شماره: ۸۹/۲۵۲۰۶۶
تاریخ: ۱۳۸۹/۱۱/۱۶
پیوست: دارد

بانک مرکزی جمهوری اسلامی ایران

بسمه تعالی

جهت اطلاع مدیران عامل محترم کلیه بانک‌های دولتی و غیردولتی، شرکت دولتی پست بانک، مؤسسه اعتباری توسعه، دیوان محاسبات کشور، سازمان بازرسی کل کشور، جامعه حسابداران رسمی ایران، سازمان حسابرسی و پژوهشکده پولی و بانکی ارسال می‌گردد.

با سلام؛

احتراماً، همان‌گونه که مستحضر می‌باشند فناوری اطلاعات و ارتباطات به عنوان یکی از مهم‌ترین چالش‌های دهه‌های اخیر سازمان‌ها، مؤسسات و شرکت‌های دولتی و خصوصی مطرح بوده و از طرف دیگر به منظور تسریع در رسیدن به اهداف و جنبه‌های رقابتی بازار، مالکان و مدیران سازمان‌های مختلف به خصوص بانک‌ها را در بکارگیری و توسعه سامانه‌های فناوری اطلاعات تشویق می‌نماید. بدیهی است بخش فناوری اطلاعات در هر سازمانی به عنوان مهم‌ترین و حساس‌ترین بخش آن نهاد شمرده شده و آگاهی از چگونگی عملکرد این بخش از الزامات نظارتی به شمار می‌آید. بنابراین شناخت کلی از نقش فناوری اطلاعات و ارتباطات و چگونگی ارزیابی عملکرد آن از الزامات اصلی و اولیه برای بازرسان و حسابرسان سازمان‌ها و مؤسسات می‌باشد.

با عنایت به مراتب فوق و جهت آگاهی و شناخت نسبت به مفاهیم نظارت بر فناوری اطلاعات بانک‌ها، یکی از جزوات آموزشی مربوط به آموزشکده FSI-Connect که زیر نظر کمیته نظارت بانکی بال فعالیت می‌نماید ترجمه گردیده است که جهت استحضار و بهره‌برداری لازم تقدیم حضور می‌گردد.

جزوات آموزشی مرتبط دیگری نیز در دست بررسی و ترجمه است که نقطه نظرات و پیشنهادات آن بانک/مؤسسه اعتباری/سازمان/جامعه، قطعاً به ارائه بهینه جزوات آتی کمک شایان توجهی خواهدنمود./۷۲۰۶۱۵/ف

اداره مطالعات و مقررات بانکی

امیرحسین امین‌آزاد ۳۸۱۶

بهزاد فخار ۳۸۳۱-۱

تهران- بلوار میرداماد- شماره ۱۴۴، تلفن: ۲۹۹۵۱

صندوق پستی: ۷۱۷۷/۱۵۸۷۵، فاکس: ۶۶۷۲۵۶۷۴، سایت اینترنتی: www.cbi.ir

بانک مرکزی جمهوری اسلامی ایران

مدیریت کل مقررات، مجوزهای بانکی و مبارزه با پولشویی

اداره مطالعات و مقررات بانکی

نظارت بر فن آوری اطلاعات بانکها

ترجمه بخش نظارت بر فن‌آوری اطلاعات لوح آموزشی FSI-Connect (نسخه دهم) نوامبر ۲۰۰۹

ترجمه : بهزاد فخار

۱۳۸۹

فهرست مطالب

پیشگفتار

یکی از مفاهیم جدید پیش روی سازمانها، موسسات و شرکتهای دولتی و خصوصی، فن‌آوری اطلاعات و چگونگی استفاده از آن به منظور تسریع در رسیدن به اهداف و جنبه های رقابتی بازار است که صاحبان و مدیران بخشهای مختلف را تشویق در بکارگیری و توسعه سامانه های فن‌آوری اطلاعات مینماید. از اینرو قسمت فن‌آوری اطلاعات در هر سازمانی به عنوان مهمترین و حساس ترین بخش آن نهاد شمرده شده و آگاهی از چگونگی عملکرد این بخش از الزامات نظارتی به شمار می‌آید. بنابر این شناخت کلی از نقش فن‌آوری اطلاعات و چگونگی ارزیابی عملکرد آن از ضروریات دست اندرکاران سازمانها، موسسات و شرکتها می باشد. این نوشتار سعی دارد مفاهیم کلی مولفه ها و عملکردهای فن‌آوری اطلاعات را بیان و نحوه نظارت و حسابرسی فن‌آوری اطلاعات را به تشریح به صورت عملی ارائه نماید.

در پایان این نوشتار شما با مطالب زیر آشنایی پیدا خواهید کرد:

- توصیف ویژگی های پنج عملکرد اصلی فن‌آوری اطلاعات.
- مفاهیم اجمالی کنترل های داخلی و روش هایی که بانک ها باید به طور موثر جهت مدیریت ریسک های ناشی از فن‌آوری اطلاعات اتخاذ نمایند.
- تعریف اجزای برنامه موثر نظارت بر فن‌آوری اطلاعات

پیش نیازها

به منظور کسب حداکثر فایده از این نوشتار، شما باید با مبانی بانکداری و مدیریت ریسک آشنایی داشته باشید. شما می توانید موضوعات مربوطه را در زمینه بانکداری و ریسکهای بانکی در کتب مختلف و یا از طریق سایت FSI Connect دنبال نمایید.

مقدمه

بانک ها و سایر موسسات مالی با شتاب زیادی در پی استفاده از صنعت فن‌آوری اطلاعات هستند. حوادث اخیر یادآور خوبی هستند که نشان میدهند بانکها با چالشهای عمده ای در حفظ و تداوم ارائه خدمت به مشتریان خود روبرو می باشند. امروزه تقریبا اغلب فعالیت های بانکی به صورت خودکار بوده و بسیاری از معاملات به صورت الکترونیکی و بدون تبادل وجه نقد ویا ارائه مدارک کاغذی انجام می شوند.

تراکنش‌ها، ذخیره سازی اطلاعات، پردازش ها و نقل وانتقال به شیوه الکترونیکی با استفاده از سیستم های اطلاعات و سامانه های فن‌آوری اطلاعات صورت می پذیرد. علاوه بر این ، بانک ها جهت تدوین استراتژیها و اتخاذ تصمیمات مدیریتی خود به طور مداوم متکی به سامانه های اطلاعات الکترونیکی هستند. در حقیقت، مدیریت عملا در همه جوانب فعالیت‌های بانکی وابسته به فن‌آوری اطلاعات است. بنابراین تهدیدهای ریسکی و امنیتی ناشی از قابلیت های الکترونیکی از طریق منابع داخلی و خارجی افزایش یافته‌اند. نکته با اهمیت، ضرورت مواجهه و تلاش در جهت کاهش ریسک های فن‌آوری اطلاعات توسط مدیریت ریسک بانکها است.

آزمون دانسته ها

قبل از مطالعه این نوشتار آگاهی های خود را در زمینه فن‌آوری اطلاعات بررسی کنید تا دریابید که در حال حاضر چقدر با ریسک های فن‌آوری اطلاعات و اقدامات بانک ها برای کاهش این ریسک‌ها آشنایی دارید. این آزمون کوتاه شما را با برخی از سر فصلهایی که در این نوشتار ارائه شده است، آشنا می‌سازد. به خاطر داشته باشید که پاسخ صحیح شما به سوالات به معنای آگاهی شما از تمامی موضوعات ارائه شده در این نوشتار نیست.

کدامیک از موارد زیر وظیفه نگهداری از تجهیزات فن‌آوری اطلاعات را بر عهده دارد؟

۱- توسعه و اکتساب
۲- مدیریت عملیات و پشتیبانی
۳- تداوم کسب و کار / بازیابی موارد آسیب دیده
۴- مدیریت امنیت
۵- برون سپاری فن‌آوری اطلاعات

پاسخ: موارد ۱و۲و۳

کدام یک از ریسک های زیر مربوط به ریسک های فن‌آوری اطلاعات است؟

۱- ریسک های استراتژیک
۲- ریسک های بانکی
۳- ریسک شهرت

پاسخ: موارد ۱و۳و۴

۴- ریسک های قانونی

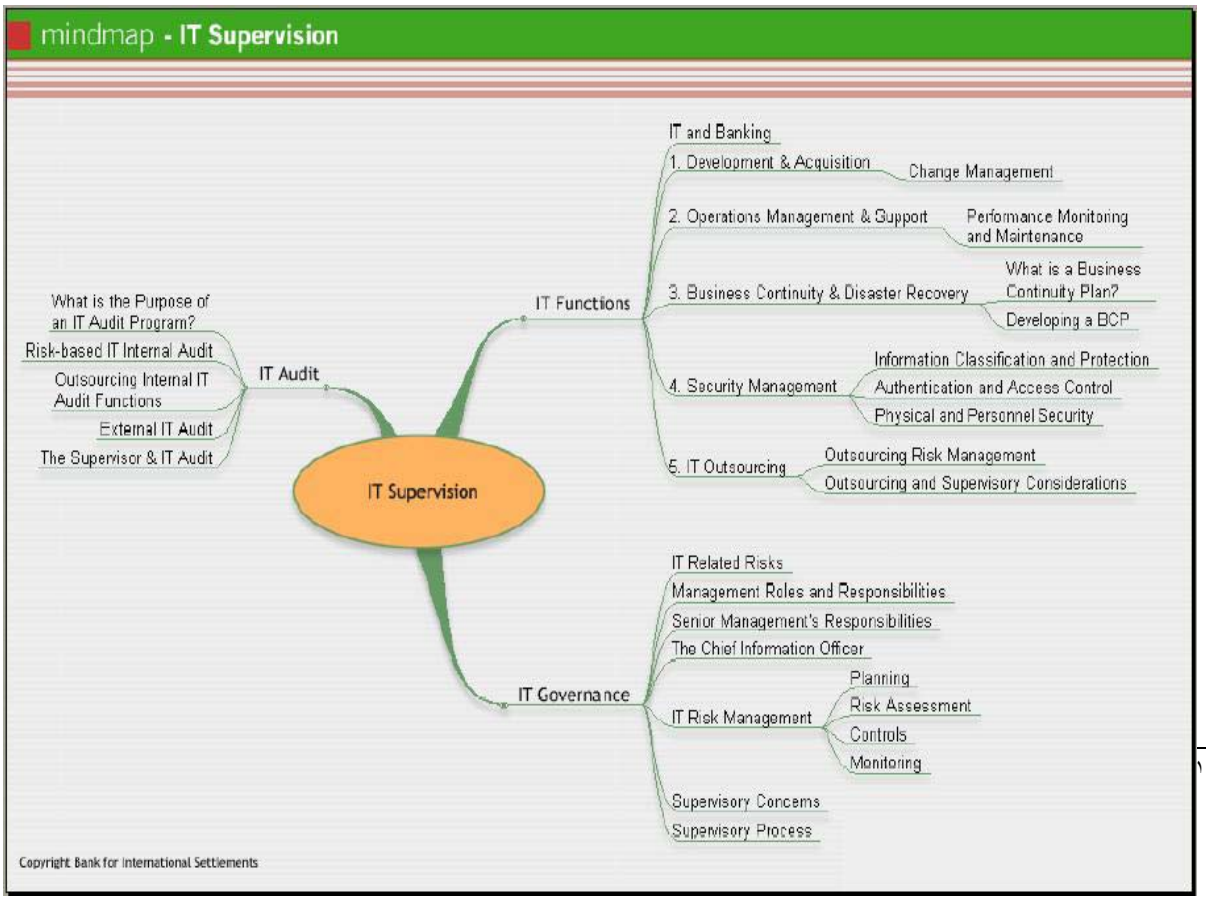
۵- ریسک های ترکیبی[۱]

هنگام بررسی عملکرد حسابرسی داخلی فن‌آوری اطلاعات بانک، کدامیک ازموارد زیر ممکن است مورد توجه قرار گیرد؟

پاسخ: موارد ۱و۳و۴و۵و۶

۱. استقلال عمل حسابرسی.
۲. محل کار حسابرسی در ساختمان فن‌آوری اطلاعات مستقر است .
۳. تخصص و تعداد پرسنل حسابرسی به محیط فن‌آوری اطلاعات وابسته است.
۴. دامنه حسابرسی فن‌آوری اطلاعات.
۵. فرآیند اطمینان از روند پیگیری و حل به موقع نقاط ضعف گزارش شده.
۶. مستندات مراحل حسابرسی فن‌آوری اطلاعات.

