و مشاوره‌ای که در برنامه حسابرسی نهایی شرح داده می‌شوند، مورد بررسی قرار می‌گیرند. به علاوه، رهنمود پیاده سازی ۲۱۱۰ به طور خاص فعالیت مسئولیت حسابرسی داخلی برای ارزیابی و تهیه توصیه‌های مناسب برای بهبود فرآیندهای راهبری سازمان را برای این موارد مشخص می‌کند:

- تهیه تصمیم‌های استراتژیک و عملیاتی.
- نظارت مدیریت ریسک و کنترل.
- ترویج اخلاق و ارزش‌های مناسب درون سازمان.
- اطمینان یافتن از عملکرد سازمانی مدیریت و پاسخگویی مؤثر.
- برقراری ارتباط ریسک و کنترل اطلاعات با نواحی مناسب سازمان.
- هماهنگی فعالیت‌ها، و برقراری ارتباط در میان هیئت مدیره، حسابرسی داخلی و خارجی، دیگر تهیه‌کنندگان اطمینان بخشی و مدیریت.

عواملی که می‌توانند به تقویت راهبری فناوری اطلاعات کمک کنند:

- شفاف سازی مالکیت و پاسخگویی فناوری اطلاعات.
- خط گزارشگری مدیر ارشد اطلاعات (CIO) به مدیریت ارشد.
- ارزش نوآوری که فناوری اطلاعات می‌تواند پیشنهاد دهد شناسایی شود.
- عملکرد فناوری اطلاعات نظارت و اندازه گیری شود.

حسابرسی داخلی راهبری فناوری اطلاعات باید بر شیوه‌های پیاده سازی راهبری سازمان تمرکز کند، که شامل سیاست‌ها، نقش‌ها و مسئولیت‌های به وضوح تعریف شده، هم‌ترازی اشتهای ریسک، ارتباط مؤثر، فضای اخلاقی در بالای سازمان، مدیریت ارزش فناوری اطلاعات و پاسخگویی واضح. ارزیابی‌های حسابرسی داخلی احتمالاً شامل فعالیت‌هایی از قبیل موارد زیر می‌باشد:

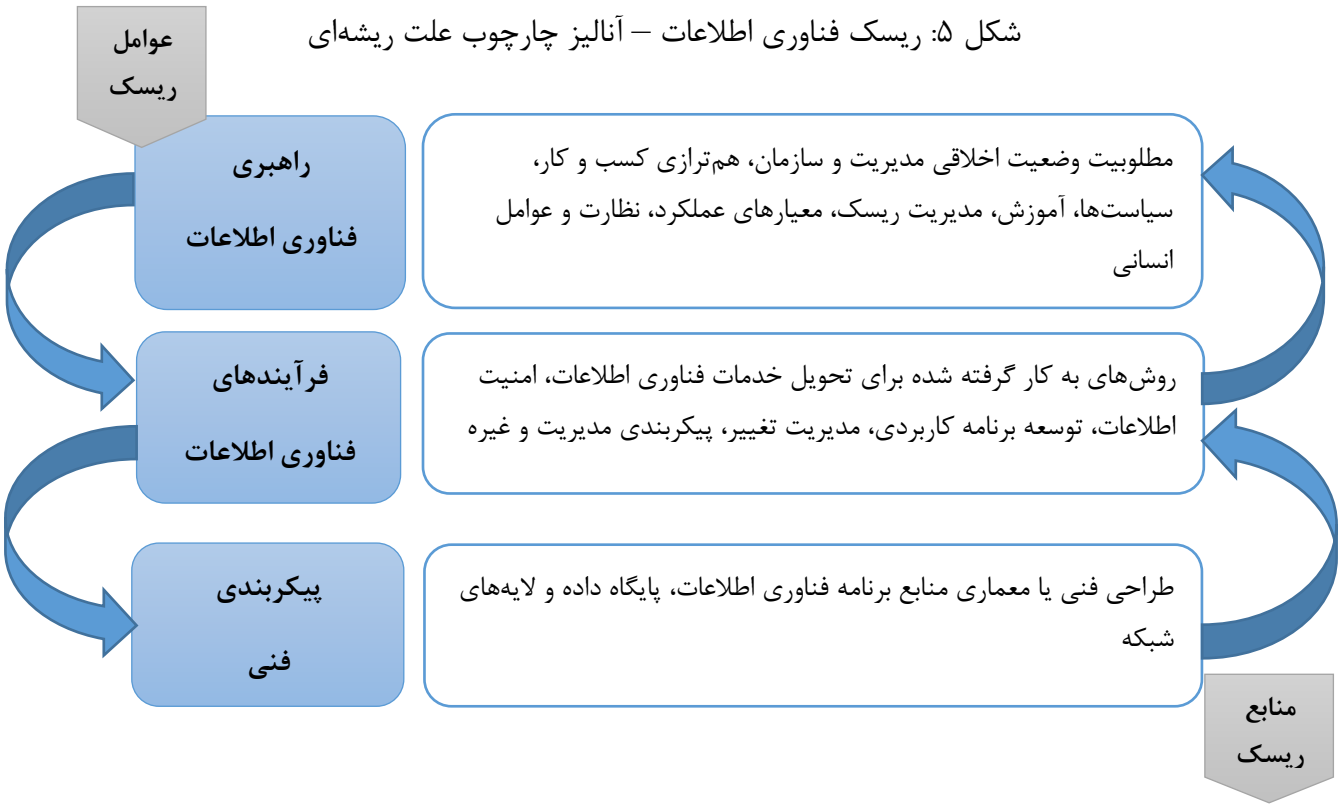
- ارزیابی درجه‌ای که فعالیت‌های راهبری و استانداردها با درک فعالیت حسابرسی داخلی از اشتهای ریسک سازمان سازگار است.
- هدایت تعاملات مشاوره‌ای مجاز از نظر منشور حسابرسی و تأیید شده توسط هیئت مدیره.
- گفتگوی مداوم با بدنه راهبری فناوری اطلاعات برای اطمینان از اینکه تغییرات اساسی سازمانی و ریسک در یک روش به موقع مشخص می‌شوند.

هنگام بررسی راهبری، حسابرسی داخلی باید بیش از آنکه فقط مشکل‌ها را شناسایی کند انجام دهد. آن‌ها نیاز به شناسایی علل ریشه‌ای و ایجاد توصیه‌های سازنده را در زمانی دارند که نقاط ضعف در کنترل‌های فناوری اطلاعات شناسایی می‌شوند؛ برای مثال، پیکربندی نامرغوب یا ضعیف دیوارآتش. در این مورد خاص، ارزیابی یک دلیل ریشه‌ای می‌تواند شامل لایه‌های مختلفی از کنترل برای شناسایی منبع مشکل باشد.

شکل ۵ یک چارچوب آنالیز علت ریشه‌ای را نشان می‌دهد که سه لایه از کنترل را نشان می‌دهد که می‌تواند برای ارزیابی نقاط ضعف فناوری اطلاعات مورد استفاده قرار گیرد. از لایه فنی شروع کنید، به لایه فرآیند بروید و بپرسید که آیا خرابی فرآیندی وجود دارد که باعث پیکربندی ضعیف دیواره آتش شده است (به عنوان مثال، عدم نظارت یا تفکیک ناکافی وظایف).

از لایه فرآیند، یک لایه دیگر به راهبری فناوری اطلاعات بالا بروید و بپرسید آیا سازمان روش‌های مؤثر فناوری اطلاعات مانند ارزیابی ریسک و توسعه سیاست، حفاظت و آموزش راجع به دیوارهای آتش دارد.

شکل ۵: ریسک فناوری اطلاعات – آنالیز چارچوب علت ریشه‌ای



فعالیت حسابرسی داخلی زمانی که علل ریشه‌ای را شناسایی کند و ایجاد برنامه‌های عمل سازنده در همکاری با مدیریت برای رسیدگی به مسئله را تضمین می‌کند، ایجاد ارزش افزوده می‌کند.

مهارت

همانطور که در استاندارد پیاده سازی 2130.A۱ اشاره شد، ارزیابی راهبری فناوری اطلاعات ممکن است شامل اطمینان بخشی و/یا خدمات مشاوره‌ای برای ارزیابی کفایت و اثربخشی کنترل‌ها در پاسخگویی به ریسک‌ها درون راهبری، عملیات‌ها، و سیستم‌های اطلاعاتی سازمان راجع به موارد زیر باشد:

- دستیابی به اهداف استراتژیک سازمان.
- قابلیت اطمینان و صحت اطلاعات مالی و عملیاتی.
- اثربخشی و کارایی عملیات‌ها و برنامه‌ها.
- حفاظت از دارایی‌ها
- انطباق با قوانین، مقررات، سیاست‌ها، رویه‌ها و قراردادها.

زمانی که به نظر می‌رسد که حسابرسی فناوری اطلاعات نیازمند تجربه گسترده فناوری اطلاعات است، جنبه‌های استراتژیک راهبری فناوری اطلاعات می‌تواند بخشی از هر تعامل عملیاتی باشد.

برنامه ریزی کار

با توجه به استاندارد ۲۲۰۰ – برنامه ریزی کار، حسابرسان داخلی باید یک برنامه برای هر کار حسابرسی شامل اهداف، محدوده، زمان بندی و تخصیص منابع کار حسابرسی ایجاد کند و مستند سازد. این برنامه باید استراتژی‌ها، اهداف و ریسک‌های سازمان مرتبط با کار حسابرسی را در نظر بگیرد. این بخش قصد دارد تا با کمک به حسابرسان داخلی جهت تعیین مناطق کلیدی که باید در برنامه حسابرسی راهبری فناوری اطلاعات باشند، نوع اسنادی که می‌توان آن‌ها را درخواست نمود، سؤالاتی که می‌توانند در مصاحبه‌ها ذکر شوند و شواهد و مدارک مستند که باید به دست آیند. مثال‌های ارائه شده جامع نیستند.

یکی از مهم‌ترین چیزهایی که یک فعالیت حسابرسی داخلی باید در برنامه‌ریزی کار حسابرسی مشخص کند این است که آیا سازمان دارای ساختار راهبری واحد و منسجم در محل، شامل سیاست‌ها، فرآیندها و ابزارهایی برای مدیریت مداوم محیط و کنترل ریسک‌های مربوط به فناوری اطلاعات است.

ممکن است حسابرسی کل برنامه راهبری فناوری اطلاعات دشوار باشد؛ به جای آن دامنه برنامه حسابرسی را می‌توان با استفاده از شاخصی که با یک هدف خاص مواجه می‌شود، تعریف کرد. برای مثال، دامنه می‌تواند توسط واحدها، مکان‌ها و اهداف استراتژیک سازمانی یا توسط هر شاخصی که برای سازمان معنی‌دار است تعریف شود.

برنامه ریزی کار حسابرسی عموماً شامل مراحل زیر می‌باشد:

- درک زمینه و هدف کار حسابرسی.
- جمع‌آوری اطلاعات برای درک منطقه یا فرآیند تحت بررسی.
- هدایت یک ارزیابی ریسک اولیه از منطقه یا فرآیند تحت بررسی .
- تشکیل دادن اهداف کار حسابرسی.
- برقرار کردن محدوده کار حسابرسی.
- تخصیص منابع.
- مستند سازی برنامه.

