ساختار حسابرسی فناوری اطلاعات

محمد جندقی قمی
دانشجوی دوره دکترای حسابداری
دانشگاه تهران

مقدمه

فناوری اطلاعات و ارتباطات به یکی از چالشی‌ترین مباحث دهه‌های اخیر سازمان‌های تبدیل شده است. ابزاری خارق‌العاده که قدرت و سرعتی سرسام‌آور به پردازش و جریان اطلاعات سازمان‌ها می‌بخشد. نیازهای نو ظهور در عرصه بازارهای رقابتی، واحدهای تجاری را به سوی توسعه و بکارگیری هر چه بیشتر سامانه‌های فناوری اطلاعات تشویق می‌نماید. بدیهی است که واحد فناوری اطلاعات در سازمان‌های امروزی نقشی راهبردی در دستیابی به اهداف کسب و کار پیدا کرده است. اما باید توجه داشت به همان اندازه که قدرت و سرعت فناوری اطلاعات می‌تواند در راستای دستیابی به اهداف و مأموریت‌ها کاربرد داشته باشد؛ به همان اندازه نیز می‌تواند تبعاتی غیر قابل جبران برای سازمان به بار آورد. نیاز به بکارگیری ساز و کارهای نظارتی و کنترلی اثربخش برای اطمینان به حصول به اهداف و مأموریت‌ها در زمینه فناوری اطلاعات به ضرورتی اجتناب‌ناپذیر در سازمان‌های امروزی تبدیل شده است (سادوسکای و همکاران ۱۳۸۴).

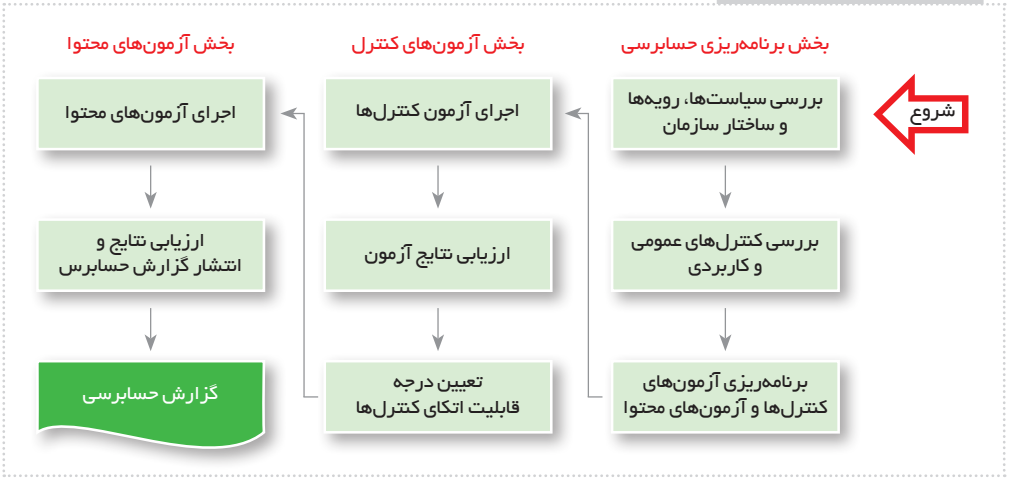
مسائل مربوط به ایمنی تشکیلات فناوری اطلاعات و کنترل‌های مربوط به آن، بیش از پیش مدیران و ذینفعان سازمان‌ها را نگران کرده است. حسابرسی فناوری اطلاعات، ابزاری حیاتی برای حل نگرانی‌های امروز سازمان‌ها در زمینه فناوری اطلاعات محسوب می‌شود. هدف از حسابرسی فناوری اطلاعات، کسب اطمینان نسبت به اثربخشی سیاست‌های سازمان در زمینه مدیریت ریسک، کنترل و راهبری واحد فناوری اطلاعات است (فخار، ۱۳۸۹). در این مقاله، چشم‌اندازی کلی از ساختار حسابرسی فناوری اطلاعات ارائه می‌گردد.

فرآیند حسابرسی

اظهارنظر حسابرس، انتهای فرآیند سیستماتیک حسابرسی صورت‌های مالی است که دربرگیرنده سه مفهوم برنامه‌ریزی حسابرسی، آزمون کنترل‌ها و آزمون‌های محتوا است. شکل ۱، گام‌های مربوط به این مفاهیم را به تصویر می‌کشد. پیدایش فناوری اطلاعات، بی‌تردید، از مهم‌ترین و اساسی‌ترین عوامل پیشرفت و تحول در زندگی بشر بوده است. فناوری اطلاعات با قدرت و سرعت بی‌نظیر خود، بهره‌وری فرآیندهای سازمانی را ارتقا می‌دهد. اما در کنار فواید خود، احتمال سوء استفاده از منابع سازمان را نیز افزایش می‌دهد. فناوری اطلاعات را می‌توان با عنوان بکارگیری رایانه و امکانات مربوط به آن در انجام امور سازمانی تعریف کرد (فخار، ۱۳۸۹).

حسابرسی فناوری اطلاعات بر جنبه‌های مبتنی بر کامپیوتر و سیستم اطلاعاتی سازمان تاکید دارد و سیستم‌های امروزی از درجات بالایی از فناوری برخوردار هستند. به عنوان نمونه، پردازش معاملات بطور خودکار و بوسیله برنامه‌های کامپیوتری انجام می‌شود. بطور مشابه اسناد، دفاتر روزنامه و دفاتر کل که سابق فیزیکی بودند، اکنون الکترونیکی هستند و در پایگاه‌های

شکل ۱ : حسابرسی فناوری اطلاعات



داده نگـه‌داری می‌شـوند. همان‌طـور کـه در ادامـه خواهیـم دیـد، کنترل‌هـای حاکـم بـر ایـن فرآیندهـا و پایگاه‌هـای داده، بـه مباحثی اصلـی در فرآینـد حسابرسـی مالـی تبدیل شـده اسـت.

برنامه‌ریزی حسابرسی

گام نخسـت حسابرسـی فنـاوری اطلاعات، برنامه‌ریزی حسابرسـی اسـت. پیـش از اینکـه حسـابرس بتواند ماهیـت و میـزان آزمون‌های خود را تعیین کند، باید نسـبت به کسـب و کار مشـتری به شـناختی کامل دسـت یابد. (شـکل ۱)

عنصـر کلیـدی این بخـش از حسابرسـی، تجزیه و تحلیل ریسـک حسابرسـی اسـت. هـدف حسـابرس، جمع‌آوری اطلاعـات کافی پیرامـون شـرکت به منظـور برنامه‌ریزی سـایر بخش‌های حسابرسـی اسـت. در تجزیه و تحلیل ریسـک، بررسـی کلی از کنترل‌های داخلی سـازمان بـه عمـل می‌آیـد. در خـلال بررسـی کنترل‌هـا، حسـابرس تـلاش می‌کنـد کـه بـه شـناختی از سیاسـت‌ها، رویه‌هـا و سـاختار سـازمان دسـت یابد. حسـابرس، در این بخش، از حسـابرس همچنین کاربردهـای بـا اهمیـت مالـی کنترل‌هـا را شناسـایی نمایـد و بـه شـناختی نسـبت بـه کنترل‌های حاکم بـر مبادلات اصلی دسـت یابد کـه بوسـیله ایـن کنترل‌هـا ارزیابی می‌شـوند.

فنـون جمع‌آوری شـواهد در ایـن بخـش از حسابرسـی شـامل پرسشـنامه، مصاحبـه بـا مدیریـت، بررسـی مسـتندات سیسـتم و مشـاهده فعالیت‌هـا اسـت. در خـلال ایـن فرآینـد، حسـابرس فنـاوری اطلاعـات، بایـد مسـائل اصلـی و کنترل‌هـای مربـوط بـه آن‌هـا را شناسـایی نمایـد. پـس از انجـام ایـن مرحلـه، حسـابرس به بخـش بعـدی، یعنـی آزمـون کنترل‌هـا بـرای تعییـن مطابقـت آن با اسـتانداردهای مصـوب می‌پـردازد.

آزمون‌های کنترل‌ها

هـدف از بخـش آزمون‌هـای کنترل‌هـا، تعییـن ایـن اسـت کـه آیا کنترل‌هـای داخلـی کافـی ایجـاد شـده و بخوبـی عمـل می‌کنـد. در ایـن راسـتا، حسـابرس آزمون‌های کنتـرل مختلفی را انجـام می‌دهد. فنـون جمـع‌آوری شـواهد اسـتفاده شـده در ایـن بخـش، می‌توانـد شـامل هم فنون دسـتی و هم فنون تخصصی حسابرسـی کامپیوتری باشـد. سـپس حسـابرس باید به ارزیابـی کنترل‌های داخلـی از طریق ارزیابی ریسـک کنتـرل بپردازد. سـطح اطمینانی که حسـابرس برای کنترل‌هـای داخلـی در نظـر می‌گیـرد، می‌توانـد ماهیـت و میـزان آزمون‌هـای محتـوای مـورد نیـاز را تحـت تأثیر قـرار دهد.

