

اعضای محترم کمیته عالی حسابرسی

موضوع: گزارش ارزیابی کلی کنترل های داخلی بانک سامان (سهامی عام)

۱. هدف :

در اجرای تکالیف مقرر در برنامه مصوب مدیریت حسابرسی داخلی و مطابق با "رهنمودهایی^۱ برای نظام موثر کنترل های داخلی بانک مرکزی به شماره م/ب/۱۱۲۲ به تاریخ ۱۳۸۶/۰۳/۳۱ و بر اساس "چارچوب یکپارچه کنترل های داخلی کوزو منتشره در سال ۲۰۱۳" کفایت و اثربخشی اجزای کنترل های داخلی، مورد ارزیابی قرار گرفته است.

۲. دامنه و دوره رسیدگی :

رسیدگی ها در حیطه اجزای کنترل های داخلی (محیط کنترلی، ارزیابی ریسک، فعالیت های کنترلی، اطلاعات و ارتباطات و فعالیت های نظارتی) در سطح بانک می باشد. جهت رسیدگی از پرسشنامه های ارزیابی کنترل های داخلی که بر مبنای دستورالعمل بانک مرکزی و چارچوب یکپارچه COSO^۲ تدوین گردیده، استفاده شده است. دوره رسیدگی مربوط به سال مالی منتهی به تاریخ ۱۴۰۲/۱۲/۲۹ می باشد.

۳. اهم مبانی و مستندات :

- مصوبات هیات مدیره محترم، هیات عامل محترم و صورتجلسات کمیته های عالی .
- دستورالعمل ها و آیین نامه های معتبر موجود در شبکه داخلی (پورتال) و ابلاغ شده توسط بانک.
- پرس و جو از واحدهای مربوطه و بررسی مدارک ارائه شده از طرف مدیریت های محترم سرمایه انسانی، روابط عمومی و صدای مشتریان، بهبود و کیفیت، فناوری اطلاعات، تطبیق و مبارزه با پولشویی، واحد ریسک و سایر واحدها.

۴. پیشنهاد :

گزارش ارزیابی کلی کنترل های داخلی بانک مربوط به سال ۱۴۰۱ در پنجمین جلسه کمیته محترم عالی حسابرسی به تاریخ ۱۴۰۲/۰۵/۰۲ مطرح و طی مصوبه شماره ۰۸ جلسه ۲۶ام مورخ ۱۴۰۲/۰۵/۲۴ به حضور اعضای محترم هیات مدیره، ارائه شده است. مدیریت حسابرسی داخلی متصدی بخش عمده وظایف مربوط به جز پنجم چارچوب کلی کنترل های داخلی (جز نظارت- بند ۶-۵ گزارش) بوده که صورتخلاصه اقدامات انجام شده از سوی مدیریت مذکور به شرح جدول زیر می باشد:

شماره	تعداد گزارشات
ارزیابی اثربخشی حسابرسی داخلی و فرآیندهای راهبری در سطح بانک و شرکت های گروه مالی سامان	۳
ارزیابی اثربخشی کنترل های داخلی در سطح فرآیندهای بانک و شرکت های گروه مالی سامان	۶
ارزیابی رعایت قوانین و مقررات	۳
بررسی سلامت گزارشگری مالی در بانک و شرکت های گروه مالی سامان	۳
ممیزی فرآیندهای حوزه فناوری اطلاعات در سطح بانک و شرکت های گروه مالی سامان	۷
سایر گزارشات	۴
مجموع گزارشات طبق برنامه مصوب در سال ۱۴۰۲	۲۶
امور ارجاعی	۱۳
مجموع گزارشات ارائه شده به کمیته عالی حسابرسی در سال ۱۴۰۲	۳۹

^۱ - دستورالعمل "حداقل الزامات ناظر بر استقرار نظام کنترل داخلی در موسسات اعتباری"، به شماره ۰۲/۳۱۸۹۴۹ مورخ ۱۴۰۲/۱۲/۲۲ توسط بانک مرکزی، جهت اجرا و استقرار نظام کنترلهای داخلی به شبکه بانکی کشور ابلاغ گردیده و از تاریخ مذکور رهنمود م/ب/۱۱۲۲ مورخ ۱۳۸۶/۰۳/۳۱ فوق اشاره منسوخ اعلام شده است. دوره رسیدگی گزارش حاضر مربوط به بخشنامه قبلی بانک مرکزی می باشد. اهم الزامات مندرج در نسخه ابلاغی جدید در جلسه کمیته عالی حسابرسی ارائه و ضوابط داخلی اجرای دستورالعمل مذکور با همکاری مدیریت محترم بهبود و کیفیت، مدون خواهد شد.

