بانک مرکزی جمهوری اسلامی ایران

مدیریت کل مقررات، مجوزهای بانکی و مبارزه با پولشویی

اداره مطالعات و مقررات بانکی

دستورالعمل حداقل الزامات ناظر بر استقرار نظام کنترل‌های داخلی در مؤسسات اعتباری

زمستان ۱۴۰۲

فهرست مطالب

«بسمه تعالی»

«دستورالعمل حداقل الزامات ناظر بر استقرار نظام کنترل‌های داخلی در مؤسسات اعتباری»

به استناد مواد (٦٣) و (٩٤) «آیین‌نامه نحوه تأسیس و اداره مؤسسات اعتباری غیردولتی» مصوب جلسه مورخ ١٤٠٠/٠٤/٢٢ شورای پول و اعتبار، بند (٢-٦) ذیل ماده (٢)، مواد (٢٩)، (٤٢) و (٦٦) الی (٦٨) «دستورالعمل الزامات ناظر بر حاکمیت شرکتی در بانک‌های دولتی» مصوب مجمع عمومی بانک‌ها، بند (٢-٦) ذیل ماده (٢)، مواد (٣٠)، (٤٤) و (٦٨) الی (٧٠) «دستورالعمل الزامات ناظر بر حاکمیت شرکتی در مؤسسات اعتباری غیردولتی» مصوب جلسه ١٣٩٦/٢/١٢ شورای پول و اعتبار و به منظور تقویت نظام کنترل داخلی در دستیابی به اهداف عملیاتی، گزارشگری مالی و رعایت قوانین و مقررات در مؤسسات اعتباری، «دستورالعمل حداقل الزامات ناظر بر استقرار نظام کنترل‌های داخلی در مؤسسات اعتباری» که از این پس به اختصار «دستورالعمل» نامیده می‌شود به شرح زیر تدوین می‌گردد:

فصل اول ــ تعاریف و کلیات

ماده ١ــ اصطلاحات و تعاریف به کار رفته در ماده (١) «دستورالعمل الزامات ناظر بر حاکمیت شرکتی در مؤسسات اعتباری غیردولتی» و «دستورالعمل الزامات ناظر بر حاکمیت شرکتی در بانک‌های دولتی» با همان معنی در این دستورالعمل به کار برده می‌شود. سایر اصطلاحات که در این دستورالعمل ذکر شده است، در معانی مشروح زیر به کار می‌روند:

١ــ ١ــ نظام کنترل داخلی: چارچوب و فرآیندی جامع است که توسط هیأت مدیره مؤسسه اعتباری، هیأت عامل و سایر کارکنان برای کسب اطمینان معقول از دستیابی به اهداف مربوط به عملیات، گزارشگری و رعایت قوانین و مقررات، طراحی و مستقر شده است که شامل سه بخش اهداف، اجزا و سطوح می‌باشد.

١ــ ٢ــ اهداف نظام کنترل داخلی:

١-٢-١- **اهداف عملیاتی:** دستیابی به اثربخشی و کارآیی فعالیت‌های مؤسسه اعتباری و نیز حفاظت از دارایی‌ها در برابر سوءاستفاده و تقلب.

۲-۲-۱- **اهداف گزارشگری:** ارایه اطلاعات مفید و سودمند به منظور افزایش آگاهی، اتخاذ تصمیم‌های صحیح و پیشگیری از گمراهی ذی‌نفعان از طریق تهیه گزارش‌های مالی و غیرمالی به‌موقع، قابل اتکاء، مربوط، قابل فهم و شفاف به صورت درون‌سازمانی و برون‌سازمانی.

۳-۲-۱- **اهداف رعایت قوانین و مقررات:** حصول اطمینان از رعایت تمامی قوانین، مقررات و استانداردهای لازم‌الاجرا توسط مؤسسه اعتباری.

۱- ۳- اجزای نظام کنترل داخلی:

۱-۳-۱- **محیط کنترلی:** مجموعه‌ای از ضوابط، فرآیندها و ساختارهایی که مبنای پیاده‌سازی نظام کنترل داخلی را در مؤسسه اعتباری فراهم می‌کند.

۲-۳-۱- **ارزیابی ریسک:** فرآیندی پویا و مستمر برای شناسایی، اندازه‌گیری و تحلیل ریسک‌های ناشی از رویدادهای بیرونی و درونی که مانع از دستیابی مؤسسه اعتباری به اهداف خود و ایجاد مخاطره برای عملیات مؤسسه اعتباری می‌گردد.

۳-۳-۱- **فعالیت‌های کنترلی:** مجموعه‌ای از خط‌مشی‌ها، رویه‌های پیشگیرانه و کشف‌کننده و اقدامات اصلاحی است که به منظور حصول اطمینان از اجرای دستورات هیأت مدیره و هیأت عامل در تمام سطوح فعالیت‌های مؤسسه اعتباری اتخاذ می‌شود.

٤-۳-۱- **اطلاعات و ارتباطات:** اطلاعات شامل داده‌های پردازش شده در راستای تحقق اهداف نظام کنترل داخلی می‌باشد که توسط هیأت مدیره و هیأت عامل مؤسسه اعتباری به منظور راهبری آن بکار گرفته می‌شود. ارتباطات شامل سیستم‌هایی است که امکان تبادل اطلاعات را درون مؤسسه اعتباری و اشخاص برون‌سازمانی نظیر مشتریان، سهامداران و مقام ناظر بانکی فراهم می‌کند.

۵-۳-۱- فعالیت‌های نظارتی: مجموعه فعالیت‌هایی که مؤسسه اعتباری به منظور ارزیابی‌های مستمر یا موردی از کارکرد صحیح نظام کنترل داخلی و میزان اثربخشی آن بکار می‌گیرد.