برای دستورالعمل‌های دقیق در مورد نحوه برنامه‌ریزی و محدوده یک کار حسابرسی، رهنمود عملی انجمن حسابرسان داخلی "برنامه‌ریزی کار: برقرار کردن اهداف و محدوده" را ببینید.

۱. درک زمینه و هدف کار حسابرسی

مدیر اجرایی حسابرسی (CAE) و حسابرسان داخلی باید با رسیدن به درک روشنی از مفهوم راهبری و مشخصات فرآیندهای راهبری معمول شروع کنند. آن‌ها همچنین باید تعریف رسمی از راهبری را در نظر بگیرند، چرا که در واژه‌نامه استانداردهای بین‌المللی برای اجرای حرفه‌ای حسابرسی داخلی، و با چارچوب‌های راهبری جهانی عموماً پذیرفته شده و مدل‌ها آشنا شوند (به عنوان مثال، کمیته سازمان‌های حامی کمیسیون تردوی [COSO] یا سازمان استانداردهای بین‌المللی [ISO] ۳۱۰۰۰ و ۳۸۵۰۰).

چارچوب‌های راهبری، مدل‌ها و نیازمندی‌ها با توجه به نوع سازمان و حوزه‌های قضایی متغیر هستند. اینکه چگونه یک سازمان اصول راهبری مؤثر را طراحی و اجرا کند به عواملی مانند اندازه، پیچیدگی، چرخه زندگی، بلوغ، ساختار سهامدار و الزامات قانونی بستگی دارد که سازمان تحت آن قرار دارد. رویکرد حسابرسی داخلی برای ارزیابی راهبری و ارائه توصیه‌هایی به مدیریت براساس چارچوب یا مدلی که سازمان از آن استفاده می‌کند متفاوت خواهد بود.

حسابرسی داخلی ابتدا باید بپرسد که سازمان از چه چارچوبی برای هدایت راهبری فناوری اطلاعات استفاده می‌کند. اگر سازمان چارچوبی پیاده‌سازی شده نداشته باشد، حسابرسی داخلی می‌تواند اجرای یک برنامه کاری مشاوره‌ای برای کمک به نقشه‌ی موجود کنترل‌ها و روش‌های مدیریت در یک چارچوب توافق شده، پیشنهاد کند.

بعد از آن ، رئیس حسابرسی داخلی (CAE) مشاهده می‌کند که آیا طرح حسابرسی داخلی فعلی فرآیندهای راهبری سازمان را در بر می‌گیرد و ریسک‌های مرتبط آن‌ها را مورد بررسی قرار می‌دهد. راهبری به عنوان مجموعه‌ای از فرآیندها و ساختارهای مستقل وجود ندارد. بلکه راهبری، مدیریت ریسک و کنترل به هم وابسته هستند. برای مثال، فعالیت‌های مؤثر راهبری در هنگام تعیین استراتژی ریسک را در نظر می‌گیرند. به همان اندازه، مدیریت ریسک بر راهبری مؤثر (مانند فضای اخلاقی در رأس سازمان، اشتهای ریسک، تحمل، و فرهنگ؛ و نظارت بر مدیریت ریسک) تکیه دارد. به همین ترتیب، راهبری مؤثر بر کنترل‌های داخلی و ارتباط با هیئت مدیره در مورد اثربخشی آن کنترل‌ها تکیه دارد.

با توجه به رهنمود پیاده سازی ۲۱۱۰ راهبری، رئیس حسابرسی داخلی ممکن است منشورهای هیئت مدیره و کمیته و همچنین دستور جلسات و صورت جلسات را بررسی کند، تا بینشی از نقش هیئت مدیره که در راهبری سازمان ایفا می‌کند به خصوص با توجه به تصمیم گیری استراتژیک و عملیاتی کسب کند. رئیس حسابرسی داخلی همچنین

راهبری فناوری اطلاعات خوب در یک نگاه

- سازمان و ساختارهای راهبری موجود نشان خوبی از این که آیا فناوری اطلاعات به سازمان در دستیابی به اهداف استراتژیک خود کمک می‌کند و از آن پشتیبانی می‌کند، ارائه می‌دهد.
- مهم است که میزان تأثیر فضای اخلاقی در بالای سازمان تعیین کنیم، اینکه چگونه این فضا به تمامی سطوح در سازمان ارتباط دارد و چگونه آن پیام بر فناوری اطلاعات تأثیر می‌گذارد.
- معیارهای تحویل خدمات، از جمله مدیریت مالی، اجزای مهم کنترل و نظارت بر اندازه گیری هزینه منفعت فناوری اطلاعات می‌باشد.
- مدیریت عملکرد استراتژیک جزء ضروری راهبری فناوری اطلاعات مؤثر است و مکانیزم‌های مناسب را قادر می‌سازد تا نیازهای سازمان و تحویل خدمات فناوری اطلاعات را اداره کنند.

ممکن است با دیگران در نقش‌های کلیدی راهبری (مانند رئیس هیئت مدیره، رأس منتخب یا منتصب در واحدهای دولتی، مدیر ارشد اخلاق، مدیر ارشد منابع انسانی، حسابرس مستقل خارجی، مدیر ارشد رعایت، مدیر ارشد ریسک) صحبت کند تا درک روشنی از فرآیندهای خاص سازمان و اطمینان بخش پیش از این به دست آورد. اگر سازمان تنظیم شده باشد، رئیس حسابرسی داخلی ممکن است بخواهد نگرانی‌های شناسایی شده توسط تنظیم کنندگان را بررسی کند.

درک راهبری اساسی برای بحث با هیئت مدیره و مدیریت ارشد در مورد آن چیزی است که راهبری را تشکیل می‌دهد، به طوری که یک طرح حسابرسی داخلی مناسب و رویکرد را می‌توان اجرا کرد.

۲. جمع آوری اطلاعات

مهم است که حسابرسان داخلی اطلاعات جمع آوری شده در طول توسعه برنامه مستند سازی کنند، مطابق با استاندارد ۲۲۰۰ – برنامه ریزی کار. مفید است که توجه داشته باشید که این فرآیند همیشه یک عدد متوالی از مراحل نیست. بلکه یک فرآیند مداوم است که باید در طول برنامه‌ریزی کار حسابرسی به روز شود چون اطلاعات جدید از طریق بررسی ارزیابی‌های پیشین (به عنوان مثال، ارزیابی ریسک و گزارش‌ها توسط ارائه دهندگان خدمات اطمینان بخش و مشاوره)، درک و برنامه ریزی جریان فرآیند و کنترل‌ها یا مصاحبه با سهامداران مربوطه به دست می‌آید.

رهنمود پیاده سازی ۲۲۱۰ همچنین نشان می‌دهد که معمولاً یک حسابرسی واحد از راهبری انجام نمی‌شود. در عوض، ارزیابی فعالیت حسابرسی داخلی از فرآیندهای راهبری محتمل است که براساس اطلاعات به دست آمده از وظایف حسابرسی متعدد در طول زمان باشد.

اگر یک ارزیابی کلی از راهبری مناسب باشد، موارد زیر در نظر گرفته می‌شود:

- نتایج حسابرسی داخلی فرآیندهای خاص راهبری که در بالا شناسایی شد.
- مسائل حاکمیت ناشی از حسابرسی که به طور خاص بر راهبری متمرکز نیستند، مانند:
  - برنامه ریزی استراتژیک.
  - بهره‌وری و اثربخشی عملیاتی.
  - کنترل داخلی بر گزارشگری مالی.
  - خطرات مرتبط با فناوری اطلاعات، تقلب، و نواحی دیگر.
  - انطباق با قوانین و مقررات قابل اجرا.

- نتایج ارزیابی ریسک.
- نتایج ارزیابی‌های مدیریتی (به عنوان مثال، بازرسی‌های رعایت، حسابرسی‌های کیفیت، و کنترل خود - ارزیابی).
- کار ارائه دهندگان اطمینان بخشی خارجی (به عنوان مثال، بازرسان قانونی، دفاتر عمومی حسابرس دولت و شرکت‌های حسابداری دولتی) و قانون گذاران.
- کار ارائه دهندگان اطمینان بخشی داخلی، یا خط دوم توابع دفاع (به عنوان مثال، سلامت و ایمنی، رعایت و کیفیت).
- سایر اطلاعات مربوط به مسائل مربوط به راهبری، مانند حوادث نامساعد، فرصتی برای بهبود فرآیندهای راهبری را نشان می‌دهند.

۲,۱ دستیابی به اطلاعات و مستند سازی اطلاعات

به دست آوردن درک کامل از سازمان و راهبری فناوری اطلاعات حسابرسان داخلی را قادر می‌سازد تا یک ارزیابی اولیه از ریسک‌های مرتبط انجام دهند، همانطور که توسط استاندارد ۲۲۱۰.A1 خواسته شده است. منابع اطلاعات شامل مستند سازی و مصاحبه با سهامداران هستند.

حداقل در پایان این مرحله برنامه کار حسابرسی باید شامل موارد زیر باشد:

- اهداف ناحیه تحت بررسی.
- استراتژی‌های مورد استفاده برای رسیدن به این اهداف.
- ریسک‌ها برای رسیدن به این اهداف.
- فرآیندها و کنترل‌های کلیدی.
- فناوری اطلاعات و سایر سیستم‌های مربوط به ناحیه یا فرآیند تحت بررسی.
- منابع و قابلیت اتکا داده‌ها در داخل یا بیرون ناحیه یا فرآیند تحت بررسی.

نمونه‌هایی از مستنداتی که حسابرس داخلی می‌تواند برای برنامه ریزی برنامه کار حسابرسی داخلی راهبری فناوری اطلاعات درخواست کند شامل موارد زیر است:

- گزارش‌های حسابرسی پیشین.
- برنامه‌های استراتژیک (مأموریت و چشم‌انداز سازمان).
- چارچوب راهبری سازمانی.

- چارچوب راهبری فناوری اطلاعات.
- سیاست امنیت اطلاعات.
- سیاست‌های معماری فناوری اطلاعات.
- چارت‌های سازمانی.
- استراتژی و اهداف سازمان.
- گزارش‌های مدیریت ریسک بنگاه.
- عملکرد گزارش‌های فناوری اطلاعات.
- صورت جلسات راهبری.
- صورت جلسات کمیته و هیئت مدیره.
- گزارش‌های مدیریت.
- مصوبات و مستندات استثناها.

پیوست C یک پرسشنامه کنترل داخلی ارائه می‌دهد که می‌تواند به حسابرسان داخلی کمک کند تا درک سطح بالا از راهبری فناوری اطلاعات موجود را توسعه دهند و چگونه بهترین دامنه رسیدگی، برنامه‌ریزی و اجرای یک برنامه کار حسابرسی را تعیین کنند.

