حسابرسی فناوری اطلاعات و گزارش‌گری آن

مرتضی اسدی و میترا یافتیان

حسابرسی فناوری اطلاعات به ارزیابی سیستماتیک و هدفمند فرایندها و فعالیت‌های مرتبط با فناوری اطلاعات پرداخته و برای شناسایی و پوشش ریسک‌های این حوزه؛ کنترل‌های به‌کارگرفته شده در فناوری اطلاعات جهت حفاظت از دارایی‌های سازمان، همسویی کنترل‌های به‌کارگرفته شده با اهداف کلی کسب و کار و یکپارچگی داده‌ها را در سطح کلان سازمانی دنبال می‌کند. با این توضیح حسابرسی فناوری اطلاعات آزمون انطباق نیست. برخی بر این باورند که حسابرسان فناوری اطلاعات به دنبال کسب اطمینان از تطبیق افراد و فرایندها با مجموعه‌ای از مقررات - ضمنی یا صریح - هستند و کاری که انجام می‌دهند گزارش استثناهایی از اجرای مقررات است. در واقع این وظیفه مدیریت است. انطباق با مقررات مورد علاقه حسابرسان فناوری اطلاعات نیست. حسابرسان فناوری اطلاعات بررسی می‌کنند که آیا سیستم‌های مربوط واحد تجاری یا فرایندهای تجاری برای دستیابی به انطباق و نظارت بر آن مؤثر است یا خیر. حسابرسان فناوری اطلاعات همچنین اثربخشی طراحی مقررات را ارزیابی می‌کنند - این‌که آیا آن‌ها به‌طور مناسب طراحی شده و یا از نظر دامنه کار، برای کاهش ریسک هدف یا رسیدن به هدف مورد نظر کافی هستند. (تامی سینگلتون،۲۰۱۴)

استانداردها و چارچوب‌های حسابرسی فناوری اطلاعات

ماهیت تخصصی حسابرسی و اطمینان‌بخشی فناوری اطلاعات و مهارت‌های لازم برای انجام چنین تعهداتی مستلزم استانداردهایی است که به‌طور خاص برای حسابرسی و اطمینان‌بخشی فناوری اطلاعات اعمال شود. تدوین و انتشار استانداردهای حسابرسی و اطمینان‌بخشی فناوری اطلاعات، سنگ بنای کمک حرفه‌ای انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی (ISACA)[1] به جامعه‌ی حسابرسی است.

استانداردهای حسابرسی و اطمینان‌بخشی فناوری اطلاعات الزامات اجباری را برای حسابرسی فناوری اطلاعات مشخص و نحوه‌ی گزارش‌گری و اطلاع‌رسانی را نیز تعیین می‌کنند. نسخه‌ی چهارم چارچوب حسابرسی فناوری اطلاعات (ITAF)[2]، چارچوبی برای سطوح مختلف راهنمایی فراهم کرده و استانداردهای حسابرسی و اطمینان‌بخشی فناوری اطلاعات را به سه دسته تقسیم می‌کند:

استانداردهای عمومی (سری ۱۰۰۰) - اصول راهنمایی است که فرد حرفه‌ای اطمینان بخش (حسابرس) در حوزه‌ی فناوری اطلاعات بر اساس آن‌ها عمل می‌کند. این استانداردها برای انجام همه‌ی کارهای حسابرسی اعمال می‌شوند و با اخلاق، استقلال، بی طرفی و مراقبت حرفه‌ای و همچنین دانش، شایستگی و مهارت حسابرسی و اطمینان‌بخشی فناوری اطلاعات سروکار دارد.

استانداردهای عملکردی (سری ۱۲۰۰) - با انجام تکالیفی همچون برنامه‌ریزی و نظارت، دامنه‌ی کار،

ارزیابی ریسک، تخصیص منابع، نظارت و مدیریت کار، شـواهد حسابرسـی و اطمینان‌بخشی، اعمال قضاوت حرفه‌ای و مراقبت حرفه‌ای سروکار دارد.

اسـتانداردهای گزارش‌گری (سـری ۱۴۰۰) - به انواع گزارش‌ها، ارتباطات و اطلاع رسانی می‌پردازد.(ارفعی سمیرا، یافتیان میترا،۱۴۰۲)

ابزارها و تکنیک‌های حسابرسی و اطمینان‌بخشی فناوری اطلاعات

یکـی از اولیـن گام‌هـا در انجـام حسابرسـی فناوری اطلاعـات، تعیین دامنه، اهـداف و معیارها اسـت. بدین منظور باید استانداردها و چارچوب‌های حسابرسـی فناوری اطلاعات مربوط را که در سـازمان و صنعت مربوطه اعمال می‌شـود، شناسـایی نمود. استانداردها و چارچوب‌هـای حسابرسـی فنـاوری اطلاعـات محبوب شـامل -COBIT ،ITAF 800-، ISO/IEC 27001، BIT2019 و NIST SP 53[۳] و PCIDSS است. این‌ها می‌توانند به تعریف دامنه‌ی حسابرسـی فنـاوری اطلاعات یک سـازمان کمک کننـد و همچنیـن بهترین شـیوه‌ها و معیارها را برای ارزیابی و بهبود عملکرد و بلوغ فناوری اطلاعات ارائه دهند.