۱- ۴- سطوح نظام کنترل داخلی: شامل مؤسسه اعتباری، ادارات مرکزی، سرپرستی مناطق، شعب، وظایف و فرآیندها.

۱- ۵- آیین رفتار حرفه‌ای: مجموعه‌ای از هنجارهای حرفه‌ای پذیرفته‌شده و رفتارهای ناهنجار منع‌شده، الزامات مقرراتی ناظر بر صلاحیت حرفه‌ای (خبرگی)، تردید و مراقبت حرفه‌ای[1]، رازداری، درستکاری، استقلال رأی، واقع‌بینی و بی‌طرفی.

۱- ۶- برنامه جانشین‌پروری: مجموعه تدابیر لازم به منظور پرورش اشخاص واجد صلاحیت جهت تصدی شغل‌های کلیدی مؤسسه اعتباری نظیر اعضای هیأت عامل، مدیران ارشد مالی، ریسک، رعایت قوانین و مقررات، حسابرسی داخلی.

۱- ۷- کارکنان مسئول وظایف کنترلی: کارکنانی که به نحوی از انحا در شرح وظایف خود، یک یا چند وظیفه کنترلی در خصوص فعالیت‌های مؤسسه اعتباری را برعهده دارند.

۱- ۸- کنترل‌های عمومی فن‌آوری: مجموعه‌ای از اقدامات شامل ساماندهی و اجرا، مستندسازی رویه‌ها، نحوه دسترسی به تجهیزات و فایل‌های اطلاعاتی و سایر کنترل‌های مربوط به فن‌آوری اطلاعات و سامانه‌های اطلاعاتی می‌باشد.

۱- ۹- افشاگران: به اشخاصی گفته می‌شود که اقدامات و فعالیت‌های نادرست، غیرقانونی و سایر اعمالی که منافع ذی‌نفعان مؤسسه اعتباری را با مخاطره مواجهه می‌سازد، افشا می‌نمایند.

۱- ۱۰- تضاد منافع: هر گونه تضاد میان منافع مؤسسه اعتباری، سهامداران یا منافع مشتریان با منافع هیأت مدیره و هیأت عامل، به نحوی که دستیابی به هر یک مستلزم چشم پوشی از تمام یا بخشی از دیگری باشد.

ماده ۲- هیأت مدیره مؤسسه اعتباری موظف است برای استقرار نظام کنترل‌های داخلی، سطوح و تعاملات لایه‌های دفاعی مشتمل بر لایه اول: واحدهای عملیاتی، لایه دوم: واحدهای نظارتی، لایه سوم؛

[1] رعایت استانداردهای فنی و اخلاقی، تلاش جهت ارتقای صلاحیت و کیفیت خدمات و ایفای مسئولیت حرفه‌ای به بهترین شکل ممکن بر مبنای توانایی فرد، از جمله ویژگی‌های فرآیندی است که باید حین اجرای فعالیت حسابرسی داخلی انجام شوند و همچنین در برابر منافع عموم سازگار باشند.

حسابرسی داخلی و لایه چهارم: بانک مرکزی و حسابرس مستقل را در چارچوب این دستورالعمل طراحی، استقرار و به روزرسانی نماید.

فصل دوم ـ محیط کنترلی

ماده ۳– هیأت مدیره مؤسسه اعتباری موظف است از طریق انجام حداقل اقدامات زیر از فراهم بودن محیط کنترلی مؤثر اطمینان حاصل نماید:

۳– ۱– تعیین آیین رفتار حرفه‌ای و ابلاغ آن؛

۳– ۲– تعیین سازوکارهای نظارت هیأت مدیره بر نظام کنترل داخلی؛

۳– ۳– طراحی ساختار سازمانی و خطوط گزارشگری؛

۳– ۴– تعیین راهبردهای جذب، توسعه و نگهداری کارکنان با صلاحیت؛

۳– ۵– تعیین سازوکارهای پاسخگویی در قبال مسئولیت‌های کنترل داخلی برای تمامی سطوح مؤسسه اعتباری؛

ماده ۴– هیأت مدیره مؤسسه اعتباری موظف است در تعیین آیین رفتار حرفه‌ای، هنجارهای حرفه‌ای پذیرفته شده و رفتارهای ناهنجار منع‌شده با تأکید بر اصول درستکاری و ارزش‌های اخلاقی را مشخص و به تمامی سطوح مؤسسه اعتباری ابلاغ نماید. اشخاص ارایه دهنده خدمات برون‌سپاری شده مؤسسه اعتباری و شرکای تجاری نیز باید از آیین رفتار حرفه‌ای مؤسسه اعتباری آگاهی داشته باشند.

ماده ۵– هیأت مدیره مؤسسه اعتباری باید فرآیندهای مناسب را به منظور ارزیابی عملکرد فردی و گروهی در پایبندی به آیین رفتار حرفه‌ای تعیین نماید.

ماده ۶– هیأت عامل مؤسسه اعتباری در اجرای آیین رفتار حرفه‌ای مصوب هیأت مدیره موظف است اقدامات زیر را انجام دهد:

۶– ۱– تهیه و تصویب راهنمای اجرایی برای بکارگیری آیین رفتار حرفه‌ای؛

۶– ۲– ترویج و آموزش آیین رفتار حرفه‌ای برای تمامی کارکنان و تقویت پاسخگویی برای رفتار مسؤولانه؛

۶– ۳– فراهم نمودن بسترهای لازم برای طرح موضوعات و سؤالات مرتبط با بکارگیری آیین رفتار حرفه‌ای توسط کارکنان؛

۶– ۴– پیاده‌سازی فرآیندهای ارزیابی عملکرد و میزان پایبندی به آیین رفتار حرفه‌ای؛

۶- ۵- شناسایی انحراف از آیین رفتار حرفه‌ای و ارایه گزارش به موقع انحرافات و اقدامات اصلاحی به هیأت مدیره.

