گامهای ۹گانه در آمادگی حسابرسی فناوری اطلاعات

استفاده از اتوماسیون داده‌ای برای عملکرد استثنا و نظارت

احمد عدالت

مقدمه‌ای بر آمادگی حسابرسی فناوری اطلاعات

با حضور فناوری اطلاعات و ارتباطات در کسب‌وکارها، ریسک جهانی و محیط نظارتی سازمانها به‌طور فزاینده‌ای در حال پیچیده‌تر شدن است و مهم‌تر این‌که سازمانها، دستگاه‌های تجاری، سیستمها، و ابرداده‌ها، در این تغییرها بیشتر در معرض خطر قرار دارند.

در این مقاله، ۹گام اصلی برای مدیریت ریسک و فعالیتهای مربوطبه انطباق، دقت، سرعت و استفاده از منابع کمتر، جهت بررسی «آمادگی حسابرسی فناوری اطلاعات» درنظر گرفته شده است. با دنبال‌کردن این گامها، حسابرسان می‌توانند کاهش ریسک و خطرهای حضور فناوری اطلاعات، کاهش پیچیدگی و چالشهای مدیریت فناوری اطلاعات را مدیریت و بینش مدیران اجرایی را نسبت به تغییرات فناورانه بهتر کنند.

چالشهای پیش‌روی مدیران فناوری اطلاعات

با توجه به صنعت دردست ارزیابی و محل اجرای حسابرسی، ترکیبی از مقررات و چارچوبهای منطبق با استانداردهای **اس‌اوایکس** (SOX)، **ای-۱۲۳** (A-123)، **اوام‌بی** (OMB)، **پی‌سی‌آی** (PCI)، **جی‌ال‌بی‌ای** (GLBA)، **اچ‌آی‌پی‌ای‌ای** (HIPAA)، **کوبیت** (COBIT)، **کوزو** (COSO)، **ایزو** (ISO)، **اس‌اوسی-۱** (SOC 1)، و **اس‌اس‌ای‌ایی ۱۶ از اس‌اوسی ۱** (SSAE 16 SOC 1)، همواره در پیش‌روی حسابرسان فناوری اطلاعات وجود دارد تا با استفاده از آن بتوانند ارزیابی و نظارت خود را در یک چارچوب مشخص انجام دهند. حسابرسان و متخصصان انطباق- چه حسابرسان داخلی و چه حسابرسان مستقل- بهتر است برای شناسایی مسائل کنترل مرتبط با حوزه فناوری اطلاعات، به بخش فناوری اطلاعات مراجعه کنند.

البته نباید فراموش کرد که گروه فناوری اطلاعات، گروهی پرکار است و محدودیت زمانی در اجرای فعالیتهای خود دارد؛ درنتیجه، چنین مراجعه‌هایی به‌طورکلی محدودیتهای بیشتری برای این گروه ایجاد می‌کند. با این حال نمی‌توان از حسابرسی عملکرد این گروه صرفنظر کرد؛ زیرا همواره خطرهای بسیار جدی و مهمی در این حوزه وجود دارد؛ خطرهایی همانند یک نقص امنیتی داده‌ها یا نقص یک برنامه کاربردی یا سیستم‌عامل که ممکن است آسیب عمده‌ای به سازمان وارد کند.

با توجه به تمام این مسئولیتها، ایده دستیابی و حفظ وضعیت آمادگی حسابرسی فناوری اطلاعات ممکن است یکی از گامهای مهم در صنعت حسابرسی تلقی شود. اما فرایندهایی وجود دارد که ممکن است نتایجی درخورتوجه از ارزیابی ریسکهای به‌روز و معنی‌دار، کنترلهای خوب مستندشده و مدیریت‌شده و کمترین یافته‌های مشکوک در حسابرسی را برای کارفرما به‌ارمغان آورد. مشکل این است که گامهای حسابرسی فناوری اطلاعات به‌دلیل دشواربودن، بیشتر ناخوشایند به‌نظر می‌رسد که این دیدگاه با بررسی «آمادگی حسابرسی فناوری اطلاعات» به کمترین حد می‌رسد.

مانند بسیاری از عملیات هرکسب‌وکار، اجرای فناوری مناسب ممکن است تفاوت بین موفقیت و شکست را به‌خوبی نشان دهد. بعضی سازمانها سعی می‌کنند ریسک فناوری اطلاعات، کنترلها و فرایندهای انطباق خود را با ابزار و فناوریهای عمومی مدیریت کنند. این موضوع نشان می‌دهد که آنها برای این کار ساخته نشده‌اند. اما حسابرسان فناوری اطلاعات با بررسیهای خود، به تغییرهای مورد نیاز سازمان در بخش مدیریت فناوری اطلاعات و فرایندهای انطباق در هنگام استفاده از فناوریهایی که به‌طور هدفمند ساخته شده‌اند، دست پیدا خواهند کرد. لذا برای دستیابی به این سطح از آگاهی، اجرای

این ۹ گام و تکمیل فهرست وارسی مربوط به هر گام ممکن است به حسابرس کمک شایانی در ارزیابیها و کشف شواهد کرده و مطمئن شود که ابزار مناسبی برای کار خود در اختیار دارد.