آزمون محتوا [۱]

بخـش سـوم فرآینـد حسابرسـی، مربـوط بـه داده‌هـای مالـی اسـت. ایـن بخـش شـامل رسـیدگی تفصیلـی به مانـده حسـاب‌ها و معامـلات خـاص از طریـق آزمون‌هـای محتوا اسـت. به عنـوان نمونه، تأییدیـه مشـتری، یـک آزمون محتوا اسـت کـه بمنظور تأییـد مانده یـک حسـاب بـکار گرفتـه می‌شـود. حسـابرس، نمونـه‌ای از مانـده حسـاب‌های دریافتنـی را انتخـاب و آنـان را به منابع آن –مشـتریان– رهگیـری می‌کننـد تا مشـخص نماید که آیـا مبالغ ذکر شـده به یک مشـتری واجد شـرایط تعلـق دارد. از ایـن طریق، حسـابرس می‌تواند صحـت هـر مانـده موجـود در نمونـه را تأییـد نمایـد. حسـابرس بـر اسـاس یافته‌هـای حاصـل از نمونـه، می‌توانـد پیرامون مطلـوب بودن مبالـغ حسـاب‌های دریافتنـی، نتیجه‌گیـری نمایـد.

برخـی از آزمون‌هـای محتـوا، از قبیل شـمارش وجه‌نقد، شـمارش موجـودی کالای انبـار، و تأییـد وجـود گواهی‌هـای سـهام موجود در گاو صنـدوق فیزیکـی و مبتنـی بـر فعالیت‌هـای دسـتی اسـت؛ در محیـط فنـاوری اطلاعـات، داده‌هـا (از قبیـل مانـده حسـاب‌ها، نـام و آدرس مشـتریان) بـا اسـتفاده از آزمون‌هـای محتوا مـورد ارزیابی قرار می‌گیرنـد و در ایـن راسـتا، اغلـب از ابزارهـای حسابرسـی مبتنـی بر کامپیوتـر و فنـون نـرم افـزاری [۲] اسـتفاده می‌گردد.

سیستم کنترل داخلی

مدیریـت سـازمان بر اسـاس الزامـات قانونی باید نسـبت بـه ایجاد و نگهـداری سیسـتم کنتـرل داخلـی مناسـب اقـدام نمایـد. در ایـن راسـتا، کمیسـیون بـورس و اوراق بهـادار ایالات متحـده بیان می‌کند: «ایجـاد و نگهـداری سیسـتم کنتـرل داخلـی، از تعهـدات بـا اهمیت مدیریت اسـت. یک جنبه بنیادی از مسـئولیت پاسـخگویی مدیریت، ارائـه اطمینـان معقـول به سـهامداران نسـبت بـه وجـود کنترل‌های داخلـی مطلـوب در سـازمان اسـت. بعـلاوه، مدیریت مسـئولیت دارد

تـا اطلاعـات مالـی قابـل اتکایی بـرای ارائه به موقـع به سـهامداران و سـرمایه‌گذاران بالقـوه تهیـه نماید».

بـه سـبب اینکـه بخـش وسـیعی از سیسـتم کنتـرل داخلـی بطـور مسـتقیم بـا پـردازش معامـلات در ارتباط اسـت، حسـابداران، مشـارکت‌کنندگان کلیـدی در کسـب اطمینـان نسـبت بـه وجـود کنترل‌هـای کافـی هس‌تـند. در ایـن بخـش، بـه مـروری کلـی بـر مفاهیـم کنتـرل داخلـی پرداختـه می‌شـود. در پایـان نیـز، چارچوب کنترلـی کـوزو ارائـه می‌شـود.

اهداف کنترل داخلی، اصول و مدل‌ها

سیسـتم کنتـرل داخلـی سـازمان شـامل سیاسـت‌ها، روش‌هـا و رویه‌هایـی بـه منظـور دسـتیابی بـه ایـن چهار هدف اساسـی اسـت:

۱. حفاظت از دارایی‌های شرکت.

۲. اطمینـان نسـبت به صحـت و قابلیت اتکای سـوابق و اطلاعات حسابداری.

۳. اثربخشی عملیات شرکت.

۴. اندازه‌گیـری میـزان رعایـت سیاسـت‌ها و رویه‌هـای ارائـه شـده از سـوی مدیریت[۳].

اصول تعدیل‌کننده

اسـاس اهـداف کنترلی ارائه شـده، چهـار اصل تعدیل‌کننده اسـت کـه طراحان و حسابرسـان سیسـتم‌های کنتـرل داخلـی را راهنمایی می‌نماید:

■ **مسـئولیت مدیریـت:** ایـن مفهـوم بیـان مـی‌دارد کـه ایجاد و نگهـداری سیسـتم کنتـرل داخلـی از وظایـف مدیریـت اسـت. قانون سـاربینز- آکسـلی، بـه ایـن امـر وجهـه قانونی می‌بخشـد.

■ **روش‌هـای پـردازش داده‌هـا:** سیسـتم کنتـرل داخلـی، صرف‌نظر از روش پردازش داده اسـتفاده شـده (دستی و کامپیوتری)، بایـد چهـار هـدف اساسـی خـود را بـرآورده سـازد. امـا فنـون مـورد اسـتفاده بـه منظـور دسـتیابی به ایـن اهـداف، از لحاظ نـوع فناوری، بسـیار متنـوع خواهـد بود.

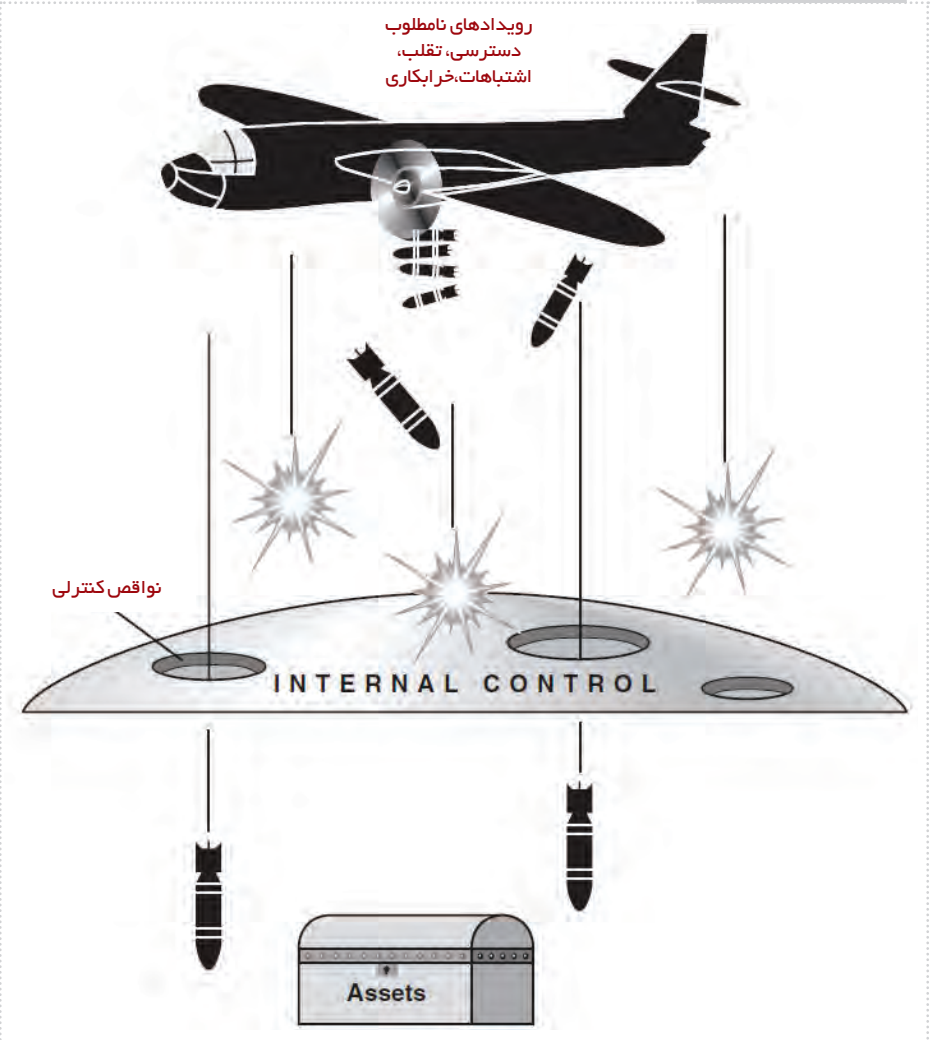
■ **محدودیت‌هـا:** هر سیسـتم کنتـرل داخلی، پیرامون اثربخشـی خـود بـا محدودیت‌هایی مواجه اسـت. ایـن مـوارد عبارتند از:

۱) احتمال اشتباه: هیچ سیستمی کامل نیست،

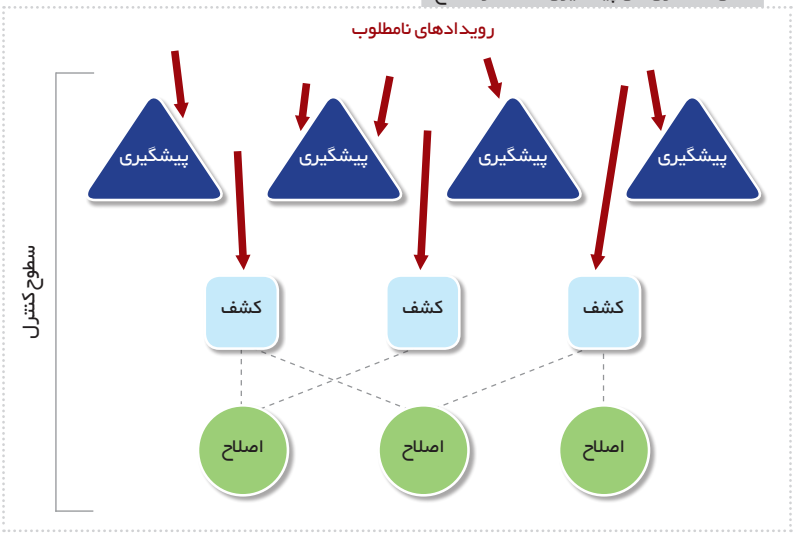
۲) دور زدن: کارکنـان ممکـن اسـت سیسـتم را از طریـق تبانی یا موارد دیگـر دور بزنند،

۳) زیـر پـا گذاشـتن کنترل‌هـا توسـط مدیریـت: مدیریـت در

شکل۲: سپر کنترل داخلی



شکل۳: کنترل‌های پیشگیری، کشف، و اصلاح



موقعیتی قرار دارد که می‌تواند شخصاً یا بوسیله کارکنان زیر دست خود، کنترل‌های موجود را زیر پاگذارد و

۴) شرایط در حال تغییر: شرایط می‌تواند به مرور زمان تغییر کند و کنترل‌های موجود، اثربخشی خود را از دست بدهند.

