محور اصلی حسابرسی فناوری اطلاعات

ترجمه: **نیوشا ابراهیمی**
T. Singleton

با پدیدارشدن موج اخیر فناوریهای اطلاعات مانند فناوریهای حوزه **داده‌های با حجم بالا**[۱] که هدف آنها تحلیل و پردازش بلادرنگ داده‌ها است، فناوریهای **رسانه‌های اجتماعی**[۲] که در پی تسریع در ارتباطات هستند و شاید از همه مهمتر، رویکرد عرضه فناوری اطلاعات در قالب بسته‌های خدماتی که **رایانش ابری**[۳] عمومی‌ترین نوع آن است، ارزشمند است زمانی را برای بازنگری مبانی حسابرسی فناوری اطلاعات در رویارویی با شرایط جدید اختصاص دهیم. به‌طور معمول، پدید آمدن چنین فناوریهایی با مباحثی همچون مباحث مطرح‌شده درباره فناوریهای پیشین همراه است و راههای پرداختن به چنین فناوریهای نوپدیدی، همان است که حسابرسان فناوری اطلاعات همیشه در برخورد با چالشهای فناوریهای نوپدید، انجام می‌دهند. اما محور اصلی و موضوع حسابرسی فناوری چیست؟ حسابرسی فناوری اطلاعات، درباره شناسایی ریسک و کنترلهای مناسب برای کاهش ریسک به سطحی قابل‌پذیرش است.

سه موردی که حسابرسی فناوری اطلاعات نیست

نخست این که برای افرادی که به‌تازگی وارد حرفه شده‌اند و برای افراد بیرون از این حرفه، باید یادآوری شود که حسابرسی فناوری اطلاعات چه مواردی را دربرنمی‌گیرد. حسابرسی فناوری اطلاعات ربطی به «کنترل‌های حسابداری متداول» یا «حسابرسی مالی مرسوم» ندارد. این دانش و مهارت در حرفه حسابرسی به‌خوبی از آغاز حسابرسی در قرون وسطی (به‌همراه خزانه‌داران و دیگر اشکال حسابرسی) تا شروع به‌کار سامانه‌های محاسباتی در دهه ۱۹۵۰، به‌خدمت گرفته شده است. در واقع، پیش از سال ۱۹۵۴ برای حسابرس امکان‌پذیر بود که در طول عمر کاری خود همواره یک برنامه حسابرسی بسیار مشابه را در کلیه پروژه‌های کاری به‌کار گیرد. به بیان ساده، به‌کارگیری رایانه‌ها در سامانه‌های حسابداری، فرایندها و اطلاعات حسابداری را با منبع جدیدی از ریسک

(ریسک داده‌ها) مواجه کرد. در نهایت، این موضوع برای آنانی که این «مورد» جدید را شناخته بودند، نیاز به شناسایی و کاهش ریسک را پدید آورد.

حسابرسی فناوری اطلاعات، «**آزمون رعایت**[۴]» هم نیست. برخی باور دارند که کار حسابرسان فناوری اطلاعات، اطمینان‌بخشی ضمنی یا صریح درباره رعایت برخی مجموعه قواعد و مقررات و گزارش موارد عدم‌رعایت آنها است. در واقع، این کار بر عهده مدیریت است. رعایت قواعد و مقررات، موضوع مورد علاقه حسابرسان فناوری اطلاعات نیست. حسابرسان فناوری اطلاعات به این آزمون می‌پردازند که آیا سامانه‌ها یا فرایندهای تجاری مرتبط با واحد تجاری در رعایت قواعد و مقررات پیشگفته و نظارت بر آنها به‌گونه‌ای اثربخش عمل می‌کنند یا خیر. آنها در این میان به ارزیابی طراحی قواعد و مقررات از جنبه‌های کفایت دامنه و تناسب با **ریسک هدف**[۵] و توانایی در کاهش سطح ریسک دستیابی به هدف مورد نظر به سطحی قابل قبول نیز می‌پردازند.