چرا فناوری اطلاعات نیاز به حسابرسی دارد؟

یکی از مهم‌ترین دلایل نیاز به حسابرسی فناوری اطلاعات، وجود فهرست طولانی قوانین و مقررات انطباق داخلی است که به‌طورکلی در حاکمیت قانون و دیوانسالاری ظاهر می‌شود. هرچند که الزامهای نظارتی و داخلی هر سازمانی موجب می‌شود که این دیوانسالاری کاهش یافته و سازمان در دستیابی به اهداف خود، بهتر اقدام کند. همچنین این الزامها موجب می‌شود تا از داراییها و سرمایه‌های شرکای عمومی و شخص ثالث سازمان محافظت گردد.

این واقعیت وجود دارد که در ارتباطات جهانی، کسب‌وکارها روزبه‌روز نیاز بیشتری به فناوری اطلاعات پیدا می‌کنند و در حال حاضر بسیاری از عملیات روزانه خود را با استفاده از این ابزار به‌انجام می‌رسانند. همچنین با توجه به گستردگی کارها و پیچیده‌شدن فعالیتها، سازمانها برای دستیابی به اهداف کلی و راهبردی خود، وابستگی زیادی به فناوری اطلاعات پیدا کرده‌اند. درنتیجه، ، اگر برخی فرایندها در فناوری اطلاعات اشتباه انجام شود، عواقب آن ممکن است فاجعه‌بار باشد. این فجایع را دنیا در شرکتهایی همچون **تارگت** (Target) و **سونی** (Sony) تجربه کرده است.

هدف از اجرای «آمادگی حسابرسی فناوری اطلاعات» این است که فرایندهای سازمانی بدون نقص عمل کنند. آمادگی حسابرسی به این معنی است که کنترلها از جمله کنترلهای مرتبط با فناوری اطلاعات، موثرتر عمل کرده تا گزارشهای مالی اعتمادپذیر و دقیق استخراج شوند.

سازمانها می‌باید توجه بیشتری را برای مدارک استخراج‌شده از مشاهده‌ها و گزارشهای «آمادگی فناوری اطلاعات» درنظر گرفته و زمان بیشتری صرف آماده‌شدن «حسابرسی فناوری اطلاعات» کنند. این موضوع موجب می‌شود تا اقدام موثری در زیرساختها و ارتقای سیستمهای کسب‌وکار رخ داده و سازمان مسیر توسعه را درپیش گیرد.

آماده‌سازی مدیران سازمانی

فرایند و فناوری دو بخش اصلی سازوکار توسعه سازمانی هستند. سومین عنصر ضروری، *نیروی‌انسانی* و به‌خصوص تصمیم‌گیران سازمان می‌باشند. راهکار «آمادگی حسابرسی» ممکن نیست موفقیت‌آمیز باشد؛ اگر تصمیم‌گیران سازمانی متوجه نشوند که چرا حسابرس عملیات «آمادگی حسابرسی» را انجام می‌دهد، یا اگر آنها آمادگی خرید براساس اهداف و فعالیتهای خود را که از بستر این اقدام منتج شده است، نداشته باشند.

درنتیجه، منطقی است که با ایجاد یک گروه متشکل از چندین متخصص در حوزه‌های مختلف، به طراحی و هدایت این فرایند کمک شود. از آنجاکه فناوری اطلاعات با بسیاری از جنبه‌های مختلف سازمان مرتبط می‌شود، پس باید برای گرداوری متخصصین هر حوزه، یک نماینده از حوزه‌های عملکردی همچون کنترل مالی، عملیات، حسابرس داخلی و خود فناوری اطلاعات (به‌عنوان مثال، متخصصین امنیت و اطلاعات) در گروه مشارکت کنند.

و در آخر، این اطمینان باید حاصل شود که عالی‌ترین فرد سازمان، آیا از اهداف «آمادگی حسابرسی» پشتیبانی می‌کند؛ کسی که می‌تواند بر موانعی که ممکن است بروز نماید، غلبه کند.

گام اول: شناسایی و ارزیابی ریسکهای فناوری اطلاعات

شروع کار با ریسکهایی که بیشترین تاثیر راهبردی در ماموریت اصلی سازمان را شامل می‌شوند، همچون ریسکهای قانونی، عملیاتی و کشف، آغاز می‌شود. این گام حیاتی است و در هسته روند مدیریت ریسک قرار می‌گیرد.