در نمودار زیر به صورت اجمالی دامنه نظارت بر فن‌آوری اطلاعات ترسیم شده است که هر یک از آنها در فصول سه گانه به تفصیل مورد بررسی قرارگرفته اند:



فصل اول :

وظایف و عملکردهای فن‌آوری اطلاعات

بانکداری و فن‌آوری اطلاعات

فن‌آوری اطلاعات را میتوان استفاده از رایانه به منظور دریافت، ضبط و نگهداری، پردازش و توزیع اطلاعات تعریف نمود. در قرن حاضر استفاده از فن‌آوری اطلاعات در بانکداری فراگیر و ضروری است. امروزه ،با توجه به اینکه داده ها در پایگاههای اطلاعاتی الکترونیکی ذخیره می شوند ،هنگام بروز هرگونه مشکلی که منجر به از کار افتادن سامانه های فن‌آوری اطلاعات گردد، تعداد معدودی از بانک ها می توانند به سرعت اطلاعات دقیق مربوط به حساب سپرده مشتریان خود را ارائه نمایند.

فشارهای رقابتی و در دسترس بودن راه حل های فنی، بانکها و دیگر موسسات مالی را مجبور می سازد تا به شدت به فن‌آوری های جدید وابسته گردند.

در حال حاضر در اکثر موسسات بانکی، مسئولیت طراحی ، مدیریت و نگهداری از سیستم های کامپیوتری و زیرساخت های فنی را بخش فن‌آوری اطلاعات بعهده دارد. در ادامه جزئیات بیشتری از پنج عملکرد عمده فن‌آوری اطلاعات بررسی می گردد:

عملکرد اول: توسعه و تملیک

عملکرد توسعه و تملیک به عنوان توانایی شناسایی، اکتساب، نصب و نگهداری مناسب سیستمها و تجهیزات فن‌آوری اطلاعات تعریف شده است .

Development

Acquisition

پروژه توسعه شامل ایجاد برنامه های نرم افزار کاربردی، و همچنین بسط و توسعه برنامه های کاربردی یکپارچه می‌گردد. توسعه پروژه های نرم افزار می تواند در داخل موسسه، یا بصورت برون سپاری و یا استفاده از ترکیبی از هر دو مورد باشد.

تملیک جایگزین پروژه های توسعه در داخل شرکت بوده که شامل خرید سیستم های سخت افزار، نرم افزار، بسته های یکپارچه و یا خدماتی است که از فروشندگان تخصصی تهیه می گردد. پروژه های تملیک باید دقیقا از نظر مفاهیم کنترلی مشابه روشهای توسعه در داخل شرکت باشد.

آمار جالب موفقیت و شکست پروژه های توسعه و تملیک

- ۱۸ درصد از پروژه های توسعه برنامه های کاربردی فن آوری اطلاعات با شکست مواجه می شوند. این پروژه ها قبل از تکمیل یا تحویل لغو شده و هیچ وقت مورد استفاده قرار نمی‌گیرند.
- ۵۳ درصد از پروژه ها با چالش روبرو می‌شوند، به این معنا که تحویل آن با تاخیر صورت می‌گیرد، و یا قیمت تمام شده آن از بودجه پیش بینی شده فراتر می‌رود و یا با امکانات و کارکرد کمتری تحویل داده می‌شوند.
- فقط ۲۹ درصد از تمام پروژه های سال ۲۰۰۴ با موفقیت روبرو شدند، که به معنی تحویل به موقع، مطابق با بودجه و با ویژگی ها و کارکردهای مورد نیاز بوده است.

مدیریت تغییر

عملیات فن‌آوری اطلاعات در بانک ها پیچیده و پویا است. با توجه به تعدد وابستگی های متقابل بین برنامه های کاربردی ، حتی کوچکترین تغییر در محیط نرم افزار یا سخت افزار می تواند تاثیرات بزرگی درپی داشته باشد.

مدیریت تغییر در فن‌آوری اطلاعات به مجموعه اقدامات مربوط به فرآیند برنامه ریزی ، زمانبندی، اجرا، ساختاربندی و پیگیری تغییرات در سامانه‌های برنامه های کاربردی، نرم افزار، سخت افزار، سیستم‌های شبکه‌ای و دیگر امکانات و تجهیزات فن‌آوری اطلاعات اتلاق می‌گردد. حوزه مدیریت تغییر مواردی نظیر تغییر در کنترل و مراقبت، بومی سازی و تبدیل را نیز در بر می‌گیرد.

روند موثر مدیریت تغییر موجبات اطمینان از یکپارچگی و قابلیت اتکاء در محیطهای فن‌آوری اطلاعات را بوجود می آورد. فرایند مدیریت تغییر موثر باید موارد زیر را فراهم آورد:

طبقه بندی و اولویت بندی تغییرات

- ارائه تعریف روشنی از نقش هر یک از عملکردهای فن‌آوری اطلاعات
- تعمیر و نگهداری از نسخه های قدیمی برنامه ها ، داده ها و سخت افزارها برای تضمین اینکه در هنگام بروز مشکل نیز خدمات لازم، ارائه خواهند شد.
- ارتقاء برنامه های تداوم فعالیت برای مقابله با مشکلات بالقوه
- اجرای عملیات بازرسی برای تایید کیفیت تغییرات انجام شده

تغییرات فن‌آوری

به عنوان مثال، بانک تغییرات کوچکی در سیستم نرم افزار خود در صبح روز شنبه که تا کنون عوارض جانبی ناخوشایندی در بر داشته ایجاد میکند. تغییر نرم افزار مانع از ثبت صحیح تراکنش‌های خودپرداز در دفتر کل بانک گردید. روشهای کند اصلاح در بانک منجرشد تا مدیریت نیز از طریق رسانه ها در جریان بروز این مشکل قرار گیرد. تبلیغات منفی از این رویداد مشکل جزئی را به کابوس عمومی بانک تبدیل نمود. همه سیستم های فن‌آوری اطلاعات به دنبال این اشکال دچار اختلال شده و برای بازگشت به حالت عادی دو روز زمان صرف گردید.

با این توصیف حتی اگر تمام اطلاعات قدیمی به صورت ایمن ذخیره می شد و تمام معاملات جدید می‌توانست مجددا تکرار شود ، آسیبی که از ناحیه تخریب شهرت به بانک رسید قابل برگشت نیست.

عملکرد دوم: مدیریت عملیات و پشتیبانی

مدیریت عملیات و پشتیبانی بصورت روزانه در مرکز داده در حال اجرا است. عملکرد مذکور در حوزه پردازش اطلاعات نیز کاربرد دارد. این عملکرد ممکن است در داخل و یا از طریق ارائه دهنده‌گان خدمات فنی انجام گردد. توافق نامه ارائه خدمات به موسسه بصورت برون‌سپاری بر مبنای استانداردها و یا استفاده از تجربیات مفید درون سازمانی انجام می پذیرد.

توافق نامه ارائه خدمات شامل موارد زیر میباشد:

- در دسترس بودن سیستم و ارائه عملکرد مورد نیاز
- دارا بودن ظرفیت رشد و ارتقاء
- تعیین سطح ارائه خدمات پشتیبانی به کاربران

دستورالعمل راهنمای عملیات فن‌آوری اطلاعات

What is an IT operations manual?

کتابچه راهنمای عملیات فن‌آوری اطلاعات دستورالعمل تدوین شده‌ای است که انجام عملیاتی از جمله وظایف اپراتور کامپیوتر ، برنامه ریزی کار و نحوه اجرای دقیق کار را نشان میدهد. همچنین نکاتی نظیر مراحل و الزامات مورد نیاز برای ایجاد سایت پشتیبان داخلی و خارجی از داده ها و نرم افزارها را در بر دارد.

سامانه های حل مشکل

What is a problem management system?

سامانه حل مشکل ابزاری برای پاسخ سریع به حوادث عملیاتی در فن‌آوری اطلاعات می باشد. این سیستم شامل روش‌های سریع گزارشدهی حوادث مربوطه به مدیریت فناوری اطلاعات است. این سامانه همچنین ابزاری برای ضبط تمام وقایع و پیگیری اقدامات صورت گرفته برای اصلاح مشکل فراهم می کند. در این سیستم واحد های اطلاع رسانی فنی (Helpdesk) به کاربران در تمام مسائل مربوط به فناوری و برقراری ارتباط به منظور شناسایی و بررسی مشکلات عملکرد های مختلف فن‌اوری اطلاعات کمک شایانی می‌کند.

نظارت بر اجرا، پشتیبانی و نگهداری

نظارت بر اجرا و گزارش دهی به موقع از رویکردها، بانک را قادر می سازد تا مشکلات را درست قبل از اینکه سیستم را تحت تأثیر قرار دهد شناسایی و اصلاح نماید. این فرآیند شامل پیش بینی حجم کار و شناسایی مسیر های انجام کار نیز میگردد. این یافته ها، اطلاعات لازم برای ارتقاء ظرفیت برنامه ریزی را فراهم می آورد.

بانک ها باید برنامه منظم نگهداری و پشتیبانی از تجهیزات مرتبط با فن‌آوری اطلاعات، از قبیل سخت افزار کامپیوتر ، دستگاه های شبکه ، توزیع برق ، تامین برق اضطراری (یو پی اس) و دستگاه تهویه هواو ... تهیه نمایند. برنامه نگهداری منظم و مرتب بر طبق توصیه های عرضه کننده تجهیزات و استانداردهای فن‌آوری اطلاعات متضمن توانایی ادامه فعالیت در تمام عرصه های ارائه خدمات فن‌آوری اطلاعات می گردد. این برنامه همچنین کمک می کند تا تمام کنترلها و ردیابی های عیوب سخت افزار و نرم افزار به سهولت میسر گردد.

عملکرد سوم: تداوم فعالیت و بازیابی خسارات

رویدادهای سالهای گذشته منجر به این شد که توجه و تمرکز بیشتری در زمینه نیاز به تداوم فعالیت موثر و برنامه ریزی جهت بازیابی موارد آسیب دیده معطوف گردد:

مشکل محدودیت کاراکتر های در نظر گرفته شده برای نمایش سال در تقویم برنامه‌های کامپیوتری

رویداد معروف به Y2K مشکلی بود که به دلیل عدم پیش بینی نیاز به ۴ کاراکتر برای نشان دادن سال ۲۰۰۰ در تقویم برخی از برنامه های کامپیوتر اتفاق افتاد چون در آن زمان ۲ کاراکتر برای نشان دادن سال در نظر گرفته شده بود (سال ۱۹۹۹ بصورت ۹۹ نمایش داده می شد) و طبعا نمایش سال ۲۰۰۰ بصورت ۰۰ باعث اختلال در محاسبات و انتقال داده ها به سال جدید میشد. جهت ارتقاء سیستم های نرم افزاری در ۳۱ دسامبر ۱۹۹۹ وقفه ای چند ساعته در انجام خدمات بانکی پدیدآمد.