برای حسابرسان فناوری اطلاعات، شناسایی دلایل عدم‌رعایت قواعد و مقررات نسبت به رعایت آنها، از اهمیت بیشتری برخوردار است. عدم‌رعایت قواعد و مقررات، ممکن است نشانه‌ای از مشکل بزرگ‌تر مرتبط با عوامل ریسک و /یا کنترل باشد و اغلب نیز همین‌گونه است؛ مانند سامانه یا فرایند تجاری دارای نارسایی که بر واحد تجاری اثر منفی می‌گذارد، یا ممکن است بگذارد. بنابراین، برای حسابرس فناوری اطلاعات، بحث عدم‌رعایت قواعد و مقررات در نهایت از منظر ریسک اهمیت دارد، نه از جنبه الزامی بودن آن قواعد و مقررات.

برخی بر این باورند که بررسی فناوری اطلاعات، اتلاف وقت است و به‌علت عدم‌تأکید صریح به اجرای آن در برخی الزامهای مقررشده، حتی می‌توان آن را خارج از دامنه کار حسابرسی به‌شمار آورد. واقعیت این است که عدم‌آگاهی مدیریت واحد تجاری از فناوری اطلاعات، می‌تواند آثار مخربی بر فرایندهای تجاری یا داده‌های مالی بگذارد و این موضوعی نیست که در استانداردهای حسابرسی به آن بی‌توجهی شده باشد.

ریسک ذاتی یگانه[۶]

فناوری اطلاعات، عوامل ریسک خاصی را برای حسابداری، حسابرسی و سامانه‌ها به‌همراه دارد؛ به این معنی که خود فناوری اطلاعات در ارتباط با سامانه‌ها، فرایندهای کسب‌وکار تجاری و پردازش مالی/ حسابداری، برای واحد تجاری ریسک به‌همراه می‌آورد. این ریسک، مختص فناوری اطلاعات است؛ به این معنی که بدون وجود فناوری اطلاعات دستکم در این سطح، این ریسک نیز به‌وجود نمی‌آید. برای این کار، نیاز است تا فردی حرفه‌ای همچون حسابرس فناوری اطلاعات، ریسک ذاتی مرتبط با فناوری اطلاعات را شناسایی و ارزیابی کند.

عوامل ریسک پیشگفته دربرگیرنده موضوع‌های مرتبط با سامانه‌ها مانند **ایجاد سامانه‌ها**[۷]، **مدیریت تغییرات**[۸]، **آسیب‌پذیری‌ها**[۹] و دیگر عوامل خاص فناوری است. بدون به‌کار گماردن متخصصان حرفه‌ای فناوری اطلاعات، چنین ریسکی ممکن است از نظر دور بماند و موجب ایجاد ضرر برای واحد تجاری شود. برای نمونه، دانشگاهی تجربه زیر را در ارتباط با سامانه‌های اعطای کمک مالی، از سر گذرانده است.

بخش فناوری اطلاعات این دانشگاه، برنامه‌ای اختصاصی برای اعطای کمک مالی نوشت. این دانشگاه به‌عنوان یک مؤسسه خصوصی، مبالغ هنگفتی کمک مالی در اختیار داشت که به اکثریت دانشجویان متقاضی دریافت برخی انواع کمکهای مالی، عرضه می‌شد. حسابرس باتجربه فناوری اطلاعات با آگاهی از این حقایق، برخی ریسکهای ذاتی مرتبط با این موضوع از جمله درستی برنامه نرم‌افزاری، امکان وجود **اشکال**[۱۰] و تقلب در برنامه که نیازمند بررسی و مستلزم آزمون و کاهش ریسک به سطح قابل پذیرش بود را شناسایی کرد. اما مدیریت دانشگاه با این فرض که واحد فناوری اطلاعات راستی‌آزمایی لازم نسبت به نرم‌افزار اعطای کمک مالی را انجام داده است، هیچ‌گونه ریسکی را شناسایی نکرد. چند سال بعد، دانشگاه به‌طور تصادفی اشکالی را در برنامه یادشده کشف کرد که بیانگر اشتباه محاسباتی نرم‌افزار طی سالهای استفاده از آن بود. در طول آن سالها، میلیون‌ها دلار کمک مالی به اشتباه اعطا شد و این کار مؤسسه را با مشکلات مالی درگیر کرده و سبب چشم‌پوشی از طرحهای دانشگاه شده بود. نمونه پیشگفته برای این ارائه شد که نیاز به شناسایی و ارزیابی ریسک ذاتی مرتبط با فناوری اطلاعات در واحد تجاری را نمایان سازد.

