حسابرسی کنترل‌های راهبری فناوری اطلاعات

محمد جندقی قمی

از قرن بیستم به بعد، فناوری اطلاعات، بطور گسترده و عمیق فرآیندهای تجاری، سازمان‌ها و حتی حسابرسی را متحول ساخته است. این تغییرات، بازنگری اساسی در فرآیند حسابرسی را اجتناب ناپذیر کرده است (بل و همکاران، ۱۹۹۷). در این مطالعه، ریسک‌ها، کنترل‌ها، و آزمون‌های کنترل مربوط به حسابرسی راهبری فناوری اطلاعات ارائه می‌شود. مطالب با تعریف راهبری فناوری اطلاعات شروع می‌شود و عناصر راهبری فناوری اطلاعات مؤثر بر کنترل داخلی و گزارشگری مالی را در بر می‌گیرد. در این راستا، نخست به انواع سازمان‌دهی واحد فناوری اطلاعات پرداخته شده و ریسک‌های پیرامون مدل‌های متداول آن تشریح می‌شود. سپس به بررسی تهدیدها و کنترل‌های مراکز رایانه‌ای شامل حفاظت در برابر تخریب و نابودی بوسیله‌ی فجایع طبیعی، انسان‌ساز و شکست سیستم پرداخته می‌شود. در پایان نیز عناصر اصلی برنامه‌ی بازیابی فجایع شامل شناسایی برنامه‌های کاربردی حیاتی، ایجاد تیم بازیابی فاجعه، ایجاد مکانی برای پشتیبان‌گیری اطلاعات، و رویه‌های پشتیبان‌گیری و بایگانی در خارج از سازمان ارائه می‌گردد. در خلال هر یک از بخش‌های مذکور، ضمن ارائه‌ی یک معرفی اجمالی، رویه‌های حسابرسی مورد نیاز برای کسب شناخت و ارزیابی ریسک‌های مربوط تشریح می‌شود.

راهبری فناوری اطلاعات چیست؟

راهبری فناوری اطلاعات[1] یک موضوع نسبتاً جدید در راهبری شرکتی است که بر مدیریت و ارزیابی استراتژیک منابع فناوری اطلاعات توجه دارد. اهداف اصلی راهبری فناوری اطلاعات، کاهش ریسک و اطمینان نسبت به این است که سرمایه‌گذاری در منابع فناوری اطلاعات، برای شرکت ارزش افزوده به ارمغان می‌آورد. پیش از قانون ساربینز- آکسلی، رویه‌ی معمول در مورد سرمایه‌گذاری‌های مربوط به فناوری اطلاعات این بود که تمامی تصمیمات در این‌باره به کارکنان فناوری اطلاعات شرکت واگذار می‌شد. اما در راهبری فناوری اطلاعات امروزین، از این فلسفه پیروی می‌شود که تمامی ذینفعان شرکت، شامل هیأت‌مدیره، مدیریت ارشد، و کارکنان دوایر مربوط به آن (مانند حسابداری و مالی)، نقشی فعال در زمینه‌ی تصمیمات کلیدی مربوط به فناوری اطلاعات ایفا نمایند. هدف راهبری فناوری اطلاعات این است که با مشارکت تمامی ذیفعان منابع فناوری اطلاعات سازمان، ریسک مربوط به فناوری اطلاعات کاهش یافته و احتمال متناسب بودن تصمیمات فناوری اطلاعات با نیازهای استفاده‌کنندگان آن، سیاست‌های شرکت، اهداف استراتژیک و الزامات کنترل داخلی قانون ساربینز- آکسلی افزایش یابد.

همسوسازی مناسب فناوری اطلاعات و اهداف سازمانی زمانی صورت می‌گیرد که: ۱) مدیریت سازمان به شناختی از منافع و محدودیت‌های فناوری اطلاعات دست یابند؛ ۲) واحد فناوری اطلاعات سازمان، اهداف و نیازهای سازمان را شناسایی کرده و ۳) نسبت به برآورده شدن نیازها و اهداف فناوری اطلاعات در سراسر سازمان اقدام شده و این امر از طریق یک ساختار و پاسخگویی راهبری مناسب تحت کنترل و نظارت باشد (انجمن حسابرسان داخلی، ۲۰۱۲). در این مطالعه، به سه مبحث راهبری فناوری اطلاعات پرداخته می‌شود که مورد توجه قانون ساربینز- آکسلی و چارچوب کنترل داخلی کوزو واقع شده است. این موارد عبارتند از:

۱. ساختار سازمان‌دهی واحد فناوری اطلاعات؛
۲. محیط مرکز رایانه؛
۳. برنامه‌ریزی بازیابی فجایع.

هر یک از این مباحث، با شناسایی ریسک‌ها و کنترل‌های مورد نیاز آغاز می‌شود. سپس، اهداف حسابرسی در راستای بررسی کارکرد کنترل‌ها مربوط مطرح می‌شود. در پایان، نمونه‌ای از آزمون‌های کنترلی ارائه می‌شود که به بررسی چگونگی جمع‌آوری شواهد حسابرسی برای برآورده کردن اهداف حسابرسی پرداخته می‌شود. این آزمون‌های می‌تواند توسط حسابرسان مستقل به عنوان بخشی از خدمات شهادت‌دهی، یا توسط حسابرسان داخلی به منظور جمع‌آوری شواهدی جهت راهنمایی مدیریت در راستای پیروی از قانون ساربینز- آکسلی به‌کار گرفته شود.

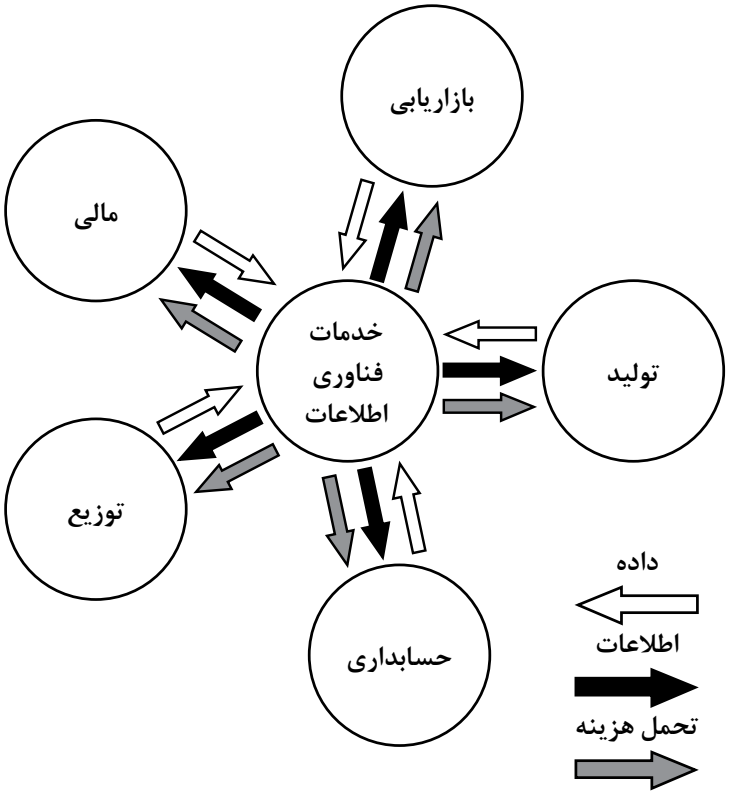
۱. ساختار سازمان‌دهی واحد فناوری اطلاعات

ساختار واحد فناوری اطلاعات، بر ماهیت و اثربخشی کنترل‌های داخلی اثرگذار است و این امر حسابرسی مربوط به این زمینه را نیز متأثر می‌سازد. در این بخش، برخی از مسائل کنترلی مهم در ارتباط با ساختار فناوری اطلاعات مورد بررسی قرار می‌گیرد. در این راستا دو مدل سازمان‌دهی شامل پردازش داده‌ی متمرکز و غیرمتمرکز مورد توجه قرار می‌گیرد. سپس ریسک‌ها، کنترل‌ها و مسائل حسابرسی مربوط به هر مدل مورد بررسی قرار می‌گیرد. با این وجود، مخاطب باید در نظر داشته باشد که بیش‌تر مدل‌های سازمانی شامل عناصری از هر دو رویکرد هستند.