^۲ Committee Of Sponsoring Organizations

۵. یافته ها :

۵-۱- محیط کنترلی:

در چارچوب یکپارچه کنترل های داخلی، اصول اجرا شده در حوزه محیط کنترلی، به شرح زیر است:

- بانک نسبت به درستکاری و ارزش های اخلاقی خود، متعهد می باشد.
- هیات مدیره استقلال خود را از مدیریت نشان می دهد و بر توسعه و عملکرد کنترل های داخلی، نظارت دارد.
- با هدف تسهیل مسئولیت های نظارتی هیأت مدیره، کمیته های تخصصی با حضور حداقل یک عضو هیأت مدیره، ایجاد شده است.
- مدیریت اجرایی برای تحقق اهداف بانک با نظارت هیات مدیره، ساختار، اختیارات، مسئولیت ها و خطوط گزارش دهی مناسب را برقرار کرده است.
- بانک در تحقق اهداف، نسبت به جذب، توسعه و نگهداشت افراد شایسته، خود را متعهد نشان داده و افراد پاسخگو در خصوص مسئولیت های کنترل داخلی را در اختیار دارد.

۵-۱-۱- رویکردی جهت بررسی ارزیابی اثربخشی عملکرد کمیته های بانک (عالی و اجرایی) به ویژه در خصوص "کمیته های اجرایی" در بازه های زمانی معین و مستمر، تدوین گردد. حسب مورد، مدیریت حسابرسی داخلی به صورت سالانه اقدام به ارزیابی عملکرد کمیته های عالی، می نماید.

جدول شماره ۱ - کمیته های راهبردی و اجرایی

کمیته های راهبردی زیرمجموعه هیأت مدیره محترم شامل:	کمیته های اجرایی زیرمجموعه هیأت عامل محترم شامل:
کمیته عالی سرمایه انسانی و انتصابات، کمیته عالی مدیریت ریسک، کمیته عالی تطبیق گروه مالی سامان، کمیته عالی امنیت و فناوری اطلاعات و کمیته عالی حسابرسی	دارایی ها و بدهی ها، اعتبارات کلان، بانکداری بین المللی، انضباط کارکنان، اعتبارات متوسط، معاملات، پیگیری و وصول مطالبات، تطبیق و تخلیفات و جرایم مالی، ایمنی و بهداشت کار و تشخیص مطالبات غیرقابل وصول

۵-۱-۲- فهرست گزارشات دریافتی و ارسالی درون سازمانی، در سند گردش کار مرتبط با فرآیندها تعیین و تصویب گردیده که نیازمند به روزرسانی می باشد.

۵-۱-۳- مطابق با مستند شرح فعالیت های سازمانی مدیریت محترم سرمایه انسانی^۳ شناسایی پست های کلیدی به منظور طراحی برنامه های جانشین پروری و مدیریت استعدادها، در فرآیند مدیریت مسیر شغلی تعریف شده؛ تا تاریخ ارائه گزارش، جانشین پروری و مدیریت استعداد، در ستاد جهت برخی از واحدها اجرا و پیاده سازی در سایر واحدها و شعب در مرحله برنامه ریزی، می باشد.

۵-۱-۴- شناسنامه پستی مشتمل بر وظایف و مسئولیت های اصلی، حداقل شرایط لازم جهت احراز پست (از جمله تجربه، تحصیلات، مهارت های حرفه ای و عمومی) بوده که در سنوات گذشته برای اغلب واحدها تهیه و توسط واحدهای مذکور، تایید شده است. به استناد تغییرات ساختار سازمانی و شرح فعالیت ها، پست ها نیازمند تدوین شناسنامه جدید یا به روزرسانی شناسنامه های قبلی، می باشند.

