Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

پژوهش‌های پولی-بانکی
سال هفتم، شماره ۱۹، بهار ۱۳۹۳
صفحات ۱۴۳-۱۶۰

ارزیابی سطح ریسک‌های عملیاتی در مؤسسات اعتباری با استفاده از روش کوبیت

علی حسن‌زاده [*] **امیرحسن قربانی** [†]

تاریخ دریافت: ۱۳۹۱/۰۸/۱۸ تاریخ پذیرش: ۱۳۹۲/۰۳/۲۰

چکیده

در این مقاله به توضیح اهمیت مدیریت ریسک‌های عملیاتی به‌واسطه پیاده‌سازی حسابرسی نظام اطلاعاتی منظم در مؤسسات اعتباری پرداخته می‌شود. روش‌شناسی اهداف کنترلی برای اطلاعات و فناوری‌های مرتبط یا کوبیت (COBIT) و نیز به‌ویژه چهارچوب قانونی ملی در جهت پیاده‌سازی حسابرسی نظام‌های اطلاعاتی در بانک‌های ایران با جزئیات بیشتری تشریح‌وتحلیل می‌شود. دراین‌ارتباط، روش و اصول پیاده‌سازی حسابرسی نظام‌های اطلاعاتی ارائه و قسمت‌های تکمیلی آن توضیح داده می‌شود. به‌منظور مطالعه میدانی نظام مذکور، روش لایکرت ۵گانه مقیاس‌بندی‌شده از «کاملاً نارضایت‌بخش» به «کاملاً رضایت‌بخش» استفاده شده است. نتایج ارزیابی و سنجش سطح ریسک‌های عملیاتی در بانک‌های ایران که به‌نحوی از این نظام بهره‌مند هستند برای سال ۱۳۹۱ ارائه می‌شود. دراین‌ارتباط، تأیید فرضیه‌های پژوهشی مطرح‌شده بیان‌کننده تاثیر مثبت معنادار روش حسابرسی بر مدیریت کارامد ریسک‌های عملیاتی است.

واژه‌های کلیدی: حسابرسی نظام‌های اطلاعاتی، روش لایکرت
طبقه‌بندی JEL: C32، C3، B12

* دانشیار، پژوهشکده پولی و بانکی، تهران؛ ali_hasanzadeh1968@yahoo.com (نویسنده مسئول)
† کارشناس ارشد مدیریت مالی، دانشگاه تهران، تهران؛ ahghorbani@ut.ac.ir

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

۱ مقدمه

مجموعه اهداف کنترلی برای اطلاعات و فناوری‌های مرتبط[1] یا کوبیت مجموعه‌ای از روش‌ها برای مدیریت فناوری اطلاعات است که توسط انجمن کنترل و ممیزی نظام‌ها و سازمان راهبری فناوری اطلاعات در سال ۱۹۹۶ ایجاد شد. کوبیت برای مدیران، ممیزان و کاربران فناوری اطلاعات مجموعه‌ای از سنجه‌ها، معیارها، فرایندها و روش‌های قابل‌قبول را ارایه می‌کند تا به آنان در افزایش سود حاصله از به‌کارگیری فناوری اطلاعات و توسعه کنترل و راهبری فناوری اطلاعات کمک نماید. این چهارچوب، به مدیران، ممیزان و کاربران این امکان را می‌دهد که نظام‌های فناوری اطلاعات خود را بهتر درک نمایند و سطح کنترل و امنیت موردنیاز سازمان خود را شناسایی و از طریق توسعه مدل راهبری فناوری اطلاعات به آن دست یابند.

براساس تجربه‌های به‌دست آمده در سال‌های اخیر، می‌توان دریافت که چنانچه ریسک‌های عملیاتی در مؤسسات مالی به شیوه‌ای صحیح مدیریت نشوند به ریسک‌های عملیاتی برای سازمان منجر می‌شوند که با تاثیرگذاری کاملاً منفی بر کسب‌وکار در بخش مالی خود را نمایان خواهند ساخت. به‌طور روشن، ریسک عملیاتی در مؤسسات مالی دربرگیرنده ریسک خسارت‌ها است و ناشی از فرایندهای داخلی ناکافی شامل نظام اطلاعاتی ناکافی و فناوری‌های پشتیبان در راهبری تراکنش‌های کسب‌وکار در سازمان هستند. برای مثال، قطع تنظیم معاملات می‌تواند تاثیرات منفی مستقیم (ازدست‌دادن درآمدها) و تاثیرات منفی غیرمستقیم (ریسک معروفیت) بر روی سازمان‌ها به دنبال داشته باشد.

هنگامی که تراکنش‌های مالی از طریق پشتیبانی فناوری‌های اطلاعاتی مدرن و نظام‌های اطلاعاتی راهبری شوند، روشن است که ریسک‌های همراه با استفاده از آن‌ها به حداقل خواهد رسید، اما بااین‌حال کسب‌وکارها نیاز به مدیریت مناسب نیز دارند. دراین‌ارتباط، گارتنر[2] (۲۰۱۰) بر ۴ نکته‌ای اصرار می‌کند که در آن ریسک‌های مربوط به فناوری اطلاعات (ریسک‌های عملیاتی) باید به‌عنوان ریسک‌های کسب‌وکار (راهبردی) تلقی گردد که رویه‌های نظارتی فناوری اطلاعات (ناظر بر کنترل مداوم) به‌منظور مدیریت آن باید جایگزین آن گردد. دراین‌ارتباط، در بسیاری از گزارش‌ها بیان می‌شود که پذیرش ریسک‌های عملیاتی به‌طور دقیق‌تر به صاحبان کسب‌وکار با اطلاعات مربوط به دارایی‌ها و

1 Control Objectives for Information and Related Technology
2 Gartner

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

فرآیندهای شغلی مربوط می‌شود. حاکمیت فناوری اطلاعات به‌عنوان یک مفهوم جدید در اواخر دهه ۱۹۹۰ معرفی گردید و در قرن بیست‌ویکم به علت فروپاشی بسیاری از شرکت‌های شناخته‌شده مانند انرون، وردکام و غیره و نیاز به نظام‌های گزارشگری و افشای بهتر، اهمیت یافت.[۱] همچنین، بندهای مربوط به آیین‌نامه‌های ملی و بین‌المللی به فهم مکانیسم‌های کنترل در محیط‌های فناوری اطلاعات و نظام اطلاعاتی امروزی کمک نموده و انگیزه زیادی در مورد موضوعات حاکمیت فناوری اطلاعات در سطح جهان ایجاد کرده است.[۲] تمرکز اصلی حاکمیت فناوری اطلاعات بر روی مسئولیت مدیریت اجرایی و هیئت مدیره در جهت کنترل صورت‌بندی و تحقق راهبرد نظام اطلاعاتی است که تنظیم نظام اطلاعاتی و کسب‌وکار را تضمین می‌کند و بر این اساس معیارهایی را به‌منظور سنجش ارزش کسب‌وکار نظام اطلاعاتی شناسایی کرده و ریسک‌های مربوط به نظام اطلاعاتی را به شیوه‌ای مؤثر مدیریت می‌کند.[۳]

