МОНГОЛБАНКНЫ
ЕРӨНХИЙЛӨГЧИЙН ТУШААЛ

2023 оны 08 сарын 18 өдөр Дугаар А - 157 Улаанбаатар хот

Журам батлах тухай

Төв банк (Монголбанк)-ны тухай хуулийн 19 дүгээр зүйлийн 1 дэх хэсэг, 28 дугаар зүйлийн 1 дэх хэсгийн 2 дахь заалтыг тус тус үндэслэн ТУШААХ нь:

1.“Банкны мэдээллийн технологийн үйл ажиллагааг зохицуулах журам”-ыг хавсралтаар баталсугай.

2.Энэ тушаал батлагдсантай холбоотойгоор Монголбанкны Ерөнхийлөгчийн 2017 оны 06 дугаар сарын 29-ний өдрийн А-189 дүгээр тушаалыг хүчингүй болсонд тооцсугай.

3.Энэ тушаалын биелэлтэд хяналт тавьж ажиллахыг Хяналт шалгалтын газар (Ц.Нарандалай), Банкны бүтцийн өөрчлөлт, бодлогын газар (Н.Ариунбат)-т тус тус үүрэг болгосугай.

ЕРӨНХИЙЛӨГЧ Б.ЛХАГВАСҮРЭН

1523011440

Монголбанкны Ерөнхийлөгчийн 2023 оны 08 дугаар сарын 18..-ны өдрийн А-157 дугаар тушаалын хавсралт

БАНКНЫ МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН ҮЙЛ АЖИЛЛАГААГ ЗОХИЦУУЛАХ ЖУРАМ

НЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1. Энэхүү журмын зорилго нь банкны мэдээллийн технологийн үйл ажиллагааг COBIT (Мэдээллийн технологийн хяналт, удирдлагын тогтолцоо) болон PCI-DSS (Төлбөрийн картын мэдээллийн аюулгүй байдлын стандарт)-ын холбогдох зохицуулалтад үндэслэн зохицуулах, хяналт тавихад оршино.

1.2. Банк нь энэ журам болон өөрийн үйл ажиллагааны онцлог, цар хүрээ болон бүтээгдэхүүн үйлчилгээг харгалзан өөрийн баримтлах бодлого, журам, дүрэм, зааврыг боловсруулан батална.

ХОЁР. МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН СТРАТЕГИ

2.1. Банк нь компанийн зохистой засаглалтай уялдсан мэдээллийн технологийн зохистой засаглалыг хэрэгжүүлнэ.

2.2. Банк нь өөрийн бизнесийн стратеги, төлөвлөгөөтэй уялдсан мэдээллийн технологийн стратеги, төлөвлөгөөг хэрэгжүүлнэ.

2.3. Банк нь тухайн стратеги, төлөвлөгөөг хэрэгжүүлэх удирдлагын зохистой бүтэц, шаардлагатай төсөв, хүний нөөцийг бүрдүүлж ажиллана.

2.4. Банк мэдээллийн технологийн стратеги төлөвлөгөөг дэмжих бодлого, дүрэм, журам, заавар болон бусад баримт бичгийг боловсруулж батална.

2.5. Банк нь мэдээллийн технологитой холбоотой журам, дүрэм, заавар болон бусад холбогдох баримт бичгийг тогтмол шинэчилж сайжруулна.

2.6. Энэ журамд мэдээллийн систем гэж үндсэн бүртгэлийн систем болон бусад системүүдийг ойлгоно.

2.7. Банк нь COBIT 4.1 болон түүнээс дээш тогтолцоог баримтлан хэрэгжүүлэх бөгөөд өөрийн бизнесийн стратегитай уялдсан процессуудыг сонгон хэрэгжүүлнэ.

2.8. Энэ журамд COBIT тогтолцоо гэж Мэдээллийн технологийн засаглалын институт /ITGI/, Мэдээллийн системийн аудит болон хяналтын холбоо /ISACA/-оос гаргасан мэдээллийн технологийн хяналт, удирдлагын тогтолцоог ойлгоно.

ГУРАВ. МЭДЭЭЛЛИЙН СИСТЕМИЙН БИЕТ БАЙРШИЛ

3.1. Банкны мэдээллийн технологийн үндсэн болон нөөц дата төвүүд нь Монгол Улсын нутаг дэвсгэрт байрлах ба Монгол Улсад үйл ажиллагаа эрхэлдэг дата төвийн үйлчилгээ үзүүлэгч этгээдийн дата төвд байршиж болно.

3.2. Энэ журамд үйлчилгээ үзүүлэгч гэж гэрээгээр үйлчилгээ, бүтээгдэхүүн нийлүүлэгч бие даасан хараат бус хувь хүн, байгууллагыг ойлгоно.

3.3. Энэ журамд үндсэн дата төв гэж үндсэн бүртгэлийн систем, түүний сервер, тоног төхөөрөмж байршиж буй дата төвийг ойлгоно.

3.4. Энэ журамд үндсэн бүртгэлийн систем гэж банкны санхүүгийн үндсэн бүртгэлийн програм хангамж, өгөгдлийн санг ойлгоно.

3.5. Нөөц дата төв нь үндсэн дата төвд нөлөөлөх боломжтой онцгой нөхцөлд өртөхөөргүй газар зүйн байршилд байна.

3.6. Энэ журамд нөөц дата төв гэж үндсэн дата төвд онцгой нөхцөл үүссэн үед хэвийн үйл ажиллагааг ханган ажиллах зорилго бүхий үндсэн бүртгэлийн нөөц систем, түүний сервер, тоног төхөөрөмж байршиж байгаа дата төвийг ойлгоно.

3.7. Энэ журамд онцгой нөхцөл гэж мэдээллийн систем болон сервер тоног төхөөрөмжийн алдаа, хүний санаатай болон санамсаргүй үйлдэл, гал түймэр, газар хөдлөлт, хүчтэй салхи, үер, аянга зэрэг гэнэтийн осол, байгалийн гамшиг болон бусад шалтгаанаар мэдээллийн систем хэвийн үйл ажиллагаагаа алдахыг ойлгоно.