■ **اطمینان معقول:** سیستم کنترل داخلی باید اطمینان معقول ارائه نماید که چهار هدف اساسی کنترل داخلی برآورده می‌شود. اطمینان معقول به این معنی است که هزینه دستیابی به کنترل مطلوب باید کمتر از منافع آن باشد.

به منظور به تصویر کشیدن اصول محدودیت‌ها و اطمینان معقول، شکل ۲، سیستم کنترل داخلی را به عنوان سپری به تصویر می‌کشد که از دارایی‌های شرکت در برابر رویدادهای نامطلوب بسیاری حفاظت می‌نماید. که سازمان را بمباران می‌کند، این موارد عبارتند از: دستیابی غیرقانونی به دارایی‌های شرکت (شامل اطلاعات)، ارتکاب به تقلب از سوی کارکنان، اشتباه از سوی کارکنان فاقد صلاحیت، نقص برنامه‌های کامپیوتری، از بین رفتن داده‌ها، اقدامات خرابکارانه از قبیل دسترسی غیرمجاز به کامپیوتر توسط هکرها و تهدیداتی از قبیل ویروس‌های کامپیوتری است که برنامه‌ها و پایگاه‌های داده را تخریب می‌کنند.

سپر کنترل داخلی در واقع از سه سطح کنترل‌های پیشگیری، کنترل‌های کشف شده و کنترل‌های اصلاحی تشکیل شده است

عدم یا ضعف کنترل‌ها در شکل ۲ به صورت سوراخ‌ها موجود در سپر کنترلی به تصویر کشیده شده است. برخی ضعف‌ها بی‌اهمیت یا قابل تحمل هستند. بر اساس اصل اطمینان معقول، بر طرف کردن این ضعف‌های کنترلی، مقرون به صرفه نیست. اما ضعف‌های بااهمیت موجود در کنترل‌ها، ریسک زیان مالی یا صدمه دیدن شرکت به سبب وقوع رویدادهای نامطلوب را افزایش می‌دهد. منافع حاصل از بر طرف کردن این ضعف‌ها، فراتر از هزینه اصلاح آنان خواهد بود.

مدل پیشگیری، کشف و اصلاح

شکل ۳ نشان می‌دهد که سپر کنترل داخلی ارائه شده در شکل ۲ در واقع، از سه سطح کنترلی کنترل‌های پیشگیری، کنترل‌های کشف‌کننده و کنترل‌های اصلاحی تشکیل شده است: این سیستم کنترلی، «مدل کنترلی پیشگیری، کشف و اصلاح» خوانده می‌شود.

■ کنترل‌های پیشگیری

پیشگیری، نخستین خط دفاعی در ساختار کنترلی است. کنترل‌های پیشگیری، فنون غیر فعالی هستند که به منظور کاهش وقوع رویدادهای نامطلوب طراحی شده‌اند. کنترل‌های پیشگیری پیروی از فعالیت‌های توصیه شده یا مطلوب را اجباری می‌کنند و از این طریق، امکان شناسایی فعالیت‌های نامطلوب را فراهم می‌آورند. در زمان طراحی سیستم کنترل‌های داخلی، توجه به فعالیت‌های پیشگیری بسیار مثمر ثمرتر از اقدامات درمانی است. پیشگیری از اشتباه و تقلب بسیار مقرون به صرفه‌تر از کشف و اصلاح آنان پس از وقوع است. بنابراین بسیاری از رویدادهای نامطلوب در سطح نخست کنترل، متوقف می‌شوند. به عنوان نمونه، یک فرآیند ورود داده مطلوب، نمونه‌ای از کنترل پیشگیری است. طراحی منطقی چنین فرآیندی موجب می‌شود که تنها نوعی خاص از اطلاعات از قبیل نام مشتری، آدرس، اقلام فروخته شده و تعداد و در نتیجه از ورود سایر داده‌ها جلوگیری به‌عمل می‌آید.

■ کنترل‌های کشف‌کننده

کشف مسائل، دومین خط دفاعی است. کنترل‌های کشف‌کننده، ابزارها، فنون و رویه‌های طراحی شده برای شناسایی و افشای اطلاعات رویدادهای نامطلوب است که از کنترل‌های پیشگیری عبور کرده‌اند. کنترل‌های کشف‌کننده انواع خاصی از اشتباهات را بوسیله مقایسه رویدادهای اتفاق افتاده با استانداردهای از پیش تعیین شده آشکار می‌سازند. زمانی که کنترل کشف‌کننده، انحراف از یک رویه استاندارد را شناسایی کرد، با ارسال علائم

هشداردهنده، موجب جلب توجه به آن رویداد خواهد شد.

برای مثال، فرض کنید که داده‌ای در صورتحساب مشتری به اشتباه درج گردیده است:

تعداد	قیمت واحد (دلار)	کل مبلغ (دلار)
۱۰	۱۰	۱,۰۰۰

پیش از پردازش این مبادله و انتقال آن به حساب‌ها، یک کنترل کشف‌کننده باید مبلغ کل صورت‌حساب را مجدداً با استفاده از داده‌های مبلغ و تعداد حساب نماید. بنابراین، اشتباه مذکور، کشف خواهد شد.

کنترل‌های اصلاحی

اقدامات اصلاحی باید به منظور بر طرف کردن اثرات اشتباهات کشف شده بکار گرفته شود. تمایز با اهمیتی بین کنترل‌های کشف‌کننده و کنترل‌های اصلاحی وجود دارد. کنترل‌های کشف‌کننده رویدادهای نامطلوب را شناسایی می‌کنند و موجب جلب توجه به مشکل می‌شوند؛ اما کنترل‌های اصلاحی اقدام به ترمیم مشکل می‌کنند. برای هرگونه مشکل شناسایی شده، ممکن است بیش از یک اقدام اصلاحی ممکن وجود داشته باشد؛ اما امکان دارد همواره بهترین روش قابل تشخیص نباشد. به عنوان نمونه، در اشتباهی که پیش از این مشاهده گردید، نخستین اقدام شما ممکن است تغییر دادن مبلغ کل از ۱,۰۰۰ دلار به ۱۰۰ دلار به منظور اصلاح اشتباه باشد. در اینجا فرض شده است که تعداد و قیمت واحد در سوابق صحیح است؛ در حالی که این امر ممکن است صادق نباشد. در این مورد، ما قادر به شناسایی دلیل واقعی این اشتباه نیستیم و فقط می‌دانیم که چنین اشتباهی وجود دارد.

متصل کردن اقدام اصلاح‌کننده به اشتباه کشف‌شده به عنوان یک واکنش خودکار، می‌تواند به مشکلی بدتر از اشتباه اولیه دامن بزند. به این دلیل، اصلاح اشتباه باید به عنوان یک گام کنترلی جداگانه در نظر گرفته شود که باید با احتیاط طی شود.

مدل کنترلی پیشگیری، کشف و اصلاح، از لحاظ مفهومی‌مناسب است اما رهکردهای کاربردی اندکی پیرامون طراحی یا حسابرسی کنترل‌ها ارائه می‌دهد. سند لازم الاجرای کنونی پیرامون اهداف و فنون کنترل‌های داخلی، بیانیه مربوط به بیانیه استانداردهای حسابرسی شماره ۱۰۹ ایالات متحده است که مبتنی بر چارچوب کوزو است. بیانیه استاندارد حسابرسی شماره ۱۰۹، رابطه پیچیده بین کنترل‌های داخلی شرکت، ارزیابی حسابرس از ریسک و برنامه‌ریزی رویه‌های حسابرسی را تشریح می‌کند. استاندارد مذکور، رهنمودی پیرامون بکارگیری چارچوب کوزو در هنگام ارزیابی ریسک تحریف با اهمیت در اختیار حسابرسان قرار می‌دهد. ما در اینجا به تشریح عناصر کلیدی این چارچوب می‌پردازیم.

قانون ساربینز- آکسلی[۴] ۲۰۰۲

تقلبات مالی گسترده متعدد (مانند شرکت‌های انرون، ورلدکام، آدلفیا و...) و نابودی منافع سهامداران، کنگره آمریکا را بر آن داشت تا برای حفظ منافع عموم وارد عمل شود. این امر به تصویب قانون ساربینز- آکسلی در ۳۰ جولای ۲۰۰۲ منتج گردید. این قانون در پی این است که با بهبود اصول راهبری شرکت‌ها، کنترل‌های داخلی و کیفیت حسابرسی، اعتماد عموم را به بازارهای سرمایه افزایش دهد.