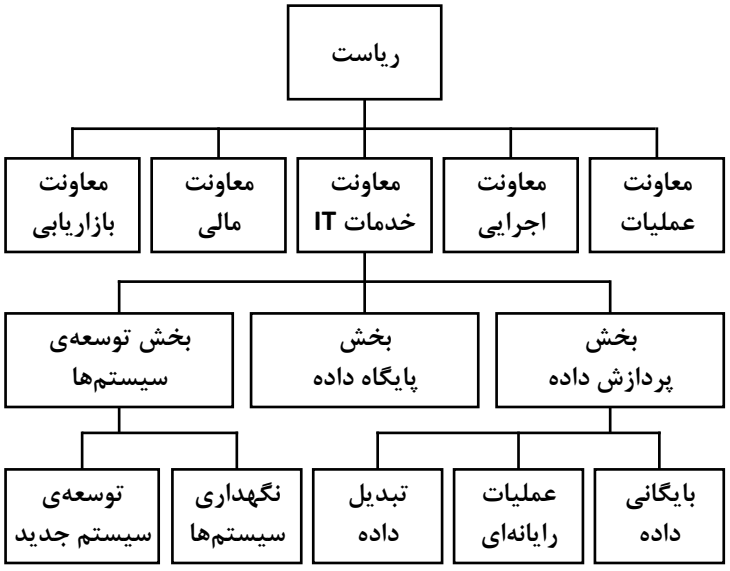
مدل پردازش داده‌ی متمرکز

تحت مدل پردازش داده‌ی متمرکز، تمامی فرآیندهای پردازش داده بوسیله‌ی یک یا تعدادی از رایانه‌های بزرگ صورت می‌گیرد که در یک سایت مرکزی مستقر است و به کاربران سازمان سرویس می‌دهند. نگاره ۱ این رویکرد را به تصویر می‌کشد. همانطور که در این نگاره مشاهده می‌شود، فناوری اطلاعات مانند یک منبع سازمانی به اشتراک گذاشته شده و به ارائه‌ی خدمات به کاربران می‌پردازد. کاربران سازمان، بر حسب نیازشان،

نگاره۱: روش پردازش داده‌ی متمرکز



نگاره۲: ساختار سازمانی واحد فناوری اطلاعات متمرکز



جهت بهره‌برداری بیش‌تر از آن با هم رقابت می‌کنند. واحد خدمات فناوری اطلاعات به‌طور معمول به عنوان یک واحد هزینه شناخته می‌شود که مخارج آن بر کاربران سازمان سرشکن می‌شود. در ساختار سازمانی مدل متمرکز، سه بخش تحت عناوین پردازش داده، پایگاه داده و توسعه‌ی سیستم به عنوان زیرمجموعه‌های معاونت فناوری اطلاعات فعالیت می‌نمایند. نگاره ۲ خدمات فناوری اطلاعات و بخش‌های اصلی مدل متمرکز را نشان می‌دهد.

بخش پردازش داده، منابع رایانه‌ای مورد استفاده جهت اجرا و پردازش مبادلات روزمره را مدیریت می‌نمایند. این امر شامل وظایف تبدیل داده، عملیات رایانه‌ای و بایگانی داده می‌شود. در مرحله‌ی تبدیل داده، داده‌ها از منابع کاغذی به ورودی رایانه‌ای تبدیل می‌شوند. طی فرآیند عملیات رایانه‌ای، پرونده‌های الکترونیکی تولید شده در مرحله‌ی تبدیل داده، به‌وسیله‌ی رایانه‌ی مرکزی پردازش می‌شوند. سرانجام طی فرآیند بایگانی داده، پرونده‌های داده را به‌صورت خارج از خط[۲] و به‌طور مطمئنی در اتاقی در نزدیکی مرکز رایانه، نگهداری می‌نماید. فردی که مسئولیت بایگانی داده را بر عهده دارد، وظیفه‌ی دریافت، ذخیره، بازیابی، حفاظت از پرونده‌های داده و کنترل دسترسی به بایگانی را بر عهده دارد.

در بخش پایگاه داده[۳]، انبوهی از اطلاعات کسب و کار شرکت‌ها نگهداری می‌شود و گروهی مستقل از سایر واحدهای فناوری اطلاعات، مسئولیت امنیت و یکپارچگی پایگاه داده را بر عهده دارند. داده‌های وارد شده به پایگاه داده ممکن است در دفعات مختلف در پرونده‌های متفاوتی ذخیره شده باشند و این امر می‌تواند دستیابی به اطلاعات مورد نیاز مانند سوابق یک مشتری را با دشواری مواجه نماید. وظیفه‌ی بخش پایگاه داده این است که ضمن نگهداری و اطمینان از ایمنی داده‌های سازمان، یک‌پارچگی و توزیع داده‌ها بین افراد مجاز را نیز مدیریت نماید. در این راستا، سیستم مدیریت پایگاه داده[۴] امکان مدیریت و کنترل پایگاه داده را فراهم می‌نماید. به‌علاوه، سیستم مدیریت پایگاه داده به‌طور اساسی از توانایی تغییر ماهیت فرآیند حسابداری و گزارشگری مالی برخوردار است. به بیان دیگر، در حالی‌که امروزه داده‌های مالی سازمان بصورت دستی و با صرف هزینه‌ها جمع‌آوری و در پایگاه داده ذخیره می‌شود، سیستم‌های مدیریت پایگاه داده‌ی نوین امکان جمع‌آوری و پردازش خودکار کلیه‌ی داده‌های مورد نیاز سازمان را فراهم نموده‌اند (رامنی و استین بارت، ۱۳۹۰).

بخش توسعه‌ی سیستم‌ها، نیازهای فناوری اطلاعات کاربران را از دو طریق شامل توسعه‌ی سیستم و نگهداری سیستم برآورده می‌سازند. در این بخش، یک تیم حرفه‌ای مسئول تجزیه و تحلیل نیازهای استفاده‌کنندگان است تا ضمن حفظ سیستم‌های موجود در وضعیت مطلوب، سیستم‌های جدید را به گونه‌ای طراحی نمایند که نیازهای موجود را برآورده سازد. مشارکت‌کنندگان در فعالیت‌های توسعه‌ی سیستم عبارتند از: متخصصان سیستم، کاربران و ذینفعان. متخصصان سیستم‌ها شامل آنالیزکنندگان سیستم، طراحان پایگاه‌های داده و برنامه‌نویسان می‌باشند. کاربران سیستم افرادی هستند که سیستم برای آن‌ها ساخته شده است. ذینفعان افراد درون و برون سازمانی هستند که در سیستم ذینفع هستند اما کاربران نهایی آن نیستند.

تفکیک وظایف ناسازگار در ساختار متمرکز

در ادبیات کنترل‌های داخلی، بر اهمیت تفکیک وظایف ناسازگار در فعالیت‌های دستی، بسیار تأکید شده است. به‌طور خاص، فعالیت‌های عملیاتی که باید تفکیک شوند عبارتند از: تفکیک وظیفه‌ی تصویب از وظیفه‌ی پردازش مبادلات؛ تفکیک وظیفه‌ی نگهداری سوابق از وظیفه‌ی نگهداری دارایی؛ تقسیم وظایف پردازش مبادلات میان چندین نفر به‌طوریکه امکان تبانی و ارتکاب به تقلب وجود نداشته باشد. گسترش فناوری اطلاعات در سازمان‌ها، به ادغام

فعالیت‌ها انجامیده است، به‌طوریکه یک برنامه‌ی کاربردی به تنهایی می‌تواند تمامی جنبه‌های یک مبادله را تصویب، پردازش و ثبت نماید. بر این اساس، در محیط سازمانی مبتنی بر فناوری اطلاعات، تمرکز کنترل‌های تفکیک وظایف از سطوح عملیاتی به سطوح بالای روابط سازمانی تعمیم می‌یابد. در ادامه، از نمودار سازمانی نگاره ۲ به عنوان یک مرجع استفاده می‌شود تا روابط متقابل بین بخش‌های توسعه‌ی سیستم، نگهداری سیستم، مدیریت پایگاه داده و فعالیت‌های عملیات رایانه‌ای ارزیابی گردد.