3.8. Үндсэн болон нөөц дата төвийн тасралтгүй, найдвартай ажиллагаанд дараах шаардлагыг тавина. Үүнд:

3.8.1. Үндсэн болон нөөц дата төвийн сервер, тоног төхөөрөмж, мэдээллийн системийн засвар үйлчилгээ, шинэчлэлийг тогтмол хийх;

3.8.2. Үндсэн болон нөөц дата төвийн сервер, тоног төхөөрөмж, мэдээллийн системийн тохиргоо, түүнд орсон өөрчлөлт бүрийг баримтжуулж хадгалах;

3.8.3. Үндсэн болон нөөц дата төвд зөвхөн эрх бүхий ажилтан нэвтрэх бөгөөд нэвтрэх бүрд бүртгэл хөтлөх;

3.8.4. Үндсэн болон нөөц дата төв нь цахилгааны нэмэлт эх үүсвэр болох тог баригч (UPS), эрчим хүчний нэмэлт шугам, генератортай байх;

3.8.5. Үндсэн болон нөөц дата төвийн сервер, тоног төхөөрөмж, хөргөлтийн систем, агаарын чийгшил тохируулагч систем, гал унтраах систем, өрөөний мэдрэгчийг цахилгааны нэмэлт эх үүсвэрт холбосон байх;

3.8.6. Үндсэн дата төвийг нөөц дата төвтэй үндсэн ба нөөц шугамаар холбосон байх.

ДӨРӨВ. ЭРСДЭЛИЙН УДИРДЛАГА

4.1. Банк нь харилцагчид мэдээллийн технологид суурилсан банк санхүү болон холбогдох бусад үйлчилгээг үзүүлэхдээ банкны стратеги зорилт, бизнес төлөвлөгөө болон банкны мэдээллийн технологийн хүчин чадал, эрсдэлийг хүлээн зөвшөөрөх хэмжээнд тохируулсан эрсдэлийг тодорхойлж, үнэлж, хянаж, тайлагнаж, удирдах зорилгоор эрсдэлийн удирдлагын бодлого, дүрэм, журам болон бусад баримт бичгийг боловсруулан баталж үйл ажиллагаандаа тогтмол хэрэгжүүлнэ.

4.2. Банк нь дараах мэдээллийн технологийн эрсдэлд тогтмол үнэлгээ хийж эрсдэлийг бууруулах арга хэмжээг тухай бүр авч хэрэгжүүлнэ. Үүнд:

4.2.1. Технологийн өөрчлөлтийн банкны мэдээллийн систем болон үйл ажиллагаанд үзүүлэх сөрөг нөлөөлөл;

4.2.2. Мэдээллийн технологитой холбоотой гадна болон дотоодын эх үүсвэртэй луйвар, залилан, хууран мэхлэх оролдлого, нууцлал алдагдах, тэдгээртэй холбоотой аюулгүй байдлын алдаа дутагдлын эрсдэл;

4.2.3. Банкны үүлэн технологид байршсан мэдээллийн систем болон үйлчилгээнд учирч болзошгүй сөрөг нөлөөлөл.

4.3. Банкны мэдээллийн технологийн үйл ажиллагаанд үйлчилгээ үзүүлэгчээс үйлчилгээ авсан тохиолдолд үйлчилгээ үзүүлэгчийн ажлын гүйцэтгэлд тогтмол хяналт тавина;

4.4. Банк нь үндсэн үйл ажиллагаанд сөргөөр нөлөөлөхүйц онцгой нөхцөл гарсан үед үйл ажиллагааг тасралтгүй үргэлжлүүлэх боломжийг хангах төлөвлөгөө боловсруулж батална. Ялангуяа, гадны хүчин зүйлд өртөмтгий үйл ажиллагаа болон дэд бүтцэд нөлөөлж болзошгүй аюулыг үнэлж, эдгээр эрсдэлтэй тулгарсан тохиолдолд нэн чухал бизнесийн үйл ажиллагааг тасалдалгүй үргэлжлүүлэх төлөвлөгөөтэй байна;

4.5. Банк нь харилцагч гүйлгээг хүлээн зөвшөөрөхгүй байх эрсдэлийг бууруулах үүднээс гүйлгээ болон үйлдлийн лог бүртгэлийг энэ журмын 8.1 дэх хэсэгт заасан хугацаагаар хадгална;

4.6. Банк нь лог бүртгэлийн бүрэн бүтэн байдалд халдаж болзошгүй аюулыг тогтмол хянах бөгөөд лог бүртгэлийг лог бүртгэлийн сервер дээр хуулж давхар хадгална.

ТАВ. ТУСГАЙЛСАН ХЯНАЛТ, УДИРДЛАГА

5.1. Банк өөрийн мэдээлэл технологийн аюулгүй байдлыг дараах байдлаар хангана:

5.1.1 Банкны удирдлага нь аюулгүй байдлын хяналтын үйл ажиллагааг хэрэгжүүлэн тогтмол хянаж ажиллах бөгөөд зөвхөн хэрэглэгчийн эрх, эрхийн матриц, хэрэглэгчийн эрхийн бүлэгт тулгуурласан хандалтыг зөвшөөрдөг байхын зэрэгцээ мэдээллийг эзэмшигч буюу тухайн мэдээллийг хариуцагч хэрэглэгч, банкны нэгжийн баталгаажуулснаар ажилтанд тухайн мэдээлэлд хандах эрхийг олгоно.

5.1.2 Энэ журамд хэрэглэгч гэж мэдээллийн системийг ашиглаж буй банкны ажилтныг ойлгоно.

5.1.3 Хэрэглэгч бүр өөрийн гэсэн дахин давтагдашгүй хэрэглэгчийн нэр, нууц үгтэй байх бөгөөд зөвхөн өөрийн хэрэглэгчийн нэр, нууц үгийг ашиглан зөвшөөрөгдсөн мэдээллийн систем болон мэдээлэлд хандана.

5.1.4 Нийтийн сүлжээгээр дамжуулан мэдээллийн системд хандах тохиолдолд хэрэглэгчийг таних хоёроос доошгүй шаттай баталгаажуулалтыг ашиглах бөгөөд мэдээллийг дамжуулахад нууцлалтай холболт ашиглана.

5.1.5 Хэрэглэгчийн эрхийг зөвхөн тухайн ажилтны ажил үүргийн хуваарийн дагуу хандах шаардлагатай мэдээллийн систем, мэдээлэлд хандах хязгаарлалттай байдлаар олгоно. Мөн нэг хэрэглэгчид бүх эрхийг олгохыг хориглох ба шат дараалсан хяналттай байна.