بطور خاص، این قانون مدیریت شرکت‌های سهامی‌عام را ملزم می‌کند که سیستم کنترل داخلی مطلوب برای فرآیند گزارشگری مالی داشته باشد. این امر شامل کنترل‌های حاکم بر سیستم‌های پردازش معاملات می‌شود که داده‌های مورد نیاز سیستم گزارشگری مالی را فراهم می‌آورد. مسئولیت‌های مدیریت در این رابطه در بخش‌های ۳۰۲ و ۴۰۴ قانون ساربینز- آکسلی، آورده شده است.

بخش ۳۰۲ مدیریت شرکت (شامل مدیر عامل) را ملزم می‌دارد که کنترل‌های داخلی سازمان را بطور دوره‌ای یا سالانه مورد تأیید قرار دهند. این بخش موارد با اهمیتی برای حسابرسی نیز در پی دارد. بطور خاص، حسابرسان خارجی باید رویه‌های زیر را بطور دوره‌ای اجرا کنند تا هر گونه ضعف با اهمیت در کنترل‌ها را شناسایی کنند که می‌تواند گزارشگری مالی را تحت تأثیر قرار دهد.

- مصاحبه با مدیریت به منظور شناسایی هر گونه تغییر با اهمیت در طراحی یا عملیات کنترل داخلی که پس از حسابرسی سالانه قبلی یا قبل از بررسی اطلاعات مالی میان دوره‌ای رخ داده است.
- ارزیابی اثرات تحریف‌های شناسایی شده بوسیله حسابرس به عنوان بخشی از بررسی میان دوره‌ای که با اثر بخشی کنترل‌های داخلی در ارتباط است.
- تعیین اینکه آیا تغییرات در کنترل‌های داخلی امکان دارد بطور با اهمیتی کنترل داخلی حاکم بر گزارشگری مالی را تحت تأثیر قرار دهد.

قانون ساربینز – آکسلی، مدیریت شرکت‌های سهامی عام را ملزم می‌کند که سیستم کنترل داخلی مطلوب برای فرآیند گزارشگری مالی داشته باشند

بعلاوه، بخش ۴۰۴ مدیریت شرکت‌های سهامی‌عام را ملزم به ارزیابی اثربخشی کنترل‌های داخلی سازمان می‌نماید. این امر مستلزم ارائه گزارشی سالانه حاوی موارد زیر است:

۱. درک جریان مبادلات شامل جنبه‌های فناوری اطلاعات، در جزئیات کافی به منظور شناسایی نقاطی که امکان دارد به یک تحریف بیانجامد.

۲. استفاده از رویکرد مبتنی بر ریسک، ارزیابی هم طراحی و هم اثر بخشی عملیات کنترل‌های داخلی مورد نظر که با حساب‌های با اهمیت در ارتباط هستند.

۳. ارزیابی امکان تقلب در سیستم و ارزیابی کنترل‌های طراحی شده به منظور پیشگیری یا کشف تقلب.

۴. ارزیابی و نتیجه‌گیری پیرامون کفایت کنترل‌های حاکم بر فرآیند حاکم بر گزارشگری صورت‌های مالی.

۵. ارزیابی کنترل‌های فراگیر سازمان (عمومی) که با اجزای چارچوب کوزو هماهنگ هستند.

در ارتباط با چارچوب کنترل‌ها، کمیسیون بورس و اوراق بهادار، بطور خاص به کوزو به عنوان مدل توصیه شده، اشاره می‌نماید.

بعلاوه، استاندارد حسابرسی شماره ۵ هیات نظارت بر حسابداری شرکت‌های سهامی‌عام، بر استفاده از کوزو به عنوان چارچوبی به منظور ارزیابی کنترل‌ها تأکید می‌نماید. گرچه چارچوب‌های مناسب دیگری نیز منتشر شده است، اما هر چارچوبی باید بطور کامل با الگوی کوزو هماهنگ باشد[۵].

حسابرسی فناوری اطلاعات، ابزاری حیاتی برای حل نگرانی‌های امروز سازمان‌ها در زمینه فناوری اطلاعات محسوب می‌شود

کمیته سازمان‌های حامی(۱۹۹۲)

در پی مجموعه رسوایی‌های شرکت پس‌انداز و وام[۶] در دهه ۱۹۸۰، در ایالات متحده کمیته‌ای برای رسیدگی به این تقلبات تشکیل گردید. این کمیته در اصل تحت نام رئیس آن، تردوی[۷] شناخته شد؛ اما در نهایت این پروژه، کوزو[۸] (کمیته سازمان‌های حامی) نامیده شد. سازمان‌های حامی‌عبارتند از: مدیران مالی بین‌المللی[۹]، انجمن حسابداران مدیریت[۱۰]، جامعه حسابداری آمریکا[۱۱]، انجمن حسابداران رسمی‌آمریکا[۱۲] و انجمن حسابرسان داخلی[۱۳] هستند. کار این کمیته چند سال به طول انجامید. آنان ابتدا به این مطلب پی بردند که بهترین مانع در برابر تقلب، کنترل‌های داخلی قوی است؛ سپس به ارائه مدلی اثربخش از کنترل‌های داخلی برای سازمان پرداختند و ماحصل آن مدل کوزو[۱۴] بود. انجمن حسابداران رسمی‌آمریکا، این مدل را در قالب استانداردهای حسابرسی بکار گرفت و استاندارد شماره ۷۸ با عنوان «ارزیابی کنترل داخلی در حسابرسی صورت‌های مالی[۱۵]» را منتشر کرد.

چارچوب کنترل داخلی کوزو

چارچوب کوزو، شامل ۵ بخش محیط کنترلی، ارزیابی ریسک، اطلاعات و ارتباطات، نظارت و فعالیت‌های کنترلی است.

محیط کنترلی

محیط کنترلی، بنیان چهار بخش دیگر کنترل محسوب می‌شود. محیط کنترلی، با فضای حاکم بر سازمان ارتباط دارد و تحت تأثیر کنترل‌هایی قرار دارد که مبتنی بر آگاهی مدیریت و کارکنان است. عناصر با اهمیت محیط کنترلی به شرح زیر است:

- درستکاری و ارزش‌های اخلاقی مدیریت.
- ساختار سازمان.
- مشارکت هیات مدیره سازمان و کمیته حسابرسی، چنانچه وجود داشته باشد.
- فلسفه مدیریت و سبک عملیاتی.
- رویه‌های محول کردن مسئولیت و اختیار امور.
- روش‌های مدیریت برای ارزیابی عملکرد.
- اثرات خارجی، از قبیل ارزیابی بوسیله سازمان‌های قانونی.
- سیاست‌ها و رویه‌های سازمان برای مدیریت منابع انسانی خود.

بیانیه استاندارد حسابرسی شماره ۱۰۹، حسابرسان را ملزم می‌دارد تا نسبت به مدیریت سازمان، هیات مدیره و افراد مرتبط با کنترل داخلی سازمان، به شناختی کافی دست یابند. در ادامه نمونه‌هایی از فنونی ارائه شده است که می‌تواند به منظور کسب شناخت از محیط کنترلی سازمان مورد استفاده قرار گیرد:

۱. حسابرسان باید درستکاری مدیریت سازمان را مورد ارزیابی قرار دهند و در این راستا می‌توانند از سازمان‌های رسیدگی‌کننده برای اخذ گزارش درباره پیشینه مدیران کلیدی استفاده کنند. برخی از چهار مؤسسه بزرگ، کارکنان سابق افبی‌آی را بکار می‌گمارند تا نسبت به کسب شناخت از پیشینه مشتریان خود، با مسئولیت بیشتری عمل کرده باشند. در این راستا، چنانچه شواهدی قطعی از عدم دستکاری مشتری بدست آید، حسابرس باید از کار خود کناره‌گیری نماید. حسن شهرت و درستکاری مدیران شرکت، عاملی کلیدی در قابل حسابرسی بودن سازمان، محسوب می‌شود. حسابرس نمی‌تواند در محیطی بدرستی به وظایف خود عمل نماید که مدیریت صاحبکار فاقد ارزش‌های اخلاقی و فاسد است.

۲. حسابرسان باید نسبت به شرایطی آگاه باشند که فرصت ارتکاب به تقلب را برای مدیریت سازمان فراهم می‌آورد. برخی از این شرایط عبارتند از عدم کفایت سرمایه در گردش، شرایط نابسامان صنعت، رتبه اعتباری نامناسب و وجود شرایط محدود کننده بسیار در قراردادهای بانکی است. اگر حسابرسان با چنین شرایطی مواجه شوند، باید در ارزیابی خود، امکان وجود گزارشگری مالی متقلبانه را در ملاحظات خود وارد کنند. در این راستا، باید مقیاس‌های مناسب بکار گرفته شود تا هرگونه تلاش متقلبانه‌ای آشکار گردد.

۳. حسابرسان باید نسبت به کسب و کار و صنعت صاحبکار خود کسب شناخت نماید و نسبت به شرایط ویژه‌ای آگاه باشند که می‌تواند حسابرسی را تحت تأثیر قرار دهد. حسابرسان باید مطالب مربوط به صنعت صاحبکار را مطالعه کنند و خود را با ریسک‌های ذاتی کسب و کار مورد رسیدگی، آشنا سازند.

۴. هیات مدیره باید مواد قانون ساربینز- آکسلی را به عنوان حداقل بپذیرد. بعلاوه، رهکردهای زیر، بهترین رویه‌ها را ارائه می‌دهد:

تفکیک مدیر عامل از ریاست هیات مدیره: وظایف مدیر عامل از وظایف ریاست هیات مدیره باید جدا باشد. این امر به هیات مدیره فرصت بررسی مسائل بدون حضور مدیر عامل را می‌دهد و در این شرایط وجود یک ریاست مستقل از مدیر عامل، موجب سهولت در انجام این قبیل نشست‌ها می‌شود.