واقعه ۱۱ سپتامبر (11/9)

در واقعه ۱۱ سپتامبر اطلاعات تجاری بیشتر شرکتهای مستقر در ساختمان تجارت جهانی نابود شد.

ویروس سارس

در سال ۲۰۰۳ میلادی شیوع ویروس سارس و مبتلا شدن هزاران نفر به این بیماری بر مناطق جغرافیایی زیادی از جمله کانادا و هنگ کنگ تاثیر گذاشت و موجب اختلال در انجام امور بانکی و تجاری وسرایت آن به دیگر مناطق جغرافیایی گردید.

این وقایع یادآور حساسیت و اهمیت موضوع تداوم کسب و کار و برنامه های بازیابی موارد آسیب دیده می باشد.

طرح تداوم فعالیت[۲] چیست؟

طرح تداوم فعالیت (BCP) برای اطمینان از نگهداری و یا بازیابی عملیات هنگام مواجه شدن با عوارض جانبی و یا حوادث غیر مترقبه مانند بلایای طبیعی ، ناتوانی فنی، خطای انسانی و اعمال تروریستی در موسسات مالی مورد استفاده قرار می گیرد.

طرح تداوم فعالیت قبل از آنی که معطوف به بازیابی آسیب های فنی باشد؛ معطوف به بازیابی فعالیت و کسب و کار است.

اهداف طرح تداوم فعالیت :

- به حداقل رساندن ضررهای مالی موسسه
- کمک به ادامه ارائه خدمات به مشتریان و فعالین بازارهای مالی

[۲] Business Continuity Plan (BCP)

طرح تداوم فعالیت باید نقشه راهی را برای کمک به موسسه به منظور کاهش اثرات اختلالات ایجاد شده در برنامه های استراتژیک ، برنامه های عملیاتی ، شهرت ،کیفیت مدیریت نقدینگی ، کیفیت مدیریت اعتباری ، موقعیت بازار و فرآیند انطباق با قوانین و مقررات فراهم کند.

مراحل تدوین طرح تداوم فعالیت

مرحله اول- تجزیه و تحلیل آثار حاصل از انجام فعالیت

تجزیه و تحلیل آثار حاصل از انجام فعالیت , وظیفه شناسایی تاثیرات بالقوه وقایع خارج از کنترل بر روی فرآیند کسب و کار موسسه و اولویت بندی فرآیندها را بر عهده دارد. این روش باید با هماهنگی تمام ادارات و دوایر موسسه انجام پذیرد، و تنها به بخش پردازش داده ها اکتفا نشود. لازم است برآوردی از حداکثر وقفه مجاز در روند فعالیت موسسه ، نقطه هدف در بازیابی موارد آسیب دیده و هزینه های مربوط به آسیب های احتمالی بصورت مداوم انجام پذیرد.

مرحله دوم- ارزیابی ریسک

ارزیابی ریسک به منظور اولویت بندی اختلالات بالقوه در روند فعالیت موسسه بر اساس شدت و احتمال وقوع آن انجام میگیرد. در این مورد از آزمون فشار[۳] با فرض وقوع سناریوهای مختلف تهدید استفاده میشود. اغلب تهدیدهای بزرگ احتمالی توسط طرحهای تداوم فعالیت پوشش داده میشوند. بیشتر تهدیدهای جدی که بدان اشاره شده است تاثیرات بزرگی را بر موسسه تحمیل مینمایند ولی احتمال وقوع آنها کم است.

استفاده از ارزیابی ریسک ، موجب انعطاف پذیری و سازگاری بیشترطرح تداوم فعالیت با انواع اختلالات سیستمی می گردد. تجارب کسب شده این فرایند منجر به تجزیه و تحلیل *گاف*[۴] (فاصله بین پیش بینی و واقعیت) برای تعیین الزام به روز رسانی طرحهای تداوم فعالیت میگردند.

مرحله سوم – پیاده سازی طرح

در مرحله پیاده سازی طرح تداوم فعالیت، مدیریت باید اطمینان حاصل نماید که طرح مذکور انعطاف پذیری لازم برای پاسخ دادن به سناریوهای تهدید پیش بینی نشده و ایجاد تغییر در شرایط بوجود آمده را داراست. باید مسئولیت ها و وظایف مربوط به هر یک از گروه های طرح تداوم فعالیت تشریح و فهرست اسامی و راههای تماس با افراد کلیدی تهیه و به موقع به روز رسانی شود.

---

[۳] Stress Testing
[۴] Gap Analisys

تمرکز بر روی چگونگی حفظ و انجام عملیات در شرایطی که امکانات و یا عملکردهای معمول مختل گردیده اند، بر شناسایی دقیق آسیب های وارده ارجحیت دارد.

مرحله چهارم - آزمون طرح

طرح تداوم فعالیت باید مرتبا مورد آزمون قرار گرفته و ضعف های آن ترمیم شود. ملاحظات برنامه ریزی فعالیت موسسه باید شامل توسعه سیستم چرخه حیات، تغییر در سیاست های کنترلی، *فرآیند همسان سازی داده‌ها* (سنکرون کردن داده ها)[۵]، آموزش کارمندان و ارتباطات باشد.

طرح بازیابی خسارات[۶] چیست؟

طرح بازیابی موارد آسیب دیده (DRP) زیر مجموعه ای ازطرح تداوم فعالیت است. این طرح ترمیم و بازیابی خدمات و سامانه های فن‌آوری اطلاعات و یا اطلاعات نگهداری شده به شکل الکترونیکی را دربر می گیرد.

برنامه ریزی تداوم فعالیت چیست؟

الف- بازیابی فعالیت های کسب و کار

ب- بازیابی فنی

ج- اجرای عملیات در شرایط سخت

"برنامه‌های تداوم فعالیت برای پشتیبانی از فعالیت‌های کسب و کار طراحی می‌گردند. بازیابی فنی و خدمات تنها بخشی از برنامه ریزی تداوم فعالیت است."

عملکرد چهارم: مدیریت امنیت

اطلاعات یکی از مهمترین دارایی های بانک به حساب می‌آید و حفاظت از آن جهت حفظ اعتماد به بانک ها ضروری است. امنیت اطلاعات عبارت است از حفاظت از سیستم ها ، رسانه ها وتجهیزاتی که پردازش و نگهداری از اطلاعات حیاتی را به عهده دارند. امنیت اطلاعات و سیستم های بانکی ضرورتی تردید ناپذیر برای حفظ ایمنی و صحت اطلاعات، و محرمانه ماندن اطلاعات مربوط به مشتریان مالی است.

---

[۵] Data Synchronization procedures

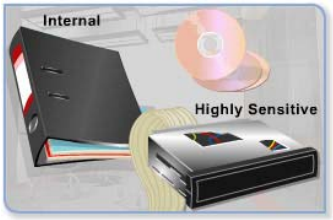
[۶] Disaster Recovery plan (DRP)

مدیریت امنیت فرایندی است که امنیت اطلاعات را میسر می سازد. بیایید سه عرصه مهم مدیریت امنیت را مورد بررسی قرار دهیم:

- طبقه بندی و حفاظت اطلاعات
- احراز هویت و کنترل دسترسی
- امنیت فیزیکی و پرسنلی

طبقه بندی و حفاظت اطلاعات

Information Classification and Protection



اطلاعات را می‌توان با توجه به درجه حساسیت، طبقه بندی نمود. مقوله های مختلف ممکن است به شکل زیر طبقه بندی گردند:

- بسیار حساس • حساس • داخلی • عمومی

موسسات باید با بسط سیاست ها و تعاریف هریک از طبقات، مجموعه‌ای مناسب از روشهای حفاظت از اطلاعات را تعریف نمایند. طبقه‌بندی اطلاعات باید تمامی رسانه‌های مختلف، از قبیل کاغذ و رسانه های الکترونیکی و از جمله نسخه های پشتیبان را شامل گردد.

واحد دارنده اطلاعات باید ارتباط کاری تنگاتنگی با مدیریت فن‌آوری اطلاعات و مدیریت ریسک به منظور حفاظت از اطلاعات مطابق با سطح ریسک فعلی وریسک پیش بینی شده داشته باشد.

احراز هویت و کنترل دسترسی

Authentication and Access Control

دسترسی به اطلاعات و سیستمهای کاربردی باید محدود به افرد خاصی باشد. نیل به این امر با استفاده ازایجاد مکانیزم سطوح دسترسی و تدوین مقررات کنترل دسترسی امکان پذیر است.

کد شناسایی منحصر به فرد کاربر، از قبیل شناسه کاربری و روشهای مناسب شناسایی، از جمله رمز عبور، محدودیت دسترسی را تضمین و نیز پاسخگویی برای هر فعالیت را فراهم می آورد.

بکار گیری قواعد کارآی رمزگذاری ، مانند اطمینان از تغییر کلمه عبور به صورت دوره ای و جلوگیری از استفاده ازکلمات عبوری که به آسانی قابل حدس زدن می باشند، اساسی و حیاتی می باشد. برای فعالیت ها و تراکنش های پر خطر، روشهای سطح دسترسی قوی تری باید به تصویب برسد. بطور مثال استفاده از کارت هوشمند و یا سخت افزارهای امنیتی نظیر توکن وکلید های سخت افزاری میتواند در ارتقاء سطح کیفی فضای امنیتی موثر واقع شود.

Physical and Personnel Security

امنیت پرسنلی و فیزیکی

تجهیزات پردازش اطلاعات حساس باید در حوزه های امن و مطمئن از قبیل مراکز داده، با موانع و کنترل های مناسب امنیتی ورود و خروج قرار داده شود. دسترسی به این حوزه ها باید صرفا به پرسنل مجاز محدود گردد. حق دسترسیها باید مرور و به طور مرتب به روز شود. ورود و خروج پرسنل خارجی ، از جمله ارائه دهندگان خدمات فنی، پرسنل تعمیر و نگهداری و نظافت، باید به درستی تایید و از نزدیک مانیتور(مراقبت) شوند.

در هنگام انتخاب محل استقرار مراکز داده ها باید شرایط محیطی نیز در نظر گرفته شود. برخی از تهدیدهای فیزیکی محیطی عبارتند از آتش ، مواد منفجره ، حرارت شدید ، آب و گرد و غبار. این مناطق باید به طور دائم مورد پایش (مانیتور) قرار گیرند. استفاده از منبع برق اضطراری (یو پی اس) و ژنراتورهای پشتیبان، خطرات ناشی از قطعی برق را کاهش می دهد.

عدم کنترل فیزیکی

در یک مثال ، هارد درایو دادههای پشتیبان اطلاعات شخصی مشتریان در یک موسسه مالی مفقود شده بود. تحقیقات بانک نشان داد که پسر یکی از کارکنان تعمیر و نگهداری برای استفاده از بازیهای کامپیوتری به هارد دیسک بزرگتری نیاز داشته و این هارد درایو را با اطلاعات آن بر روی کامپیوتر خود در خانه نصب کرده است. در این مثال، تنها به خطر افتادن یکپارچگی اطلاعات بانک مطرح نیست، بلکه می توانست نتایج فاجعه آمیزی در بر داشته باشد.

در این مورد، بانک قادر به حفاظت از اطلاعات بسیار حساس خود نبوده است. با این حال، جنبه مثبت قضیه این است که موجودی تجهیزات بانک به روز بوده است. این مسئله باعث شناسایی هارد درایو از دست رفته با استفاده از شماره سریال دستگاه و در نهایت، مطالبه دستگاه به سرقت رفته گردید.