ارزیابی ریسک باید دارای یک روند مستمر در طول سال باشد؛ زیرا به وجود و اثربخشی کنترلهایی که برای رفع ریسکها وجود دارند، بستگی دارد (**جدول ۱**- شناسایی ریسکها).

جدول ۱- شناسایی ریسکها

برای شناسایی و ساختن فضای ریسک سازمان، ابتدا خطرها را بر اساس پیامدها طبقه‌بندی کنید؛ به‌عنوان مثال، فضا را به سه سطح زیر تقسیم کنید: **تاثیر عمده**: شکست سایبری منجربه سرقت پایگاه داده‌های کارفرما می‌شود؛ برای مثال، شکست پیاده‌سازی سیستم **برنامه‌ریزی منابع بنگاه** (ERP)، (در برخی از شرکتهای بزرگ ایران پیاده‌سازی این سیستم با شکست مواجه شد). **تاثیر متوسط**: جریمه ناشی از نقض قوانین تجارت الکترونیک و یا حق تالیف. **تاثیر کم**: تقلب کارکنان با استفاده از دسترسی‌های غیرمجاز.	سپس، ریسکها و خطرهایی که تاثیر نهفته‌ای در دستیابی به اهداف کلان و راهبردی سازمان دارند را باید به اهداف سازمان پیوند داد. به‌یاد داشته باشید که تاثیر ریسک و خطر همیشه باید: • از نظر توان درونی مالی و یا تاثیر موارد دیگر، کم باشد، • با توجه به احتمالها ارزیابی شود، • نسبت به سایر خطرها رتبه‌بندی شود.

ریسکهای جدید و خطرناک

این گام همچنین شامل یک روند مداوم شناسایی ریسکهای جدید و نوپدید است؛ زیرا تغییر، یک ویژگی ذاتی فناوری است. پس باید همواره از تغییر قوانین و مقررات فناوری باخبر بود و شرایط فرایند متاثر از فناوری را با وضع جدید انطباق داد.

این فرایند نیاز به ترکیبی از مهارتها و دانش تفکر انتقادی و تجزیه‌وتحلیل داده‌ها دارد؛ به‌طوری که به‌کمک آن بتوان تغییر روند ریسک و ریسک را کنترل کرد. از نمونه‌های آن که در مجموعه داده‌های الکترونیکی برای نشان‌دادن ریسکهای احتمالی فناوری اطلاعات وجود دارد، می‌توان به دسترسی به شبکه و پایگاه داده‌ها، دسترسی به جداول مجوزها و ثبت‌وقایع مربوط به انتقال پرونده، اشاره کرد.

چالشهای این گام

- اعتماد به این‌که ریسکها و الزامهای قانونی مورد نیاز در محدوده کاری، به‌اندازه کافی جامع باشد.
- عادی‌سازی و ارزیابی ریسکهای کشف‌شده در بخشهای مختلف با استفاده از روشهای متناقض و فناوریها.
- کمبود مجموعه‌ای از مقررات فناوری اطلاعات و الزامهای قانونی.
- به‌دست‌آوردن آگاهی در خصوص ریسکهای جدید و توانمند، بدون فناوری تجزیه‌وتحلیل.

الزامهای فناوری

- رتبه‌بندی و ریسک گزارش توسط معیارها و ابزار مختلف.
- مقایسه ریسکهای راهبردی نسبت به سایر ریسکها.
- ریسکهای مرتبط با اهداف راهبردی سازمان و مواردی که آنها را زیرتاثیر قرار می‌دهد.
- ریسکهای مرتبط با فناوری اطلاعات، ریسک و چارچوبهای انطباقی و نظارتی.
- ثبت توصیف ریسکها، دسته‌ها، رتبه‌های ارزیابی، تعریفها و احتمال.
- دسترسی و تجزیه‌وتحلیل طیف گسترده‌ای از پرونده‌های داده‌ای و سیستمی.
- تولید شاخص و آمار از ناهنجاریها و بی‌نظمیهای سیستمی.
- تهیه تجزیه‌وتحلیل تصویری جهت به‌تصویرکشیدن روند عوامل ریسک.

گام دوم: شناسایی کنترلها

ریسکهایی را که در گام اول شناسایی کرده‌اید، در این گام باید با کنترلهایی که احتمال وقوع ریسک را

کاهش می‌دهند، یا مانع آن می‌شوند، تطبیق دهید.