با این فرض که تقریباً تمام واحدهای تجاری، فناوری اطلاعات

مهم است که حسابرسان فناوری اطلاعات در زمینه‌های شناخت تحلیل و ارائه نتایج مرتبط با ریسک و کنترلها مهارت داشته باشند

را در سطوح مختلفی به‌کار می‌گیرند، زمان آن فرا رسیده است که آنها برای ارزیابی ریسک ذاتی فناوری اطلاعات خود، از خدمات حسابرسان فناوری اطلاعات بهره‌مند شوند. حسابرسان فناوری اطلاعات به‌طور ویژه برای انجام این وظیفه آموزش دیده و از مهارت برخوردار هستند. حسابرسان فناوری اطلاعات توانایی شناسایی ماهیت و ریسک فناوریهای اطلاعات و سامانه‌ها را دارند.

اگر به مباحث فناوریهای نوپدید بازگردیم، نقطه آغاز کار روی آنها ارزیابی مناسب ماهیت، ویژگی و سطح ریسک ارزیابی‌شده است. هنگامی که به این نتیجه دست یافتیم که این کار با کوشش مقتضی انجام پذیرفته است، حسابرس فناوری اطلاعات و دیگران می‌توانند کنترلهای مناسب را برای کاهش ریسک به‌گونه‌ای رضایت‌بخش برقرار کنند.

نقش کنترلها

یکی از دلایل اصلی کنترل، کاهش برخی ریسکهای شناسایی‌شده است. راه کنار آمدن با ریسک ذاتی که در سطحی بالاتر از سطح قابل پذیرش است، استقرار کنترل مؤثر برای کاهش آن ریسک به سطح قابل پذیرش است.

بر پایه آنچه گفته شد، نکاتی برای یادآوری کنترلها و نقشی که در حسابرسی فناوری اطلاعات یا حسابرسی در کل بازی می‌کنند، وجود دارد. نخست، لازم است حسابرسان فناوری اطلاعات نسبت به امنیت کاذب مربوط به کفایت اثربخشی یک کنترل در کاهش ریسک به سطح قابل پذیرش آن، هشیار باشند؛ در واقع، حسابرسانِ کارآزموده فناوری اطلاعات در کل در این مورد خوب کار می‌کنند، اما مدیریت و دیگران ممکن است نسبت به شناخت واقعیت یک کنترل، مهارت نداشته باشند.

از سوی دیگر، حسابرسان فناوری اطلاعات باید هزینه و منفعت کنترلها را مدنظر داشته باشند. هزینه‌ها تقریباً همیشه به مبالغ پولی واقعی هستند و در برگیرنده هزینه‌های شناخت، طراحی، استقرار و مدیریت کنترل می‌باشند. همچنین ممکن است یک هزینه اثرگذار، موجب دردسر برای یک فرایند یا اثرگذار بر کاهش کارایی عملیاتی آن باشد. برخی از موارد پیشگفته، مشاهده‌های ملموسی را دربرنمی‌گیرند و بیشتر استنباط و انتظار اثرگذاری یک کنترل را به نمایش می‌گذارند. کار اصلی حسابرسان فناوری اطلاعات، جستجوی تعادل میان این هزینه‌ها (**واقعی**[11]، **عینی**[12] و **اثرگذار**[13]) و منافع است. منافع نیز می‌توانند واقعی و عینی باشند؛ به این معنی که تفاوت نسبی در داشتن یک کنترل که به‌گونه‌ای اثربخش کار می‌کند و کارکردن بدون آن، تشخیص داده شود. تشریح این تعادل از تشخیص اثربخش آن، آسان‌تر است.