تفکیک توسعه‌ی سیستم‌ها از عملیات رایانه‌ای

تفکیک توسعه‌ی سیستم‌ها (هم توسعه‌ی سیستم‌های جدید و هم نگهداری) و فعالیت‌های عملیاتی بسیار با اهمیت است. روابط بین این گروه‌ها باید بی‌نهایت رسمی باشد و مسئولیت‌های آن‌ها نباید به هیچ وجه با هم ادغام شود. تخصص‌های توسعه و نگهداری سیستم‌ها، به خلق (و نگهداری) سیستم‌ها برای کاربران می‌پردازند و به هیچ وجه نباید با کارکردهای ورود داده یا اجرای برنامه‌های کاربردی (یعنی عملیات رایانه) ارتباطی پیدا کنند. کارکنان عملیاتی باید سیستم‌ها را اجرا کنند و هیچ‌گونه ارتباطی با طراحی آن‌ها نداشته باشند. این وظایف ذاتاً ناسازگار هستند و ادغام آن‌ها به اشتباه و تقلب منجر می‌شود. فردی با دانشی عمیق از منطق برنامه‌های کاربردی و پارامترهای کنترلی و دسترسی به سیستم عامل و برنامه‌های رایانه‌ای می‌تواند در حین انجام کار خود، تغییرات غیر مجازی را در برنامه‌های کاربردی ایجاد نماید. این تغییرات می‌تواند موقتی (گذرا) باشند و بدون هیچ‌گونه ردپایی ناپدید شوند.

تفکیک مدیریت پایگاه داده از سایر وظایف

یک کنترل سازمانی با اهمیت دیگر، تفکیک مدیریت پایگاه داده از سایر وظایف مرکز رایانه است. مدیریت پایگاه داده مسئول تعدادی از وظایف حساس مربوط به امنیت پایگاه داده، شامل ایجاد مدل پایگاه داده و نماهای کاربری، ارائه اجازه‌ی دسترسی به پایگاه داده توسط کاربران، نظارت بر استفاده از پایگاه داده، و برنامه‌ریزی برای توسعه آتی سیستم است. واگذاری این وظایف به افرادی که وظایف ناسازگار را بر عهده دارند، یکپارچگی پایگاه داده را با تهدید مواجه می‌سازد. بنابراین، همانطور که در نگاره ۲ مشاهده می‌شود، وظیفه‌ی مدیریت پایگاه داده مستقل از وظایف توسعه و نگهداری سیستم است.

تفکیک توسعه‌ی سیستم‌های جدید از نگهداری

برخی از شرکت‌ها وظیفه‌ی توسعه‌ی سیستم‌ها را به دو بخش شامل تحلیل سیستم‌ها و برنامه‌ریزی تقسیم می‌نمایند. بخش تحلیل سیستم‌ها با کاربران در ارتباط است تا به طراحی تفصیلی سیستم‌های جدید بپردازد. بخش برنامه‌ریزی به کد نویسی برنامه‌ها بر اساس ویژگی‌های طرح تهیه‌ی شده می‌پردازند. تحت این رویکرد، برنامه‌نویس که برنامه‌های اولیه را کد نویسی می‌کند، به نگهداری سیستم در خلال فرآیند نگهداری چرخه‌ی عمر توسعه‌ی سیستم‌ها نیز می‌پردازد. علی‌رغم اینکه این رویه، رویه‌ای مرسوم است اما با دو منگاره کنترلی مواجه است: مستندات ناکافی و احتمال تقلب برنامه‌ای.

مستندات ناکافی. ضعف مستندات، پاشنه‌ی آشیل سیستم‌های مبتنی بر فناوری اطلاعات و یک چالش اساسی برای بسیاری از سازمان‌هایی است که به دنبال برآورده کردن الزامات قانون ساربینز- آکسلی می‌باشند. این پدیده حداقل از دو عامل نشأت می‌گیرد. نخست، مستندسازی در سیستم‌ها به میزان طراحی، آزمون و اجرای آن‌ها مورد توجه واقع نمی‌شود. متخصصان سیستم‌ها بیش‌تر ترجیح می‌دهند که به سراغ یک پروژه‌ی جدید بروند تا اینکه به مستندسازی یک پروژه‌ی کامل شده بپردازند. دلیل احتمالی دوم برای مستندسازی ضعیف، امنیت شغلی است. زمانی که یک سیستم بطور ضعیف مستندسازی شده باشد، تفسیر، آزمون و بهبود آن دشوار می‌شود. بنابراین، برنامه‌نویسی که سیستم را می‌شناسد (آن را کدنویسی کرده است)، توانایی بهبود سیستم را دارد و این امر تقریباً اجتناب‌ناپذیر است. اما زمانی که برنامه‌نویس شرکت را ترک می‌کند، برنامه‌نویس جدید مسئولیت نگهداری سیستمی را به ارث می‌برد که بطور کافی مستندسازی نشده است. متناسب با پیچیدگی سیستم، این اقدام می‌تواند برای شرکت زمان‌بر و پر هزینه باشد.

تقلب برنامه‌ای. زمانی که برنامه‌نویس اولیه‌ی سیستم، مسئولیت نگهداری آن نیز واگذار می‌شود، احتمال تقلب افزایش می‌یابد. تقلب برنامه‌ای بیان‌گر ایجاد تغییرات غیر مجاز در برنامه‌ها جهت دست‌یابی به منافع نامشروع است. برنامه‌نویس اولیه ممکن است بطور موفقیت‌آمیزی کد تقلبی را در میان هزاران سطر برنامه‌ی صحیح و صدها برنامه‌ی موجود در یک سیستم پنهان سازد. اما به منظور تداوم موافقیت‌آمیز تقلب، برنامه‌نویس باید نسبت به دسترسی گسترده و نامحدود به کدها و کشف احتمالی تقلب توسط برنامه‌نویس دیگری که وظیفه‌ی نگهداری یا حسابرسی سیستم را بر عهده دارد، مراقب باشد.

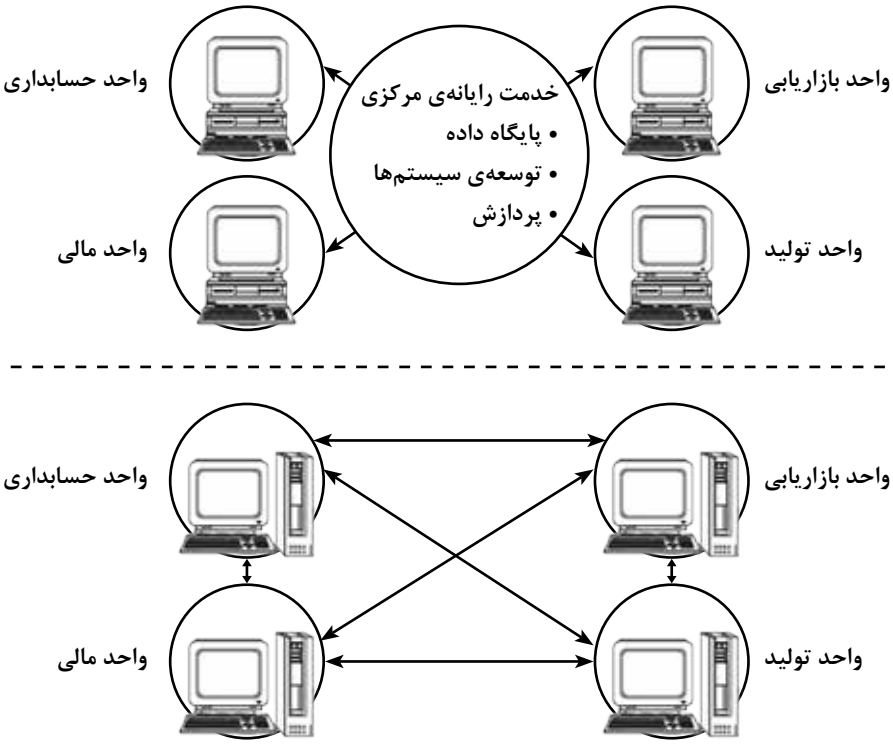
بنابراین، تفکیک مسئولیت نگهداری سیستم، نقشی مهم در پیش‌گیری از تقلب برنامه‌ای ایفا می‌نماید. در این شرایط، مسئول نگهداری سیستم، بطور آزادانه به سیستم دسترسی داشته و کدهای تقلبی را در خلال حسابرسی شناسایی و غیر فعال کرده و سیستم را ترمیم می‌نماید. تقلب‌هایی از این نوع می‌تواند برای سال‌ها، کشف نشده باقی بماند.