البته لازم نیست برای همه ریسکها کنترلی درنظر گرفته شود. ممکن است گاهی لازم باشد یک ریسک منفی در حال وقوع را بپذیرید، به‌خصوص زمانی که انتظار می‌رود هزینه کنترل موثر، بیش از احتمال درونی آن باشد. برای مثال، کنترل احتمال دسترسی غیرمجاز به ساعتهای کارکرد همکاران، هزینه‌ای هنگفت را بر سازمان تحمیل می‌کند و با توجه به کم‌ارزش‌بودن این اطلاعات در برخی از سازمانها، کنترل مربوط درنظر گرفته نمی‌شود. در حقیقت، در این فرایند باید ریسک‌پذیری سازمان را درنظر گرفت؛ یعنی سطح اولویتی که توسط مدیریت عالی سازمان تعیین و تعریف شده است (**جدول ۲**- مثال کنترل).

جدول ۲- چند مثال کنترل

- تنظیم دیواره‌های آتش جهت جلوگیری از دسترسی به سیستمهای خارجی.
- تهیه جداول مجوز و دستیابی، جهت محدود کردن قابلیتها و امکانات سیستمی دراختیار کاربر.
- تعیین روشهای کاهش احتمال شکست در پروژه‌های جدید توسعه سیستم.

در این گام، کنترلها و فرایندهای کاهش ریسک (آنهایی که در محل کارفرما بوده و در حال اجرا هستند) تعریف و مستند می‌شوند. همچنین، هزینه‌های اجرا و رسیدگی ارزیابیها ممکن است با استفاده از یک کنترل، تخمین زده شود. توضیحها و اسناد کنترل باید به‌اندازه کافی برای حمایت از حسابرسی و بررسی مستقل، دقیق باشد.

چالشهای این گام

- همانند گام اول، عمده‌ترین چالش این گام پیدا کردن و بررسی تمام کنترلهای کاهش‌دهنده ریسک منابع سازمانی است که ممکن است دشوار و خسته‌کننده باشد.

الزامهای فناوری

- کنترلهای ثبت‌شده باید در چارچوبی مدیریت‌شده و با قابلیت استفاده مجدد، همراه با جزئیات کافی، طراحی شوند تا برای پشتیبانی از روندهای حسابرسی و ارزیابی (برای مثال پشتیبانی از متن، گرافیک، نمودار جریان

و ...) به‌طور مستمر بتوان از آنها استفاده کرد.

- تهیه نقشه کنترلها به‌ازای هر ریسک (در هر دو سطح راهبردی و فرایند).
- به‌سادگی، مدیریت تغییر برای به‌روزرسانی کنترلها به‌طور مرکزی و به‌روش آبشاری (از بالا به پایین) برای الگوهای مختلف پروژه‌های فناوری اطلاعات باید فعال شود. همچنین حسابرسان داخلی یا مستقل نیز جهت بررسی، امکان تغییر داشته باشند.

گام سوم: ایجاد نقشه کنترلها در یک قالب اصلی کنترل

این گام به‌طور دقیق به روند شناسایی کنترلهای کاهش‌دهنده ریسک مرتبط می‌شود؛ به‌طوری که آنها را در صورت امکان به نقشه کلی ساختار کنترل متصل کند. در این گام، ساختاری برای ارتباط بین کنترلها، صاحبان کنترل و الزامهای قانونی فراهم می‌شود. درنتیجه، چارچوبها و قالبهای کنترل شخص ثالث، جهت انعکاس شرایط جدید و مقررات قانونی و همچنین تشخیص بهترین روشهای کنترل به‌طور مستقل نگهداری و به‌روز می‌شوند.

چالشهای این گام

- مطمئن‌بودن نسبت به‌این‌که ریسکها و الزامهای قانونی تهیه‌شده، به‌اندازه کافی جامع و کامل است.
- عادی‌سازی و ارزیابی ریسکهای شناسایی‌شده در بخشهای مختلف، با استفاده از روشهای ارزیابی و فناوری.
- دراختیارداشتن مجموعه‌ای از مقررات به‌روز فناوری اطلاعات و الزامهای تطبیقی.
- به‌دست‌آوردن آگاهی در خصوص ریسکهای درونی جدید بدون فناوری تجزیه‌وتحلیل.

الزامهای فناوری

- رتبه‌بندی و گزارش ریسکها با استفاده از معیارهای مختلف.
- امکان مقایسه ریسکهای راهبردی نسبت به سایر ریسکها.
- ارتباط ریسکها با اهداف راهبردی و تاثیر آنها بر فرایندها.
- پیوند با الزامهای قانونی و نیازمندیهای تطبیقی.
- ارتباط با فناوری اطلاعات، ریسک یا چارچوب نظارتی و تطبیقی.
- ثبت توصیف ریسکها، دسته‌ها، رتبه‌های ارزیابی، تعریفها و احتمال.
- دسترسی و تجزیه‌وتحلیل طیف گسترده‌ای از پرونده‌های داده‌ای و سیستمی.

- تولید شاخص و آمار از ناهنجاریها و بی‌نظمی سیستمی.
- تهیه تجزیه‌وتحلیل تصویری جهت به‌تصویرکشیدن روند عوامل ریسک.