پرکاربردتـرین راهـنماهـای حسابرسی فناوری اطلاعات

به‌طور کلی، هشت دسـتورالعمل IT مرتبط با حسابرسـی فناوری اطلاعات وجود دارد که در سطح جهانی پذیرفته شده و در نمایه ۱ آمده است. (مجموعه کنفرانس IOP)

جایـگاه حسابرسـی فناوری اطلاعات

برنامه‌های حسابرسـی کوتاه‌مدت و بلندمدت بایـد با موافقـت افرادی که مسـئولیت راهبری و نظارت را بر عهده دارند (به‌طور مثال کمیته‌ی حسابرسی سـازمان) باشـد و در داخل سـازمان

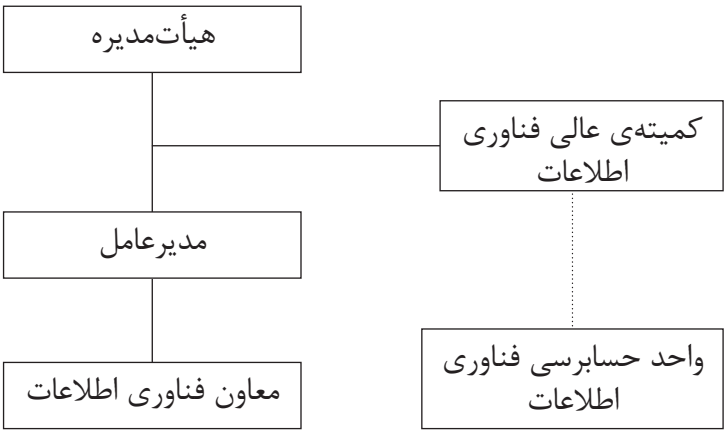
نمایه ۱- پرکاربردترین راهنماهای حسابرسی فناوری اطلاعات

راهنماهای حسابرسی فناوری اطلاعات	عنوان
	Information Technology Audit Framework (ITAF) چارچوب حسابرسی فناوری اطلاعات (ایتف)
	Global Technology Audit Guides (GTAG) رهنمودهای حسابرسی فناوری جهانی (گتاگ)
	Information system Audit and Assurance Guidance (Audit Programs) راهنمای حسابرسی و اطمینان‌بخشی سیستم اطلاعاتی (برنامه‌های حسابرسی)
	IT Assurance Guide using COBIT راهنمای اطمینان‌بخشی فناوری اطلاعات با استفاده از هدف‌های کنترلی فناوری اطلاعات (کوبیت)
	ISO 27007 & ISO/IEC TR27008 استاندارد ۲۷۰۰۷ و ۲۷۰۰۸ای ای سی-تی آر سازمان بین‌المللی استاندارد (ایزو)
	Trust Service Criteria (TSP section100) معیار خدمت اعتماد دهی (تی اس پی بخش ۱۰۰)
	ISO 20000 استاندارد ۲۰۰۰۰ سازمان بین‌المللی استاندارد (ایزو)
	IT Infrastructure Library (ITIL) کتابخانه‌ی زیربنایی فناوری اطلاعات

اطلاع‌رسانی شود. بنابراین جایگاه حسابرسی فناوری اطلاعات مطابق با چارچوب حسابرسی فناوری اطلاعات (ITAF) انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی (ISACA) ذیل کمیته‌ی حسابرسی هر سازمان است.

با این حال در ماده ۶ بخشنامه‌ی «حداقل الزامات ناظر بر ریسک فناوری اطلاعات مؤسسات اعتباری» مورخ ۱۴۰۰/۰۷/۰۶ ابلاغی بانک مرکزی جمهوری اسلامی ایران آمده است «هیأت مدیره موظف است به منظور انجام صحیح و دقیق وظایف خود در حوزه‌ی فناوری اطلاعات کمیته‌ای تحت عنوان کمیته‌ی عالی فناوری اطلاعات را ایجاد نماید» و در ماده ۹ بخشنامه مزبور آمده است مؤسسه‌ی اعتباری می‌تواند در راستای وظایف نظارتی کمیته عالی فناوری اطلاعات، واحدی را تحت عنوان «واحد حسابرسی فناوری اطلاعات» ذیل کمیته‌ی مزبور تشکیل دهد.