عملکرد پنجم: برون سپاری فن‌آوری اطلاعات

پیشرفتهای فن‌آوری اطلاعات، بانک ها را قادر می سازد تا محصولات و خدمات وسیعی را در اختیار مشتریان قرار دهند. استفاده از ارائه دهندگان خدمات خارجی ، عموما با عنوان برون سپاری، توانایی بانک را در ارائه خدمات وسیع تر با هزینه کمترافزایش می دهد.

برون سپاری، با این حال ، ریسک های اساسی مرتبط با IT (فن‌آوری اطلاعات) و یا فعالیت های در معرض خطر را کاهش نمی دهد. خطراتی مانند زیان های مالی ، از دست دادن مزیت رقابتی ، از دست

دادن شهرت، افشاء اطلاعات نادرست همچنان درجای خود باقی است. میزان ریسک خدمات فن‌آوری اطلاعات برون سپاری شده، به نحوه برون سپاری، عملکرد ارائه دهنده خدمات و تکنولوژی بکار گرفته شده توسط ارائه دهنده خدمات بستگی دارد.

علیرغم برون سپاری خدمات، مسئولیت تضمین اجرای صحیح مدیریت ریسک فن‌آوری اطلاعات به طور موثر بر عهده بانک باقی می ماند.

نحوه کنترل عملکرد ارایه دهنده گان خدمات فن‌آوری اطلاعات

معمولا بانکها (به عنوان مشتری)، شرکتهای ارائه دهنده خدمات فن‌آوری اطلاعات (TSP) را بصورت مجزا توسط بخش حسابرسی داخلی خود، مورد ارزیابی و نظارت قرار می دهند. این حسابرسی ها می تواند موجب دوباره کاری شده و بار سنگینی را بر مدیریت و منابع موسسات ارائه دهنده خدمات تحمیل نماید. ارائه دهنده گان خدمات فن‌آوری اطلاعات می توانند به منظور کاهش این بار از یک موسسه مستقل به عنوان شخص ثالث برای تشریح وضعیت خود و قابلیت اطمینان کنترل های داخلی به عنوان موسسه حسابرسی فن‌آوری اطلاعات استفاده نمایند. به طور کلی، حسابرس فن‌آوری اطلاعات به عنوان شخص ثالث و به صورت کاملا مستقل به ارزیابی میزان کفایت تمامی سیستم های کنترل داخلی مرکز داده (Data Center)، از جمله عملیات کامپیوتری، سیستم ها، برنامه ها، و کنترل ورودی / خروجی داده ها می پردازد.

در ایالات متحده ، انجمن حسابداران خبره عمومی (AICPA) راهنمای حسابرسی ارائه دهندگان خدمات فن‌آوری اطلاعات را تحت عنوان (SAS70) برای حسابرسان مستقل تدوین نموده است. در کانادا ، راهنمایی مشابه توسط مؤسسه حسابداران خبره کانادا تحت عنوان (CICA 5900) ارائه شده است. بانکهایی که از چنین ممیزانی برای تکمیل فرایند حسابرسی داخلی موسسات ارائه دهنده خدمات فن‌آوری اطلاعات استفاده می نمایند، باید اطمینان داشته باشند که حسابرس مستقل جهت بررسی گزارشات ممیزان فن‌آوری اطلاعات واجد شرایط می باشند، تا اعتماد رضایت بخشی از اهداف حسابرسی حاصل آمده و نقصان های حسابرسی مالی از این طریق جبران شوند.واحد های نظارتی نیز می توانند از گزارشات ممیزان فن‌آوری اطلاعات استفاده نمایند.

برای نمونه تعدادی از موسسات و اشخاص صلاحیت داری که مبادرت به انجام امور ممیزی فن‌آوری اطلاعات مینمایند عبارتند از:

حسابرسان خبره سیستم های اطلاعات Certified Information Systems Auditor (CISA) – administer by Information Systems Audit and Control Association

مدیر خبره امنیت اطلاعات

Certified Information Security Manager (CISM)

متخصص خبره امنیت سیستم های اطلاعات

Certified Information Systems Security Professional (CISSP)

ارائه دهنده مستقل خدمات شبکه

Vendor Neutral Network - National Association of Communications Systems Engineers (NACSE)

تحلیلگر خبره کیفیت نرم افزار

Certified Software Quality Analyst (CSQA) – administered by Quality Assurance Institute

مهندس خبره تست نرم افزار

Certified Software Test Engineer (CSTE) – administered by Quality Assurance Institute

مدیریت ریسک برون سپاری

در صورت برون سپاری وظایف فن‌آوری اطلاعات، درست مانند زمانی که خود بانک مسئولیت اجرای وظایف فن‌آوری اطلاعات را بعهده دارد، باید مسئولیت تمامی مفاهیم مدیریت ریسک ، امنیت ، حریم خصوصی و دیگر سیاست ها را به عهده بگیرد.

مراحل برون سپاری

گام اول: تعیین نیازمندیها

یکی از شرایط برون سپاری توسعه همکاری همه ذینفعان در شناسایی وظایف یا فعالیتها جهت برون سپاری، ارزیابی ریسکهای متوجه برون سپاری و سنجش کنترل های مناسب در این زمینه است.

مولفه های کلیدی شرایط برون سپاری عبارتند از:

- دامنه و ماهیت پروژه
- سطح استانداردها و خدمات
- تعیین حداقل ویژگی های قابل قبول ارائه دهنده خدمات
- مراقبت و گزارشدهی
- طول مدت قرارداد ، نحوه فسخ و نحوه گمارش
- ایجاد تضمین در قبال عدم مسئولیت پذیری شرکت ارائه دهنده خدمات

گام دوم: تهیه گزارش درخواست پیشنهاد (RFP[۷])

درخواست پیشنهاد، شرح مفصلی از نیازمندیها است. تصمیم‌گیری در مورد برون‌سپاری خدمات و بررسی مستندات، پس از حصول اطمینان از تطابق کالا و خدمات شرکت ارائه دهنده خدمات با نیازمندی‌ها صورت میگیرد.

[۷] Request For Proposal

گام سوم: ارزیابی طرح های دریافتی

موارد پاسخ داده شده توسط ارائه دهنده خدمات باید ایفا کننده تمامی نیاز های مندرج در درخواست پیشنهاد(RFP) باشد. تفاوت میان طرحها و درخواست پیشنهاد (RFP) ممکن است شامل اختلاف در فرآیند گردش کار یا رویه های گزارشدهی، روشهای قیمت‌گذاری و یا تفاوتهای فنی باشد. اگر تفاوتی مشاهده گردید، موسسه باید تاثیری را که این تفاوت در رسیدن به اهداف و انتظارات سرویس دهی دارد را مورد ارزیابی قرار دهد. توانایی ارائه دهندگان خدمات بابت جبران خسارت ناشی از اشتباهات و قصور نیز بخشی از این ارزیابی ها محسوب می شود.

گام چهارم: نوشتن قرارداد

قرارداد برون سپاری از نظر قانونی سند لازم الاجرا است که همه جوانب ارتباط با ارائه دهنده خدمات فنی را تعیین می نماید. مشاور حقوقی بانک باید پیش نویس قرارداد را بررسی و از انطباق آن با مقررات و استانداردها و دستورالعمل ها اطمینان احاصل نماید. موافقت نامه رئوس مطالب مورد نیاز موسسه و مشوق ها و جرائم مربوط به زمان و نحوه ارائه خدمت را مشخص می نماید.

گام پنجم: مراقبت مستمر

مدیریت بانک باید بر نحوه عملکرد ارائه دهنده خدمات در طول دوره قرارداد نظارت داشته باشد. تغییرات بالقوه ناشی از تغییرات نیازهای موسسه نیز باید به صورت دوره ای مشخص شوند. این تغییرات در صورت توافق بین بانک و ارائه دهنده خدمات قابل اجرا می باشد.

ملاحظات نظارتی در موارد برون سپاری

این نکته مهم و بدیهی است که ناظرین از همان اختیاراتی که در دسترسی به اطلاعات بانکها دارند به اطلاعات نگهداری شده نزد ارائه دهندگان خدمات فنی نیز برخوردار باشند.

این مورد می تواند در هنگامی که هم پوشانی و یا زنجیره ای از برون سپاری ها اتفاق افتاده باشد به چالش بزرگی تبدیل شود. اختیارات ناظران ، توسط قانون در برخی از کشورها تضمین می شود، در غیر اینصورت حقوق واحدهای نظارتی باید در مفاد قرارداد بین بانک و ارائه دهندگان خدمات، قید گردد.

در برخی از کشورها ، بانک ها موظف هستند قبل از برون سپاری خدمات خود، تاییدیه رسمی واحد ناظر را کسب نمایند، یا حداقل واحد ناظر را قبل از انجام هرگونه اقدامی در جریان امر قرار دهند. در صورت برون سپاری خدمات در خارج از کشور اقدامات و الزامات دیگری نیز مد نظر ناظرین قرار می گیرد. این امر شامل نگهداری کپی داده ها در داخل کشور و یا پردازش داده ها به صورت کد شده و غیر قابل شناسایی عملی می گردد.

ناظران همچنین باید در مورد تمرکز برون سپاری خدمات به تعداد کمی از ارائه دهندگان خدمات فنی، که احتمال وقوع ریسک تمرکز را زیاد مینماید توجه لازم مبذول دارند.

واحد ناظر باید اطمینان حاصل نماید که بانکها و موسسات بطور کامل استراتژی های جایگزین و خروج از قرار داد برون سپاری را مد نظر قرار داده اند.

مسئولیت نهایی در قبال برون سپاری خدمات با کیست؟

الف- هیات مدیره

ب- مدیران ارشد

ج- مدیریت فن‌آوری اطلاعات

د- ارئه دهندگان خدمات فنی

" در عین حالی که بانک خدمات خود را برون‌سپاری می‌کند ولی مسئولیت آن بر عهده خود بانک است. شرکت ارائه دهنده خدمات مسئول کار خود بر طبق مفاد قرارداد و مدیر فن‌آوری اطلاعات مسئولیت مدیریت و نظارت بر نحوه ارائه خدمات را بر عهده دارد، اما مسئولیت نهایی با هیئت مدیره موسسه مالی است."

جمع بندی:

در این فصل پنج عملکرد اصلی فن‌آوری اطلاعات مورد بررسی قرار گرفت.

۱ توسعه و خرید

شناسایی ، تحصیل نصب و نگهداری سیستم های فن‌آوری اطلاعات.

۲. مدیریت عملیات و پشتیبانی

عملیات روزانه سیستم های فن‌آوری اطلاعات در بانک یا موسسه اعتباری.

۳. تداوم فعالیت و بازیابی موارد آسیب دیده

تجزیه و تحلیل سناریو های احتمالی ریسک و توسعه طرح های بازیابی.

۴. مدیریت امنیت

حفظ سطح مناسب امنیت فن‌آوری اطلاعات در تمام سطوح

۵. برون سپاری فن‌آوری اطلاعات

اطمینان از کنترل های کافی با توجه به محصولات و خدمات برون سپاری شده.

فصل دوم :

حاکمیت فن‌آوری اطلاعات

حاکمیت و ریسک فن‌آوری اطلاعات

مسئولیت حاکمیت فن‌آوری اطلاعات به عهده هیأت مدیره بانک یا موسسه اعتباری است و یکی از اجزاء حیاتی حاکمیت شرکتی (سهامی) بانکها محسوب میشود. حاکمیت فن‌آوری اطلاعات به ساختار سازمانی وشرح وظایف آن اشاره دارد تا اطمینان حاصل شود که فن‌آوری اطلاعات بانک، عملیات بانکی را به خوبی پشتیبانی و تسهیل می نماید. همچنین تضمین می نماید که منابع فن‌آوری اطلاعات به طور موثر مورد استفاده قرار گرفته و ریسکهای مرتبط با فن‌آوری به نحو احسن مدیریت می شوند.تعدادی از ریسکهای مرتبط با فن‌آوری اطلاعات ، عبارتند از:

ریسک استراتژیک

ریسک استراتژیک به عملیات فن‌آوری اطلاعات که به طور بالقوه بر توانایی یا عدم توانایی بانک برای رسیدن به اهداف استراتژیک آن موثر است، اشاره دارد. به عنوان مثال ، تاخیر و یا چشم پوشی از ارتقاء لازم در زیرساخت های فن‌آوری اطلاعات بانک می تواند منجر به عدم دسترسی به اهداف استراتژیک در زمینه سود دهی یا از دست دادن سهم بازار شود.