در این مطالعه، بر اهمیت آیین‌نامه حسابرسی نظام اطلاعاتی (IS) تاکید می‌شود، به‌طوری‌که توسط آن سطح ریسک‌های عملیاتی می‌تواند موردسنجش قرار گیرد. چهارچوب آیین‌نامه نظارت حسابرسی نظام اطلاعاتی در مؤسسات اعتباری ایران شرح داده می‌شود و بحث می‌گردد و تحلیلی جامع بر روی شاخص‌های مؤسسات اعتباری نمونه ارائه می‌شود.

هدف اصلی از این مطالعه تاکید بر ضرورت سنجش سطح ریسک‌های مختلفی بوده که مؤسسات مالی در بخش‌های گوناگون خود با آن مواجه هستند. دراین‌ارتباط، به‌طور خاص بر روش‌ها و چهارچوب‌های سنجش و مدیریت سطح ریسک‌های عملیاتی در مؤسسات اعتباری ایران متمرکز هستیم.

پرسش اصلی مطالعه آن است که آیا استفاده از روش حسابرسی نظام اطلاعاتی به‌طور معناداری بر مدیریت ریسک‌های عملیاتی در مؤسسات مالی-اعتباری (بانک‌ها) در ایران مؤثر است؟ پرسش‌های فرعی پژوهش به این شرح است که آیا استفاده از روش حسابرسی نظام اطلاعاتی به‌طور معناداری بر جلوگیری از

۱) خطای انسانی و عمدی و غیرعمدی در مؤسسات مالی-اعتباری (بانک‌ها) در ایران مؤثر است؟

---

[1] Nicho & Cusack (2007)

[۲] همان

[3] Singleton (2010)

۲) خطاهای یارانه‌ای و عملیات مالی در مؤسسات مالی-اعتباری (بانک‌ها) در ایران مؤثر است؟
۳) خطا در تصمیم‌گیری‌ها، سوءاستفاده و تقلب در اسناد مالی، سرقت‌های مالی و اختلاس در تسویه حساب‌ها در مؤسسات مالی-اعتباری (بانک‌ها) در ایران مؤثر است؟

فرضیه اصلی پژوهش آن است که استفاده از روش حسابرسی نظام اطلاعاتی به‌طور معناداری بر مدیریت ریسک‌های عملیاتی در مؤسسات مالی-اعتباری (بانک‌ها) در ایران مؤثر است. فرضیه‌های فرعی مطالعه به این شرح است که استفاده از روش حسابرسی نظام اطلاعاتی به‌طور معناداری بر جلوگیری از

۱) خطای انسانی و عمدی و غیرعمدی در مؤسسات مالی-اعتباری (بانک‌ها) در ایران مؤثر است.
۲) خطاهای یارانه‌ای و عملیات مالی در مؤسسات مالی-اعتباری (بانک‌ها) در ایران مؤثر است.
۳) خطا در تصمیم‌گیری‌ها، سوءاستفاده و تقلب در اسناد مالی، سرقتهای مالی و اختلاس در تسویه حساب‌ها در مؤسسات مالی-اعتباری (بانک‌ها) در ایران مؤثر است.

۲ روش‌شناسی مطالعه

مسیری را که پیمودن آن برای انجام مطالعه حاضر پژوهشی درنظرگرفته شده است می‌توان در قالب چهار فاز زیر معرفی نمود:

به‌عنوان فاز اول مطالعات این پژوهش سعی می‌شود که در ابتدا با مطالعه ناهنجاری‌ها یا اتفاقات نامطلوب موجود در سازمان‌های مالی-اعتباری (بانک‌ها) ایران که به‌نحوی با مسئله ریسک‌های عملیاتی مؤسسات مالی در ارتباط هستند مجموعه‌ای از نشانه‌ها و علامت‌های راهنمایی‌کننده[1] را برای درک و کشف مسئله اصلی فراهم نماییم. درواقع، براساس تفکر نظامی چنین نشانه‌ها و یا علامت‌ها قادرند که پژوهشگر را در جهت شناخت بهتر فضای مسئله[2] و درنتیجه یافتن راه‌حل‌های مناسب راهنمایی نمایند. به‌طور مشخص، بانک‌ها و مؤسسات مالی-اعتباری (صادرات، تجارت، ملت، رفاه کارگران، پارسیان، پاسارگاد، اقتصاد نوین، سامان، کارآفرین، سرمایه، انصار، فردوسی و قوامین) که درواقع

[1] symptoms
[2] problem space

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

مجموعه‌ای از مؤسسات، بانک‌های خصوصی و دولتی در ایران را معرفی می‌نمایند، به‌عنوان جامعه آماری این مطالعه در نظر گرفته خواهد شد.

در فاز دوم تلاش می‌شود که با اجرای مصاحبه‌های حضوری یا غیرحضوری با کارشناسان و نخبگان[1] مرتبط با موضوع تحت پژوهش اطلاعات خام موردنیاز برای تحلیل‌های آتی فراهم گردد.

فاز سوم پژوهش به تحلیل محتوایی نتایج حاصل از اجرای مصاحبه‌های مذکور به‌منظور طراحی پرسش‌های کلیدی موردنیاز در پرسش‌نامه‌های ویژه این مطالعه اختصاص می‌یابد. در این فاز پس از یافتن متغیرهای موردنیاز برای انجام مطالعه و بررسی عمیق روش حسابرسی نظام اطلاعاتی بر مدیریت ریسک‌های عملیاتی نظام‌های مالی هر یک از سازمان‌ها با طراحی یک، یا چند پرسش‌نامه - در صورت لزوم-، و مراجعه مجدد به افراد موردمصاحبه واقع‌شده و نیز دیگر کارشناسانی که درک صحیح و عمیقی در ارتباط با نحوه کارکرد نظام تحت مطالعه دارند از شناسایی و فهم کامل متغیرهای موردنیاز برای انجام مطالعه و تحلیل چگونگی تاثیرگذاری روش حسابرسی نظام اطلاعاتی بر مدیریت ریسک‌های عملیاتی نظام مالی سازمان اطمینان حاصل خواهد شد.