گام چهارم: برنامه‌ریزی، تعیین محدوده کاری و ریسکهای آزمون خطای فرایند محور با کنترل

کنترلها برای رفع ریسکها و خطرهای بسیاری از فرایندها و بخشهای مختلف آن طراحی شده‌اند، به‌همین خاطر، ممکن است به‌طور فزاینده‌ای فرصتها و آسیب‌پذیریهای مربوط را منعکس کنند. بخشی از مدیریت موثر ریسک، شناختن این موضوع است که آیا می‌توان یک ریسک خاص را پذیرفت و یا این‌که تا چه اندازه در اجرای کنترل اقدام کنیم.

گاهی، هزینه کاهش ریسک ممکن است احتمال آسیب را بیشتر کند؛ اما برای مدیریت موثر آن باید به‌طور مرتب میزان ریسکهای مربوط به کنترلهای طراحی‌شده را ارزیابی کرد. همچنین باید بتوان تاثیر ارتباط کلی ریسکهای پذیرفته‌شده و نبودکنترل را به مدیریت ارشد به‌صورت صفحه‌نمایش، ارائه داد.

چالشهای این گام

- تهیه و فراهم کردن میزان ریسک فناوری اطلاعات سازمان.
- اگر یک ریسک فرایندی، با احتمال بالا در وضعیت نامناسبی تشخیص داده شده، باید بررسی کرد که آیا اقدام مناسبی برای آن درنظر گرفته شده است؟
- درک خطرهای ناشی از کنترلی که ممکن نباشد در سازمان انجام شود.
- وجود تناقض در داده‌ها و گامهای اساسی برای یکدست‌کردن و ارائه گزارش ریسک کلی و تصویر کنترل.

الزامهای فناوری

- اهمیت‌دادن به ارزیابی و اثربخشی کنترلهای فناوری اطلاعات که برای کاهش ریسک سطح فرایندی طراحی شده‌اند.
- گرداوری، ترکیب و نرمال‌کردن داده‌ها از منابع مختلف.
- تعیین میزان ضمانت ریسک توسط کنترل، هدف کنترل و طرح فناوری اطلاعات.

گام پنجم: ارزیابی اثربخشی کنترلهای موجود

بخش عمده‌ای از آمادگی حسابرسی براساس اطمینان به‌دست‌آمده از درستی عملکرد کنترلها به‌وجود می‌آید. در صورتی تجزیه‌وتحلیل داده‌ها یک اقدام اصلی محسوب می‌شود که به‌ارزیابی اثربخشی کنترل بپردازد.

بنابراین، می‌توان کل مجموعه داده‌ها را بررسی کرده و مورد آزمایش قرار داد تا بتوان متوجه شد چه اتفاقهایی در طی یک دوره مشخص برای فرایند مورد ارزیابی رخ داده است.

کنترلها، همچنین ممکن است با استفاده از پرسشنامه‌های منظم توسط کارفرما ارزیابی شوند. در برخی موارد، فعالیتهای کارفرما ممکن است بخشی از فرایند صدور گواهینامه‌ای باشد که به‌امضای مدیریت ارشد رسیده و در اجرای سیستمهای کنترل موثر کمک می‌کند. ارزیابیهای کنترل به‌طور معمول به‌صورت دوره‌ای انجام می‌شود. با این حال، باید در رابطه با گام ششم، که در آن کنترلهای اصلی با استفاده از روشهای خودکار در حال نظارت هستند، مورد توجه قرار گیرد.

چالشهای این گام

- تعیین این‌که آیا کنترلها به‌درستی عمل می‌کنند یا نه.
- تعیین این‌که کنترلهای طراحی‌شده در ارزیابی نادیده گرفته شده و یا به‌عمد مورد توجه کافی قرار نگرفته‌اند.
- پیگیری این‌که چه کسی مسئول و پاسخگوی چه کنترلی است و اطمینان از این‌که آن کنترل رها نشده باشد.

الزامهای فناوری

- تجزیه‌وتحلیل و خودکار کردن نظرسنجیها و پرسشنامه‌ها.
- تجسم داده‌های گرداوری‌شده در بسیاری از آزمایشها برای روشن‌شدن غلطگیرها.
- گرداوری الکترونیکی داده‌های مربوط به فرضهای انجام شده در بسیاری از آزمایشها جهت رفع ناهنجاریها.
- انجام آزمایشهای متعدد جهت شناسایی نواقص عملکردی کنترل.

گام ششم: بررسی، ردیابی و گزارش کمبودها

هنگامی که نقص هر یک از کنترلها شناسایی شدند، مهم است که به‌سرعت برای رفع اشکال اقدام شده و فرایند کنترل بهبود یابد. در بسیاری از موارد، تجزیه‌وتحلیل داده‌های تکراری ممکن است برای تقویت کنترل یا ایجاد یک لایه کنترل اضافی، استفاده شود.