مدل پردازش داده‌ی غیرمتمرکز

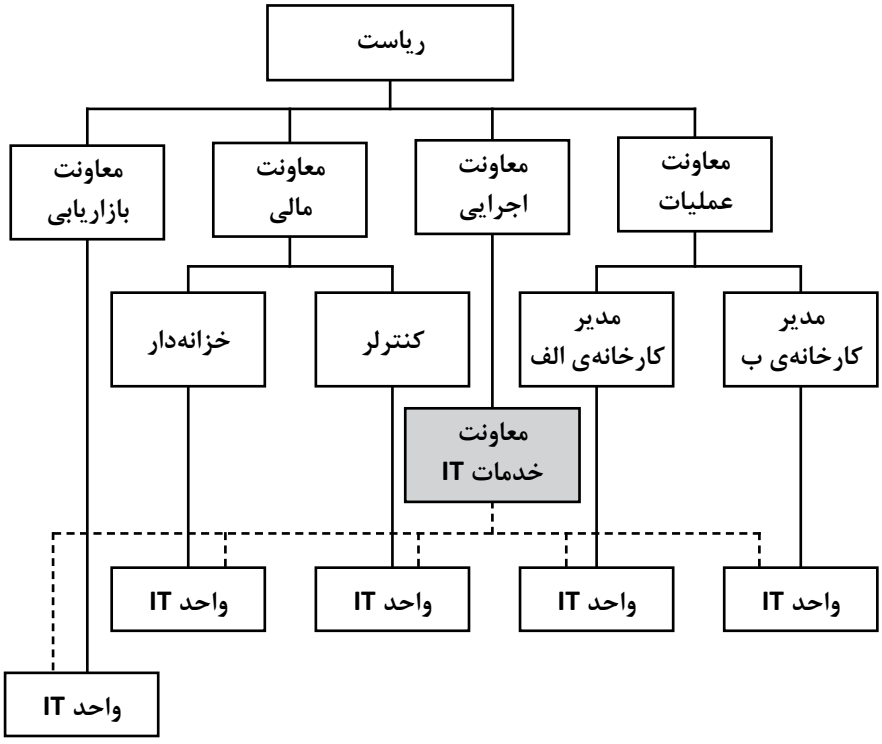
برای سالیان بسیار، صرفه‌جویی حاصل از مقیاس، سازمان‌ها را به استفاده از رایانه‌های بزرگ، قوی و پردازش مرکزی ترغیب می‌کرد. اما امروز، سیستم‌های کوچک، قوی و ارزان این وضعیت را بطور قابل ملاحظه‌ای تغییر داده است. یک جایگزین برای مدل متمرکز، مفهوم پردازش داده‌ی غیرمتمرکز[5] است. موضوع پردازش داده‌ی توزیع شده، بسیار گسترده است و با موضوعاتی از قبیل کاربران، نرم افزارهای تجاری، شبکه و اتوماسیون اداری ارتباط پیدا می‌کند. پردازش داده‌ی توزیع شده با سازمان‌دهی مجدد واحد فناوری اطلاعات مرکزی به واحدهای فناوری اطلاعات کوچک‌تر و تحت کنترل کاربران سر و کار دارد. واحدهای فناوری اطلاعات می‌توانند بر حسب کارکرد تجاری، موقعیت جغرافیایی یا هر دو توزیع شده باشند. بر حسب فلسفه و اهداف مدیریتی سازمان، همه یا هر یک از بخش‌های فناوری اطلاعات که در نگاره ۲ ارائه شده است، می‌تواند غیرمتمرکز شده باشد. نگاره ۳ دو رویکرد توزیع شده‌ی جایگزین را ارائه می‌دهد.

رویکرد الف، بطور کلی یک مدل متمرکز متفاوت است. وجه تمایز آن، این است که پایانه‌ها (یا رایانه‌های کوچک) بین کاربرانی توزیع شده است که مسئول ورود داده و دریافت

نگاره۳: دو نوع پردازش داده‌ی توزیع شده



نگاره۴: ساختار سازمانی برای محیط پردازش داده‌ی توزیع شده



خروجی هستند. این امر، ضرورت وجود پایگاه داده‌ی مرکزی را از بین می‌برد؛ زیرا کابران بطور مستقل قادر به انجام وظایف خود می‌باشند. اما، تحت این مدل، توسعه‌ی سیستم‌ها، عملیات رایانه‌ای، و مدیریت پایگاه داده بطور مرکزگرا باقی می‌ماند.

رویکرد ب، بطور قابل ملاحظه‌ای از مدل متمرکز متمایز است. در این رویکرد، تمامی خدمات رایانه‌ای به کاربران واگذار شده است و آن‌ها به عنوان واحدهای مستقل فعالیت می‌نمایند. نتیجه‌ی این رویکرد، حذف واحد فناوری اطلاعات مرکزی از ساختار سازمانی است. به روابط بین واحدهای تعمیم‌داده شده در نگاره ۳ توجه نمایید. این روابط، یک ساختار شبکه‌ای را ارائه می‌دهد که باعث نقل و انتقال داده بین واحدها می‌شود. نگاره ۴ یک ساختار سازمانی نمونه را ارائه می‌دهد که تمامی وظایف پردازش داده‌ی مرسوم، در آن به کاربران واگذار شده است.

ریسک‌های مربوط به پردازش داده‌ی غیرمتمرکز

گرچه مدل پردازش داده‌ی غیرمتمرکز مزایای بالقوه‌ای از قبیل کاهش هزینه‌ی سربار، بهبود تصمیمات سازمانی، بهبود رضایت کاربران و انعطاف‌پذیری در اختیارات و پشتیبان‌گیری را به دنبال دارد، اما با ریسک‌های متعدد سازمانی نیز همراه است که باید بوسیله‌ی حسابرسان مورد توجه قرار گیرد. استفاده‌ی ناکافی از منابع، تخریب زنجیره‌ی عطف حسابرسی، تفکیک وظایف ناکافی، احتمال افزایشی اشتباهات برنامه‌ریزی و شکست پروژه‌ی سیستم‌ها، و نقص استانداردها از جمله این موارد هستند که در ادامه تشریح می‌شوند.

استفاده‌ی ناکارا از منابع. پردازش داده‌ی غیرمتمرکز می‌تواند

سازمان را در معرض سه نوع ریسک مربوط به استفاده ناکارا از منابع سازمانی قرار دهد. مورد اول، ریسک سوء مدیریت منابع فناوری اطلاعات سازمان بوسیله‌ی کاربران است. برخی ادعا می‌کنند زمانی که منابع فناوری اطلاعات سازمان از یک میزان آستانه‌ای فراتر رود (برای مثال به میزان ۵ درصد کل بودجه‌ی عملیاتی)، راهبری فناوری اطلاعات اثربخش مستلزم مدیریت و نظارت متمرکز بر این قبیل منابع است. دوم، پردازش داده‌ی غیرمتمرکز، به دلیل احتمال انجام کارهای حاشیه‌ای و شخصی‌سازی بوسیله‌ی کاربران، می‌تواند ناکارایی عملیاتی را افزایش دهد. سوم، محیط پردازش داده‌ی توزیع شده، ریسک ناسازگاری بین سخت افزار و نرم افزار کاربران را موجب خواهد شد. برای مثال، تصمیم‌گیرندگان در واحدهای سازمانی مختلف، ممکن است از سیستم عامل‌های ناسازگار، ساختارهای متفاوت برای محیط‌های کاربری، صفحه گسترده‌ها گوناگون، انواع مختلفی از پردازنده‌ها و پایگاه‌های داده استفاده نمایند. سخت افزار و نرم افزارهای ناسازگار ممکن است به ارتباطات بین واحدهای کاربری آسیب بزند و به از بین رفتن تراکنش‌ها و زنجیره عطف حسابرسی منجر شود.

تخریب زنجیره‌های عطف حسابرسی. زنجیره عطف حسابرسی، بین فعالیت‌های مالی شرکت (مبادلات) و صورت‌های مالی حاوی گزارش فعالیت‌ها ارتباط برقرار می‌کند. حسابرسان از زنجیره عطف حسابرسی جهت رهگیری مبادلات مالی انتخاب شده به اسناد مثبته‌ی حاوی رویدادها، از طریق دفاتر روزنامه، دفاتر معین و حساب‌های دفتر کل که رویدادها در آن‌ها ثبت شده‌اند و در نهایت به صورت‌های مالی استفاده می‌نمایند. وجود زنجیره‌ی عطف حسابرسی برای خدمات شهادت‌دهی حسابرس ضروری است. در سیستم‌های پردازش داده‌ی غیرمتمرکز، زنجیره‌ی عطف حسابرسی شامل مجموعه‌ای از پرونده‌های مبادلات الکترونیکی و فایل‌های اصلی است که در برخی یا تمامی رایانه‌های کاربران مستقر است. اگر یک کاربر بطور غیر عمدی پرونده‌ای را حذف نماید، زنجیره‌ی عطف حسابرسی ممکن است تخریب و غیر قابل بازیابی شود. بطور مشابه، چنانچه کاربری بطور غیر عمدی، عملیات اشتباهی را روی زنجیره‌ی عطف حسابرسی انجام

دهد، ممکن است آن را از بین ببرد.