۲,۲ مصاحبه با سهامداران مربوطه

مصاحبه با سهامداران مربوطه یک گام بحرانی است که به حسابرسان داخلی کمک می‌کند تا اهداف، طراحی، عملیات و محیط کنترل محدوده یا فرآیند تحت بررسی را بهتر درک کنند. در اغلب موارد، چارت سازمانی می‌تواند به حسابرسان داخلی در شناسایی سهامداران مربوطه کمک کند.

مصاحبه با رؤسای اداری ممکن است نشان آشکار کند که چه فرآیندهایی به تصمیمات استراتژیک و عملیاتی هدایت می‌شوند، اندازه گیری اینکه آیا تلاش‌های سازمان به آگاهی کافی از جایگاه اخلاقی آن منجر می‌شود، و اینکه آیا کارمندان درک روشنی از مسئولیت‌های خود بر روی فرآیندهای ریسک و کنترل و تأثیر بر سازمان دارند.

نمونه‌هایی از سؤالات مصاحبه

- آیا هیئت مدیره وابستگی سازمان به فناوری اطلاعات را درک می‌کند؟ چگونه این درک در برنامه استراتژیک منعکس می‌شود؟
- آیا تعریف روشنی از نقش شما در راهبری فناوری اطلاعات دارید؟ از کجا می‌دانید که شما انتظارات را برآورده می‌کنید؟
- شما با کدام اعضای تصمیم گیری هنگام تصمیم گیری‌های مرتبط با فناوری اطلاعات مشورت می‌کنید؟

- چه سیاست‌هایی وجود دارد و چگونه آن‌ها توسط کمیته‌های مختلف راهبری و کمیته‌های فرعی منتشر می‌شوند؟
- سازمان چگونه ارزش را اندازه‌گیری می‌کند؟

علاوه بر این، حسابرسان داخلی ممکن است با پرسنل فردی یا در گروه‌های منتخب برای شناسایی خطرات مرتبط اندیشه گشایی کنند. برای این منظور، حسابرسان ممکن است بپرسند، "چه چیزی اهداف کسب و کار را از دیده شدن محافظت خواهد کرد؟" علاوه بر این، برای شناسایی ریسک‌های ذاتی، حسابرسان داخلی ممکن است بپرسند، "چه مشکلی پیش خواهد آمد اگر هیچ کنترلی در محل وجود نداشته باشد؟"

۳. انجام یک ارزیابی ریسک اولیه

به دلیل محدودیت‌های زمانی و منابع، تمام خطرات را نمی‌توان در طول یک کار حسابرسی مورد بررسی قرار داد. بنابراین، حسابرسان داخلی باید یک ارزیابی ریسک اولیه انجام دهند و ریسک‌ها را با توجه به اهمیت، که به صورت ترکیبی از عوامل ریسک اندازه‌گیری می‌شود، اولویت‌بندی کنند.

یک روش مؤثر برای انجام و مستند کردن یک ارزیابی ریسک سطح کار حسابرسی اولیه، ایجاد یک نمودار نشان‌دهنده خطرات و کنترل‌های مربوطه، مانند یک ماتریس ریسک و کنترل است. یک ماتریس ریسک و کنترل ابزاری است که به طور معمول توسط حسابرسان داخلی برای شناسایی، سازماندهی و ارزیابی خطرات مورد استفاده قرار می‌گیرد که ممکن است اهداف تجاری محدوده تحت بررسی، و نیز هر گونه کنترل‌های کاهش دهنده را تحت تأثیر قرار دهند.

برای دستورالعمل‌های دقیق در مورد توسعه :

- سناریوهای ریسک.
- ماتریس ریسک و کنترل.
- نقشه‌های اولویت‌بندی ریسک (به عنوان مثال، نقشه بوته).

به رهنمود تمرین انجمن حسابرسان داخلی "برنامه‌ریزی کار حسابرسی: تعیین اهداف و دامنه رسیدگی" مراجعه کنید.

شکل ۶ نمونه‌ای از ماتریس ریسک و کنترل ایجاد شده با استفاده از خطرات شناسایی شده در سناریوهای ریسک را نشان می‌دهد. در این ماتریس، تأثیر و احتمال رتبه بندی نیز گنجانده می‌شوند.

شکل 6: ماتریس ریسک و کنترل برای راهبری فناوری اطلاعات

سناریو ریسک	ریسک	کنترل
در یک مدل عملیاتی غیر متمرکز، واحدهای کسب‌وکار استراتژیک (SBUs) اجازه دارند که بیشتر مستقل و خودگردان عمل کنند، با بودجه‌های فناوری اطلاعات خود و استفاده از برنامه‌های کاربردی مختلف و زیرساخت فناوری اطلاعات.	سازمان احتمالاً موفق نخواهد بود یک مجموعه از استانداردهای فناوری اطلاعات را در سراسر سازمان با توجه به برنامه‌های کاربردی، زیرساخت فناوری اطلاعات، فرآیندها، و رویه‌ها به طور مؤثر مستقر کند.	معماری بنگاه فناوری اطلاعات باید ساختار سازمانی را نشان دهد تا هم‌ترازی بهتر و برآورده کردن نیازهای سازمان را ممکن سازد. توسعه ساختار راهبری فناوری اطلاعات باید بر اساس طراحی‌های معماری فعلی و پیش‌بینی شده فناوری اطلاعات باشد.
سازمان مدیریت ریسک را به عنوان بخشی از شیوه‌های مدیریت پروژه شامل نمی‌شود.	پروژه‌ها می‌توانند به دلیل برنامه‌ریزی ضعیف برای رسیدگی به ریسک‌ها شکست بخورند.	یک فرآیند برای ارزیابی، بررسی و ارتباط دادن ریسک‌های فناوری اطلاعات به سهامداران کلیدی و مدیریت اجرایی در طول پروژه، تغییر، و انتشار فرآیندهای مدیریت وجود دارد.

پیوست D یک ماتریس ریسک و کنترل برای راهبری فناوری اطلاعات ارائه می‌دهد. این ماتریس به عنوان نمونه تهیه شده است و باید برای مواجهه با نیازهای خاص سازمان تحت بررسی سفارشی باشد.

۴. شکل دهی اهداف کار حسابرسی

هنگامی که حسابرسان داخلی ارزیابی اولیه ریسک را کامل کردند و خطرات قابل‌توجهی را برای ارزیابی در طول کار حسابرسی شناسایی کردند، می‌توانند اهداف کار حسابرسی را شکل دهند. اهداف کار حسابرسی بیان می‌کنند که کار حسابرسی به طور خاص در تلاش برای انجام چیست؛ بنابراین، اهداف باید هدف مشخصی داشته باشند، مختصر باشند و با ارزیابی ریسک مرتبط باشند (استاندارد 2210.A1).

اهداف کار حسابرسی برای راهبری فناوری اطلاعات می‌توانند به نیازمندی‌های راهبری فناوری اطلاعات خارجی و داخلی، یا عملکرد عملیاتی فرآیندهای راهبری فناوری اطلاعات مرتبط باشند، و می‌توانند در راه‌های مختلف تعریف شوند. برای مثال، اهداف را می‌توان به عنوان بخشی از برنامه حسابرسی سالانه تعریف کرد، یا به عنوان نتیجه‌ای از نتایج مدیریت ریسک بنگاه (ERM)، یافته‌های حسابرسی قبلی، الزامات قانونی، یا با نیازهای اطمینان بخشی خاص از هیئت مدیره یا کمیته حسابرسی.

حسابرسان داخلی نیز باید معیارهای کافی برای ارزیابی راهبری، مدیریت ریسک، و کنترل محدوده یا فرآیند تحت بررسی را شناسایی کرده و تعیین کنند که آیا اهداف و اهداف کسب و کار انجام شده‌اند. شناسایی این معیارها

اطمینان می‌دهد که اهداف اطمینان بخشی کار حسابرسی قابل اندازه‌گیری، عملی و هم‌تراز با اهداف سازمان و محدوده یا فرآیند تحت بررسی است.

با توجه به استاندارد 2210.A3، حسابرسان داخلی باید از معیارهایی که پیش از این توسط مدیریت و/یا هیئت مدیره ایجاد شده‌اند استفاده نمایند، اگر چنین معیارهایی وجود داشته باشد. اگر هیچ معیاری وجود نداشته باشد، حسابرسان داخلی باید معیارهای مناسب را از طریق بحث با مدیریت و هیئت مدیره شناسایی کنند. حسابرسان داخلی نیز باید به دنبال ورودی از موضوع اهمیت متخصصان برای کمک به توسعه معیارهای مربوطه باشند.

نمونه‌هایی از معیار شامل موارد زیر است:

- عملکرد شاخص‌های کلیدی موجود.
- اهداف تنظیم شده در طول برنامه ریزی استراتژیک.
- درجه‌ی انطباق با محدوده یا سیاست‌ها و رویه‌های فرآیند، قوانین خارجی، و مقررات، و/یا قراردادها.
- استانداردها و معیارهای صنعتی.

برای اجتناب از تفسیر اشتباه یا چالش هر پرسنلی که مسئول محدوده یا فرآیند تحت بررسی باشد، معیار ارزیابی باید مرتبط، قابل اطمینان و مستند باشد. با این حال، معیارهای مناسب، مرجعی برای حسابرسان داخلی برای ارزیابی شواهد، درک یافته‌ها و ارزیابی کفایت کنترل‌ها در محدوده یا فرآیند تحت بررسی ارائه می‌دهد. معیار یا فقدان آن باید با معیارهای صنعتی، گرایش‌ها، و پیش‌بینی‌ها و همچنین سیاست‌ها و رویه‌های سازمان مقایسه شوند.

موارد زیر مثال‌هایی از این هستند که چگونه می توان اهداف کار حسابرسی اطمینان بخش را برای کار حسابرسی راهبری فناوری اطلاعات فرموله کرد.

فعالیت حسابرسی داخلی اطمینان می‌دهد که:

- فعالیت‌های راهبری فناوری اطلاعات و استانداردها با درک فعالیت حسابرسی داخلی از اشتهای ریسک سازمان سازگار هستند.
- اعضای راهبری فناوری اطلاعات در حال پرداختن به تغییرات اساسی سازمانی و ریسک در یک روش به موقع هستند.
- پیوند ماتریس‌ها و اهداف فناوری اطلاعات و با اهداف سازمان هم‌تراز است.
- معیارها به درستی اجرا می‌شوند تا دیدگاه‌های واقع بینانه از عملیات‌های فناوری اطلاعات و راهبری بر پایه تاکتیکی و استراتژیک ارائه دهند.

۴,۱ اهداف مشاوره کار حسابرسی

حسابرسان داخلی می‌توانند در تعدادی از ظرفیت‌های مختلف برای ارزیابی و توصیه کردن راه‌هایی برای بهبود شیوه‌های راهبری عمل کنند. آن‌ها ممکن است ارزیابی‌های مستقل و هدفمند از طراحی و اثربخشی فرآیندهای راهبری را در سازمان تهیه کنند. به علاوه – یا به جای – ارائه اطمینان بخشی، حسابرسان داخلی ممکن است انتخاب کنند که خدمات مشاوره‌ای ارائه دهند.