5.1.6 Хэрэглэгчийн эрхийн бүлгийг тухайн хэрэглэгчийн эрхийн бүлэгт хамаатай мэдээллийн систем болон мэдээлэлд хандах байдлаар тодорхойлно. Энэхүү хэрэглэгчийн эрхийн бүлгийг ажил үүргийн зөв зохистой хуваарилалт, тусгаарлалтыг дэмжсэн байдлаар тодорхойлж ялгана.

5.1.7 Хэрэглэгчийн эрх болон хэрэглэгчийн эрхийн бүлгүүдийг тогтмол хянан шалгаж, банкны бүтэц зохион байгуулалт, мэдээллийн технологи болон мэдээллийн

системийн өөрчлөлтөд нийцүүлэн тухай бүр шинэчилнэ.

5.2. Банк нь гүйлгээний бүрэн бүтэн байдлыг дараах байдлаар хангана:

5.2.1. Банк мета дата, мастер дата болон гүйлгээ бүрийн бүрэн бүтэн байдлыг хангах зорилгоор тогтмол лог бүртгэл хийх бөгөөд тухайн лог бүртгэлд өөрчлөлт орсон бол тухайн өөрчлөлтийг буцаан сэргээх хэмжээний дэлгэрэнгүй мэдээллийг багтаана.

5.2.2. Гүйлгээ болон үйлдлийн лог бүртгэл энэ журмын 8.1 дэх хэсэгт заасан хугацааны мэдээллийг агуулах бөгөөд дараах шаардлагыг хангана. Үүнд:

5.2.2.1. Мэдээлэлд хандаж өөрчлөлт хийсэн, өөрчлөх оролдлого хийсэн хүн, хэрэглэгч, мэдээллийн системийг бүртгэнэ.

5.2.2.2. Өөрчлөлт хийсэн,өөрчлөх оролдлого хийсэн он, сар, өдөр, цаг, минут, секундийн мэдээллийг бүртгэнэ.

5.2.2.3. Өөрчлөлт хийсэн, өөрчлөх оролдлого хийсэн мэдээллийн систем болон мэдээллийг бүртгэх бөгөөд өөрчлөлтийн өмнөх утга болон шинэчлэгдсэн утгыг бүртгэнэ.

5.2.2.4. Зөвхөн зөвшөөрөгдсөн хэрэглэгч лог бүртгэлийн системд хандаж лог бүртгэлийг харах эрхтэй байна.

5.2.2.5. Лог бүртгэлийн мэдээллийг зөвхөн хадгалах хугацаа хэтэрсэн тохиолдолд устгаж болно.

5.2.2.6. Лог бүртгэлийн систем нь зөвшөөрөлгүй хандах оролдлого бүрийг бүртгэнэ.

5.2.2.7. Лог бүртгэлд тогтмол хяналт тавих бөгөөд бүрэн бүтэн байдал алдагдсан тохиолдлыг тухай бүр илрүүлж, засан залруулах арга хэмжээ авна.

5.2.2.8. Банкны харилцагчтай холбоотой гүйлгээ хийх гэрээ бүхий үйлчилгээ үзүүлэгчийн лог бүртгэлд банк хандах эрхтэй байна.

5.3. Банк нь татгалзах боломжгүй байдлыг дараах байдлаар хангана:

5.3.1. Харилцагч гүйлгээг хүлээн зөвшөөрөөгүй тохиолдолд банк тухайн харилцагч гүйлгээг хийсэн гэдгийг батлах зорилгоор дараах мэдээлэл бүхий лог бүртгэлийг харилцагчтай хуваалцана. Үүнд:

5.3.1.1. Харилцагчийг нотлох хувь хүний мэдээлэл;

5.3.1.2. Хандалтын мэдээлэл буюу IP хаяг;

5.3.1.3. Гүйлгээний он, сар, өдөр, цаг, минут, секунд.

5.4. Банк нь өгөгдөл оруулах хяналт, удирдлагыг дараах байдлаар хэрэгжүүлнэ:

5.4.1. Өгөгдөл оруулах хяналт, удирдлага нь холбогдох журам болон хяналтууд дараах үүргийг биелүүлж байгаа эсэхийг баталгаажуулна. Үүнд:

5.4.1.1. Хүлээж авсан өгөгдлийн бүрэн бүтэн байдал;

5.4.1.2. Хүлээж авсан өгөгдлийн өмнө нь боловсрогдоогүй байдал;

5.4.1.3. Хүлээж авсан өгөгдлийн алдаагүй байдал;

5.4.1.4. Шаардлагатай зөвшөөрөл авсан байдал;

5.4.1.5. Мэдээллийн системд давхардаж ороогүй байдал.

5.4.2. Хэрэглэгч болон гадны эх үүсвэрээс өгөгдөл шууд авах тохиолдолд өгөгдлийг шалгаж баталгаажуулдаг хяналттай байна.

5.4.3. Өгөгдөл шинээр үүсгэх, оруулахад дараах хяналтууд байна. Үүнд:

5.4.3.1. Өгөгдөл оруулах зөвшөөрөл:

Өгөгдөл хүлээн авах мэдээллийн систем бүрийн өгөгдөл оруулах зөвшөөрлийг тодорхой болгож, мөрддөг байна.

5.4.3.2. Багцын хяналт:

Тоо ширхгийн нийт дүн, гүйлгээний нийт дүн, баримт бичгийн нийт дүнг тулган баталгаажуулах зэрэг багцын хяналтыг хийхээс гадна зарим өгөгдлийг гараар оруулсан тохиолдолд, эх өгөгдөл болон гараар тооцоолсон өгөгдлийн нийт дүн нь компьютерын нийт дүнтэй нийцэж байгаа эсэхийг шалгана.

5.4.3.3. Алдааны тайлан:

Банк өгөгдөл оруулахтай холбоотой үүсч болох алдааг зохицуулах, тайлагнах баримт бичгийг боловсруулж баталсан байна. Уг баримт бичиг нь багц өгөгдөл орох үед алдаа илэрсэн бол энэхүү багцыг бүхэлд нь буцаах, алдааг засагдтал хүлээх, хүлээн авч боловсруулсны дараа алдааг гараар засаж залруулга хийх шаардлагатай гэж тэмдэглэх зэрэг шийдлүүдээс сонгох боломжуудыг дурдсан байна.

