Олон улсын стандарт ISO/IEC 27007

2020 оны 1-р сар

3 дах хэвлэл

Мэдээллийн аюулгүй байдал, кибер аюулгүй байдал болон хувийн нууцлалын хамгаалалт- Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоонд аудит хийх удирдамж

Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

Лавлах дугар

ISO/IEC 27007:2020(E)

© ISO/IEC 2020

ЗОХИОГЧИЙН ЭРХЭЭР ХАМГААЛАГДСАН БАРИМТ БИЧИГ

© ISO/IEC 2020

Бүх эрх хуулиар хамгаалагдсан. Хэрэв урьдчилан бичгээр зөвшөөрөл аваагүй тохиолдолд үүнийг хэрэгжүүлэхдээ хэрвээ өөрөөр заагаагүй, эсхүл шаардаагүй бол энэхүү нийтлэлийн аль ч хэсгийг хуулбарлах, интернет эсвэл дотоод сүлжээнд байршуулах зэрэг цахим болон механик хэлбэрээр ямар ч хэлбэрээр хуулбарлаж, ашиглахыг хориглоно. Зөвшөөрлийг доорх хаягаар ОУСБ-аас эсвэл хүсэлт гаргагчийн улсын ОУСБ-ын гишүүн байгууллагаас авах боломжтой.

ОУСБ-ын зохиогчийн эрхийн газар
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org
Швейцарьт хэвлэв.

Агуулга

Өмнөх үг

ISO (Олон улсын стандартчиллын байгууллага) ба IEC (Олон улсын цахилгаан техникийн комисс) нь дэлхийн стандартчиллын тусгай системийг бүрдүүлдэг. ISO эсвэл IEC-ийн гишүүн үндэсний байгууллагууд нь техникийн үйл ажиллагааны тодорхой салбарыг шийдвэрлэхээр холбогдох байгууллагаас байгуулсан техникийн хороодоор дамжуулан олон улсын стандартыг боловсруулахад оролцдог. ISO болон IEC-ийн техникийн хороод харилцан сонирхсон чиглэлээр хамтран ажилладаг. ISO болон ОУЦХБ-тай хамтран ажилладаг төрийн болон төрийн бус бусад олон улсын байгууллагууд ч уг ажилд оролцдог. Энэхүү баримт бичгийг боловсруулахад ашигласан болон цаашид засвар хийх журмыг ISO/IEC-ийн удирдамжийн 1-р хэсэгт тайлбарласан болно. Ялангуяа төрөл бүрийн төрлийн баримт бичигт шаардагдах өөр өөр шалгууруудыг анхаарч үзэх хэрэгтэй. Энэхүү баримт бичгийг ISO/IEC удирдамжийн 2-р хэсгийн найруулгын дүрмийн дагуу боловсруулсан. (www.iso.org/ удирдамжийг үзнэ үү). Энэхүү баримт бичгийн зарим элемент нь патентын эрхийн сэдэв байж болзошгүйд анхаарлаа хандуулав. ISO болон IEC нь патентын аливаа эрхийг эсвэл бүгдийг нь тодорхойлоход хариуцлага хүлээхгүй. Баримт бичгийг боловсруулах явцад тодорхойлсон аливаа патентын эрхийн талаарх дэлгэрэнгүй мэдээллийг хүлээн авсан патентын мэдүүлгийн танилцуулга ба/эсвэл ISO жагсаалтад (www.iso.org/ patents-ийг үзнэ үү) эсвэл хүлээн авсан патентын мэдүүлгийн IEC жагсаалтад (http://patents.iec.ch). Энэхүү баримт бичигт ашигласан аливаа худалдааны нэр нь хэрэглэгчдэд нийцтэй байх үүднээс өгсөн мэдээлэл бөгөөд баталгаа биш юм. Стандартуудын сайн дурын шинж чанар, тохирлын үнэлгээтэй холбоотой ISO-ийн тусгай нэр томьёо, хэллэгүүдийн утга, түүнчлэн Худалдааны техникийн саад тотгорын ОУСБ-ын Дэлхийн Худалдааны Байгууллагын (ДХБ) зарчмуудыг дагаж мөрдөж байгаа талаарх мэдээллийг www.iso.org/ iso.- ээс үзнэ үү. Энэхүү баримт бичгийг ISO/IEC JTC 1, Мэдээллийн технологи, Дэд хороо SC 27, Мэдээллийн аюулгүй байдал, кибер аюулгүй байдал, хувийн нууцыг хамгаалах хамтарсан техникийн хороо бэлтгэв. Энэхүү гурав дахь хэвлэлээр техникийн хувьд шинэчлэгдсэн хоёр дахь хэвлэлийг (ISO/IEC 27007:2017) цуцалж, орлуулна.

Өмнөх хэвлэлтэй харьцуулахад гол өөрчлөлтүүд нь дараах байдалтай байна:

— баримт бичгийг ISO 19011:2018 стандартад нийцүүлсэн;

— Танилцуулга шинэчлэгдсэн, өргөтгөсөн;

- 5.1-д текстийг бүхэлд нь хассан;

- 5.2.2-т өмнөх d) зүйлийг хассан;

- 5.3-т бичвэрийг бүхэлд нь хассан;

- 5.5.2.2-т өмнөх б) зүйл ба доорх хэсгийг хассан;

— 6.5.2.2-т эхний заалтыг хасч, ТАЙЛБАР-ыг шинэчлэн найруулав.

Энэхүү баримт бичгийн талаархи санал хүсэлт, асуултыг хэрэглэгчийн үндэсний стандартын байгууллагад илгээнэ. A.

Оршил

Мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны (МАБУТ) аудитыг аудитын хэд хэдэн шалгуурын дагуу тусад нь эсвэл хослуулан хийж болно, Үүнд:

- ISO/IEC 27001:2013 стандартад тодорхойлсон шаардлага;
- холбогдох сонирхогч талуудын тодорхойлсон бодлого, шаардлага;
- хууль тогтоомж, зохицуулалтын шаардлага;
- байгууллага эсвэл бусад талуудын тодорхойлсон МАБУТ-ны үйл явц, хяналт;
- Мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны аудитын тодорхой үр дүнг хангахтай холбоотой удирдлагын тогтолцооны төлөвлөгөө(нүүд) (жишээлбэл, МАБУТ-г гүйцэтгэх бий болсон эрсдэл, боломжуудыг шийдвэрлэх төлөвлөгөө, мэдээллийн аюулгүй байдлын зорилтод хүрэх төлөвлөгөө, эрсдэлийг багасгаж даван туулах төлөвлөгөө, төслийн төлөвлөгөө).

Энэхүү баримт бичиг нь төрөл бүрийн үйл ажиллагааны цар хүрээтэй, янз бүрийн хэмжээтэй байгууллагад зориулагдсан бөгөөд үүний дотор томоохон байгууллагуудын аудитын олон хүнтэй багууд, түүнчлэн том эсвэл жижиг хэмжээний байгууллагуудад нэг аудиторууд хийж гүйцэтгэх МАБУТ-ны аудитын удирдамжийг агуулсан болно.

МАБУТ-ны аудитын хөтөлбөрийн хамрах хүрээ, нарийн төвөгтэй байдлыг харгалзан энэхүү удирдамжид тохируулж мөрдөх стой.

Энэхүү баримт бичиг нь мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны (МАБУТ) дотоод аудит (нэг тал) болон байгууллагуудад гаднаас үйлчилгээ үзүүлэгч болон бусад гадны сонирхогч талууд (нөгөө тал)-ын хийсэн мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны аудит хийх тухай юм.

Энэхүү баримт бичиг нь гуравдагч этгээдийн удирдлагын тогтолцооны баталгаажуулалтаас бусад зорилгоор хийгдсэн МАБУТ-ийн хөндлөнгийн аудитад мөн хэрэглэгдэнэ.

ISO/IEC 27006 стандарт нь гуравдагч этгээдийн баталгаажуулалтанд зориулан МАБУТ-ийн аудитын шаардлагууд, аудит хийхэд хэрэглэгдэх нэмэлт зааврыг агуулдаг.

Энэхүү баримт бичгийг ISO 19011:2018 стандартад заасан зааварчилгаатай хамт хэрэглэнэ.

Энэхүү баримт бичиг нь ISO 19011:2018 стандартыг дагасан бүтэцтэй.

ISO 19011:2018 стандарт нь аудитын хөтөлбөрүүдийн удирдлага, удирдлагын тогтолцооны дотоод болон гадны аудитыг хийх, түүнчлэн удирдлагын тогтолцооны аудиторуудын чадамж, үнэлгээний талаарх зааварчилгааг агуулдаг.

Хавсралт А нь ISO/IEC 27001:2013 стандартын 4-10 дугаар зүйлийн шаардлагын зэрэгцээ МАБУТ-ийн аудитын практикт хэрэглээний зааварчилгааг өгдөг.

Мэдээллийн аюулгүй байдал, кибер аюулгүй байдал болон хувийн нууцлалын хамгаалалт - Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоонд аудит хийх удирдамж

1. Хамрах хүрээ

Энэ стандарт нь ISO 19011 стандартад тусгагдсан зааварчилгаанаас гадна мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны (МАБУТ) аудитын хөтөлбөрийг удирдах, аудит хийх, МАБУТ-ийн аудиторуудын ур чадварын талаар зааварчилгааг нэмэлтээр агуулсан болно. Энэхүү стандарт нь МАБУТ-ийн дотоод болон гадаад аудитыг ойлгох, хийж гүйцэтгэх, эсвэл МАБУТ аудитын хөтөлбөрийг удирдах шаардлагатай байгууллагад хэрэглэгдэнэ.

2. Норматив эшлэлүүд

Энэхүү баримт бичигт шаардлагатай дараах баримт бичгүүдийн зарим буюу бүх агуулгыг эшилсэн болно.

Огноотой эшлэлийн хувьд зөвхөн иш татсан хэвлэлийг хэрэглэнэ.

Огноогүй эшлэлийн хувьд эш татсан баримт бичгийн хамгийн сүүлийн хэвлэл (бүх өөрчлөлтийг оруулсан) хамаарна.

ISO 19011:2018, Удирдлагын тогтолцооны аудитын удирдамж

ISO/IEC 27000:2018, Мэдээллийн технологи — Аюулгүй байдлын техникүүд — Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо — Тойм ба үгсийн сан

3. Хэллэг, тодорхойлолтууд

Энэ стандартад ISO 19011 ба ISO/IEC 27000-д дурдсан хэллэг, тодорхойлолтуудыг хэрэглэнэ. ISO ба IEC нь стандарчлалыг хэрэглэх зориулалтаар тодорхойлолтын дараах мэдээллийн санг үүсгэсэн:

— ISO онлайн хайлтын платформ : https:// www .iso .org/ obp

— IEC цахим лавлах: http:// www .electropedia .org/ линкээр тус тус нэвтэрнэ .

4. Аудитын зарчмууд

ISO 19011:2018 –ын 4 –р заалт дах аудитын зарчимыг хэрэглэнэ.

5. Аудитын хөтөлбөрийг удирдах нь

5.1 Ерөнхий зүйл

ISO 19011:2018 –ын 5.1 заалт дах удирдамжийг хэрэглэнэ.

5.2 Аудитын хөтөлбөрийн зорилгыг тодорхойлох

5.2.1 ISO 19011:2018 –ын 5.2 заалт дах удирдамжаас гадна 5.2.2 дах зааварчилгааг хэрэглэнэ.

5.2.2 Мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны аудитын хөтөлбөрийн зорилтыг тодорхойлох онцлог зүйлүүдэд :

a) мэдээллийн аюулгүй байдлын шаардлагыг таньж тогтоосон байдал;

b) ISO/IEC 27001-ын шаардлагууд;

c) Мэдээллийн аюулгүй байдлын үйл явдал, будлиан гарсан байдал, МАБУТ-ны үр нөлөөнд тусгагдсан аудит хийлгүүлж буй байгууллагын гүйцэтгэлийн түвшин

Тэмдэглэл: Аудитын хяналт шинжилгээний гүйцэтгэл, хэмжилт, дүгнэлт болон үнэлгээний талаарх бусад мэдээллийг ISO/IEC 27004- аас үзэх

d) Оролцогч талууд буюу аудит хийлгэж буй этгээд болон ба түүний үйлчлүүлэгч)-ийн МАБ-ын эрсдэлүүд хамаарна.

Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоонд зориулагдсан аудитын хөтөлбөрийн жишээ нь дараах зорилтуудыг агуулна . Үүнд:

— холбогдох эрх зүйн болон гэрээний шаардлагуудаас гадна аюулгүй байдлын үр дагавар бүхий бусад шаардлагуудын нийцлийг харуулах ;

— аудит хийлгэж буй этгээдийн эрсдэлийг удирдах чадварт итгэх, дэмжих;

— мэдээллийн аюулгүй байдлын эрсдэл, боломжуудыг шийдвэрлэх арга хэмжээний үр нөлөөг үнэлэх.

5.3 Аудитын хөтөлбөрийн эрсдэл, боломжийг тодорхойлох, үнэлэх

5.3.1 ISO 19011 : 2018 стандартын 5.3 заалт дах зааврыг хэрэглэнэ.

5.3.2 Мэдээллийн аюулгүй байдал, нууцлалыг хангах арга хэмжээг тогтоохдоо аудит хийлгэж буй байгууллага болон холбогдох талуудын бусад шаардлагыг харгалзана. Бусад талын шаардлагад холбогдох эрх зүйн болон гэрээний шаардлагыг багтааж болно.

5.4 Аудитын хөтөлбөрийг боловсруулах

5.4.1 Аудитын хөтөлбөрийг удирдаж буй хувь хүн(хүмүүс)-ий үүрэг, хариуцлага ISO 19011:2018 стандартын 5.4.1-т заасан удирдамжийг мөрдөнө. Түүнчлэн 5.4.1.2-т заасан зааварчилгааг дагаж мөрдөнө.

5.4.2 Аудитын хөтөлбөрийг удирдаж буй хувь хүн(хүмүүс)-ийн ур чадвар.

ISO 19011:2018 стандартын 5.4.2-ын удирдамжийг мөрдөнө.

5.4.3 Аудитын хөтөлбөрийн цар хүрээг тогтоох

5.4.3.1 ISO 19011:2018 стандартын 5.4.3-ын удирдамжийг мөрдөнө. Түүнчлэн 5.4.3.2-т заасан зааварчилгааг дагаж мөрдөнө.

5.4.3.2 Аудитын хөтөлбөрийн хүрээ нь дараах зүйлийг агуулж болно. Үүнд:

a) Дараах зүйлийг багтаасан МАБУТ-ны хэмжээ:

1. Байгууллагын хяналтанд ажиллаж буй болон мэдээллийн аюулгүй байдлын удирдлагын системд нэгдмэл хамаарал бүхий талууд ба гүйцэтгэгчийн нийт ажиллагсадын тоо;

2. Мэдээллийн системийн тоо;

3. Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоонд хамрагдсан сайтуудын тоо;

b) МАБУТ-ны хамрах хүрээн дэх сайтуудын ялгааг харгалзсан МАБУТ-ны нарийн төвөгтэй байдал (үйл явц, үйл ажиллагааны тоо, чухал байдлыг оруулаад);

c) бизнестэй холбоотой МАБУТ-д тодорхойлсон мэдээллийн аюулгүй байдлын эрсдлийн ач холбогдол;

d) МАБУТ-ны төлөвлөлтөөр тодорхойлсон эрсдэл, боломжуудын ач холбогдол;

e) МАБУТ-ны хүрээнд мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжийг хадгалахын ач холбогдол;

f) аудит хийлгэж байгаа мэдээллийн системд ашигласан нарийн төвөгтэй мэдээллийн технологийн байдал,

g) ижил төстэй сайтуудын тоо.

Аудитын хөтөлбөрийг боловсруулахад, мэдээллийн аюулгүй байдлын эрсдэлд үндэслэн илүү нарийвчлан авч үзэх шаардлагатай, МАБУТ-ны хэрэглээний хүрээтэй холбоотой, бизнесийн шаардлагуудын ач холбогдлыг тогтооход анхаарлаа хандуулах нь зүйтэй .

ТАЙЛБАР: Аудитын хугацааг тодорхойлох талаар нэмэлт мэдээллийг ISO/IEC 27006 стандартаас олж болно. Олон талбарт түүвэрлэлтийн талаарх дэлгэрэнгүй мэдээллийг ISO/IEC 27006 стандарт болон Олон улсын итгэмжлэлийн форум (IAF MD1, лавлагаа [11]-ыг үзнэ үү)-ын заавал дагаж мөрдөх баримт бичиг 1-ээс олж болно.

ISO/IEC 27006 болон IAF MD 1-д агуулагдсан мэдээлэл нь зөвхөн баталгаажуулалтын аудиттай холбоотой.

5.4.4 Аудитын хөтөлбөрийн нөөцийг тодорхойлох

5.4.4.1 ISO 19011:2018, 5.4.4-ийн удирдамжийг мөрдөнө. Мөн 5.4.4.2-т заасан удирдамжийг дагаж мөрдөнө.

5.4.4.2 Ялангуяа аудит хийгдэж буй этгээдэд хамаарах болон аудитын хөтөлбөрийн зорилгод хамаарах бүхий л чухал эрсдэлийн хувьд мэдээллийн аюулгүй байдлын эрсдэл, МАБУТ-тай холбоотой эрсдэл, боломжуудыг шийдвэрлэх арга хэмжээний үр нөлөөг шалгах хангалттай цагийг МАБУТ-ийн аудиторуудад хуваарилах ёстой.

5.5 Аудитын хөтөлбөрийг хэрэгжүүлэх

5.5.1 Ерөнхий зүйл

ISO 19011:2018, 5.5.1-ийн удирдамжийг мөрдөнө.

5.5.2 Тухайн аудитын зорилго, хамрах хүрээ ба шалгуурыг тогтоох

5.5.2.1 ISO 19011:2018, 5.5.2-ын удирдамжийг мөрдөнө. Мөн 5.5.2.2-т заасан зааврыг хэрэглэнэ.

5.5.2.2 Аудитын зорилгод дараах зүйлс багтаж болно:

a) МАБУТ нь МАБ-ын шаардлагыг хангалттай таньж тогтоосон эсэх тухай дүгнэлт
b) Мэдээллийн аюулгүй байдлын хяналт нь МАБУТ-ийн шаардлага, журамтай нийцэж байгаа эсэхийг тодорхойлсон байдал

Аудитын хамрах хүрээ нь мэдээллийн аюулгүй байдлын эрсдэл, холбогдох бусад эрсдэл, боломжуудыг анхааран авч үзнэ.

Дараах зүйлүүдийг аудитын шалгуур гэж үзэж, тохирлыг тодорхойлох лавлагаа болгон ашиглаж болно.

a) мэдээллийн аюулгүй байдлын бодлого, зорилт,аудитлад хамрагдсан этгээдийн баталсан бодлого, журам;
b) аудит хийлгэж буйтай холбоотой бусад шаардлагууд болон гэрээнд заасан шаардлага;

c) аудитад хамрагдсан этгээдийн эрсдэлийг давах үйл явц, мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явц, мэдээллийн аюулгүй байдлын эрсдлийн шалгуур үзүүлэлт;
d) Хэрэглэх мэдэгдэл, аливаа салбарын онцлог болон бусад шаардлагатай хяналтыг тодорхойлох, оруулахгүй байх үндэслэл, тэдгээрийг хэрэгжүүлж байгаа эсэх, ISO/IEC 27001:2013-ийн хяналтыг хасах үндэслэл, Хавсралт А дахь;
e) эрсдэлийг зохих ёсоор тодорхойлох хяналтын хэрэгслэлийн тодорхойлолт;
f) МАБУТ-ны үр өгөөж ба мэдээллийн аюулгүй байдлын гүйцэтгэлийг хэмжих шинжилгээ хийх, үнэлэх арга, шалгуурууд;
g) хэрэглэгчийн тогтоосон мэдээллийн аюулгүй байдлын шаардлагууд;
h) ханган нийлүүлэгч болон аутсорсингийн тавьсан мэдээллийн аюулгүй байдлын шаардлага.