تفکیک وظایف ناکافی. دستیابی به تفکیک وظایف مناسب ممکن است در برخی از محیط‌های پردازش داده‌ی غیرمتمرکز امکان‌پذیر نباشد. تفکیک وظایف ناسازگار در توزیع خدمات فناوری اطلاعات به کاربران در واحدهای کوچک ممکن است بطور مناسب صورت نگیرد. برای مثال، در یک واحد انفرادی، شخص واحدی ممکن است برنامه‌های کاربردی را بنویسد، نگهداری سیستم را بر عهده داشته باشد، داده‌ی مبادلات را به رایانه وارد نماید و به عنوان کاربر از رایانه استفاده نماید. در این قبیل مواقع، کنترل داخلی با ضعفی عمده دست به گریبان خواهد بود.

استخدام متخصصان دارای صلاحیت. مدیران ممکن است دانش اندکی درباره‌ی ارزیابی گواهینامه‌های فنی و تجربه‌ی داوطلبان تصدی موقعیت‌های حرفه‌ای فناوری اطلاعات سازمان داشته باشند. همچنین، اگر واحد سازمانی کوچکی اقدام به استخدام یک کارمند جدید نماید، فرصت رشد ، آموزش مستمر و ترفیع فرد می‌تواند محدود باشد. به این دلیل، مدیران ممکن است در جذب افراد با صلاحیت بالا با چالش مواجه شوند. همچنین ریسک اشتباهات برنامه‌نویسی و شکست سیستم، بطور مستقیم با عدم صلاحیت کارکنان افزایش می‌یابد.

ضعف استانداردها. به دلیل توزیع مسئولیت در محیط پردازش داده‌ی توزیع شده، استانداردها برای توسعه و مستندسازی سیستم‌ها، انتخاب زبان‌های برنامه‌نویسی، بکارگیری سخت افزار و نرم افزار، و ارزیابی عملکرد ممکن است اجرا نشود و یا حتی وجود نداشته باشد. مخالفان پردازش داده‌ی توزیع شده بیان می‌کنندکه ریسک‌های مربوط به این سیستم، حتی با وجود اجرای مناسب استانداردهای مربوط نیز وجود خواهد داشت.

حسابرسی واحد فناوری اطلاعات

هدف حسابرس کسب شناخت از ساختار واحد فناوری اطلاعات از لحاظ تفکیک مناسب وظایف ناسازگار و ارزیابی سطح ریسک مطابق با اهداف از پیش تعیین شده است. محیط فناوری اطلاعات، بیش‌تر محیطی رسمی است تا اینکه محیطی مبتنی بر روابط بین افراد دارای وظایف ناسازگار باشد. رویه‌های حسابرسی زیر در یک سازمان با واحد فناوری اطلاعات متمرکز به اجرا می‌شود:

- بررسی مستندات مربوط؛ از قبیل نمودار سازمانی، بیانیه‌ی مأموریت و شرح وظایف مشاغل کلیدی سازمان ارزیابی می‌شود تا چنانچه تفکیک وظایف ناسازگار بطور مناسب صورت نگرفته بود، مشخص گردد.
- بررسی مستندات سیستم و سوابق نگهداری برای نمونه‌ای از برنامه‌های کاربردی؛ بررسی اینکه وظایف نگهداری پروژه‌های فناوری اطلاعات از وظیفه‌ی تدوین آن‌ها بطور مناسب تفکیک شده است.
- بررسی اینکه اپراتورهای رایانه به منطق داخلی سیستم دسترسی نداشته باشند. مستندات سیستم‌ها از قبیل فلوچارت‌های سیستم‌ها، فلوچارت‌های منطقی و فهرست‌های کدهای برنامه نباید در دسترس اپراتور سیستم قرار داشته باشد.
- از طریق مشاهده مشخص شود که سیاست تفکیک وظایف بطور مناسب در عمل اجرا شده است. با بررسی نام کاربری برنامه‌نویسان مشخص گرددکه آیا آنان به دلایلی غیر از نواقص سیستمی، به سیستم ورود پیدا کرده‌اند یا خیر.

رویه‌های حسابرسی زیر می‌تواند در سازمانی با مدل پردازش داده‌ی غیرمتمرکز بکار گرفته شود:

- نمودار سازمانی، بیانیه‌ی مأموریت و شرح وظایف مشاغل کلیدی در سازمان بررسی و مشخص شود که آیا تفکیک وظایف ناسازگار بطور مناسبی انجام شده است یا خیر.
- سیاست‌ها و استانداردهای شرکت برای طراحی، مستندسازی و تحصیل سخت افزار و نرم افزار توزیع شده بین واحدهای فناوری اطلاعات مورد ارزیابی قرار گیرد.

• بررسی شود که آیا کنترل‌های جبرانی از قبیل سرپرستی و نظارت مدیریت که در صورت عدم تفکیک مناسب وظایف ناسازگار در سازمان بکار گرفته می‌شود، صرفه‌ی اقتصادی دارد یا خیر.

• مستندات سیستم‌ها بررسی شود تا نسبت به مطابقت برنامه‌های کاربردی، رویه‌ها و پایگاه‌های داده‌ی طراحی و اجرا شده با استانداردهای شرکت، اطمینان حاصل شود.

۲. محیط مرکز رایانه

حسابرسان معمولاً محیط فیزیکی مرکز رایانه را به عنوان بخشی از حسابرسی سالانه‌ی خود مورد ارزیابی قرار می‌دهند. مکان فیزیکی مرکز رایانه بطور مستقیم ریسک تخریب مربوط به فجایع طبیعی یا انسانی را تحت تأثیر قرار می‌دهد. تا حد امکان مرکز رایانه باید از خطرات انسانی و طبیعی از قبیل ماشین‌آلات، مخازن سوخت و آب، فرودگاه‌ها، محیط‌های ناامن، مسیل‌ها و گسل‌ها و نیز مکان‌های عمومی سازمان دور باشد. همچنین استقرار رایانه‌ها در طبقات زیرین ساختمان نیز ریسک خسارت در اثر آب گرفتگی و سیل را افزایش می‌دهد. خطوط رفاهی (انرژی و تلفن) باید بصورت زیر زمینی باشد. پنجره‌های ساختمان باید بسته بوده و سیستم تهویه‌ی هوای مطبوعی برای جلوگیری از ورود گرد و خاک به مرکز تعبیه شده باشد.

در حالت ایده‌آل، مرکز رایانه باید در یک ساختمان مجزا، ایمن و مجهز به کنترل‌های دسترسی مستقر باشد. دسترسی به مرکز رایانه باید به اپراتورها و سایر کارکنان مرکز محدود شود. کنترل‌های فیزیکی از قبیل درب‌ها قفل شده باید به منظور محدود کردن دسترسی به مرکز تعبیه شود. همچنین دسترسی باید از طریق کلید یا کارت عبور کنترل شود و زنگ هشدار

برای مواقع اضطراری مثل آتش‌سوزی نیز تعبیه شده باشد. به منظور ایمنی بالاتر مرکز، باید کنترل‌هایی از نوع دوربین مدار بسته و سیستم‌های ضبط ویدئویی در مرکز تعبیه شود. همچنین جهت دسترسی به سیستم‌های مستقر در مرکز نیز باید برای برنامه‌نویسان و تحلیل‌گران گذر واژه‌های مخصوص استفاده شود. بعلاوه، باید تمامی ورود و خروج‌ها به مرکز رایانه بطور مطمئنی ثبت و ضبط شود.

بعلاوه، واحد فناوری اطلاعات باید از برنامه‌ی تحمل شرکت بهره‌مند باشد. تحمل شکست به توانایی سیستم به تداوم فعالیت در زمانی رخداد نواقص سخت افزاری، نرم افزاری و اشتباهات انسانی اشاره دارد. حسابرسان با اجرای کنترل توان تحمل شکست، اطمینان حاصل می‌شود که هیچ‌گونه احتمالی برای شکست سیستم وجود نخواهد داشت. دو مثال از فن‌آوری‌های توان تحمل شکست در ادامه آورده شده است.