برای نمونه، سازمانی خواهان استقرار سیاست گذرواژه عبور اثربخش در دوره عمر گذرواژه‌های عبور است. منطقی است که دوره عمر گذرواژه‌های عبور با میزان ریسک مرتبط با دسترسی غیرمجاز، همبستگی معکوس داشته باشد؛ به این معنی که اگر در خصوص دسترسی غیرمجاز ریسک بالایی وجود داشته باشد، دوره عمر گذرواژه‌های عبور باید کوتاه‌مدت باشد (برای نمونه، ۹۰ روز برای حساب بانکی **بَرخط**[14]). هرچند، هنگامی که برای نخستین بار این سیاست مستقر شود، می‌تواند هزینه‌های ناخواسته

مرتبط با گذرواژه‌هـای عبور ازیادرفته به‌دلیـل تناوب تغییرات در آنهـا را به‌وجـود آورد. نتیجه می‌تواند این باشـد که کاربران به‌طور متنـاوب گذرواژه‌های عبـور را فراموش کننـد و مجبور باشند از منابع واحد تجاری برای دسترسی یافتن کمک بگیرند؛ هزینـه‌ای که افزون‌بـر دیگر پیامدها، شـامل هزینه تأخیرها و هزینه‌های ناخواسته می‌شـود. بنابراین، نکته اصلی این است که در زمینه ارزیابی عایدی خالص واقعی یک کنترل، کوشـش مقتضی انجام پذیرد.

ملاحظـه دیگـر در این بـاره این اسـت که واحـد تجاری، کسـب‌وکار یا هدفی دارد که برای آن کار می‌کند. نیاز اسـت این هدف، بخشی از ملاحظات باشـد. بی‌توجهی به آثار ناخواسته مؤثر بر عملیات، کار آسانی است.

به بیان کلی، هرچه ریسـک ذاتی بالاتر باشد، گرایش به یک کنترل کاهنده ریسـک افزایش می‌یابد. بنابراین، نیاز اسـت که حسابرسان فناوری اطلاعات هنگام ارائه پیشنهاد برای کنترلها، سطح ریسک ذاتی و **ریسک باقیمانده**[۱۵] را در نظر بگیرند.

در پایان ایـن که، کنترلها اغلـب در فناوری‌ها یا سـامانه‌ها جاسـازی شـده‌اند. این واقعیت به‌تنهایی بیانگر این اسـت که لازم اسـت حسابرسـان فناوری اطلاعات تا جایی که استقلال آنها حفظ می‌شـود، در کمک دادن بـرای طراحی کنترل درگیر شـوند. همچنین، این موضوع بیانگر اهمیت بالای به‌کارگیری حسابرسان فناوری اطلاعات در ارزیابی اثربخشی سامانه کنترل داخلی اسـت. چگونه می‌توان کنترل جاسازی‌شـده در فناوری اطلاعـات را ارزیابـی کرد، بدون این کـه از متخصص موضوع فنـاوری اطلاعات در درک چگونگی اثربخشـی کارکرد کنترل، کمک گرفته شود؟

شناخت ریسک باقیمانده واقعی

یکی از موضوع‌های مرتبط با تحلیل ریسک این است که تحلیل به‌طور معمول نسبی و وابسـته به قضاوت حرفه‌ای است. همه ذینفعان گرایش دارند که کنترلها «به اندازه کافی خوب» باشند تا این که همه چیز «درست» بماند. اما، چه چیزی «به اندازه کافی خوب» و چه چیزی «درست» اسـت؟ ریسک، چیزی نیست که بشود آن را به‌طور مطلق اندازه‌گیری کرد.