^۳ مستند شماره ۴۲۰-۰۱-۳۱۰- مورخ ۱۴۰۲/۰۷/۰۱

۵-۱-۵- مطابق شناسنامه کمیته عالی سرمایه انسانی و انتصابات^۴، یکی از وظایف کمیته مذکور تصویب سیاست‌ها، مکانیزم‌ها و دستورالعمل‌های مربوط به ارزیابی عملکرد و توانمندی کارکنان براساس اهداف و سیاست‌های کلان می‌باشد. فرم‌های ارزیابی عملکرد کارکنان مطابق با چارچوب شایستگی بانک سامان طراحی گردیده که در سنوات گذشته مورد تصویب مدیریت ارشد، قرار گرفته است.

۵-۱-۶- شاخص‌های ارزیابی عملکرد، بازه زمانی ثبت نتایج و نحوه اندازه‌گیری آنها، طی دستورالعمل مدیریت عملکرد واحدهای سازمانی و کارکنان بر مبنای اهداف سازمانی^۵ تصویب و ابلاغ شده است. ابزار ثبت و ارزیابی عملکرد بانک، سامانه تبلو می‌باشد.

۵-۱-۷- روش اجرایی با عنوان نظام نظرسنجی از کارکنان^۶ مصوب و ابلاغ گردیده که به دلیل تغییرات در رویه‌های اجرا، نیازمند به روز رسانی است.

۵-۲- ارزیابی ریسک:

هر سازمانی جهت دستیابی به اهداف خود با انواع ریسک‌های درون و برون سازمانی مواجه می‌باشد. مدیریت ریسک، فرایندی پویا و مستمر برای شناسایی و ارزیابی ریسک‌های دستیابی به اهداف سازمان است.

- سند راهبرد در سطح بانک و فعالیتهای مهم، با مشارکت مدیران کلیدی تدوین و تصویب گردیده و کارکنان از چشم‌انداز و راهبرد بانک، آگاه شده‌اند.
- واحد ریسک متناسب با ساختار و پیچیدگی‌های فعالیت بانک، ایجاد شده و سطوح مناسبی از مدیران در فرایند شناسایی و ارزیابی ریسکها مشارکت می‌کنند.
- اهداف با شفافیت کافی، به تفکیک مالی و عملیاتی مشخص شده، به صورتی که شناسایی و ارزیابی ریسک‌های مربوط به اهداف مذکور، مقدور گردد.
- بانک ریسک‌های دستیابی به اهدافش را شناسایی و آنها را تجزیه و تحلیل کرده و بر این اساس تعیین می‌کند که ریسک‌های مذکور، چگونه باید مدیریت شود.
- سازمان تغییراتی را که می‌تواند بر کنترل داخلی تاثیر عمده‌ای داشته باشد، مورد شناسایی و ارزیابی قرار می‌دهد.

۵-۲-۱- مستند تهیه شده در خصوص شاخص‌های اشتباهی ریسک و حدود آن برای سال ۱۴۰۲ در سومین جلسه کمیته عالی مدیریت ریسک به تاریخ ۱۴۰۲/۰۴/۲۰ بررسی و تایید شده است.

۵-۲-۲- واحد ریسک باید در فرآیندهای تصمیم‌گیری اصلی سازمان نظیر برنامه ریزی راهبردی، برنامه ریزی در خصوص سرمایه و نقدینگی، محصولات و خدمات جدید، تدوین و اجرای طرح جبران خدمات کارکنان مشارکت داشته باشد^۷ ساز و کار نظام مند برای مشارکت واحد ریسک در شناسایی ریسک‌های حوزه محصولات و خدمات جدید و تدوین و اجرای طرح جبران خدمات، طراحی خواهد شد.

^۴ مستند ۱۱-۰۶-SCO مورخ ۱۴۰۲/۰۴/۰۷

^۵ مستند شماره ۱۵-۲۶۸۸-IN-۳۱۰ مورخ ۱۴۰۲/۰۱/۲۹

^۶ مستند شماره ۹۱/۳۱۰/۱۷۷۴ در تاریخ ۹۱/۰۷/۰۱

^۷ فصل دهم - بند ۶۱-۴ دستورالعمل الزامات ناظر بر حاکمیت شرکتی در موسسات اعتباری غیر دولتی به شماره ۹۶/۵۱۹۳۵ مورخ ۱۳۹۶/۰۲/۲۴.

۳-۲-۵- نظام مدیریت ریسک جامع (ERM^۸) با برقراری ارتباط بین استراتژی (اهداف راهبردی کسب و کار) با مدیریت ریسک منجر به خلق ارزش برای کلیه سطوح بانک و شرکت های گروه مالی سامان خواهد شد، لذا پیاده سازی آن منوط به اجرای کامل پروژه مدیریت جامع ریسک عملیاتی، می باشد.