فاز چهارم این پژوهش به دریافت تأیید نهایی از تمامی کارشناسان و خبرگان مطالعه‌شده در ارتباط با موضوع تحت پژوهش به‌منظور معتبر ساختن فرایند طی‌شده اختصاص خواهد یافت.

۳ جامعه آماری و روش نمونه‌گیری

به‌منظور انتخاب افراد جامعه آماری معرفی‌شده و به‌دست آوردن اطلاعات موردنیاز از طریق اجرای مصاحبه‌های حضوری یا غیرحضوری و نیز در اختیار قراردادن پرسشنامه‌های طراحی‌شده مربوطه برای شناسایی متغیرهای موردنیاز برای انجام مطالعه و بررسی عمیق نحوه تاثیرگذاری روش حسابرسی نظام اطلاعاتی بر مدیریت ریسک‌های عملیاتی نظام مالی سازمان‌های مورد مطالعه، تمامی کارشناسان و نخبگان عالی مرتبط با موضوع مورد پژوهش در مرحله نخست مطالعه و پس‌ازآن، از دیگر کارشناسان مرتبه عالی فعال و مرتبط

[1] در این پژوهش, واژه نخبه یا خبره به فردی اطلاق می‌شود که در زمینه مباحث مربوط به بحث تخصصی علوم مالی و حسابرسی دارای دست‌کم درجه تحصیلی کارشناسی ارشد بوده و همچنین از تجربه دست‌کم ۲۰ ساله نیز در فعالیت‌های مربوطه برخودار است.

با نظام مالی سازمان به‌عنوان مجموعه نهایی از افرادی که جامعه آماری این پژوهش را تشکیل میدهند در مرحله دوم این مطالعه استفاده گردیده است.

در مرحله نخست از انتخاب یک جامعه آماری مناسب برای انجام مطالعات میدانی این پژوهش از نمونه‌گیری غیراحتمالی «گلوله برفی»[1] استفاده شده است.

بنابراین، پس از انجام مصاحبه غیرحضوری با ۱۲ نفر از کارشناسان و نخبگان شناسایی‌شده، به‌عنوان افراد موردمطالعه در یک نمونه‌گیری غیراحتمالی و در اختیار قراردادن پرسش‌نامه‌هایی باز[2] به تجزیه‌وتحلیل مقدماتی نتایج حاصله پرداخته شده است که پژوهشگر را به سمت طراحی یک پرسش‌نامه چند گزینه‌ای و پرسش مجدد از تمامی افرادی که در نمونه‌گیری غیراحتمالی شرکت کرده بودند هدایت نموده است. نمونه‌گیری اخیر به‌عنوان یک نمونه‌گیری مقدماتی با حجم ۱۲ نمونه در سطح بانک‌های ایران معرفی شده تلقی می‌گردد که نتایج آن به‌عنوان پایه و راهنمایی برای تعیین حجم نمونه اصلی و نیز چگونگی انتخاب اعضای نمونه است.

جدول ۱

نمونه‌گیری مقدماتی و ویژگیهای مربوط به آن

عنوان	ویژگی‌های مربوط
ماهیت روش نمونه‌گیری	نمونه‌گیری غیراحتمالی
منطق موجود در رویکرد اتخاذ شده در فرایند نمونه‌گیری	گلوله برفی
حجم نمونه انتخاب‌شده	۱۲ واحد
روش استفاده شده برای گردآوری اطلاعات و داده‌ها	انجام مصاحبه‌های حضوری و غیرحضوری
ابزار به‌کارگرفته‌شده برای به‌دست‌آوردن اطلاعات/ داده‌ها	پرسش‌نامه‌های باز- بسته

در مرحله دوم انتخاب جامعه آماری مناسب برای انجام مطالعات میدانی پژوهش، با تکیه بر منطق توضیح‌داده‌شده، از نمونه‌گیری طبقه‌بندی ساده استفاده می‌گردد. به‌طور روشن‌تر، در این مرحله سعی می‌شود که برای هر یک از مؤسسات مالی-اعتباری (بانک‌ها) مطالعه شده، که درواقع به‌عنوان طبقات این مطالعه در نظر گرفته شده اند، به‌طور تصادفی تعدادی از کارشناسان و نخبگان مرتبط با موضوع تحت پژوهش که به‌نحوی نیز با نظام مالی سازمان نیز در ارتباط بوده‌اند موردمطالعه قرار گیرند و بدین‌ترتیب نمونه اصلی و نهایی

[1] snow ball

[2] open-ended questions

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

تعیین می‌گردد. دراین‌بین، مسئله مهم تصمیم‌گیری در مورد تعداد کارشناسان و نخبگان موردنیاز برای هریک از سازمان‌های موردمطالعه در این پژوهش است که از طریق فرایند محاسباتی زیر قابل تعیین است.

در رابطه ۱ فرض می‌شود که متغیرهای تعریف‌شده در جامعه تحت مطالعه، به‌عبارت‌دیگر، هر یک از پرسش‌های مطرح‌شده در پرسش‌نامه‌ها، از توزیع احتمال نرمال پیروی می‌کند. همچنین، باتوجه به اینکه نمونه‌گیری انجام‌شده در سازمان مذکور به‌صورت بدون جایگذاری بوده است. بنابراین، باتوجه به ادبیات آماری موجود در این زمینه از رابطه ۱ برای محاسبه حجم نمونه نهایی موردنیاز استفاده می‌کنیم.

$$x \sim N(\mu, \frac{\sigma^2}{n}) \qquad (۱)$$

در رابطه ۲، z نقطه‌ای از توزیع محور افقی احتمال نرمال است که به ازای مقادیر مختلف احتمال (سطح زیر نمودار) دارای مقادیر متناظر معینی است و برای $\alpha = ۰/۰۵$ مقدار عددی آن را تقریبا عدد ۲ درنظر می‌گیریم. در رابطه ۲، μ نشان‌دهنده میانگین توزیع احتمال متغیر موردمطالعه است. همچنین، r نیز کران بالای خطای نسبی است که توسط پژوهشگر تعیین می‌گردد و در این مطالعه ۳ درصد درنظرگرفته شده است. واضح است که N نشان‌دهنده حجم اصلی هر طبقه است که براساس اسناد موجود، ۳ نفر تعیین‌شده است.

$$n = \frac{n_.}{۱+n_./N}, \quad n_. = (\frac{z}{r}.\frac{S}{\mu})^۲ \qquad (۲)$$

دراین‌ارتباط، برای محاسبه حجم نمونه نهایی موردنیاز در این مطالعه لازم است که در ابتدا براساس نمونه‌گیری مقدماتی برآورد یا تخمینی از دو پارامتر μ و S حاصل گردد و سپس با تکیه بر مقادیر برآوردی حجم نمونه نهایی موردنیاز را مورد برآورد قرار دهیم. بر این اساس حجم نمونه نهایی موردنیاز برای هر یک از پرسش‌های مطرح‌شده در پرسش‌نامه‌های مربوط به هر جامعه تحت مطالعه معین شده‌اند. روشن است که نمی‌توان برای تمامی پرسش‌های مطرح‌شده در پرسش‌نامه‌های طراحی‌شده حجم نمونه نهایی یکسانی را انتظار داشت. بنابراین، کمترین حجم نمونه نهایی به‌دست آمده به‌عنوان حجم نمونه نماینده آن طبقه درنظرگرفته شده است.