مدیـران کارناآزموده به قضاوت نادرسـت یا کاربرد نادرسـت کنترلهـا و ریسـک گرایش دارنـد. آنها با تمرکز بـر بقای واحد تجاری و ایجاد سـود برای آن، گاهی واقعیت ریسک باقیمانده را نمی‌بینند و با شـتاب رو به جلو می‌روند تـا این که با پیامدی ناگوار روبه‌رو شـوند، یا به نوعی **کج‌اندیشـی**[۱۶] دچار می‌شوند و از پذیرش درست ریسـک خودداری می‌کنند و در برابر زیان، اقدامی انجـام نمی‌دهند. هرچند، مدیـران کارآزموده واقعیت ریسـک باقیمانده را درمی‌یابند و به‌طـور معمول، تصمیمهای درست می‌گیرند و اگر با ریسـک روبه‌رو شوند، اغلب یک طرح اقتضایی دارند. یکی از چالشهای حسابرسان فناوری اطلاعات این اسـت که به مدیران کمک کنند تا از راه شـناخت ریسـک باقیمانده واقعی و انجام اقـدام لازم در برابر آن، مدیرانی خوب و بزرگ باشند.

چالشِ پیرامون شـناخت واقعیت ریسـک باقیمانده، ارزیابی درسـت ریسـک و کنترلها با درنظر گرفتن همه جوانب اسـت. نخست این که برخی کنترلها به فناوری اطلاعات ارتباطی ندارند و برخی افراد به‌رغم پتانسـیل کاهش ریسـک مرتبط با فناوری اطلاعات در برخی کنترلهای دستی، گرایش به نادیده انگاشتن کنترلهای دسـتی دارند. برای نمونه، بررسـی و تطبیق از سوی یک فرد کنترل‌کننده، ممکن اسـت به‌گونه‌ای مناسـب ریسک دسترسی غیرمجاز به داده‌ها و **پایگاه‌های داده**[۱۷] را کاهش داده یا پایین بیـاورد؛ به این معنی که اگر فردی توانسـت کنترلهای دسترسـی را پشت‌سر گذاشته و از آنها گذر کند یا در صورت نبود آن کنترلها، توانست داده‌های پایگاه داده مالی/ حسابداری را به خطر بیندازد، هرگونه اشـتباه یا تقلب ایجادشده بی‌درنگ کشف و اصلاح شود. بنابراین، ریسـک باقیمانده ممکن است به‌طور نسبی مربوط به کم‌توجهی به کنترل دستی باشد.

دوم این که به ریسک باقیمانده‌ای که در یک حوزه وجود دارد، ممکن اسـت در حوزه‌ای دیگر از طریق یـک کنترل اثربخش، پاسـخ داده شـود. برای نمونه، ممکن اسـت چنین اتفاق افتد که **دیوار آتش**[۱۸] پوشـش مناسـبی در برابر افـراد بیگانه‌ای که وارد محیط می‌شوند و به سـامانه نفوذ می‌کنند را نداشته باشد. نتیجه‌گیری سریع درباره ریسک باقیمانده سطح بالا و مرتبط با داده‌های مالی و همچنین گزارشـگری مالی، در چنین وضعیتی آسـان اسـت؛ گرچه در صورتی کـه واحد تجـاری **کنترلهای دسترسـی**[۱۹] قوی در لایه **شـبکه**[۲۰] (برای مثـال، ماتریس

