جداسازی مناسب فعالیتهای ناسازگار در حوزه فناوری اطلاعات

ترجمه: نیوشا ابراهیمی

حسابرسی **کارکرد فناوری اطلاعات**[۱] یکی از اجزای حسابرسی فناوری اطلاعات است. در حالیکه حسابرسی کارکرد فناوری اطلاعات به‌طور احتمالی در حسابرسی مستقل (برون‌سازمانی) رایج‌تر است، اما این حسابرسی به‌ویژه در فعالیت براورد خطر یا در طراحی کارکرد فناوری اطلاعات، می‌تواند به‌گونه‌ای اطمینان‌بخش، به‌عنوان بخشی از حسابرسی داخلی اجرا شود. در هنگام نیاز، جنبه‌های بااهمیت کارکرد فناوری اطلاعات در یک حسابرسی یا براورد خطر نیز می‌تواند بررسی شود. یکی از این جنبه‌ها، **تفکیک وظایف**[۲] به‌گونه‌ای مناسب است؛ به‌ویژه اگر با خطر مرتبط باشد؛ مانند تفکیک وظایف سنتی در **کارکردهای حسابداری**[۳] و تفکیک وظیفه‌ها در فناوری اطلاعات که نقشی عمده در کاهش برخی خطرها و موارد مشابه بازی می‌کند. این نوشتار به برخی نقشها و کارکردهای کلیدی اشاره دارد که نیازمند جداسازی هستند.

وظایف فناوری اطلاعات در مقایسه با بخشهای کاربر

اساسی‌ترین تفکیک، یک نوعی تفکیک رایج است: تفکیک وظایف کارکرد فناوری اطلاعات از **بخشهای کاربر**[۴]. در کل، این به آن معنی است که بخش کاربر، وظایف فناوری اطلاعات خود را انجام نمی‌دهد. هنگامی که یک بخش، گاهی اوقات پشتیبانی فناوری اطلاعات خود را فراهم می‌کند (برای نمونه، **میز همکاری**[۵])، آن بخش نباید **تامین امنیت**[۶]، **برنامه‌نویسی**[۷] و دیگر وظایف فناوری اطلاعات دارای اهمیت را خود انجام دهد. درهم‌سازی وظیفه‌های فناوری اطلاعات با بخشهای کاربر، موجب افزایش خطر مرتبط با **اشتباه‌ها**[۸]، **تقلب**[۹] و **خرابکاری عمدی**[۱۰] خواهد شد.

از بخشهای کاربر انتظار می‌رود که اطلاعات ورودی را برای سیستمها و **ایجاد برنامه‌های کاربردی**[۱۱] (برای نمونه، **نیازهای اطلاعاتی**[۱۲]) و یک کارکرد اطمینان کیفی را در جریان مرحله آزمون فراهم کنند. در واقع، اصل مشترک ایجاد برنامه کاربردی این است که از کاربران درخواست شود تا برنامه جدید را پیش از عملیاتی شدن آزمون نموده و توافقنامه پذیرش کاربر را به امضا برسانند تا نشان داده شود این کار با توجه به نیازهای اطلاعاتی اجرا شده است. هرچند، بخش کارکرد فناوری اطلاعات باید از بخشهای کاربر جدا شود.

مدیریت پایگاه داده در مقایسه با بقیه کارکرد فناوری اطلاعات

مدیریت پایگاه داده[۱۳]، جایگاهی بااهمیت است که نیازمند سطحی بالا از تفکیک وظایف است. مدیریت پایگاه داده همه چیز را می‌داند یا تقریبا از همه چیز درباره داده، ساختار پایگاه داده و سیستم مدیریت پایگاه داده آگاه است. بدین ترتیب، کاربر برتر آنچه راکه متخصصان امنیت از آن با عنوان «کلید پادشاهی» یاد می‌کنند از جمله توانایی ذاتی برای دستیابی به تغییر و حذف هر چیز در پایگاه داده مرتبط را دارد. این موقعیتی است که به‌سوی براورد خطر در سطحی بسیار بالا پیرامون کارکرد فناوری اطلاعات هدایت شده است.