ریسک عملیاتی

ریسک عملیاتی اولین ریسکی است که با فن آوری اطلاعات همراه است. این ریسک قسمت های مختلف بخش فن‌آوری اطلاعات از جمله واحد تسویه و پایاپای، واحد عملیات ، واحد پردازش تراکنش ها و واحد های توسعه سیستم را تهدید می نماید. احتمال وقوع ریسک در منابع فن‌آوری اطلاعات می تواند منشاء داخلی یا خارجی داشته و منجر به اختلال در ارائه خدمات بانکی گشته و عملیات بانکی را با بحران مواجه سازد.

ریسک شهرت

ریسک شهرت، ریسک تخریب بانک است ، به عنوان مثال ، ناتوانی فن‌آوری اطلاعات در حفظ اطلاعات محرمانه مشتریان به اعتبار و شهرت بانک آسیب می رساند. نتایج عملکرد نامناسب فن‌آوری اطلاعات می تواند مشکلات بسیاری را در نقدینگی، سودآوری و کفایت سرمایه بانک پدید آورد.

برای کسب اطلاعات بیشتر در مورد ریسک های مرتبط با فن‌آوری اطلاعات می توانید به سایت های الکترونیکی زیر مراجعه فرمایید:

IT Governance Institute http:www.itgovernance.org

Information Systems Audit and Control Association. http://*www.* isaca org

Code of Practice for Information Security Management http://www.iso.ch

Information Security Forum http:llwww.secuhtyforum org

مسئولیت اعضای هیأت مدیره

هیأت مدیره، مسئولیت نهایی شناسایی ریسکهای فن‌آوری اطلاعات و نظارت بر طراحی و پیاده سازی یک سیستم مدیریت ریسک مناسب را به عهده دارد.

سیستم مدیریت ریسک فن‌آوری اطلاعات مناسب شامل حاکمیت فن‌آوری اطلاعات، فرایند مستمر مدیریت ریسک فن‌آوری‌اطلاعات و اجرای شیوه های صحیح با توجه به کنترل های فن‌آوری اطلاعات می باشد. حسابرسی فن‌آوری‌اطلاعات، ارزیابی مستقلی از فرآیندهای مدیریت ریسک فن‌آوری و کنترلهای فن‌آوری اطلاعات را ارائه می نماید.

هیأت مدیره باید طرح های فن‌آوری اطلاعات ، سیاست ها و هزینه های عمده مربوطه را به تصویب برساند. هدف هیات مدیره حصول اطمینان از انجام فعالیت ها به نحو مطلوب ، اتخاذ برنامه های راهبردی

مؤثر فن‌آوری اطلاعات و نظارت کارا بر عملکرد فن‌آوری اطلاعات می باشد. برای انجام این مهم، اعضای هیأت مدیره باید با مفاهیم فن‌آوری اطلاعات و مرکز داده ها و فعالیتهای آن آشنا باشد.

هیأت مدیره اغلب امور مربوط به حاکمیت فن‌آوری اطلاعات را از طریق کمیته های نظارتی از جمله کمیته حسابرسی، کمیته بحران اجرا می نمایند. فن‌آوری اطلاعات یک مقوله بحرانی است و بانک ها می توانند کمیته فن‌آوری اطلاعات را در سطح هیأت مدیره راه اندازی نمایند، به عنوان مثال کمیته راهبردی فن‌آوری اطلاعات برای کمک به هیأت مدیره در نظارت بر مسائل مرتبط با فن‌آوری اطلاعات تشکیل و از مد نظر قرار گرفتن حاکمیت فن‌آوری اطلاعات دردستورالعملهای تهیه شده اطمینان حاصل می نماید.

مسئولیتهای مدیریت ارشد

مدیریت ارشد مسئولیت اجرای برنامه‌های استراتژیک هیأت مدیره را (از جمله طرح های استراتژیک فن‌آوری اطلاعات) بر عهده دارد. ایجاد یک کمیته مدیریت ارشد، به عنوان مثال کمیته راهبردی فن‌آوری اطلاعات، می تواند مدیریت ارشد را در رسیدن به اهداف ومقاصد خود کمک کند. چنین کمیته ای می تواند متشکل از نمایندگان مدیریت ارشد بخش های فن‌آوری اطلاعات و ادارات اصلی که به عنوان کاربران عمده سیستمهای فن‌آوری اطلاعات هستند، می‌باشد.

وظایف خاص مدیران ارشدی که با کمیته راهبردی همکاری می کنند (در صورتی که بانک چنین ساختاری را تعیین کرده باشد)، شامل موارد زیر میگردد:

- نظارت بر اجرای طرح های استراتژیک فن‌آوری اطلاعات
- تایید عرضه کنندگان کالاها و خدمات فنی و کنترل وضعیت مالی آنها
- تصویب و نظارت بر پروژه های بزرگ ، بودجه های فن‌آوری اطلاعات ، اولویت ها ، استانداردها ، فرآیندها وعملکرد کلی فن‌آوری اطلاعات
- ایجاد هماهنگی عالی بین بخش فن‌آوری اطلاعات و بخش هایی که به عنوان کاربر از سیستم های فن‌آوری اطلاعات استفاده می نمایند.
- بررسی کفایت منابع فن‌آوری اطلاعات و اختصاص منابع مذکور در مقوله های تامین مالی، تامین نیروی کار، تامین تجهیزات و خدمات.

مدیریت فن‌آوری اطلاعات یا رئیس اداره اطلاعات

مدیریت فن‌آوری اطلاعات ، و یا رئیس اداره اطلاعات (CIO)[۸] ، مسئولیت کلیدی برای اجرای طرح های ابتکاری فن‌آوری اطلاعات در درون بانک را بر عهده دارد.

مدیریت فن‌آوری اطلاعات، عضو مدیریت ارشد بانک با مسئولیت دخالت مستقیم در تصمیم گیری های کلیدی بوده و باید نتایج کار را به طور مستقیم به مدیر عامل گزارش دهد. در جایی که بانک دارای کمیته فن‌آوری اطلاعات می باشد ، مدیریت فن‌آوری اطلاعات باید در آن کمیته نقش پیشرو داشته باشد.

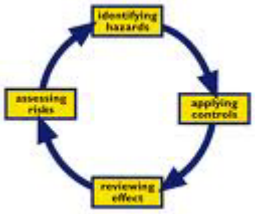
مدیریت فن‌آوری اطلاعات، باید به مسائل استراتژیک و اثربخشی کلی ساختار فن‌آوری اطلاعات توجه کافی داشته باشد. مدیر ارشد فن‌آوری اطلاعات، معمولا عهده دار مسئولیت های زیر است:

- نظارت بر بودجه فن‌آوری اطلاعات
- مدیریت اجرایی
- بکار گیری جامع فن‌آوری اطلاعات
- ارتقاء مهارتهای شغلی و آموزش بخش فن‌آوری اطلاعات
- معماری فن‌آوری اطلاعات
- برنامه ریزی عالی استراتژیک

مدیریت ریسک فن‌آوری اطلاعات

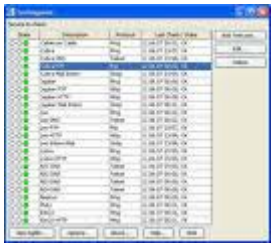
مدیریت ریسک فن‌آوری اطلاعات شامل چهار کارکرد ضروری است

برنامه ریزی



ارزیابی ریسک

کنترلهای داخلی



پایش

پیچیدگی فرایند مدیریت ریسک، بسته به اندازه و پیچیدگی سازمان متفاوت است.

[۸] Chief Information Officer

برنامه ریزی

برنامه ریزی فن‌آوری اطلاعات شامل دو حوزه اصلی برنامه ریزی استراتژیک فن‌آوری اطلاعات و برنامه ریزی عملیاتی فن‌آوری اطلاعات است.

برنامه ریزی استراتژیک معمولا افق سه تا پنج ساله را پوشش می دهد. این برنامه به اهداف بلند مدت و چگونگی تخصیص منابع فن‌آوری اطلاعات برای دستیابی به آن اهداف اشاره دارد. این موضوع باید سازگار و یا همسو با طرح عملیاتی (Business Plan) بوده تا موسسه به اهداف خود دست یابد.

برنامه ریزی استراتژیک فن‌آوری اطلاعات باید موارد زیر را تحت پوشش قرار دهد:

- معماری سخت افزار و نرم افزار
- منابع و داده های محاسباتی مورد استفاده کاربران
- پردازش عملیات توسط اشخاص ثالث (در موارد برون سپاری)

برنامه ریزی عملیاتی بر اقدامات کوتاه مدت و فرایند تدوین بودجه سالانه متمرکز می باشد. برنامه های عملیاتی ، برنامه های استراتژیک را تعقیب نموده و از نیازهای اساسی عملیات جاری موسسه پشتیبانی می کند.

برنامه های عملیاتی فن‌آوری اطلاعات سطح منابع مورد نیاز فن‌آوری اطلاعات را تعیین می نماید. منابع مذکور شامل زیرساخت های فن‌آوری اطلاعات، نرم افزارهای کاربردی، سیستم عامل ، سخت افزار و پرسنل می باشد.

ارزیابی ریسک

Risk Assessment

ارزیابی ریسک فن‌آوری اطلاعات معطوف به نحوه انتخاب تکنولوژی و پیاده سازی کنترل های داخلی است. فرآیند ارزیابی ریسک شامل ارزیابی های خاصی مانند امنیت، تداوم فعالیت و مدیریت برون سپاری می باشد.

ارزیابی ریسک شامل چهار مرحله مهم است:

۱. نظارت مستمر حوزه های ریسک، از جمله جمع آوری اطلاعات از سامانه های جدید
۲. تجزیه و تحلیل اثرات بالقوه ریسک
۳. اولویت بندیهای کنترلی و تبیین اقدامات کاهنده ریسک
۴. نظارت مستمربر اقدامات کاهنده ریسک

کنترل های داخلی

کنترلهای داخلی بیانگر انسجام کلی محیط فن‌آوری اطلاعات بوده و دارای مشخصه های ذیل است:

- اهداف اجرائی روشن و قابل اندازه گیری
- نحوه تفویض مسئولیت های خاص برای پیاده سازی پروژه های کلیدی
- ساز و کار مستقل برای اندازه گیری ریسک و به حداقل رساندن تاثیرات مخرب ریسک

کنترل های داخلی باید تمامی کارکردهای فن‌آوری اطلاعات که در فصل اول این نوشتار بدان اشاره شد را پوشش داده و به طورمنظم و ساختار یافته ای اطمینان حاصل نماید که:

- تفکیک مناسب وظایف و نقشها مورد پایش قرار می گیرد.
- ثبت ها بطور صحیح ایجاد ، منتقل و ذخیره گیری می شوند.
- اطلاعات گزارش شده به مدیریت و هیأت مدیره از کفایت و قابلیت اتکاء لازم برخوردار است.
- در شرایط پر ریسک، وظایف و فعالیت ها بخوبی تعریف شده و نظارت می شوند.