5.5. Банкны өгөгдөл боловсруулах болон түүний алдааг зохицуулах хяналт, удирдлага нь хүлээж авах өгөгдөл үнэн зөв боловсруулагдан гарч байгаа эсэхэд хяналт тавих бөгөөд дараах хяналтын арга хэмжээг авсан байна. Үүнд:

5.5.1. Гүйлгээний боловсруулалтын бүрэн бүтэн байдлыг хангах;

5.5.2. Гүйлгээ бүр дахин давтагдашгүй байх;

5.5.3. Бүх гүйлгээ хүчин төгөлдөр байх;

5.5.4. Компьютерын үйл ажиллагаанд аудит хийж шалгах боломжтой байх;

5.5.5. Мэдээллийн систем хүлээж авах болон мэдээллийн системээс гарах өгөгдлийг шалган баталгаажуулах;

5.5.6. Зөв мэдээлэл, файлуудыг боловсруулах;

5.5.7. Боловсруулалтын үе шатуудаар дамжих өгөгдлийг зөв зохистой дамжуулах;

5.5.8. Боловсруулалтын өмнө, боловсруулалтын үеэр болон боловсруулалтын дараах өгөгдлүүдийг тулган шалгаж байх;

5.5.9. Боловсруулалтын явцад алдаа илрүүлсэн тохиолдолд алдаа гаргасан этгээдэд буцааж, алдааг арилгаж, залруулга хийсний дараагаар дахин боловсруулалт хийх;

5.5.10. Өгөгдлийн шинэчлэлийг хянах;

5.5.11. Өгөгдөл боловсруулалтад өөрчлөлт хийх хүсэлт, баталгаажуулалт болон зөвшөөрлийг хянах;

5.5.12. Өгөгдлийн боловсруулалт дахь алдааны боловсруулалт;

Гүйлгээ саатахаас урьдчилан сэргийлэх зорилгоор өгөгдлийн боловсруулалтаас өмнө алдааг илрүүлэх, тогтоох аргачлалтай байна.

5.6. Банкны өгөгдөл хадгалах хяналт, удирдлага нь мета дата, мастер дата болон урт хугацааны суурь өгөгдлийн бүрэн бүтэн байдлыг хадгалах зорилготой. Мета дата, мастер дата болон урт хугацааны суурь өгөгдөлд хадгалагдаж буй мэдээлэл нь санхүүгийн болон үйл ажиллагааны тайлан, тэдгээрийн боловсруулалтад чухал үүрэг гүйцэтгэдэг тул өндөр түвшинд хамгаалах бөгөөд дараах хяналтын арга хэмжээг авна. Үүнд:

5.6.1. Өгөгдөл нэмэх, засах үйлдлийг зөвхөн зөвшөөрөгдсөн болон хянагдсан үед хийнэ.

5.6.2. Өгөгдөлд хандах логик болон биет хандалтыг хязгаарлаж, хяналт тавих бөгөөд зөвхөн банкны мэдээллийн ангилал, хэрэглэгчийн эрхийн матрицын дагуу хандах эрхийг олгоно.

5.6.3. Өгөгдлийн шинэчлэлтэй холбоотой журам, зааврыг батлуулж гаргасан байна.

5.6.4. Өгөгдлийг хадгалах үйл явцыг хараат бус этгээдээр тогтмол хянуулж, өгөгдлийн шинэчлэлтэй холбоотой журам, зааврын хэрэгжилтийг шалгана.

5.7. Банкны гарах өгөгдлийн хяналт, удирдлага нь гарах өгөгдөл бүрэн бүтэн байхын зэрэгцээ зөв хуваарилагдаж очиж байгаа эсэхийг хянах зорилготой. Өгөгдөл гарах сүүлийн үе шатуудад хийгдэх хяналт, удирдлага нь өмнөх үе шатууд үнэн зөв хийгдсэн байдлыг баталгаажуулж, залруулах бөгөөд дараах хяналтуудаас бүрдэнэ. Үүнд:

5.7.1. Өгөгдөл нь цаг тухайд нь үнэн зөв боловсруулагдан хуваарилагдаж байна.

5.7.2. Тогтмол логик болон биет хяналтын дор байх бөгөөд гарах өгөгдлийн нууцлал болон хэрэглэгчдийн хандалтын түвшинд дараах шаардлага тавигдана. Үүнд:

5.7.2.1. Гарах өгөгдөлд зөвхөн зөвшөөрөгдсөн, эрх бүхий хэрэглэгчид хандана.

5.7.2.2. Сүлжээгээр дамжин хэрэглэгчид хүрэх гарах өгөгдлийг нууцлалтай холболт ашиглан дамжуулна.

5.7.2.3. Гарах биет өгөгдөлд зөвхөн зөвшөөрөгдсөн, хязгаарлагдмал орчинд хандах боломжийг олгоно.

5.7.3. Гарах өгөгдөл нь тухайн өгөгдөл оруулах үеийн хяналтын тохиргоо, параметр үзүүлэлттэй бүрэн тохирч байна.

5.7.4. Өгөгдлийн бүрэн бүтэн, алдаагүй байдлыг шалгаж баталгаажуулна. Дэлгэрэнгүй лог бүртгэл нь энэхүү баталгаажуулалтыг хялбарчлах бөгөөд үйл ажиллагааны тайланг үнэн зөв гарсан эсэхийг шалгахад дэмжлэг болохоос гадна алдаатай өгөгдлийг тодорхойлоход тусална.

5.7.5. Гарах өгөгдөл нь алдаагүй байна. Алдаа гарсан тохиолдолд эрх бүхий хэрэглэгч алдаатай гарах өгөгдлийг засан залруулж болох бөгөөд энэ арга хэмжээг журам, заавар бусад баримт бичгээр зохицуулсан байна.

ЗУРГАА. ДОТООД АУДИТ

6.1. Банкны дотоод аудитын нэгж нь дараах шаардлагыг хангасан мэдээллийн технологийн аудитортай байна. Үүнд:

6.1.1. Банкны мэдээллийн технологийн аудитор нь мэдээллийн технологийн чиглэлээр бакалавр эсхүл түүнтэй дүйцэхүйц чиглэлээр бакалавр болон түүнээс дээш зэрэгтэй,мэдээллийн технологийн чиглэлээр гурваас доошгүй жилийн ажлын туршлагатай байна.

6.1.2. Банк нь нэгээс доошгүй CISA гэрчилгээ бүхий мэдээллийн технологийн аудитортай байна. CISA гэрчилгээ бүхий мэдээллийн технологийн аудитор байхгүй тохиолдолд CISA гэрчилгээ бүхий гуравдагч талаар мэдээллийн технологийн аудитыг хийлгэж болно.