نمودار جایگاه کمیته‌ی عالی فناوری اطلاعات/ واحد حسابرسی فناوری اطلاعات/ معاونت فناوری اطلاعات در ساختار سازمانی موسسه اعتباری



منبع - جایگاه حسابرسی فناوری اطلاعات در ساختار سازمانی مؤسسه‌ی اعتباری (بانک مرکزی ج.ا.ا، ۱۴۰۰)

شرح وظایف واحد حسابرسی فناوری اطلاعات

بنابر ماده ۹ فوق، شرح وظایف واحد حسابرسی فناوری اطلاعات به شرح ذیل است:

- تهیه‌ی برنامه‌ی جامع حسابرسی فناوری اطلاعات مؤسسه‌ی اعتباری و هدایت و راهبری فرایندهای مرتبط براساس آخرین نسخه‌ی چارچوب حسابرسی فناوری اطلاعات ایساکا؛
- حسابرسی فناوری اطلاعات حداقل شامل فرایندها، اسناد، قراردادها، معاملات، پروژه‌ها و گزارش‌های تهیه شده مربوط به حوزه فناوری اطلاعات مؤسسه‌ی اعتباری؛
- ارزیابی دوره‌ای میزان انطباق عملکرد فناوری اطلاعات مؤسسه‌ی اعتباری با مفاد الزامات و ارایه‌ی گزارش به معاونت نظارت بانک مرکزی و کمیته‌ی عالی فناوری اطلاعات در مقاطع ۶ ماهه.
- ارزیابی میزان تحقق سیاست‌ها و برنامه‌های مؤسسه‌ی اعتباری و مصوبات

هیأت مدیره در حـــوزه‌ی فناوری اطلاعات و ارایه‌ی گـــزارش به کمیته‌ی عالی فناوری اطلاعات؛

• ارزیابی فرایندهای فناوری اطلاعات از منظـــر توجیـــه اقتصـــادی، کارایی و اثربخشی؛

• ارزیابـــی کارآمدی منابـــع فناوری اطلاعـــات از قبیـــل نیـــروی انســـانی، تجهیزات و سامانه‌ها؛

• نظارت بر حسابرسی فناوری اطلاعات برون سازمانی (برون‌سپاری شده)

• دریافت و بررســـی پیشـــنهادها و توصیه‌هـــای حسابرســـان مســـتقل در ارتبـــاط با حـــوزه فنـــاوری اطلاعات و پیگیری آن‌ها؛

• انجـــام حسابرســـی‌های موردی در صورت لزوم بنا به درخواســـت معاونت نظارت بانک مرکزی و یا کمیته‌ی عالی فناوری اطلاعات مؤسسه‌ی اعتباری؛

• انجـــام فعالیت‌های پژوهشـــی در حوزه‌ی حسابرسی فناوری اطلاعات.

ســـاختار و محتـــوای گزارش حسابرسی فناوری اطلاعات

گزارش حسابرســـی فناوری اطلاعات محصول نهایی کار حسابرســـی اســـت. فرمـــت دقیق این گـــزارش بســـته به ویژگی‌های هر ســـازمان متفاوت اســـت با این حال یک حســـابرس باید اجزای اساســـی گـــزارش حسابرســـی و نحوه انتقال یافته‌های حسابرسی به مدیریت حسابرســـی شـــونده را بداند. (راهنمای گواهینامـــه حســـابرس سیســـتم‌های اطلاعاتی- CISA[۴]، ۲۰۲۰، ویرایش۲۷)

اجزای این گزارش به نوع حسابرسی نیز بستگی دارد. بنابر اعلام انجمن حسابرسی و کنترل ســـامانه‌های اطلاعاتی (ISACA) سه نوع حسابرسی وجود دارد: رسیدگی، بررســـی و روش‌های توافقی. در این مقاله بر مدل رسیدگی تمرکز شده که فرایندی سیســـتماتیک اســـت و از طریق آن یک شخص مستقل و باصلاحیت به صورت بی طرفانه، شواهد مرتبط با ادعاهای مربوط به یک واحد تجاری یا رویدادها، فرایندها، عملیات یا کنترل‌های داخلی را به منظور اظهارنظـــر و ارائه گـــزارش بی‌طرفانه به دســـت آورده و ارزیابی می‌کند. درجه‌ی انطباق ادعاها با مجموعه‌ای از استانداردها مشخص شده و اساساً این نوع حسابرسی، حسابرسی «استاندارد» است.