تفکیک مناسب وظایف تمامی کارکردهای فن‌آوری اطلاعات برای اطمینان از عملکرد موثر کنترل های محیط فن‌آوری اطلاعات حیاتی است. تفکیک مسئولیت از دیدگاه کنترلهای داخلی فن‌آوری اطلاعات در برخی از موسسات ، به ویژه آنهایی که حجم کوچکتری دارند، دشوار است. در این گونه موارد ، کنترل های جبرانی مناسب در جای خود برای کاهش ریسک باید وجود داشته باشد.

پایش (مراقبت)

در صورتیکه مدیریت ریسک کارا و کنترل های مناسب در موسسه وجود داشته باشد، پایش موثر و اندازه گیری صحیح ریسکها معنی دار می شوند. موارد زیر از مصادیق پایش در مبحث مدیریت ریسک می‌باشد:

۱- تطبیق برنامه ها با رویدادهای واقعی

بررسی دوره ای برنامه ها با عملکردهای واقعی تضمینی است از اینکه نتایج واقعی عملکرد ها با برنامه ها، اهداف و انتظارات از پیش تعیین شده از تطابق کامل برخوردارند. عدم انجام این بررسیها با توجه

به هزینه‌های هر یک از عملکردهای فن‌آوری اطلاعات و اتکاء بانک به عملکرد فن‌آوری اطلاعات، می‌تواند بانک را در معرض ریسک قرار دهد.

۲- معیارهای اجرایی

لازم است که بانکها در هنگام استقرار فن‌آوری اطلاعات معیارهای اجرایی ویژه ای را تدوین و تطابق عملکردهای اجرایی را با این استانداردها به صورت مستمر مورد رسیدگی و مراقبت قرار دهند. این امر کمک شایانی به شناسایی مشکلات بالقوه کرده و اطمینان حاصل می نماید که وظایف و عملکرد های فن‌آوری اطلاعات با اهداف تعیین شده سازمانی مطابقت دارند.

معیار های عمومی شامل میزان کارایی کارکرد پردازنده مرکزی و شبکه ، میزان کارایی مراکز داده، قابلیت راه اندازی مجدد سیستم ، زمان پاسخگویی، میزان خطاها و گزارشات مربوط به اشکالات سیستمی می باشد.

۳- عملکرد اشخاص ثالث

برای تعامل با اشخاص ثالث به معیارها و استانداردهای مصوب و رسمی نیاز است. این معیارها به عنوان موافقتنامه سطح کیفی و کمی خدمات (SLAs)[۹] شناخته می شود. این موافقتنامه موجب تفهیم انتظارات کارفرما و فراهم کردن معیار اندازه گیری نحوه عملکرد فن‌آوری اطلاعات می گردد. مشوق ها و جریمه های مرتبط با عملکرد اجرایی از دیگر مفاد این موافقتنامه هستند.

۴- تضمین کیفیت

تضمین کیفیت باید دربرگیرنده کلیه جوانب باشد. علاوه بر انجام خود ارزیابی های مربوط به ممیزی فن‌آوری اطلاعات و ممیزی اشخاص ثالث، سایر عواملی که متضمن اجرای صحیح سیاست ها ، استانداردها و رویه ها هستند نیز باید توسط سازو کارهای خود ارزیابی مورد توجه قرار گیرند و از موثر بودن مکانیزم های خود ارزیابی اطمینان کافی حاصل گردد.

مقولات (دغدغه های) نظارتی در فن آوری اطلاعات

به همان اندازه ای که ریسک های امنیت و تکنولوژی اطلاعات با اهمیت هستند، ناظران در مورد ریسکهای عملیاتی و سیستمیک نیز توجه کافی مبذول می دارند. اهمیت فن‌آوری اطلاعات در بانک این امر را برای ناظران ضروری میسازد که چگونگی مدیریت و کنترل اثر بخش منابع فن‌آوری اطلاعات در قبال ریسک‌های مربوطه را مورد ارزیابی قرار دهند.

[۹] Service Level Agreements

برخی از سازمان های نظارتی دارای واحد/ تیم فن‌آوری اطلاعات و یا اداره ریسک عملیاتی / فن‌آوری اطلاعات با متخصصان با تجربه در این زمینه میباشند. این تیم می تواند بصورت متمرکز فقط به بازرسی فن‌آوری اطلاعات بپردازد و یا اینکه با بازرسان عمومی برای ارزیابی های ویژه نظیر بررسی مکانیزم های بازار پول و سرمایه همراه شوند. این امر بستگی به اهداف نظارتی و توقعات واحد نظارت کننده از پروسه بازرسی دارد. برخی از نهاد های نظارتی یک نفر را در تیم بازرسی برای تمرکز بروی موضوعات مرتبط با فن‌آوری اطلاعات اختصاص می دهند. در برخی از کشورها نیز ارزیابی فن‌آوری اطلاعات را متکی به نظر حسابرسان مستقل می دانند.

رهنمود حسابرسی فن‌آوری اطلاعات

یکی از منابع قابل دسترس برای عموم، کتابچه راهنمای بازرسی فن‌آوری اطلاعات شورای بازرسی موسسات مالی فدرال (FFIEC) است. این کتابچه به ۱۲ دفترچه تقسیم شده که تمامی موضوعات مربوط به حاکمیت، کارکرد های فن‌آوری اطلاعات و فعالیت های خاص مبتنی بر فن‌آوری اطلاعات نظیر بانکداری و نظام های پرداخت را شامل می شود.

با این حال باید توجه داشت که این منابع برای رویکرد نظارتی نظام بانکداری در ایالات متحده طراحی گردیده و ممکن است به طور کامل قابل انطباق با رویکردهای نظارتی سایر کشور ها نباشد.

مراحل نظارت بر فن آوری اطلاعات

یکی از روشهایی که ناظران می توانند در بررسی و ارزیابی ریسک فن‌آوری اطلاعات استفاده نمایند، انجام بررسی های فن‌آوری اطلاعات در بانک ها به صورت طرح سئوالات زیر میباشد:

تعداد کارکنان بخش فن‌آوری اطلاعات چقدر است؟

از این اطلاعات برای محاسبه نسبت بین کارکنان فن‌آوری اطلاعات و کل پرسنل استفاده کنید. این نسبت سطح تمرکز بر فن‌آوری اطلاعات در یک موسسه در مقایسه با وضعیت متوسط صنعت را نشان میدهد. حتی شما میتوانید تعداد کارکنان تمام وقت شرکتی که خدماتی را به آن برونسپاری نموده اید نیز در محاسبه لحاظ نمایید.

میزان هزینه های مصروفه در بخش فن‌آوری اطلاعات چقدر می باشد؟

این سوال نیز به طور مجزا شامل هزینه های عملیاتی و تعمیر و نگهداری ، توسعه ، سرمایه گذاری در بخش فن‌آوری و هزینه های برون سپاری است. این نسبت میتواند از تقسیم هزینه های فن‌آوری به درآمد، هزینه های عملیاتی و یا کل دارایی ها محاسبه گردد.

خدمات برون سپاری شده چه هستند و چه کسانی این خدمات را ارائه می دهند؟(شامل موسسات وابسته نیز می گردد)

پاسخ این سئوال نمایی کلی از نحوه برون سپاری و خدماتی که برون سپاری شده اند را باید نشان دهد.

نام برنامه هایی خریداری شده چیست و تامین کنندگان آنها چه کسانی هستند؟

محصولات مشابه از تامین کنندگان مختلف قابل مقایسه و ارزیابی است. این امر در تعامل با فروشندگان یا ارائه دهندگان خدمات که به طور گسترده درک درستی از محصول رادارند مفید واقع می شود.

سئوالات باید شما را قادر به ارزیابی کیفیت و اثر بخشی مراحل مدیریت ریسک فن‌آوری‌اطلاعات بانک نماید.

سئوال در مورد حاکمیت فن‌آوری اطلاعات

در حالی که تمرکز بازرسی بر ریسک نرخ سود است ، شما مشاهده می کنید که بازرسی داخلی طی گزارشی اعلام نموده که تائیدیه مالیاتی سرمایه گذاری در طرح ها به دلیل مشکلات فن‌آوری اطلاعات با تاخیر تهیه می شود. شما از گروه بازرسی فن‌آوری اطلاعات در خصوص مشکلات 'فن‌آوری اطلاعات درخواست کمک مینمایید.

در تماس تلفنی بین بخش فن‌آوری اطلاعات و واحد بازرگانی مشخص می شود که برنامه اجرایی فن‌آوری اطلاعات در خصوص محاسبات سود نمی تواند تاییدیه مالیاتی را بصورت اتوماتیک چاپ کند. این تاییدیه ها باید بصورت دستی پردازش شوند. ارتقاء نرم افزار برای فراهم آوردن امکان چاپ نیاز به صرف زمانی بیش از دو هفته برای برنامه نویسی دارد.

مدیریت به صورت غیر رسمی از کارکنان فن‌آوری اطلاعات خواسته است تا روی این پروژه کار کنند ولی کار پروژه تا کنون زمانبندی نشده است.

آیا می توانید تشخیص دهید که مشکل حاکمیت فن‌آوری اطلاعات در این موسسه چیست؟

- ✓ فرایند اولویت بندی در بخش فن‌آوری اطلاعات وجود ندارد.
- ✗ منابع واحد فن‌آوری اطلاعات ناکافی است.
- ✗ برنامه های ذخیره سازی تجهیزات فن‌آوری اطلاعات ضعیف است.
- ✓ هیچ فرآیند رسمی برای درخواست تغییرات فن‌آوری اطلاعات وجود ندارد.
- ✓ کنترل پروژه های بخش فن‌آوری اطلاعات ضعیف است.

ظاهرا مکانیسم خاصی در زمینه حاکمیت فن‌اوری اطلاعات، مانند کمیته راهبردی فن آوری اطلاعات برای نظارت بر برنامه های تغییر و یا نرم افزار های کاربردی جدید وجود ندارد. هیچگونه فرایند اولویت بندی برای انجام کار موجود نیست. موسسه فاقد نظارت موثر مدیریت ارشد فناوری اطلاعات در زمینه کنترل پروژه ها در بخش فناوری است.

جمع بندی

به طور کلی فن‌آوری اطلاعات دغدغه اساسی دنیای مدرن امروز به شمار می رود و از اهمیت خاصی برای بانک بر خوردار است. فرآیند حاکمیت فن‌آوری اطلاعات مشتمل بر روشهای مختلف و تفصیلی زیادی است که برای اطمینان از استفاده موثر از منابع فن‌آوری اطلاعات و اعمال صحیح مدیریت ریسک بکار گرفته است.

هیأت مدیره مسئول نهایی حصول اطمینان از موثر بودن حاکمیت فن‌آوری اطلاعات است. مدیر ارشد اطلاعات(CIO) مسئول اجرای طرح های فن‌آوری اطلاعات در داخل بانک می‌باشد.

ریسک های مربوط به فن‌آوری اطلاعات شامل ریسکهای عملیاتی ، استراتژیک ، شهرت و حقوقی است. مدیریت ریسک فن‌آوری اطلاعات موارد زیر را پوشش می دهد:

- برنامه ریزی
- ارزیابی ریسک
- کنترل
- مراقبت و پایش

فصل سوم :

حسابرسی فن‌آوری اطلاعات

هدف از برنامه های حسابرسی فن‌آوری اطلاعات چیست؟

اهداف حسابرسی های داخلی، از قبیل، ارزیابی و بهبود اثربخشی مدیریت ریسک، فرآیند کنترل و حاکمیت، بر حسابرسی فن‌آوری اطلاعات نیز صدق می کند. در این بخش تنها به ویژگی های منحصر به فرد حسابرسی فن‌آوری اطلاعات اشاره شده است. مسائلی مانند استقلال حسابرسی فن‌آوری اطلاعات، نحوه تامین نیروی انسانی و آموزش کارکنان حسابرسی فن‌آوری اطلاعات در این فصل بیان می شوند.