6.2. Энэ журамд CISA гэрчилгээ гэж Мэдээллийн системийн аудит болон хяналтын холбоо /ISACA/-оос олгодог мэдээллийн системийн аудиторын гэрчилгээг ойлгоно.

6.3. Банк нь мэдээллийн технологийн үйл ажиллагаа болон мэдээллийн системд хийх хяналт, удирдлагын аудитыг хамгийн багадаа улиралд нэг удаа хийнэ. Аудитын тайланг дараа улирлын эхний сарын 10-ны өдрийн дотор Монголбанканд хүргүүлнэ.

6.4. Тайланг ирүүлэхдээ аудитаар илэрсэн асуудлуудыг эрсдэл болон шийдвэрлэх боломжит хугацаагаар эрэмбэлэн жагсаасан байна.

ДОЛОО. ХӨНДЛӨНГИЙН АУДИТ

7.1. Банкны санхүүгийн тайланд хөндлөнгийн аудит хийх баг нь CISA гэрчилгээ бүхий гуравдагч талаас мэдээллийн технологийн аудитын үйлчилгээ авч болно.

7.2. Банкны санхүүгийн хөндлөнгийн аудитыг хийх баг нь санхүүтэй холбоотой мэдээллийн системд мэдээллийн технологийн хяналт, удирдлагын аудитыг хийх бөгөөд тус тайланг санхүүгийн тайлантай хамтад нь Монголбанканд хүргүүлнэ.

7.3. COBIT тогтолцоонд суурилсан Мэдээллийн технологийн хяналт, удирдлагын аудитыг энэ журмын 2.7 дахь хэсэгт заасны дагуу хэрэгжүүлж буй процессуудад хамгийн багадаа хоёр жилд нэг удаа хийх бөгөөд тус аудитын тайланг, тайлан бэлэн болсноос хойш 14 хоногийн дотор Монголбанканд хүргүүлнэ.

НАЙМ. ЛОГ БҮРТГЭЛ

8.1. Банк нь гүйлгээний лог бүртгэл буюу үндсэн бүртгэлийн системийн санхүүгийн гүйлгээ хийсэн, хийхийг завдсан дэлгэрэнгүй түүхийн сүүлийн 10 жилийн мэдээллийг хадгална. Үйлдлийн лог бүртгэл буюу үндсэн бүртгэлийн системд нэвтэрсэн, өөрчлөлт хийсэн, хийхийг завдсан болон өөрчлөлт хийсэн үйлдлийн түүхийн сүүлийн 3 сарын мэдээллийг онлайн хадгалах ба сүүлийн 3 жилийн мэдээллийг офлайн лог бүртгэлд хадгалж болно.

8.2. Лог бүртгэлийн систем нь бизнесийн тасралтгүй ажиллагааны төлөвлөгөөг мөн адил ханган ажиллана.

8.3. Лог бүртгэлийг үйлдлийн системд бүртгэхийн зэрэгцээ зориулалтын лог бүртгэлийн серверт тухай бүр давхар бүртгэнэ.

8.4. Лог бүртгэлийн серверт хандах эрх хязгаарлалттай байх бөгөөд нэг хэрэглэгч үйлдлийн систем болон лог бүртгэлийн системд хоёуланд нь хандах эрхтэй байж болохгүй.

8.5. Лог бүртгэлийн серверээс мэдээлэл устгах боломжийг бүрэн хязгаарлана.

8.6. Энэ журамд лог бүртгэл гэж гүйлгээний болон үйлдлийн лог бүртгэлийг ойлгоно.

ЕС. МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН ҮЙЛЧИЛГЭЭ АВАХ

9.1. Мэдээллийн технологийн үйлчилгээг үйлчилгээ үзүүлэгчээс авах тохиолдолд банк эрсдэлийн удирдлагад болон үйлчилгээ үзүүлэгчид хяналт тавих бөгөөд дараах хяналтын арга хэмжээнүүд хэрэгжүүлнэ. Үүнд:

9.1.1. Үйлчилгээ үзүүлэгчээс үйлчилгээ авах тохиолдолд үүдэн гарах дэд бүтцийн эрсдэлийг хянана.

9.1.2. Мэдээллийн технологийн үйлчилгээ авах гэрээ байгуулахаас өмнө үйлчилгээ үзүүлэгчийг магадлан шалгана.

9.1.3. Мэдээллийн технологийн үйлчилгээ авах гэрээ болон үүсэх харилцаа нь банкны эрсдэлийн удирдлага, мэдээллийн аюулгүй байдал, харилцагчийн мэдээллийн нууцлалын бодлого, журам болон холбогдох бусад баримт бичгүүдтэй нийцтэй байна.

9.2. Банк үйлчилгээ үзүүлэгчээс үйлчилгээ авсан тохиолдолд үйлчилгээ үзүүлэгч банкны өмнө хариуцлага хүлээх бөгөөд доорх заалтуудыг гэрээнд тусгана. Үүнд:

9.2.1. Гүйцэтгэлийн хэмжигдэхүүн, зорилтууд болон гүйцэтгэл хангалтгүй тохиолдолд гэрээг цуцлах, ногдуулах торгууль, хохирол барагдуулах заалтууд;

9.2.2. Гэрээ хүчингүй болсон тохиолдолд үйлчилгээ үзүүлэгч үйлчилгээг өөр үйлчилгээ үзүүлэгч эсвэл банканд шилжүүлэн өгөх заалтууд;

9.2.3. Гэрээний хэрэгжилтийн хугацаанд бий болох, худалдан авах, мөн хуваалцах өмч хөрөнгийн эзэмших эрхийг тодорхой заасан заалтууд;

9.2.4. Үйлчилгээ үзүүлэгч нь үйлчилгээг туслан гүйцэтгэгчээс авах зөвшөөрөл болон туслан гүйцэтгэгчээс авах үйлчилгээний хязгаарыг заасан заалтууд;

9.2.5. Туслан гүйцэтгэгчийн зөвшөөрөл авсан тохиолдолд үндсэн гэрээт үйлчилгээ үзүүлэгчид тавигдах шаардлагууд туслан гүйцэтгэгчид мөн адил үйлчлэхийг туслан гүйцэтгэгчтэй хийх гэрээнд заасан байна.