۳-۵- فعالیت های کنترلی:

فعالیت های کنترلی بانک باید جهت دستیابی به اهداف عملیاتی، گزارشگری مالی و رعایتی، متناسب با اندازه و نوع عملیات بانک، طراحی و پیاده سازی گردد.

- در شناسایی فعالیت های کنترلی، به ریسک ها و تغییرات با اهمیت موثر بر آنها، توجه می شود.
- سطوح و ترکیب مناسبی از فعالیت های کنترلی شناسایی و مستقر شده است.
- تفکیک مناسب وظایف بر اساس رویکردی مشخص، مورد توجه قرار می گیرد.
- سطح مناسبی از کنترل ها در فناوری های مورد استفاده در کسب و کار، تعریف و سطوح دسترسی به سیستم های نرم افزاری و رویه های تحصیل، توسعه و نگهداری آنها، تعیین شده است.
- از آیین نامه ها، دستورالعمل ها و روش های اجرایی استاندارد به منظور اعمال فعالیت های کنترلی، استفاده و نسبت به نظارت بر اجرای درست، کامل و به موقع آنها، اطمینان حاصل می شود.

۱-۳-۵- بانک به منظور جاری سازی نظام مدیریت فرآیندها، در اولین مرحله اقدام به شناسائی و مستندسازی فرایندها و ابلاغ آن در سند جامع مصوب سال ۱۳۹۱ نموده؛ در سال ۱۴۰۲ بخشی از مفاد مندرج در شناسنامه فرآیندهای بانک توسط مدیریت بهبود و کیفیت، بروزرسانی گردیده است.

۲-۳-۵- در صورت پیاده سازی کامل پروژه مدیریت جامع ریسک عملیاتی اجرای کنترل های داخلی بهبود و زیان های عملیاتی، کاهش یافته و فرآیند شناسایی فعالیت های کنترلی و ارزیابی ریسک مربوط به هریک از کنترلها، یکپارچه خواهد شد.

۳-۳-۵- ساز و کار مشخصی برای حصول اطمینان معقول از اجرای خط مشی ها، رویه ها، دستورالعمل ها و بخشنامه ها توسط مدیریت های حسابرسی داخلی، تطبیق و مبارزه با پولشویی و اداره بازرسی و ... تعریف شده، در این راستا فرآیند خود ارزیابی واحدهای سازمانی جهت کسب اطمینان از اجرای کنترل ها، تدوین خواهد شد.

۴-۳-۵- بخشنامه ها و دستورالعمل های بانک متناسب با پیشنهادات اصلاح که از سوی سایر واحدها مطرح شده یا الزام مراجع خارج از سازمان، تدوین یا بروزرسانی می گردد.

۴-۵- اطلاعات و ارتباطات:

در چارچوب یکپارچه کنترل های داخلی، اصول مربوط به اطلاعات و ارتباطات به شرح زیر است:

- اطلاعات مورد نیاز کاربران در سطوح مختلف بانک، براساس رویکردی مشخص، شناسایی می گردد.
- از ساز و کار مشخصی برای گردآوری منابع داخلی و بیرونی داده ها و اطلاعات، استفاده می شود.
- بانک با استفاده از اطلاعات مربوط و با کیفیت که به دست آورده و یا ایجاد نموده، از کارکرد کنترل داخلی پشتیبانی می کند.
- استفاد از اطلاعات مرتبط از اهداف و مسئولیت های کنترل داخلی بوده و برای پشتیبانی از کارکرد کنترل های مذکور، ضروری می باشد.

^۸Enterprise Risk Management

- بانک، ارتباط با اشخاص بیرونی را در مورد موضوعات موثر بر کارکرد کنترل داخلی، برقرار می کند.
- ساز و کار و رویکرد مشخص برای برقراری ارتباط درون سازمانی، وجود دارد.
- مسیر گزارش تخلف های احتمالی به مقامی غیر از سرپرست مستقیم، تعریف شده است.