ماده ۷- هیأت مدیره مؤسسه اعتباری مسئولیت نظارت عالی بر اجرای سیاست‌ها و دستیابی به اهداف راهبردی مؤسسه اعتباری، رعایت الزامات قانونی و مقرراتی و نحوه استقرار و پیاده‌سازی اجزای نظام کنترل داخلی را بر عهده دارد.

ماده ۸- هیأت مدیره مؤسسه اعتباری موظف است در اجرای تکالیف هیأت مدیره در قبال نظام کنترل‌های داخلی، کمیته حسابرسی را در چارچوب ضوابط ابلاغی بانک مرکزی تشکیل دهد. وظایف کمیته مذکور در چارچوب این دستورالعمل عبارتند از :

۸- ۱- نظارت بر اثربخشی نظام کنترل داخلی در خصوص گزارشگری مالی و ارزیابی ریسک‌ها و بررسی ناکارآمدی‌های قابل توجه و ضعف‌های بااهمیت آن؛

۸- ۲- ارزیابی مدیران در زمینه موضوعات بااهمیت نظام کنترل داخلی، نظیر گزارشگری مالی و اقدامات اصلاحی مورد نیاز؛

۸- ۳- ایجاد ارتباطات بین بخش‌های مختلف مؤسسه اعتباری با واحد حسابرسی داخلی در مورد هرگونه موضوع با اهمیت؛

۸- ۴- نظارت بر کیفیت گزارشگری مالی و افشاء اطلاعات؛

۸- ۵- بررسی و پیشنهاد به کارگیری و حق الزحمه حسابرس مستقل؛

۸- ۶- تعامل با بانک مرکزی و حسابرس مستقل.

ماده ۹- کمیته حسابرسی موظف است گزارش‌های ارزیابی ریسک واحد حسابرسی داخلی، گزارش های ریسک ارایه اطلاعات نادرست در گزارشگری مالی و اطلاعات به دست آمده از گزارش‌های افشاگران نقض قوانین و مقررات را به دقت بررسی و نتایج را به همراه پیشنهادهای اصلاحی به هیأت مدیره ارایه نماید.

ماده ۱۰- هیأت مدیره مؤسسه اعتباری موظف است در طراحی ساختار سازمانی مناسب به منظور حصول اطمینان از ارزیابی صحیح ریسک‌ها، ایجاد فعالیت‌های کنترلی مناسب، برقراری جریان مؤثر اطلاعات و ارتباطات و استقرار دقیق فعالیت‌های نظارتی در سطوح مختلف مؤسسه اعتباری نسبت به تفکیک مناسب وظایف، مسئولیت‌ها، فرآیندهای تصویب، تعیین خطوط گزارشگری و تعیین سطوح دسترسی به اطلاعات و اسناد، اقدام و به صورت دوره‌ای بازبینی نماید.

ماده ۱۱– هیأت مدیره مؤسسه اعتباری موظف است اطمینان حاصل نماید که گزارش‌های واحد حسابرسی داخلی برای هیأت مدیره بدون هرگونه صلاحدید مدیریتی تهیه شده است و حسابرسان داخلی به هیأت مدیره و اعضای کمیته حسابرسی دسترسی مستقیم دارند.

ماده ۱۲– هیأت عامل مؤسسه اعتباری موظف است بر اساس قراردادهای مربوط به خدمات برون‌سپاری شده و ضوابط ابلاغی بانک مرکزی در خصوص برون‌سپاری خدمات و الزامات ناظر بر ریسک فناوری اطلاعات، سازوکارهای مقتضی را برای نظارت بر حسن اجرای قراردادهای مذکور با تأکید بر مسئولیت‌های کارکنان معرفی شده جهت انجام خدمات برون سپاری شده مشخص نماید.

ماده ۱۳– هیأت مدیره مؤسسه اعتباری موظف است انتظارات و معیارهای شایستگی شغلی و رفتار سازمانی کارکنان، خط‌مشی‌ها و شیوه‌های رفتاری آن‌ها را به منظور جذب، توسعه و نگهداری کارکنان با صلاحیت تعیین و به روزرسانی نماید.

ماده ۱۴– هیأت مدیره مؤسسه اعتباری موظف است مسئولیت‌های اصلی با اهمیت برای تحقق اهداف نظام کنترل داخلی برای افراد و بخش‌های مختلف نظیر مدیر عامل، مدیران ارشد ریسک، واحدهای حسابرسی داخلی، مالی و رعایت قوانین و مقررات و نیز شایستگی‌های مرتبط با هر کدام از آن‌ها را تعیین و ارزیابی نموده و برای هر یک از این مسئولیت‌ها، برنامه‌های جانشین پروری تدوین نماید.

ماده ۱۵– هیأت مدیره مؤسسه اعتباری موظف است به منظور پاسخگویی کارکنان (اعم از اعضای هیأت عامل، مدیران و سایر کارکنان) در خصوص ایفای مسئولیت‌های محوله در نظام کنترل داخلی، سازوکارهای مناسب نظیر شاخص‌های عملکرد، مشوق‌ها و پاداش‌ها و اقدامات انضباطی مرتبط با انجام مسئولیت‌های کنترل داخلی را تعیین و تصویب و در مقاطع زمانی منظم حداکثر دو ساله ارزیابی و به روزرسانی نماید.