ایجاد استانداردهای اخلاقی: هیات مدیره باید آیین نامه‌ای از استانداردهای اخلاقی تدوین نماید و تمام مدیران و کارکنان سازمان به آن پایبند باشند. حداقل مواردی که باید در آیین‌نامه مذکور وجود داشته باشد عبارتند از: اختلافات با افراد برون سازمانی، پذیرش هدیه‌ای که می‌تواند جنبه رشوه داشته باشد، تحریف داده‌های مالی و یا مربوط به عملکرد، تضاد منافع، مشارکت‌های سیاسی، حفاظت از اطلاعات شرکت و مشتریان، درستکاری در برقراری رابطه با حسابرسان داخلی و خارجی، و عضویت در هیات مدیره‌های خارج از سازمان است.

ایجاد کمیته حسابرسی: کمیته حسابرسی مسئول انتخاب و بکارگماری حسابرس مستقل، اطمینان نسبت به اجرا شدن حسابرسی سالانه، بررسی گزارش حسابرس و اطمینان

نسبت به اینکه نواقص شناسایی شده مورد پیگیری قرار گرفته‌اند. سازمان‌های بزرگ همراه با رویه‌های حسابداری پیچیده ممکن است نیاز داشته باشند تا کمیته‌های زیر مجموعه حسابرسی ایجاد کنند که بطور خاص به امور خاص رسیدگی کنند.

کمیته‌های پاداش: کمیته پاداش نباید مهر تأییدی برای مدیریت باشد. استفاده بیش از اندازه از اختیار سهام در کوتاه مدت به منظور اعطای پاداش به هیات مدیره و مدیر عامل می‌تواند منتج به تصمیماتی شود که قیمت سهام را به بهای سلامت شرکت در بلند مدت تحت تأثیر قرار دهد. الگوهای پاداش باید به دقت مورد ارزیابی قرار بگیرند تا اطمینان حاصل شود که انگیزه‌های مطلوب را در مدیریت ایجاد می‌کنند.

کمیته‌های نامزدی: کمیته نامزدهای هیات مدیره باید برنامه‌ای داشته باشند تا بتوانند برای سالیان متمادی هیات مدیره‌ای دربرگیرنده افرادی دارای صلاحیت داشته باشند. این کمیته باید نیاز به مدیران مستقل را تشخیص دهند و ضوابطی برای تعیین استقلال داشته باشند. به عنوان نمونه، شرکت جنرال الکتریک بر اساس استانداردهای راهبری جدید خویش، مدیران را در صورتی مستقل ارزیابی می‌کنندکه فروش به آن، یا خرید آن از شرکت کمتر از ۱ درصد درآمد شرکت‌هایی باشد که وی در آن مسئولیت اجرایی دارد. استانداردهای مشابه نیز به منظور ارائه کمک‌های خیرخواهانه از شرکت جنرال الکتریک به هر سازمانی با توجه بر این وجود داردکه آیا مدیری از شرکت جنرال الکتریک، ریاست یا مدیریت آن را بر عهده دارد، بعلاوه، این شرکت دارای هدفی است که بر اساس آن، دو سوم از اعضای هیات مدیره، اعضای مستقل غیر موظف باشند(۱۶).

دسترسی به افراد حرفه‌ای خارج از سازمان: تمام کمیته‌های هیات مدیره باید به وکلا و مشاورانی علاوه بر وکلا و مشاوران معمول شرکت، دسترسی داشته باشند. براساس مواد قانون ساربینز- آکسلی، کمیته حسابرسی شرکت سهامی‌عام، باید در ظاهر کاملاً مستقل بنظر برسد.

ارزیابی ریسک

سازمان‌ها باید ارزیابی ریسک انجام دهند تا ریسک‌های مربوط به گزارشگری مالی را شناسایی، تجزیه و تحلیل و مدیریت کنند. ریسک‌ها می‌توانند به سبب شرایطی یا تغییرات از قبیل موارد زیر ایجاد شوند:

- تغییرات در محیط عملیاتی که موجب ایجاد یا تغییر فشارها رقابتی بر شرکت می‌شود.
- کارکنان جدید که شناختی متفاوت یا ناکافی از کنترل داخلی دارند.
- سیستم‌های اطلاعاتی جدید یا تجدید نظر شده که پردازش معاملات را تحت تأثیر قرار می‌دهد.
- رشد با اهمیت و سریع که کنترل‌های داخلی موجود را تحت فشار قرار می‌دهد.
- اجرای فناوری جدید در فرآیند تولید یا سیستم اطلاعاتی که پردازش معاملات را تحت تأثیر قرار می‌دهد.
- معرفی خطوط تولید محصولات یا فعالیت‌های جدید که سازمان نسبت به آن‌ها تجربه کمی‌دارد.
- تجدید ساختار سازمان که موجب کاهش یا تخصیص مجدد کارکنان می‌شود و عملیات شرکت و فرآیند پردازش مبادلات را تحت تأثیر قرار می‌دهد.
- ورود به بازارهای خارجی که می‌تواند عملیات را تحت تأثیر قرار دهد (به این معنی که با انجام مبادلات ارزی، ریسک دیگری ایجاد می‌گردد).
- پذیرفتن اصل حسابداری جدید که تهیه صورت‌های مالی را تحت تأثیر قرار می‌دهد.

بیانیه استاندارد حسابرسی شماره ۱۰۹، حسابرسان را ملزم می‌کند که به شناختی کافی پیرامون رویه‌های ارزیابی ریسک سازمان، به منظور آگاهی نسبت به نحوه شناسایی، ریشه‌یابی و مدیریت ریسک‌ها مربوط به گزارشگری مالی دست یابند.

اطلاعات و ارتباطات

سیستم اطلاعاتی حسابداری دربرگیرنده سوابق و روش‌های استفاده شده به منظور وارد کردن، تعریف کردن، تجزیه و تحلیل، طبقه‌بندی و ثبت مبادلات سازمان و منظور کردن به حساب دارایی‌ها و بدهی‌های مربوط است. کیفیت اطلاعات ایجاد شده توسط سیستم اطلاعاتی حسابداری، توانایی مدیریت در اداره و اتخاذ تصمیمات مربوط به عملیات سازمان را تحت تأثیر قرار می‌دهد و به صورت‌های مالی قابل اتکا می‌انجامد.

سیستم اطلاعاتی حسابداری اثربخش:

- تمام مبادلات مالی معتبر را تعریف و ثبت می‌نماید.
- اطلاعاتی به هنگام پیرامون مبادلات با جزئیات کافی تهیه می‌نماید تا بطور مناسب گزارش‌های مالی تهیه و ارائه شود.
- اندازه‌گیری دقیق ارزش مالی مبادلات و نیز اثرات آن‌ها بر صورت‌های مالی.
- ثبت دقیق و به هنگام مبادلات به محض وقوع.

بیانیه استاندارد حسابرسی شماره ۱۰۹ الزامی‌می‌نماید که حسابرسان دانش کافی پیرامون سیستم اطلاعاتی سازمان کسب کنند تا نسبت به موارد زیر به شناخت دست یابند:

- طبقات مبادلات که در صورت‌های مالی با اهمیت هستند و اینکه چگونه این مبادلات ایجاد می‌شود.
- سوابق حسابداری و حساب‌ها که در پردازش مبادلات با اهمیت مورد استفاده قرار می‌گیرند.
- گام‌های پردازش مبادلات از لحظه انجام مبادله تا زمان ارائه در صورت‌های مالی.
- فرآیند گزارشگری مالی که در تهیه صورت‌های مالی، افشای اطلاعات و برآورد حساب‌ها انجام می‌شود.

نظارت

مدیریت باید مشخص نماید که کنترل‌های داخلی، مطابق با اهداف خود کار می‌کنند. نظارت فرآیندی است که در آن کیفیت طراحی کنترل داخلی و عملیات می‌تواند مورد ارزیابی قرار گیرد. نظارت می‌تواند بصورت رویه‌های جداگانه یا از طریق

سازمان‌ها باید ارزیابی ریسک انجام دهند تا ریسک‌های مربوط به گزارشگری مالی را شناسایی، تجزیه و تحلیل و مدیریت نمایند

شکل۴: طبقه بندی فعالیت‌های کنترلی

فعالیت‌های مستمر انجام شود.

حسابرسان داخلی سازمان، می‌توانند فعالیت‌های واحد گزارشگر در قالب رویه‌هایی جداگانه مورد نظارت قرار دهند. آن‌ها به جمع‌آوری شواهدی پیرامون کفایت کنترل بوسیله اجرای آزمون‌های کنترل می‌پردازند و سپس نقاط قوت و ضعف را به مدیریت منتقل می‌کنند. حسابرسان داخلی به عنوان بخشی از این پروژه، توصیه‌هایی ویژه به منظور بهبود کنترل‌ها ارائه می‌دهند.

نظارت مستمر می‌تواند از طریق تعبیه برنامه‌های ویژه کامپیوتری در سیستم اطلاعاتی انجام گیرد؛ به‌طوری‌که این برنامه‌ها به جمع‌آوری داده‌های کلیدی یا انجام آزمون‌های کنترل به عنوان بخشی از عملیات عادی سیستم می‌پردازند. در نتیجه این برنامه‌ها به مدیریت و حسابرسان این امکان را می‌دهد که بر اجرای کنترل‌های داخلی نظارتی مستمر داشته باشند.