۱-۴-۵- در حوزه مدیریت رخداد^۹ به منظور پاسخگویی به حوادث رایانه ای، گروه^{۱۰} CERT مشغول به فعالیت می باشند، لازم است سیاست و فرایند اجرا از مرحله ثبت شرح رخداد تا مراحل بعدی شامل پیگیری دلایل ایجاد رخداد، ثبت راهکارهای ارائه شده برای رفع آنها و نحوه بایگانی سوابق جهت مراجعه در مواقع تکرار، مدون گردد.

۲-۴-۵- با هدف ارائه چارچوب مناسب جهت ایجاد بستر امن و کاهش ریسک های حوزه فناوری اطلاعات، ضوابط "حداقل الزامات ناظر بر ریسک فناوری اطلاعات" از سوی بانک مرکزی ابلاغ گردیده؛ مراتب مغایر با چارچوب مذکور مشخص شده و اقدامات لازم جهت ایجاد انطباق با آن، در حال پیگیری می باشد.

۵-۵- نظارت:

مطابق چارچوب یکپارچه کنترل های داخلی، اصول نظارت به شرح زیر است:

- بانک ارزیابی های مستمر و یا موردی را برای اثبات این که آیا اجزای کنترل داخلی وجود دارند و یا اجرا می شوند، انتخاب کرده، توسعه داده و انجام می دهد.
- واحد حسابرسی داخلی ایجاد شده و تحت نظارت کمیته عالی حسابرسی، فعالیت می نماید.
- فعالیت واحد حسابرسی داخلی در چارچوب مندرجات منشور فعالیت حسابرسی داخلی، انجام می شود.
- منشور کمیته عالی حسابرسی مدون شده و مورد تصویب هیأت مدیره قرار گرفته است.
- واحد حسابرسی داخلی موارد مستعد بهبود کنترل داخلی را ارزیابی و به موقع، به اشخاص مسئول انجام اقدامات اصلاحی، مدیریت ارشد و هیات مدیره هر کدام که مناسب باشد، گزارش می کند.

۱-۵-۵- مطابق بند یک ماده سه منشور فعالیت حسابرسی داخلی مصوب هیات مدیره محترم، امکان دسترسی نامحدود به کلیه اسناد و مدارک، دارایی ها، کارکنان و مشاهده فرآیندهای بانک و شرکت های فرعی برای حسابرسی داخلی وجود دارد. هماهنگی های لازم جهت دسترسی بر خط به اطلاعات شرکت های گروه مالی سامان نیز، در دست اقدام می باشد.

۲-۵-۵- کنترل های داخلی توسط مدیریت حسابرسی داخلی بر اساس رویکردی فرآیند محور ارزیابی می شود، به روز رسانی اسناد گردش کار در حال پیگیری می باشد.

۶- توصیه ها:

۱-۶- ایجاد ساز و کار پیگیری مصوبات و ارائه گزارش در خصوص عملکرد سالانه کمیته های عالی و اجرایی به هیات مدیره محترم.

^۹ Incident management

^{۱۰} Computer Emergency Response Team

۶-۲- به روزرسانی فهرست گزارشات دریافتی و ارسالی درون سازمانی در سند گردش کار مرتبط با فرایندها و تدوین سند جامعی با موضوع عناوین گزارشهای درون سازمانی و برون سازمانی با توجه به سطح اهمیت و میزان دقت مورد نظر مدیریت ارشد.

۶-۳- تدوین شناسنامه پستی جدید یا بروز رسانی شناسنامه های پستی قبلی متناسب با آخرین تغییرات ساختار سازمانی، شرح فعالیت ها و پست ها.

۶-۴- به روز رسانی روش اجرایی نظام نظرسنجی کارکنان جهت تطابق با رویه های اجرایی فعلی.

۶-۵- برنامه ریزی برای پیاده سازی نظام مدیریت ریسک جامع (ERM) توسط مدیریتهای ریسک و بهبود و کیفیت.

۶-۶- تدوین و تصویب فرآیند خود ارزیابی واحدهای سازمانی پس از پیاده سازی کامل پروژه مدیریت جامع ریسک عملیاتی.

۶-۷- تدوین و تصویب سیاست های مدیریت رخداد شامل پیگیری دلایل ایجاد و شناسایی راهکارهای رفع مشکلات تا بایگانی سوابق جهت مراجعه در مواقع تکرار.

باتشکر

مدیریت حسابرسی داخلی

مهیلا فلاح (۱۹۴۸)

محمد علی ریاحی نیا (۱۹۰۹)