5.5.3 Аудитын аргуудыг сонгох, тодорхойлох

5.5.3.1 ISO 19011:2018, 5.5.3-ын удирдамжийг мөрдөнө. Мөн 5.5.3.2-т заасан зааврыг хэрэглэнэ.

5.5.3.2 Хэрэв хамтарсан аудит хийсэн бол холбогдох талуудын хооронд мэдээлэл задруулахад онцгой анхаарал хандуулж аудит эхлэхээс өмнө энэ талаар бүх сонирхогч талуудтай тохиролцох шаардлагатай.

5.5.4 Аудитын багийг сонгох, тодорхойлох

5.5.4.1 ISO 19011:2018, 5.5.4-ийн удирдамжийг мөрдөнө. Нэмэлтээр 5.5.4.2-т заасан зааврыг хэрэглэнэ.

5.5.4.2 Аудитын ерөнхий багийн ур чадвар нь дараах мэдлэг, ойлголтыг хангалттай агуулсан байх ёстой:

a) мэдээллийн аюулгүй байдлын эрсдэлийн удирдлага нь аудитлагдаж буй этгээдийн ашигласан аргуудыг үнэлэхэд хангалттай байх

b) мэдээллийн аюулгүй байдал ба түүний удирдлага нь МАБУТ-ийн хяналтыг тодорхойлох, төлөвлөх, хэрэгжүүлэх, засвар үйлчилгээ, үр нөлөөг үнэлэхэд хангалттай байх

5.5.5 Ганцаарчилсан аудитын хариуцлагыг аудитын багийн ахлагчид даалгах

ISO 19011:2018, 5.5.5-ын удирдамжийг мөрдөнө.

5.5.6 Аудитын хөтөлбөрийн үр дүнг удирдах

ISO 19011:2018, 5.5.6-ын удирдамжийг мөрдөнө.

5.5.7 Аудитын хөтөлбөрийн бүртгэлийг удирдах, хөтлөх

ISO 19011:2018, 5.5.7-гийн удирдамжийг мөрдөнө.

5.6 Аудитын хөтөлбөрт хяналт шинжилгээ хийх

ISO 19011:2018, 5.6-гийн удирдамжийг мөрдөнө.

5.7 Аудитын хөтөлбөрийг хянаж, сайжруулах

ISO 19011:2018, 5.7-гийн удирдамжийг мөрдөнө.

6. Аудит хийх

6.1 Ерөнхий зүйл

ISO 19011:2018, 6.1-ийн удирдамжийг мөрдөнө.

6.2 Аудитыг эхлүүлэх

6.2.1 Ерөнхий нөхцөл

ISO 19011:2018, 6.2.1-ийн удирдамжийг мөрдөнө.

6.2.2 Аудитад хамрагдагчтай холбоо тогтоох

6.2.2.1 ISO 19011:2018, 6.2.2-ын удирдамжийг мөрдөнө. Мөн 6.2.2.2 дах зааврыг ашиглана.

6.2.2.2 Шаардлагатай тохиолдолд аудиторууд баримтжуулсан мэдээлэл эсвэл аудитын үйл ажиллагаанд шаардлагатай бусад мэдээлэл (нууц, эмзэг мэдээлэл багтах ба үүгээр хязгаарлагдахгүй)-д хандахдаа зохих төвшний аюулгүй байдлын зөвшөөрөл авсан эсэхэд анхаарал хандуулах хэрэгтэй.

6.2.3 Аудит хийж гүйцэтгэх боломжийг тодорхойлох

6.2.3.1 ISO 19011:2018, 6.2.3-ын удирдамжийг мөрдөнө.Мөн 6.2.3.2 дах зааврыг ашиглана.

6.2.3.2 Аудит эхлэхийн өмнө аудитын баг, хянан үзэх боломжгүй, жишээлбэл хувь хүний нууцын эсвэл бусад нууц / чухал мэдээллийг агуулсан нотлох баримт байгаа эсэхийг аудит хийлгэж буй этгээдээс асууна. Аудитын хөтөлбөрийг удирдагч нь аудитын нотлох баримт байхгүй тохиолдолд МАБУТ-д хангалттай аудит хийх боломжтой эсэхийг тодорхойлно.

Хэрэв дүгнэлт нь тухайн аудитын нотолгоог хянахгүйгээр МАБУТ-д аудит хийх боломжгүй гэж үзвэл аудитын хөтөлбөрийн удирдагч нь зохих хандалтын зохицуулалт хийх эсвэл аудитлагдагч эсхүл аудиторын санал болгосон өөр арга хэрэгслээр хандах хүртэл аудит хийх боломжгүй гэдгийг аудитлагдагчид мэдэгдэнэ.

Хэрэв аудит үргэлжилэхээр бол аудитын төлөвлөгөөнд аливаа хандалтын хязгаарлалтыг харгалзан үзэх шаардлагатай.

6.3 Аудитын үйл ажиллагаанд бэлтгэх

6.3.1 Баримтжуулсан мэдээлэлд хяналт хийх

ISO 19011:2018, 6.3.1-ийн удирдамжийг мөрдөнө.

6.3.2 Аудитын төлөвлөлт

6.3.2.1 ISO 19011:2018, 6.3.2-ын удирдамжийг мөрдөнө.Мөн 6.3.2.2 дах зааврыг ашиглана.

6.3.2.2 Аудитын багийн ахлагч аудитын багийн гишүүд байлцсанаас шалтгаалж буй этгээдэд учирч болзошгүй эрсдэлийг мэдэж байх ёстой.

Аудитын баг байгаа нь мэдээллийн аюулгүй байдалд нөлөөлж, аудит хийлгэгчийн мэдээлэлд нэмэлт эрсдлийн эх үүсвэр үүсгэж болно, жишээлбэл. нууц эсвэл эмзэг бүртгэл эсвэл системийн дэд бүтэц (жишээлбэл, санамсаргүйгээр устгах, мэдээллийг зөвшөөрөлгүй задруулах, мэдээллийг санамсаргүй өөрчлөх).

6.3.3 Аудитын багт ажил хуваарилах оноох

ISO 19011:2018, 6.3.3-ын удирдамжийг мөрдөнө.

6.3.4 Аудит хийхэд зориулж баримтжуулсан мэдээллийг бэлтгэх

6.3.4.1 ISO 19011:2018, 6.3.4-ийн удирдамжийг мөрдөнө.Мөн 6.3.4.2 дах зааврыг ашиглана

6.3.4.2 Аудитын багийн ахлагч нь аудитын ажлын бүх баримт бичгийг зохих ёсоор ангилж, тухайн ангиллын дагуу зохицуулсан эсэхийг шалгах ёстой.

6.4 Аудитын үйл ажиллагаа явуулах

6.4.1 Ерөнхий зүйл

ISO 19011:2018, 6.4.1-ийн удирдамжийг мөрдөнө

6.4.2 Хөтөч, ажиглагчийн үүрэг, хариуцлагыг хуваарилах

ISO 19011:2018, 6.4.2-ын удирдамжийг мөрдөнө

6.4.3 Нээлттэй уулзалт хийх

ISO 19011:2018, 6.4.3-ын удирдамжийг мөрдөнө

6.4.4 Аудитын явцад мэдээлэл солилцох

ISO 19011:2018, 6.4.4-ийн удирдамжийг мөрдөнө

6.4.5 Мэдээллийн хүртээмж ба олдоцод аудит хийх

6.4.5.1 ISO 19011:2018, 6.4.5-ын удирдамжийг мөрдөнө. Мөн 6.4.5.2 дах зааврыг ашиглана

6.4.5.2 Хэрэв аудитын багт ангиллын болон нууцлалын шалтгаанаар аудитын нотлох баримт байхгүй бол энэ нь аудитын үр дүн, хийсэн дүгнэлтэд хэр зэрэг нөлөөлж байгааг ахлах аудитор тодорхойлж мөн дутуу гэх нотлох баримтын нууцлалыг алдагдуулахгүйгээр аудитын тайланд тусгана.

6.4.6 Аудит хийх үеийн баримт бичгийн мэдээллийг шалгах

6.4.6.1 ISO 19011:2018, 6.4.6-ын удирдамжийг мөрдөнө. Мөн 6.4.6.2 дах зааврыг ашиглана

6.4.6.2 Аудиторууд нь баримтжуулсан мэдээллийг аудитын шалгуурууд ба аудитын хамрах хүрээтэй холбоотой эсэхийг шалгаж, аудитын шалгуурын шаардлагад МАБУТ нийцэж байгаа эсэхийг баталгаажуулна.

МАБУТ-ны аудиторууд нь аудитын хүрээнд хянагдах эрсдлийн үнэлгээ, эрсдлийг бууруулах ажлын үр дүнг баталгаажуулан цаашид мэдээллийн аюулгүй байдлын бодлого, зорилтуудад тусган мөрдөж болно.

Тайлбар: Хавсралт А нь МАБУТ-ны аудитын практикт, холбогдох баримтжуулсан мэдээллийг ашиглан МАБУТ-нд аудит хэрхэн хийх зааврааар хангадаг.

6.4.7 Мэдээлэл цуглуулах, баталгаажуулах

6.4.7.1 ISO 19011:2018, 6.4.7-ын удирдамжийг мөрдөнө. Мөн 6.4.7.2 дах зааврыг ашиглана

6.4.7.2 Аудитын явцад холбогдох мэдээллийг цуглуулах боломжит аргууд нь:

а) баримтжуулсан мэдээллийн тойм(Компьютерийн log бүртгэл, тохиргооны өгөгдлийг оролцуулан);

б) мэдээлэл боловсруулах байгууламжид зочлох;

в) МАБУТ-ны процесс болон холбогдох хяналтыг ажиглах;

г) аудитын автоматжуулсан хэрэгслийг ашиглах.

Тайлбар 1: Хавсралт А нь МАБУТ-ийн үйл явцыг хэрхэн аудит хийх талаар заавар өгдөг.

Тайлбар 2: ISO / IEC TS 27008 нь мэдээллийн аюулгүй байдлын хяналтыг хэрхэн үнэлэх талаар нэмэлт заавар өгдөг.

МАБУТ-ны аудитын багийн гишүүд нь аудитын үйлчлүүлэгч, аудитын баг болон аудит хийлгэж буй этгээдийн дунд гэрээний дагуу аудит хийлгэж буй этгээдийн хүлээн авсан бүх мэдээлэлд зохих есоор хандах естой

6.4.8 Аудитын үед олдсон үр дүнг боловсруулах
ISO 19011:2018, 6.4.8-ын удирдамжийг мөрдөнө.
6.4.9 Аудитын дүгнэлт гаргах
ISO 19011:2018, 6.4.9-ийн удирдамжийг мөрдөнө.
6.4.10 Хаалтын уулзалт хийх
ISO 19011:2018, 6.4.10-ын удирдамжийг мөрдөнө.

6.5 Аудитын тайланг бэлтгэх, хүргэх
6.5.1 Аудитын тайланг бэлтгэх
ISO 19011:2018, 6.5.1-ийн удирдамжийг мөрдөнө.
6.5.2 Аудитын тайланг хүргэх

6.5.2.1 ISO 19011:2018, 6.5.2-ын удирдамжийг мөрдөнө. Мөн 6.5.2.2 дах зааврыг ашиглана
6.5.2.2 Тайлбар
ТАЙЛБАР: Аудитын тайланг түгээхдээ зохих шифрлэлт бүхий цахим хэрэгслийг ашиглах нь нууцлалын шаардлагыг хангах боломжит арга хэрэгсэл юм.

6.6 Аудитыг дуусгах
ISO 19011:2018, 6.6-ын удирдамжийг мөрдөнө.

6.7 Аудитын дараах үйл ажиллагаа
ISO 19011:2018, 6.7-ийн удирдамжийг мөрдөнө.

7 Аудиторын ур чадвар, үнэлгээ

7.1 Ерөнхий нөхцөл
ISO 19011:2018, 7.1-ийн удирдамжийг мөрдөнө.
7.2 Аудиторын ур чадварыг тодорхойлох
7.2.1 Ерөнхий нөхцөл

7.2.1.1 ISO 19011:2018, 7.2.1-ийн удирдамжийг мөрдөнө. Мөн 7.2.1.2 дах зааврыг ашиглана

7.2.1.2 МАБУТ-ны аудиторын зохих мэдлэг, ур чадварын төвшний талаарх шийдвэр гаргахдаа дараах зүйлийг анхаарч үзсэн байх: Үүнд:

a) МАБУТ-ны нарийн төвөгтэй байдал (жишээ нь, МАБУТ доторх мэдээллийн системийн онцгой байдал, МАБУТ-ийн эрсдлийн үнэлгээний үр дүн);
b) МАБУТ-ны хүрээнд гүйцэтгэсэн бизнесийн үйл ажиллагааны төрөл(үүд);
c) МАБУТ-ны бүрэлдэхүүн хэсгүүдийг хэрэгжүүлэхэд ашигласан олон төрлийн технологи, түүний цар хүрээ (хэрэгжүүлсэн хяналт, баримтжуулсан мэдээлэл ба/эсвэл үйл явцын хяналт, оролцсон технологийн платформ, шийдэл гэх мэт.);
d) өмнө нь үзүүлсэн МАБУТ-ны гүйцэтгэл;
e) МАБУТ-ны хүрээнд ашигласан аутсорсинг болон гадаад талын зохицуулалтын хэмжээ;
f) аудитын хөтөлбөртэй холбогдох стандарт, эрх зүйн болон бусад шаардлагууд.

7.2.2 Хувийн зан чанар

ISO 19011:2018, 7.2.2-ын удирдамжийг мөрдөнө.

7.2.3 Мэдлэг, ур чадвар

7.2.3.1 Ерөнхий нөхцөл

ISO 19011:2018, 7.2.3.1-ийн удирдамжийг мөрдөнө.

7.2.3.2 Удирдлагын тогтолцооны аудиторуудын ерөнхий мэдлэг,ур чадвар

ISO 19011:2018, 7.2.3.2-ын удирдамжийг мөрдөнө.

7.2.3.3 Аудиторын сахилга дэг журам ба салбарын онцлог шаардсан ур чадвар

7.2.3.3.1 ISO 19011:2018, 7.2.3.3-ын удирдамжийг мөрдөнө. Мөн 7.2.3.3.2 дах зааврыг ашиглана

7.2.3.3.2 МАБУТ-ны аудиторууд нь холбогдох бизнесийн шаардлагыг ойлгох чадвартай байна.

7.2.3.4 Аудитын багийн ахлагчийн ерөнхий чадвар

ISO 19011:2018, 7.2.3.4-ийн удирдамжийг мөрдөнө.

7.2.3.5 Олон чиглэлээр аудит хийх мэдлэг,чадвар

ISO 19011:2018, 7.2.3.5-ын удирдамжийг мөрдөнө.

7.2.4 Аудиторын ур чадварыг эзэмших

7.2.4.1 ISO 19011:2018,7.2.4-ийн удирдамжийг мөрдөнө. Мөн 7.2.4.2 дах зааврыг ашиглана.

7.2.4.2 МАБУТ-ны аудиторуудын мэдээллийн технологи, мэдээллийн аюулгүй байдлын талаархи мэдлэг, ур чадвар нь тухайлбал холбогдох гэрчилгээгээр нотлогдсон байх шаардлагатай. (жишээлбэл, ISO/IEC 17024-д итгэмжлэгдсэн).

МАБУТ-ийн бие даасан аудиторууд нь өөрийн ажлын туршлагаар МАБУТ салбарын мэдлэг, ур чадварын хөгжилд хувь нэмэр оруулсан байна.

ТАЙЛБАР: МАБУТ-ийн аудиторуудад зориулсан гэрчилгээ олгох тухай нэмэлт мэдээллийг ISO/IEC 27006-аас олж болно.

7.2.5 Аудитын багийн ахлагчийн ур чадвар эзэмших

ISO 19011:2018, 7.2.5-ын удирдамжийг мөрдөнө.

7.3 Аудиторын үнэлгээний шалгуурыг тогтоох

ISO 19011:2018, 7.3-ын удирдамжийг мөрдөнө.

7.4 Аудиторын үнэлгээний зохистой аргыг сонгох

ISO 19011:2018, 7.4.-ийн удирдамжийг мөрдөнө.

7.5 Аудиторын үнэлгээ хийх

ISO 19011:2018, 7.5-ын удирдамжийг мөрдөнө.

7.6 Аудиторы ур чадвартай байлгах, байнга сайжруулах

ISO 19011:2018,7.6-ын удирдамжийг мөрдөнө.

Хавсралт А

(мэдээллийн чанартай)

Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоонд аудит хийх удирдамж

А.1 Тойм

Энэхүү хавсралтаар ISO/IEC 27001-стандартыг нэвтрүүлэх гэж буй аливаа байгууллагад зориулан түүний Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоонд -(МАБУТ) (Information security management systems- ISMS) хэрхэн аудит хийх тухай ерөнхий удирдамжийг өгч байна. Тухайн байгууллагын хэмжээ, ямар чиглэлийн үйл ажиллагаа эрхэлдэгээс үл хамааран бүгдэд нь ийм МАБУТ-д аудит хийх зорилго агуулсан тул уг удирдамж нь ерөнхийлсэн шинж чанартай юм. Энэхүү удирдамж нь МАБУТ-д аудит хийж буй дотоод болон гадаад аудиторуудад зориулагдсан болно.

ТАЙЛБАР: ISO/IEC 27003 нь ISO/IEC 27001 стандартын дагуу МАБУТ-ийг хэрхэн хэрэгжүүлэх болон үйл ажиллагааны талаарх зааварчилгааг өгдөг.

А.2 Ерөнхий

А.2.1 Аудитын зорилго, хамрах хүрээ, шалгуур үзүүлэлт, аудитын нотлох баримт

Аудитын үйл ажиллагааны явцад тухайн аудитын зорилго, хамрах хүрээ, шалгуурт хамаарах мэдээлэл, түүний дотор чиг үүрэг, үйл ажиллагаа, үйл явц хоорондын холбоост (интерфейст) хамаарах мэдээллийг зохих түүврийн аргаар олж авч, баталгаажуулах ёстой. Зөвхөн баталгаажуулах боломжтой мэдээллийг аудитын нотлох баримт болгон хүлээн зөвшөөрбөл зохино. Аудитын дүгнэлтэд хүргэх аудитын нотлох баримтыг бүртгэлийн тайланд авах ёстой.

Мэдээлэл олж авах арга нь дараахь зүйлийг агуулна.

— ярилцлага;

— ажиглалт;

— бүртгэлийн тайланг оролцуулан баримт бичгүүдийг хянан шалгах.

А.2.2 МАБУТ-д аудит хийх стратеги

ISO/IEC 27001:2013 стандартын зарим дэд заалтууд хоорондоо нягт уялдаатай байдаг бөгөөд бодит байдал дээр аудит хийхэд хамгийн сайн тохирдог. Холбогдох жишээг Хүснэгт

A.2-оос үзнэ үү. Жишээ нь ISO/IEC 27001:2013:6.1.3 болон 8.3, мөн 6.2, 5.1, 5.2, 5.3, 7.1, 7.4, 7.5, 9.1, 9.3, ба 10.2 нь эдгээр дэд зүйлүүдийг тэдгээрт хамаатай болон холбогдох дэд зүйлүүдэд аудит хийхэд ашиглах нь зүйтэй юм.

ISO/IEC 27001:2013, 7.5 нь баримтжуулсан мэдээлэлд тавигдах шаардлагыг тусгасан болно. Хүснэгт A.2, A.4.5-д тайлбарласнаар аудиторууд баримтжуулсан мэдээллийг шалгах бүрд ISO/IEC 27001:2013, 7.5-ын шаардлагад нийцэж байгаа эсэхийг баталгаажуулах боломжийг олгодог. Үүнийг хэрхэн хийх зааврыг Хүснэгт A.2, A.4.5-д үзүүлсэн. Хүснэгтэд "баримтжуулсан мэдээлэл" гарч ирэх бүрт баримтжуулсан мэдээлэлд тавигдах шаардлагыг давтахгүй.