اجزای گزارش حسابرسی

اجـــزای اجباری گزارش حسابرســـی فناوری اطلاعات مطابق با دستورالعمل ۲۴۰۱ مندرج در ITAF -منتشـــر شده توســـط ISACA - شرح داده شده است. علاوه بر این، ISACA مؤلفه‌های اختیاری بیشـــتری را پیشـــنهاد می‌کنـــد (نمایه

نمایه ۲- اجزای گزارش حسابرسی فناوری اطلاعات

اجزای گزارش حسابرسی فناوری اطلاعات	
مؤلفه‌ی گزارش	منبع
عنوان مناسب و متمایز	ITAF
مشخص کردن گیرندگانی که گزارش به آن‌ها ارسال می‌شود	ITAF
مشخص کردن طرف مسئول	ITAF
فهرست مطالب	گزارش حسابرسی سیستم‌های اطلاعاتی
مقدمه	گزارش حسابرسی سیستم‌های اطلاعاتی
شرح دامنه‌ی کار حسابرسی	ITAF
گزاره‌ای که منبع نمایندگی مدیریت در مورد اثربخشـــی رویه‌های کنترل را مشخص می‌کند	ITAF
گزاره‌ای مبنی بر این‌که کارشناسان، کار حسابرسی را برای اظهارنظر در مورد اثربخشی رویه‌های کنترلی انجام داده اند.	ITAF
مشخص کردن اهداف حسابرسی	ITAF
شرح ضوابط یا افشای منبع ضوابط	ITAF
گزاره‌ای مبنی بر این‌که کار حسابرســـی مطابق با اســـتانداردهای حسابرسی و اطمینان‌بخشی یا سایر استانداردهای حرفه‌ای قابل اجرا انجام شده است.	ITAF
جزئیات بیشتر در مورد متغیرهای مؤثر بر اطمینان ارایه شده	ITAF
یافته‌ها، نتیجه‌گیری‌ها و توصیه‌ها برای اقدامات اصلاحی از جمله پاسخ مدیریت	ITAF
برخورد حسابرس	گزارش حسابرسی سیستم‌های اطلاعاتی
پاراگرافی که بیان می‌کند به دلیـــل محدودیت‌های ذاتی هر کنترل داخلی، تحریف‌های ناشی از اشتباه یا تقلب ممکن است رخ دهد و کشف نشود.	ITAF
خلاصه‌ای از کار(حسابرسی) انجام شده	ITAF
اظهارنظر (حسابرس) در مورد این‌که آیا از تمام جنبه‌های بااهمیت، طراحی و یا اجرای رویه‌های کنترلی در رابطه با حوزه فعالیت مؤثر بوده است یا خیر.	ITAF
خلاصه‌ی اجرایی	گزارش حسابرسی سیستم‌های اطلاعاتی
ارجاع به گزارش‌های جداگانه دیگر که در صورت لزوم باید در نظر گرفته شود.	ITAF
تاریخ صدور گزارش کار حسابرســـی (در بیشتر موارد تاریخ گزارش مطابق با تاریخ صدور است)	ITAF
نام افراد یا نهاد مسئول گزارش	ITAF
ضمایم	گزارش حسابرسی سیستم‌های اطلاعاتی

شماره ۱). این اجزاء لزوماً به ترتیب نیستند (در صورت نیاز به اطلاعات بیشتر به منابع اشاره شده مراجعه شود). با این حال، موارد به صورت مورب در نمایه‌ی ارزش بحث بیشتری دارند. توجه به این نکته مهم است که اگرچه براساس ITAF به این اجزا نیاز است، اما لزوماً به این معنی نیست که گزارش حسابرسی دارای بخش یا عنوان جداگانه برای هر یک باشد. اجزاء ممکن است با بخش‌های مختلف ترکیب شوند. (مجله ایساکا، ۲۰۲۰)

دامنه‌ی کار حسابرسی

دامنه‌ی حسابرسی باید موضوع حسابرسی و محدودیت‌های حسابرسی را مشخص کند. دامنه‌ی حسابرسی می‌تواند شامل یک سازمان، یک بخش در سازمان، یک فرایند تجاری، یک سیستم کاربردی یا فناوری پشتیبانی مانند یک پلت فرم یا شبکه خاص باشد. گزاره‌ی دامنه همچنین باید دوره مورد بررسی و زمان انجام حسابرسی را مشخص کند. برای یک خواننده آگاه، دامنه‌ی حسابرسی باید وسعت مورد انتظار کار حسابرسی و حوزه‌های موضوعی تحت پوشش را نشان دهد.

منبع نمایندگی مدیریت

مدیریت ممکن است در مورد اثربخشی رویه‌های کنترلی اظهارنظر کند. این‌ها معمولاً به صورت ادعاها یا هرگونه اظهارات رسمی یا مجموعه‌ای از اظهارات در مورد موضوعی است که توسط مدیریت ارائه می‌شود. ادعاهای رایج شامل محرمانه بودن، صداقت، در دسترس بودن و انطباق است. به‌طور مثال مدیریت ممکن است ادعا کند که برنامه تحت بررسی مطابق با استاندارد امنیت داده صنعت کارت پرداخت است. این موارد باید در گزارش حسابرسی درج شود.