۱. لوح‌های فشرده‌ی مستقل حاوی داده‌های همسان[۶]. در این فن‌آوری، لوح‌های فشرده‌ای حاوی داده‌ها و برنامه‌های کاربردی همسان، نگهداری می‌شوند و چنانچه یکی از لوح‌های فشرده با منگاره مواجه شد، بطور خودکار از داده‌های ذخیره شده در لوح‌های فشرده‌ی دیگر استفاده می‌شود.

۲. تأمین نیروی پیوسته. استفاده از انرژی الکتریسیته، به سبب منگارهات بسیاری از قبیل قطعی و نوسانات ممکن است عملیات مرکز رایانه را مختل نماید. تجهیزاتی که به منظور کنترل این منگارهات بکار گرفته می‌شود عبارتند از تنظیم‌کننده‌ی شدت جریان، محافظ‌های نوسانات نیرو، مولدهای نیرو و باتری‌های پشتیبان. در صورتی که جریان نیرو دچار اختلال شود، این تجهیزات برای مدتی عملیات سیستم را پشتیبانی خواهند کرد. در این شرایط، این امکان فراهم خواهد شد که سیستم رایانه‌ای بطور مناسب خاموش شود و از تخریب داده‌های سیستم جلوگیری بعمل آید.

حسابرسی محیط مرکز رایانه

هدف حسابرسی در کسب شناخت از محیط مرکز رایانه، ارزیابی کنترل‌های مربوط به ایمنی مرکز است. بطور خاص، حسابرس باید مورد زیر را ارزیابی نماید:

• کفایت کنترل‌های ایمنی فیزیکی، بطوریکه سیستم‌های سازمان را در برابر تهدیدهای فیزیکی محافظت شود.

• کفایت پوشش بیمه‌ای تجهیزات سازمان، بطوریکه برای جبران هر گونه خسارت یا تخریب مرکز رایانه مناسب باشد.

آزمون‌های حسابرسی برای ارزیابی کنترل‌های مرکز رایانه به شرح زیر می‌باشند:

آزمون‌های فیزیکی ساختمان. حسابرس باید برنامه‌های طراحی ساختمان مرکز رایانه را از لحاظ بکارگیری مواد ضد آتش بررسی نماید. همچنین کف ساختمان باید به اندازه‌ی کافی بالا برده شده باشد تا جریان آب ناشی از وسائل مهار آتش یا سایر حوادث به مرکز آسیبی وارد ننماید. بعلاوه، حسابرس باید مکان فیزیکی استقرار مرکز رایانه را نیز ارزیابی نماید. مرکز باید در مکانی استقرار یافته باشد که احتمال هرگونه خسارت ناشی از هرگونه تهدیدی از قبیل آتش‌سوزی، آشوب‌های اجتماعی و سایر موارد در حداقل ممکن باشد.

آزمون‌های سیستم شناسایی آتش‌سوزی. حسابرس باید اطمینان حاصل نماید که تجهیزات شناسایی و مهار آتش، هم بصورت دستی و هم بصورت خودکار در محل مناسب خود مستقر بوده و بطور منظم ارزیابی

می‌شود. سیستم شناسایی آتش باید هرگونه دود، حرارت و بخار را تشخیص دهند. شواهد حسابرسی می‌تواند بوسیله‌ی بررسی سوابق رسمی مربوط به تجهیزات آتش‌نشانی موجود در مرکز رایانه جمع‌آوری شود.

آزمون‌های کنترل دسترسی. حسابرس باید نسبت به محدود شدن دسترسی‌ها به مرکز رایانه به افراد مجاز اطمینان حاصل نماید. در این راستا حسابرس به ارزیابی مستندات تفصیلی مربوط به وارد شوندگان به مرکز (برنامه‌نویسان یا سایرین) می‌پردازد. مواردی از قبیل زمان‌های ورود و خروج، هدف و تناوب دسترسی می‌تواند از طریق بررسی سوابق مورد ارزیابی قرار گیرد. به منظور اطمینان نسبت به صحت سوابق، حسابرس می‌تواند از طریق مشاهده یا دوربین‌های مدار بسته، کنترل‌های دسترسی را مورد ارزیابی قرار دهد.

آزمون‌های لوح‌های فشرده‌ی حاوی داده‌های یکسان. اکثر سیستم‌هایی که از فناوری لوح‌های فشرده‌ی حاوی داده‌های یکسان استفاده می‌نمایند، از نقشه‌ای گرافیکی برای نشان دادن محل نگهداری لوح‌های فشرده استفاده می‌نمایند. از طریق این نقشه، حسابرسان می‌توانند به کفایت لوح‌های فشرده‌ی حاوی داده‌ی یکسان سازمان پی ببرند و سطح ریسک مربوط به آن‌ها را ارزیابی نمایند. اگر سازمانی از این فناوری استفاده ننماید، احتمال شکست کل سیستم وجود خواهد داشت. در این شرایط، حسابرس باید رویه‌های جایگزین استفاده شده توسط مدیر سیستم برای بازیابی شکست سیستم را بررسی نماید.

آزمون‌های تأمین نیروی پیوسته. مرکز رایانه باید بطور دوره‌ای تجهیزات تأمین نیروی پشتیبان مرکز و تهویه هوا را مورد بررسی قرار دهد. این بررسی‌ها از اهمیت بالایی برخوردار است و سوابق آن باید بطور رسمی ثبت و نگهداری شود. زمانی که سیستم‌های رایانهی شرکت توسعه داده می‌شود و انرژی مورد نیاز آن‌ها نیز افزایش می‌یابد، بطور مشابه، نیروی پشتیبان مرکز هم باید ارتقا داده شود. در غیر اینصورت، سازمان ممکن است زمانی به عدم کفایت نیروی پشتیبان پی ببرد که بسیار دیر شده است.

آزمون‌های پوشش بیمه‌ای. حسابرس باید بطور سالانه، پوشش بیمه‌ای سخت افزار، نرم افزار و تجهیزات فیزیکی مربوطه را بررسی نمایند. حسابرس باید اطمینان حاصل کندکه تمامی تجهیزات جدیدی که خریداری شده است، بطور کامل و صحیح ثبت و ضبط شده و تمامی تجهیزاتی که کنار گذاشته شده نیز در سوابق لحاظ شده است. سیاست‌های بیمه‌ای سازمان، منعکس‌کننده‌ی نیازهای مدیریت برای میزان پوشش مناسب است. برای مثال، در یک سازمان ممکن است میزان پوشش بیمه در سطح حداقل ممکن باشد؛ در حالیکه در سازمانی دیگر، تمامی امکانات بطور کامل بیمه شده باشد.

۳. برنامه‌ریزی بازیابی فجایع

فجایعی از قبیل حوادث طبیعی، انسان‌ساز و شکست سیستم می‌تواند مرکز رایانه و سیستم‌های اطلاعاتی سازمان را با بحران مواجه سازد. فجایع طبیعی از قبیل طوفان، سیل و زلزله نسبت به دو دسته‌ی دیگر محتمل‌تر هستند؛ چرا که هر سازمانی را در هر منطقه‌ی جغرافیایی ممکن است تحت تأثیر قرار دهد. فجایع انسانی از قبیل اقدامات خرابکارانه یا اشتباهات، فقط سازمانی خاص را فرا می‌گیرد و قلمرو محدودی را تحت تأثیر قرار می‌دهد. شکست‌های سیستم از قبیل قطع نیرو یا خراب شدن حافظه‌ی رایانه بطور معمول از شدت کمتری برخوردارند، اما وقوع آن‌ها بسیار محتمل است. تمامی این فجایع می‌تواند سازمان را از امکانات پردازش داده‌ی خود محروم، فعالیت‌های مبتنی بر رایانه شرکت را مختل و سازمان را از ارائه کالا یا خدمات خود ناتوان نماید. هر چقدر وابستگی سازمان به فناوری مبتنی بر رایانه بیش‌تر باشد، ریسک رخ دادن چنین فجایعی نیز افزایش می‌یابد. برای برخی از شرکت‌ها از قبیل آمازون[۷] یا ای‌بای[۸]، از دست دادن سیستم رایانه‌ای حتی برای اندکی زمان، مصیبت‌بار خواهد بود.