این می‌تواند یک رویکرد ارجح باشد، به خصوص زمانی که مسایل شناخته شده وجود دارند و یا فرآیند راهبری رشد نیافته است. خواه اینکه اطمینان بخشی یا خدمات مشاوره‌ای ارائه دهند، رئیس حسابرسی داخلی ممکن است تصمیم به استفاده از روش‌های نظارت مستمر بگیرد، مانند تخصیص حسابرسان داخلی به مشاهده جلسات نهادهای مرتبط با راهبری و مشاوره آن‌ها به صورت مداوم، همانطور که در رهنمود پیاده سازی ۲۱۱۰ نشان داده شده است.

به دلیل اینکه خدمات مشاوره‌ای در طبیعت مشورتی هستند، اهداف و انتظارات یا به وسیله یا در ارتباط با مشتری کار حسابرسی تعیین می‌شوند. بنابراین، برنامه‌ریزی کار حسابرسی مشاوره‌ای معمولاً بعد از اهداف و دامنه رسیدگی کار حسابرسی که قبلاً تعیین شده است، اتفاق می‌افتد. بنابراین حسابرسان داخلی ممکن است نیاز به تکمیل ارزیابی اولیه ریسک نداشته باشند، چرا که آن‌ها در هنگام برنامه‌ریزی یک کار حسابرسی اطمینان‌دهی انجام می‌دهند. با این حال، استاندارد 2201.C1 به حسابرسان داخلی نیاز دارد تا درکی با مشتری کار حسابرسی مشاوره‌ای درباره اهداف، دامنه رسیدگی، مسئولیت‌ها و دیگر انتظارات ایجاد نماید. برای کارهای حسابرسی قابل توجه، این درک باید سندسازی شود.

علاوه بر این، حسابرسان داخلی باید به راهبری، مدیریت ریسک، و فرآیندهای کنترل تا حد مورد توافق با مشتری کار حسابرسی مشاوره‌ای بپردازند (استاندارد 2210.C1). اگرچه هدف و انتظارات کار حسابرسی مشاوره‌ای توسط مشتری کار حسابرسی هدایت می‌شود، حسابرسان داخلی باید اطمینان حاصل کنند که اهداف کار حسابرسی با ارزش‌ها، استراتژی‌ها و اهداف استراتژیک سازمان سازگار هستند (استاندارد 2210.C2).

یک کار حسابرسی الگوبرداری می‌تواند نقطه شروع مؤثر در یک برنامه حسابرسی چندین ساله را فراهم کند، زیرا به زمان مدیریت اجازه می‌دهد تا پیش از انجام بررسی‌های بیشتر، به شکاف طراحی در ساختار راهبری بپردازد.

یک هدف برای کار حسابرسی مشاوره‌ای راهبری فناوری اطلاعات می‌تواند این موارد باشد:

- فعالیت حسابرسی داخلی بر اثربخشی ساختارهای سازمانی موجود توصیه می‌کند که فعالیت‌های اصلی راهبری فناوری اطلاعات را پشتیبانی می‌کنند.

- فعالیت حسابرسی داخلی بر اثربخشی کنترل‌های راهبری موجود بر تغییر و اصلاح مدیریت توصیه خواهد کرد.

۵. تعیین دامنه رسیدگی کار حسابرسی

هنگامی که اهداف مبتنی بر ریسک شکل گرفتند، دامنه رسیدگی کار حسابرسی را می‌توان تعیین کرد. از آنجا که یک کار حسابرسی عموماً نمی‌تواند همه چیز را پوشش دهد، حسابرسان داخلی باید تعیین کنند که چه چیزی را شامل خواهد بود و چه چیزی را شامل نخواهد بود. دامنه رسیدگی کار حسابرسی مرزهای کار حسابرسی را تعیین می‌کند و اینکه چه چیزی در بررسی شامل شود را از قبل تعیین می‌کند. حسابرسان داخلی باید به دقت مرزهای کار حسابرسی را در نظر بگیرند تا اطمینان حاصل شود که این دامنه رسیدگی برای رسیدن به اهداف کار حسابرسی کافی خواهد بود (استاندارد ۲۲۲۰ – دامنه رسیدگی کار حسابرسی).

دامنه رسیدگی ممکن است چنین عناصری را به عنوان فرآیندهای خاص و/یا محدوده‌ها، موقعیت‌های جغرافیایی، و دوره زمانی تعریف کند (به عنوان مثال، نقطه به زمان ، سه ماهه مالی یا سال تقویمی) که توسط کار حسابرسی، منابع موجود داده شده پوشش داده می‌شود. حسابرسان داخلی باید به دقت وسعت دامنه رسیدگی را در نظر بگیرند تا اطمینان حاصل شود که شناسایی به موقع اطلاعات قابل اتکا، مرتبط، و مفید را برای به انجام رساندن اهداف شناسایی شده کار حسابرسی، ممکن سازد (استاندارد ۲۲۱۰ – اهداف کار حسابرسی و استاندارد ۲۳۱۰ – شناسایی اطلاعات).

تیم کار حسابرسی داخلی باید برای تعیین دامنه رسیدگی و اجرای کار حسابرسی راهبری فناوری اطلاعات، این کار را انجام دهد:

- تعیین اینکه تابع فناوری اطلات با اهداف و استراتژی‌های سازمان هم‌تراز است و آن‌ها را درک می‌کند یا نه.
- ساختار سازمانی را بررسی کنید تا مشخص کنید آیا مدیر ارشد اطلاعات وجود دارد یا خیر، و اینکه آیا این فرد عضو تیم مدیریت ارشد است یا خیر.
- ارزیابی درجه‌ای که در آن فعالیت‌ها و استانداردهای راهبری با درک فعالیت حسابرسی داخلی از اشتهای ریسک سازمان سازگار هستند.
- تعیین اثربخشی منبع فناوری اطلاعات و عملکرد مدیریت.
- ارزیابی ریسک‌هایی که ممکن است به طور زیان‌آور بر محیط فناوری اطلاعات تأثیر بگذارند.

۶. تخصیص دادن منابع

بعد از تعیین اهداف و دامنه رسیدگی کار حسابرسی، حسابرسان داخلی باید منابع مناسب و کافی برای دستیابی به اهداف کار حسابرسی تعیین کنند، همانطور که در استاندارد ۲۲۳۰ – تخصیص منابع کار حسابرسی خواسته شده. تفسیر اطلاعات استاندارد ۲۲۳۰ روشن می‌کند که واژه *مناسب* به ترکیبی از دانش، مهارت‌ها، و صلاحیت‌های دیگر مورد نیاز برای انجام کار حسابرسی اشاره دارد، و واژه *کافی* به مقدار منابع مورد نیاز برای انجام کار جسابرسی با توجه به مراقبت حرفه‌ای اشاره دارد.

منابع بر اساس موارد زیر به کار حسابرسی تخصیص داده می‌شوند:

- دانشی که حسابرسان داخلی در طول برنامه ریزی کار حسابرسی به دست می‌آورند.
- ماهیت و پیچیدگی کار حسابرسی.
- محدودیت‌های زمانی و/یا تعداد ساعت‌هایی که برای کار حسابرسی در نظر گرفته شده است.
- دانش، مهارت‌ها و تجربه‌ی منابع در دسترس.

حسابرسان داخلی باید در نظر بگیرند که آیا منابع خارجی (به عنوان مثال، متخصصان یا منابع مکمل) یا فناوری زمانی که فعالیت حسابرسی داخلی منابع مناسب یا کافی ندارد، ضروری خواهد بود.

۷. مستندسازی برنامه

در طول برنامه ریزی، حسابرسان داخلی اطلاعات دا در کاربرگ‌های حسابرسی مستندسازی می‌کنند. این اطلاعات بخشی از برنامه کاری حسابرسی می‌شود که باید برای دستیابی به اهداف حسابرسی ایجاد شوند، همانطور که در استاندارد ۲۲۴۰ – برنامه کار حسابرسی خواسته شده است.

فرآیند ایجاد اهداف و دامنه رسیدگی حسابرسی ممکن است هر یا همه‌ی کاربرگ‌های زیر را تهیه کند:

- نقشه فرآیند.
- خلاصه مصاحبه‌ها و جلسات ایده پردازی.
- ارزیابی ریسک اولیه (مانند ماتریس ریسک و کنترل و نقشه حرارتی).
- استدلال برای تصمیمات با توجه به اینکه کدام ریسک‌ها در حسابرسی شامل می‌شوند.
- معیارهایی که برای ارزیابی محدوده یا فرآیند تحت بررسی استفاده خواهند شد (خواسته شده برای حسابرسی‌های اطمینان بخش، با توجه به استاندارد پیاده سازی 2210.A3).

گزارش نتایج کار حسابرسی

سبک و فرمت گزارش نتایج کار حسابرسی در سازمان‌ها متفاوت است و باید قوانین و مقررات، فرهنگ سازمانی و سیاست‌های ارتباطی، و انتظارات مدیریت ارشد و هیئت مدیره یا معادل اعضای راهبری را به حساب بیاورند.

به دلیل اینکه راهبری فناوری اطلاعات یک عنصر استراتژیک کل ساختار راهبری یک سازمان است، مهم است که رئیس حسابرسی داخلی برای برقراری ارتباط با مدیریت ارشد، هیئت مدیره و کمیته حسابرسی نتایج حاصله از حسابرسی راهبری فناوری اطلاعات را بررسی کنند تا آن‌ها بتوانند هر گونه ضعف آشکار را در حین کار برای انجام مسئولیت‌های فردی خود مورد بررسی قرار دهند. استاندارد ۲۰۶۰ - گزارش به مدیریت ارشد و هیئت مدیره توضیح می‌دهد که مسئولیت رئیس حسابرسی داخلی شامل مسائل مهم ریسک و کنترل می‌شود، شامل مسائل حکومتی که نیازمند توجه این نهادها هستند. راهبری فناوری اطلاعات برای ساختار و استراتژی کل سازمان کلیدی است، و کسانی که موظف هستند با مسئولیت پذیری برا تصمیم گیری در بالاترین سطوح سازمان باید مطلع باشند همانطور که آن‌ها تأثیر استراتژیک راهبری فناوری اطلاعات را در نظر می‌گیرند.

به رهنمود عملی انجمن حسابرسان داخلی: "برقراری ارتباط نتایج حسابرسی اطمینان بخش" برای راهنمایی دقیق در مورد چگونگی تهیه گزارش حسابرسی داخلی مراجعه کنید.

راهبری فناوری اطلاعات از الزامات مقرراتی، قانونی، محیطی و عملیاتی سازمان حمایت می‌کند تا دستیابی به برنامه‌های استراتژیک و آرمان‌ها را ممکن سازد، بنابراین لازم است که مدیریت ارشد، هیئت مدیره و کمیته حسابرسی به موقع از نتایج حسابرسی راهبری فناوری اطلاعات مطلع شوند.