اهداف حسابرسی

مقصود از انجام حسابرسی در اهداف حسابرسی مشخص می‌شود. چرا حسابرسی انجام می‌شود؟ اهداف، مواردی را که باید توسط حسابرس ارزیابی یا بررسی شوند، مشخص می‌کند. لذا هر گزارش حسابرس باید پشتوانه‌ی مناسبی نسبت به اهداف حسابرسی ارایه کند. به‌طور مثال اگر هدف حسابرسی تعیین این باشد که «آیا کنترل‌های کافی برای ایجاد اطمینان معقول از این‌که فقط دسترسی فیزیکی مجاز به مرکز داده قابل دستیابی است؛ وجود دارد یا خیر» در این صورت گزارش باید نتیجه‌گیری یا نظر حسابرس را در مورد کفایت کنترل‌ها برای رسیدن به آن هدف بیان کند. همچنین اگر برای دستیابی به هدف لازم است کنترل‌ها اجرا یا تقویت شوند در این صورت گزارش باید توصیه‌ای برای رفع این نیاز ارایه کند. (CISA، ۲۰۲۰، ویرایش۲۷)

منبع ضوابط

ضوابط؛ استانداردها و معیارهایی هستند که برای اندازه‌گیری و ارائه‌ی موضوع مورد استفاده قرار می‌گیرند و حسابرس سیستم‌های اطلاعاتی براساس آن‌ها موضوع را ارزیابی می‌کند. ضوابط اغلب توسط واحد مورد بررسی تعریف می‌شود به عنوان مثال قراردادها، قراردادهای سطح خدمات (SLA)[۵]، سیاست‌ها، استانداردها.

با این حال، مواردی وجود دارد

نمایه ۳- ویژگی‌های یافته حسابرسی

پنج ویژگی یافته حسابرسی		
نام ویژگی	شرح	موارد قابل شناسایی
وضعیت موجود	یافته‌ها	یافته‌های حسابرسی بیانی از مشکل یا نارسایی است. این ممکن است در مواردی مانند ضعف کنترل، مشکلات عملیاتی یا عدم رعایت الزامات مدیریتی یا قانونی باشد.
ضوابط	الزامات و خطوط پایه	گزاره‌ی الزامات و مشخص کردن خطوط پایه که برای مقایسه با یافته‌های حسابرسی براساس شواهد حسابرسی مورد استفاده قرار می‌گیرد.
علت	دلیل وضعیت موجود	توضیح علت ممکن است نیاز به مشخص کردن شخص مسئول داشته باشد. مگر در مواردی که سیاست حسابرسی اقتضا کند. گزارش باید واحد کسب و کاری سازمانی یا عنوان شخص را مشخص کند و نه نام فرد را. همین امر باید در مورد مشخص کردن شخصی که مسئول پاسخگویی است نیز اعمال شود.
اثر	تأثیردر وضعیت موجود	تأثیر نامطلوب بر هدف عملیاتی یا کنترلی، با بیان تأثیر و ریسک آن توضیح داده می‌شود. جزءاثر در کمک به ترغیب مدیریت واحد حسابرسی شده، برای انجام اقدامات اصلاحی بسیار مهم است.
توصیه	اقدام اصلاحی پیشنهادی	در حالی که اقدام اصلاحی باید مشکل یا نارسایی ذکر شده در وضعیت موجود را برطرف کند، اقدام اصلاحی باید در جهت رسیدگی به علت باشد.

کـــه ضوابط دیگـــری باید اعمال شـــود ایـــن زمانی اســـت کـــه یک ســـازمان اســـتانداردهای خود را تعریـــف نکرده اســـت. ضوابط منتشـــره توسط ISACA و ســـایر ارگان‌های تخصصـــی (از جمله ISO,IIA،...)، الزامـــات قانونـــی و قوانین و مقررات تعیین می‌شـــود و یا می‌تواند به‌طور خاص برای کار حسابرسی تدوین شده باشـــد. (به‌طور نمونه بانک مرکزی جمهوری اســـلامی ایران به استناد مفاد بند (ب) ماده (۱۱)، بند (۲) ماده (۱۴) و ماده ۳۷ قانون پولی و بانکی کشـــور و مفاد بند (الـــف) ماده (۴۹) قانون برنامه پنجم توســـعه کشور و به منظور حصول اطمینـــان از صحت عملکرد مؤسســـات اعتبـــاری در حـــوزه فنـــاوری اطلاعات بخشنامه «حداقل الزامات ناظر بر ریسک فناوری اطلاعات مؤسســـات اعتباری» را تدویـــن و در تاریـــخ ۱۴۰۰ /۰۷/۰۶ به تمامی بانک‌ها و مؤسســـات اعتباری ابلاغ کرد. بنابر ماده ۶ بخشنامه مذکور هیأت‌مدیره‌ی مؤسسه‌ی اعتباری موظف اســـت به منظور انجـــام صحیح و دقیق وظایف خـــود در حوزه فناوری اطلاعات کمیته‌ای تحت عنـــوان «کمیته‌ی عالی فناوری اطلاعات» ایجاد نماید. مطابق با ماده ۷ این بخشـــنامه نظارت بر فرایند حسابرسی فناوری اطلاعات در مؤسسه‌ی اعتبـــاری و نیـــز نظارت بـــر فرایندها و منابع فنـــاوری اطلاعات از منظر توجیه اقتصادی، کارآیی و اثربخشـــی از جمله وظایف و مســـئولیت‌های کمیته‌ی عالی فناوری اطلاعات در مؤسســـات اعتباری است.