فجایعی که پیش از این به آن‌ها اشاره شد، معمولاً قابل پیش‌گیری یا جلوگیری نیستند. بقای شرکت قربانی به چگونگی و سرعت واکنش به آن‌ها بستگی دارد. بنابراین، با استفاده از برنامه‌ریزی می‌توان فاجعه را مهار کرده و شرایط سازمان را به حالت عادی برگرداند. سازمان‌ها در برابر این قبیل حوادث از برنامه‌ی بازیابی فجایع[۹] استفاده می‌نمایند. این برنامه دربرگیرنده‌ی بیانیه‌ای فراگیر از تمامی اقداماتی است که در زمان‌های قبل، بعد و در حین رخداد هرگونه فاجعه‌ای در سازمان باید انجام گیرد. گرچه جزئیات هر برنامه بر حسب نیاز سازمان، منحصر به فرد است، اما تمامی آنان معمولاً دارای چهار ویژگی هستند:

۱. شناسایی برنامه‌های کاربردی حیاتی

۲. ایجاد تیم بازیابی فاجعه

۳. ایجاد مکانی برای پشتیبان‌گیری اطلاعات

۴. رویه‌های پشتیبان‌گیری و بایگانی در خارج از سازمان

باقیمانده‌ی این بخش به عناصر اساسی برنامه‌ی بازیابی فجایع اثربخش اختصاص داده شده است.

شناســـایی برنامه‌های کاربردی حیاتی

نخســـتین عنصر اساســـی برنامه‌ی بازیابـــی فجایع، شناســـایی برنامه‌های کاربـــردی و پرونده‌های داده‌ی حیاتی ســـازمان اســـت. در اقدامات بازیابی، باید بر بازیابـــی آن قبیل از برنامه‌های کاربردی تأکید شـــود کـــه برای بقای کوتاه مدت ســـازمان حیاتی می‌باشد. مســـلماً در بلنـــد مدت بایـــد تمامی برنامه‌های کاربردی سازمان به وضعیت پیـــش از فاجعه بر گردانده شـــود. اما برنامه‌ی بازیابی فجایع، ســـندی کوتاه مدت اســـت، بطوریکه نباید به گونه‌ای باشـــد که تمامی امکانات سازمان را در کوتاه‌ترین زمـــان ممکن بازیابی نماید. اگر برنامه به این گونه طراحی شـــود، منابع ســـازمان صرف امور غیر حیاتی خواهد شـــد و فرآیند بازیابی با تأخیر مواجـــه می‌شـــود. بنابرایـــن برنامه‌ی مذکور باید بر بقای کوتاه مدت سازمان تأکید داشته باشد؛ بطوریکه بر هرگونه شرایط بحرانی چیره شود.

بـــرای اکثر ســـازمان‌ها، بقای کوتاه مدت آن‌ها در گرو اقداماتی اســـت که به جریـــان وجه‌نقد کافی برای برآورده کـــردن تعهـــدات کوتاه مـــدت منتج می‌شـــود. برنامه‌های کاربردی رایانه‌ای که بطـــور مســـتقیم از وظایفی مانند فـــروش و ارائه خدمات به مشـــتریان، برآورده کردن تعهدات قانونی، نگهداری و جمـــع‌آوری حســـاب‌های دریافتنی، تصمیمـــات تولیـــد و توزیع،اقدامـــات خرید، پرداخت‌های نقدی (حساب‌های تجاری، و حقوق و دستمزد) پشتیبانی می‌نمایـــد، بـــرای ســـازمان حیاتـــی می‌باشند. بنابراین، آن‌ها باید شناسایی شـــده و در برنامه‌ی بازیابی در اولویت قرار داده شـــود. وظیفه‌ی شناســـایی موارد حیاتی و اولویت‌بندی برنامه‌های کاربـــردی مســـتلزم مشـــارکت فعال کاربران بخش‌های مختلف ســـازمان از جمله حســـابداران و حســـابرس است.

اما اغلب، به این وظیفه بطور نادرســـت نگریسته شده و به عنوان یک مسئله‌ی رایانهی فنـــی، در حیطه‌ی متخصصان فناوری اطلاعات قلمداد می‌شود. گرچه مشارکت متخصصان فناوری اطلاعات در این راســـتا ضروری خواهد بود، اما برنامه‌ی بازیابی فجایع تصمیمی است که بایـــد تمامی افراد ســـازمان در آن مشارکت داشته باشند تا به نحو بهتری مســـائل واحد تجاری مـــورد تجزیه و تحلیل قرار گیرد.

ایجاد تیم بازیابی فاجعه

بازیابی سازمان از بحران، به اقدامی صحیـــح و به هنگام بســـتگی دارد. هر گونـــه تأخیـــری در اجـــرای اقدامات حیاتی به طولانی شدن دوره‌ی بازیابی و کاهش احتمال بازیابی موفقیت‌آمیز منجر می‌شـــود. به منظور جلوگیری از هر گونه غفلت یا دوباره‌کاری در خلال اجرای برنامه، مســـئولیت کارکنان در جریـــان رخداد هر گونـــه بحرانی، باید از قبل بطور کاملاً شـــفاف تعریف و به آن‌ها منتقل شـــده باشـــد. در پی یک فاجعـــه، اعضای تیم، مســـئولیت خود را در قالـــب مســـئولیت‌های فرعی به زیرمجموعه‌های خود واگذار می‌نمایند. قابل ذکر است که در این سازمان‌دهی به نگرانی‌های کنترلی مرسوم توجهی صورت نمی‌گیرد. در شـــرایطی که در پس یک فاجعه ایجاد می‌شـــود ممکن اســـت نادیـــده گرفتن برخـــی اصول کنترلـــی از قبیـــل تفکیـــک وظایف، کنترل‌های دسترســـی و سرپرستی را الزامی نماید.

ایجاد مکانی برای پشتیبان‌گیری

برنامـــه‌ی بازیابـــی فاجعـــه ایجاب می‌نماید که امکانـــات پردازش داده‌ی مســـتقلی، پس از یک فاجعـــه به کار گرفته شود. در میان گزینه‌ها موجود، معمول‌ترین گزینه‌ها عبارتند از پیمان هدف مشـــترک، ســـاختمان خالی یا مکان ســـرد، مرکز عملیـــات بازیابی یا مکان گرم، و پشـــتیبان فراهم شده‌ی داخلی.

پیمان هدف مشترک، قراردادی بین دو یا چند ســـازمان (بـــا امکانات رایانه‌ای همســـان) اســـت که با هدف پشتیبانی از پردازش داده‌ی یکدیگر در مواقع بحران منعقد می‌شود. در صورت رخ داد یک فاجعه، شرکت میزبان باید برنامه‌ی پـــردازش داده‌ی معمول خود را متوقف ســـازد و به پردازش مبادلات حیاتی سازمان آســـیب دیده از فاجعه بپردازد. در این شـــرایط، رایانه میزبان

با حالت وضعیت اضطراری فعالیت می‌کند و با قطع پردازش برنامه‌های کاربردی با اولویت پایین، منابع فناوری اطلاعات را در اختیار امور حیاتی قرار می‌دهد. آنچه باعث روی آوردن سازمان‌ها به این قراردادهای متقابل می‌شود، اقتصادی بودن آن می‌باشد؛ بطوریکه این تدبیر، تقریباً برای طرفین بدون هزینه خواهد بود.

ساختمان خالی یا مکان سرد

برنامه‌ای است که بر اساس آن شرکت ساختمانی را خریداری یا اجاره می‌نماید تا به عنوان یک مرکز داده مورد استفاده قرار گیرد. در صورت رخداد یک فاجعه، این مرکز در دسترس بوده و آماده ارائه خدمات فناوری اطلاعات و برآورده کردن نیازهای موقتی کاربران تا راه‌اندازی سیستم‌های حیاتی خواهد بود.

مرکز عملیات بازیابی یا مکان گرم، مرکزی برای پشتیبانی از داده‌ها و امکانات رایانه‌ای بسیاری از شرکت‌ها می‌باشد. این مرکز امکانات سخت افزاری و پشتیبان‌گیری را در قالب خدمات فنی به مشتریان خود در قبال پرداخت حق اشتراک سالانه‌ی ارائه می‌دهد. در صورت رخداد فاجعه‌ای، مشترکان قادر خواهند بود تا در کمترین زمان ممکن، سیستم‌های حیاتی خود را بازیابی نمایند.