با توجه به سطوح خطر، اصل این است که مدیران پایگاه داده

مدیریت پایگاه داده جایگاهی بااهمیت است که نیازمند سطحی بالا از تفکیک وظایف است

از هرچیزی که انتظار می‌رود آنها باید برای اجرای وظایف خود انجام دهند (برای نمونه، طراحی پایگاه‌های داده، مدیریت پایگاه داده به‌عنوان یک فناوری، نظارت بر کاربرد و اجرای پایگاه داده)، تفکیک شوند. حسابرس فناوری اطلاعات باید بتواند نمودار سازمانی را برای مشاهده شرح تفکیک وظایف بررسی کند؛ به این معنی که مدیریت پایگاه داده درون یک نماد به‌شکل یک جزیره قرار گرفته باشد، هیچ کارکرد دیگری به مدیریت پایگاه داده گزارش ندهد و هیچگونه مسئولیت یا تعاملی با برنامه‌نویسی، تامین امنیت یا عملیات رایانه‌ای وجود نداشته باشد (**نمودار ۱**).

برای مدیران سیستم و مدیران سیستم‌عاملها نیز موقعیتی همانند وجود دارد.

ایجاد برنامه کاربردی در مقایسه با مدیریت پایگاه داده و عملیات فناوری اطلاعات

ایجاد و **نگهداشت برنامه‌های کاربردی**[۱۴] باید از عملیات برنامه‌های کاربردی و سیستمها و از مدیریت پایگاه داده، تفکیک شود. یعنی، افرادی که مسئولیت وظایفی مانند ورود اطلاعات، پشتیبانی، مدیریت ساختار فناوری اطلاعات و دیگر عملیات رایانه‌ای را برعهده دارند، باید از افراد مسئول ایجاد، نوشتن و مدیریت برنامه‌ها جدا باشند. همین موارد برای مدیریت پایگاه داده نیز صدق می‌کند.

همچنین، فردی که برنامه کاربردی را به عملیاتی تبدیل می‌کند نیز باید از برنامه‌نویسان فناوری اطلاعات مسئول کدنویسی و آزمون، متفاوت باشد.

این تفکیک وظایف باید در نمودار سازمانی، بازتاب بسیار دقیقی داشته باشد (**نمودار ۱**).

ایجاد برنامه کاربردی جدید در مقایسه با نگهداشت برنامه کاربردی

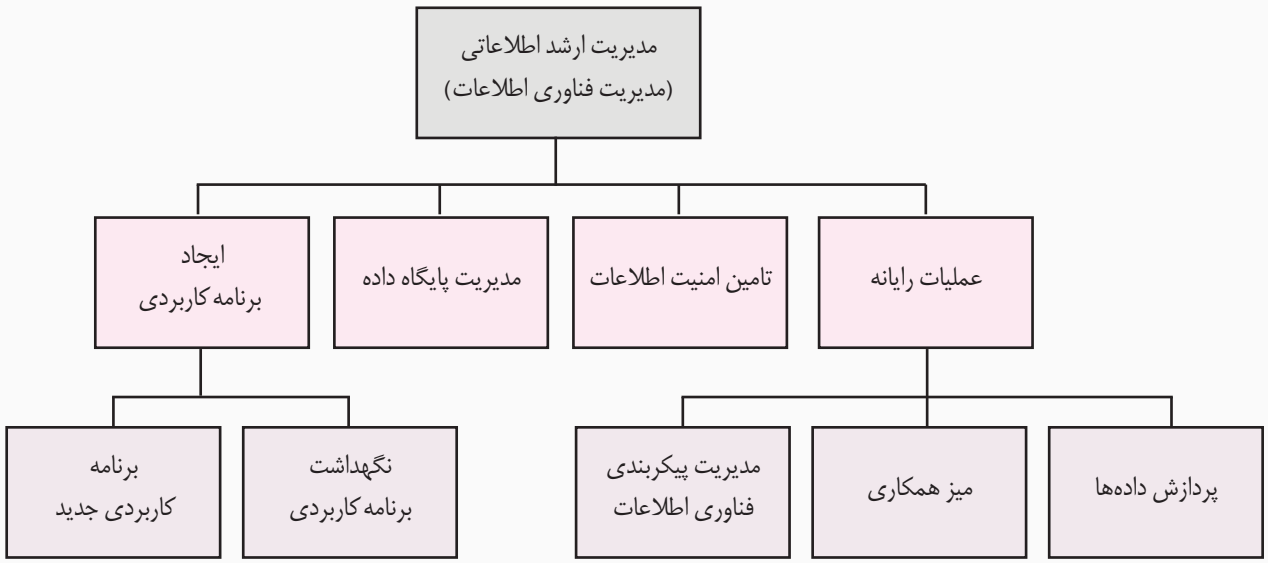
برای سازمانهایی که کارشان برنامه‌نویسی است یا برنامه‌های کاربردی را بنابر سفارش مشتری فراهم می‌کنند، خطری در برنامه‌نویسی وجود دارد که نیازمند کاهش است. یک راه برای کاهش خطر ترکیبی برنامه‌نویسی، جداکردن فرایند ایجاد برنامه کاربردی اصلی از نگهداشت آن برنامه است.