همچنین براســـاس ماده ۹ بخشنامه مزبور مؤسســـه‌ی اعتبـــاری می‌تواند در راســـتای وظایف نظارتی کمیته‌ی عالی فناوری اطلاعات، واحدی را تحت عنوان «واحد حسابرســـی فنـــاوری اطلاعات» ذیل کمیتـــه‌ی مزبـــور (کمیته‌ی عالی فنـــاوری اطلاعات) با شـــرح وظایفی از جمله تهیه‌ی برنامه‌ی جامع حسابرسی فنـــاوری اطلاعات مؤسســـه‌ی اعتباری و هدایت و راهبـــری فرایندهای مرتبط براســـاس آخریـــن نســـخه چارچـــوب حسابرســـی فنـــاوری اطلاعات ایســـاکا تشکیل دهد.

یافته‌ها، نتیجه‌گیری‌ها و توصیه‌ها

گـــزارش حسابرســـی بایـــد شـــامل مشـــاهدات، یافته‌هـــا، نتیجه‌گیری‌ها و توصیه‌ها و در صورت امـــکان به همراه تعییـــن هزینه‌هـــای اصلاح باشـــد. لذا یافته‌های حسابرســـی زمانی در گزارش حسابرسی ارائه می‌شوند که برای اصلاح نارســـایی در یک فراینـــد یا کنترل‌های مربوط به آن، اقدامی لازم باشد.

پنج جزء کلیدی یـــا ویژگی‌هایی که بایـــد هنگام ارائه یافته‌های حسابرســـی مورد توجه قرار گیرند، در نمایه شـــماره ۳ توضیح داده شده است.

مثال ۱:

یافته‌ی حسابرسی: سطح کمیته استاندارد مرکز داده		
نام ویژگی	شرح	موارد قابل شناسایی
وضعیت موجود	سطح پایین استاندارد مرکز داده	براساس استاندارد DC100 و متناسب با سطح خدمات مبتنی بر فناوری اطلاعات در سازمان ... زیرساخت‌های عملیاتی و مرکز داده سازمان ... در سطح پایین قرار دارد.
ضوابط	الزامات و خطوط پایه	استاندارد DC100 ارایه شده توسط سازمان استاندارد ایران
علت	دلیل وضعیت موجود	قدیمی بودن زیرساخت‌ها و مرکز داده سازمان ...، شرایط ساختمان مرکز داده و ...
اثر	تأثیردر وضعیت موجود	تأثیر نامطلوب بر اهداف عملیاتی سازمان که همانا ارایه خدمات مبتنی بر فناوری اطلاعات با کمترین اختلال و قطعی سرویس دارد.
توصیه	اقدام اصلاحی پیشنهادی	تهیه‌ی طرح به روزآوری مرکز داده براساس استاندارد DC100

مثال ۲:

یافته‌ی حسابرسی: بازبودن دسترسی به USB و CD-ROM کارکنان ستاد		
نام ویژگی	شرح	موارد قابل شناسایی
وضعیت موجود	دسترسی کارکنان ستاد به USB و CD-ROM	مطابق بررسی‌های انجام شده دسترسی به USB و CD-ROM در شعب تنها برای افراد دارای مجوز باز بوده اما در مورد کارکنان ستاد، این دسترسی عمومی است و نظارت دوره‌ای بر آن نیز وجود ندارد.
ضوابط	الزامات و خطوط پایه	الزامات افتا و پدافند غیرعامل
علت	دلیل وضعیت موجود	عدم وجود کنترل‌های لازم در خصوص امنیت اطلاعات عدم جلوگیری از رخداد موارد ضد امنیتی و کاهش تأثیرات بالقوه ریسک‌های موجود عدم طبقه بندی اطلاعات براساس اهمیت و محرمانگی (Data Classification)
اثر	تأثیردر وضعیت موجود	انتقال نامناسب و غیرمجاز اطلاعات سیستم‌ها سوء استفاده از اطلاعات بانکی و در نتیجه از دست رفتن اعتبار سازمان آسیب رسیدن با هک شدن سیستم اطلاعاتی سازمان
توصیه	اقدام اصلاحی پیشنهادی	به روز رسانی سیاست‌های امنیت اطلاعات در سازمان و نظارت دقیق بر اجرای آن‌ها

تخصیص یک رتبه برای نشـان دادن اهمیت هر یافته، به همراه یک شـماره مرجـع منحصر به فرد برای تشـخیص آسان هر مورد، تمرین خوبی است. این می‌تواند توسـط مدیریت برای اولویت بندی پاسخ خود و توسط حسابرس برای ردیابی یافته‌ها تا تکمیل استفاده شود.