پیوست A. استانداردها و رهنمودهای مرتبط انجمن حسابرسان داخلی (IIA)

انتخاب‌های زیر از استانداردهای بین‌المللی از انجمن حسابرسان داخلی (IIA) برای عمل حرفه‌ای حسابرسی داخلی مربوط به راهبری فناوری اطلاعات است. این انتخاب‌ها لزوماً به طور کامل ارائه نمی‌شوند؛ آن‌ها ممکن است یک زیرمجموعه از استاندارد باشند که به طور خاص مربوط به این راهنما است. لطفاً برای اعلامیه کامل به استانداردها رجوع کنید. برای کمک به اجرای این استانداردها، انجمن حسابرسان داخلی توصیه می‌کند که حسابرسان داخلی به راهنمای پیاده سازی مربوط به هر استاندارد مراجعه کنند.

رهنمود پیاده سازی	استاندارد
IG1210 - مهارت	1210 - مهارت
IG2000 - مدیریت فعالیت‌های حسابرسی داخلی	2000 - مدیریت فعالیت حسابرسی داخلی
IG2110 - راهبری	2110 - راهبری
IG2130 - کنترل	2130 - کنترل
IG2200 - برنامه ریزی کار حسابرسی	2200 - برنامه ریزی کار حسابرسی
IG2201 - برنامه ریزی ملاحظات	2201 - برنامه ریزی ملاحظات
IG2210 - اهداف کار حسابرسی	2210 - اهداف کار حسابرسی
IG2220 - دامنه حسابرسی	2220 - دامنه حسابرسی
IG2230 - تخصیص منابع حسابرسی	2230 - تخصیص منابع حسابرسی
IG2400 - نتایج برقراری ارتباط	2400 - نتایج برقراری ارتباط

رهنمود مرتبط انجمن حسابرسان داخلی

رهنمود عملی، "برقراری ارتباط نتایج کار حسابرسی اطمینان بخش،" انجمن حسابرسان داخلی، اکتبر. 2016.
رهنمود عملی، "برنامه ریزی حسابرسی: تعیین اهداف و دامنه رسیدگی،" انجمن حسابرسان داخلی، آگوست. 2017
رهنمود عملی، "برنامه ریزی حسابرسی: ارزیابی ریسک‌های تقلب،" انجمن حسابرسان داخلی، اکتبر. 2017.

پیوست B. واژه نامه

Assurance Services (خدمات اطمینان بخش) – یک بررسی عینی از شواهد و مدارک برای هدف ارائه یک ارزیابی مستقل از راهبری، مدیریت ریسک، و فرآیندهای کنترل برای سازمان. نمونه‌هایی از آن عبارتند از: مالی، عملکرد، رعایت، امنیت سیستم، و دقت عمل کارهای حسابرسی.

Board (هیئت مدیره) – بالاترین سطح اعضای راهبری (برای مثال هیئت مدیره، هیئت نظارت، و هیئت امنا) که عهده‌دار مسئولیت هدایت کردن و/یا نظارت بر فعالیت‌های سازمان و حفظ پاسخگویی مدیریت ارشد می‌باشد. اگرچه چیدمان راهبری در بین حوزه‌ها و بخش‌ها متفاوت است، اما معمولاً هیئت مدیره شامل اعضایی است که جزئی از مدیریت نیستند. اگر که هیئت مدیره وجود نداشته باشد، کلمه "board" در استانداردها به گروه یا شخصی اشاره دارد که عهده‌دار راهبری در سازمان است. علاوه بر این، "board" در استانداردها ممکن است به کمیته یا اعضای دیگری اشاره داشته باشد که وظایف خاص را انجام می‌دهند (برای مثال، کمیته حسابرسی).

Chief Audit Executive (رئیس اجرایی حسابرسی) – نقش یک فرد در مقام ارشد که مسئول مدیریت مؤثر فعالیت حسابرسی داخلی مطابق با منشور حسابرسی داخلی و عناصر الزامی چارچوب اجرای حرفه‌ای بین‌المللی است را توصیف می‌کند. رئیس اجرایی حسابرسی یا افراد دیگر که به رئیس اجرایی حسابرسی گزارش می‌دهند، گواهی‌نامه‌ها و صلاحیت‌های حرفه‌ای لازم را خواهند داشت. عنوان خاص شغل و/یا مسئولیت رئیس اجرایی حسابرسی ممکن است در میان سازمان‌ها متفاوت باشد.

Compliance (رعایت) – تبعیت از سیاست‌ها، برنامه‌ها، روش‌ها، قوانین، مقررات، قراردادها یا سایر الزامات.

Consulting Services (خدمات مشاوره‌ای) – مشاوره و فعالیت‌های مربوط به خدمات مشتری، ماهیت و دامنه رسیدگی که با مشتری توافق شده است، برای افزودن ارزش و بهبود راهبری سازمان، مدیریت ریسک، و کنترل فرآیندها بدون اینکه حسابرس داخلی مسئولیت مدیریت را در نظر بگیرد، در نظر گرفته شده‌اند. مانند مشورت، مشاوره، تسهیلات و آموزش.

Control Processes (فعالیت‌های کنترل) – سیاست‌ها، روش‌ها (هم دستی و هم خودکار) و فعالیت‌هایی که بخشی از یک چارچوب کنترل هستند، طراحی‌شده و اجرا شده برای اطمینان از اینکه ریسک‌ها در سطحی هستند که یک سازمان مایل به پذیرش آن است.

Governance (**راهبری**) – ترکیب فرآیندها و ساختارهای اجرا شده توسط هییت مدیره برای اطلاع رسانی، هدایت، مدیریت و نظارت بر فعالیت‌های سازمان در جهت رسیدن به اهداف آن.

Information Technology Governance (**راهبری فناوری اطلاعات**) – شامل رهبری، ساختارهای سازمانی، و فرآیندهایی که تضمین می‌کنند که فناوری اطلاعات شرکت از استراتژی‌ها و اهداف سازمان پشتیبانی می‌کند.

Internal Audit Activity (**فعالیت حسابرسی داخلی**) – یک قسمت، بخش، گروهی از مشاوران، یا دیگر متخصصان است که اطمینان بخشی مستقل و عینی و خدمات مشاوره‌ای طراحی شده برای افزودن ارزش و بهبود عملیات یک سازمان را ارائه می‌دهد. فعالیت حسابرسی داخلی به یک سازمان کمک می‌کند تا اهداف خود را با آوردن یک رویکرد سیستماتیک و منظم برای ارزیابی و بهبود اثربخشی راهبری، مدیریت ریسک، و فرآیندهای کنترل به انجام برساند.

Management (**مدیریت**) – برای به اجرا در آوردن کنترل و نظارت درون قدرت و مسئولیت برقرار شده توسط راهبری. اصطلاح مدیریت اغلب به عنوان یک عبارت جمعی برای افراد با مسئولیت کنترل یک سازمان یا بخشی از یک سازمان به کار می‌رود.

Risk (**ریسک**) – امکان اتفاق افتادن رویدادی که بر دستیابی به اهداف تاثیرگذار خواهد بود. ریسک برحسب تأثیر و احتمال اندازه‌گیری می‌شود.

Risk Appetite (**اشتهای ریسک**) – سطح ریسکی که یک سازمان مایل به پذیرش آن است.

Senior Management (**مدیریت ارشد**) – گروهی از افراد که از اعضای راهبری که به منظور اجرای استراتژی‌ها و سیاست‌ها برای تحقق اهداف سازمان منصوب شده‌اند. این گروه می‌تواند شامل نقش‌هایی باشد که به اعضای راهبری یا رئیس سازمان گزارش می‌دهند یا مسئولیت کلی برای عملکرد گزارش دهی عمده دارند، به عنوان مثال مدیر ارشد اجرایی (CEOs)، رئیس سازمان‌های دولتی، مدیر ارشد اطلاعات (CIOs) و نقش‌های مشابه.

Significance (**اهمیت**) – اهمیت نسبی یک موضوع مربوط به یک زمینه که در نظر گرفته شده است، شامل عوامل کمی و کیفی، مانند اندازه، ماهیت، اثر، ارتباط، و تأثیر. قضاوت حرفه‌ای در هنگام ارزیابی اهمیت مسائل در زمینه اهداف مربوطه به حسابرسان داخلی کمک می‌کند.

Standard (استاندارد) – یک بیانیه حرفه‌ای که توسط هیئت استانداردهای حسابرسی داخلی بین‌المللی منتشر شده است که الزامات برای اجرای طیف وسیعی از فعالیت‌های حسابرسی داخلی و برای ارزیابی عملکرد حسابرسی داخلی را مشخص می‌کند.

پیوست C. پرسشنامه کنترل‌های داخلی راهبری فناوری اطلاعات

پرسشنامه زیر برای کمک به حسابرسان داخلی جهت ارزیابی وضعیت فعلی راهبری فناوری اطلاعات به عنوان بخشی از مرحله برنامه‌ریزی کار حسابرسی تدوین شده است.

ساختارهای سازمان و راهبری	
پرسش‌های زیر به حسابرس داخلی کمک خواهد کرد تا درجه یا حضور راهبری فناوری اطلاعات را درک کند:	
پرسش	**ارزیابی/پیشنهادات**
آیا در اینجا مدیر ارشد اطلاعات وجود دارد، و آیا این یکی از اعضای تیم مدیریت ارشد است؟	
آیا ساختار سازمان و اجزای عملیاتی آن به وضوح سازماندهی شده است که عملکرد فناوری اطلاعات می‌تواند به طور کافی و مؤثر به ممکن ساختن دستیابی به اهداف سازمان کمک کند؟	
آیا نهادهای تصمیم گیری در جایی برای ممکن ساختن هم‌ترازی نیازهای سازمانی با خدمات فناوری اطلاعات قرار دارند و آیا آن‌ها دارای توانمند سازی و پاسخگویی کافی هستند؟	
آیا نیازهای سازمانی و الزامات خدمات فناوری اطلاعات در طرح‌های استراتژیک و تاکتیکی تعریف شده‌اند، و تحت نظارت هستند؟	
آیا مدیر ارشد اطلاعات و مدیریت ارشد با هم ملاقات کرده و درباره پیشرفت برنامه‌ها به طور منظم بحث و تبادل نظر می‌کنند؟	
آیا نقش‌ها و مسئولیت‌ها به وضوح تعریف شده مرتبط هستند، و آیا رهبران سازمان برای نتایج توانمند و پاسخگو هستند؟	

رهبری و پشتیبانی اجرایی	
پرسش‌های زیر به حسابرس داخلی کمک خواهد کرد تا درکی از درجه‌ای که عملکرد فناوری اطلاعات در سازمان ادغام می‌شود به دست آورد:	
پرسش	**ارزیابی/پیشنهادات**
آیا مدیریت ارشد به روشنی نقش و مسئولیت‌های مربوط به عملکرد فناوری اطلاعات را با توجه به دستیابی سازمانی به اهداف استراتژیک و تاکتیکی تعریف و ابلاغ کرده است؟	
آیا نقش‌ها و مسئولیت‌های مدیر ارشد اطلاعات به وضوح تعریف و ابلاغ شده است؟	
آیا سازمان در استراتژی خود به رسمیت شناخته می‌شود که عملکرد فناوری اطلاعات یک شرکت کننده مهم در توانمند سازی دستیابی به اهداف، و همچنین حمایت از سازمان در یک مبنای روز به روز است؟	
آیا مدیر ارشد اطلاعات با هیئت مدیره و تیم مدیریت ارشد برای بحث در مورد تحویل خدمات فناوری اطلاعات مرتبط با برنامه‌های استراتژیک و تاکتیکی به طور منظم شرکت می‌کند؟	
آیا تأمین بودجه کافی برای برآورده کردن نیازهای سازمان وجود دارد؟	