به‌عنوان مثال، اگر کنترلهای «دسترسی به اطلاعات حساس» به‌طور کامل موثر نباشد، تجزیه‌وتحلیل منظم داده‌ها ممکن است جهت شناسایی نمونه‌هایی از دسترسیهای پرمخاطره، اجرا شود. با شناسایی زودهنگام دسترسیهای پرمخاطره به داده‌ها، می‌توان پیش از آن که این دسترسی به یک مشکل بزرگ تبدیل شود، آن را کنترل کرد.

چالشهای این گام

- کنترل واقعا موثر است؟
- مقاومت افرادی که «تنها می‌خواهند کار را انجام دهند» و کنترلها را دور می‌زنند.

الزامهای فناوری

- ایجاد مرکز پاسخدهی به کمبودها و مشکلات کنترلها و پیگیری آن با عنوان **میزکمک**[۱].
- شناسایی تراکنشهای اطلاعاتی پرریسک با توجه به حجم وسیع معیارهای آزمون.

گام هفتم: نظارت و خودکارشدن آزمون کنترل

تمام گامهای موجود در فرایند «آمادگی حسابرسی» مهم هستند، از نظارت یک جزء حیاتی در فرایند سازمانی گرفته تا ارزیابیِ به‌لحظه اثربخشی مدیریت ریسک موجود و کنترل فعالیتهای موجود در فناوری اطلاعات. همچنین خودکارشدن آزمون کنترل ممکن است به شناسایی شاخصهای خطرهای جدی و مهمی که در حال حاضر هیچ کنترلی ندارند، کمک کند.

تجزیه‌وتحلیل داده‌ها به‌تقریب در همه موارد مربوط به آزمون کنترلها و ارزیابی ریسکها، موثر است. همچنین باید فرمهایی مشابه فرم نتایج تجزیه‌وتحلیل داده‌ها تهیه کرد تا به‌طور مرتب و مستمر، و در دوره‌های روزانه، هفتگی و ماهانه، اطلاعات مفیدی برای حسابرس فناوری اطلاعات و سازمان به‌دست آورد (**جدول ۳**).

جدول ۳- تجزیه‌وتحلیل فرایند نظارت

تجزیه‌وتحلیل فرایند نظارت را می‌توان برای بسیاری از فعالیتهای فناوری اطلاعات مطابق موارد زیر اعمال کرد	
• تعیین سطح دسترسی در حد مدیریت سیستم و دسترسی به سیستمهای خاص، • نظارت بر جداسازی وظایف، • کنترل بر ابطال و یا تغییر داده،	• تغییر دیوار آتش، • تغییر اطلاعات حساس، • ثبت تغییرات شبکه، • ثبت دستیابی فیزیکی.

چالشهای این گام

- تهیه و فراهم‌کردن میزان ریسک فناوری اطلاعات سازمان
- در صورتی که یک ریسک فرایند با احتمال بالا ارزیابی شود، به‌سرعت اقدام مناسب انجام شود.
- شناسایی ریسک ناامن در سازمان اگر کنترل آن با خطا مواجه شود.
- تناقض در داده‌ها و تلاش مضاعف جهت تهیه گزارش ریسک مهم و طراحی کنترل مربوط.

الزامهای فناوری

- دستیابی و سنجش اثربخشی کنترلهای فناوری اطلاعات که برای کاهش سطح ریسک فرایندهای سازمان طراحی شده‌اند.
- گرداوری، ادغام و نرمال‌کردن داده‌ها از منابع مختلف.
- تعیین میزان ضمانت ریسک توسط کنترل، هدف کنترل و طرح فناوری اطلاعات.

گام هشتم: شناسایی موارد استثنا، بازنگری، بررسی و اصلاح آنها

گام قبلی، نظارت و کشف شاخصهایی بود که مشکلهای بالقوه فرایندها و کارآمدی کنترلهای مربوط به آن را نشان می‌داد و این‌که یک خطر تا چه میزان ممکن است افزایش یابد.

در این گام، به تعیین خط قرمزهای یک فرایند که توسط افراد آگاه مشخص می‌شود، نیاز داریم. افرادی که با ساختار فرایند آشنا بوده و کنترلهای مربوط به آن را می‌دانند. در طول این کار، مدیریت استثنا و یا مدیریت عملکردی حوزه مورد بررسی، جهت تعیین خط قرمزها درنظر گرفته می‌شوند. باید به یاد داشت که برخی از خط قرمزها، مثبت کاذب هستند، در حالی که برخی دیگر ممکن است نشان‌دهنده اختلال کنترل باشند، اختلالی که نیاز به اصلاح کنترل دارد.