کنترلی قوی برای **جدول جستجوی فعال**[۲۱] و **تفکیک منطقی وظایف**[۲۲]، در لایه **برنامه کاربردی**[۲۳] و بر **سامانه عامل**[۲۴] و بر دسترسی به پایگاه داده داشته باشد، حتی اگر اخلال‌گران به محیط دسترسی پیدا کنند، چه کاری می‌توانند انجام دهند؟ بنابراین، ضروری است که یک **بررسی کامل ذهنی**[۲۵] در این باره انجام شود که اگر ریسک باقیمانده و ادراک‌شده به واقعیت درآید، چگونه عمل خواهد کرد تا مشخص شود که آیا ریسک باقیمانده واقعی است یا خیر. در این مثال فرض می‌شود که هدف حسابرسی به گزارشگری مالی ارتباط دارد. روشن است چنانچه این موقعیت مربوط به حالتی بود که هدفهای حسابرسی در کل به سامانه‌ها یا دیوار آتش به‌طور اخص، ارتباط داشت، ریسک باقیمانده، ممکن بود واقعی باشد و نیاز به توجه داشت. در هر دو حالت، دیوار آتش فروریخته و با نارسایی مواجه می‌شود و به احتمال بسیار، نیازمند بازسازی است.

بررسی دامنه ریسک باقیمانده به این معناست که حسابرسی فناوری اطلاعات همچنین نیازمند یک **نگاشت ذهنی**[۲۶] از همه موارد آسیب‌دیده در فضای فناوری اطلاعات است و این که کدام واقعی/ مربوط و کدام آسیب‌دیده هستند؛ کدام در دامنه حسابرسی و کدام بیرون از این دامنه هستند. واقعیت این است که تمام حسابرسیهای فناوری اطلاعات به احتمال بسیار، موارد متعددی را آشکار می‌سازد، ولی امکان دارد همه آنها در دامنه حسابرسی نباشند.

همچنین، ضروری است که حسابرس فناوری اطلاعات یک استدلال منطقی را مبنی بر این بسط دهد که چرا موارد یافت‌شده در حسابرسی فناوری اطلاعات، نیازمند توجه و بهبود است و اطمینان دهد که این موضوع از دورنمای کسب‌وکار، درک‌پذیر و معنادار است. گرایش حسابرسان فناوری اطلاعات، یافتن موارد آسیب‌دیده است و خواهان آن هستند که همه آنها به‌دلیل نارسایی و آسیب‌دیدگی، بازسازی شوند. حسابرسان فناوری اطلاعات برای تعیین این که چه چیزی در واقع نیازمند بازسازی است، باید از منظر کسب‌وکار به بررسی بپردازند. این منطق کار باید از یک سناریوی منطقی، واقع‌گرایانه، مبتنی بر کسب‌وکار و از ریسک بالا برخوردار باشد تا به ثمر برسد.

این موضوع بیانگر این ضرورت است که حسابرسان فناوری اطلاعات باید توانایی ارتباط اثربخش داشته باشند.

نتیجه‌گیری

آنچه حسابرسان فناوری اطلاعات انجام می‌دهند، به‌طور معمول دربرگیرنده عرصه ریسک و کنترل است. بنابراین، مهم است که حسابرسان فناوری اطلاعات در زمینه‌های شناخت، تحلیل و ارائه نتایج مرتبط با ریسک و کنترلها، مهارت داشته باشند و این کاری است که ما انجام می‌دهیم.

پانوشتها:

1- Big Data
2- Social Media
3- Cloud Computing
4- Compliance Testing
5- Target Risk
6- Unique Inherent Risk
7- Systems Development
8- Change Management
9- Vulnerabilities
10- Bug
11- Real
12- Concrete
13- Impact
14- Online
15- Residual Risk
16- Paranoid
17- Databases
18- Firewall
19- Access Controls
20- Network
21- Active Directory
22- Logical Segregation of Duties
23- Application
24- Operating System
25- Mental Walk- through
26- Mental Map

منبع:

• Singleton T., **The Core of IT Auditing**, ISACA Journal, Vol. 6, 2014