در یک کارگاه برنامه‌نویسی بزرگ، غیر معمول نیست که مدیر فناوری اطلاعات، برای ایجاد و نگهداشت یک بخش از مجموعه برنامه‌های کاربردی، گروهی را با هم مسئول این کار کند. برای نمونه، گروهی ممکن است مسئولیت کامل **برنامه‌های کاربردی مالی**[۱۵] را برعهده داشته باشند. این موقعیت باید کارامد باشد؛ اما خطرهای مرتبط با مستندسازی مناسب، اشتباهها، تقلب و خرابکاری عمدی را نیز نشان دهد.

این سناریو در کل به‌عنوان یک کنترل کاهنده خطر، باید تحلیلگران سیستم را نیز از برنامه‌نویسان جدا کند؛ هرچند، این کنترل ضعیف‌تر از تفکیک فرایند ایجاد برنامه کاربردی اصلی از نگهداشت آن است.

سناریوی پیشگفته به‌گونه‌ای مناسب، برخی خطرهای مربوط به مستندنساختن برنامه‌های کاربردی را از زمانی ارائه می‌کند که یک گروه هر چیزی را در یک بخش برای تمام برنامه‌های کاربردی انجام می‌دهد. این مورد به‌ویژه در حالی صدق می‌کند که فردی مسئول برنامه کاربردی خاصی باشد. مستندسازی نامناسب می‌تواند به خطر جدی منجر شود. برای نمونه، چنانچه کارکنان کلیدی از سازمان بروند، کارکرد فناوری اطلاعات ممکن است به چالش کشیده شده و زمانی بیهوده برای شناسایی کدها، جریان کدها و چگونگی

نمودار ۱- نمودار سازمانی نمونه، نمایشگر تفکیک اثربخش وظایف فناوری اطلاعات



انجام تغییر مورد نیاز، صرف شود. به این ترتیب مستندسازی، جایگزینی برای فرایند مربوط به برنامه‌نویسی کاراتر به‌وجود می‌آورد.

نبود تفکیک وظایف مناسب، فرصتهای بیشتری را برای یک فرد پدید می‌آورد تا کدهای مخرب را بدون آشکار شدن به (سیستم/برنامه) وارد کند- چون شخصی که کدهای اصلی را نوشته و رمزهای مخرب را وارد کرده، همان شخصی است که کدها را بررسی و بهنگام‌سازی کرده است. بنابراین، نبود تفکیک وظایف، خطر تقلب را افزایش می‌دهد. اگر **بخش‌بندی کردن**[۱۶] برنامه‌نویسان برای گروهی از برنامه‌نویسان مجاز و برخی از مسئولیتها به آنها واگذار شود، گروه‌های بررسی و کدنویسی باقی می‌مانند که در این صورت، خطر تقلب نیز می‌تواند تا حدی کاهش یابد.

موقعیتی مشابه از نظر خطر اشتباه در کدنویسی وجود دارد. اگر شخصی که کدها را می‌نویسد، همان شخصی باشد که کدها را نگهداری می‌کند، این احتمال وجود دارد که اشتباهی روی دهد و توسط کارکرد برنامه‌نویسی یافت نشود. این خطر را می‌توان با آزمون دقیق و اجرای کنترل کیفیت در کل آن برنامه‌ها، تا حدی کاهش داد.

یک نمودار سازمانی مناسب باید قادر باشد سیاست واحد تجاری درباره ایجاد و نگهداشت برنامه کاربردی اصلی و اینکه آیا تحلیلگران سیستم از برنامه‌نویسان جدا شده‌اند یا خیر را به نمایش بگذارد.