فصل سوم ــ ارزیابی ریسک

ماده ۱۶– هیأت عامل مؤسسه اعتباری موظف است به منظور برخورداری از نظام کنترل داخلی مؤثر، ریسک‌های مهم از قبیل ریسک اعتباری، ریسک نقدینگی، ریسک بازار و ریسک عملیاتی را شناسایی و تأثیرات آن بر دستیابی به اهداف مؤسسه اعتباری را مورد ارزیابی قرار داده و در پاسخ به

ریسک‌های شناسایی شده، اقدامات لازم را برای اجتناب، پذیرش، کاهش و تسهیم آن‌ها تا سطح قابل پذیرش مصوب هیات مدیره انجام دهد.

ماده ۱۷– هیأت عامل مؤسسه اعتباری موظف است به منظور پوشش ریسک‌های جدید یا ریسک‌های کنترل نشده، حسب مورد هر یک از اجزای نظام کنترل‌های داخلی را موردبازنگری قرار داده و اقدامات اصلاحی مقتضی را به هیأت مدیره پیشنهاد نماید.

ماده ۱۸– هیأت عامل مؤسسه اعتباری موظف به ایجاد سازوکارهای کنترلی لازم به منظور حصول اطمینان از صحت و درستی داده‌ها و محاسبات مربوط به صورت‌های مالی و نیز انعکاس صحیح همه رویدادهای بااهمیت و قابل فهم بودن صورت‌های مالی برای استفاده کنندگان می‌باشد.

ماده ۱۹– هیأت مدیره مؤسسه اعتباری موظف است به منظور شناسایی تقلب و انگیزه‌های موجد آن، سیستم‌ها و فرآیندهایی را تعیین و تصویب نموده و بر اجرای آن‌ها نظارت نماید.

ماده ۲۰– هیأت مدیره مؤسسه اعتباری موظف است به منظور جلوگیری از بروز تقلب و انگیزه‌های موجد آن، برنامه‌های جبران خدمات و فرآیند ارزیابی عملکرد کارکنان را به طور مستمر بازبینی نماید.

ماده ۲۱– واحد مدیریت ریسک مؤسسه اعتباری موظف است به منظور ارزیابی ریسک تقلب، گزارش‌های واصله مربوط به اعمال متقلبانه، سرقت و سوء استفاده از دارایی‌ها، فساد ناشی از وقوع تقلب و روش‌هایی که ممکن است توسط کارکنان منجربه بی‌اثر شدن و یا نادیده گرفتن کنترل‌های در نظر گرفته شده برای شناسایی تقلب می‌شود را بررسی و ارزیابی نموده و در گزارشات ارزیابی ریسک تقلب با در نظرگرفتن احتمال وقوع و اثرات بالقوه آن‌ها مورد استفاده قرار داده و نسخه‌ای از گزارش مذکور را به واحد حسابرسی داخلی ارایه نماید.

ماده ۲۲– مدیر ارشد واحد حسابرسی داخلی مؤسسه اعتباری موظف است نتایج حاصل از ارزیابی ریسک تقلب را بررسی نموده و در مراحل مختلف برنامه حسابرسی داخلی شامل برنامه‌ریزی، اجرای برنامه، انتقال نتایج و پیگیری و نظارت، مورد استفاده قرار دهد.

ماده ۲۳– هیأت عامل مؤسسه اعتباری موظف است، به منظور ارزیابی آثار تغییرات برون سازمانی بر نظام کنترل داخلی، فرآیندهای شناسایی ریسک‌های ناشی از تغییر در مقررات، شرایط اقتصادی، شرایط محیطی، رویکردهای مدیریتی، فعالیت‌های جدید و فن‌آوری‌های نوین بانکی را ایجاد نماید.

فصل چهارم ـ فعالیت‌های کنترلی

ماده ۲۴– هیأت مدیره مؤسسه اعتباری موظف است به منظور پیاده‌سازی نظام کنترل داخلی مؤثر، فعالیت‌های کنترلی لازم برای تمامی فرآیندها، فعالیت‌ها و اقدامات در تمام سطوح نظام کنترل داخلی شامل حداقل موارد زیر را تعیین و به روزرسانی نماید:

۲۴– ۱– ارزیابی‌های لازم مبتنی بر گزارش‌های عملکرد؛

۲۴– ۲– کنترل مناسب فعالیت‌های واحدها یا بخش‌های مختلف؛

۲۴– ۳– کنترل‌های فیزیکی شامل تعیین میزان دسترسی به دارایی‌ها؛

۲۴– ۴– میزان انطباق با حدود تعیین شده برای منابع در معرض ریسک و پیگیری موارد عدم تطبیق؛

۲۴– ۵– فرآیندهای تصویب و سطوح اختیارات؛

۲۴– ۶– فرآیند رسیدگی‌ها و رفع مغایرت‌ها.

ماده ۲۵– هیأت عامل مؤسسه اعتباری موظف است نسبت به شناسایی وظایفی که با یکدیگر در تعارض هستند و نیز تفکیک مناسب وظایف و مسئولیت‌ها اقدام و در صورتی‌که انجام چنین تفکیکی امکان‌پذیر نباشد، فعالیت‌های کنترلی مقتضی را ایجاد نماید.

ماده ۲۶– هیأت عامل مؤسسه اعتباری موظف است فعالیت‌های کنترلی مرتبط با کنترل‌های عمومی فن‌آوری و نیز فعالیت‌های کنترلی مرتبط با موارد زیر را در چارچوب ضوابط ابلاغی بانک مرکزی در خصوص الزامات ناظر بر ریسک فناوری اطلاعات به منظور حصول اطمینان از کامل بودن، صحت و آماده بودن فن‌آوری، پیاده‌سازی و مستندسازی نماید:

۲۶– ۱– زیرساخت‌های فن‌آوری؛

۲۶– ۲– مدیریت امنیت اطلاعات؛

۲۶– ۳– توسعه و نگهداری برنامه‌های کاربردی؛

۲۶– ۴– ارتباط بین سایر سیستم‌ها و برنامه‌های کاربردی.