АРАВ. МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН АУДИТЫН ҮЙЛЧИЛГЭЭГ ГЭРЭЭТ ГҮЙЦЭТГЭГЧЭЭС АВАХ

10.1. Банк нь мэдээллийн технологийн аудитын үйлчилгээг гуравдагч талд даатгах боломжтой бөгөөд гуравдагч тал нь дараах шаардлагыг хангасан байна. Үүнд:

10.1.1. Гуравдагч тал буюу мэдээллийн технологийн аудитын үйлчилгээ үзүүлэгч байгууллага нь CISA гэрчилгээтэй, мэдээллийн технологийн чиглэлээр бакалавр болон түүнээс дээш зэрэгтэй,мэдээллийн технологийн чиглэлээр тавааc доошгүй жилийн ажлын туршлагатай үүнээс мэдээллийн технологийн аудитын чиглэлээр хоёроос доошгүй жилийн ажлын туршлагатай мэдээллийн технологийн аудитортай байна.

10.1.2. Тухайн банканд сүүлийн гурван жил бүтээгдэхүүн, үйлчилгээ нийлүүлээгүй байна. Үүнд хөндлөнгийн аудитын үйлчилгээ хамаарахгүй.

10.1.3. Мэдээллийн технологийн аудит хийх гуравдагч талын хувьцаа эзэмшигч болон гүйцэтгэх удирдлага нь аудитын үйлчилгээг авч байгаа банкны холбогдох этгээд байж болохгүй.

10.1.4. Мэдээллийн технологийн аудит хийх гуравдагч тал болон банк хоорондын эрх, үүрэг, хариуцлагатай холбоотой харилцааг зохицуулах зорилгоор гэрээ байгуулах бөгөөд тус гэрээ нь энэхүү журмын заалтуудтай бүрэн нийцсэн байна.

АРВАН НЭГ. НУУЦЛАЛ

11.1. Банк нь мэдээллийг эрсдэлийн үнэлгээ болон мэдээллийн нууцлалын зэрэгт үндэслэн задруулахаас урьдчилан сэргийлж аюулгүй байдал болон нууцлалыг хангасан байдлаар хадгалах бөгөөд нууцлал, аюулгүй байдал нь дараах шаардлагыг хангана. Үүнд:

11.1.1. Мэдээллийг өндөр зэрэглэлийн нууцлалын алгоритм ашиглан нууцална.

11.1.2. Мэдээллийг хадгалах болон нийтийн сүлжээ ашиглан дамжуулах тохиолдолд өндөр зэрэглэлийн нууцлал болон нууцлалтай холболт ашиглана.

11.1.3. Нууцлалын алгоритм нь олон нийтэд аюулгүй байдлыг хангасан буюу найдвартай гэж хүлээн зөвшөөрөгдсөн алгоритм байх бөгөөд өндөр зэрэглэлийн түлхүүр ашиглана.

11.1.4. Банк өөрийн нууцлалын алгоритмуудад хяналт тавих бөгөөд шаардлага хангаж байгаа эсэхийг тогтмол шалгаж шинэчлэн сайжруулна.

11.1.5. Аюулгүй байдлыг хангасан түлхүүрийн дэд бүтцийг дэмжих түлхүүр болон нууцлалын удирдлагын шаардлагыг банкны ажилтан, үйлчилгээ үзүүлэгч, болон банкны оролцогч талуудад ханган ажиллана.

11.2. Энэ журамд банкны оролцогч тал гэж тухайн банкны үйл ажиллагаанд нөлөөлж буй эсвэл нэгдмэл ашиг сонирхол бүхий бүлгийг ойлгоно.

11.3. Энэ журамд нууцлалын алгоритм гэж криптографи ашиглан мэдээлэл унших боломжгүй хэлбэрт хувиргах нууцлалын алгоритмыг ойлгоно.

11.4. Энэ журамд түлхүүрийн дэд бүтэц гэж түлхүүрийн гэрчилгээг олгох, хадгалах ба устгах үүрэгтэй бүтцийг ойлгоно.

АРВАН ХОЁР. ХАРИЛЦАГЧИЙН МЭДЛЭГ

12.1. Харилцагчийн банкны үйлчилгээтэй холбоотой мэдлэг нь аюулгүй байдлын чухал хэсэг бөгөөд банк дараах мэдээллүүдийг банкны ажилтан болон харилцагчид тогтмол хүргэж байна. Үүнд:

12.1.1. Дараах үйлчилгээг ашиглах үед гарч болох эрсдэл, онцгой тохиолдол. Үүнд:

12.1.1.1. Мобайл банк;

12.1.1.2. Интернэт банк;

12.1.1.3. Гар утас;

12.1.1.4. АТМ;

12.1.1.5. Банкны үйлчилгээний бусад сувгууд.

12.1.2. Харилцагч тогтмол мөрдсөнөөр эрсдэлийг бууруулахад чиглэсэн аюулгүй

байдлын болон урьдчилан сэргийлэх арга хэмжээ;

12.1.3. Банкны үйлчилгээний сувгуудтай холбоотой түгээмэл болон шинээр гарч буй эрсдэл, аюул занал, алдаа, дутагдал, эмзэг байдал;

12.1.4. Харилцагч тулгарсан асуудлыг хэрхэн шийдэх, санал гомдол гаргах, банкны эрсдэлтэй тулгарсан тохиолдолд алдааг хэрхэн засах, хохирлыг хэрхэн барагдуулах талаарх мэдээлэл;

12.1.5. Татгалзах боломжгүй байдлын эрсдэлийн удирдлагын хяналт болон холбогдох лог бүртгэл;

12.1.6. Санаатай бус дахин давтагдсан харилцагчийн хувийн мэдээллийн задрал.

12.2. Энэ журамд эмзэг байдал гэж аливаа аюулыг хэрэгжүүлэх, халдлага үйлдэхэд ашиглаж болох суваг, сул цоорхой байдлыг ойлгоно.

12.3. Энэ журамд татгалзах боломжгүй байдал гэж ямар нэг үйлдэл хийгдсэн, учрал тохиолдол болсон байхад түүнийг дараа нь үгүйсгэх боломжгүй байх шинж чанар чадварыг ойлгоно.

АРВАН ГУРАВ. БИЗНЕСИЙН ТАСРАЛТГҮЙ АЖИЛЛАГААНЫ ТӨЛӨВЛӨГӨӨ

13.1. Банк дараах шаардлага бүхий бизнесийн тасралтгүй ажиллагааны төлөвлөгөө/цаашид БТАТ гэх/-г боловсруулан баталж жил бүр хэрэгжүүлнэ. Үүнд:

13.1.1. Оролцогч тус бүрийн үүрэг, хариуцлагыг төлөвлөгөөнд тодорхой тусгана.