امنیت اطلاعات در مقایسه با بقیه کارکرد فناوری اطلاعات

در این مورد، بیشتر مانند مدیریت پایگاه داده، شخص (اشخاص) مسئول تامین امنیت اطلاعات که در جایگاهی مهم قرار گرفته است و «کلید پادشاهی» را در دست دارد، باید از دیگر اجزای کارکرد فناوری اطلاعات جدا شود. شخص مسئول، بیشتر تنظیمها، پیکربندیها، مدیریت و نظارت امنیتی (برای نمونه، پیروی از سیاستها و رویه‌های امنیتی) را اجرا می‌کند. اعتبار ورود به سیستم نیز ممکن است از سوی این شخص اجرا شده، یا از سوی منابع انسانی

حسابرس فناوری اطلاعات باید بتواند نمودار سازمانی را برای مشاهده شرح تفکیک وظایف بررسی کند

یا به‌وسیله سیستمی خودکار انجام شود. بنابراین، شخص مورد نظر، دانش کافی برای وارد ساختن آسیب عمده (به سیستم/ برنامه) را دارد. این خطر برای کوششهای مربوط به خرابکاری عمدی، بالا است.

حسابرسی کارکرد فناوری اطلاعات و تفکیک وظایف

برنامه حسابرسی باید دربرگیرنده موارد زیر باشد:

- بررسی سیاست و روش تامین امنیت اطلاعات،
- بررسی سیاستها و روشهای مستندسازی،
- بررسی نمودار سازمانی کارکرد فناوری اطلاعات (و شرح وظایف احتمالی)،
- پرس‌وجو از (مصاحبه با) کارکنان کلیدی فناوری اطلاعات درباره وظایفشان (این کار برای مدیر ارشد اطلاعات الزامی است)،
- بررسی نمونه‌ای از ثبتهای مربوط به مستندسازی و نگهداشت فرایند ایجاد برنامه کاربردی برای شناخت تفکیک

یک راه برای کاهش خطر ترکیبی برنامه‌نویسی جدا کردن گسترش برنامه کاربردی اصلی از نگهداشت آن برنامه است

وظایف (اگر در دامنه رسیدگی باشد)،

- مشاهده حضوری کارکنان از دیدگاه تفکیک وظایف،
- بررسی اینکه آیا برنامه‌نویسان بخش نگهداشت، برنامه‌نویسان طراح برنامه کاربردی اصلی هستند یا خیر، و
- بررسی دسترسی امنیتی برای اطمینان از نظر حفاظتی و اینکه برنامه‌نویسان طراح برنامه کاربردی اصلی، به کدها دسترسی نداشته باشند.

نتیجه‌گیری

نمودار ۱ برخی از تفکیکهای اصلی را نشان می‌دهد که باید در حسابرسی، تنظیم یا براورد خطر کارکرد فناوری اطلاعات، به آن توجه شود. نمودار سازمانی نمونه که به‌عنوان مثال، مدیریت پایگاه داده را به‌شکل جزیره نشان داده، تفکیک مناسبی از دیگر وظایف فناوری اطلاعات را به نمایش می‌گذارد. همین مورد برای تامین امنیت اطلاعات نیز صادق است. فعالیت ایجاد برنامه کاربردی به برنامه‌های کاربردی جدید و نگهداشت برنامه‌های کاربردی، تفکیک می‌شود. حسابرسان فناوری اطلاعات نیاز دارند تا اجرای اثربخش تفکیک وظایف در هنگام کاربردپذیر بودن آن برای حسابرسیها، براورد خطر و دیگر کارکردهایی که ممکن است حسابرس فناوری اطلاعات اجرا کند را ارزیابی کنند. دلیل تفکیک وظایف، کاهش خطر تقلب، اشتباه‌ها، خرابکاری عمدی، برنامه‌ریزی برای ناکارامدیها و موارد مشابه دیگر خطر پیرامون فناوری اطلاعات است.

پانوشتها:

1- Information Technology (IT) Function
2- Segregation of Duties (SoD)
3- Accounting Functions
4- User Departments
5- Help Desk
6- Security
7- Programming
8- Errors
9- Fraud
10- Sabotage
11- Application Development (AppDev)
12- Information Requirements
13- Database Administrator (DBA)
14- Maintenance of Applications
15- Financial Applications
16- Departmentalization

منبع:

• Singleton T.W., **What Every IT Auditor Should Know About Proper Segregation of Incompatible IT Activities**, ISACA Journal, Vol. 6, 2012