ماده ۲۷– هیأت عامل مؤسسه اعتباری موظف است در خصوص اشخاص ارایه دهنده خدمات برون‌سپاری مربوط به زیرساخت‌های فن‌آوری اطلاعات، سازوکارهای اعمال فعالیت‌های کنترلی فن‌آوری را منطبق با استانداردها و ضوابط ابلاغی بانک مرکزی در خصوص خدمات برون‌سپاری شده و الزامات ناظر بر ریسک فناوری اطلاعات ایجاد نماید.

ماده ۲۸– هیأت عامل مؤسسه اعتباری موظف است فرآیند کنترلی مشخصی را برای ارتقاء و به‌روزرسانی سیستم‌های فن‌آوری به شرح زیر تعیین نماید:

۲۸– ۱– ارزیابی ماهیت ارتقاء و به‌روزرسانی سیستم‌ها؛

۲۸– ۲– اجرای آزمایشی قبل از پیاده‌سازی و ارتقاء؛

۲۸– ۳– تأیید ذی‌نفعان اصلی قبل از پیاده‌سازی و ارتقاء؛

۲۸– ۴– مستندسازی صحیح تغییرات انجام شده.

ماده ۲۹– هیأت مدیره مؤسسه اعتباری موظف است خط‌مشی‌ها و رویه‌های انجام فعالیت‌های کنترلی را با توجه به موارد زیر تعیین، بازبینی و به روز رسانی نماید:

۲۹– ۱– ریسک‌های مربوط به تحقق اهداف موسسه اعتباری؛

۲۹– ۲– سمت‌ها، واحدها و فرآیندهایی که خط‌مشی‌ها و رویه‌ها راجع به آن‌ها تدوین شده است؛

۲۹– ۳– نقش‌ها و مسئولیت‌های مرتبط با ایجاد، بکارگیری، اجرا و تداوم خط‌مشی‌ها و رویه‌ها؛

۲۹– ۴– اقدامات اصلاحی مورد نیاز به عنوان بخشی از اعمال فعالیت‌های کنترلی؛

۲۹– ۵– ایجاد ارتباط بین خط‌مشی‌ها و رویه‌ها؛

۲۹– ۶– شایستگی‌های مورد نیاز برای کارکنان مسئول اجرای رویه‌ها و برنامه‌های آموزشی مورد نیاز؛

۲۹– ۷– چارچوب زمان‌بندی اجرای رویه‌ها.

ماده ۳۰– هیأت مدیره مؤسسه اعتباری موظف است، خط‌مشی‌های انجام فعالیت‌های کنترلی مربوط به رویه‌های مواجهه با بروز استثنائات در خط‌مشی‌ها را تعیین، بازبینی و در حداقل زمان ممکن به‌روزرسانی نماید.

ماده ۳۱– هیأت عامل مؤسسه اعتباری موظف است بر اساس خط‌مشی‌ها و رویه‌های موضوع ماده ۲۹–، انجام فعالیت‌های کنترلی را با استفاده از روش‌هایی نظیر شرح‌نوشته، نمودار گردش کار و چک‌لیست‌های کنترلی برای هر یک از عملیات و خدمات بانکی و فعالیت‌های روزلنه کارکنان تدوین نماید. در این خصوص موارد زیر باید مدنظر قرار گیرد:

۳۱– ۱– تعیین مدیران یا کارکنان مسئول و پاسخگوی اجرای فعالیت‌های کنترلی متناسب با واحدهای عملیاتی و کارکردها؛

۳۱- ۲- انجام فعالیت‌های کنترلی بر اساس برنامه زمانبندی مطابق با خط‌مشی‌ها و رویه‌های تعیین شده توسط مدیران یا کارکنان مسئول؛

۳۱- ۳- بررسی نتایج اجرای فعالیت‌های کنترلی و اعمال اقدامات اصلاحی لازم توسط مدیران یا کارکنان مسئول.

ماده ۳۲- هیأت عامل مؤسسه اعتباری موظف است به منظور کاهش ریسک معاملات غیرمجاز، فعالیت‌های متقلبانه و جعلی و اختلال در فرآیند عملیات، میزان دسترسی به محل‌های خاص نظیر اتاق معاملات، مراکز داده‌ها و حوزه مبادلات مالی را تعریف و خط‌مشی‌ها و رویه‌های نظارت و فعالیت‌های کنترلی مربوط به دسترسی‌های مذکور را تدوین و عملیاتی نماید.

فصل پنجم ـ اطلاعات و ارتباطات

ماده ۳۳- هیأت عامل مؤسسه اعتباری موظف است به منظور پشتیبانی از نظام کنترل داخلی و گزارشگری مالی، برنامه مدیریت داده را تدوین و به تصویب هیأت مدیره برساند. برنامه مدیریت داده باید شامل خط‌مشی‌ها و رویه‌هایی، برای حداقل مقاصد زیر باشد:

۳۳- ۱- تأیید منابع داده‌ها؛

۳۳- ۲- ایجاد الزامات کیفیت داده‌ها قبل از ورود آنها به سیستم اطلاعات؛

۳۳- ۳- ارزیابی صحت داده‌های اصلی و اطلاعات تولیدشده مرتبط در پردازش‌ها؛

۳۳- ۴- پیاده‌سازی روش‌های امن انتقال و ذخیره‌سازی اطلاعات.