براین‌مبنا، حجم نمونه نهایی موردنیاز برای مطالعه حاضر ۳۰ واحد نمونه‌گیری برآورد گردیده است که دربرگیرنده نخبگان، مدیران و کارشناسان عالی مرتبط با موضوع موردمطالعه هستند و در دوره زمانی که این پژوهش انجام گرفته است در سطح نظام مالی مؤسسات مورد مطالعه فعالیت داشته‌اند.

۴ مدیریت ریسک‌ها در مؤسسات اعتباری

روشن است که بانک‌ها و مؤسسات اعتباری با مجموعه‌ای از ریسک‌ها در فعالیت‌های کسب‌وکار روزمره خود روبرو هستند. دراین‌ارتباط، به‌نظر می‌رسد ارائه یک تعریف نظری برای هر یک از ریسک‌های ممکن می‌تواند در فهم بهتر مسئله مفید باشد.

۱) ریسک اعتباری، به مفهوم احتمالی است که وام‌گیرندگان بانکی یا شرکای دیگر موفق به برآورده‌کردن تعهدات خود مطابق با توافق‌های به‌عمل آمده نباشند. این ریسک شامل زیان‌های بالقوه ناشی از انواع اعتبارات بانکی مانند وام‌ها و اوراق بهادار بدهی است.

۲) ریسک نقدینگی، احتمالی است که اوراق بهادار تعیین‌شده یا اشکال دیگر دارایی بانک نمی‌تواند سریعاً در بازار برای جلوگیری از خسارت یا سوددادن در حد نیاز، معامله شود.

۳) ریسک‌های بازار، شامل انواع مختلف از ریسک‌هایی است که در ارتباط با کاهش در ارزش موجودی اوراق بهادار به علت تغییرات در نرخ‌های سود، نرخ‌های تسعیر یا قیمت‌های سهام در بازارهای مالی است.

۴) ریسک شهرت، احتمال تجربه آسیب‌ها یا خسارت‌ها به دلیل دریافت‌های منفی عموم از موسسه بوده که روابط کاری جدید، آتی و موجود با مشتریان، شرکا، سهام‌داران و سرمایه‌گذاران است که مورد پرسش و پاسخ واقع می‌شود.

۵) ریسک عملیاتی، شامل ریسک زیان‌هایی است که از فرایندهای داخلی ناکافی ناشی می‌شوند و دربرگیرنده حمایت از نظام اطلاعاتی ناکافی بوده که از تنظیم قراردادها و معاملات کاری حمایت می‌کند. ریسک‌های عملیاتی زیادی وجود دارند که منجر به اظهار اشتباه نمای ریسک بانکی می‌گردد و موسسه در معرض خسارت‌های جدی یا ریسک شهرت قرار می‌گیرد. در فعالیت‌ها و اعمال دقیق مدیریت و نظارت بر ریسک

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

عملیاتی، کمیته بال[1] نظارت بر بانکداری بر چندین مورد کاری چنین رویدادهایی تاکید کرد، که به‌طور مفصل در زیر به آن پرداخته می‌شود.

- تقلب‌های داخلی به شکل گزارشگری اشتباه موقعیت‌ها، دزدی کارمند به نفع خود، دزدی پول به اسم شخص دیگر و موارد دیگری از این قبیل.
- سوءاستفاده‌ها و ورشکستگی‌های فعالیت‌های کسب‌وکار که شامل سوءاستفاده در اطلاعات محرمانه مشتری، فعالیت‌های تجاری ناصحیح در حساب بانکی، پول‌شویی، حمایت مالی‌کردن از تروریسم یا دیگر اشکال جرم، فروش محصولات غیرمجاز، گریز از مالیات، صدور پرداخت پیش‌نویس‌های تقاضا در محدوده‌های تعیین‌شده، که موفق نمی‌شود که الزامات نظم‌دهنده را برآورده کند.
- تقلب‌های خارجی مانند دزدی، امضای جعلی، سفته‌کردن چک و آسیب‌ناشی از هک‌کردن کامپیوتر.
- انتخاب منفی در راهبردهای استخدام و ناکامی‌های سازماندهی امنیت محل‌کار شامل نقص قوانین امنیت و سلامت کارمند، ادعای تبعیض و ...
- خسارت به دارایی‌های مادی که از طریق تروریسم، تخریب، زلزله، آتش‌سوزی، سیل و دیگر ریسک‌های محیطی ایجاد می‌شود.
- وقفه در کسب‌وکار مانند نارسایی‌های نظام سخت‌افزاری و نرم‌افزاری، مشکلات ارتباط از دور و قطع برق، دردسرهای مدیریت فرایند، تحویل و اجرا که شامل خطاهای ورود داده‌ها، قصورات مدیریت وثیقه، اسناد قانونی ناکامل، دسترسی به تأیید نرسیده به حساب‌های مشتریان، عملکرد غلط مشارکتی غیرمشتری و مشاجرات فروشنده.

۵ ادبیات نظری

حسابرسی نظام اطلاعاتی اساساً به بخش واقعاً تحلیلی حاکمیت فناوری اطلاعات اشاره دارد که سطح عملکرد نظام اطلاعاتی می‌تواند اندازه‌گیری و رشد نظام اطلاعاتی برآورد گردد.[2] حسابرسی نظام اطلاعاتی حوزه گسترده‌ای از فعالیت‌های حسابرسی، مدیریتی، تحلیلی و فناورانه را ارائه می‌دهد که هدف اصلی مرور کامل کارآمدی‌های رویه‌های کنترلی در بخش‌های مختلف نظام اطلاعاتی، انجام آزمون‌های تحلیلی و جمع‌آوری اطلاعات بوده

[1] Basel committee

[2] Mashour & Zaatreh (2008)

که به ارزیابی سطح ریسک‌های عملیاتی کمک می‌کند و درنهایت به هیئت مدیره شرکت در سنجش‌های متقابل صحیح در جهت کاستن ریسک‌های غیرقابل‌قبول کمک می‌کند.