این عمل ممکن است شامل شناسایی مشکل اتفاق افتاده (مانند مواجه‌شدن با دسترسی غیرمجاز کارکنان به اطلاعات حساس) و یا تنظیم کنترل و کاهش احتمال رخدادن مجدد مشکل باشد. بسیاری از وضعیتهای غلط را می‌توان با آزمون سازگاری و تنظیم شرایط تجزیه‌وتحلیل داده‌ها، برای موارد غیرخطرناکی که گزارش نشده، تخمین زد.

چالشهای این گام

- مدیریت عملکرد کنترل، به‌خصوص در مورد حجم وسیعی از قوانین و مقررات حوزه فناوری اطلاعات ممکن است دارای مشکل باشد.

- حجم زیادی از نتایج مثبت کاذب ممکن است منجربه چشم‌پوشی در شاخصهایی شود که در آن یک مشکل واقعی کنترل وجود دارد.
- حجم زیادی از موارد استثنای ایجادشده در سیستمهای چندگانه ممکن است موجب انباشت مشکلها و فشردگی کارها برای مدیریت شود.
- اگر نقاط ضعف کنترل و تراکنشهای خطرناک شناسایی شده اما مورد توجه قرار نگیرند، مدیریت از میزان مشکلهای ناشناخته بی‌اطلاع خواهد بود.

الزامهای فناوری

- آزمون رویه‌ها و فرایندها را تهیه کنید تا فعالیتهای کم‌خطر و یا بدون‌خطر به‌عنوان استثنا گزارش نشوند.
- به‌راحتی روشهای گردش کار را ایجاد و اصلاح کنید.
- به‌طور خودکار شرایط استثنا و تراکنشهای خطرناک را برای بازنگری مدیریت ارشد به صورت داشبوردی ایجاد کنید.
- گزارشی جهت نمایش وضعیت فعالیتهای مدیریت استثنا ایجاد کنید.
- گزارشی مبنی‌بر میزان خطر موجود براساس نتایج بدست آمده از تحقیق موارد استثنا را تهیه کنید.

گام نهم: بهبود مستمر فرایندهای کنترل و نظارت

با گذشت زمان، خطرها کاهش می‌یابد و کل فرایند کنترل، از طریق یک چرخه مستمر آزمون، نظارت کنترلها و رفع مشکلات استثنا، بهبود می‌یابد.

پس از اجرای آمادگی حسابرسی فناوری اطلاعات، احتمال یافته‌های حسابرسی ناچیز شده و به میزان قابل‌توجهی کاهش می‌یابد؛ به‌طوری که مجموعه فناوری اطلاعات سازمان هنگامی که تحت بررسی و تطابق عملکرد حسابرسی داخلی یا مستقل قرار می‌گیرد، نکته قابل‌توجهی در آن وجود ندارد.

چالشهای این گام

- مدیریت تمام بخشهای منتقل‌شده دشوار است؛ درنتیجه، تمرکز باید روی بیشترین ریسکهای معنی‌دار و کنترلهای مهم قرار بگیرد.
- استفاده از روشهای دستی و یا صفحه‌های گسترده همچون اکسل، ممکن نیست روی میلیونها و میلیاردها تراکنش، به‌خوبی عمل کند.

الزامهای فناوری

- پشتیبانی از تمام گامها در ارزیابی ریسک / کنترل و نظارت بر فرایند.
- ایجاد گزارشهایی که بتواند نگرش جامعی از وضعیت آمادگی حسابرسی در کل زیرساختهای فناوری اطلاعات، ارائه دهد.

گام اضافی: روند پیش‌بینی ریسک فناوری اطلاعات

با طی‌شدن گامهای یادشده، آمادگی حسابرسی به‌دست می‌آید. در حقیقت با انجام گام‌به‌گام هر یک از این گامها، گروه حسابرسی مطمئن می‌شود که سیستمهای کنترل فناوری اطلاعات به‌درستی عمل کرده و گزارش نتایج حاصل از کل فرایند را ممکن است تهیه کند. در حقیقت پس از حسابرسی فناوری اطلاعات و اطمینان از این‌که زیرساختهای فناوری اطلاعات به‌درستی عمل می‌کنند، حسابرسان می‌توانند با آسودگی خاطر به حسابرسی صورتهای مالی بپردازند. این نتایج را می‌توان با استفاده از یک داشبود الکترونیکی نشان داد و شواهد تصویری و قابل اندازه‌گیری از روشهای تجزیه‌وتحلیل و آزمونهای انجام‌شده همراه با نتایج آن برای ذینفعان حسابرسی را ارائه کرد.