13.1.2. Бизнесийн үйл ажиллагаанд учирч болох онцгой нөхцөлийн эрсдэлийн үнэлгээ.

13.1.3. Дараах бүрэлдэхүүн хэсэг бүхий бизнесийн нөлөөллийн үнэлгээ. Үүнд:

13.1.3.1. Банкны нэн чухал бизнесийн үйл ажиллагаа;

13.1.3.2. Банкны нэн чухал бизнесийн үйл ажиллагааг дэмжиж буй дэд бүтэц, түүний эрсдэлийн түвшин;

13.1.3.3. Сэргээн ажиллуулах зорилтот хугацаа буюу мэдээллийн системийн үйл ажиллагаа тасалдсан тохиолдолд үйл ажиллагааг сэргээн ажиллуулахад шаардлагатай хугацаа;

13.1.3.4. Үйлчилгээний хүргэлтийн зорилго буюу сэргээгдсэн мэдээлэл болон үйл ажиллагааны хүлээн зөвшөөрөгдөх түвшин;

13.1.3.5. Сэргээгдсэн цэгийн зорилго буюу сэргээгдсэн мэдээлэл болон үйл ажиллагааны хүлээн зөвшөөрөгдөх алдагдлын түвшин;

13.1.4. БТАТ нь нөөц дата төвийг зохицуулсан заалтуудтай байна.

13.1.5. БТАТ нь дараах үндсэн бүрэлдэхүүн хэсгүүдтэй байна. Үүнд:

13.1.5.1. Гэмтлийн өмнөх бэлэн байдал ба төлөвлөлт;

13.1.5.2. Нөөц дата төвийн бэлэн байдал;

13.1.5.3. БТАТ-ний үүрэг хариуцлага ба багийн гишүүд;

13.1.5.4. БТАТ-г хэрэгжүүлэх аргачлал ба нөөц дата төвд үйл ажиллагааг шилжүүлэх;

13.1.5.5. БТАТ-г дуусгах;

13.1.5.6. Үйл ажиллагааг нөөц дата төвөөс буцаан үндсэн дата төвд шилжүүлэх.

13.1.6. БТАТ-ний сургалтын төлөвлөгөө;

13.1.7. БТАТ-ний туршилтын төлөвлөгөө ба туршилтын үр дүнгийн тайлан;

13.1.8. БТАТ-ний засвар үйлчилгээ ба шинэчлэл.

АРВАН ДӨРӨВ. ТӨЛБӨРИЙН КАРТЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН СТАНДАРТ

14.1. Банк нь PCI-DSS буюу төлбөрийн картын мэдээллийн аюулгүй байдлын стандартын дараах ерөнхий шаардлагуудыг хэрэгжүүлнэ. Үүнд:

14.1.1. Аюулгүй байдлыг хангасан найдвартай сүлжээ болон систем байгуулах;

14.1.1.1. Карт эзэмшигчийн мэдээллийг хамгаалах галт ханын тохиргоо суулган ажиллуулах;

14.1.1.2. Үйлчилгээ үзүүлэгч болон үйлдвэрээс ирсэн өгөгдмөл /default/ хэрэглэгчийн нэр, нууц үг болон бусад өгөгдмөл аюулгүй байдлын тохиргоо, параметрүүдийг ашиглахгүй байх.

14.1.2. Карт эзэмшигчийн мэдээллийг хамгаалах;

14.1.2.1. Хадгалагдсан (өгөгдлийн сан болон бусад) карт эзэмшигчийн мэдээллийг хамгаалах;

14.1.2.2. Карт эзэмшигчийн мэдээллийг нийтийн сүлжээгээр дамжуулах тохиолдолд өндөр түвшний нууцлал болон нууцлалтай холболт ашиглана.

14.1.3. Эмзэг байдлын удирдлагын тогтолцоо хэрэгжүүлэх;

14.1.3.1. Мэдээллийн системийг вирус болон бусад төрлийн хорлон сүйтгэх програм хангамжуудаас хамгаалах бөгөөд вирусийн эсрэг програм хангамжийг тогтмол шинэчлэн сайжруулах;

14.1.3.2. Аюулгүй байдлыг хангасан найдвартай мэдээллийн систем хөгжүүлэх.

14.1.4. Хэрэглэгчийн эрхийн хяналтын арга хэмжээ хэрэгжүүлэх;

14.1.4.1. Карт эзэмшигчийн мэдээлэлд хандах хэрэглэгчийн эрхийг зөвхөн шаардлагатай хэрэглэгчид олгох;

14.1.4.2. Мэдээллийн системийн бүрэлдэхүүн хэсгүүдэд хандах хэрэглэгчийн эрхийг тодорхойлж, хандалтыг баталгаажуулж хяналт тавих;

14.1.4.3. Карт эзэмшигчийн мэдээлэл бүхий сервер, компьютерт биет хандалт хийхийг хязгаарлах, шаардлагатай бол хаах.

14.1.5. Сүлжээнд тогтмол хяналт тавих, нэвтрэлтийн туршилт хийх;

14.1.5.1. Сүлжээ болон карт эзэмшигчийн мэдээллийн хандалтын лог бүртгэлд хяналт тавих;

14.1.5.2. Аюулгүй байдлын систем, түүний үйл ажиллагаанд нэвтрэлтийн

туршилт тогтмол хийх.

14.1.6. Банкны нийт ажилтнуудыг хамруулсан мэдээллийн аюулгүй байдлын бодлого хэрэгжүүлэх.

14.2. Энэ журамд нэвтрэлтийн туршилт гэж мэдээллийн систем болон нууц мэдээлэлд зөвшөөрөлгүй хандах боломж олгох аюулгүй байдлын сул тал, эмзэг байдлыг илрүүлэх зорилготой туршилтыг ойлгоно.

АРВАН ТАВ. НЭВТРЭЛТИЙН ТУРШИЛТ

15.1. Нэвтрэлтийн туршилтыг банк нь хамгийн багадаа жилд нэг удаа, гуравдагч талаар хамгийн багадаа хоёр жилд нэг удаа хийлгэх бөгөөд туршилтын явцад илэрсэн эмзэг байдлыг цаг алдалгүй шийдвэрлэнэ.