کالدول[1] (۲۰۰۹) بیان می‌کند که متخصصان امنیت فناوری اطلاعات بنگاه اقتصادی با وضعیت پیچیده و حتی متناقض روبرو هستند که همانند بحران اقتصادی جهانی تداوم دارد. در هر دوره از فعالیت، منابع مالی و انسانی بالای دردسترس، تغییرات سریع و ریسک گسترده محیطی و پاسخ به الزامات مربوط قانونی و تنظیمی روبه گسترش باید مدیریت شود. دامری[2] (۲۰۰۹) مزایای همراه نظام اطلاعاتی را ترجیحاً از طریق نقش حاکمیت فناوری اطلاعات مورد تحلیل قرار می‌دهد. ماشور و زاتره[3] (۲۰۰۸) اثر مثبت و مؤثر نظام اطلاعاتی را بررسی و به آن اعتبار می‌بخشد. انجمن حسابرسان داخلی راهنمای برآورد ریسک فناوری اطلاعات منتشر کرد و گزارش داد که اعمال یک اصول استاندارد به حسابرس کمک خواهد کرد که بر آنچه واقعاً در برآورده‌ساختن اهداف و به‌حداقل‌رساندن ریسک‌های عملیاتی سازمان مهم است، تمرکز کند. گارتنر (۲۰۱۰) به این نتیجه می‌رسد که هیچ استانداردی نیست که تمامی بخش‌های حاکمیت فناوری اطلاعات و بازبینی نظام اطلاعاتی را با خیلی از بخش‌های متقارن پوشش دهد. سینگلتون[4] (۲۰۱۰) در مورد مدل فناوری اطلاعات با توجه به بندهای تنظیمی نظارت بر کنترل حداقلی فناوری اطلاعات استدلال می‌کند که شامل مفهوم نظارت بوده که از میزان ریسک‌های در گزارش مالی کاسته و پذیرش تنظیمی را تقویت می‌کند. سینگلتون همچنین اعلام می‌کند که آزمون کردن کنترل‌های فناوری اطلاعات به‌علت قانون ساربینز-اکسلی[5] و افزایش تکیه و اعتماد به کنترل‌های فناوری اطلاعات ضروری شده است.

بنابراین، با مرور ادبیات نظری مرتبط با موضوع مورد مطالعه به این نتیجه می‌رسیم که شواهد اندکی در ارتباط با این مهم که چگونه بندهای تنظیم حسابرسی نظام اطلاعاتی به مدیریت ریسک عملیاتی کمک می‌کند در دسترس است. بنابراین، سعی بر این است که شکاف پژوهش را با خطاب قرار دادن کاربردها و کارآمدی‌های آن پر کنیم. به‌طور مشخص،

[1] Caldwell
[2] Dameri
[3] Mashour & Zaatreh
[4] Singleton
[5] Sarbanes-Oxley

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

علاقمندیم تا بدانیم که آیا بندهای تنظیمی ملی در بازبینی نظام اطلاعاتی به بهبود رویه‌های مدیریت ریسک احتمالی و حاکمیت فناوری اطلاعات کمک خواهند نمود یا خیر.

۶ چهارچوب‌های معمول در حوزه مدیریت فناوری اطلاعات و حسابرسی نظام اطلاعاتی

هدف اصلی فعالیت‌های حسابرسی نظام اطلاعاتی بررسی رویه‌های کنترلی همراه با نظام اطلاعاتی شرکت، گردآوری شواهد تحلیلی درباره اشتباهات ممکن، ارزیابی سطح ریسک‌های عملیاتی برای زمینه‌های کنترلی متفاوت و پیشنهاد معیارهای کنترلی مناسب به مدیریت است. این مهم به‌طور روشن به این مفهوم است که با درگیرشدن شرکت‌های حسابرسی نظام اطلاعاتی به‌طور دوره‌ای می‌توان عملکرد حاکمیت فناوری اطلاعات و رشد نظام اطلاعاتی را اندازه‌گیری و ارزیابی نمود. چنین تمایلاتی عمدتاً با قوانین تنظیمی خاص ایجاد انگیزه می‌کنند تا نسبت به ابتکارات ارزش‌افزوده فناوری اطلاعات. حاکمیت فناوری اطلاعات و بازبینی نظام اطلاعاتی تاحدودی با قوانین خارجی مانند قانون ساربینز-اکسلی، بال ۲ و غیره هدایت می‌گردند. شرکت‌هایی که در بازارهای چندملیتی فعالیت می‌کنند مجبورند از چندین مقررات قانون تبعیت کنند که از طریق حقوق مردمی در سطح بین‌المللی یا ملی ایجاد گردیده است. به‌عنوان مثال، SOX در ایالات متحده و نیز بال ۲ در اروپا. همچنین، NCA[1] به‌عنوان بال ۲ شناخته می‌شود که درواقع به‌صورت مجموعه‌ای از پیشنهاداتی است که توسط کمیته بال در نظارت بانکی مطرح گردیده است که کافی‌بودن سرمایه بانک‌ها را در رابطه با در معرض ریسک قرارگرفتن تنظیم می‌کند. بندهای بال ۲ به بانک فعال در سطح بین المللی در کشورهای گروه ۱۰ اعمال می‌شود. اتحادیه اروپا یک اصل را پذیرفته است و بندهای التزام را برای تمامی بانک‌ها در کشورهای عضو اتحادیه اروپا تا سال ۲۰۰۷ ارائه می‌دهند. به‌طور مشخص، Accord با الزامات نظام اطلاعاتی بانک‌ها سروکار دارد که به‌عنوان بخشی از ریسک عملیاتی به‌عنوان یک کل، تنها از طریق اصول حاکمیت فناوری اطلاعات مطرح است. با توجه به اینکه ممکن نیست قوانین دشواری را با احتساب تغییرات فناوری سریع و تفاوت‌های میان بانک‌ها بنا نهاد، کمیته بر اهمیت اعتقاد به نظام اطلاعاتی، به‌خصوص در اصلاح امنیت اطلاعات و در دسترس‌بودن نظام، تاکید فراوان دارد. این مهم به این مفهوم است که شروط Accord برای بانک‌ها

[1] New Capital Accord

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

آزادی عمل بیشتری را در ارتباط با تصمیم‌گیری در مورد سنجش‌های کاهش ریسک عملیاتی به بار آورده‌اند که با تحقق نظام اطلاعاتی یا فناوری اطلاعاتی مطرح گردیده است. اما همزمان به بانک‌ها واداشته است که فعالیت‌های حاکمیت فناوری اطلاعات قطعی را باید به‌کار گیرند تا مطیع باشد. در چند سال اخیر، چندین گروه در سطح جهان شکل گرفته‌اند که با بهترین اعمال حاکمیت فناوری اطلاعات و چهارچوب‌ها شناخته‌شده‌اند که به مدیریت در ریسک‌های عملیاتی و سنجش تکامل نظام اطلاعاتی کمک می‌کنند.