برنامه‌ریزی استراتژیک و عملیاتی	
حسابرس داخلی می‌تواند درکی از اینکه چگونه عملکرد استراتژیک مدیریت که توسط مدیریت ارشد پیاده سازی شده است را با پرسیدن پرسش‌های زیر به دست آورد:	
پرسش	**ارزیابی/پیشنهادات**
آیا هیئت مدیره و مدیریت ارشد فناوری اطلاعات را به عنوان یک شریک استراتژیک سازمانی می‌بینند؟	
آیا طرح استراتژیک سازمان شامل این می‌شود که چگونه فناوری اطلاعات برای پشتیبانی و ممکن ساختن خلق ارزش مورد نیاز است؟	
آیا برنامه استراتژیک که پشتیبانی شده توسط طرح‌های عملیاتی تاکتیکی منحصر به فرد است نیازها و خروجی‌های فناوری اطلاعات را در نظر می‌گیرد؟	
آیا شاخص‌های کلیدی عملکرد (KPIs) توسط مدیریت ارشد برای اندازه گیری و نظارت بر اثربخشی تابع فناوری اطلاعات استفاده می‌شوند؟	
آیا تصمیمات استراتژیک سرمایه گذاری فناوری اطلاعات مبتنی بر تجزیه و تحلیل دقیق منفعت - هزینه هستند و پس از پیاده سازی برای تعیین اینکه آیا ROI برنامه ریزی شده تحقق یافته است، مورد ارزیابی قرار می‌گیرد؟	
آیا درس‌ها در تصمیمات آتی سرمایه‌گذاری فناوری اطلاعات به حساب می‌آیند؟	
آیا سازمان فناوری اطلاعات نسبت به اندازه و ترکیب بندی سازمان به طور مؤثر سازماندهی شده است؟	
آیا مدیر ارشد اطلاعات و رهبری فناوری اطلاعات واجد شرایط و با تجربه هستند؟	

تحویل و اندازه‌گیری خدمات	
حسابرس داخلی می‌تواند درک درستی از چگونگی عملکرد مدیریت مالی فناوری اطلاعات با پرسیدن سؤالات زیر به دست آورد:	
پرسش	**ارزیابی/پیشنهادات**
آیا هیئت مدیره و مدیریت ارشد درک روشنی از هزینه‌های فناوری اطلاعات دارند و چگونه در دستیابی به اهداف استراتژیک سازمان شرکت می‌کنند؟	
آیا رهبران سازمان ارزش فناوری اطلاعات و خروجی‌ها را اندازه‌گیری می‌کنند؟ اگر اینطور است، چگونه؟	
هزینه‌های فناوری اطلاعات چگونه با دیگر سازمان‌های قابل‌مقایسه، مقایسه می‌شود؟	
آیا عملکرد مدیر ارشد اطلاعات با داده‌های مالی و غیرمالی سنجیده می‌شود؟	
آیا ترتیبات منبع یابی در محل وجود دارد؟ اگر بله، آیا آن‌ها اندازه گیری و نظارت می‌شوند؟	

سازمان فناوری اطلاعات و مدیریت ریسک	
حسابرسان داخلی می‌توانند با پرسیدن سوالات زیر، درک سطح بالایی از محیط راهبری فناوری اطلاعات را به دست	
پرسش	**ارزیابی/پیشنهادات**
تا چه درجه‌ای فرآیندهای سازمانی خودکار شده‌اند؟	
زیرساخت فناوری اطلاعات چقدر پیچیده است و چه تعداد برنامه کاربردی در آن استفاده می‌شود؟	
آیا داده‌ها استانداردسازی شده و به راحتی در میان برنامه‌های کاربردی تقسیم شده‌اند؟	
آیا استاندارد فناوری اطلاعات سخت افزار، نرم افزار، و سیاست‌های تدارکات خدمات، روش‌ها، و کنترل‌ها در محل وجود دارد؟	
فرآیندهای مدیریت فناوری اطلاعات چگونه کامل شده‌اند و چارچوب‌های شناخته شده چگونه به کار گرفته می‌شوند (به عنوان مثال، ISO ،ITIL، COBIT)؟	
چگونه ریسک‌ها در ارتباط با نیازهای جمعی سازمانی، امنیت و الزامات رعایت مدیریت می‌شوند؟	
اهمیت استراتژیک فناوری اطلاعات چیست؟	

پیوست **D**. ماتریس ریسک و کنترل برای راهبری فناوری اطلاعات

این پیوست نمونه‌هایی از اهداف کسب و کار، ریسک‌ها، و کنترل‌ها را برای کمک به حسابرسان داخلی فراهم می‌کند تا برنامه کار حسابرسی را توسعه دهند.

ساختارهای سازمان و راهبری	
هدف کنترل: ساختارهای سازمانی باید شامل خطوط شفاف گزارش و نقش مسئولیت‌ها باشند.	
ریسک	**کنترل**
پاسخگویی به وضوح تعریف نشده است و منجر به فقدان شفافیت در هزینه‌های فناوری اطلاعات، فرآیندها، پروژه‌ها و خدمات می‌شود.	اهداف و مقاصد استراتژیک سازمان باید اهداف عملیاتی را هدایت کنند، و مسئولیت پذیری برای دستیابی به اهداف باید بر روی رهبران واحد جهت ارتقا پاسخگویی شفاف قرار گیرد.
فقدان توانمند سازی و پاسخگویی که منجر به فرصت‌های از دست رفته بالقوه برای نوآوری و هم‌کاری می‌شود.	رهبران فناوری اطلاعات و واحد کسب و کار باید قادر به مدیریت منابع درون محدوده مسئولیت خود باشند، و آن‌ها را قادر به مدیریت به سوی اهداف عملکرد مورد انتظار می‌کند.
هم‌ترازی استراتژیک و درک مبهم بین سازمان و عملکردهای فناوری اطلاعات منجر به کاهش سهم بازده سهامداران می‌شود.	ایجاد ساختارهای سازمانی چند رشته‌ای اجازه نمایندگی منافع مختلف درون سازمان از جمله حسابرسی داخلی را می‌دهد که منافع کل سازمان را نشان می‌دهد.
مدیریت ارشد و هیئت مدیره رابطه اولیه فناوری اطلاعات و اهداف کسب و مار را درک نمی‌کنند، که می‌تواند منجر به تخصیص غیر مؤثر منابع به ابتکارات استراتژیک و/یا درک ضعیف از هزینه‌های کلی فناوری اطلاعات و ورودی آن‌ها به عوامل بازده سرمایه گذاری (ROI) گردد.	نقش‌ها و مسئولیت ها باید مکانیزم‌هایی را ارائه دهند که استفاده از فناوری اطلاعات را به استراتژی‌ها و اهداف کلی سازمان پیوند دهند.
هدف کنترل: ساختارهای سازمانی شامل ماهیت عملیاتی اجزای آن‌ها و پروتکل‌های ارتباطی هستند.	
ریسک	**کنترل**
کانال‌های ارتباطی مبهم بین فناوری اطلاعات و رهبران واحد سازمانی، منجر به برنامه‌ریزی و سیستم نظارتی غیر مؤثر می‌شود.	برای اطمینان از ثبات در سراسر سازمان، ارتباط مؤثر مداوم در مورد راهبری فناوری اطلاعات باید در تمام واحدها و عملکردها حفظ شود. یک برنامه ارتباطی مناسب باید شامل ابعاد و معیارهایی باشد که باید اطلاع رسانی شود، تهیه کننده‌ها و گیرنده‌ها، فرکانس و روش‌های تشدید.

هدف کنترل: پرسنل فناوری اطلاعات قادر به تخصیص منابه به اهداف کسب و کار هستند.	
ریسک	**کنترل**
نقش‌های فناوری اطلاعات و مسئولیت‌های مبهم منجر به عدم توازن منابع و اهداف عملیاتی می‌گردد.	فرآیندها، نقش‌ها، و مسئولیت‌های پرسنل فناوری اطلاعات تعریف، مستند سازی و ابلاغ شده است.
به کار گیری غیر مسئولانه منابع فناوری اطلاعات و دارایی‌ها به دلیل عدم وجود فرآیندهای فناوری اطلاعات سازگار و قابل تکرار.	فرآیندها به صورت دوره‌ای هستند و ارزیابی می‌شوند تا مطمئن شوند آن‌ها سازگار و قابل تکرار هستند.
هدف کنترل: سازمان و فناوری اطلاعات درباره اولویت‌های منابع، ابتکارات و تصمیمات کلی سرمایه‌گذاری هم‌کاری می‌کنند.	
ریسک	**کنترل**
مدیریت ارشد فناوری اطلاعات در فرآیند تصمیم‌گیری گنجانده نشده است تا فناوری اطلاعات و اهداف سازمان را همسو کند، که منجر به ناتوانی فناوری اطلاعات در پشتیبانی از تصمیم‌گیری‌ها یا تنظیم تغییر به موقع اولویت‌ها می‌شود.	مدیریت ارشد و هیئت مدیره باید فناوری اطلاعات را در تصمیمات استراتژیک در مورد راهبری دخیل سازند و فناوری اطلاعات را قادر به افزودن ارزش در تصمیمات کلیدی کنند.
فقدان یا ضعیف بودن پرتفوی فرآیندهای مدیریت فناوری اطلاعات ممکن است منجر به اولویت بندی ضعیف سرمایه گذاری‌های فناوری اطلاعات گردد.	یک فرآیند مدیریت پورتفوی قوی وجود دارد که به سازمان و فناوری اطلاعات اجازه می‌دهد تا در اولویت‌های منابع، ابتکارات و تصمیمات کلی سرمایه‌گذاری هم‌کاری کنند.
ناهماهنگی بین منابع فناوری اطلاعات و اهداف عملیاتی ناشی از نارضایتی ذینفعان خارجی و داخلی از روشی که سازمان عمل می‌کند و نتایج مالی (دولت، تنظیم کنندگان، جامعه به طور کلی، سهامداران ، هیئت مدیره، شرکای تجاری، مشتریان، تأمین کنندگان، مشاوران، کارمندان و حسابرسان خارجی).	رهبران واحد سازمان با مدیر ارشد اطلاعات و دیگر رهبران عملکرد فناوری اطلاعات تشکیل جلسه می‌دهند تا مؤثرترین روش‌ها برای حمایت و دستیابی بیشتر به اهداف هر رهبر واحد را تعیین کنند.
هدف کنترل: ساختار راهبری فناوری اطلاعات هم‌تراز با معماری فناوری اطلاعات تعریف شده است (برای مثال، اگر مدیریت استراتژیک درون ستاد متمرکز شده باشد، ساختار راهبری نیز باید متمرکز باشد).	
ریسک	**کنترل**
معماری شرکت ناکافی می‌تواند منجر به سرمایه‌گذاری غیر ضروری در تکنولوژی‌های اضافی یا ناسازگار شود.	معماری شرکت فناوری اطلاعات باید ساختار سازمانی را منعکس کند تا همسویی بهتر را ممکن سازد و نیازهای سازمان را برآورده کند.
ناهماهنگی بین ساختار راهبری فناوری اطلاعات و معماری فناوری اطلاعات می‌تواند منجر به فرآیندهایی شود که نیازهای سازمان را پشتیبانی نمی‌کنند و می‌تواند برای اصلاح کردن بیش از حد گران باشند.	توسعه ساختار راهبری فناوری اطلاعات باید براساس طراحی‌های فعلی و پیش‌بینی‌شده معماری فناوری اطلاعات باشد.