نیازهای نوظهور در عرصه بازارهای رقابتی، واحدهای تجاری را به سوی توسعه و بکارگیری هر چه بیشتر سامانه‌های فناوری اطلاعات تشویق می‌نمایند

روش دیگر دستیابی به نظارت مستمر، استفاده مناسب از گزارش‌های مدیریت است. گزارش‌های به هنگام، به مدیران این امکان را می‌دهد که در حوزه‌های عملکردی از قبیل فروش، خرید، تولید و توزیع وجه‌نقد سرپرستی و کنترل داشته باشند. گزارش‌های مدیریتی که به خوبی طراحی شده‌اند، بوسیله خلاصه کردن فعالیت‌ها، برجسته کردن فرآیندها و شناسایی استثناها از عملکرد معمول، شواهدی از کارایی یا نقص کنترل داخلی ارائه می‌دهد.

■ فعالیت‌های کنترلی

فعالیت‌های کنترلی، سیاست‌ها و رویه‌هایی است که به منظور اطمینان از برخورد مناسب با ریسک‌های شناسایی شده سازمان، بکار گرفته می‌شود. فعالیت‌های کنترلی می‌تواند در دو دسته مجزا کنترل‌های فیزیکی و کنترل‌های فناوری اطلاعات طبقه‌بندی شوند: شکل ۴ فعالیت‌های کنترلی در هر یک از این طبقات را به تصویر می‌کشد.

■ کنترل‌های فیزیکی

این طبقه از کنترل‌ها، اساساً به فعالیت‌های انسانی موجود در سیستم‌های حسابداری، ارتباط پیدا می‌کند. این فعالیت‌ها می‌تواند کاملاً دستی شامل حفاظت فیزیکی از دارایی‌ها و کامپیوترها به منظور ثبت معاملات یا بروز رسانی حساب‌ها باشد. کنترل‌های فیزیکی به منطق کامپیوتر به کارگرفته شده در اجرای فرآیندهای حسابداری ارتباطی ندارد. در مقابل، این کنترل‌ها به فعالیت‌های انسانی ارتباط می‌یابد که فرمان‌های کامپیوتری را اجرا و از نتایج آن استفاده می‌کنند. به عبارت دیگر، کنترل‌های فیزیکی بر افراد تاکید دارد، اما تنها محدود به کارکنانی نمی‌شود که اسناد فیزیکی را بطور دستی بروز رسانی کنند. بطور کلی در تمام سیستم‌ها، صرف‌نظر از میزان پیچیدگی آن‌ها، فعالیت‌های انسانی باید تحت کنترل باشد.

در این راستا، فعالیت‌های کنترلی فیزیکی در شش دسته تصویب مبادلات، تفکیک وظایف، سرپرستی، سوابق حسابداری، کنترل دسترسی، و بررسی مستقل طبقه‌بندی می‌شود.

تصویب مبادلات: هدف از تصویب مبادلات، حصول اطمینان نسبت به این است که تمام مبادلات با اهمیت معتبر و مطابق با اهداف مدیریت است که بوسیله سیستم اطلاعاتی پردازش می‌شود، تصویب می‌تواند بطور عمومی‌یا اختصاصی صورت گیرد. اختیار تصویب عمومی‌به کارکنان

شکل۵: اهداف تفکیک وظایف

عملیاتی اعطا می‌شود که فعالیت‌های روزمره سازمان را انجام می‌دهند. نمونه‌ای از تصویب عمومی، تصویب خرید موجودی مواد و کالا از یک فروشنده مشخص شده است، زمانی‌که سطح موجودی از میزان از پیش تعیین شده پایین‌تر می‌آید. این اقدام، «یک رویه برنامه‌ریزی شده» نامیده می‌شود (ضرورتی به کامپیوتری بودن، وجود ندارد)؛ زیرا در آن ضوابط تصمیم‌گیری کاملاً مشخص است و نیازی به هیچ‌گونه قضاوت دیگری ندارد. از طرف دیگر، تصویب رویدادهای خاص، به سبب اینکه با رویدادهای عادی سر و کار ندارد، نیاز به اتخاذ تصمیمات موردی بوجود می‌آید. نمونه‌ای از این قبیل تصمیمات، اعطای اعتبار به مشتری به میزانی بالاتر از حد معمول است. تصویب امور خاص، بطور معمول از مسئولیت‌های مدیریت است. (شکل۵)

تفکیک وظایف: از مهم‌ترین فعالیت‌های کنترلی، تفکیک وظایف است تا میزان تجمیع وظایف ناسازگار در سازمان به حداقل ممکن برسد. تفکیک وظایف می‌تواند در اشکال مختلف بر حسب وظایفی صورت می‌گیرد که باید مورد کنترل باشند. در هر حال، در این راستا، سه هدف زیر به عنوان رهکردهای کلی در بیشتر سازمان‌ها بکار گرفته می‌شود. این اهداف در شکل ۵،۱ ارائه شده است.

هدف ۱. تفکیک وظایف عبارت است از اینکه فعالیت تصویب مبادلات باید از فعالیت پردازش مبادلات تفکیک شود. به عنوان نمونه، دایره خرید نباید تا زمانی اقدام به خرید نماید که دایره کنترل موجودی مواد و کالا اجازه خرید را صادر نکرده است، این تفکیک وظیفه، در واقع اقدام کنترلی است تا از خریدهای غیر ضروری کالا جلوگیری به عمل آید.

هدف ۲. مسئولیت نگهداری فیزیکی دارایی‌ها باید از مسئولیت نگهداری سوابق تفکیک شود. به عنوان نمونه، دایره مسئول حفاظت فیزیکی از کالاهای تکمیل شده (انبار)، نباید سوابق رسمی‌موجودی مواد و کالا را نگهداری کنند. سوابق موجودی مواد و کالا به عنوان یک اقدام کنترلی، بوسیله دایره حسابداری تهیه و نگهداری می‌شود. زمانی که یک فرد یا دایره واحد، هم مسئولیت نگهداری دارایی و هم مسئولیت سوابق مربوط به آن را به عهده داشته باشد، زمینه ارتکاب به تقلب فراهم می‌شود. در این شرایط دارایی‌ها می‌توانند دزدیده یا مفقود شوند و سوابق حسابداری آن‌ها نیز این رویدادها را پنهان کنند.

هدف ۳. در سازمان که تفکیک وظایف به خوبی صورت گرفته باشد، انجام تقلب موفق نیاز به تبانی بین دو یا چند نفر با وظایف ناسازگار خواهد داشت. به عنوان نمونه، هیچ فردی نباید به آن اندازه به سوابق حسابداری دسترسی داشته باشد که بتواند مرتکب تقلب شود. بنابراین، دفاتر روزنامه، کل و معین بطور جداگانه نگهداری می‌شوند. برای بیشتر افراد، اینکه به دیگران پیشنهاد تبانی برای ارتکاب به تقلب ارائه دهند، از لحاظ روانشناسی مانع غیر قابل نفوذ است. این امر به سبب ترس از قبول نکردن و پیامدهای آتی آن است. اما، زمانی این مانع از بین خواهد رفت که کارکنان دارای مسئولیت‌های ناسازگار در کنار هم کار می‌کنند و با هم آشنا می‌شوند و روابطی نزدیک با هم خواهند داشت، به این دلیل، تفکیک وظایف ناسازگار، باید بطور فیزیکی نیز در سازمان صورت گیرد. همچنین، وجود روابط خویشاوندی بین افراد دارای مسئولیت‌های ناسازگار نیز باید مد نظر قرار گیرد.

فعالیت‌های کنترلی، سیاست‌ها و رویه‌هایی است که به منظور اطمینان از برخورد مناسب با ریسک‌های شناسایی شده سازمان به کار گرفته می‌شود

سرپرستی: اجرای تفکیک کافی وظایف در درون شرکت، مستلزم بکارگیری تعدادی کافی از کارکنان خواهد بود. این امر در حالی است که تحقق این شرایط در شرکت‌های کوچک اغلب امکان‌پذیر نیست. بنابراین، در سازمان‌های کوچک یا مراکز مسئولیت که با فقدان کارکنان کافی مواجه هستند، مدیریت باید با سرپرستی خود، فقدان کنترل‌های ناشی از تفکیک مناسب وظایف را جبران نماید. به این دلیل، سرپرستی اغلب کنترل جبرانی خوانده می‌شود.

فرض زیربنایی کنترل از طریق سرپرستی این است که کارکنان شرکت، افرادی دارای صلاحیت و قابل اعتماد هستند. مسلماً هیچ سازمانی نخواهد توانست با کارکنانی فاقد صلاحیت و درستکاری، برای مدتی طولانی به کار خود ادامه دهد. صلاحیت و درستکار بودن کارکنان، فرضی است که با برقرار بودن آن، سرپرستی اثربخش خواهد بود. بنابراین شرکت‌ها می‌توانند با طراحی برنامه

کنترلی، به هر مدیر، سرپرستی تعدادی از کارکنان را واگذار کنند. در سیستم‌های دستی که مدیران و کارکنان از لحاظ مکان فیزیکی در کنار یکدیگر کار می‌کنند، بکارگیری سرپرستی از اثر بخشی بالاتری برخوردار خواهد بود.