۷ اصول رویکرد کوبیت در پیاده‌سازی نظام حسابرسی نظام اطلاعاتی

به‌طور روشن، کوبیت چهارچوب حاکمیت فناوری اطلاعات بوده که به‌طور گسترده پذیرفته‌شده و با هدف کلیدی کنترل فناوری اطلاعات سازماندهی گردیده و به کنترل‌های فناوری اطلاعات جامع تقسیم‌بندی گردیده است. نوع جدید کوبیت ۴.۱، فناوری اطلاعات را به چهار حوزه کلیدی تقسیم‌بندی می‌کند که این خود نیز به ۳۴ فرایند کلیدی فناوری اطلاعات تقسیم‌بندی می‌شود و سپس به بیش از ۳۰۰ اهداف کنترلی فناوری اطلاعات جرئی تقسیم‌بندی می‌کند که توسط TTGi و iSACA ظهور یافته‌اند. واقعیت آن است که کوبیت کاملاً پذیرفته‌شده است و به‌عنوان یک چهارچوب برای تحقق راهبردهای حاکمیت فناوری اطلاعات و رویه‌ها به‌منظور هدایت بازرسی نظام اطلاعاتی است که یک استاندارد جامع و وسیع شامل تمامی فعالیت‌ها، فرایندها و خدمات بوده که به شرکت‌ها کمک می‌کند تا سطح ریسک‌های عملیاتی را مدیریت کنند.

۸ تجزیه‌وتحلیل داده‌ها

روشن است که پس از گردآوری داده‌ها و اطلاعات آماری موردنیاز ضروری است که با تکیه بر مدل‌های تصادفی و اصول معرفی‌شده در آمار استنباطی به تجزیه‌وتحلیل داده‌ها در محیط یکی از نرم‌افزارهای آماری دراختیار پرداخته شود. برای این منظور، در این پژوهش با استفاده از آزمونهای آماری وابسته (آزمون تی‌استیودنت) در محیط نرم‌افزاری SPSS نسخه ۱۶ سعی شده است تا خروجی‌های موردنظر برای بررسی‌وتحلیل نحوه تاثیرگذاری روش حسابرسی IS بر مدیریت ریسک‌های عملیاتی هر یک از مؤسسات مالی موردمطالعه فراهم گردند. شواهد تجربی تأیید می‌کند که طرز عمل درباره متغیرهای ترتیبی، درصورتی که طبقه‌ها فاصله یکسانی داشته باشند، می‌تواند مانند مقیاس‌های فاصله‌ای باشد. بنابراین، بسیاری از تجزیه‌وتحلیل آمار پارامتری برای متغیرهای ترتیبی موجه دانست. به‌طور روشن‌تر، اگر در فرایند یک پژوهش از مقیاس ترتیبی لایکرت ۵تایی یا بیشتر (از

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

خیلی کم تا خیلی زیاد یا قویاً مخالف تا قویاً موافق) استفاده شده باشد، می‌توان از یک نظام کددهی با تخصیص اعداد ۱ تا ۵ استفاده نمود و بدین‌ترتیب بسیاری از تجزیه‌وتحلیل‌های آماری را اعمال نمود.

با توجه به داده‌های به‌دست‌آمده از آخرین نمونه انتخابی که جمعیت معناداری از نخبگان و کارشناسان (مرتبه عالی، میانی و پایین) فعال و مرتبط با مسئله مطالعه تاثیرگذاری روش حسابرسی IS بر مدیریت ریسک‌های عملیاتی نظام مالی مؤسسات تحت مطالعه (بانک‌ها) را که به‌نحوی نیز با نظام مذکور در ارتباط بوده‌اند به خود اختصاص می‌دهد قادر هستیم هر یک از فرضیه‌های مطرح‌شده را آزمون نماییم.

در اینجا سعی شده است تا هر یک از متغیرهای تعریف‌شده به تنهایی مورد آزمون قرار گیرد و همان‌طور که ملاحظه می‌گردد نتایج آزمون‌های آماری مذکور تأیید کننده برقراری تمامی شاخص‌های (فرضیه‌ها) تعریف شده در بالا هستند (جدول ۲).

۹ نظام پیشنهادی برای حاکمیت فناوری اطلاعات و حسابرسی نظام اطلاعاتی در بانک‌های ایران

در ارتباط با معرفی نظام پیشنهادی مطالعه حاضر برای حاکمیت فناوری اطلاعات و حسابرسی نظام اطلاعاتی در بانک‌های ایران، چهارچوب آیین‌نامه حسابرسی نظام اطلاعاتی باید با پیشنهاد بانک مرکزی انجام پذیرد و هدف اصلی از آن معرفی قوانین التزامی و مدیریت مؤثر سطح ریسک‌های عملیاتی است و می‌تواند تحت عنوان نظام اطلاعاتی یا فناوری اطلاعاتی مرتبط با ریسک در مؤسسات اعتباری (بانک‌ها و غیره) نامیده شود. دراین‌ارتباط، قانون در مورد مؤسسات اعتباری و تصمیم‌گیری در مورد مدیریت نظام اطلاعاتی کافی است و همچنین سنگ بنای قانون نیز باید حاکمیت فناوری اطلاعات باشد به‌طوری‌که هر موسسه اعتباری را وادار ساخته تا حسابرسی نظام اطلاعاتی به ویژه خارجی را اجرا نمایند (سنجش ریسک‌های عملیاتی) و گزارش‌های موردنیاز را برای افرادی که متعادل‌کننده سازمان هستند و همچنین برای هیئت مدیره شرکت فراهم سازند. آیین‌نامه‌ها به تنهایی براساس کوبیت بوده و در رابطه با چهارچوب و حوزه ارزیابی تکامل استفاده از ISAT است. یک چهارچوب منظم می‌تواند در ۱۱ حوزه که حوزه حسابرسی نظام اطلاعاتی را در مؤسسات اعتباری در ایران تعیین می‌کنند ارائه می‌گردد. این حوزه‌ها در ادامه آمده‌اند:

- مدیریت امنیت نظام اطلاعاتی؛

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

- مدیریت واقعه و ریسک نظام اطلاعاتی؛
- حقوق دسترسی کاربر و مدیریت رمز عبور؛
- مدیریت شبکه کامپیوتر و حفاظت از کد در برابر عنادورزی‌ها؛
- مدیریت ریسک منابع فناوری اطلاعات؛
- مدیریت دارایی نظام اطلاعاتی و مدیریت امنیت مادی؛
- مدیریت تغییر و ظهور نظام اطلاعاتی؛
- مدیریت تداوم کار؛
- پشتیبانی، کارکردی و ضبط نظام؛
- آزمون رویه‌های کنترل نظام اطلاعاتی یا فناوری اطلاعات در فرایندهای کلیدی کسب‌وکار؛ و
- تحقق قانون داخلی مربوط به نظام اطلاعاتی یا فناوری اطلاعات.