یافته‌ها همچنین می‌توانند به ترتیب اهمیـت ارائه شـوند. هنـگام دریافت پاسـخ‌های مدیریـت، همیشـه مدیر مسئول و تاریخ اجرای توافق شده ثبت شود. این‌ها به فرایند پیگیری حسابرسی کمک خواهد کرد.

اظهارنظر

هـدف ایـن بخـش ارائـه‌ی یـک نتیجه‌گیـری یا نظـر کلـی در رابطه بـا اهداف کار حسابرسـی اسـت. نظر حسـابرس یک گزاره‌ی رسمی است که توسـط حسـابرس فناوری اطلاعات و اطمینان‌بخشی بیان می‌شود و دامنه‌ی حسابرسی، رویه‌های مورد استفاده برای تهیه‌ی گزارش و این‌کـه آیا یافته‌ها از برآورده شـدن معیارهای حسابرسـی حمایـت می‌کنند یا خیـر، را توصیف می‌کند. انواع اظهارنظرها عبارتند از:

• **اظهارنظـر مقبول** - اسـتثنایی برای نارسـایی قابل ملاحظـه نبوده و یـا اسـتثنائات ذکر شـده در مجموع محدودیت قابل ملاحظه ندارد. اساسـاً با توجه به اهداف حسابرسـی، یک سند بدون نقص و سلامت بودن است.

• **اظهارنظر مشروط** - موارد استثنا یک نارسـایی قابل ملاحظه (اما نه یک ضعـف بااهمیت) را نشـان می‌دهد. در این مثال، گزارش باید شـامل یک بند (پاراگراف) توضیحی باشد که دلایل ابراز نظر مشروط در گزارش را بیان کند.

• **اظهارنظر مردود** - به یک یا چند نارسایی بااهمیت اشاره می‌کند که به یک ضعف بااهمیت منجر می‌شـود. از منظر کنترل داخلی، زمانـی اظهارنظر مردود می‌شود که کنترل‌های کافی برای ایجاد اطمینان معقول از دسـتیابی به اهداف کنترلی مؤثر نباشد یا وجود نداشته باشد و یا احتمال معقولی وجود دارد که اهداف کنترلی برآورده نشـده است. وجود یک بند توضیحی که دلایل رسـیدن به این نظر را بیان می‌کند، نیز ضروری است.

عدم اظهارنظر زمانی صادر می‌شـود که حسـابرس نتواند شواهد حسابرسی کافی و مناسـبی را به دسـت آورد که بر اسـاس آن اظهارنظر کند یا به دلیل تعاملات بالقوه ابهامـات متعدد و تأثیر تجمعـی احتمالـی آن‌هـا، اظهارنظر غیرممکن باشد.

رویدادهای آتی

رویدادهایی که تأثیـر قابل‌توجهی بر موضوع یا فعالیت حسابرسی دارند، گاهی اوقات پس از بررسـی کنترل‌ها، اما قبل از تاریـخ صدور گزارش حسابرسـی رخ می‌دهند. ایـن رویدادهایی که به عنوان رویدادهای آتی نامیده می‌شـوند، ممکن اسـت نیاز به افشـا داشته باشـند زیرا ممکن اسـت یک ادعا یا یـک نتیجه را تغییر دهند. (ITAF، ۲۰۲۰). به‌طور مثال حسابرسی سیستم اصلی بانکداری (Core Banking) انجـام و تعدادی از ضعف‌ها

و یافته‌هـــا در طول فرایند حسابرســـی شناسایی شـــده است اما همزمان با دوره رسیدگی، پروژه مهاجرت از سیستم فعلی به سیستم جدید بانکداری در حال انجام است و ممکن اســـت در آینده یافته‌های فعلی را تحت تأثیر قرار داده و بعضاً منجر به حذف یافته و یا شناسایی نقاط ضعف بیشتری شود.

ارتباطات بیشتر

حسابرســـان باید قبل از نهایی شدن و انتشار گزارش، محتویات پیش نویس گزارش را با مدیریت حسابرســـی شونده در حوزه موضوعی مذاکره کنند و پاسخ مدیریت حسابرسی شـــونده به یافته‌ها، نتیجه‌گیری‌هـــا و توصیه‌ها را در گزارش نهایی بگنجانند.