15.2. Нэвтрэлтийн туршилтын явцад санамсаргүйгээр мэдээллийн систем унах, зогсох магадлалтай тул туршилтыг мэдээллийн системийн ачаалал бага үед дараах түвшинд хийнэ. Үүнд:

15.2.1. Нөлөө бүхий мэдээллийн систем;

15.2.2. Харилцаа холбооны дэд бүтцийн болон сүлжээний төхөөрөмж;

15.2.3. DNS үйлчилгээ;

15.2.4. Эцсийн хэрэглэгчийн компьютер, зөөврийн компьютер болон бусад мобайл төхөөрөмж;

15.2.5. Цахим шуудангийн үйлчилгээ;

15.2.6. Өгөгдлийн сангийн систем;

15.2.7. Веб хуудас болон веб мэдээллийн систем;

15.2.8. Мобайл мэдээллийн систем;

15.2.9. Утасгүй сүлжээний систем (Wi-Fi, GSM гэх мэт);

15.2.10. АТМ-ийн систем;

15.2.11. Үйлчилгээ бусниулах халдлага буюу санаатайгаар мэдээллийн системийг хандах боломжгүй болгох, үйл ажиллагаа чиг үүргийг саатуулж улмаар системд нэвтрэх халдлага;

15.2.12. Тархсан үйлчилгээ бусниулах халдлага буюу олон систем, сервер, компьютерыг хамарсан нэг зорилготой үйлчилгээ бусниулах халдлага;

15.2.13. Сошиал инженеринг туршилт буюу аюулгүй байдалд халдаж, системийн алдаа гаргах зорилгоор хувь хүнээс хувийн болон нууц мэдээлэл авах, сэтгэлзүйн дайралт, халдлага хийх үйлдэл.

15.3. Нэвтрэлтийн туршилтыг дараах хандалтын буюу нэвтрэх цэгүүдэд хийнэ. Үүнд:

15.3.1. Интернэтээр шууд хандах боломжтой банкны бүх үйлчилгээ болон мэдээллийн системд дараах хэрэглэгчийн төрлийг ашиглан туршилтыг хийнэ. Үүнд:

15.3.1.1. Бүртгэлгүй гадны хэрэглэгч буюу мэдээллийн системд хандах эрхгүй дурын интернэт хэрэглэгч;

15.3.1.2. Банкны харилцагч буюу мэдээллийн системд интернэтээр хандах эрхтэй банкны харилцагч.

15.3.2. Банкны дотоод сүлжээнд банкны дотоод хэрэглэгч болгон хандах боломжтой мэдээллийн системд дараах хэрэглэгчийн төрлийг ашиглан туршилтыг хийнэ. Үүнд:

15.3.2.1. Банкны ажилтан:

а. Хамгийн түгээмэл ашиглагддаг банкны хэрэглэгчийн эрх;

б. Банкны дотоод администратор хэрэглэгчийн эрх.

15.3.2.2. Банкны зочин:

а. Тодорхой мэдээллийн системд тогтмол хандах эрх бүхий урт хугацааны үйлчилгээ үзүүлэгч болон харилцагч байгууллага;

б. Дотоод сүлжээгээр дамжуулан интернэтэд хандах боломжтой, дотоодын мэдээллийн системд хязгаарлалтай хандах эрх бүхий богино хугацааны банкны зочин.

15.3.3. Салбар сүлжээний хэрэглэгч хандах боломжтой мэдээллийн системд дээрх жагсаалтын банкны ажилтан болон зочны бүх төрлийг ашиглан туршилтыг хийнэ.

15.4. Нэвтрэлтийн туршилтын явцад илэрсэн үр дүнг эрсдэлийн түвшингийн дагуу дараах зэрэглэлээр ангилна. Үүнд:

15.4.1. Онцгой эрсдэл буюу бага түвшний чадвартай этгээд халдлага хийж банкны мэдээллийн системийн хяналт болон удирдлагыг гартаа авах боломжтой.

15.4.2. Шийдвэрлэх шаардлагатай эрсдэл буюу өндөр түвшний чадвартай этгээд халдлага хийж банкны мэдээллийн системийн хяналт болон удирдлагыг гартаа авах боломжтой.

15.4.3. Өндөр зэрэглэлийн эрсдэл буюу интернэтээр дамжуулан мэдээллийн системд хязгаарлалтай хандах боломжтой эсвэл үйлчилгээг бусниулах буюу татгалзуулах боломжтой.

15.4.4. Дунд зэрэглэлийн эрсдэл буюу банкны дотоод сүлжээ болон салбар сүлжээгээр дамжуулан үйлчилгээг бусниулах буюу татгалзуулах боломжтой.

15.4.5. Доод зэрэглэлийн эрсдэл буюу мэдээллийн системийн сул тал, дутагдлыг арилгаж аюулгүй байдлыг хангах арга хэмжээ дутмаг хийгдсэнтэй холбоотой, мэдээллийн системд хохирол учруулах эрсдэл багатай халдлага.

15.5. Нэвтрэлтийн туршилтын явцад илэрсэн үр дүнг дараах дэлгэрэнгүй тайлбарын хамт тайланд тусгана.

15.5.1. Дахин давтагдашгүй бүртгэлийн дугаар;

15.5.2. Илэрсэн үр дүнг илэрхийлэх нэр(SQL injection, Man-in-the-middle гэх мэт);

15.5.3. Эрсдэлийн зэрэглэл буюу энэ журмын 15.4 дахь хэсэгт тодорхойлсон зэрэглэл;

15.5.4. Илэрсэн үр дүнгийн үзүүлэх нөлөө;

15.5.5. Хандалтын цэг буюу IP хаяг;

15.5.6. Хэрэглэгчийн төрөл буюу энэ журмын 15.3 дахь хэсэгт тодорхойлогдсон хэрэглэгчийн төрөл;

15.5.7. Халдлагад өртсөн мэдээллийн систем буюу URL хаяг, IP хаяг, домэйн нэр болон халдлагад өртсөн мэдээллийн систем, үзүүлсэн нөлөөллийн талаар тодорхой тайлбар;

15.5.8. Үр дүнгийн талаар дэлгэрэнгүй тайлбар;

15.5.9. Илэрсэн эмзэг байдлыг арилгах заавар болон зөвлөмж.

АРВАН ЗУРГАА. ХАРИУЦЛАГА

16.1. Монголбанк энэ журмын биелэлтэд хяналт тавьж, журмын заалтыг зөрчсөн этгээдэд Банкны тухай хууль болон бусад холбогдох хууль тогтоомжийн дагуу хариуцлага хүлээлгэнэ.

_____oOo_____