A.2.3 Аудитын болон баримтжуулсан мэдээлэл

Аудитын үйл ажиллагаа нь баримтжуулсан мэдээллийг агуулж болно. Тухайлбал:

a) ISO/IEC 27001 стандартын баримтжуулсан мэдээллийн шаардлагын мэдэгдлийг аудитын шалгуур болгон ашиглаж болно;

b) ISO/IEC 27001:2013, 7.5.1-д заасан баримтжуулсан мэдээлэл;

c) ISO/IEC 27001:2013 стандартын 7.5.1-ийн МАБУТ -ийг үр дүнтэй ажиллахад шаардлагатай гэж байгууллагаас тодорхойлсон баримтжуулсан мэдээлэл.

Аудиторуудын ярилцлага, ажиглалт хийх, баримт бичгүүдийг шалгах замаар олж авах боломжтой A.2.3 b)-аас өөр бусад аудитын нотлох баримт байж болно. ISO/IEC 27001-тэй холбоотой баримтжуулсан мэдээллийн дэлгэрэнгүй хэлэлцүүлгийг A.3-аас үзэж болно.

A.3 Баримтжуулсан мэдээлэлд тавигдах ISO/IEC 27001 стандартын шаардлагын тухай заавар

A.3.1 Үндэслэл

Нийцэж байгаа эсэхийг нь нотлох баримт болгон авах баримтжуулсан мэдээллийг хүсэхдээ аудиторууд дараах зүйлд болгоомжтой хандах хэрэгтэй. Үүнд:

a) Хүснэгт A.1-д заасан баримтжуулсан мэдээлэлд тавигдах 16 тодорхой шаардлага, түүний дотор Хэрэглэх боломжтой байдлын мэдэгдэл;

b) нэмэлт шаардлагууд нь дараах утгатай:

1) дээр дурдсан баримтжуулсан мэдээллээс тохирлын нотолгоог олно гэж хүлээх нь үндэслэлтэй байх;

2) баримтжуулсан мэдээлэлд тодорхой ил болон далд утгатай шаардлага байхгүй.

Хүснэгт A.1 — ISO/IEC 27001 стандартын баримтжуулсан мэдээлэлд тавигдах шаардлага

Баримтжуулсан мэдээлэлд тавигдах шаардлага	**ISO/IEC 27001:2013** **Дэд зүйл**
МАБУТ-ийн хамрах хүрээ	4.3
Мэдээллийн аюулгүй байдлын бодлого	5.2
Мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явц	6.1.2
Мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх үйл явц	6.1.3
Хэрэглэх тухай мэдэгдэл	6.1.3 d)
Мэдээллийн аюулгүй байдлын зорилтууд	6.2
Чадамжтай байдлын нотолгоо	7.2 d)
МАБУТ-ийг үр дүнтэй болгоход шаардлагатай гэж байгууллагаас тодорхойлсон баримтжуулсан мэдээлэл	7.5.1 b)
Үйл ажиллагааны төлөвлөлт, хяналт	8.1
Мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үр дүн	8.2
Мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэсэн үр дүн	8.3
Хяналт, хэмжилтийн үр дүнгийн нотлох баримт	9.1

Аудитын хөтөлбөр(үүд) болон аудитын үр дүнгийн нотлох баримт	9.2 g)
Удирдлагын хянан шалгалтын үр дүнгийн нотолгоо	9.3
Үл тохирлын шинж чанар болон дараа нь авсан аливаа арга хэмжээний нотолгоо	10.1 f)
Аливаа засч залруулах арга хэмжээний үр дүнгийн нотолгоо	10.1 g)

ТАЙЛБАР: Аудитын тодорхойлолтод энэ нь баримтжуулсан үйл явц гэж заасан байдаг тул аудитор ISO/IEC 27001:2013, 9.2-ын шаардлагыг биелүүлснээр аудитын үйл явцыг баримтжуулсан гэж итгэж болно.

A.3.2 Баримтжуулсан мэдээллийн далд шаардлагын жишээ

A.3.1 b) 1)-ын жишээ болгон, ISO/IEC 27001:2013, 6.1.2-ыг авч үзье. Үүнд байгууллагууд "мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явцын талаарх баримтжуулсан мэдээллийг хадгалах" шаардлагатай. Өмнөх шаардлагууд [ISO/IEC 27001:2013, 6.1.2 a)-д)] бүгд эрсдэлийн үнэлгээний үйл явцад хамаардаг. Иймд эрсдэлийн үнэлгээний үйл явцтай холбоотой шаардлагатай баримтжуулсан мэдээллээс эдгээр шаардлагад нийцэж байгаа нотолгоог олно гэж найдах тодорхой үндэслэл бий.

A.3.3 Баримтжуулсан мэдээлэлд ил болон далд шаардлага байхгүйн жишээ

A.3.1 b) 2)-ын жишээ болгон ISO/IEC 27001:2013, 4.1.1-ийг авч үзье. Гадаад, дотоод асуудалтай холбоотой баримтжуулсан мэдээлэл байх шаардлагагүй. Тиймээс аудиторууд үүнийг шалгаж үзэхийг шаардах ёсгүй. Гэсэн хэдий ч байгууллага эдгээр асуудлыг тодорхойлсон гэдгээ нотлохгүй байх нь ISO/IEC 27001:2013, 4.1.1-д нийцэхгүй байна. Гэсэн хэдий ч байгууллага нь нийцлийг хэрхэн харуулахаа сонгох үүрэгтэй. Үүнийг дээд удирдлага нь тайлбарлаж болно (өөрөөр хэлбэл хэн нэгэн мэддэг хүн нь) эсвэл тухайн сэдвийг хэлэлцсэн хурлын тэмдэглэл байж болно.

Үүнийг албан ёсны тохиргооны менежментэд байгаа баримтжуулсан мэдээллээр нотлох эсвэл өөр аргаар нотлох боломжтой. Үнэн хэрэгтээ, МАБУТ-ийн баримтжуулсан мэдээллээр нотлох баримтууд тараагдах магадлалтай. Жишээлбэл, ISO/IEC 27001:2013, 4.1.1-ийн зорилго нь МАБУТ -ын нөхцөлийг ойлгоход байгууллагад туслах явдал юм. Энэ

нөхцөл байдал нь МАБУТ -д, ялангуяа хамрах хүрээ, бодлогыг тодорхойлох, эрсдэлийн үнэлгээ, эрсдэлийн асуудлыг шийдвэрлэх үйл явцын гүйцэтгэлд давамгайлж байна. Хэрэв байгууллага ISO/IEC 27001:2013, 4.1.1-ийн шаардлагыг хангасан бол гадаад болон дотоод асуудлын талаарх мэдлэгээ МАБУТ -ын эдгээр бусад салбарт ашиглах, түүний хэрэглээ тууштай байх бөгөөд эдгээр бусад чиглэлийн тухай баримтжуулсан мэдээлэлд нийцэж байгааг нотлох баримт байх болно.

A.4 Хэрэглэх боломжтой байдлын мэдэгдэл

Хэрэглэх боломжтой байдлын мэдэгдэл (ХББМ) (The Statement of Applicability-SoA) нь анхааралвал зохих өөр нэг талбар юм.

ХББМ нь эрсдэл хүлээх шалгуурыг хангахын тулд мэдээллийн аюулгүй байдлын эрсдэлийн нөхцөл байдлыг өөрчлөхөд зайлшгүй шаардлагатай гэж тодорхойлсон эрсдэлийг шийдвэрлэх үйл явцын үр дүнд байгууллага нь өөрт байгаа [ISO/IEC 27001:2013, 6.1.3 c)] бүх шаардлагатай хяналтуудыг агуулсан байх ёстой. Хэрэгцээт бүх хяналт нь байгууллагын өөрийн нөхцөл шаардлага юм. Шаардлагатай хяналтууд нь ISO/IEC 27001:2013 -ын Хавсралт А-д заасан хяналт байж болох ч заавал дагаж мөрдөх албагүй. Эдгээр хяналт нь бусад стандарт (жишээ нь ISO/IEC 27017) эсвэл бусад эх сурвалжаас авсан байж болно. Эсвэл тухайн байгууллагаас тусгайлан боловсруулсан байж болно.

Зарим тохиолдолд байгууллага нь ISO/IEC 27001:2013- Хавсралт А-гийн хяналтын өөрчлөлт болох хяналтыг ашигладаг бөгөөд байгууллагын өөрчлөлтөөр сольсон анхны ISO/IEC 27001:2013- Хавсралт А-гийн хяналтыг энд оруулаагүй болно. Өөрөөр хэлбэл, өөрчлөлт нь ISO/IEC 27001:2013, Хавсралт А-гийн хяналтыг агуулж болох тул үүнийг хасч болохгүй.

Аудиторууд нь ISO/IEC 27001:2013, Хавсралт А-д өгөгдсөн тодорхойлолтод бус өөрийн байгууллагад шаардлагатай хяналтын тодорхойлолттой нийцэж байгаа эсэхийг хайх ёстой. Хэрэв байгууллагын тодорхойлолтод баримтжуулсан журам шаардлагатай бол энэ нь тухайн байгууллагын ISO/-д нийцэж байгаагийн нэг хэсэг болно. IEC 27001:2013, 7.5.1 b). Үгүй бол аудиторууд үүнийг үзэхийг шаардах ёсгүй. Гэсэн хэдий ч аудиторууд [ISO/IEC 27001:2013, 8.1)] "үйл явц төлөвлөсний дагуу явагдсан гэдэгт итгэлтэй байхын тулд шаардлагатай хэмжээгээр баримтжуулсан мэдээллийг хадгалах" ёстой гэсэн шаардлагыг аудиторууд анхаарах ёстой.

ISO/IEC 27001:2013, 8.1 нь ISO/IEC 27001:2013, 6.1-д хамаарах тул байгууллагын эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөө, шаардлагатай хяналт нь баримтжуулсан мэдээллийн энэхүү шаардлагын хүрээнд багтдаг.

Хяналтын сонгон шалгаруулалтад аудит хийхдээ хэрэглэх боломжтой байдлын тухай мэдэгдэлд заасан бие даасан шаардлагатай хяналтаас илүүтэй [ISO/IEC 27001:2013, 6.1.3 е) заасны дагуу] мэдээллийн аюулгүй байдлын эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөөнд нь аудит хийх нь илүү чухал юм.

Учир нь мэдээллийн аюулгүй байдлын эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөө(үүд) нь шаардлагатай хяналтуудын хоорондын харилцан үйлчлэлийг тодорхойлсон байх магадлалтай бөгөөд үүнийг зөвхөн хэрэглэх боломжтой байдлын мэдэгдлийг ашигласан тохиолдолд орхигдуулж болох юм.

A.5 Бусад баримтжуулсан мэдээлэл

ISO/IEC 27001 стандартын гол анхаарах зүйл нь үр дүн юм. Баримтжуулсан мэдээлэлд тавигдах 16 ил шаардлагын (Хүснэгт А.1-ийг үзнэ үү) зөвхөн гурав нь техникийн шинж чанартай (мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явц, мэдээллийн аюулгүй байдлын эрсдэлийг боловсруулах үйл явц, аудитын хөтөлбөр) хамаарна. Гэсэн хэдий ч энэ нь байгууллагад баримтжуулсан журамтай болоход нь саад болохгүй. Ийм дагалдах баримт бичиг нь ISO/IEC 27001:2013, 7.5.1 b)-ийн хамрах хүрээнд багтдаг (байгууллага МАБУТ-ийг үр дүнтэй ажиллахад шаардлагатай гэж тодорхойлсон баримтжуулсан мэдээлэл). Энэ нь тухайн байгууллагад тавигдах шаардлага болж, аудитын хүрээнд байх ёстой.

A.6 Тэмдэглэл

Энд шаардлагатай мэдээлэл нь вэб хуудасны нэг хэсэг эсвэл уншигчдын мэдээллийн сангаас хайсан асуултын үр дүн байж болно. Түүнчлэн, хэрэглэх боломжтой байдлын мэдэгдлийг эс тооцвол ISO/IEC 27001 баримт бичигт нэр заагаагүй болно. Иймд мэдээллийн аюулгүй байдлын бодлоготой холбоотой баримтжуулсан мэдээлэл нь “Мэдээллийн аюулгүй байдлын бодлого” хэмээх баримт бичиг, цахим хуудсанд байхгүй байх магадлалтай. Байгууллага нь мэдээллийн аюулгүй байдлын бодлогыг өөрөөр нэрлэх эрхтэй. Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо нь ISO/IEC 27001:2013, 5.3 а) стандартын шаардлагад нийцэж байгаа эсэхийг баталгаажуулах үүрэг, эрх бүхий этгээд(үүд) нь ISO/IEC 27001:2013, 5.3 а)-ын шаардлагад нийцэж байгаа бөгөөд ISO/IEC

27001 ба тэдгээрийн баримтжуулсан мэдээлэлд заасан баримтжуулсан мэдээллийн шаардлагуудын хоорондын хамаарлыг мэдэж байх ёстой.

A.7 МАБУТ-д аудит хийх заавар

Хүснэгт A.2-д дараах мэдээллийг жагсаав. Үүнд:

- эхний эгнээ: ISO/IEC 27001:2013 стандартын хамаатай дэд зүйлийн дугаар, нэр;
- хоёр дахь эгнээ: холбогдох заалтууд (энэ мөрийг хэрхэн ашиглах талаарх мэдээллийг A.2.2-оос үзнэ үү);
- гуравдугаар эгнээ: ISO/IEC 27000:2018 стандартын холбогдох тодорхойлолтууд ISO/IEC 27001:2013-ын холбогдох дэд зүйлд;
- дөрөв дэх эгнээ: ISO/IEC 27001:2013-ын хамаатай дэд зүйлийн талаархи мэдээллийн боломжит эх сурвалжууд "Аудитын нотлох баримт";
- тав дахь эгнээ: Аудитын практик удирдамж (A.3-ыг үзнэ үү);
- зургаа дахь эгнээ: ISO/IEC 27001:2013-ын холбогдох дэд зүйлд нийцүүлэн аудит хийхэд тустай нэмэлт баримт бичгийн "нэмэлт дэмжих баримт бичиг"-ийн лавлагаа.

Хүснэгт A.2 — ISO/IEC 27001 стандартын аудитын удирдамж

A.1 Байгууллагын нөхцөл байдал (ISO/IEC 27001:2013, 4-р зүйл)	
A.1.1 Байгууллага ба түүний нөхцөл байдлын талаарх ойлголт (ISO/IEC 27001:2013, 4.1)	
ISO/IEC 27001-ийн хамаатай дэд зүйл	ISO/IEC 27001:2013, 6.1, 9.3
Холбогдох ISO/IEC 27000 тодорхойлолтууд	Гадаад нөхцөл байдал, мэдээллийн аюулгүй байдал, дотоод нөхцөл байдал, удирдлагын тогтолцоо, зохион байгуулалт
Аудитын нотлох баримт	Аудитын нотлох баримтыг дараах баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно. Үүнд: a) МАБУТ-д эерэг эсвэл сөрөг нөлөө үзүүлж болох чухал асуудлууд;

	b) Байгууллага; c) Байгууллагын зорилго; d) МАБУТ-ийн төлөвлөсөн үр дүн. Чухал асуудлын боломжит эх сурвалжууд нь: a) уур амьсгал, бохирдол, нөөцийн хүртээмж, биологийн олон янз байдалтай холбоотой байгаль орчны шинж чанар, нөхцөл байдал, эдгээр нөхцөл байдал нь байгууллагын зорилгодоо хүрэх чадварт үзүүлэх нөлөө; b) гадаад соёл, нийгэм, улс төр, хууль эрх зүй, зохицуулалт, санхүү, технологи, эдийн засаг, байгалийн болон өрсөлдөөний нөхцөл байдал, олон улсын, үндэсний, бүс нутгийн болон орон нутгийн шинж чанартай; c) байгууллагын засаглал, мэдээллийн урсгал, шийдвэр гаргах үйл явц зэрэг байгууллагын онцлог, нөхцөл; — байгууллагын бодлого, зорилго, түүнд хүрэх стратеги; — байгууллагын соёл; — байгууллагаас баталсан стандарт, заавар, загвар; — байгууллагын бүтээгдэхүүн, үйлчилгээний амьдралын мөчлөг; — мэдээллийн аюулгүй байдлын удирдлагын үндэс суурь болох мэдээллийн систем, үйл явц, шинжлэх ухаан, технологи; d) аудит ба эрсдэлийн үнэлгээний чиг хандлага.

Аудитын практик гарын авлага	Байгууллага нь дараахь зүйлийг хангаж байгааг аудиторууд баталгаажуулах ёстой. Үүнд: a) МАБУТ-д эерэг эсвэл сөрөг нөлөө үзүүлж болох чухал асуудлуудын талаар өндөр түвшинд (жишээлбэл, стратегийн түвшний) ойлголттой байх; b) Өөрийн зорилгод нийцсэн, МАБУТ-ийн төлөвлөсөн үр дүнд хүрэх чадварт нөлөөлөх гадаад болон дотоод асуудлуудыг мэддэг. ТАЙЛБАР 1: ISO/IEC 27001:2013, 4.3-т заасан шаардлага нь “ISO/IEC 27001:2013, 4.1-д дурдсан гадаад болон дотоод асуудлыг авч үзэх”. Байгууллага нь гарцад заавал харагдахгүй зүйлийг анхаарч үзэх боломжтой. Эрсдэлийн удирдлагын процессыг ашиглан мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдлыг хадгалах, эрсдэлийг зохих ёсоор удирдаж байгаа эсэхийг аудиторууд баталгаажуулах ёстой. Аудиторууд тухайн асуудалд тухайн байгууллагын чухал сэдэв, мэтгэлцээн, хэлэлцүүлгийн асуудал, нөхцөл байдал өөрчлөгдөж байгаа эсэхийг шалгахаас гадна олж авсан мэдлэгээ удирдлагын тогтолцоог төлөвлөх, хэрэгжүүлэх, ажиллуулахад байгууллагын хүчин чармайлтыг чиглүүлэхэд ашиглаж байгаа эсэхийг шалгах ёстой.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.1
A.1.2 Сонирхогч талуудын хэрэгцээ, хүлээлтийг ойлгох (ISO/IEC 27001:2013, 4.2)	
ISO/IEC 27001-ийн хамаатай дэд зүйл	ISO/IEC 27001:2013, 4.1, 4.3

Холбогдох ISO/IEC 27000 тодорхойлолтууд	Сонирхогч тал
Аудитын нотлох баримт	Аудитын нотлох баримтыг дараах баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно.Үүнд: a) сонирхогч талууд; b) МАБУТ болон ISO/IEC 27001-д хамаарах холбогдох сонирхогч талуудын хэрэгцээ, хүлээлт. ТАЙЛБАР 2: Боломжит сонирхогч талууд дараахь зүйлийг агуулж болно.Үүнд: a) хууль эрх зүйн болон зохицуулах байгууллагууд (орон нутгийн, бүс нутгийн, муж улсын/аймаг, үндэсний эсвэл олон улсын); b) дээд байгууллага; c) үйлчлүүлэгчид; d) худалдааны болон мэргэжлийн холбоод; e) олон нийтийн бүлгүүд; f) төрийн бус байгууллага; g) ханган нийлүүлэгчид; h) хөршүүд; i) байгууллагын гишүүд болон байгууллагын нэрийн өмнөөс ажиллаж буй бусад хүмүүс; j) мэдээллийн аюулгүй байдлын мэргэжилтнүүд.