پشتیبان فراهم شده‌ی داخلی. سازمان‌های بزرگ‌تر، با چندین مرکز پردازش داده، اغلب ترجیح می‌دهند که برای اطمینان خاطر خود، ظرفیت مازاد داخلی ایجاد نمایند. این امر، به شرکت‌ها این امکان را می‌دهد که به توسعه‌ی تشکیلات سخت افزاری و نرم افزاری استاندارد بپردازند که با مراکز پردازش داده، سازگار باشند و منگارهات پس از رخداد یک فاجعه را به حداقل ممکن برساند.

رویه‌های پشتیبان‌گیری و ذخیره‌ی برون سازمانی

تمامی پرونده‌های داده، برنامه‌های کاربردی، مستندسازی و سایر منابع اطلاعاتی و رایانه‌ای مورد نیاز امور حیاتی سازمان، باید بطور خودکار پشتیبان‌گیری شده و در یک مکان ایمن خارج از سازمان نگهداری می‌شود. کارکنان پردازش داده باید بطور معمول پشتیبان‌گیری را انجام داده و رویه‌ها را ذخیره نمایند تا این منابع حیاتی را مورد حفاظت و نگهداری قرار دهند. اگر شرکت از مکان سرد یا روش دیگر پشتیبان‌گیری استفاده نماید که دارای سیستم عامل سازگار نمی‌باشد، رویه‌های لازم جهت دریافت نسخه‌ی جاری آن سیستم عامل را باید دنبال نماید. برنامه‌ی بازیابی فاجعه باید شامل رویه‌هایی برای تهیه‌ی رونوشت از نسخه‌های جاری برنامه‌های کاربردی باشد. در پایگاه داده‌ی پشتیبان، تمامی داده‌های مربوط به فعالیت جاری شرکت ثبت و ضبط می‌شود. اما تمامی سازمان‌ها مایل یا قادر به ایجاد چنین تشکیلات پشتیبانی نیستند. اما به عنوان یک حداقل، باید بطور روزانه از پایگاه‌های داده رونوشت تهیه شده و در ابزارهای با ظرفیت و سرعت بالا مانند انواع لوح‌های فشرده و مکانی ایمن در خارج از سازمان ذخیره شود.

حسابرسی برنامه‌ی بازیابی فجایع

حسابرس باید کفایت و توانایی برنامه‌ی بازیابی فاجعه‌ی مدیریت در مقابله با فجایعی که می‌تواند منابع رایانه‌ای سازمان را از بین ببرد، مورد ارزیابی قرار دهد. در ارزیابی برنامه‌ی بازیابی فاجعه‌ی مدیریت، آزمون‌های زیر می‌توان صورت گیرد:

پشتیبان‌گیری. حسابرس باید کفایت برنامه‌ریزی سازمان برای پشتیبان‌گیری را مورد ارزیابی قرار دهد. ناسازگاری سیستم و دستی بودن فرآیندها، اثربخشی پشتیبان‌گیری را کاهش می‌دهد. در مورد روش‌های ساختمان خالی و مرکز عملیات بازیابی، بنابراین حسابرس باید وجود قراردادهای معتبری را ارزیابی نماید که طی آن‌ها فروشندگان سخت افزار، تأمین نیازهای سخت افزاری سازمان را در کوتاه‌ترین زمان بعد از فاجعه را تضمین کرده‌اند. اگر شرکت عضو یک مرکز عملیات بازیابی باشد، حسابرس باید نسبت به تعداد اعضای مرکز و پراکندگی جغرافیایی آن‌ها هوشیار باشد. یک فاجعه‌ی فراگیر ممکن است

تقاضایی را برای مرکز عملیات بازیابی ایجاد نماید که از توان آن خارج باشد.

فهرست برنامه‌های کاربردی حیاتی. حسابرس باید اطمینان حاصل نماید که فهرست برنامه‌های کاربردی حیاتی سازمان تکمیل شده است. از قلم افتادن برنامه‌های حیاتی از فهرست، می‌تواند عملیات بازیابی را با شکست مواجه سازد. این امر در مورد برنامه‌های کاربردی غیرضروری نیز صادق است. اگر فهرست برنامه‌های حیاتی حاوی برنامه‌هایی باشد که برای بقای کوتاه مدت شرکت ضروری نیست، این امر می‌تواند به منحرف کردن منابع سازمان از موارد با اهمیت و جلب توجه به سوی مسائل فرعی شود.

پشتیبان‌گیری نرم افزار. حسابرس باید نسبت به رونوشت‌های برنامه‌های کاربردی حیاتی و سیستم عامل‌ها، و ذخیره آن‌ها در خارج از سازمان اطمینان حاصل نماید. حسابرس باید همچنین همسان بودن شماره‌ی نسخه‌های نرم افزاری ذخیره شده و نرم افزارهای مورد استفاده را ارزیابی نمایند.

پشتیبان‌گیری داده. حسابرس باید نسبت به پشتیبان‌گیری پرونده‌های داده‌های حیاتی، مطابق با برنامه‌ی بازیابی فاجعه اطمینان حاصل نماید.

تدارکات، مستندات و مستندسازی پشتیبان‌گیری. مستندسازی سیستم، تدارکات و مستندات مرجع مورد نیاز برای پردازش مبادلات حیاتی باید پشتیبان‌گیری شده و در مکانی خارج از سازمان نگهداری شود. حسابرس باید نوع و کمیت مستندات لحاظ شده در برنامه‌ی بازیابی فاجعه از قبیل اوراق بهادار، موجودی‌ها، سفارشات خرید و هر گونه فرم خاص دیگر را ارزیابی نمایند.

تیم بازیابی فاجعه. برنامه‌ی بازیابی فاجعه باید بطور واضح اسامی، آدرس، و شماره تلفن ضروری اعضای تیم بازیابی فاجعه را فهرست نماید. حسابرس باید نسبت به آگاهی اعضای تیم به مسئولیت خود اطمینان حاصل نماید.

خلاصه

در این مطالعه، به معرفی راهبری فناوری اطلاعات و عناصر کنترل‌های داخلی مدنظر قانون ساربینز-آکسلی شامل ساختار سازمانی واحد فناوری اطلاعات، محیط مرکز رایانه و برنامه‌ریزی بازیابی فجایع پرداخته شد. در این راستا بیان شد که واحد فناوری اطلاعات می‌تواند به دو مدل متمرکز و غیرمتمرکز در سازمان‌ها استقرار یابد و سپس به ریسک‌ها هر یک از مدل‌ها و رویه‌های حسابرسی مورد نیاز در هر یک از ساختارهای سازمانی بیان شد. در بخش محیط مرکز رایانه به مواردی بررسی شد که باید از لحاظ شرایط فیزیکی و ریسک‌های کنترلی مورد توجه حسابرسان قرار گیرد. سپس، رویه‌های حسابرسی لازم به منظور کسب اطمینان از کفایت کنترل‌های ایمنی فیزیکی و جبران خسارت معرفی شدند. در بخش پایانی، ضرورت برنامه‌ریزی بازیابی فجایع و ویژگی‌های کلیدی آن شامل شناسایی برنامه‌های کاربردی حیاتی، ایجاد تیم بازیابی فاجعه، ایجاد مکانی برای پشتیبان‌گیری اطلاعات، و رویه‌های پشتیبان‌گیری و بایگانی در خارج از سازمان ارائه گردید و سپس به موارد مدنظر حسابرسان در فرآیند ارزیابی برنامه‌ی بازیابی فجایع پرداخته شد. ■

منابع

این مقاله ترجمه‌ی آزادی از کتاب زیر، و همچنین استفاده از منابع بعدی است.

James, H. A. (2011). Information Technology Auditing and Assurance. Mason, Ohio: South-Western Cengage Learning.

رامنی، م. ب.، و استین بارت، پ. ج. (۱۳۹۰). سیستم های اطلاعاتی حسابداری (نسخه ۳، جلد ۱). (س. سجادی، مترجم) اهواز: دانشگاه شهید چمران.

Bell, T. B., Marrs, F. O., Solomon, I., & Thomas, H. (1997). Auditing Organizations Through a Strategic- Systems Lens. Swiss association: KPMG LLP.

The Institute of Internal Auditors. (2012). Global Technology Audit Guide (GTAG) 17 Auditing IT Governance. The Institute of Internal Auditors.

پی‌نویس‌ها:

1.Information Technology (IT) Governance
2.Off-Line
3.Database Administrator (DBA)
4.Data Base Management System
5.Distributed Data Processing (DDP)
6.Redundant Arrays of Independent Disks (RAID)
7.Amazon.com
8.eBay
9.Disaster Recovery Plan (DRP)