مدیریت حسابرسی فن‌آوری اطلاعات - شیوه های مطلوب

برنامه حسابرسی فن‌آوری اطلاعات باید موارد زیر را به اجرا گذارد :

- ارزیابی اثر بخشی برنامه ریزی های مدیریتی و نظارتی فعالیت های فن‌آوری اطلاعات
- ارزیابی اثربخشی فرآیندهای عملیاتی و کنترلهای داخلی
- سنجش کفایت تطابق اقدامات بعمل آمده و روشهای کنترل داخلی با سیاست های فن‌آوری اطلاعات
- شناسایی نارسایی‌ها
- پیشنهاد اقدامات اصلاحی

برنامه حسابرسی فن‌آوری اطلاعات ارتقاء دهنده محرمانگی، صحت و در دسترس بودن سیستم های اطلاعاتی می‌باشد.

عملکرد توسعه و خرید فن‌آوری اطلاعات مثالی برای برنامه‌ریزی حسابرسی

پروژه های توسعه نرم افزار ، خرید سخت افزار و نرم افزار و تبدیل از یک سیستم به سیستم دیگر اغلب طولانی و پیچیده است. این مهم نیاز به تعامل میان کارکنان برنامه نویسی ، ادارات کاربر و حسابرسی داخلی دارد.

به طور معمول ، یک پروژه به مراحل مختلف تقسیم می شود. در پایان هر مرحله ، حسابرس باید کنترل های داخلی، آزمون ها، و ممیزی ها لازم را در بررسی برنامه های کاربردی به کار بندد. تعامل حسابرس فن‌آوری اطلاعات در جهت راهنمایی توسعه دهندگان نرم افزار به جهت در نظر گرفتن استاندارد های مناسب و کنترل های لازم در طول پروژه مفید می باشد.

حسابرسی داخلی فن‌آوری اطلاعات مبتنی بر ریسک

شیوه صحیح آن است که برنامه حسابرسی فن‌آوری اطلاعات مبتنی بر ریسک برای پوشش تمام فعالیتهای عمده یک بانک به مورد اجرا گذارده شود. ماهیت و گستره یک برنامه حسابرسی به اندازه و پیچیدگی بانک بستگی دارد. برنامه حسابرسی باید به صورت مجزا برای تک تک واحد ها و سیستم های مستقر در یک بانک تدوین گردد.

مرحله اول برنامه حسابرسی فن‌آوری اطلاعات، شناسایی نواحی عمده در معرض ریسک است. سیستم اندازه گیری، یا امتیاز دهی، عوامل مختلف ریسک را شناسایی و رتبه بندی کرده و گستره و ماهیت برنامه حسابرسی فن‌آوری اطلاعات و تناوب حسابرسی ها را تعیین می‌کند.

عوامل ریسکی مورد استفاده در سیستم امتیاز دهی ممکن است شامل موارد زیر باشد:

- ماهیت معاملات (به عنوان مثال ، تعداد ، اندازه و پیچیدگی)
- عمر سیستم و یا نرم افزار کاربردی
- تجربه مدیریت و کارکنان ، از جمله صلاحیت های فنی
- نتایج حسابرسی قبلی و واکنش و مسئولیت پذیری مدیریت در پرداختن به مسائل و حل آن

برنامه حسابرسی فن‌آوری اطلاعات مبتنی بر ریسک باید:

- مطابق با برنامه ای که توسط هیأت مدیره ، کمیته حسابرسی (در صورت اطلاق) تایید شده است، انجام پذیرد.
- اطلاعات بانک ، برنامه ها و سیستم عامل ، فن‌آوری ها ، امکانات و پرسنل مورد شناسایی کامل قرار گیرند.
- فعالیتهای موسسه و فرایندهای آن در هر رده شناسایی گردند.
- مشخصه و وضعیت هر یک از فرآیندهای فعالیت (نظیر اقدامات الف تا ی اعطای تسهیلات) بطور کامل تشریح شود.
- اندازه گیری ریسک ها و کنترلهای مرتبط با هر یک از فرآیندهای فعالیت بر اساس مشخصه ها و وضعیت بند فوق صورت پذیرد.

برون سپاری حسابرسی داخلی فن‌آوری اطلاعات

بانکها و سایر موسسات مالی انجام فعالیت هایی که به طور معمول خود به عهده داشتند را به صورت فزاینده ای به اشخاص ثالث محول می نمایند. برون سپاری به طور فزاینده به عنوان وسیله ای برای کاهش هزینه ها و دستیابی به اهداف استراتژیک استفاده می شود.

برون سپاری حسابرسی فن‌آوری اطلاعات در صورتی مفید خواهد بود که دارای ساخت مناسبی بوده و و بصورت عاقلانه و احتیاطی اداره گردد. مدیریت بانک باید اطمینان حاصل نماید که هیچگونه تضاد منافعی در این زمینه وجود ندارد.

ناظران باید از وجود سیستم های رضایتبخش کنترل های داخلی که گستره فعالیتها و مدیریت های برون سپاری را در بر گیرد اطمینان حاصل نمایند. آنها همچنین باید تعیین نمایند که آیا مدیران و مدیران ارشد مسئولیت های خود را برای حفظ نظام موثر کنترل داخلی و نظارت بر عملکرد حسابرسی داخلی در حوزه های برون سپاری شده به نحو احسن به اجرا می گذارند.

حسابرسی مستقل فن‌آوری اطلاعات

حسابرسان مستقل معمولا روشهای کنترل فن‌آوری اطلاعات را به عنوان بخشی از ارزیابی کلی از کنترل های داخلی به هنگام اظهار نظر درمورد کفایت و مقبول بودن صورتهای مالی موسسه بررسی می کنند.

حسابرسان مستقل نحوه حسابرسی داخلی کنترل‌های مؤثر بر نگهداری و حفاظت از دارایی‌ها و یکپارچگی کنترل در تهیه صورتهای مالی و گزارش دهی را مورد بررسی قرار می دهند. آنها به بررسی دو دسته از کنترلها اقدام می نمایند:

۱- کنترل های عمومی

کنترل های عمومی عبارتند از:

- سازماندهی و اجرا
- مستند سازی رویه ها
- نحوه دسترسی به تجهیزات و فایل های اطلاعاتی
- سایر کنترل های مربوط به اجرای سامانه های اطلاعاتی

۲- کنترل های کاربردی

کنترل های کاربردی مربوط به وظایف خاص سیستم های اطلاعاتی است. این کنترلها به منظور اطمینان از صحت عملیات ثبت، پردازش و گزارشدهی اطلاعات تهیه و مورد استفاده قرار میگیرند.

ارتباط ناظران و حسابرسان فن‌آوری اطلاعات

هنگام بررسی فرآیندهای ممیزی داخلی فن‌آوری اطلاعات ، نقش ناظر ارزیابی اثربخشی آنها می باشد. این ارزیابی شامل بررسی توانایی بانک در سرعت شناسایی و گزارش ریسکهای خاص به هیأت مدیره و مدیریت ارشد بانک میباشد. ارزیابی عملکرد حسابرسی فن‌آوری اطلاعات میزان اتکا به اهداف نظارتی را تعیین میکند.

حوزه نظارت با توجه به حسابرسی داخلی فن‌آوری اطلاعات موارد زیر را در نظر دارد:

- استقلال نقش حسابرسی (داخلی و مستقل)
- گزارش نحوه ارتباط کارکردهای حسابرسی با هیأت مدیره یا کمیته حسابرسی
- ارتباط تخصص و تعداد حسابرسان فن‌آوری اطلاعات با محیط فن‌آوری اطلاعات
- اثربخشی فرآیند ارزیابی ریسک حسابرسی
- گستره و تناوب حسابرسی فن‌آوری اطلاعات
- فرآیند اطمینان از کشف به موقع و حل و فصل نقاط ضعف گزارش شده
- مستندات حسابرسی های فن‌آوری اطلاعات ، شامل کاربرگها، گزارش‌ها، پیگیری‌ها و اقدامات اصلاحی

تخصص ناظران فن‌آوری اطلاعات

تخصص ناظرین ممکن است در مواقع رسیدگی به عملکردهای خاص، محدود باشد. بسیاری از کشورها دارای سازمانهای دولتی متخصص در امنیت اطلاعات هستند. با استفاده از منابع این سازمان های دولتی میتوان تلاش ناظران فن‌آوری اطلاعات را تکمیل و موجب صرفه جویی در هزینه ها شد. همکاری بین سازمان های نظارتی و سایر سازمانها میتواند به صورت مشورتی و یا به شکل مشارکت در ارزیابیهای فن‌آوری اطلاعات عمل شود.

به عنوان مثال دو نمونه از همکاری های موفقیت آمیز در ایالات متحده و آلمان در ادامه آمده است. در ایالات متحده ، سازمان های نظارتی برخی اوقات با بخش جرائم رایانه ای دفتر بازجویی فدرال (اف‌بی‌آی) تماس برقرار مینمایند. در آلمان ، مقامات نظارتی لحظه به لحظه با آژانس امنیت اطلاعات آلمان (GISA) در ارتباط هستند.

استفاده از مشاوران و یا شرکت های خصوصی متخصص جایگزینی دیگر برای سازمان‌های دولتی است. در این مورد ، تضاد منافع، هزینه ها و محدودیت های قانونی باید برای جلوگیری از مشکلات بالقوه در نظر گرفته شود.

درست یا غلط؟

- نقش ناظر، ارزیابی اثربخشی حسابرسی داخلی فن‌آوری اطلاعات بانک میباشد.
- حسابرسی داخلی جامع فن‌آوری اطلاعات به صورت مستمر انجام می پذیرد.
- حسابرسی داخلی فن‌آوری اطلاعات نیاز به تخصص ویژه ای دارد که باید ازتخصص شرکتهای ارایه دهندگان خدمات فنی استفاده نمود.
- گزارش حسابرسان مستقل فن‌آوری اطلاعات می تواند مورد استفاده ناظران قرار گیرد در صورتیکه حسابرسان مستقل از بانک باشند.

پاسخ

گزینه اول صحیح است.گزینه دوم نادرست است، زیرا حسابرسی جامع داخلی به صورت دوره‌ای انجام شده و نیاز به استمرار در طول دوره ندارد. گزینه سوم نادرست است. گزینه چهارم صحیح است لیکن ملاحظات استقلال رای ناظرین باید لحاظ گردد.

جمع بندی

حسابرسی داخلی عملکرد فن‌آوری اطلاعات به طور خاص بر دو موضوع اشاره دارد:

- شناسایی ریسک فن‌آوری اطلاعات
- ارزیابی نحوه برنامه ریزی و نظارت فن‌آوری اطلاعات

پیچیدگی و پختگی برنامه حسابرسی داخلی فن‌آوری اطلاعات باید در تناسب با اندازه و ماهیت زیرساخت های فن‌آوری اطلاعات بانک باشد. زیرساخت های فن‌آوری اطلاعات به خودی خود عامل پیچیدگی عملیات بانکی است.

حسابرسان مستقل فن‌آوری اطلاعات چگونگی نگهداری و حفاظت از دارایی های بانک را تحت تاثیر عملکرد فن‌آوری اطلاعات مورد بررسی قرار میدهند. ارزیابی کنترل های عمومی همانند ارزیابی کنترل های کاربردی انجام میشود.

اهتمام نظارت بر ارزیابی اثربخشی عملکرد حسابرسی فن‌آوری اطلاعات(مستقل و داخلی) متمرکز شده است.