	ТАЙЛБАР 3: Сонирхогч этгээдийн шаардлагад дараах зүйлс орно. Үүнд: a) хууль тогтоомж; b) зөвшөөрөл, лиценз эсвэл зөвшөөрлийн бусад хэлбэр; c) зохицуулах байгууллагаас гаргасан тушаал; d) шүүх, захиргааны хэргийн шүүхийн шийдвэр; e) гэрээ, конвенц, протокол; f) холбогдох салбарын дүрэм, стандарт; g) байгуулсан гэрээ; h) олон нийтийн бүлэг, төрийн бус байгууллагатай байгуулсан гэрээ; i) төрийн эрх бүхий байгууллага, үйлчлүүлэгчидтэй байгуулсан гэрээ; j) зохион байгуулалтын шаардлага; k) сайн дурын зарчим буюу үйл ажиллагааны дүрэм; l) сайн дурын зүүлт тэмдэг буюу шошго, байгаль орчныг хамгаалах үүрэг; m) байгууллагатай байгуулсан гэрээний дагуу үүссэн үүрэг; n) мэдээлэл, харилцаа холбооны солилцоо. ТАЙЛБАР 4: Сонирхогч талууд нь байгууллагын бизнесийн зорилгод бүрэн нийцсэн, хэсэгчлэн нийцүүлсэн эсвэл эсрэг тэсрэг байж болох өөр өөр ашиг сонирхолтой байж болно. Сонирхогч этгээд байгууллагын зорилгод харш ашиг сонирхол байдгийн жишээ бол хакер юм. Хакер нь

	байгууллага сул хамгаалалттай байхыг хүсдэг. Байгууллага нь сонирхогч талын энэхүү шаардлагыг харгалзан үзэх ёстой бөгөөд үүний эсрэгээр, өөрөөр хэлбэл хүчтэй хамгаалалттай байх ёстой. МАБУТ нь дотоод болон гадаад эрсдэлийн бүх эх үүсвэрийг авч үздэг гэдгийг аудиторууд мэдэж байх ёстой. Тиймээс тухайн байгууллагыг эсэргүүцэж буй сонирхогч талуудын талаарх ойлголт, тэдний хүсэл сонирхол, шаардлагууд маш чухал юм.
Аудитын практик гарын авлага	Байгууллага нь МАБУТ болон ISO/IEC 27001-д хамаарах холбогдох сонирхогч талуудын хэрэгцээ, хүлээлтийг дээд түвшний (жишээ нь, стратегийн) ойлголттой байна гэдгийг аудиторууд батлах ёстой. Аудиторууд тухайн байгууллага нь сайн дурын үндсэн дээр батлах буюу гэрээ, гэрээ байгуулахаар шийдвэрлэсэн сонирхогч этгээдийн шаардлага, түүнчлэн засгийн газар эсвэл шүүхийн арга хэмжээний хүрээнд хууль тогтоомж, дүрэм журам, зөвшөөрөл, лицензүүдэд тусгагдсан тул зайлшгүй шаардлагатай хэрэгцээ, хүлээлтийг тодорхойлсон эсэхийг шалгах ёстой. Сонирхогч этгээдийн бүх шаардлага нь тухайн байгууллагын шаардлага биш бөгөөд зарим нь тухайн байгууллагад хамаарахгүй эсвэл МАБУТ-д хамаарахгүй гэдгийг энд тэмдэглэж байна. Сонирхогч этгээдийн зарим хэрэгцээ (жишээ нь, хакерын хэрэгцээ) нь МАБУТ-ийн зорилгод харшлах бөгөөд байгууллага нь мэдээллийн аюулгүй байдлын зохих хяналтыг ашиглан ийм хэрэгцээ, хүлээлтийг нь хангахгүй байх ёстой. Аудиторууд МАБУТ -д хамаатай гэж үзэж байгаа сонирхогч талууд байгаа эсэхийг баталгаажуулж, хэрэв байгаа бол энэ талаар тухайн байгууллагад мэдэгдэнэ. Аудиторууд мөн байгууллага нь МАБУТ-ийг төлөвлөх, хэрэгжүүлэх,

	ажиллуулахад хүчин чармайлтаа чиглүүлэхийн тулд олж авсан мэдлэгээ ашиглаж байгаа эсэхийг шалгаж болно.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.2
A.1.3 Мэдээллийн аюулгүй байдлын удирдлагын системийн хамрах хүрээг тодорхойлох (ISO/IEC 27001:2013, 4.3)	
ISO/IEC 27001-ийн хамаатай дэд зүйл	ISO/IEC 27001:2013, 4.1, 4.2
Холбогдох ISO/IEC 27000-ийн тодорхойлолтууд	Аутсорсинг
Аудитын нотлох баримт	Аудитын нотлох баримтыг дараах баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно. Үүнд: — байгууллагын удирдлагын тогтолцооны хамрах хүрээ (ISO/IEC 27001:2013, 4.3-т тодорхойлсон); — хэрэв байгаа бол байгууллагын баталгаажуулалтын хамрах хүрээ; — Хэрэглэх тухай мэдэгдэл. ТАЙЛБАР 5: Байгууллагын баталгаажуулалтын хамрах хүрээ нь түүний МАБУТ-ийн хамрах хүрээтэй ижил байх албагүй. Ерөнхийдөө баталгаажуулалтын хамрах хүрээ нь МАБУТ-ийг хэрэгжүүлсэн байгууллагаар л хязгаарлагдана.
Аудитын практик гарын авлага	Байгууллага нь МАБУТ-ийг хэрэглэх биет болон мэдээллийн, хууль эрх зүйн болон зохион байгуулалтын хил хязгаарыг өөрийн хүслээр тогтоож, ISO/IEC 27001 стандартыг байгууллагын хэмжээнд эсвэл тодорхой нэгж эсвэл тодорхой чиг үүрэг болгон хэрэгжүүлэхээр сонгосон гэдгийг аудиторууд батлах ёстой.

	Аудиторууд тухайн байгууллагын нөхцөл байдлын талаарх ойлголт (ISO/IEC 27001:2013, 4.1), холбогдох сонирхогч талуудын нөхцөл шаардлагууд (ISO/IEC 27001:2013, 4.2) болон тухайн байгууллагын гүйцэтгэсэн үйл ажиллагаа болон бусад байгууллагууд гүйцэтгэдэг үйл ажиллагаа хоорондын харилцан хамаарал байгаа эсэхийг шалгаж[ISO/IEC 27001:2013,4.3 c)], МАБУТ -ийн хамрах хүрээг тогтоохдоо зохих ёсоор авч үзсэн гэдгийг баталгаажуулах ёстой. Аудиторууд байгууллагын мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээ, эрсдэлийн асуудлыг шийдвэрлэх нь түүний үйл ажиллагааг зөв тусгаж, МАБУТ-д тодорхойлсон үйл ажиллагааны хил хязгаар, аудитын хамрах хүрээг хамарч байгааг баталгаажуулах ёстой. Аудиторууд хамрах хүрээ бүрд дор хаяж нэг ХББМ байгаа эсэхийг шалгах ёстой бөгөөд эрсдэлийн удирдлагын үйл явцад тодорхойлсон бүх хяналтыг ХББМ(үүд)-д оруулсан эсэхийг шалгах ёстой. Эдгээр хяналтууд нь ISO/IEC 27001:2013, 6.1.3 b)-д дурдсан шаардлагатай хяналтууд бөгөөд ISO/IEC 27001:2013, Хавсралт А-д заасан хяналтууд байх албагүй. Эдгээрт тухайн байгууллагын боловсруулсан эсвэл аль ч эх сурвалжаас тодорхойлсон салбарын тусгай хяналт, хяналт багтаж болно. Аудиторууд мөн МАБУТ-ийн хамрах хүрээнд бүрэн хамааралгүй үйлчилгээ, үйл ажиллагаатай харилцах харилцааг аудитад хамрагдах МАБУТ-д тусгаж, байгууллагын мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээнд оруулсан болохыг баталгаажуулах ёстой. Ийм нөхцөл байдлын жишээ бол бусад байгууллагуудтай тоног төхөөрөмжийг (жишээлбэл, мэдээллийн технологийн систем, мэдээллийн сан, харилцаа холбооны систем эсвэл

	бизнесийн үйл ажиллагааны аутсорсинг) хуваалцах явдал юм. Хамрах хүрээний баримт бичгийг баримтжуулсан мэдээллийн шаардлагын дагуу (ISO/IEC 27001:2013, 7.5) бий болгож, хянаж байгаа эсэхийг шалгах хэрэгтэй.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.3 ISO/IEC 27006:2015, 8.2, 9.1.3.5 (IS 9.1.3 Баталгаажуулалтын хамрах хүрээ) ISO/IEC 17021-1:2015, 8.2.2
A.1.4 Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо (ISO/IEC 27001:2013, 4.4)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 6.1.1, 6.1.2, 6.1.3, 8.1, 8.2, 8.3
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Байнгын сайжруулалт, мэдээллийн аюулгүй байдал, удирдлагын тогтолцоо
Аудитын нотлох баримт	Аудитын нотлох баримтыг ISO/IEC 27001 стандартад заасан үйл явцын талаарх баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно. Үүнд: a) удирдлагын тогтолцооны үйл явц (ISO/IEC 27001:2013, 4.4); b) үйл ажиллагааны төлөвлөлт, хяналтын үйл явц, түүний дотор аутсорсингийн үйл явц (ISO/IEC 27001:2013, 8.1); c) Мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явц (ISO/IEC 27001:2013, 6.1.2 ба/эсвэл 8.1.2) болон мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх үйл явц (ISO/IEC 27001) зэрэг мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний

	үйл явц (ISO/IEC 27001) :2013, 6.1.3 ба/эсвэл 8.1.3); зэрэг МАБУТ-ийг төлөвлөхдөө эрсдэл болон боломжуудыг шийдвэрлэх процессууд. d) мэдээллийн аюулгүй байдлын зорилгод хүрэх үйл явцууд.
Аудитын практик гарын авлага	Аудиторууд байгууллага нь ISO/IEC 27001 стандартын дагуу үр дүнтэй удирдлагын тогтолцоог бүрдүүлдэг "шаардлагатай боловч хангалттай" үйл явц, хяналтыг бий болгож, харилцан уялдаатай буюу харилцан үйлчлэгч элементүүдээс тогтсон МАБУТ-ийг бий болгож байгааг баталгаажуулах ёстой. Аудит хийж буй байгууллага нь одоо байгаа хүчин чадлаараа эрх мэдэл, хариуцлага, бие даасан байдлаа хэвээр хадгалж үлдэж байгааг, МАБУТ-ийн тавигдах шаардлагуудыг хэрхэн биелүүлэх талаарх шийдвэр шаардлагууд, түүний дотор МАБУТ-ийн шаардлагатай байгууллагын бизнэс үйл ажиллагаагаа уялдуулан нэгтгэх нарийвчилсан түвшин, цар хүрээг нь аудиторууд батлах ёстой.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.4
A.2 Манлайлал (ISO/IEC 27001:2013, 5-р зүйл)	
A.2.1 Манлайлал ба хүлээсэн үүрэг (ISO/IEC 27001:2013, 5.1)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 4.1, 4.2, 4.4, 5.2, 5.3, 6.1.1, 6.2, 7.1, 7.4, 8.1, 9.3, 10.2
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Мэдээллийн аюулгүй байдал, дээд удирдлага

Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно. Үүнд: a) мэдээллийн аюулгүй байдлын бодлого [ISO/IEC 27001:2013, 5.1 a)]; b) мэдээллийн аюулгүй байдлын зорилтууд [ISO/IEC 27001:2013, 5.1 a)]; c) байгууллагын үйл явцууд; d) удирдлагын хянан үзсэн үнэлгээний үр дүн [ISO/IEC 27001:2013, 5.1 c), ба g)]; e) нөөцийн хэрэгцээний үнэлгээ; f) мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны шаардлагад нийцүүлэх, мэдээллийн аюулгүй байдлын үр дүнтэй удирдлагын ач холбогдлын талаар харилцан мэдээлэл өгөх. Нотлох баримтыг дээд удирдлагатай ярилцлага хийх замаар олж авах боломжтой. Удирдлагын хяналт шалгалтын үр дүнь ISO/IEC 27001:2013, 5.1 c), e) ба g)-аас бусад дэд зүйлд заасан аудитын нотлох баримтыг бүрдүүлж болно.
Аудитын практик гарын авлага	Аудиторууд ISO/IEC 27001 стандартыг амжилттай хэрэгжүүлэхэд чухал ач холбогдолтой байгууллагын дээд удирдлагын харагдахуйц дэмжлэг, оролцоо, хүлээх үүрэг хариуцлагыг шалгах ёстой. Аудиторуудмөн дараахь зүйлийг баталгаажуулах ёстой. Үүнд: a) дээд удирдлагын бусдад өгсөн үүрэг даалгаврыг тодорхойлсон;

	b) дээд удирдлага нь байгууллагад даалгасан үйл ажиллагааг хангалттай гүйцэтгэсний төлөө хариуцлага хүлээдэг; c) дээд удирдлага нь мэдээллийн аюулгүй байдлын бодлого, зорилтыг бий болгож, тэдгээрийг нийт байгууллагын стратегийн чиглэлтэй уялдуулах; d) дээд удирдлага нь мэдээллийн аюулгүй байдлын үр дүнтэй удирдлага, МАБУТ-ийн шаардлагад нийцүүлэхийн ач холбогдлын талаар мэдээлэх; e) дээд удирдлага нь мэдээллийн аюулгүй байдлын удирдлагын бүхий л үйл явцыг хэрэгжүүлэхэд дэмжлэг үзүүлэх, ялангуяа МАБУТ-ийн байдал, үр дүнтэй байдлын талаарх тайланг хүсэлт гаргах, хянан шалгах замаар зорилгодоо хүрсэн үр дүнд хүрэхийг баталгаажуулдаг [ISO/IEC 27001:2013-ыг үзнэ үү. , 5.3 b)]; f) дээд удирдлага нь мэдээллийн аюулгүй байдал, мэдээллийн аюулгүй байдлын системтэй шууд холбоотой асуудлаар байгууллагын ажилтнуудаа удирдаж, дэмждэг; g) дээд удирдлага нь МАБУТ-ийн нөхцөл шаардлагыг байгууллагын үйл явцтай уялдуулан нэгтгэхийг баталгаажуулдаг; h) дээд удирдлага нь МАБУТ-ийг үр дүнтэй байлгах нөөцийн хүртээмжтэй байдлыг баталгаажуулдаг; i) дээд удирдлага нь удирдлагын үнэлгээний явцад нөөцийн хэрэгцээг үнэлж, төлөвлөсөн үйл ажиллагааны үр ашгийг хянах, тасралтгүй сайжруулах зорилтуудыг тавьдаг;

	j) дээд удирдлага нь МАБУТ-ийн шаардлагыг хэрэгжүүлэх, мэдээллийн аюулгүй байдлын зорилгод хүрэхийн тулд ажилтнуудаа идэвхтэй ажиллахад түлхэц өгөх соёл, орчныг бүрдүүлдэг.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 4.2 ISO/IEC 27003:2017, 5.1
A.2.2 Бодлого (ISO/IEC 27001:2013, 5.2)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 6.2, 7.4
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Мэдээллийн аюулгүй байдал, бодлого
Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно. Үүнд: a) мэдээллийн аюулгүй байдлын бодлого (ISO/IEC 27001:2013, 5.1); b) мэдээллийн аюулгүй байдлын зорилтууд [ISO/IEC 27001:2013, 5.2 b) ISO/IEC 27001:2013, 6.2].
Аудитын практик гарын авлага	Аудиторууд дараахь зүйлийг баталгаажуулах ёстой. Үүнд: a) мэдээллийн аюулгүй байдлын бодлого нь байгууллагын зорилгыг харгалзан ISO/IEC 27001 стандартын дагуу өндөр түвшний байгууллагын үүрэг амлалтыг тодорхойлсон; b) мэдээллийн аюулгүй байдлын бодлогыг тухайн байгууллагын өөртөө тавьсан мэдээллийн аюулгүй байдлын зорилтуудыг боловсруулах, бий болгоход ашигладаг, эсвэл мэдээллийн аюулгүй байдлын

	бодлогын нэг хэсэг болгон тодорхой тусгасан; в) мэдээллийн аюулгүй байдлын бодлогын баримтжуулсан мэдээллийг баримтжуулсан мэдээллийн шаардлагын дагуу үүсгэж, хянадаг (ISO/IEC 27001:2013, 7.5); c) мэдээллийн аюулгүй байдлын бодлогыг харилцаа холбооны заалтын шаардлагын дагуу дотооддоо мэдээлэх (ISO/IEC 27001:2013, 7.4); d) мэдээллийн аюулгүй байдлын бодлогыг зохих ёсоор бусад сонирхогч талуудад нээлттэй болгох. Мэдээллийн аюулгүй байдлын бодлого нь холбогдох шаардлага, тухайлбал холбогдох хууль тогтоомжийг хангах үүрэг амлалтыг агуулсан тул зөрчлийн тохиолдлуудад нөлөөлсөн системийн дутагдлыг цаг алдалгүй илрүүлж, засч залруулах арга хэмжээ авахад МАБУТ нь тохиромжгүй гэж үзэж болохгүй.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 4.3.2 ISO/IEC 27003:2017, 5.2
А.2.3 Байгууллагын үүрэг, хариуцлага, эрх мэдэл (ISO/IEC 27001:2013, 5.3)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 7.4, 9.2, 9.3
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Мэдээллийн аюулгүй байдал, зохион байгуулалт, дээд удирдлага
Аудитын нотлох баримт	ISO/IEC 27001:2013, 7.5.1 б)-ийг харгалзан аудитын нотлох баримтыг дараах баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр авах боломжтой:

	a) зохион байгуулалтын үүрэг; b) байгууллагын мэдээллийн аюулгүй байдлын гүйцэтгэлд нөлөөлж болохуйц өөрийн хяналтан дор ажилладаг хүмүүсийн ажлын байрны тодорхойлолт; c) дотоод аудитын хөтөлбөрийн хэрэгжилт, аудитын үр дүн; d) МАБУТ-ийн хамрах хүрээ, байгууллагын бүтэц. Нэмж дурдахад, удирдлагын хянан шалгасан үр дүнгийн талаарх баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр аудитын нэмэлт нотлох баримт байж болно.
Аудитын практик гарын авлага	Аудиторууд баримтжуулсан мэдээллийг шалгах ба/эсвэл ярилцлага хийх замаар дараахь зүйлийг батлах ёстой. Үүнд: a) МАБУТ-ийн нөхцөл шаардлагуудыг хэрэгжүүлэх үүрэг, эрх мэдлийг байгууллага доторх холбогдох чиг үүргээр хуваарилсан; b) дээд удирдлага нь эдгээр үүрэг хариуцлагыг хариуцаж, эрх мэдлийг тухайн үүргийг гүйцэтгэж буй ажилтнуудад хуваарилж, дамжуулах; c) харилцах заалтын шаардлагын дагуу үүрэг хариуцлага, эрх мэдлийг мэдээлэх (ISO/IEC 27001:2013, 7.4); d) ISO/IEC 27001 стандартын шаардлагад нийцэж буйг нотлох ажиллагааг дотоод аудитын шаардлагын дагуу явуулсан (ISO/IEC 27001:2013, 9.2);

	e) гүйцэтгэлийн тайлагналыг удирдлагын хянан шалгах үнэлгээний шаардлагын дагуу (ISO/IEC 27001:2013, 9.3) хэрэгжүүлнэ. Аудиторууд МАБУТ-ийн байдал, гүйцэтгэлийн талаар удирдлагад мэдээлэл өгөхийн тулд үүрэг хариуцсан хүмүүс дээд удирдлагатай хангалттай уулзах, хандах боломжтой байгаа эсэхийг шалгах ёстой. ТАЙЛБАР 6: Удирдлагын тогтолцоог ISO/IEC 27001 стандартын шаардлагад нийцүүлэхийг баталгаажуулах үүргийг хувь хүнд хуваарилж, хэд хэдэн хүн хуваалцаж эсвэл багт хуваарилж болно.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 4.3.3 ISO/IEC 27003:2017, 5.3
A.3 Төлөвлөлт (ISO/IEC 27001:2013, 6-р зүйл)	
A.3.1 Эрсдэл, боломжуудыг шийдвэрлэх арга хэмжээ (ISO/IEC 27001:2013, 6.1)	
A.3.1.1 Ерөнхий (ISO/IEC 27001:2013, 6.1.1)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 4.1, 4.2, 8.1, 9, 10.2
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Мэдээллийн аюулгүй байдал, эрсдэл, эрсдэлийн удирдлага
Аудитын нотлох баримт	Аудитын нотлох баримтыг дараах баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно. Үүнд:

	a) ISO/IEC 27001:2013, 6.1.1, 7.5.1 b) ба 8.1)]-ийн төлөвлөлт; b) мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явц (ISO/IEC 27001:2013, 6.1.2); c) мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үр дүн (ISO/IEC 27001:2013, 8.2); d) мэдээллийн аюулгүй байдлын эрсдэлийн асуудлыг шийдвэрлэх үйл явц (ISO/IEC 27001:2013, 6.1.3); e) мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх үйл явцын үр дүн (ISO/IEC 27001:2013, 8.3); f) хяналт-шинжилгээ, хэмжилтийн үр дүн (ISO/IEC 27001:2013, 9.1); g) дотоод аудитын хөтөлбөр(үүд) ба дотоод аудитын үр дүн (ISO/IEC 27001:2013, 9.2); h) удирдлагын хянан шалгасан үнэлгээний үр дүн (ISO/IEC 27001:2013, 9.3); i) байгууллагын нөхцөл байдал (ISO/IEC 27001:2013, 4); j) мэдээллийн аюулгүй байдлын зорилтууд (ISO/IEC 27001:2013, 6.2).
Аудитын практик гарын авлага	Аудиторууд байгууллагын төлөвлөгөө нь дараах зүйлийг хангаж байгааг батлах ёстой. Үүнд: a) МАБУТ-ийг төлөвшүүлэхэд төлөвлөгөө нь тохирсон түвшинд хийгдэж байгаа эсэх; b) ISO/IEC 27001:2013, 6.1.1-тэй холбоотой үр дагавар a)- с хүртэлх) –д хамаарах аливаа сөрөг эсвэл эерэг асуудлыг шийдвэрлэхийн тулд (ISO/IEC 27001:2013, 4.1) болон (ISO/IEC 27001:2013, 4.3)-д тодорхойлсон