همچنین باید نارسایی‌ها و ضعف‌های قابل توجه در محیط کنترلی را مسئولین راهبری و در صورت لزوم مقام مســـئول اطـــلاع دهند و در گـــزارش به صراحت اعلام کننـــد که نارســـایی‌ها و ضعف‌ها ابلاغ شده است.

سایر ملاحظات

حسابرس فناوری اطلاعات باید نکات دارای بار مالی یا ضعف‌های معنی دار و مهم و تأثیر آن‌ها بر دستیابی به اهداف حسابرسی را در گزارش شرح دهند.

هرگونه گزارش جداگانه را در گزارش نهایی ارجاع داده و استانداردهای اعمال شـــده در انجام حسابرسی را شناسایی و موارد عدم انطباق با اســـتانداردها را در صورت لزوم اعلام کنند.

خلاصه‌ی اجرایی

خلاصه‌ی اجرایی یک ســـند مختصر است که مســـائل، یافته‌ها و توصیه‌های یک گزارش طولانی‌تر را نشان می‌دهد. معمـــولاً شـــامل توصیف ســـطح بالایی از پیـــام اولیه گزارش، اهـــداف کلیدی حسابرســـی و خلاصه مختصری از نتایج حسابرســـی اســـت. این مورد در ITAF اجباری نشـــده است، اما به‌شدت توصیه می‌شود زیرا اغلب تنها بخشی از گزارش اســـت که توســـط مدیران ارشد خوانده خواهد شد.

تاریـــخ صـــدور گـــزارش کار حسابرسی (در بیشتر موارد تاریخ گزارش منطبق با تاریخ صدور است)

توصیـــه می‌شـــود در صـــورت عدم ذکـــر تاریخ در خلاصه کار انجام شـــده تاریخ‌های انجام حسابرســـی در گزارش ذکر شود.

نام افراد یا نهاد مسئول گزارش

گـــزارش حسابرســـی بایـــد شـــامل گیرندگان موردنظر و هر گونه محدودیت در گردش باشد همچنین شامل امضا و موقعیت افراد یا نهادهای مسئول گزارش باشد.

نتیجه‌گیری

متخصصـــان حسابرســـی فنـــاوری اطلاعات ســـاعت‌های زیـــادی را صرف جســـت‌وجو و بحث در مورد برنامه‌های حسابرســـی فناوری اطلاعـــات می‌کنند زیـــرا این امـــر می‌تواند بـــر کیفیت کار انجام‌شـــده و در نهایـــت اطمینان ارائه شـــده به سازمان مؤثر باشد. با این حال، محتویات گزارش حسابرســـی به ندرت مـــورد بحث قـــرار می‌گیـــرد، حتی اگر از آن‌هـــا برای پیشـــبرد فرایند پیگیری حسابرسی استفاده شـــود و اغلب منجر به ایجاد هزینه در سازمان خواهد شد.

ISACA استانداردها، دستورالعمل‌ها، مقـــالات وایت پیپر و یک الگوی گزارش را تولید کرده اســـت که بایـــد به آن‌ها ارجاع داده شود تا اطمینان حاصل شود که گزارش‌های حسابرســـی هر سازمانی با اســـتانداردهای حرفه‌ای ســـطح بالا مطابقت دارد. همچنین زمانی که نتایج گزارش حسابرســـی به چالش کشـــیده می‌شـــود، پایبندی به این اســـتانداردها بـــرای حســـابرس فنـــاوری اطلاعـــات ارزشمند خواهد بود.

لذا یک حســـابرس باید یک گزارش متوازن را ارایه کند که شامل موضوعات منفی از نظر یافته‌ها و نیز نظرات سازنده مثبت در مـــورد فرایندها و کنترل‌های بهبودیافته یـــا کنترل‌های مؤثری که از قبل وجود داشته است، را توصیف کند.

منابع:

-ســـینگلتون تامـــی، ۲۰۱۴، اصول حسابرسی سیستم‌های اطلاعاتی، مجله ایساکا.

- ارفعی ســـمیرا و یافتیان میترا، اول ۱۴۰۲، چارچـــوب حسابرســـی فناوری اطلاعات.

- بانـــک مرکزی جمهوری اســـلامی ایران، بخشـــنامه «حداقل الزامات ناظر بر ریســـک فناوری اطلاعات مؤسســـات اعتباری»، مهر ۱۴۰۰.

- https://iopscience.iop.org/article/10.1088/1757-899X/662/2/022055/pdf

- https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2020/volume-1/the-components-of-the-it-audit-report_joa_eng_0120

پی‌نویس:

1. Information Systems Audit and Control Association (ISACA)
2. IT Audit Framework (ITAF™)
3. Payment Card Industry Data Security Standard
4. Certified Information System Auditor (An ISACA Certification)
5. Service Level Agreement