رهبری و پشتیبانی اجرایی	
هدف کنترل: چشم‌انداز، مأموریت و استراتژی وابسته به سازمان به طور جمعی مسیر سرمایه‌گذاری فناوری اطلاعات را فراهم می‌کند.	
ریسک ذاتی	**کنترل**
فقدان یک چشم‌انداز واضح، مأموریت و برنامه استراتژیک برای سازمان و نقش فناوری اطلاعات می‌تواند منجر به استفاده غیر مؤثر از سرمایه فناوری اطلاعات و سایر منابع مورد نیاز برای تحقق اهداف استراتژیک سازمان شود.	چشم انداز سازمانی مبنایی برای تعریف چارچوب‌ها، فرآیندها، فعالیت‌ها، نقش‌ها و روابط می‌باشد. این دیدگاه باید به شکل یک برنامه استراتژیک مستند سازی شود که وابستگی‌های فناوری اطلاعات را تعریف می‌کند.
یک رابطه شفاف بین شاخص‌های عملکرد پروژه فناوری اطلاعات و اهداف سازمانی وجود ندارد.	اهداف سازمانی و فناوری اطلاعات و معیارها هم‌تراز هستند.
مدیریت ارشد در فرآیند تصمیم‌گیری فناوری اطلاعات که می‌تواند به گمراهی منابع فناوری اطلاعات منجر شود، به طور مناسب درگیر نیست.	نقش‌ها مشخص، ابلاغ و پذیرفته می‌شوند و به صراحت برای تصمیم‌گیری سرمایه‌گذاری، حمایت از برنامه، مدیریت برنامه، مدیریت پروژه، تحویل خدمات و نقش‌های پشتیبانی مربوطه پذیرفته می‌شوند.
فقدان تعریف ارزش و هزینه فناوری اطلاعات از لحاظ تأثیر بر مقاصد و اهداف سازمان می‌تواند منجر به توانایی ضعیف فناوری اطلاعات برای رسیدن به مقاصد و اهداف آن و همچنین مقاصد و اهداف کلی استراتژیک سازمان شود.	آموزش رسمی باید برای صاحبان اطلاعات و مدیران فراهم شود. این آموزش باید در طول روند شبانه روزی کارمند اجباری باشد و جلسات توجیهی متناوب باید برای توضیح هر گونه تغییر در سیاست‌ها و چگونگی تأثیر آن بر شیوه‌های کاری توسعه یابد.
هدف کنترل: بودجه فناوری اطلاعات به مدیریت ارشد مرتبط می‌باشد.	
ریسک ذاتی	**کنترل**
مدیریت ارشد از تأمین مالی فناوری اطلاعات و مفاهیم آن برای منابع شرکت آگاهی ندارد.	بودجه‌ها به صورت دوره‌ای به روز شده و ابلاغ می‌شوند.
هدف کنترل: بودجه‌ها کنترل و نظارت می‌شوند.	
ریسک ذاتی	**کنترل**
بودجه‌های فناوری اطلاعات به پروژه‌های غیر استراتژیک بدون بررسی و تأیید مناسب مجدداً تخصیص می‌یابند.	شیوه‌های برنامه‌ریزی مالی فناوری اطلاعات به طور منظم مورد بررسی قرار می‌گیرند و اطمینان وجود دارد که منابع در صورت ارائه مستندات و تأییدات مناسب، مجداً تخصیص داده می‌شوند.
هزینه‌های فناوری اطلاعات با اهداف تجاری هم‌تراز نیستند، که ممکن است منجر به تخصیص منابع به اهداف غیر بحرانی شوند.	لازم است که مدیریت به عنوان مبنایی برای هیئت مدیره و مدیریت ارشد برای ایجاد بهترین تصمیمات ممکن، یک تجزیه و تحلیل منفعت هزینه و محاسبات بازدهی سرمایه سرمایه گذاری‌های فناوری اطلاعات را فراهم کند.

هدف کنترل: رهبری سازمانی سرمایه‌گذاری‌های انجام شده در فناوری اطلاعات را درک می‌کند.	
ریسک ذاتی	**کنترل**
مدیریت ارشد و رهبران واحد، درک درستی از فناوری اطلاعات ندارند، که می‌تواند منجر به از دست دادن فرصت‌ها یا کاهش بازدهی سرمایه گذاری شود.	برای کاهش احتمال تصمیمات نادرست سرمایه‌گذاری فناوری اطلاعات، رهبران سازمان باید مشخصات مهم فناوری اطلاعات را درک کنند. برای رسیدن به این هدف، از مدیر ارشد اطلاعات برای شرکت در جلسات هیئت مدیره برای بحث در مورد ریسک و فرصت‌های مرتبط با فناوری دعوت شده است.
فقدان تمرکز سازمانی محوری توسط مدیریت ارشد فناوری اطلاعات می‌تواند به این معنا باشد که فناوری اطلاعات قادر به تمرکز بر تلاش‌ها یا شناسایی استفاده ناکارآمد از منابع نیست.	مدیریت ارشد و هیئت مدیره باید درک روشنی از اهداف و استراتژی‌های اصلی داشته باشند.
هدف کنترل: ابتکارات فناوری اطلاعات به درستی با اهداف سازمانی هم‌تراز هستند.	
ریسک ذاتی	**کنترل**
اهمیت استراتژیک فناوری اطلاعات ارزیابی نشده است، که منجر به درک اشتباه از نقشی که فناوری اطلاعات در سازمان ایفا می‌کند، می‌شود.	فناوری اطلاعات و رهبران سازمانی بر مبنای دوره‌ای برای بازبینی اقدامات فعلی و آتی فناوری اطلاعات جهت ارزیابی مجدد هم‌ترازی با اهداف سازمانی (به عنوان مثال، ارزیابی اعتبار و صحت اسناد و مدارک کسب و کار) تشکیل جلسه می‌دهند.
قابلیت ناکافی فناوری اطلاعات و/یا تخصیص منابع به ارائه خدمات خواسته شده می‌تواند منجر به فواید فناوری به دست نیایند، و منجر به از دست دادن فرصت‌ها شود؛ ناتوانی در دستیابی به اهداف سازمانی و فناوری اطلاعات.	
منابع فناوری اطلاعات به اهدافی اختصاص می‌یابند که ضروری نیستند.	
هدف کنترل: راهبری فناوری اطلاعات به دفاع نوآوری در فناوری اطلاعات و کل سازمان کمک می‌کند.	
ریسک ذاتی	**کنترل**
عدم تعهد رهبری اجرایی می‌تواند به دفاع ناکافی از نوآوری در عملکرد فناوری اطلاعات و در سراسر سازمان منجر شود.	تعهد رهبری با اقداماتی که استراتژی فناوری اطلاعات را پشتیبانی می‌کند ثابت شده است.

برنامه ریزی استراتژیک و عملیاتی	
هدف کنترل: استراتژی‌های فناوری اطلاعات و کسب و کار هم‌تراز شده‌اند.	
ریسک ذاتی	**کنترل**
هم‌ترازی و درک استراتژیک مبهم بین سازمان و عملکردهای فناوری اطلاعات می‌تواند منجر به موارد زیر شود: کاهش مشارکت به بازده سهامداران. تخصیص غیر مؤثر منابع به اقدامات استراتژیک. فقدان شفافیت هزینه‌های فناوری اطلاعات، فرآیندها، پروژه‌ها و خدمات. درک ضعیف از هزینه‌های کلی فناوری اطلاعات و ورودی آن‌ها به عوامل بازدی سرمایه.	پاسخگویی‌ها و روش‌ها در چارچوب‌های راهبری مستند سازی شده‌اند. مدیر ارشد اطلاعات در جلسات اجرایی هیئت مدیره شرکت می‌کند و مشارکت فناوری اطلاعات در اهداف شرکت مورد بحث قرار می‌گیرد.
ساختارهای سازمانی مبهم و/یا ناکافی می‌تواند منجر به موارد زیر شود: عدم مدیریت منابع و فعالیت‌های متناقض. عدم توازن با منابع و اهداف عملیاتی. عدم رضایت ذینفعان خارجی و داخلی از روشی که سازمان عمل می‌کند.	چارجوب راهبری از فرآیندها تشکیل شده است و شامل اطلاعات درباره‌ی فعالیت‌های فرآیند، مالکان و محدوده‌های بهبود می‌باشد.
کانال‌های ارتباطی مبهم بین فناوری اطلاعات و رهبران واحد سازمانی می‌تواند منجر به برنامه ریزی و روش‌های نظارت غیر مؤثر گردد.	سازمان استراتژیک باید شامل پروتکل‌های ارتباطی باشد تا اطمینان حاصل شود که فناوری اطلاعات و سازمان یک گفتگوی آزاد را برقرار می‌کنند.
هدف کنترل: سازمان نقش‌ها را شامل پاسخگویی، سطوح اختیار، و حقوق تصمیم گیری تعریف می‌کند.	
ریسک ذاتی	**کنترل**
استفاده غیر مسئولانه از منابع فناوری اطلاعات و دارایی‌ها به دلیل عدم وجود فرآیندهای فناوری اطلاعات سازگار و قابل تکرار.	توصیفات شغلی رسمی و روابط گزارش دهی برای همه موقعیت‌های فناوری اطلاعات ایجاد و ابلاغ شده است. فرآیندها به درستی مستندسازی و منتشر می‌شوند، و کارمندان می‌دانند که چگونه آن‌ها را پیدا کنند.
سرمایه‌گذاری‌های فناوری اطلاعات و اولویت‌ها با اهداف کسب و کار هم‌تراز نیستند.	استراتژی فناوری اطلاعات اغلب برای ثبت بازخورد از ذینفعان مستند و به روز می‌شود.
هدف کنترل: منابع فناوری اطلاعات زمان بیشتری را به وظایف مربوط به اهداف استراتژیک اختصاص می‌دهند.	
ریسک ذاتی	**کنترل**
تخصیص ناکافی منابع برای ارائه خدمات ضروری فناوری اطلاعات می‌تواند منجر به عدم دستیابی به مزایای تکنولوژی، از دست دادن فرصت‌ها، یا ناتوانی کامل در دستیابی به اهداف سازمانی گردد.	منابع فناوری اطلاعات (کارمندان، برنامه‌ها، سخت‌افزار) به پشتیبانی از اهداف سازمانی اختصاص داده شده‌اند.