گزارشهای کاربردی و بسیار مفید آمادگی حسابرسی الکترونیکی در قالب یک داشبورد، مسائل مربوط به ریسک و کنترل را با معیارهایی مانند محدوده کاری، عملکرد کسب‌وکار یا اقدامهای مدیریتی، طبقه‌بندی می‌کنند. علاوه‌بر آن، گزارشهای داشبوردی ممکن است نقاط بحرانی فناوری اطلاعات که نیاز به اقدام فوری دارند را قبل از هر اتفاق منفی، به نمایش درآورد.

چالشهای این گام

- گزارش داشبوردی از طریق گرداوری اطلاعات از منابع مختلف سازمان باید تهیه و به‌گونه‌ای ارائه شود که برای سطوح فنی و مدیریت ارشد، قابل لمس باشد.
- تهیه متنها و مسائل مربوط به ریسک و کنترل سخت است؛ به همین خاطر، ماهیت و میزان فعالیتهای نظارت و آزمون بدون فناوری تخصصی، کاری دشوار است.

الزامهای فناوری

- گرداوری داده‌ها در خصوص ماهیت و حجم فعالیتهای آزمون، نتایج و پیگیری پاسخها.
- گزارش جامع در مورد وضعیت فعالیتهای انجام‌شده، از جمله میزان سنجش آزمونها، نتایج و پاسخها.
- ایجاد ارتباط بین آزمونها و داده‌های پاسخ با ریسک و کنترلهای اساسی.

گام آخر: ادغام فرایندهای مدیریت ریسک فناوری اطلاعات در مدیریت ریسک سازمانی

در انتها باید بدانیم که هدف اصلی از دستیابی به آمادگی حسابرسی فناوری اطلاعات، مدیریت بهتر مسئولیتهای کنترل و نظارت اداری است. به‌عبارت دیگر، منطقی است که فرایندهای فناوری اطلاعات برای مدیریت ریسک، کنترل و انطباق را در قیاس با چارچوب فعالیتهای مدیریت ریسک کل سازمان و شرکتهای بزرگ‌تر، قرار دهیم.

با درنظر گرفتن یک رویکرد جامع، مدیریت عالی سازمان می‌تواند خطرها و ریسکهای فناوری اطلاعات را در کنار دیگر گروه‌های ریسک سازمانی، مورد توجه قرار دهد. یکی دیگر از مزایای استفاده از یک رویکرد جامع و یکپارچه، این است که چگونگی ارتباط بین ریسکها و کنترلها را به سادگی نمایان می‌سازد. ریسکهای فناوری اطلاعات را به‌ندرت می‌توان از دیگر ریسکهای سازمانی جدا دانست و اغلب این ریسکها به‌همراه ریسکهای کنترل سیستمهای مالی و عملیاتی درنظر گرفته می‌شود.

چالشهای این گام

- بخشهای مختلف درگیر با مدیریت و کنترل ریسک یک سازمان ممکن است مسائل مربوط به ریسک و کنترل را از طریق روشهای مختلف ارزیابی کند. که این موضوع مشکلی برای مدیریت در دستیابی به یک تصویر جامع از مقایسه‌های معنی‌دار در سازمان را ممکن است به‌وجود می‌آورد.
- سازمانها ممکن است از فناوری و روشها و رویکردهای مختلفی برای ارزیابی مسائل مربوط به ریسک/ کنترل و آمادگی حسابرسی در بخشهای مختلف خود استفاده کنند.
- ایجاد یک دیدگاه جامع از آمادگی حسابرسی در تمامی بخشهای سازمان، کار آسانی نیست.

الزامهای فناوری

- تشریح گسترده از فعالیتهای مختلف حسابرسی، ریسک و کنترل در بخشهای مختلف سازمان.
- ادغام با سایر فناوریهای مدیریت ریسک و کنترل.

سخن آخر

آمادگی حسابرسی فناوری اطلاعات اقدامی است برد-برد؛ به همین دلیل است که اجرای صحیح و استفاده مناسب از فناوری، ارزش پیدا می‌کند.

این ۹ گام و دو گام پایانی آن، به گروه حسابرسی فناوری اطلاعات کمک می‌کند که فرایندهای خسته‌کننده

و ناکارآمد را به اقدامی تبدیل کنند که نیاز به تلاش کمتری داشته و به‌طور قابل‌توجهی هزینه‌های کلی منابع سازمانی را کاهش دهد.

بسیاری از فناوریهای موجود، فرایند امنیت و کنترل فناوری اطلاعات را پشتیبانی می‌کنند؛ اما یکی از بزرگ‌ترین چالشها، مدیریت جامع و یکپارچه کل فرایندهای سازمانی است که به‌صورت سازگار بتواند یک دید کلی ازوضعیت ریسک فناوری اطلاعات و انطباق آن با طیف وسیعی از دیگر فرایندهای سازمانی را نشان دهد.

پانوشتها

1- Help Desk

منبع:

Ebook: **9 Steps IT Audit Readiness; Wegalvanize.com;** ©2019 ACL Services Ltd.