جدول ۲

آزمون آماری فرضیه‌های پژوهشی

سطح تاثیرگذاری روش حسابرسی IS در جلوگیری از:	میانگین	انحراف معیار	آماره تی استیودنت	سطح معناداری
خطاهای انسانی و عمدی	۴/۵۱۴۳	۰/۶۵۸۴۹	۲۰/۱۶۷	۰/۰۰
خطاهای انسانی غیرعمدی	۴/۵۱۴۳	۰/۷۸۱۰۸	۱۷	۰/۰۰
خطاهای یارانه‌ای	۴/۳۷۱۴	۰/۹۴۲۰۲	۱۲/۷۶	۰/۰۰
خطاهای عملیات مالی	۴/۲۱۸۷	۰/۲۵۸۱	۱۲/۳۷	۰/۰۰
خطا در تصمیم‌گیری‌ها	۴/۱۴۹۳	۰/۷۴۱۰	۸/۳۴	۰/۰۳۱
سوءاستفاده و تقلب در اسناد مالی	۴/۸۸۲۵	۰/۴۲۱۳	۲۴/۰۳	۰/۰۰
سرقت‌های مالی	۴/۸۷۲۵	۰/۶۹۸۱	۱۴/۴۳	۰/۰۰
اختلاس‌های مالی	۴/۹۲۱۰	۰/۶۸۵۴	۱۵/۰۷	۰/۰۰
اختلاس در تسویه‌حساب‌ها	۴/۷۳۰۹	۰/۳۸۹۱	۲۳/۹۳	۰/۰۰
اختلاس در گزارش‌های مالی	۴/۲۲۴۷	۰/۹۱۹۳	۷/۱۶	۰/۰۲

یادداشت. درجه آزادی در تمامی موارد ۲۹ است.

با توجه به چهارچوب تنظیمی، هیئت مدیره هر موسسه مالی در ایران می‌تواند مسئول کاهش ریسک‌های عملیاتی باشد که به تک‌تک حوزه‌ها مربوط می‌شود و به‌طور مؤثر سطح ریسک نظام اطلاعاتی یا فناوری اطلاعات قابل‌قبول را مدیریت می‌کنند. برخی از این مسئولیت‌های آیین‌نامه‌ای در ادامه آمده‌اند:

- عضو هیئت مدیره‌ای را که مسئول مدیریت و کنترل نظام اطلاعاتی است را معرفی می‌کند.

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

- قوانین داخلی را در نظارت فناوری اطلاعات می‌پذیرد و مسئولیت‌ها را برای نظارت آنها تعیین می‌کند.
- معیارها و روش‌ها را برای مطلع ساختن هیئت‌های نظارتی و مدیریتی حقایق مرتبط را تعریف می‌کند که به ایمنی و کارکرد نظام اطلاعاتی مربوط می‌شوند.
- راهبرد نظام اطلاعاتی را تعیین می‌کند.
- مسئولیت‌های آشکار را برای مدیریت نظام اطلاعاتی تعیین می‌کند.
- کارکرد CISO مستقل را معرفی می‌کند(کارمند امنیت اطلاعات اصلی).
- کمیته هدایت فناوری اطلاعات را معرفی می‌کند.
- اصول مدیریت ریسک نظام اطلاعاتی را معرفی می‌کند
- هیئت مدیره که مسئول وضع سطح قابل قبولی از ریسک به نظام اطلاعاتی است (ریسک مؤثر).
- اطلاعات را طبقه‌بندی و حفاظت می‌کند.
- نظام مدیریت حقوق دسترسی کاربر را وضع می‌کند که شامل ثبت نام، مسئولیت، شناسایی، سندیت و نظارت از حقوق دسترسی کاربر است.
- تغییرات در مؤلفه‌های نرم‌افزاری نظام اطلاعاتی به ثبت و سندیت به‌منظور حادثه نیازمندند که همراه با زمان حادثه است.
- هیئت مدیره مسئول وضع فرایند برنامه ریزی فرایند کسب‌وکار است.
- هیئت مدیره مسئول وضع فرایند برگشت داده‌ها است که در محل دیگر ذخیره گردیده‌اند.

۱۰ اصول پیشنهادی برای اجرای حسابرسی نظام اطلاعاتی در ایران:

در ارتباط با اصول پیشنهادی برای حسابرسی نظام اطلاعاتی در ایران، هر موسسه مالی مجبور به اجرای حسابرسی‌های نظام اطلاعاتی داخلی و خارجی با هدف سنجش سطح ریسک‌های عملیاتی است. هر موسسه نظام اطلاعاتی خارجی باید به گزارش جامع ختم گردد که حسابرسان نظام اطلاعاتی برای هیئت مدیره اعتباری ارائه می‌دهند. دراین‌ارتباط، بخش‌های اصلی گزارش‌های حسابرسی نظام اطلاعاتی خارجی شامل موارد زیر است:

- تشریح اصول حسابرسی نظام اطلاعاتی و روش‌های سنجش سطح ریسکهای عملیاتی؛
- حوزه حسابرسی‌های نظام اطلاعاتی (حوزه‌های کنترل نظام اطلاعاتی و اهداف وابسته به تعیین حسابرسی نظام اطلاعاتی)؛

- نتایج حسابرسی کامل و مفصل رویه‌های کنترل نظام اطلاعاتی در حوزه‌های بازبینی انتخاب؛
- سنجش سطح ریسک عملیاتی برای هر بخش حسابرسی با توصیه هایی برای هیئت مدیره برای سنجش‌های اصلاحی؛ و
- پاسخ هیئت مدیره برای یافته‌های بازبینی‌های نظام اطلاعاتی.