ماده ۳۴- هیأت عامل مؤسسه اعتباری موظف است بر اساس خط مشی مصوب هیأت مدیره در خصوص مدیریت اطلاعات، سیستم‌های اطلاعاتی یکپارچه را به منظور دریافت داده‌های مورد نیاز از منابع درونی و بیرونی ایجاد نموده و حداقل ویژگی‌های زیر را برای تعیین رویه‌های تبدیل داده‌ها به اطلاعات، مورد توجه قرار دهد:

۳۴- ۱- تأمین‌کنندگان و استفاده‌کنندگان اطلاعات؛

۳۴- ۲- اهمیت، اولویت و حساسیت ؛

۳۴- ۳- فراوانی و تواتر؛

۳۴- ۴- فرآیندهای پشتیبان و دوره‌های نگهداری؛

۳۴- ۵- حفظ تقارن اطلاعاتی در خصوص روندها و ریسک‌های برون‌سازمانی و درون‌سازمانی؛

۳۴- ۶- تعریف طبقه‌بندی داده‌ها و سطوح دسترسی امن به اطلاعات.

ماده ۳۵- هیأت عامل مؤسسه اعتباری موظف است فرآیند تبادل و انتشار اطلاعات ضروری مرتبط با اهداف گزارشگری مالی، رعایت قوانین و مقررات، اثربخشی عملیاتی، الزامات کنترل مالی، خط‌مشی‌ها و فرآیندهای کنترل داخلی را برای تعیین مسئولیت‌های کارکنان در نظام کنترل داخلی و اجرای آن‌ها، طراحی و تدوین نماید.

ماده ۳۶- هیأت عامل مؤسسه اعتباری موظف است فرآیند تبادل و انتشار اطلاعات را با توجه به ماهیت اطلاعات، الزامات قانونی و مقرراتی و امکان بهره‌گیری از راه‌حل‌های فن‌آوری بر اساس روش‌های زیر انتخاب نماید:

۳۶- ۱- اطلاع‌رسانی در خصوص مأموریت، چشم‌انداز و اهداف مؤسسه اعتباری از طریق تابلو اعلانات یا پایگاه اطلاع‌رسانی مؤسسه اعتباری؛

۳۶- ۲- برگزاری جلسات و دوره‌های آموزشی در خصوص موضوعات کنترل داخلی و سایر موضوعات مرتبط با آن؛

۳۶- ۳- ایجاد درگاه اطلاع‌رسانی داخلی مختص موضوعات کنترل داخلی شامل آیین رفتار حرفه‌ای، نقش‌ها و مسئولیت‌های کاری، خط‌مشی‌ها، فرآیندها و دیگر موضوعات مرتبط؛

ماده ۳۷- هیأت مدیره مؤسسه اعتباری موظف است به منظور گزارش هرگونه خطای مشاهده شده و نیز موضوعات مربوط به گزارشگری مالی و یا سایر موضوعاتی که می‌تواند بر کنترل داخلی اثرگذار باشد، خط‌مشی لازم در خصوص نحوه حمایت و حفاظت از افشاگران درون‌سازمان با در نظر گرفتن حفظ محرمانگی و اطمینان از عدم شناسایی آن‌ها تعیین نموده و سازوکارهای مطمئنی برای ایجاد مسیرهای ارتباطی ویژه نظیر ایجاد خط ارتباط اضطراری مستقیم با مدیریت مهیا نماید.

ماده ۳۸- هیأت مدیره مؤسسه اعتباری موظف است فرآیندهایی اتخاذ نماید تا اطلاعات مربوط و به‌موقع به اشخاص برون‌سازمانی نظیر سهامداران، بانک مرکزی و سایر مقامات نظارتی ذی‌صلاح، مشتریان، تحلیل‌گران مالی و سایر ذی‌نفعان، اطلاع‌رسانی و در چارچوب قانون و مقررات مربوط مسیرهای ارتباطی متناسب را برای اشخاص مزبور در کنار مسیرهای ارتباطی معمول با افشاگران برون‌سازمانی فراهم آورد.

ماده ۳۹– هیأت مدیره مؤسسه اعتباری موظف است در کنار مسیرهای تبادل اطلاعات معمول با افشاگران برون‌سازمانی، سازوکارهایی را به منظور ایجاد مسیرهای ارتباطی مجزا نظیر خط ارتباط اضطراری مستقیم با مدیریت با حفظ محرمانگی و بدون افشای نام فراهم نماید.

فصل ششم ــ فعالیت‌های نظارتی

ماده ۴۰– هیأت مدیره مؤسسه اعتباری موظف است برنامه‌های ارزیابی مستمر و موردی در خصوص فعالیت‌های نظارتی را متناسب با شرایط مؤسسه اعتباری تعیین نموده و تناسب و کفایت برنامه‌های مذکور را با در نظر گرفتن حداقل موارد زیر مورد بررسی قرار دهد:

۴۰– ۱– الزامات مقرراتی مؤسسه اعتباری و اهداف نظام کنترل داخلی؛

۴۰– ۲– سرعت تغییرات محیط قانونی و یا کسب و کار مؤسسه اعتباری؛

۴۰– ۳– نتایج حاصل از سوابق ارزیابی‌های مربوط به اثربخشی کنترل‌های داخلی؛

۴۰– ۴– معیارهای پایش مستمر فرآیندهای سطوح نظام کنترل داخلی؛

۴۰– ۵– تغییرات مؤثر بر اجزای نظام کنترل داخلی.

ماده ۴۱– هیأت مدیره مؤسسه اعتباری موظف است در صورت وقوع هر یک از موارد زیر دفعات ارزیابی‌های موردی و فعالیت‌های نظارتی را افزایش دهد:

۴۱– ۱– شناسایی ناکارآمدی‌های موجود در نظام کنترل داخلی توسط فعالیت‌های نظارتی؛

۴۱– ۲– نقض حدود مقرر مربوط به شاخص‌های کلیدی عملکرد به دلیل ناکارآمدی نظام کنترل داخلی.