سوابق حسابداری: سوابق حسابداری سازمان شامل اسناد و مدارک، دفاتر روزنامه و دفاتر کل است. این سوابق در برگیرنده رویدادهای اقتصادی است و زنجیره عطفی از رویدادهای اقتصادی ارائه می‌دهند. زنجیره عطف حسابرسی، حسابرس را قادرمی‌سازد که پردازش هرگونه مبادله‌ای را از ابتدای شکل‌گیری تا گزارش در صورت‌های مالی رهگیری نماید. سازمان‌ها باید از زنجیره عطف حسابرسی به دو دلیل نگهداری کنند. نخست اینکه این اطلاعات به منظور اداره عملیات روزمره مورد نیاز است. زنجیره عطف حسابرسی به کارکنان کمک می‌نماید تا به نیازهای مشتریان با مشاهده وضعیت موجود پاسخ دهند. دلیل دوم اینکه زنجیره عطف حسابرسی نقشی اساسی در حسابرسی مالی شرکت ایفا می‌نماید. این امر حسابرسان مستقل (و داخلی) را قادر می‌سازد تا مبادلات انتخاب شده را از صورت‌های مالی تا حساب‌های دفتر کل، دفتر روزنامه و اسناد و مدارک اولیه رهگیری کنند. بنابراین شرکت‌های تجاری باید هم به دلایل عملی و هم به دلایل نظارتی، سوابق حسابداری کافی را به منظور زنجیره عطف حسابرسی نگهداری کنند.

هدف از حسابرسی فناوری اطلاعات، کسب اطمینان نسبت به اثربخشی سیاست‌های سازمان در زمینه مدیریت ریسك، کنترل و راهبری واحد فناوری اطلاعات است

کنترل دسترسی: هدف کنترل دسترسی حصول اطمینان نسبت به این است که تنها افراد مجاز به دارایی‌های شرکت دسترسی دارند. دسترسی غیر مجاز به دارایی‌های منجر به سوء استفاده، تخریب و سرقت می‌شود. بنابراین، کنترل‌های دسترسی، نقشی اساسی در حفاظت از دارایی‌ها ایفا می‌کنند. دسترسی به دارایی‌ها می‌تواند مستقیم یا غیر مستقیم باشد. ابزارهای امنیت فیزیکی از قبیل قفل‌ها، گاو صندوق‌ها، حصارها و سیستم‌های هشداردهنده الکترونیکی، کنترل‌هایی در برابر دسترسی مستقیم هستند. دسترسی غیر مستقیم به دسترسی به سوابق و اسنادی اشاره دارد که در بر دارنده اطلاعات مربوط به استفاده، مالکیت و کنارگذاری دارایی است. به عنوان نمونه، یک فرد با دسترسی به تمام سوابق حسابداری مربوط می‌تواند زنجیره عطف حسابداری مربوط به مبادله فروش خاص را از بین ببرد. بنابراین با حذف سوابق این رویداد، شامل مانده حساب دریافتنی، این فروش هرگز ثبت و ضبط نمی‌شود و شرکت نیز هرگز وجوه مربوط به اقلام فروخته شده را دریافت نخواهد کرد. کنترل‌های دسترسی بکار گرفته شده در سازمان، متناسب با فناوری سیستم حسابداری متفاوت است. کنترل دسترسی غیر مستقیم بوسیله بکارگیری اسناد و سوابق در سازمان را کنترل می‌کند و بوسیله تفکیک وظایف، افرادیرا مشخص می‌سازد که باید به سوابق دسترسی و اجازه پردازش آن‌ها را داشته باشند.

بررسی مستقل: بررسی مستقل به معنی ارزیابی مستقل سیستم حسابداری به منظور شناسایی اشتباهات و تحریف‌ها است. بررسی متفاوت از سرپرستی است؛ زیرا بررسی پس از تحقق رویداد و بوسیله فردی انجام می‌شود که هیچگونه ارتباطی با رویداد انجام شده یا وظایف مرتبط با آن ندارد. سرپرستی در حین اجرای رویدادها انجام می‌شود و فرد سرپرست نیز شخصی است که در قبال رویدادهای انجام شده، مسئولیت دارد. از طریق فرآیند بررسی مستقل مدیریت می‌تواند: ۱) عملکرد افراد را ارزیابی نماید، ۲) یکپارچگی سیستم پردازش مبادلات، و ۳) صحت داده‌های موجود در سوابق حسابداری. نمونه‌هایی از بررسی مستقل مواردی به این شرح است:

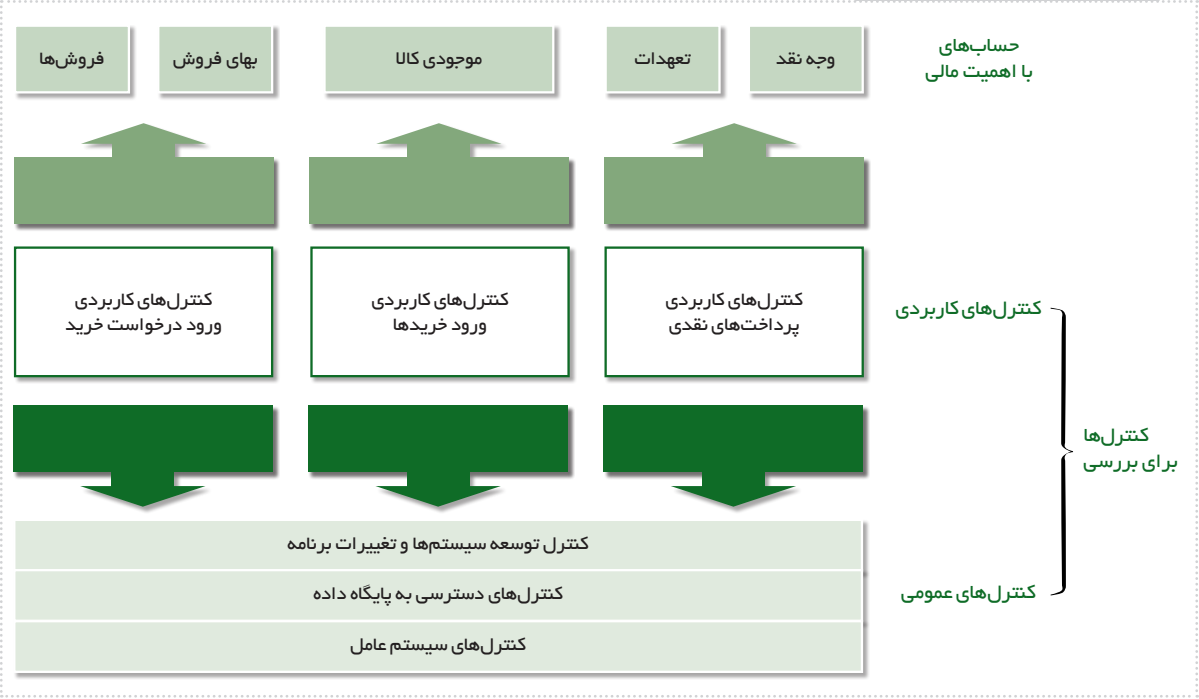
- تلفیق مجموع مبالغ در خلال فرآیند پردازش مبادلات.
- مقایسه دارایی‌های فیزیکی با سوابق حسابداری.
- تلفیق حساب‌ها معین با حساب‌های کنترلی.
- بررسی گزارش‌های مدیریت (کامپیوتری و دستی) که در برگیرنده خلاصه‌ای از فعالیت شرکت است.

زمان‌بندی بررسی به فناوری بکار گرفته شده در سیستم حسابداری و وظایف تحت بررسی بستگی دارد. بررسی می‌تواند چندین بار در یک ساعت یا در یک روز باشد. در برخی موارد، عملیات بررسی بطور روزانه، هفتگی، ماهانه یا سالانه انجام می‌شود.

کنترل‌های فناوری اطلاعات

فناوری اطلاعات، فرآیندهای گزارشگری مالی سازمان‌های امروزی را دگرگون ساخته است. سیستم‌های خودکار، مبادلات را شناسایی، تصویب، ثبت و اثرات مالی آن‌ها را گزارش می‌کنند. این امر در برگیرنده مباحثی لاینحلی در گزارشگری مالی است که قانون ساربینز- آکسلی آن را مورد توجه قرار داده است و باید

شکل۶: روابط کنترلی فناوری اطلاعات



مـورد کنتـرل واقع شـوند. کـوزو کنترل‌های فنـاوری اطلاعـات را در دو طبقـه، کنترل‌هـای کاربـردی و کنترل‌هـای عمومی‌دسـته‌بندی می‌نمایـد. اهـداف کنترل‌هـای کاربـردی، حصول اطمینان نسـبت به اعتبـار، کامـل بـودن و صحـت مبـادلات مالـی اسـت. ایـن کنترل‌ها بصـورت اختصاصـی طراحی می‌شـوند.

نمونه‌هایی از این موارد عبارتند از:

- بررسـی میـزان وجه‌نقـد پرداخت شـده بـه فروشـندگان و میزان مبلغـی کـه در معیـن حسـاب پرداختنی مربوط منظور شـده اسـت.
- بررسـی معتبـر بودن مشـتری و نیز مبلـغ فروش انجام شـده که در حسـاب پرداختنی مربوط درج شـده اسـت.
- بررسـی سـاعت کار گـزارش شـده بـه سیسـتم پرداخـت حقـوق و دسـتمزد از طریـق سـوابق کارت زمـان کارکنـان بـا محدوده‌هـای زمانـی از پیـش تعییـن شـده بـرای کارکنان.

ایـن نمونه‌هـا نشـان می‌دهـد کـه چگونـه کنترل‌هـا، بـر صحـت داده‌هایـی تأثیـر می‌گذاردکـه از رویدادهای مختلف نشـأت می‌گیرند و سـپس پردازش شـده و از طریق صورت‌های مالی گزارش می‌شـوند.