	байгууллагын нөхцөлтэй холбоотой асуудлуудыг авч үзэхийг багтаасан эсэх. c) болзошгүй нөхцөл байдал, үр дагаврыг урьдчилан тооцоолсон байх ба хүсээгүй үр дагаврыг үүсэхээс нь өмнө арилгахад урьдчилан сэргийлэх; d) эрсдэлийн удирдлагын үйл явцыг хэрэгжүүлэх замаар мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжийг хадгалах зэрэг байгууллагаас тодорхойлсон зорилтот үр дүнг [ISO/IEC 27001:2013, 6.1.1 a)] шийдвэрлэх; e) зорилгоо тодорхойлох (ISO/IEC 27001:2013, 6.2), үйл ажиллагааны хяналт (ISO/IEC 27001:2013, 8.1) эсвэл МАБУТ-ын бусад тусгай заалтуудаар дамжуулан шаардлагатай эсвэл ашигтай гэж үзсэн үйлдлүүдийг МАБУТ-д хэрхэн оруулахыг тодорхойлох асуудал орно. ISO /IEC 27001, жишээ нь. нөөцийн заалтууд (ISO/IEC 27001:2013, 7.1), чадвар (ISO/IEC 27001:2013, 7.2), мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээ (ISO/IEC 27001:2013, 8.2), мэдээллийн аюулгүй байдлын эрсдэлийн асуудлыг шийдвэрлэх (ISO/IEC 27001: 2013, 8.3); f) төлөвлөсөн арга хэмжээний үр нөлөөг үнэлэх механизмыг тодорхойлох, мөн үүнд хяналт-шинжилгээ мониторинг, хэмжилтийн арга техник (ISO/IEC 27001:2013, 9.1), дотоод аудит (ISO/IEC 27001:2013, 9.2) эсвэл удирдлагын хянан шалгалт (ISO/IEC 27001:2013, 9.3) гэх зэрэг багтаж болно.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 5.3-5.7 ISO/IEC 27003:2017, 6.1.1

A.3.1.2 Мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээ (ISO/IEC 27001:2013, 6.1.2)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 8.2
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Боломжтой байдал, нууцлал, мэдээллийн аюулгүй байдал, бүрэн бүтэн байдал, эрсдэл хүлээн даах, эрсдэлийн шинжилгээ, эрсдэлийн үнэлгээ, эрсдэлийн шалгуур, эрсдэлийг тодорхойлох
Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно. Үүнд: a) ISO/IEC 27001:2013, 6.1.1, 7.5.1 b) ба 8.1)]-ийн төлөвлөлт; b) мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явц (ISO/IEC 27001:2013, 6.1.2) болон мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үр дүн (ISO/IEC 27001:2013, 8.2).
Аудитын практик гарын авлага	Аудиторууд мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээнд дараах зүйлийг баталгаажуулах ёстой. Үүнд a) МАБУТ-тэй холбоотой аюулгүй байдлын мэдээллийн эрсдлийг тодорхойлох; b) эрсдэлийг тодорхойлох, эрсдэлд дүн шинжилгээ хийх, эрсдэлийг үнэлэх үйл явцаас бүрдэнэ.
	Эрсдлийн шалгуур [ISO/IEC 27001:2013, 6.1.2 a)]
	Аудиторууд тухайн байгууллага нь эрсдэл хүлээх шалгуур болон мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээг хийх шалгууруудыг тогтоож, хадгалж байгаа эсэхийг баталгаажуулах ёстой. Байгууллага нь эрсдэл хүлээх шалгуур, мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээ хийх шалгуур, мэдээллийн

	аюулгүй байдлын эрсдлийн үнэлгээ хийх зэрэг эрсдэлийн шалгууруудыг тогтоохдоо хамааралтай гэж үзсэн хүчин зүйлсийг харгалзан үзэх эрх чөлөөтэй боловч хэрхэн үндэслэлтэй шийдвэрт үндэслэн тухайн байгууллага эрсдэл хүлээх шалгуур, түүний шалгуур үзүүлэлтийг бий болгосон эсэхийг нь аудиторууд үнэлэх ёстой. Эрсдэлийн үнэлгээний үйл явцтай холбоотой баримтжуулсан мэдээлэлд байгууллагын эрсдэлийн шалгуурыг тусгасан байх нь үндэслэлтэй юм. Хэрэв тийм биш бол байгууллага нь аудиторуудад юу болохыг тайлбарлах боломжтой байх ёстой. Наад зах нь байгууллагын эрсдэлийг хүлээх шалгуур, эрсдэлийн үнэлгээ хийх шалгууруудыг багтаасан байх ёстой. ТАЙЛБАР 7: ISO/IEC 27001:2013, 8.2-д заасны дагуу байгууллагууд мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээг төлөвлөсөн хугацаанд (интервалаар) эсвэл томоохон өөрчлөлт хийхээр төлөвлөж байгаа эсвэл өөрчлөлт тохиолдсон үед хийхийг шаарддаг. Эрсдлийн үнэлгээг бүх МАБУТ эсвэл түүний зарим хэсэгт хийж болно (энэ нь сүүлийн тохиолдол нь МАБУТ-ны зарим хэсэгт томоохон өөрчлөлтүүд нөлөөлж, дараа нь хэсэгчилсэн эрсдэлийн үнэлгээ хийх шаардлагатай байгааг харуулж болно).
	Үр дүнгийн тууштай байдал, хүчин төгөлдөр байдал, харьцуулалт [ISO/IEC 27001:2013, 6.1.2 b)]
	Мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явцаар хийсэн эрсдлийн үнэлгээний үр дүн тууштай, хүчинтэй, харьцуулах боломжтой гэдгийг аудиторууд баталгаажуулах ёстой. Энэхүү баталгаажуулалтыг дараах байдлаар хийж болно:.

	— өөрийн эрсдэлийн үнэлгээний үр дүн яагаад тууштай, хүчинтэй, харьцуулж болохуйц байгааг байгууллагаас асуух; — мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үр дүнгийн талаархи баримтжуулсан мэдээллийн түүвэрлэлт. Тогтвортой байдал, үнэн зөв байдлыг үнэлэхийн тулд аудиторууд дараах зүйлийг шалгаж болно: — ижил төстэй нөхцөл дэх ижил төстэй эрсдлийг ижил төстэй байдлаар үнэлсэн; — өөрөөр үнэлэгдсэн эрсдэлүүд нь ийм зөрүүтэй байх үндэслэлтэй байх; — ерөнхий үнэлгээний үр дүн хоёрдмол утгагүй ойлгомжтой. Харьцуулах чадварыг үнэлэхийн тулд аудиторууд дараах зүйлийг шалгаж болно: — өмнөх эрсдэлийн үнэлгээнд ижил эрсдэл хэрхэн үнэлэгдсэн, хэрэв өөрчлөгдсөн бол ойлгомжтой эсэх; — эрсдэл нь бусдаас өндөр эсвэл бага байх нь ойлгомжтой бол.
	Эрсдэлийг тодорхойлох [ISO/IEC 27001:2013, 6.1.2 c)]
	Аудиторууд мэдээллийн аюулгүй байдлын эрсдэлийг тухайн байгууллага нь МАБУТ-ийн хүрээнд нууцлал, бүрэн бүтэн байдал, мэдээллийн хүртээмжийг алдагдуулахтай холбоотой тодорхойлсон болохыг баталгаажуулах ёстой. ТАЙЛБАР 8: ISO/IEC 27001:2013 нь хөрөнгө, аюул, эмзэг байдлыг тодорхойлох замаар эрсдэлийг тодорхойлох

	шаардлагагүй. Үйл явдал, үр дагаврыг харгалзан эрсдэлийг тодорхойлох зэрэг эрсдэлийг тодорхойлох бусад аргуудыг хүлээн зөвшөөрөх боломжтой. Эрсдлийн үнэлгээний үйл явцтай холбоотой баримтжуулсан мэдээллээс байгууллагын эрсдэлийг тодорхойлох үйл явцын тодорхойлолтыг олох нь үндэслэлтэй юм (доороос үзнэ үү). Байгууллага эрсдэлийг тодорхойлох арга барилаа боловсруулахдаа анхаарч үзэх (гэхдээ заавал шаардлагагүй) хүчин зүйлүүд нь: a) эрсдэлийг хэрхэн олж, хүлээн зөвшөөрч, тодорхойлсон; b) авч үзэх эрсдэлийн эх үүсвэр. Байгууллагын анхаарч үзэх боломжтой (гэхдээ заавал шаардлагагүй) бусад хүчин зүйлүүд нь: a) эрсдэл нь байгууллагын мэдээллийн аюулгүй байдлын зорилтыг хэрхэн бий болгох, нэмэгдүүлэх, урьдчилан сэргийлэх, доройтуулах, хурдасгах, хойшлуулах; боломжийг эрэлхийлэхгүй байхтай холбоотой эрсдэл; b) эрсдэлийн эх үүсвэр, шалтгаан нь тодорхойгүй байсан ч эх үүсвэр нь байгууллагын хяналтад байгаа эсэхээс үл хамаарсан эрсдэл; c) тодорхой үр дагаврын уналтын нөлөө, түүний дотор шаталсан болон хуримтлагдсан нөлөөг судлах; d) эрсдэлийн эх үүсвэр, шалтгаан нь тодорхойгүй байсан ч өргөн хүрээний үр дагаврыг авч үзэх; e) ямар үр дагавар гарч болохыг харуулсан боломжит шалтгаан, хувилбаруудыг авч үзэх; f) бүх чухал шалтгаан, үр дагаврыг харгалзан үзэх;

	g) эрсдлийн иж бүрэн жагсаалтыг хэрхэн бий болгох. ТАЙЛБАР 9: Олон тооны шаардлагатай хяналтыг санамсаргүйгээр орхигдуулсан нь эрсдэлийг тодорхойлох үйл явц сул байгааг илтгэнэ. МАБУТ-ны хамрах хүрээний бүх чухал мэдээллийг эрсдлийн үнэлгээнд оруулсан гэдгийг түүвэрлэлтийн явцад баталгаажуулах ёстой. Аудиторууд эрсдэлийн үнэлгээний үр дүнгийн талаарх баримтжуулсан мэдээлэлд МАБУТ-ны хүрээнд мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмж алдагдахтай холбоотой эрсдэл байгаа эсэхийг шалгах ёстой. Байгууллагын мэдээллийн аюулгүй байдлын зорилтууд нь мэдээллийн аюулгүй байдлын эрсдлийг тодорхойлоход аудиторуудад тусалдаг. Аудиторууд дараах зүйлийг баталгаажуулах ёстой. Үүнд: a) эрсдэл бүрийн хувьд эрсдэл хүлээгч(үүд)-ийг тодорхойлсон; b) эрсдэл хүлээгч бүр өөрийн тодорхойлсон эрсдэл(үүд)-ийг удирдах хариуцлага, эрх мэдэлтэй байна.
	Эрсдлийн шинжилгээ [ISO/IEC 27001:2013, 6.1.2 d)]
	Аудиторууд дараах зүйлийг баталгаажуулах ёстой. a) мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явцад эрсдэлийн дүн шинжилгээ хийх зорилгоор байгууллага нь тодорхойлсон эрсдлийн мөн чанарыг ойлгож, эрсдлийн түвшинг тодорхойлох;

	b) эрсдлийн шинжилгээ нь эрсдлийг үнэлэх, эрсдэлийг хэрхэн шийдвэрлэх, эрсдэлийн хамгийн оновчтой шийдэл, стратеги, аргуудын талаар шийдвэр гаргахад орц өгдөг. Мөн байгууллага нь ISO/IEC 27001:2013, 6.1.2 c)-ийн дагуу тодорхойлсон эрсдэлтэй холбоотой болзошгүй үр дагавар, магадлалыг үнэлж, эрсдэлийн түвшинг тодорхойлсон болохыг аудиторууд баталгаажуулах ёстой. Эрсдэлийн үнэлгээний үйл явцтай холбоотой баримтжуулсан мэдээллээс тухайн байгууллагын эрсдэлийн шинжилгээнд хандах хандлагын тодорхойлолтыг олох нь үндэслэлтэй бөгөөд үр дүн нь эрсдэлийн үнэлгээний үр дүнгийн талаарх баримтжуулсан мэдээлэлд байх болно (дооpоос үзнэ үү). Аудиторууд байгууллагын эрсдэлийн удирдлагын бодлого, стратеги, арга барилд хандах ёстой. Эрсдлийн шинжилгээ нь дараах шинжтэй байж болно. a) эрсдэл, шинжилгээний зорилго, байгаа мэдээлэл, өгөгдөл, нөөцөөс хамааран янз бүрийн нарийвчлалтайгаар хийгдсэн; b) нөхцөл байдлаас шалтгаалан чанарын, хагас тоон, тоон буюу тэдгээрийн хослол.
	Эрсдэлийн үнэлгээ [ISO/IEC 27001:2013, 6.1.2 e)]
	Аудиторууд тухайн байгууллага нь эрсдэлийн шинжилгээний үр дүнг мэдээллийн аюулгүй байдлын эрсдэлийг хүлээх шалгууртай харьцуулж, тодорхойлсон эрсдэлийг хүлээн зөвшөөрөх боломжтой эсэхийг баталгаажуулах ёстой. Аудиторууд эрсдэлийн үнэлгээний үр дүн нь эрсдэлийг хүлээх шалгуурыг зохих ёсоор

	хэрэгжүүлсэн, илрүүлсэн, дүн шинжилгээ хийсэн эрсдэлийн асуудлыг шийдвэрлэхийн тулд эрэмбэлэгдсэн болохыг нь нотлох ёстой. Илүү нарийвчилсан байдлаар авч үзвэл аудиторууд эрсдэлийн үнэлгээг шалгахдаа дараах зүйлийг харах ёстой: a) эрсдэлийг хэрхэн шийдвэрлэх шаардлагатай болон тэргүүлэх ач холбогдлын талаарх эрсдлийн шинжилгээний үр дүнд үндэслэн шийдвэр гаргахад тусалдаг; b) шинжилгээний явцад илэрсэн эрсдлийн түвшинг тухайн нөхцөл байдлыг авч үзэх үед тогтоосон мэдээллийн аюулгүй байдлын эрсдэлийн шалгуур үзүүлэлттэй харьцуулах зэрэг орно. Аудиторууд дараах шийдвэрүүдийг үнэлэх ёстой: a) эрсдэлийн өргөн хүрээг харгалзан үзэх; b) хууль эрх зүй, зохицуулалтын болон бусад шаардлагыг оролцуулан холбогдох сонирхогч талуудын шаардлагыг харгалзан үзэх.
	Баримтжуулсан мэдээлэл (ISO/IEC 27001:2013, 6.1.2 ба 8.2)
	Аудиторууд эрсдэлийн үнэлгээний үйл явцтай холбоотой баримтжуулсан мэдээлэл байгаа эсэхийг баталгаажуулах ёстой. Мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явцын талаарх баримтжуулсан мэдээлэл нь дараахь зүйлийг агуулна гэж хүлээх нь үндэслэлтэй байх болно:

	a) эрсдэл хүлээн авах шалгуур, мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээ хийх шалгуурыг багтаасан эрсдэлийн шалгуурын тодорхойлолт; b) үр дүнгийн тууштай байдал, үнэн зөв, харьцуулах боломжтой байдлын үндэслэл; c) эрсдэлийг тодорхойлох үйл явцын тодорхойлолт (эрсдэл хүлээж буй этгээдийг тодорхойлох зэрэг); d) мэдээллийн аюулгүй байдлын эрсдэлд дүн шинжилгээ хийх үйл явцын тодорхойлолт (болзошгүй үр дагавар, бодит магадлал, эрсдлийн түвшинг үнэлэх); e) үр дүнг эрсдэлийн шалгуур үзүүлэлттэй харьцуулах үйл явцын тодорхойлолт, эрсдэлийн асуудлыг шийдэхийн тулд эрсдэлийг эрэмбэлэх. ТАЙЛБАР 10: Дээр дурдсан зүйлүүд нь ISO/IEC 27001 стандартын шаардлагад нийцэж байгаа тул эрсдэлийн үнэлгээний үйл явцтай холбоотой баримтжуулсан мэдээллээс тэдгээрийн талаарх мэдээллийг олж авах нь үндэслэлтэй юм.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 5.3, 5.4, 5.7 ISO/IEC 27003:2017, 6.1.2, 8.2
A.3.1.3 Мэдээллийн аюулгүй байдлын эрсдэлийн эмчилгээ (ISO/IEC 27001:2013, 6.1.3)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 8.3, Хавсралт А

Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Хяналт, хяналтын зорилго, баримтжуулсан мэдээлэл, мэдээллийн аюулгүй байдал, үлдэгдэл эрсдэл, эрсдлийн үнэлгээ, эрсдэлийн шалгуур, эрсдэл хүлээгч этгээд, эрсдэлийн асуудлыг шийдвэрлэх
Аудитын нотлох баримт	Аудитын нотлох баримтыг дараах баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно: a) МАБУТ-ны төлөвлөлт; b) мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх үйл явц; c) мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх явцын үр дүн; d) Хэрэглэх боломжтой байдлын мэдэгдэл.
Аудитын практик гарын авлага	**Мэдээллийн аюулгүй байдлын эрсдэлийн асуудлыг шийдвэрлэх (ISO/IEC 27001:2013, 6.1.3)**
	Байгууллага нь мэдээллийн аюулгүй байдлын эрсдлийг мэдээллийн аюулгүй байдлын эрсдэлийн асуудлыг шийдвэрлэх процесс болгон өөрчилдөг гэдгийг аудиторууд батлах ёстой. Аудиторууд мэдээллийн аюулгүй байдлын эрсдэлийн асуудлыг шийдвэрлэхэд дараах зүйлийг багтаасан эсэхийг шалгах ёстой. Үүнд: a) мэдээллийн аюулгүй байдлын эрсдлийг өөрчлөх нэг буюу хэд хэдэн хувилбарыг сонгох, хяналтыг хангах эсвэл өөрчлөх хувилбаруудыг хэрэгжүүлэх; b) тухайн эрсдэлийн асуудлыг шийдвэрлэх үр дүнг үнэлэх мөчлөгийн үйл явц.
	Мэдээллийн аюулгүй байдлын эрсдэлийн асуудлыг шийдвэрлэх тохиромжтой хувилбаруудыг сонгох [ISO/IEC 27001:2013, 6.1.3 a)]