چکیده

فن‌آوری اطلاعات چیست؟

فن‌آوری اطلاعات (IT) استفاده از کامپیوتر برای به دست آوردن ، ذخیره سازی. پردازش و توزیع اطلاعات تعریف شده است

عملکردهای اصلی فن‌آوری اطلاعات چیست؟

۱. توسعه و خرید

این عملکرد فن‌آوری اطلاعات توسعه نرم افزارها در داخل مؤسسه و یا خرید نرم افزارها و تجهیزات فن‌آوری اطلاعات است. مدیریت پروژه مؤثر منوط به شناخت این وظیفه و کاهش خطرات مربوط به ایجاد تغییرات در سیستم های موجود است.

۲. مدیریت اجرایی و پشتیبانی

این عملکرد فن‌آوری اطلاعات معطوف به اجرای عملیات روزانه مرکز داده با توجه عمیق به نگهداری از تجهیزات فیزیکی فن‌آوری اطلاعات است.

۳. تداوم کسب و کار و بازیابی اطلاعات

این وظیفه فن‌آوری مسئول تجزیه و تحلیل سناریو های ایجاد صدمات احتمالی و برنامه های تداوم فعالیت در هنگام بروز حوادث غیر مترقبه میباشد.

۴. مدیریت امنیت

این عملکرد فن‌آوری اطلاعات، چگونگی اجرای کنترلهای کافی جهت حفاظت از اطلاعات را بیان میدارد.

۵. فن‌آوری برون سپاری

این عملکرد فن‌آوری اطلاعات نحوه تعامل با اشخاصی که قسمتی از فعالیت های فن‌آوری اطلاعات در قالب برون سپاری به آنها محول میشود را بر عهده دارد.

ریسک های مربوط به فن‌آوری اطلاعات را نام ببرید.

ریسکهای مرتبط با فن‌آوری اطلاعات مشتمل بر ریسک عملیاتی ، ریسک استراتژیک ، ریسک شهرت و ریسک حقوقی می باشد.

چه کسی مسئول حاکمیت فن‌آوری اطلاعات است؟

- هیأت مدیره مسئول نهایی حاکمیت فن‌آوری اطلاعات می باشد.
- هیات مدیره می تواند کمیته فن‌آوری اطلاعات را برای انجام وظایف حاکمیت فن‌آوری اطلاعات تشکیل دهد.
- مسئولیت روزانه حاکمیت فن‌آوری اطلاعات بر عهده افسر ارشد اطلاعات که توسط کمیته راهبری انتخاب میگرددگذارده میشود.

وظایف اصلی حاکمیت فن‌آوری اطلاعات چه هستند؟

چهار وظیفه اصلی حاکمیت فن‌آوری اطلاعات عبارت هستند از:

- برنامه ریزی
- ارزیابی ریسک
- کنترل
- پایش[۱۰]

[۱۰] Monitoring

نکات کلیدی در مورد حسابرسی فن‌آوری اطلاعات چه هستند؟

حسابرسی فن‌آوری اطلاعات وظیفه دارد که بصورت خاص بر چگونگی مدیریت ریسکهای فن‌آوری اطلاعات و مدیریت برنامه ریزی فن‌آوری اطلاعات و کنترل های لازم از سوی بانک یا موسسه، نظارت داشته و عملکرد مدیریت اجرایی موسسه را ارزیابی نماید. بهترین روش انجام حسابرسی فن‌آوری اطلاعات اجرای حسابرسی فن‌آوری اطلاعات مبتنی بر ریسک است.

حسابرسی داخلی فن‌آوری اطلاعات را می توان به منظور کاهش هزینه ها و دستیابی به اهداف استراتژیک برون سپاری نمود.

حسابرسی مستقل فن‌آوری اطلاعات باید دو فاکتور زیر را مد نظر قرار دهد:

- ارزیابی کنترل های عمومی
- کنترل برنامه های کاربردی

خود را بیازمایید:

سوالات مربوط به نظارت بر فناوری اطلاعات تسلط شما را بر موضوع مورد ارزیابی قرار میدهد.
شش سوال در این آزمون وجود دارد که برخی از آنها ممکن است بیش از ۱ جواب داشته باشد. شما برای هر جواب صحیح یک امتیاز برای خود در نظر بگیرید.

سوال ۱ از ۶

کدام یک از موارد زیر جزء کنترلهای عمومی حسابرسی مستقل محسوب نمی شود؟

۱- سازماندهی و اجرا

۲- مستندسازی رویه ها

۳- نحوه دسترسی به تجهیزات و فایل های اطلاعاتی

۴- پردازش داده ها

پاسخ سئوال ۱ گزینه ۴

کنترل های عمومی که توسط حسابرسان مستقل مورد بررسی قرار می گیرند، عبارتند از :

- سازماندهی و اجرا
- مستند سازی رویه ها
- نحوه دسترسی به تجهیزات و فایل های اطلاعاتی
- سایر کنترل های مربوط به اجرای سامانه های اطلاعاتی

سوال ۲ از ۶

یکی از سطوح مسئولیت پذیری، تفویض اختیار به مدیر ارشد اطلاعات (CIO) است.

کدام یک از موارد زیر از وظایف مدیر ارشد اطلاعات است؟

۱. نظارت بر بودجه فن آوری اطلاعات
۲. نظارت بر توسعه برنامه های استراتژیک فناوری اطلاعات
۳. مدیریت اجرایی
۴. خرید تجهیزات فن آوری اطلاعات
۵. تایید فروشندگان طرف قرارداد موسسه
۶. ارتقاء مهارتهای شغلی و آموزش بخش فن‌آوری اطلاعات
۷. معماری فن آوری اطلاعات
۸. برنامه ریزی عالی استراتژیک

پاسخ سئوال ۲ موارد ۱،۳ ،۴، ۶، ۷، ۸

مسؤلیتهای مدیر ارشد اطلاعات به شرح زیر است:

- نظارت بر بودجه فن‌آوری اطلاعات
- مدیریت اجرایی
- بکار گیری جامع فن‌آوری اطلاعات
- ارتقاء مهارتهای شغلی و آموزش بخش فن‌آوری اطلاعات
- معماری فن‌آوری اطلاعات
- برنامه ریزی عالی استراتژیک

سوال ۳ از ۶

ناظران در جستجوی چه نوع کمک هایی در جهت افزایش توانایی های خود در ارزیابی عملیات فن‌آوری اطلاعات هستند؟

۱. استفاده از تخصص شرکت های مشاوره فن آوری اطلاعات
۲. همکاری با سازمان های دولتی که دارای تخصص در زمینه فن آوری اطلاعات هستند.
۳. اتکا به متخصصان فن آوری اطلاعات در درون بانک تحت نظارت

پاسخ سئوال ۳ موارد ۱ و ۲

تعداد ناظرین و متخصصین فن آوری اطلاعات محدود است ، به طوری که واحدهای نظارتی مجبور باشند از خدمات شرکت های مشاوره‌ای در زمینه فن آوری اطلاعات استفاده نمایند. آنها همچنین ممکن است با دیگر سازمان های دولتی همکاری کنند. با این حال ، ناظران نباید بر متخصصین فن آوری اطلاعات بانک بدون ارزیابی ظرفیت های آنها تکیه نمایند.

سوال ۴ از ۶

کدام یک از موارد زیر تعریف دقیقی از فناوری اطلاعات ارائه میکند؟

۱. فرایند توزیع و انتشار اطلاعات از طریق رایانه
۲. استفاده از فن آوری برای به دست آوردن، ذخیره‌کردن، پردازش و توزیع اطلاعات
۳. استفاده از کامپیوتر برای به دست آوردن ، ذخیره‌کردن، پردازش و توزیع اطلاعات مشتریان
۴. استفاده از نرم افزارهای پردازشی برای به دست آوردن ، ذخیره‌کردن، پردازش و توزیع اطلاعات

پاسخ سئوال ۴

مورد دوم صحیح است. فن آوری اطلاعات عبارت است از استفاده از فن آوری برای به دست آوردن، ذخیره‌کردن، پردازش و توزیع اطلاعات، سایر موارد یا محدود بوده و یا توصیف کاملی از فن آوری اطلاعات را ارائه نمی دهند.

سئوال ۵ از ۶

برون سپاری فن آوری اطلاعات دربانک ها به شکل روز افزونی انجام می پذیرد. نشان دهید کدامیک از اظهارات زیر صحیح می باشند.

۱. اصولا خدمات فناوری اطلاعات به دلیل انتقال ریسک های فن آوری اطلاعات به اشخاص ثالث برون سپاری می شوند.
۲. برون سپاری فن آوری اطلاعات مسئولیتهای بیشتری را بر دوش حسابرسان داخلی و مستقل تحمیل می نماید.
۳. برون سپاری فناوری اطلاعات موجب بی نیازی بانک به طرح تداوم فعالیت میگردد.
۴. نهادهای نظارتی قائل به کاهش ریسک های فن آوری اطلاعات از طریق تنوع برون سپاری خدمات هستند.
۵. **پاسخ سئوال ۵**

گزینه ۱ نادرست است برون سپاری عملکرد های فن آوری اطلاعات منجر به خروج ریسک‌ها و مسئولیت‌های بانک نمی‌گردد و عدم ایفای تعهدات شرکتهای ارائه دهنده خدمات با توجه به مفاد قرارداد تنها منجر به زیان شرکت شده لیکن ریسک های مرتبط با فن‌آوری اطلاعات به خود بانک بر می‌گردد. گزینه دوم درست می باشد. حسابرسان داخلی و مستقل علاوه بر ارزیابی هایی که در بانک انجام می دهند موظف به ارزیابی سامانه ها و کنترل های داخلی شرکت های ارائه دهنده خدمات فنی نیز هستند. گزینه ۳ نادرست است، بانکها موظف به تدوین طرحهای تداوم فعالیت در صورت ایجاد مشکل در اجرای صحیح وظایف محوله به شرکتهای ارائه دهنده خدمات فنی هستند. گزینه ۴ نیز نادرست است، زیرا برون سپاری منجر به خلق ریسک تمرکز میگردد. به عنوان مثال در جایی که شرکت ارائه دهنده خدمات فنی خدمات گسترده ای را به گروه‌های مختلف بانکی ارائه می نماید باعث ایجاد ریسک تمرکز در شبکه بانکی میگردد.

سوال ۶ از ۶

ریسک های مرتبط با هر یک از عبارات زیر را بیان نمایید.

۱. تأخیر در توسعه فن‌آوری اطلاعات در یک بنگاه اقتصادی بزرگ باعث عدم دستیابی به اهداف سودآوری آن بنگاه گردید.

۲. اطلاعات محرمانه مشتریان یک بانک به دلیل نقص فنی در سامانه امنیت اطلاعات شرکت ارائه دهنده خدمات فنی افشاء گردید.
۳. ایجاد اختلال در ارائه خدمات به مشتریان به دلیل قصور بخش تسویه (Back Office) منجر به کاهش قابل توجه سود بانکی گردید.
۴. تفسیر نامطلوب مفاد قرارداد با شرکت ارائه دهنده خدمات فنی باعث زیان بانک گردید.

پاسخ سئوال ۶

۱- ریسک استراتژیک به دلیل عدم توانایی بانک در دستیابی به اهداف استراتژیک بروز می نماید. ۲- بانک به دلیل شکست در حفظ امنیت اطلاعات محرمانه با ریسک شهرت روبرو میگردد. ۳- ریسک های فن‌آوری اطلاعات زیر مجموعه ریسک های عملیاتی هستند، اختلال در عملیات بانک باعث زیان عملیاتی می شود. ۴-ریسک حقوقی ناشی از اقدامات نامساعد حقوقی در زمینه فن آوری اطلاعات است.