۱۱ اسناد حسابرسی نظام اطلاعاتی

حسابرسان نظام اطلاعاتی نیازمند درک تحقق کامل رویه‌های کنترل در فرایندهای کسب‌وکار کلیدی و حمایت نظام اطلاعاتی یا فناوری اطلاعات هستند. همانگونه که قبلا نیز بیان شد هدف اصلی حسابرسی نظام اطلاعاتی مرور کامل کارامدی‌های رویه‌های کنترل در بخش‌های مختلف نظام اطلاعاتی در مؤسسات اعتباری است، به‌طوری‌که سطح ریسک‌های عملیاتی را مورد سنجش قرار می‌دهد و سنجش‌های صحیح را برای اعضای هیئت مدیره پیشنهاد می‌کند این به این مفهوم است که حسابرسان نظام اطلاعاتی نیاز به سنجش و مرور ارقام بیشتری از کنترل داخلی نظام اطلاعاتی، آزمون‌های تحلیلی انبوه اجرای هستند(به‌عنوان مثال آزمایش نفوذ شبکه کامپیوتری، تداوم کسب‌وکار و آزمایشات بازگشت رخداد، آزمایش حقوق دسترسی منطقی کاربران نظام اطلاعاتی و غیره) یک سری از شواهد حسابرسی را گردآوری و سطح ریسکهای عملیاتی را می‌سنجند و گزارش حسابرسی جامع نظام اطلاعاتی را تهیه می‌کنند. هر سطح حسابرسی باید کاملاً با هدف گردآوری شواهد حسابرسی کافی مرور و تجدید نظر گردد به‌طوریکه حسابرسان نظام اطلاعاتی را توانمند می‌کنند که کارایی رویه‌های کنترل را ارزیابی نمایند. به‌عنوان مثال، فرایندهای کسب‌وکار کلیدی عادی در مؤسسات مالی که نظام اطلاعاتی را حمایت می‌کند، نیاز به ارزیابی‌های زیر است:

- سپرده‌های خرده‌فروشی و حقوقی؛
- وام‌های خرده‌فروشی و حقوقی؛
- فرایند خزانه‌داری؛
- فرایند مدیریت ریسک؛
- پردازش دستمزد؛ و
- فرایند محصور صورت حساب مالی.

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019

سطح تکامل فرایندهای مدیریت نظام اطلاعاتی در تمام بخش‌های ۱۱گانه حسابرسی به‌طور منظم براساس مصاحبه‌ها، فرایندهای آزمون سازی و بازبینی‌های جامع است. دراین‌ارتباط، سطوح رشد در تمام بخش‌های حسابرسی براساس سنجش کوبیت است.

۰- فقدان تکامل نظام اطلاعاتی و یا فرایندهای کنترل نظام اطلاعاتی
۱- رشد نظام اطلاعاتی اولیه، غیرعمومی یا فرایندهای کنترل نظام اطلاعاتی؛
۲- تکرارپذیر اما فرایندهای کنترل نظام اطلاعاتی شهودی؛
۳- فرایند معین در فرایندهای کنترل نظام اطلاعاتی؛
۴- فرایندهای کنترل نظام اطلاعاتی قابل سنجش و مدیریت؛
۵- رشد نظام اطلاعاتی مطلوب و یا فرایندهای کنترل نظام اطلاعاتی؛
۶- گزارش حسابرسی نظام اطلاعاتی باید ارائه گردد و باید مورد موافقت هیئت مدیره موسسه مالی قرار گیرد، درحالی‌که کپی گزارش باید با اجزای آیین‌نامه مطرح گردد؛ و
۷- بانک مرکزی ایران و واحدهای نظارتی آنها.

۱۲ بحث و نتیجه گیری

این مطالعه بر اهمیت چهارچوب تنظیمی بازبینی نظام اطلاعاتی تأکید دارد، به‌طوریکه مؤسسات مالی را در جهت مدیریت سطح ریسک عملیاتی هدایت می‌کند. با تأیید هر یک از فرضیه‌های پژوهشی، مطالعه حاضر نظارت فناوری اطلاعات و اصطلاحات حسابرسی نظام اطلاعاتی به‌خصوص چهارچوب آیین‌نامه ملی به‌طور مشخص و خارجی بانک‌های ایران مفید ارزیابی می‌کند و براین‌اساس اصول اجرای حسابرسی نظام اطلاعاتی ارائه گریده است. این مطالعه با تحقیق در مورد جزئیات دیگر فعالیت‌های اعمال قدرت فناوری اطلاعات در مؤسسات مالی-اعتباری (بانک‌ها)، در شرایطی کنونی ریسک اعمال مدیریت را تا حدی نامطلوب ارزیابی می‌کند. دراین‌ارتباط، به‌طور عمومی، می‌توان پیاده‌سازی نظام حسابرسی هدایت نظام اطلاعاتی خارجی را برآورد کردن سطح ریسک‌های اجرایی دانست به‌طوری‌که افراد مربوطه و مسئول می‌تواند آن را با استفاده از متدولوژی استاندارد پذیرفته‌شده جهانی مثل کوبیت انجام دهند. بهبود در رشد نظام اطلاعاتی و فعالیت‌های اعمال قدرت فناوری اطلاعات آشکار و واضح است (کوبیت یک متدولوژی خیلی دقیق است) تا حدی سطح نارضایت‌بخش ریسک اجرای مدیریتی مربوط به این است که هنوز روش‌ها و روال‌کاری کنترل ناکارآمد در بعضی مناطق کلیدی اعمال قدرت فناوری اطلاعات وجود ندارد (مثل BCP، امنیت اطلاعات، دسترسی به شبکه کامپیوتر، به کار گرفتن IS/IT و غیره).

ازسوی‌دیگر، مدیریت بانکی نیز باید دیدی واضح و اعتبار کافی داشته باشد تا توصیه‌ها و پیشنهادهای حسابرسان نظام اطلاعاتی و امید برای سطح رضایت مدیریت اجرایی ریسک اجرا گردد.

فهرست منابع

Caldwell, F. (2009). *Selecting and applying GRC frameworks and standards*. Gartner Symposium ITExpo.

Dameri, R. P. (2009). Improving the benefits of IT compliance using enterprise management information systems. *The Electronic Journal Information Systems Evaluation*, 12(1), 27-38.

Gartner (2010). *Magic quadrant for continuous controls monitoring*, Gartner Inc.

Mashour, A., Zaatreh, Z. (2008). A framework for evaluating effectiveness of information systems at Jordan banks: an empirical study. *Journal of Internet Banking and Commerce*, April 2008, 13(1), 1-14.

Nicho, M. & Cusack, B. (2007). *A metrics generation model for measuring the control objectives of information systems audit*. Proceedings of the 40th Annual Hawaii International Conference on System.

Singleton, T. (2010). The minimum IT controls tob assess in a financial audit, *ISACA Journal*, 2, 1-5.

Downloaded from jmbr.mbri.ac.ir at 4:41 +0330 on Tuesday November 19th 2019