ماده ۴۲– هیأت مدیره مؤسسه اعتباری موظف است با پیاده‌سازی فعالیت‌های نظارتی و نتایج حاصل از آن حداقل موارد زیر را انجام دهد:

۴۲– ۱– شناسایی تغییرات ضروری در طراحی و اجرای نظام کنترل داخلی در نتیجه فعالیت‌های نظارتی؛

۴۲– ۲– ارزیابی تغییرات در اشخاص، فرآیندها و فن‌آوری که می‌تواند بر طراحی و اجرای کنترل‌ها تأثیر گذارد؛

۴۲– ۳– ارزیابی اقدامات یا فعالیت‌های کنترلی در سطح کلیه فرآیندها و فعالیت‌های مؤسسه اعتباری؛

ماده ۴۳– هیأت عامل مؤسسه اعتباری موظف است به عنوان بخشی از ارزیابی مستمر، سامانه‌ها و داشبوردهای مدیریتی را برای مدیران و سرپرستانی که به طور مستقیم وظیفه پاسخگویی نسبت به فرآیندها و فعالیت‌های نظارتی را بر عهده دارند، با استفاده از شاخص‌ها و امتیازها ایجاد نماید. داشبورد مذکور باید شامل حداقل اطلاعات زیر باشد:

۴۳– ۱– امتیازدهی عملکرد اجزای نظام کنترل داخلی؛

۴۳– ۲– شاخص‌ها و یا اطلاعات بااهمیت برای انجام ارزیابی و پیگیری‌های بعدی؛

۴۳– ۳– تناوب ارزیابی‌های انجام‌شده و آخرین ارزیابی؛

۴۳– ۴– ناکارآمدی‌های شناسایی شده و اصلاحات مربوط؛

ماده ۴۴– هیأت عامل مؤسسه اعتباری موظف است با بهره‌گیری از فن‌آوری اطلاعات، برنامه کاربردی پایش خودکار[۲] نظام کنترل داخلی را تهیه و مورد استفاده قرار دهد. برنامه کاربردی مذکور شامل حداقل موارد زیر می‌باشد:

۴۴– ۱– بررسی و تطبیق مبادلات و تراکنش‌ها با آستانه‌های از پیش‌تعریف شده به منظور شناسایی مبادلات و تراکنش‌های غیرعادی؛

۴۴– ۲– پایش مبادلات و تراکنش‌ها برای بررسی روندها یا الگوها؛

۴۴– ۳– ارزیابی شاخص‌ها و معیارهای عملکرد در راستای بهبود فرآیندهای کسب و کار.

ماده ۴۵– هیأت عامل مؤسسه اعتباری موظف است ارزیابی‌های موردی کنترل‌های داخلی را از طریق روش‌هایی نظیر موارد زیر انجام دهد:

۴۵– ۱– انجام بررسی‌ها و بازدیدهای نظارتی بدون اطلاع قبلی؛

۴۵– ۲– انجام بررسی‌های تطبیقی کنترل داخلی میان واحدهای عملیاتی مشابه در مؤسسه اعتباری؛

۴۵– ۳– بکارگیری اشخاص مستقل بیرونی به منظور انجام ارزیابی ویژه.

ماده ۴۶– واحد حسابرسی داخلی مؤسسه اعتباری موظف است ارزیابی‌های جداگانه‌ای را در خصوص اجزای اصلی نظام کنترل داخلی انجام دهد.

ماده ۴۷– هیأت عامل مؤسسه اعتباری موظف است رویه مناسبی به منظور بررسی شکایات مشتریان با هدف بررسی ضعف‌های نظام کنترل داخلی ایجاد و به تصویب هیأت مدیره برساند.

---

[۲] . Automated monitoring

فصل هفتم: گزارشگری

ماده ۴۸– هیأت مدیره مؤسسه اعتباری موظف است شیوه‌های ناظر بر تهیه گزارش ناکارآمدی‌های نظام کنترل داخلی را تعیین نموده و پس از بررسی نتایج گزارش‌های مذکور، بر برنامه‌ها و اقدامات اصلاحی هیأت عامل در این خصوص نظارت عالی نماید.

ماده ۴۹– هیأت عامل مؤسسه اعتباری موظف است ناکارآمدی‌های نظام کنترل داخلی را ارزیابی به‌هنگام نموده و بر اساس معیارهایی نظیر ماهیت، منشأ و میزان اهمیت ناکارآمدی به هیأت مدیره گزارش و اقدامات اصلاحی مقتضی را پیشنهاد نماید.

ماده ۵۰– واحدهای سازمانی و افراد مسئول اجرای کنترل‌ها موظفند گزارشی از موارد عدم رعایت کنترل‌های تعریف شده بر اساس این دستورالعمل را در مقاطع زمانی حداکثر سه ماهه به واحدهای مدیریت ریسک و حسابرسی داخلی ارایه نمایند.

ماده ۵۱– واحد مدیریت ریسک مؤسسه اعتباری موظف است گزارشات مأخوذه از اجرای مفاد این دستورالعمل را در فرآیند شناسایی، اندازه‌گیری، پایش، کنترل و گزارشگری ریسک‌های مؤسسه اعتباری نظیر ریسک عملیاتی، اعتباری، نقدینگی و بازار مد نظر و مورد استفاده قرار دهد.

ماده ۵۲– واحد حسابرسی داخلی مؤسسه اعتباری موظف است فعالیت کنترلی مرتبط با اجرای سیاست‌ها، خط مشی‌ها و رویه‌های اجرایی مصوب هیأت مدیره و مسئول اجرای کنترل‌های مذکور را در برنامه حسابرسی تعیین و گزارش موارد با اهمیت از عدم اجرای صحیح فعالیت‌های یادشده را در مقاطع زمانی حداکثر سه ماهه به کمیته حسابرسی ارایه نماید.