تحویل و اندازه‌گیری خدمات	
هدف کنترل: فناوری اطلاعات برنامه‌ها، بودجه‌ها و تعهدات خود را ارائه می‌دهد.	
ریسک ذاتی	**کنترل**
ارائه ضعیف خدمات فناوری اطلاعات تأثیر منفی بر فرآیندهای اصلی کسب و کار دارد.	برای بررسی معیارهای عملکرد کلیدی و موارد صحیح که در زیر سطوح معقول قرار دارند، فرآیندهایی در حال انجام است.
هدف کنترل: بخش فناوری اطلاعات معیارهای عملکرد را به ذینفعان کلیدی گزارش می‌دهد.	
ریسک ذاتی	**کنترل**
مدیریت ارشد و هیئت مدیره آگاهی روشنی از عملکرد فناوری اطلاعات براساس داده‌های قابل سنجش ندارند.	یک برنامه ارتباطی مناسب باید شامل ابعاد و معیارهایی برای اطلاع رسانی، تهیه کنندگان و دریافت کنندگان، فرکانس، و روش‌های تشدید باشد.
دستیابی به اهداف استراتژیک نظارت و گزارش نشده است.	اهداف استراتژیک به جای اینکه تغییر کرده باشند یا دیده نشده باشند، به دست می‌آیند.
فعالیت‌های مدیریت عملکرد شامل معیارهای سه طرفه نمی‌شود.	فعالیت‌های عملکرد مدیریت هم فعالیت‌های داخلی و هم سه طرفه فناوری اطلاعات را در نظر می‌گیرند.
عدم واکاوی از کل به جزء قابلیت‌ها به معیارهای سطح پایین‌تر در صورت نیاز می‌تواند منجر به موارد زیر شود: بازدهی سرمایه سرمایه گذاری فناوری اطلاعات نظارت نمی‌شود. فقدان اطلاعات تصمیم گیری. هزینه‌های بیشتر از واحدهای قابل مقایسه.	گزارشگری مالی باید با جزئیات کافی تعریف شود تا قابلیت‌های واکاوی از کل به جزء و تجزیه و تحلیل هزینه مجاز شوند.
فقدان داده‌های مالی دقیق می‌تواند منجر شود که ارزش ارائه شده توسط فناوری اطلاعات به درستی پی‌گیری نشود.	داده‌های مالی مربوط به سرمایه‌گذاری فناوری اطلاعات به دست آمده و به ذینفعان گزارش شده است.
هدف کنترل: عملکرد فناوری اطلاعات در شرایط فناوری اطلاعات و کسب و کار گزارش شده است.	
ریسک ذاتی	**کنترل**
گزارش‌های فناوری اطلاعات با استفاده از اصطلاحات خاص فناوری اطلاعات تهیه می‌شوند.	گزارش‌ها عملکرد فناوری اطلاعات باید به روش‌هایی سازماندهی شوند که درک آن‌ها توسط ذینفعان فناوری اطلاعات و غیر فناوری اطلاعات آسان باشد.
هدف کنترل: معیارهای مبتنی بر تغییر نیازهای کسب و کار.	
ریسک ذاتی	**کنترل**
شاخص‌های عملکرد مبهم موفق به ارائه یک وضعیت دقیق از اقدامات فناوری اطلاعات نیستند.	شاخص‌های عملکرد از جمله معیارها و محک‌ها تعریف شده‌اند.

سازمان فناوری اطلاعات و مدیریت ریسک	
هدف کنترل: سطح ریسک مربوط به فناوری اطلاعات که شرکت مایل به پذیرفتن آن برای رسیدن به اهداف خود است تعریف شده است (اشتهای ریسک).	
ریسک ذاتی	**کنترل**
ریسک فناوری اطلاعات از اشتهای ریسک سازمان تجاوز می‌کند.	سازمان نظارت بر مدیریت ریسک فناوری اطلاعات و فعالیت‌های کنترل را فراهم می‌کند.
ریسک فناوری اطلاعات از قدرت تحمل ریسک سازمان تجاوز می‌کند.	ارزیابی‌های ریسک و سناریوهای ریسک مکرراً به روز می‌شوند و نتایج به درستی انتقال داده می‌شوند.
ریسک فناوری اطلاعات در مدیریت ریسک شرکت (ERM) ادغام نشده است.	استراتژی مدیریت ریسک سازمان شامل ریسک‌های مرتبط با فناوری اطلاعات می‌باشد.
اطلاعات ریسک و کنترل به مناطق مناسب سازمان ارسال نمی‌شود، که می‌تواند منجر به تصمیم گیری در خارج از تحمل ریسک سازمان شود.	یک فرآیند برای ارزیابی، اداره و ارتباط دادن ریسک‌های فناوری اطلاعات به ذینفعان کلیدی و مدیریت اجرایی در طول پروژه، تغییر، و انتشار فرآیندهای مدیریت وجود دارد.
هدف کنترل: یک تداوم کسب و کار و برنامه بازیابی فاجعه وجود دارد و بر مبنای دوره‌ای آزمایش می‌شود .	
ریسک ذاتی	**کنترل**
سازمان شکاف‌های با اهمیت امنیت اطلاعات را تجربه می‌کند که منجر به واکنش منفی مشتری و آسیب به شهرت عمومی سازمان می‌شود.	سازمان یک فرآیند برای مدیریت ریسک‌های بزرگ، تهدیدها، تغییرات و احتمالات فعالانه پیاده سازی کرده است.
هدف کنترل: پروژه‌های به موقع و طبق بودجه تحویل داده می‌شوند.	
ریسک ذاتی	**کنترل**
فرآیندهای مدیریت پروژه شامل ارزیابی‌های ریسک نیستند.	یک برنامه مدیریت ریسک وجود دارد و فعالیت‌های مدیریت ریسک در پروژه، تغییر، و منتشر کردن فرآیندهای مدیریتی گنجانده می‌شوند.
هدف کنترل: پروفایل ریسک فناوری اطلاعات مرتباً به روز می‌شود.	
ریسک ذاتی	**کنترل**
پروفایل ریسک فناوری اطلاعات به درستی مدیریت نمی‌شود، که منجر به ریسک‌های اداره نشده یا ریسک بالاتر از حدود تحمل می‌شود.	پروفایل ریسک فناوری اطلاعات به عنوان بخشی از اقدامات خوب مدیریت ریسک شرکت (ERM) به روزرسانی می‌شود.

سازمان فناوری اطلاعات و مدیریت ریسک	
هدف کنترل: طبقه‌بندی دارایی مشخص می‌کند که سطح کنترل برای اداره و استفاده کردن از آن مورد نیاز است.	
ریسک ذاتی	**کنترل**
کارکنان شخصی و یا داده‌های مشتری می‌توانند برای دسته‌های غیر مجاز داخلی و خارجی منتشر شده یا در دسترس باشند.	جزییات طبقه‌بندی، استفاده، مبدأ و مکان باید در یک دفتر ثبت اطلاعات دارایی وارد شوند. این باید توسط مدیران فناوری اطلاعات انجام شود.
دفتر ثبت دارایی به روز نمی‌شود تا ریسک‌های جدید، تهدیدات یا آسیب‌پذیری‌ها منعکس کند.	فرآیندها برای حفظ ثبت، باید توسعه داده شوند و به طور مداوم مناطق پر ریسک را شناسایی کنند.
هدف کنترل: برنامه‌های تشویقی سازمان برای پیش‌گیری یا شناسایی رفتار غیرقابل‌قبول، طراحی شده‌اند.	
ریسک ذاتی	**کنترل**
عملکرد مدیریت و پاسخگویی ناسازگار می‌تواند منجر به اقداماتی شود که از اهداف استراتژیک پشتیبانی نمی‌کنند.	این سازمان سیاست‌ها و فرآیندهای مربوط به پاداش کارکنان، تنظیم هدف و ارزیابی عملکرد را اجرا کرده است.
رفتار غیر قابل قبول یا ریسک بیش از حد، تشخیص داده نمی‌شود.	اندازه‌گیری‌های مرتبط (به عنوان مثال، شاخص‌های عملکرد کلیدی) و طرح‌های تشویقی (به عنوان مثال، پاداش) به طور مناسب برای جلوگیری یا شناسایی رفتار غیر قابل قبول یا اتخاذ ریسک بیش از حد و برای حمایت از اقدامات هتراز با اهداف استراتژیک سازمان طراحی و اجرا می‌شوند.

پیوست E. منابع اضافی

The Committee on the Financial Aspects of Corporate Governance, Financial Aspects of Corporate Governance (The Cadbury Report), 1992. http://www.ecgi.org/codes/documents/cadbury.pdf.

COBIT is a framework for the governance of enterprise IT published by ISACA in 2012. www.isaca.org/cobit/pages/default.aspx.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 38500:2015, Governance of IT for the Organization, 2015 version is a framework for corporate governance of IT and is a key input to other frameworks such as ITIL and COBIT. https://www.iso.org/standard/62816.html.

IT Infrastructure Library (ITIL) is a framework developed by the United Kingdom's Cabinet Office as a library of best practice processes for IT service management. https://www.itil-itsmworld.com/index.htm.

The Institute of Directors in Southern Africa (IoDSA), King Report on Corporate Governance and King Code of Corporate Governance (King III) was compiled by the King Committee in response to the emergence of the South African companies Act 71 of 2008. A new King IV was published on Nov. 1, 2016. http://www.iodsa.co.za/?kingIII.

National Computing Centre, IT Governance: Developing a successful governance strategy, NACD 2005.

NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, NIST 2011.

Organisation for Economic Co-operation and Development (OECD), G20/OECD Principles of Corporate Governance, 2015 version.

سپاس‌گزاری‌ها

تیم توسعه رهنمودها

Himi Tina Kim CIA, CGAP, CRMA, United States (Chairman)
Avin Mansookram, South Africa (Project Lead)
Kenneth Drinkard, United States
Sajay Rai, United States
Terence Washington, CIA, CRMA, United States

همکاران رهنموهای جهانی

Harun Abdul Haqq, CIA, CISA, CFE, Trinidad and Tobago
Graciela Braga, CGEIT, CSX (F), Argentina
Jason Brucker, CISA, CGEIT, United States
Elastos Chimwanda, CIA, CISA, Zimbabwe
Jamie DuBray, CIA, CRMA, CISA, CGEIT, CISSP, United States
Ulrich Hahn, CIA, CGAP, CRMA, CISA, Germany
Nigel James, CISA, United States
Stephen Stanbury, CIA, CRMA, CFE, United Kingdom

استانداردها و رهنمودهای جهانی انجمن حسابرسان داخلی

Eva Sweet, Director (Project Lead)
Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President
Debi Roth, CIA, Managing Director
Lauressa Nelson, Technical Writer
Michael Citro, Technical Writer

انجمن حسابرسان داخلی مایل است از نهادهای نظارتی زیر برای حمایتشان تشکر کند: کمیته رهنمودهای فناوری اطلاعات، شورای مشورتی رهنمودهای حرفه‌ای، هیئت استانداردهای بین‌المللی حسابرسی داخلی، مسئولیت حرفه‌ای وکمیته اخلاق و شورای نظارت چارچوب اجرای حرفه‌ای بین‌المللی.