دسـته دوم کنترل‌هـای معرفـی شـده بوسـیله چارچـوب کـوزو «کنترل‌هـای عمومـی» خوانـده می‌شـود. دلیـل ایـن نام‌گـذاری ایـن اسـت کـه ایـن کنترل‌هـا بطـور اختصاصـی بـرای یـک وظیفـه خـاص طراحـی نشـده‌اند؛ بلکـه در تمـام سیسـتم‌ها مـورد اسـتفاده قـرار می‌گیرنـد. کنترل‌هـای عمومـی‌در چارچوب‌هـای دیگـر دارای نام‌هـای دیگـری از قبیـل کنترل‌هـای عمومی‌کامپیوتـری و کنترل‌هـای فنـاوری اطلاعـات اسـت. بطـور کلـی هـر یـک از ایـن نام‌هـا بـکار گرفتـه شـود، بیانگـر کنترل‌هـای حاکـم بـر راهبـری فنـاوری اطلاعات، تشـکیلات فنـاوری اطلاعـات، امنیت و دسترسـی بـه سیسـتم‌های عملیاتـی و پایگاه‌هـای داده، بکارگیری، توسـعه و یا تغییـر در برنامه‌هـای کاربـردی اسـت.

گرچـه کنترل‌هـای عمومی‌به کنتـرل مبادلات خاصـی نمی‌پردازد، امـا یکپارچگـی و درسـتی رویدادهـا را تحـت تأثیـر قـرار می‌دهد. به عنـوان نمونـه، سـازمانی را در نظـر بگیریـد کـه کنترل‌هـای امنیتـی ضعیفـی بـرای پایـگاه آن تعبیـه شـده اسـت. در ایـن قبیـل مـوارد، حتـی داده‌هـای پردازش شـده توسـط سیسـتم‌هایی می‌توانند حاوی ریسـک باشـندکه دارای کنترل‌هـای کاربـردی کافـی هسـتند، در ایـن شـرایط هـر فـردی می‌توانـد داده‌هـای رویدادهـا را تغییـر دهد، سـرقت کنـد یـا از بین ببـرد. بنابرایـن، کنترل‌های عمومی‌بـه منظور پشـتیبانی از فعالیـت کنترل‌هـای کاربـردی مـورد نیـاز هسـتند و به منظـور اطمینـان از صحـت گزارشـگری مالـی، وجود هر دو دسـته از کنترل‌هـا ضروری اسـت.

مفاهیم حسابرسـی قانون ساربینز- آکسلی

حسابرسـان مسـتقل، پیـش از تصویـب قانون سـاربینز- آکسـلی، الزامی‌بـرای آزمـون کنترل‌هـای داخلـی بـه عنـوان بخشـی از وظیفه اطمینان‌بخشـی خـود نداشـتند. آن‌ها ملـزم بودند کـه از کنترل‌های داخلـی سـازمان شـناخت کسـب کننـد، امـا ایـن امـر مـورد توجـه قـرار نمی‌گرفـت و آزمون‌هـای کنتـرل نیـز اجـرا نمی‌شـد. بنابرایـن حسابرسـان اغلـب فقـط بـه آزمون‌هـای محتـوا می‌پرداختند.

قانون سـاربینز- آکسـلی، بطـور قابل ملاحظه‌ای نقش حسابرسـان مسـتقل را در شـهادت‌دهی پیرامـون کیفیـت کنترل‌هـای داخلـی صاحبـکار گسـترش داده اسـت. بر اسـاس ایـن قانون حسـابرس باید در اظهارنظـر جداگانـه عـلاوه بـر اظهارنظـر دربـاره ارائـه منصفانـه صورت‌هـای مالـی، دربـاره کنترل‌هـای داخلـی نیـز گـزارش دهـد. اسـتاندارد مربـوط بـه ایـن اظهارنظـر جدیـد حسـابرس، بسـیار سـخت‌گیرانه اسـت؛ به‌طوری‌کـه اگـر حسـابرس تنهـا یـک ضعـف بـا اهمیـت در کنتـرل داخلـی کشـف نمایـد، از ارائه گـزارش مقبول

منع شده است. آنچه که در این زمینه جالب به نظر می‌رسد این است که حسابرسان اجازه دارند که بطور همزمان نسبت به کنترل‌های داخلی گزارش تعدیل شده و نسبت به صورت‌های مالی گزارش مقبول ارائه دهند. به عبارت دیگر، این امکان از نظر فنی وجود دارد که حسابرسان کنترل‌های داخلی حاکم بر گزارشگری مالی را ضعیف ارزیابی کنند، اما با انجام آزمون‌های محتوا به این نتیجه برسند که این ضعف، منجر به تحریف با اهمیت در صورت‌های مالی نشده است.

استاندارد حسابرسی شماره ۵ هیات نظارت بر حسابداری شرکت‌های سهامی‌عام به عنوان بخشی از مسئولیت شهادت‌دهی جدید حسابرسی، بطور خاص حسابرسان را به کسب شناخت از جریان مبادلات شامل کنترل‌های حاکم بر چگونگی شناسایی رویدادها، تصویب، ثبت و گزارش آن‌ها ملزم می‌کند. در این راستا، ابتدا حساب‌هایی شناسایی می‌شود که اثرات با اهمیتی بر گزارشگری مالی دارند سپس حسابرس به کنترل‌های مربوط به این حساب‌ها می‌پردازد. همانطور که پیش از این اشاره گردید، قابلیت اتکای کنترل‌های کاربردی، به اثربخش بودن کنترل‌های عمومی‌بستگی دارد. شکل ۶، رابطه بین کنترل‌های فناوری اطلاعات را به تصویر می‌کشد. مجموع این کنترل‌ها، کاربردی و عمومی، کنترل‌های فناوری اطلاعات حاکم بر گزارشگری مالی را تشکیل می‌دهند که حسابرسان باید آن‌ها را بررسی کنند. (شکل۶)

در واقع آنچه که به آن پرداخته می‌شود مجموعه‌ای از روش‌های کنترلی و آزمون‌های کنترل‌ها است که می‌تواند تحت قانون ساربینز- آکسلی بکار گرفته شود. استاندارد حسابرسی شماره ۵ هیات نظارت بر حسابداری شرکت‌های سهامی‌عام تأکید می‌کنند که مدیریت و حسابرسان از رویکردی مبتنی بر ریسک به جای بکارگیری روش فراگیر به منظور طراحی و اجرای آزمون‌های کنترل‌ها، استفاده کنند. به عبارت دیگر، اندازه و پیچیدگی سازمان باید در تعیین ماهیت و میزان کنترل‌ها مورد نیاز مدنظر واقع شود. بنابراین، کنترل‌ها و رویه‌های حسابرسی بیانگر نیازهای عمومی‌سازمان است و ممکن است در شرایط خاصی کاربرد نداشته باشند.

خلاصه

در این مقاله، چشم‌اندازی از حسابرسی فناوری اطلاعات ارائه گردید. در این راستا، ساختار یک حسابرسی فناوری اطلاعات، ادعاهای مدیریت، اهداف حسابرسی، آزمون کنترل‌ها و آزمون‌های محتوا تشریح گردید. در این پژوهش، به شرح مختصری از جنبه‌های کلیدی چارچوب کنترل کوزو پرداخته شد. که به تشریح کنترل‌های داخلی در محیط‌های دستی و مبتنی بر فناوری اطلاعات، می‌پردازد. بخش نهایی، این مطالعه نیز به بررسی مباحث حسابرسی و مفاهیم مربوط به قانون ساربینز- آکسلی پرداخته و یک چارچوب مفهومی‌درباره روابط کنترل‌های عمومی، کنترل‌های کاربردی و یکپارچگی داده‌های مالی ارائه گردید.

• این مقاله ترجمه آزادی از کتاب زیر است:

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

پی‌نوشت‌ها:

1. Substantive Testing
2. Computer-Assisted Audit Tools and Techniques (CAATTs)
3. American Institute of Certified Public Accountants, AICPA Professional Standards, vol. 1 (New York: AICPA, 1987) AU Sec. 35–320.30.
4. Sarbanes-Oxley Act

۵. اهداف کنترلی برای اطلاعات و فناوری (کوبیت)، یک چارچوب کنترلی متداول است که توسط انجمن راهبری فناوری اطلاعات منتشر شده است. این چارچوب، از الگوی کوزو تبعیت می‌نماید.

6. Savings and Loan Scandals (S&L)
7. Treadway
8. COSO (Committee of Sponsoring Organizations)
9. Financial Executives International (FEI)
10. Institute of Management Accountants (IMA)
11. American Accounting Association (AAA)
12. AICPA
13. IIA
14. COSO Model
15. SAS No. 78—Consideration of Internal Control in a Financial Statement Audit.
16. Rachel E. Silverman, "GE Makes Changes in Board Policy," The Wall Street Journal (New York: November 2002 ,8).

منابع و ماخذ:

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

۲. سادوسکای، ج.، دمپزی، ج. ا.، گرین برگ، آ.، مک، ج. ب.،و شوارتز، آ. (۱۳۸۴). راهنمای امنیت فناوری اطلاعات. (م. میردامادی، ز. شجاعی،و م. صمدی، مترجم) تهران: دبیرخانه شورای عالی اطلاع رسانی.

۳. فخار، ب. (۱۳۸۹). ترجمه بخش نظارت بر فن آوری اطلاعات لوح آموزشی FSI-Connect (نسخه دهم) نوامبر ۲۰۰۹. تهران: بانک مرکزی جمهوری اسلامی‌ایران.