ماده ۵۳– مدیر ارشد حسابرسی داخلی موظف است برنامه حسابرسی داخلی را مبتنی بر ریسک و در مقاطع زمانی حداکثر سالیانه تدوین و گزارش نماید به نحوی که اولویت‌های فعالیت حسابرسی داخلی در راستای اهداف و راهبردهای مصوب هیأت مدیره تعیین شود.

تبصره- برنامه حسابرسی داخلی موضوع این ماده در صورت بروز هرگونه تغییر در اهداف، اجزا و سطوح نظام کنترل داخلی مؤسسه اعتباری در حین اجرای برنامه حسابرسی داخلی، باید متناسب با تغییرات مذکور در حداقل زمان ممکن به‌روزرسانی گردد.

ماده ۵۴– واحد حسابرسی داخلی مؤسسه اعتباری موظف است گزارش یافته‌های برنامه حسابرسی را حسب مورد به مسئولین واحدهای عملیاتی یا هیأت عامل مؤسسه اعتباری ارایه نماید و پاسخ‌ها و اقدامات انجام شده واحد عملیاتی را در خصوص نقاط ضعف کنترل‌های داخلی مربوط مستندسازی نماید.

تبصره- در صورت عدم رفع نقاط ضعف کنترل‌های داخلی موضوع این ماده، مدیر ارشد حسابرسی داخلی موظف است مراتب را به کمیته حسابرسی گزارش نماید.

ماده ۵۵– واحد حسابرسی داخلی مؤسسه اعتباری موظف است در صورت بروز تقلب و سوء استفاده از دارایی‌های مؤسسه اعتباری، مراتب را به واحد مدیریت ریسک گزارش دهد و واحد مذکور موظف است موضوع را در فرآیند مدیریت ریسک عملیاتی مد نظر و مورد استفاده قرار دهد به گونه‌ای که از بروز مجدد تقلب و سوء استفاده مذکور ممانعت به عمل آید.

ماده ۵۶– مدیر ارشد واحد حسابرسی داخلی مؤسسه اعتباری موظف است در صورت با اهمیت بودن نقاط ضعف اجرای سازوکارهای کنترلی مورد اشاره در این دستورالعمل یا بروز تقلب با اهمیت، اقدامات اصلاحی مقتضی مربوط به نظام کنترل داخلی را به کمیته حسابرسی پیشنهاد نماید.

تبصره ۱- کمیته حسابرسی مؤسسه اعتباری موظف است گزارش ارایه شده موضوع این ماده را بررسی و تا صدور مصوبه هیأت مدیره پیگیری نماید.

تبصره ۲- مدیر ارشد حسابرسی داخلی موظف است مصوبه هیأت مدیره موضوع تبصره (۱) این ماده را به مدیریت کل نظارت بر بانک‌ها و مؤسسات اعتباری بانک مرکزی و حسابرس مستقل ارسال نماید.

ماده ۵۷– مدیر ارشد حسابرسی داخلی مؤسسه اعتباری موظف است موارد بسیار بااهمیت ناکارآمدی‌های نظام کنترل داخلی را در مقاطع زمانی شش ماهه یا حسب درخواست بانک مرکزی، به بانک مرکزی گزارش نماید.

ماده ۵۸– مدیر ارشد رعایت قوانین و مقررات (تطبیق)، موظف است گزارش‌های مربوط به رعایت مفاد این دستورالعمل و مصادیق عدم رعایت آن را به کمیته رعایت قوانین و مقررات (تطبیق) ارایه نموده و پس از تأیید در کمیته یادشده، مراتب را در هیأت مدیره برای تصویب، گزارش نماید و مصوبه هیأت مدیره را به مدیریت کل نظارت بر بانک‌ها و مؤسسات اعتباری بانک مرکزی ارسال کند.

ماده ۵۹– هیأت مدیره مؤسسه اعتباری موظف است به صورت سالانه گزارش کنترل داخلی مشتمل بر نحوه استقرار نظام کنترل داخلی بر اساس مفاد این دستورالعمل و نتایج حاصل از ارزیابی اثربخشی آن را به بانک مرکزی و حسابرس مستقل ارایه دهد.

فصل هشتم ــ سایر موارد

ماده ۶۰– هیأت مدیره مؤسسه اعتباری موظف است ضوابط داخلی پیشنهادی مدیر ارشد حسابرسی داخلی ناظر بر اجرای کارا و اثربخش این دستورالعمل را ظرف مدت شش ماه از تاریخ ابلاغ آن تصویب نماید و نسخه‌ای از آن را به بانک مرکزی ارسال نماید.

ماده ۶۱– تخطی از احکام این دستورالعمل موجب اعمال مجازات‌های مقرر در قوانین و مقررات ذی‌ربط می‌شود.

«دستورالعمل حداقل الزامات ناظر بر استقرار نظام کنترل‌های داخلی در مؤسسات اعتباری» در (٦١) ماده و (٤) تبصره در پنجاه و یکمین جلسه مورخ ۱۴۰۲/۱۱/۲۹ کمیسیون مقررات و نظارت مؤسسات اعتباری به تصویب رسید و پس از تاریخ ابلاغ، لازم‌الاجرا بوده و از تاریخ لازم‌الاجرا شدن این دستورالعمل، «رهنمودهایی برای نظام مؤثر کنترل داخلی در مؤسسات اعتباری» موضوع بخشنامه شماره ۱۱۷۲/مب مورخ ۱۳۸٦/۳/۳۱ و سایر ضوابط و مقررات مغایر با دستورالعمل حاضر منسوخ می‌گردد.