	Аудиторууд эрсдэлийн асуудлыг шийдвэрлэх үйл явцтай холбоотой баримтжуулсан мэдээлэл нь мэдээллийн аюулгүй байдлын эрсдэлийн асуудлыг шийдвэрлэх оновчтой хувилбаруудыг сонгоход тухайн байгууллагын ашигладаг аргын тайлбарыг агуулсан болохыг баталгаажуулах ёстой. Аудиторууд энэ тодорхойлолт нь тухайн байгууллагын бодитой хийж байгаа зүйлтэй тохирч байгааг батлах ёстой. Тайлбар 1-д ISO/IEC 27000:2018, 3.72, эрсдэлийн асуудлыг шийдвэрлэх долоон хувилбарыг жагсаасан бөгөөд тэдгээрээс гаралтай ISO/IEC 27001:2013, 6.1.3-т ISO 31000-ыг иш татсан тэмдэглэл байгааг анхаарна уу. Аудиторууд эрсдэлийн шалгуур болон эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөөний хоорондын уялдааг шалгах ёстой. Байгууллага эрсдэлийн асуудлыг шийдвэрлэх хувилбаруудын талаар гаргасан шийдвэрээ баримтжуулаагүй байсан ч тайлбарлах чадвартай байх ёстой. Аудиторууд байгууллагын сонгосон эрсдэлийн асуудлыг шийдвэрлэх хувилбаруудыг хянаж үзэх ёстой. Аудиторууд эрсдэлийн асуудлыг шийдвэрлэх сонгосон хувилбаруудын зохистой байдлыг мөн хянаж үзэх ёстой. Аудиторууд эрсдэлийн үнэлгээ болон эрсдэлийн асуудлыг шийдвэрлэх шийдвэрт сүүлийн үеийн өөрчлөлтүүд (жишээлбэл, мэдээллийн технологийн шинэ систем эсвэл бизнесийн үйл явц) зохих ёсоор тусгагдсан эсэхийг шалгах ёстой.
	Шаардлагатай бүх хяналтыг тодорхойлох [ISO/IEC 27001:2013, 6.1.3 b)]

	Аудиторууд эрсдэлийн асуудлыг шийдвэрлэх үйл явцтай холбоотой баримтжуулсан мэдээлэл нь мэдээллийн аюулгүй байдлын шаардлагатай хяналтыг тодорхойлоход тухайн байгууллагын ашигладаг аргын тайлбарыг агуулсан болохыг баталгаажуулах ёстой. Аудиторууд мөн энэ тодорхойлолт нь тухайн байгууллагын хийж байгаа зүйлтэй тохирч байгааг батлах ёстой. Энэ нь Хэрэглэх боломжтой байдлын мэдэгдэлд [ISO/IEC 27001:2013, 6.1.3 d)] шаардлагатай хяналтуудыг агуулсан байх ёстой ба шаардлагатай хяналтууд нь ISO/IEC 27001:2013, Хавсралт А-ын хяналт байх албагүй. Эдгээр нь тухайн салбарын хяналт байж болно (ISO/IEC 27011, ISO/IEC 27017 гэх мэт салбарын тусгай стандартад тодорхойлсон). Байгууллагууд өөрсдөө эсвэл ямар ч эх сурвалжаас тодорхойлж болох тул тэдгээр нь "захиалгат хяналт" байж болно [ISO/IEC 27001:2013, 6.1.3 б-г үзнэ үү]. Эрсдэлийн асуудлыг шийдвэрлэх хувилбаруудыг хэрэгжүүлэхээр тодорхойлсон бүх хяналтыг Хэрэглэх боломжтой байдлын мэдэгдэлд оруулах ёстой. Түүнчлэн аливаа захиалгат хяналтыг шаардлага болон хэрэгжилтийн аль алинд нь тодорхой зааж өгөх ёстой.
	Хавсралт А-тай харьцуулна уу [ISO/IEC 27001:2013, 6.1.3 c)]
	Энэхүү шаардлагад нийцэж байгаа нь доор тайлбарласны дагуу Хэрэглэх боломжтой байдлын мэдэгдлийг хянан үзэх замаар нотлогддог.
	Хэрэглэх боломжтой байдлын мэдэгдэл гаргах [ISO/IEC 27001:2013, 6.1.3 d)]

	Аудиторууд Хэрэглэх боломжтой байдлын тухай мэдэгдэлд дараах зүйлийг агуулж байгаа эсэхийг шалгах ёстой. a) ISO/IEC 27001:2013, 6.1.3-ыг хэрэглэх явцад тодорхойлсон шаардлагатай хяналтууд b) ба c); b) тэдгээрийг оруулах үндэслэл (жишээ нь, эрсдэлийг арилгах хувилбаруудыг ашигласан тохиолдолд); c) шаардлагатай хяналтыг хэрэгжүүлсэн эсэх; d) хавсралт A-д хасагдсан бүх хяналтын үндэслэл, тухайлбал: 1) хяналт нь тухайн байгууллагын эрхэлдэггүй үйл ажиллагааны хүрээнд хамаарах; 2) байгууллага нь A хавсралтын хяналтын хэрэгцээг бууруулсан захиалгат хяналтыг ашигладаг; 3) байгууллага нь A хавсралтын хяналттай ижил зорилготой захиалгат хяналтыг ашигладаг (дэлгэрэнгүй мэдээллийг ISO/IEC 27003-аас үзнэ үү); e) шаардлагатай хяналт гэж томилогдсон эсвэл хавсралт A-аас хасагдсан хяналттай адилаар авч үзэх холбогдох салбарын тусгай хяналтууд. Тиймээс аудиторууд эрсдэлийн асуудлыг шийдвэрлэх сонгосон хувилбаруудыг хэрэгжүүлэхэд шаардлагатай хяналтууд болон Хэрэглэх боломжтой байдлын мэдэгдэл хоёрын уялдаа холбоог баталгаажуулах ёстой.
	Эрсдлийн асуудлыг шийдвэрлэх төлөвлөгөө боловсруулах [ISO/IEC 27001:2013, 6.1.3 e)]
	Аудиторууд эрсдэлийн асуудлыг шийдвэрлэх үйл явцтай холбоотой баримтжуулсан мэдээлэлд тухайн байгууллагын эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөөг

	боловсруулахдаа ашигладаг аргын тайлбарыг агуулсан болохыг баталгаажуулах ёстой.
	Аудиторууд эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөөг ISO/IEC 27001:2013, 6.1.3 a)-аас c)-ийн үр дүнд боловсруулсан болохыг баталгаажуулах ёстой. Аудиторууд эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөөнд тусгагдсан мэдээлэл нь дараах зүйлийг агуулж байгаа эсэхийг баталгаажуулах ёстой. a) төлөвлөгөөнд тусгагдсан эрсдэл(үүд); b) шаардлагатай хяналт(ууд); c) эрсдэлийг хүлээн авах шалгуурыг хангахын тулд эрсдэлийг өөрчлөхөд шаардлагатай хяналтууд хэрхэн хүлээгдэж байгаа; d) эрсдэл хүлээгчид; ТАЙЛБАР 11: Эрсдэл хүлээгчид эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөөг баталж, шийдэгдээгүй үлдсэн эрсдэлийг хүлээн зөвшөөрөх үүрэгтэй. e) эрсдэлийн асуудлыг шийдвэрлэх сонгосон хувилбар(ууд); f) шаардлагатай хяналтын хэрэгжилтийн байдал; g) эрсдэлийн асуудлыг шийдвэрлэх аргыг сонгох шалтгаан, түүний дотор хүлээгдэж буй үр өгөөж; h) санал болгож буй арга хэмжээ, үүнд хариуцлагатай хүмүүс, хугацаа, хуваарь; i) нөөцийн шаардлага, түүний дотор болзошгүй нөхцөл байдал; j) гүйцэтгэлийн хэмжүүр, хязгаарлалт; k) тайлагнах, хяналт тавих.

	Аудиторууд эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөө нь байгууллагын зорилго, удирдлагын үйл явцыг харгалзан үзэж, холбогдох сонирхогч талуудтай хэлэлцсэн эсэхийг шалгах ёстой.
	Эрсдэл хүлээгчээс зөвшөөрөл авах [ISO/IEC 27001:2013, 6.1.3 f)]
	Аудиторууд байгууллага нь дараах зүйлийг хийж байгаа гэдгийг батлах ёстой: a) зохих эрсдэлийг хүлээгч эздийг тодорхойлох; b) шийдэгдээгүй үлдсэн эрсдлийг баримтжуулах; c) Мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх төлөвлөгөөнд эрсдэл хүлээгчдээс зөвшөөрөл авах, үлдсэн эрсдэлийг хүлээн зөвшөөрөх.
	Баримтжуулсан мэдээлэл
	Аудиторууд эрсдэлийн асуудлыг шийдвэрлэх үйл явцтай холбоотой баримтжуулсан мэдээлэл байгаа эсэхийг баталгаажуулах ёстой. Мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх үйл явцын талаарх баримтжуулсан мэдээлэлд дараах зүйлсийн тайлбарыг агуулсан байх нь үндэслэлтэй байх болно. Үүнд: a) мэдээллийн аюулгүй байдлын эрсдэлийн асуудлыг шийдвэрлэх оновчтой хувилбаруудыг сонгох арга; b) шаардлагатай хяналтыг тодорхойлох арга; c) ISO/IEC 27001:2013, Хавсралт А-ыг шаардлагатай хяналтыг санамсаргүй орхигдуулаагүйг тодорхойлоход хэрхэн ашигласан;

	d) ХББМ-ийг хэрхэн бэлтгэсэн; e) эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөөг хэрхэн боловсруулсан; f) эрсдэл хүлээгчийн зөвшөөрлийг хэрхэн авсан. ТАЙЛБАР 12: Байгууллагын эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөөний агуулга, хэлбэрт тавигдах тусгай шаардлага байхгүй.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 5.5, 5.7 ISO/IEC 27003:2017, 6.1.3, 8.3 ISO/IEC 27006
A.3.2 Мэдээллийн аюулгүй байдлын зорилтууд ба түүнд хүрэх төлөвлөлт (ISO/IEC 27001:2013, 6.2)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 5.1, 5.2, 7.1, 7.3, 7.4, 7.5, 9.1, 9.3, 10.2
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Мэдээллийн аюулгүй байдал, зорилго
Аудитын нотлох баримт	Аудитын нотлох баримтыг мэдээллийн аюулгүй байдлын зорилго, түүнд хүрэх төлөвлөгөөний талаарх баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно.
Аудитын практик гарын авлага	Мэдээллийн аюулгүй байдлын зорилтууд болон түүнд хүрэх төлөвлөлт нь (ISO/IEC 27001:2013, 6.2) манлайлал, үүрэг хариуцлага (ISO/IEC 27001:2013, 5.1) болон бодлоготой (ISO/IEC 27001:2013, 5.2) холбоотой юм Аудиторууд дараах зүйлийг баталгаажуулах ёстой:

	a) мэдээллийн аюулгүй байдлын зорилтыг байгууллагын холбогдох чиг үүрэг, түвшинд тогтоосон; b) мэдээллийн аюулгүй байдлын зорилтуудыг тэдгээрийн хэрэгжилтийг тодорхойлох боломжтой байдлаар тодорхойлсон; c) хэрэв боломжтой бол зорилтуудыг хэмжих боломжтой (мэдээллийн аюулгүй байдлын зорилтыг хэмжих боломжгүй нөхцөл байдал байж болно); d) мэдээллийн аюулгүй байдлын зорилт, түүнд хүрэх төлөвлөгөөний байдал, ахиц дэвшлийг хяналт-шинжилгээ, хэмжилт, дүн шинжилгээ, үнэлгээний шаардлагын дагуу үе үе шалгаж (ISO/IEC 27001:2013, 9.1) шаардлагатай бол тасралтгүй сайжруулах (ISO/IEC 27001:2013, 10.2) шаардлагад нийцүүлэн шинэчилж байх e) мэдээллийн аюулгүй байдлын зорилтууд, түүнд хүрэх төлөвлөгөөг харилцаа холбооны шаардлагын дагуу мэдээлэх (ISO/IEC 27001:2013, 7.4); f) зорилтуудын баримтжуулсан мэдээллийг баримтжуулсан мэдээллийн шаардлагын дагуу үүсгэж, хянадаг (ISO/IEC 27001:2013, 7.5). Аудиторууд мөн дараах зүйлийг баталгаажуулах ёстой. Үүнд: a) мэдээллийн аюулгүй байдлын зорилгод хүрэхэд шаардагдах арга хэмжээ (жишээ нь "юу") болон холбогдох хугацааг (жишээ нь "хэзээ") тодорхойлсон; b) байгууллагын үүрэг, хариуцлага, эрх мэдлийн шаардлагын дагуу (ISO/IEC 27001:2013, 5.3) үүнийг

	хийх хариуцлагын хуваарилалт (өөрөөр хэлбэл "хэн") тогтоогдсон; c) мэдээллийн аюулгүй байдлын холбогдох шаардлагууд, эрсдэлийн үнэлгээ, эрсдлийн эмчилгээний үр дүнг зорилго, түүнд хүрэх төлөвлөлтөд харгалзан үзсэн; d) зорилгодоо хүрэхийн тулд төсөв, тусгай ур чадвар, технологи, дэд бүтцийн аливаа хэрэгцээг нөөцийн шаардлагын дагуу тодорхойлох (ISO/IEC 27001:2013, 7.1); e) хийж гүйцэтгэсэн ажлын ерөнхий үр дүнг үнэлэх механизмыг хяналт-шинжилгээ, хэмжилт, дүн шинжилгээ, үнэлгээний шаардлагын дагуу (ISO/IEC 27001:2013, 9.1) тодорхойлж, удирдлагын үнэлгээний дагуу тайлагнана (ISO/IEC 27001). :2013, 9.3).
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO/IEC 27003:2017, 6.2 A.4
A.4 Дэмжлэг (ISO/IEC 27001:2013, 7-р зүйл)	
A.4.1 Нөөцүүд (ISO/IEC 27001:2013, 7.1)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 5.1, 6.2, 7.2
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Байнгын сайжруулалт, удирдлагын тогтолцоо
Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээлэл эсвэл байгууллагад шаардлагатай нөөцийн талаарх бусад мэдээллээр олж авч болно. Үүнд:

	a) МАБУТ-ийг (түүний үйл ажиллагаа, хяналтыг оруулаад) бий болгох, хэрэгжүүлэх; b) МАБУТ-ийг хадгалах, байнга сайжруулах. Нөөцүүд нь дараах зүйлийг агуулж болно. a) ажилтнууд; b) тусгай ур чадвар, мэдлэг; c) байгууллагын дэд бүтэц (жишээлбэл, барилга байгууламж, холбооны шугам гэх мэт); d) технологи; e) мэдээлэл, мэдээлэл, мэдээлэл боловсруулах хэрэгсэлтэй холбоотой бусад хөрөнгө; f) мөнгө (жишээлбэл, бэлэн мөнгө, хөрвөх чадвартай үнэт цаас, зээлийн шугам).
Аудитын практик гарын авлага	Байгууллага нь МАБУТ-г бий болгох, хэрэгжүүлэхэд шаардагдах нөөцийг (түүний үйл ажиллагаа, хяналтыг оруулаад), түүнчлэн түүнийг засварлах, тасралтгүй сайжруулахад шаардлагатай нөөцийг урьдчилан харж, тодорхойлж, хуваарилж байгааг аудиторууд баталгаажуулах ёстой.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 4.3.5
A.4.2 Чадамж (ISO/IEC 27001:2011, 7.2)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 5.3, 7.1, 7.5.1 Тайлбар, 9.1 d) ба e), 9.2 e)

Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Чадамж, үр дүнтэй байдал
Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээллээр болон бусад мэдээллээр олж авч болно холбогдох мэдээлэл: a) байгууллагын үүрэг, хариуцлага, эрх мэдэл; b) ажлын байрны тодорхойлолт; c) шаардлагатай ур чадвар; d) боловсролын бүртгэл; e) сургалтын хөтөлбөр, курс, боловсролын үйл ажиллагаа; f) шаардлагатай ур чадварыг олж авах, хадгалахын тулд хийсэн үйл ажиллагааны бүртгэл; g) тэдгээрийн үр нөлөөг үнэлэх. ISO/IEC 27001:2013, 7.2 нь чадамжийн хамрах хүрээг байгууллагын гишүүн бус хүмүүсээр өргөжүүлсэн. Уг шаардлагад “байгууллагын хяналтан дор ажиллаж байна” гэж заасан. Жишээ нь энд туслан гүйцэтгэгч болон сайн дурын ажилчдыг оруулж болно. Гуравдагч этгээдээс хүссэн аудитын нотлох баримтууд нь МАБУТ-ийн байгууллагад гүйцэтгэсэн чиг үүрэг, үйл ажиллагааны нотлох баримтаар хязгаарлагдах ёстой.
Аудитын практик гарын авлага	Аудиторууд байгууллага нь дараах зүйлийг баталгаажуулах ёстой. a) тодорхойлдоо:

	1) мэдээллийн аюулгүй байдлын гүйцэтгэлд нөлөөлж буй түүний хяналтан дор ажил хийж байгаа хүмүүс; 2) хүссэн үр дүнд хүрэх хүмүүсийн мэдлэг, ур чадвар; 3) хүссэн үр дүнд хүрэхийн тулд хүмүүсийн мэдлэг, ур чадвараа ашиглах чадвар; b) эдгээр хүмүүсийг зохих боловсрол, сургалт, туршлагын үндсэн дээр чадвартай байлгах; c) шаардлагатай бол шаардлагатай чадварыг олж авах арга хэмжээ авч, авсан арга хэмжээний үр нөлөөг үнэлэх.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO/IEC 27003:2017, 7.2 ISO/IEC 27021:2017, Хавсралт А
А.4.3 Мэдэж байх зүйлс (ISO/IEC 27001:2013, 7.3)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 5.1 d), 5.2, 9.1, 9.2, 10.1, 10.2
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Тохиромжтой байдал, үр дүнтэй байдал, гүйцэтгэл, бодлого
Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно: a) мэдээллийн аюулгүй байдлын бодлого; b) мэдээллийн аюулгүй байдлын зорилтууд; c) мэдээллийн аюулгүй байдлын гүйцэтгэл; d) үл тохирол, залруулах арга хэмжээ; e) байгууллагын үүрэг, хариуцлага, эрх мэдэл; f) ажлын байрны тодорхойлолт;

	g) боломжтой бол мэдлэг олгох хөтөлбөр, сургалтын материал.
Аудитын практик гарын авлага	Аудиторууд байгууллагын хяналтан дор ажил хийж байгаа хүмүүс дараахь зүйлийг мэдэж байгааг баталгаажуулах ёстой. Үүнд: a) мэдээллийн аюулгүй байдлын бодлого; b) мэдээллийн аюулгүй байдлын гүйцэтгэлийг сайжруулахын үр өгөөжийг багтаасан МАБУТ-ийн үр ашгийг дээшлүүлэхэд оруулсан хувь нэмэр; c) МАБУТ-ийн шаардлагад нийцэхгүй байгаагийн үр дагавар. Аудиторууд эдгээр мэдээллийн талаар мэдэж байгаа эсэхийг баталгаажуулахын тулд түүвэрлэлтийн хувьд зохих тооны хүмүүстэй ярилцлага хийх ёстой. Бодлогын талаар мэдлэгтэй байх нь түүнийг цээжлэх шаардлагатай гэж ойлгож болохгүй. Харин хүмүүс бодлогын үндсэн амлалтууд, түүнийг хэрэгжүүлэхэд гүйцэтгэх үүргийн талаар мэддэг байх ёстой. Аудиторууд мэдээллийн аюулгүй байдлын талаарх мэдлэгийн нотолгоог мэдээллийн аюулгүй байдалд зориулагдаагүй мэдлэг, сургалтын санаачлагуудаас олж болно. Эдгээр үйл ажиллагаа нь дээд удирдлагын харилцааны үйл ажиллагаатай нягт холбоотой байж болно [ISO/IEC 27001:2013, 5.1 d) ба 7.4.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO/IEC 27003:2017, 7.3
A.4.4 Харилцаа холбоо (ISO/IEC 27001:2013, 7.4)	

ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 5.1, 5.2, 5.3, 6.2, 9.2
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Бодлого
Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авах боломжтой. Үүнд: a) мэдээллийн аюулгүй байдлын бодлого; b) байгууллагын үүрэг, хариуцлага, эрх мэдэл; c) мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явц; d) мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх үйл явц; e) мэдээллийн аюулгүй байдлын зорилтууд; f) үйл явц төлөвлөсний дагуу явагдсан тухай мэдээлэл; g) мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үр дүн; h) мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх үйл явцын үр дүн; i) МАБУТ-ийн гүйцэтгэл; j) аудитын үр дүн; k) удирдлагын үнэлгээний үр дүн.
Аудитын практик гарын авлага	Аудиторууд байгууллагын харилцааны хэрэгцээг ISO/IEC 27001 стандартын харилцааны шаардлагын дагуу тодорхойлж, хэрэгжүүлж, үр дүнтэй байлгаж байгаа эсэхийг баталгаажуулах ёстой. Нотлох баримтын жишээнд дараах зүйлийг оруулж болно. Үүнд:

	a) хуралдааны тэмдэглэлд баримтжуулсан хариулт, эсвэл b) албан ёсны харилцааны төлөвлөгөө, баримтжуулсан журам, үр дүн, эсвэл c) Тэд өөрсдийн үүрэг хариуцлагатай холбоотой харилцаа холбооны хувьд юу, хэзээ, хэнтэй харилцах, ийм харилцаа холбоог явуулах эрх мэдэлтэй хүмүүс, харилцаа холбоонд хэрхэн нөлөөлж байгааг мэддэг гэдгийг нь мэдэхийн тулд тодорхой үүрэг хариуцлага хүлээсэн хүмүүстэй ярилцлага хийх. Ийм нотлох баримтыг дараах байдлаар нэмж болно: a) дараах харилцааны мэдээлэл: 1) мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны шаардлагад нийцүүлэх, мэдээллийн аюулгүй байдлын үр дүнтэй менежментийн ач холбогдол; 2) бодлого; 3) үүрэг хариуцлага, эрх мэдэл; 4) МАБУТ-ийн гүйцэтгэл; 5) зорилго; 6) МАБУТ-ийн үр ашгийг дээшлүүлэхэд оруулсан хувь нэмэр, түүний дотор гүйцэтгэлийг сайжруулахын ашиг тус; 7) МАБУТ-ийн шаардлагад нийцэхгүй байгаагийн үр дагавар; 8) аудитын үр дүн;

	b) албан ёсны харилцааны төлөвлөгөө, баримтжуулсан журам, үр дүн. Байгууллага нь МАБУТ-тэй холбоотой харилцааны хэрэгцээгээ тодорхойлсон эсэхийг аудиторууд шалгах ёстой. Жишээлбэл, эдгээрт ил тод байдал, зохистой байдал, найдвартай байдал, хариу үйлдэл үзүүлэх чадвар, ойлгомжтой байдал, хамгаалалт багтаж болно. Харилцаа нь аман болон бичгийн, нэг талын эсвэл хоёр талын, дотоод болон гадаад байж болно.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 4.3.6, 4.3.7 ISO/IEC 27003:2017, 7.4
A.4.5 Баримтжуулсан мэдээлэл (ISO/IEC 27001:2013, 7.5)	
A.4.5.1 Ерөнхий (ISO/IEC 27001:2013, 7.5.1)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 4.3, 5.2 e), 6.1.2, 6.1.3, 6.2, 7.2 d), 8.1, 8.2, 8.3, 9.1, 9.2 g), 9.3, 10.1
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Баримтжуулсан мэдээлэл
Аудитын нотлох баримт	Аудитын нотлох баримтыг МАБУТ-д бий болгосон, хянагддаг ба/эсвэл хадгалсан баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно. Үүнд: a) удирдлагын тогтолцооны хамрах хүрээ; b) бодлого; c) зорилго; d) ур чадварын нотлох баримт; e) удирдлагын тогтолцоог төлөвлөх, ажиллуулахад шаардлагатай гадаад гарал үүслийн мэдээлэл;

	f) мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явц; g) мэдээллийн аюулгүй байдлын эрсдлийг эмчлэх үйл явц; h) Хэрэглэх боломжтой байдлын мэдэгдэл; i) үйл явц, тогтоосон хяналтыг төлөвлөсний дагуу гүйцэтгэсэн гэдэгт итгэлтэй байх шаардлагатай мэдээлэл; j) мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үр дүн; k) мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх ажлын үр дүн; l) хяналт-шинжилгээ, хэмжилт, шинжилгээ, үнэлгээний үр дүн; m) дотоод аудитын хөтөлбөр, түүний хэрэгжилтийг нотлох баримт; n) дотоод аудитын үр дүн; o) удирдлагын хяналт үнэлгээний үр дүн; p) үл тохирлын шинж чанар, авсан арга хэмжээ; q) залруулах арга хэмжээний үр дүн. ISO/IEC 27001 стандартын шаардлагыг биелүүлэхээс өөр зорилгоор анх үүсгэсэн баримтжуулсан мэдээллийг ашиглаж болно.
Аудитын практик гарын авлага	Аудиторуудбайгууллагын МАБУТ нь дараахь зүйлийг агуулж байгааг батлах ёстой.

	а) ISO/IEC 27001 стандартад заасан баримтжуулсан мэдээлэл; б) МАБУТ-г үр дүнтэй болгоход шаардлагатай гэж байгууллагаас тодорхойлсон баримтжуулсан мэдээлэл. Энд "..."-ын нотлох баримт болгон баримтжуулсан мэдээлэл" гэсэн хэллэг нь өмнөх "бичлэг" гэсэн нэр томъёог илэрхийлдэг. Аудиторууд байгууллага нь МАБУТ-г үр дүнтэй байлгахын тулд ISO/IEC 27001-д зааснаас гадна өөрт нь ямар баримтжуулсан мэдээлэл шаардлагатайг тодорхойлж байгааг баталгаажуулах ёстой. Үүнд анхаарах ёстой хүчин зүйлсийг аудитын нотлох баримтын эгнээнд жагсаасан болно. “Баримтжуулсан мэдээлэл” гэсэн нэр томъёо нь ISO/IEC 27001 стандартын дагуу аливаа хэлбэр, мэдээллийн хэрэгслээр хянах, хадгалахад шаардлагатай гэж тодорхойлсон мэдээллийг хэлнэ (ISO/IEC 27001:2013, 7.5.3-ыг үзнэ үү). Аудитор нь баримтжуулсан мэдээллийг ISO/IEC 27001:2013, 7.5.2, 7.5.3-ын шаардлагын дагуу үүсгэж, хянаж байгааг баталгаажуулах ёстой.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 5.7 ISO/IEC 27003:2017, 7.5.1
A.4.5.2 Үүсгэх, шинэчлэх (ISO/IEC 27001:2013, 7.5.2)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 4.3, 5.2 e), 6.1.2, 6.1.3, 6.2, 7.2 d), 8.1, 8.2, 8.3, 9.1, 9.2 g), 9.3, 10.1

Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Баримтжуулсан мэдээлэл
Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно: a) тодорхой бөгөөд өвөрмөц таних боломжийг олгодог нийтлэг шинж чанарууд; b) ашигласан хэлбэр, зөөвөрлөгч; c) хамгийн сүүлд хянан шалгах буюу шинэчлэх огноо; d) өөрчлөлтийн түүх; e) хянагч ба зөвшөөрөгчийн нэр.
Аудитын практик гарын авлага	Аудиторууд баримтжуулсан мэдээллийг бий болгож, шинэчлэхдээ тухайн байгууллага дараах зүйлийг зохих ёсоор мөрдсөн эсэхийг баталгаажуулах ёстой: a) таних тэмдэг, тодорхойлолт (жишээ нь гарчиг, огноо, зохиогч эсвэл лавлагааны дугаар); b) формат (жишээ нь хэл, програм хангамжийн хувилбар, график) болон зөөвөрлөгч (жишээ нь цаасан, цахим); c) баримтжуулсан мэдээлэлд тохирох, хангалттай эсэхийг хянаж, батлах. ТАЙЛБАР 13: Баримтжуулсан мэдээлэлд ашигласан таних тэмдэг, хэлбэр, зөөвөрлөгч нь ISO/IEC 27001 стандартыг хэрэгжүүлэгч байгууллагын сонголт юм; Энэ нь текст хэлбэрээр эсвэл цаасан гарын авлага хэлбэрээр байх шаардлагагүй.

	Аудиторууд МАБУТ-ны хүрээнд баримтжуулсан мэдээллийг аудитад танилцуулах бүрд эдгээр аудитын ажлыг гүйцэтгэх боломжийг ашиглах ёстой. Тэдгээрийг нэг бүрчлэн хийх шаардлагагүй, зөвхөн ISO/IEC 27001:2013, 7.5.2-д нийцэж байгааг батлахад хангалттай.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO/IEC 27003:2017, 7.5.2
A.4.5.3 Баримтжуулсан мэдээллийн хяналт (ISO/IEC 27001:2013, 7.5.3)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 4.3, 5.2 e), 6.1.2, 6.1.3, 6.2, 7.2 d), 8.1, 8.2, 8.3, 9.1, 9.2 g), 9.3, 10.1
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Баримтжуулсан мэдээлэл
Аудитын нотлох баримт	Аудитын нотлох баримтыг дараахь үйл ажиллагааны талаархи баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно: a) түгээх, хандах, хайх, ашиглах; b) хадгалалт, хадгалалт, түүний дотор унших боломжтой байдлыг хадгалах; c) өөрчлөлтийг хянах (жишээ нь, хувилбарын хяналт); d) хадгалах, захиран зарцуулах; e) баримтжуулсан мэдээллийн номын сангийн бүтэц, тохиргоо.
Аудитын практик гарын авлага	Аудиторууд МАБУТ болон ISO/IEC 27001-д заасан баримтжуулсан мэдээлэл нь дараах зүйлийг баталгаажуулахын тулд хянагдаж байгааг үзэх ёстой:

	a) хаана болон хэзээ шаардлагатай үед үүнийг ашиглах боломжтой, ашиглахад тохиромжтой гэдгийг b) зохих ёсоор хамгаалагдсан эсэхийг (жишээ нь, нууцлалыг алдагдуулах, зүй бусаар ашиглах, бүрэн бүтэн байдлыг алдагдуулах гэх мэт). Аудитор нь тухайн байгууллага шаардлагатай бол дараах үйл ажиллагаа явуулж байгааг баталгаажуулах ёстой. Үүнд: a) түгээх, хандах, хайх, ашиглах; b) хадгалалт, хадгалалт, түүний дотор унших боломжтой байдлыг хадгалах (дижитал болон бусад хэлбэрээр эсвэл гараар бичсэн); c) өөрчлөлтийг хянах (жишээ нь, хувилбарын хяналт); d) хадгалах ба захиран зарцуулах. Аудиторууд МАБУТ-ны хүрээнд баримтжуулсан мэдээллийг аудитад танилцуулах бүрт эдгээр аудитын ажлыг гүйцэтгэх боломжийг ашиглах ёстой. Тэдгээрийг нэг бүрчлэн хийх шаардлагагүй, зөвхөн ISO/IEC 27001:2013, 7.5.3-д нийцэж байгааг батлахад хангалттай тоо байна.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 5.7 ISO/IEC 27003:2017, 7.5.3
A.5 Үйл ажиллагаа (ISO/IEC 27001:2013, 8-р зүйл)	
A.5.1 Үйл ажиллагааны төлөвлөлт ба хяналт (ISO/IEC 27001:2013, 8.1)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 4.4, 6.1.1, 6.1.2, 6.1.3, 6.2, 7.5.1, 9.1, 9.2

Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Үр дагавар, мэдээллийн аюулгүй байдал, зорилго, зохион байгуулалт, аутсорсинг, үйл явц, шаардлага
Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно. Үүнд: a) Байгууллагад үйл ажиллагааны хяналтын үйл явц төлөвлөсний дагуу хийгдсэн гэдэгт итгэлтэй байх шаардлагатай (ISO/IEC 27001:2013, 8.1); b) МБОУС-ыг үр дүнтэй болгоход шаардлагатай гэж байгууллагаас тогтоосон [ISO/IEC 27001:2013, 7.5.1 b)]; c) ISO/IEC 27001:2013, 6.1.1-ийн зааснаар МАБУТ-ийн төлөвлөлтийн тухай; d) мэдээллийн аюулгүй байдлын зорилтуудын тухай (ISO/IEC 27001:2013, 6.2).
Аудитын практик гарын авлага	Тухайн байгууллага нь ISO/IEC 27001 стандартын шаардлагыг хангаж, тэргүүлэх эрсдэл, боломжуудыг шийдвэрлэхийн тулд байгууллагын үйл ажиллагааны хүрээнд мэдээллийн аюулгүй байдлын шаардлагыг хангахад шаардлагатай үйл явцыг төлөвлөж, хэрэгжүүлж, хянаж байгааг аудиторууд баталгаажуулах ёстой. Аудиторууд байгууллагын үйл ажиллагааны хяналт нь бизнесийн үйл ажиллагаа, үйл ажиллагаа эсвэл тоног төхөөрөмж нь тогтоосон нөхцөл, гүйцэтгэлийн стандарт эсвэл зохицуулалтын нийцлийн хязгаарт нийцэж байгаа эсэхийг баталгаажуулах арга, мэдээллийн аюулгүй байдлын хяналтыг багтаасан болохыг баталгаажуулна. Эдгээр хяналтууд нь техникийн үзүүлэлтүүд эсвэл үйл ажиллагааны параметрүүд эсвэл тогтоосон аргачлал зэрэг бизнесийн үйл явцын хүссэн оновчтой ажиллагааг хангахад

	шаардлагатай техникийн шаардлагыг тогтоодог. Үйл ажиллагааны хяналт, мэдээллийн аюулгүй байдлын хяналт байхгүй байх нь бодлого, зорилтоос хазайхад хүргэж болзошгүй эсвэл хүлээн зөвшөөрөгдөөгүй эрсдэл үүсгэж болзошгүй бизнесийн үйл явцтай холбоотой үйл ажиллагааны хяналт, мэдээллийн аюулгүй байдлын хяналт шаардлагатай нөхцөл байдалд хяналт шалгалт хийх ёстой. Эдгээр нөхцөл байдал нь бизнесийн үйл ажиллагаа, үйл ажиллагаа, үйл явц, үйлдвэрлэл, суурилуулалт, үйлчилгээ, засвар үйлчилгээ эсвэл гүйцэтгэгч, ханган нийлүүлэгч эсвэл борлуулагчидтай холбоотой байж болно. Хяналтын түвшин нь гүйцэтгэсэн чиг үүрэг, тэдгээрийн ач холбогдол, нарийн төвөгтэй байдал, хазайлт, хэлбэлзлийн болзошгүй үр дагавар эсвэл байгаа техникийн ур чадвар зэрэг олон хүчин зүйлээс хамаарч өөр өөр байх болно. Аудиторууд байгууллага нь дараах зүйлийг хийснийг баталгаажуулах ёстой. Үүнд: a) “Эрсдэл, боломжийг шийдвэрлэх арга хэмжээ” (ISO/IEC 27001:2013, 6.1)-д тодорхойлсон арга хэмжээг хэрэгжүүлнэ; b) Мэдээллийн аюулгүй байдлын зорилтуудад тодорхойлсон мэдээллийн аюулгүй байдлын зорилтод хүрэх төлөвлөгөө, түүнд хүрэх төлөвлөлтийг хэрэгжүүлэх (ISO/IEC 27001:2013, 6.2); c) үйл ажиллагааны хяналтын үйл явц болон мэдээллийн аюулгүй байдлын хяналтыг баримтжуулсан мэдээллийн шаардлагын дагуу төлөвлөсний дагуу гүйцэтгэсэн гэдэгт итгэлтэй байхын тулд шаардлагатай баримт бичгийг бүрдүүлж, хянадаг (ISO/IEC 27001:2013, 7.5) эсэх;

	d) техникийн шаардлагыг биелүүлэхгүй байх эсвэл шинэ эрсдэл үүсэхээс урьдчилан сэргийлэх, эсвэл өөр аргаар багасгахын тулд төлөвлөсөн өөрчлөлтийг хянаж, төлөвлөөгүй өөрчлөлтийн үр дагаврыг хянан үзэх; e) үйл ажиллагааны хяналт амжилтгүй болсон үед үүсэх аливаа хүсээгүй үр нөлөөг арилгахад шаардлагатай арга хэмжээ авах; f) аутсорсингийн үйл явцыг тодорхойлж, хянаж байгаа эсэхийг баталгаажуулах, өөрөөр хэлбэл хяналтын зэрэг нь хэсэгчилсэн хяналт эсвэл нөлөөлөлөөр хязгаарлагдах боломжтой бөгөөд аутсорсингийн үйл явцыг гүйцэтгэж буй гадны байгууллагатай ямар нэгэн эрх зүйн харилцааг өөрчлөх зорилгогүй байхаар авч үзэж байгаа үйл ажиллагааны хяналтыг хэрэгжүүлэх; .
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO/IEC 27003:2017, 8.1
A.5.2 Мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээ (ISO/IEC 27001:2013, 8.2)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 6.1.2
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Мэдээллийн аюулгүй байдал
Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно: a) МАБУТ-ны төлөвлөлт (ISO/IEC 27001:2013, 6.1.1);

	b) мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явц (ISO/IEC 27001:2013, 6.1.2); c) мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үр дүн (ISO/IEC 27001:2013, 8.2); d) хэрэглэх боломжтой байдлын мэдэгдэл; e) эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөө.
Аудитын практик гарын авлага	Аудиторууд (ISO/IEC 27001:2013, 6.1)-д тодорхойлсон мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний үйл явц хэрэгжиж, байгууллагын үйл ажиллагаатай уялдан нэгтгэгдэж, эдгээр нь төлөвлөсөн хугацаанд эсвэл томоохон өөрчлөлт санал болгож буй үед эсвэл өөрчлөлт гарах үед ISO/IEC 27001:2013, 6.1.2 а)-д заасан шалгууруудын дагуу гүйцэтгэснийг баталгаажуулах ёстой. Аудиторууд дараахь зүйлийг үнэлэх ёстой. a) эрсдэлийн үнэлгээ хийхээр төлөвлөсөн хугацааны интервалууд нь МАБУТ-д тохирсон байх; b) МАБУТ (эсвэл түүний нөхцөл байдал)-д мэдэгдэхүйц өөрчлөлт гарсан эсвэл мэдээллийн аюулгүй байдлын осол гарсан тохиолдолд байгууллага нь эдгээр өөрчлөлт, ослын алинд нь мэдээллийн аюулгүй байдлын эрсдлийн нэмэлт үнэлгээ шаардлагатайг, эдгээр үнэлгээг хэрхэн хийгдэж байгааг тодорхойлдог. Нэмэлт мэдээллийг А.3.1.2-ын аудитын практик гарын авлагаас үзнэ үү.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 5.4.1 ISO/IEC 27003:2017, 8.2 ISO/IEC 27005

A.5.3 Мэдээллийн аюулгүй байдлын эрсдэлийн асуудлыг шийдвэрлэх (ISO/IEC 27001:2013, 8.3)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 6.1.3, Хавсралт А
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Хяналт, хяналтын зорилго, баримтжуулсан мэдээлэл, мэдээллийн аюулгүй байдал, үлдэгдэл эрсдэл, эрсдлийн үнэлгээ, эрсдэлийн шалгуур, эрсдэл хүлээгч, эрсдэлийн асуудлыг шийдвэрлэх
Аудитын нотлох баримт	Аудитын нотлох баримтыг дараах баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно: a) МАБУТ-ийн төлөвлөлт; b) мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх үйл явц; c) эрсдлийн асуудлыг шийдвэрлэх төлөвлөгөө; d) мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх явцын үр дүн; e) хэрэглэх боломжтой байдлын мэдэгдэл.
Аудитын практик гарын авлага	Аудиторууд мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний давталт бүрийн дараа "ISO/IEC 27001:2013, 6.1"-д тодорхойлсон мэдээллийн аюулгүй байдлын эрсдлийн асуудлыг шийдвэрлэх үйл явц хэрэгжсэн эсвэл эрсдэлийн асуудлыг шийдвэрлэх явцын хэрэгжилт амжилтгүй болсон үед энэ нь байгууллагын үйл ажиллагаанд уялдуулан нэгтгэгдсэн эсэхийг баталгаажуулах ёстой. Нэмэлт мэдээллийг А.3.1.3 дахь аудитын практик гарын авлагаас үзнэ үү.

Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO 31000:2018, 5.5 ISO/IEC 27003:2017, 8.3 ISO/IEC 27005
A.6 Гүйцэтгэлийн үнэлгээ (ISO/IEC 27001:2013, 9-р зүйл)	
A.6.1 Хяналт, хэмжилт, дүн шинжилгээ, үнэлгээ (ISO/IEC 27001:2013, 9.1)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 5.3 b), 6.1.1 e), 6.2
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Тасралтгүй сайжруулалт, үр нөлөө, хэмжилт, мониторинг, гүйцэтгэл, мэдээллийн аюулгүй байдлын үйл явдал, мэдээллийн аюулгүй байдлын будлиан, мэдээллийн хэрэгцээ, хэмжүүр
Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээлэл эсвэл хяналт, хэмжилт, дүн шинжилгээ, үнэлгээний үр дүнгийн талаарх бусад мэдээллээр олж авч болно (ISO/IEC 27001:2013, 9.1-ийг үзнэ үү). Мөн дараах баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр нотлох баримтыг авч болно: a) холбогдох чиг үүрэг, түвшний мэдээллийн аюулгүй байдлын зорилтууд; b) мэдээллийн аюулгүй байдлын зорилгод хэрхэн хүрэхийг төлөвлөх; c) мэдээллийн аюулгүй байдлын зорилтуудын хэрэгжилтийн байдал, хэмжээ; d) МАБУТ-ны гүйцэтгэлийн талаар дээд удирдлагад тайлагнасан байдал [ISO/IEC 27001:2013, 5.3 б-г үзнэ үү]]; e) эрсдэлийн үнэлгээний үр дүн, эрсдэлийн асуудлыг шийдвэрлэх төлөвлөгөөний төлөв байдал;

	f) хяналт-шинжилгээ, хэмжилт, дүн шинжилгээ, үнэлгээ хийх арга; g) дотоод аудитын хөтөлбөр(үүд) ба аудитын үр дүн; h) удирдлагын үнэлгээ(үүд) болон удирдлагын үнэлгээний үр дүн; i) мэдээллийн аюулгүй байдлын үйл явдлын тайлан (ISO/IEC 27001:2013, A.16.1.2-ыг үзнэ үү); j) мэдээллийн аюулгүй байдлын сул талуудын тайлан (ISO/IEC 27001:2013, A.16.1.3-ыг үзнэ үү); k) мэдээллийн аюулгүй байдлын будлианы тайлан (ISO/IEC 27001:2013, A.16.1.4-ийг үзнэ үү).
Аудитын практик гарын авлага	Аудиторууд байгууллагын дараах зүйлийг шалгаж баталгаажуулах ёстой. Үүнд: a) мэдээллийн аюулгүй байдлын гүйцэтгэл, МАБУТ-ны үр нөлөөг үнэлсэн; b) Мөн дараах зүйлээр тодорхойлсон: 1) юуг хянах, хэмжих (чанарын болон тоон), үүнд мэдээллийн аюулгүй байдлын үйл явц, хяналт; 2) хүчинтэй үр дүнг баталгаажуулахын тулд хяналт, хэмжилт, дүн шинжилгээ, үнэлгээний аргууд; 3) хяналт-шинжилгээ, хэмжилт хийх үед; 4) хяналт-шинжилгээ, хэмжилтийг хэн гүйцэтгэдэг; 5) хяналт-шинжилгээ, хэмжилтийн үр дүнд дүн шинжилгээ хийх, үнэлэх үед; 6) эдгээр үр дүнгийн дүн шинжилгээ, үнэлгээг хэн хийдэг.

	Аудиторууд мэдээллийн аюулгүй байдлын гүйцэтгэлийг баримтжуулсан мэдээлэл, тухайлбал төлөвлөгөө, МАБУТ-ны гүйцэтгэлийн талаар дээд удирдлагад өгсөн тайлан, удирдлагын шалгалтын үр дүн, дотоод аудитын тайлан, мэдээллийн аюулгүй байдлын үйл явдал, сул талуудын тохиолдлын тайлан зэрэг нотлох баримтуудыг ашиглан хянан шалгах ёстой. Аудиторууд үл тохирол, боловсруулалтын алдаа, мэдээллийн аюулгүй байдлын будлиан болон бусад тохиолдлуудыг урьдчилан таамаглах, илрүүлэх, мэдээлэх, шийдвэрлэх арга хэмжээг үнэлэх ёстой. Аудиторууд тухайн байгууллага эрсдэлийг арилгах арга хэмжээний үр нөлөөг хэрхэн үнэлж байгаа эсэх, эрсдлийн асуудлыг шийдвэрлэхэд тодорхойлсон мэдээллийн аюулгүй байдлын хяналтыг үр дүнтэй хэрэгжүүлж, ажиллаж байгаа эсэхийг тодорхойлох ёстой. Аудиторууд мэдээллийн аюулгүй байдлын гүйцэтгэлийн үнэлгээг мөн МАБУТ-ийг тасралтгүй сайжруулахад ашиглаж байгаа эсэхийг үнэлэх ёстой. Аудиторууд үр дүнгийн дагуу анхаарах ёстой өөрчлөлтүүд (ISO/IEC 27001:2013, 8.1 ба 8.2) эрсдэлийн үнэлгээ болон эрсдэлийг арилгах үйл явцад тусгагдсан болохыг баталгаажуулах ёстой. Түүнчлэн аудиторууд эрсдэл, боломжуудыг шийдвэрлэх арга хэмжээнүүдтэй холбоотой баримтжуулсан мэдээлэл шинэчлэгдсэнийг баталгаажуулах ёстой. Аудиторууд хянаж, хэмжиж, дүн шинжилгээ хийж, үнэлдэг шинж чанаруудын мэдээлэл нь МАБУТ-ны төлөвлөсөн үйл ажиллагаа хэр зэрэг хэрэгжиж, төлөвлөсөн үр дүндээ хүрч байгааг дүгнэхэд шаардлагатай бөгөөд хангалттай эсэхийг шалгах ёстой. Аудиторууд хяналт-шинжилгээ, хэмжилт, дүн шинжилгээ, үнэлгээний үр дүнд олж авсан мэдээллийг

	удирдлагын хяналтын шаардлагын (ISO/IEC 27001:2013, 9.3) дагуу дээд удирдлагад танилцуулж байгааг баталгаажуулах ёстой. ТАЙЛБАР 14: Хэрэв байгууллага ISO/IEC 27004 стандартад заасан зааврыг дагаж мөрдвөл "мэдээллийн хэрэгцээ"-ээс гадна "гүйцэтгэлийн хэмжүүр" болон "үр ашгийн хэмжүүр" гэсэн нэр томъёог ашиглаж болно.
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	ISO/IEC 27004
A.6.2 Дотоод аудит (ISO/IEC 27001:2013, 9.2)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 9.3
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Аудит, аудитын хамрах хүрээ, чадамж
Аудитын нотлох баримт	Аудитын нотлох баримтыг дараах баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно: a) дотоод аудитын хөтөлбөр(үүд); b) дотоод аудитын төлөвлөгөө; c) дотоод аудитын үр дүн; d) дотоод аудиторуудын ур чадвар; e) удирдлагын хяналт үнэлгээний үр дүн.
Аудитын практик гарын авлага	ТАЙЛБАР 15: Энэхүү дэд зүйл нь дотоод аудитын талаарх хөндлөнгийн аудит эсвэл өөрийгөө шалгах эсвэл харилцан бие биенээ харилцан үнэлэх үнэлгээний удирдамжийг агуулна.

	Тухайн байгууллагын МАБУТ нь ISO/IEC 27001 стандартын шаардлага болон МАБУТ-тай холбоотой нэмэлт шаардлагуудын аль алинд нь нийцэж байгаа эсэх талаар мэдээлэл өгөх зорилгоор дотоод аудитын хөтөлбөрийг төлөвлөгөөнийхөө дагуу төлөвлөж, хэрэгжүүлж, хөтөлж байгааг аудиторууд баталгаажуулах ёстой. Дотоод аудитын хөтөлбөр нь дараах байдалтай байгаа эсэхийг аудиторууд шалгах ёстой. Үүнд: a) аудит хийсэн үйл явцын ач холбогдол, өмнөх аудитын үр дүнд үндэслэн дотоод аудитыг төлөвлөдөг; b) дотоод аудитыг төлөвлөх, явуулах арга барилыг тогтоосон; c) дотоод аудитын үйл явцын бүрэн бүтэн байдал, хараат бус байдлыг харгалзан аудитын хөтөлбөрийн хүрээнд үүрэг, хариуцлагыг хуваарилах; d) төлөвлөсөн аудит бүрийн зорилго, аудитын шалгуур, аудитын хамрах хүрээг тогтоосон; e) МАБУТ нь дараах зүйлд нийцэж байгааг баталгаажуулах мэдээллээр хангах зорилготой юм: 1) ISO/IEC 27001 стандартын шаардлага; 2) байгууллагын өөрийн шаардлага; f) энэ нь МАБУТ-г үр дүнтэй хэрэгжүүлж байгааг баталгаажуулах мэдээллээр хангах зорилготой юм.

	Аудитын шалгуурын жишээ бол холбогдох баталгаажуулах боломжтой бүртгэл, баримтын мэдэгдэл эсвэл бусад мэдээллийг харьцуулах лавлагаа (жишээ нь, бодлого, журам, шаардлага) юм. Аудитын хамрах хүрээ нь бодит байршил, зохион байгуулалтын нэгж, үйл ажиллагаа, үйл явцын тодорхойлолт, түүнчлэн холбогдох аудитад хамрагдсан хугацааг багтааж болно. Дотоод аудитын хөтөлбөр, аудитыг дотоод ажилтнууд төлөвлөж, хэрэгжүүлдэг, эсвэл байгууллагын нэрийн өмнөөс ажилладаг гадны хүмүүс удирддаг гэдгийг аудиторууд батлах ёстой. Аль ч тохиолдолд аудиторууд дотоод аудитын хөтөлбөрийг удирдах үүрэгтэй хүмүүс болон дотоод аудитыг явуулж буй аудиторуудыг сонгох нь ур чадвар (ISO/IEC 27001:2013, 7.2 ба 9.2-ыг үзнэ үү), шаардлага, 27001:2013, 7.2) удирдамжид (ISO/IEC-ийг үзнэ үү) нийцэж байгааг баталгаажуулах ёстой. Аудиторууд дотоод аудитын үр дүнг харилцааны шаардлагын дагуу аудит хийлгэсэн чиг үүрэг/нэгж хариуцсан удирдлага болон зохих гэж үзсэн бусад хүмүүст тайлагнаж байгааг баталгаажуулах ёстой (ISO/IEC 27001:2013, 7.4). Аудиторууд дотоод аудитын үр дүнгийн талаарх мэдээлэл, чиг хандлагыг удирдлагын үнэлгээний шаардлагын дагуу хянаж байгааг баталгаажуулах ёстой (ISO/IEC 27001:2013, 9.3-ыг үзнэ үү).
Дэмжиж байна баримт бичиг	Энэхүү баримт бичиг, тухайлбал ISO/IEC 27007 ISO/IEC TS 27008 ISO/IEC 17021-1:2015, 9.3.1.2.2 g), 9.3.1.3 e), 9.4.8.3 a), 9.6.2.2 a) ISO/IEC 27006:2015, 9.1.5.1, 9.3.1.2.2 h), 9.5.1, 9.6.2.1.1 a)

A.6.3 Удирдлагын хянан шалгалт (ISO/IEC 27001:2013, 9.3)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 4.1, 4.2, 8.1.2, 8.1.3, 9.1, 9.2, 10.1, 10.2
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Байнгын сайжруулалт, үр нөлөө, гүйцэтгэл
Аудитын нотлох баримт	Аудитын нотлох баримтыг дараах баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно: a) төлөвлөгөөт хугацаанд хяналт шалгалт хийх; b) өмнөх удирдлагын үнэлгээний үйл ажиллагааны төлөв байдал; c) МАБУТ-той холбоотой гадаад болон дотоод асуудлын өөрчлөлт; d) мэдээллийн аюулгүй байдлын гүйцэтгэлийн талаархи санал хүсэлт, үүнд үл нийцэл, залруулах арга хэмжээний чиг хандлага, хяналт-шинжилгээ, хэмжилтийн үр дүн, аудитын үр дүн, мэдээллийн аюулгүй байдлын зорилтуудын биелэлт; e) сонирхогч талуудын санал хүсэлт; f) эрсдлийн үнэлгээний үр дүн, эрсдэлийг арилгах төлөвлөгөөний төлөв байдал; g) тасралтгүй сайжруулах боломж.
Аудитын практик гарын авлага	Аудиторууд байгууллагын дээд удирдлага нь төлөвлөсөн хяналт шалгалтын хуваарийн дагуу удирдлагын хяналт шалгалтыг хийж, хамрагдах мэдээллийг хянаж, хүлээгдэж буй үр дүнг хангасан эсэхийг баталгаажуулах ёстой. Аудиторууд МАБУТ-д өөрчлөлт оруулах, байнгын сайжруулалтын тэргүүлэх чиглэл, ялангуяа байгууллагын нөхцөл байдалд өөрчлөгдөж буй асуудлууд, төлөвлөсөн үр

	дүнгээс хазайсан эсвэл ашигтай үр дүн бүхий давуу талыг авч ирэх нөхцөлүүд, таатай нөхцөл байдал зэрэгтэй холбоотой энэхүү механизмыг хэрэгжүүлснээр энэхүү хяналт шалгалтад дээд удирдлага биечлэн оролцож байгаа эсэхийг аудитаар үнэлэх ёстой. Аудиторууд удирдлагын хяналтад A.6.3-д заасан аудитын нотлох баримтад дурдсан b)-ээс g) хүртэлх бүх зүйлийг харгалзан үзсэн эсэхийг шалгах ёстой. Удирдлагын хяналт шалгалтын үр дүнд байнгын сайжруулалт хийх боломжууд болон МАБУТ-д өөрчлөлт оруулах шаардлагатай холбоотой шийдвэрүүд багтсан гэдгийг аудиторууд баталгаажуулах ёстой.
A.7 Сайжруулалт (ISO/IEC 27001:2013, 10-р зүйл)	
A.7.1 Үл тохирол ба залруулах арга хэмжээ (ISO/IEC 27001:2013, 10.1)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 7.5, 8.1, 10.2
Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Залруулга, залруулах арга хэмжээ, үр нөлөө, үл тохирол
Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно: a) үл тохирлын шинж чанар, дараа нь авсан аливаа арга хэмжээ; b) аливаа засч залруулах арга хэмжээний үр дүн; c) хяналт-шинжилгээ, хэмжилтийн үр дүн; d) аудитын хөтөлбөр(үүд) ба аудитын үр дүн; e) удирдлагын шалгалтын үр дүн;

	f) мэдээллийн аюулгүй байдалтай холбоотой сонирхогч талуудын шаардлага; g) залруулах үйл ажиллагаанаас үүдэлтэй МАБУТ-нд гарсан өөрчлөлтүүд.
Аудитын практик гарын авлага	Аудиторууд дараах зүйлийг баталгаажуулах ёстой.Үүнд: a) байгууллага ISO/IEC 27001 болон МАБУТ-ны (үйл ажиллагааны гэх мэт) шаардлагыг хангаагүй тохиолдолд үл тохирол олж, засч залруулах арга хэмжээ авах замаар хариу үйлдэл үзүүлэх; b) үл тохирол болон залруулах арга хэмжээ нь нөхцөл байдлыг засч залруулах арга хэмжээ авах, шалтгааныг судлах, дахин давтагдахаас урьдчилан сэргийлэх арга хэмжээ авах боломжтой бусад тохиолдол байгаа эсэхийг тодорхойлох; c) байгууллагын хариу арга хэмжээ нь төлөвлөсөн үр дүнд хүрсэн эсэхийг баталгаажуулах арга хэмжээний үнэлгээ, ирээдүйд ижил төстэй үл тохирол гарахаас зайлсхийхийн тулд өөрчлөлт оруулах шаардлагатай эсэхийг тодорхойлох МАБУТ-ны үнэлгээг хамарна; d) үл тохирол, залруулах арга хэмжээ, үр дүнгийн баримт бичгийг баримтжуулсан мэдээллийн шаардлагын дагуу бүрдүүлж, хянадаг (ISO/IEC 27001:2013, 7.5-ыг үзнэ үү).
Дэмжих (нэмэлт хэрэгцээтэй) баримт бичиг	
A.7.2 Тасралтгүй сайжруулалт (ISO/IEC 27001:2013, 10.2)	
ISO/IEC 27001-ийн хамаатай заалтууд	ISO/IEC 27001:2013, 5.1, 5.2, 6.1, 6.2, 7.1, 8.1, 9.1, 9.2, 9.3, 10.1

Холбогдох ISO/IEC 27000-ын тодорхойлолтууд	Байнгын сайжруулалт, үр ашиг, гүйцэтгэл
Аудитын нотлох баримт	Аудитын нотлох баримтыг баримтжуулсан мэдээлэл эсвэл бусад мэдээллээр олж авч болно: a) үл тохирлын шинж чанар, дараа нь авсан аливаа арга хэмжээ, түүний дотор засч залруулах арга хэмжээний тухай мэдээлэх; b) аливаа засч залруулах арга хэмжээний үр дүн; c) хяналт-шинжилгээ, хэмжилтийн үр дүн; d) аудитын хөтөлбөр(үүд) ба аудитын үр дүн; e) удирдлагын шалгалтын үр дүн; f) мэдээллийн аюулгүй байдалтай холбоотой сонирхогч талуудын шаардлага; g) мэдээллийн аюулгүй байдлын үйл явдал, будлианы үнэлгээ, шийдвэр (ISO/IEC 27001:2013, A.16.1.4-ийг үзнэ үү).
Аудитын практик гарын авлага	Аудиторууд байгууллага нь МАБУТ-ны зохистой байдал, хүрэлцээтэй байдал, үр дүнтэй байдлын хэмжигдэхүйц үр дүнг сайжруулахын тулд тогтмол үйл ажиллагаагаа явуулж байгааг батлах ёстой. Байгууллагын МАБУТ-ны шаардлагад нийцүүлэх, зорилго, бодлогын амлалтаа биелүүлэх чадварыг сайжруулахын тулд байнгын сайжруулалт нь МАБУТ-ны дизайн, хэрэгжилтэд өөрчлөлт оруулах явдал гэдгийг аудиторууд хянаж, баталгаажуулах ёстой. Аудиторууд байгууллагын дараах зүйлийг аудитаар баталгаажуулах ёстой. Үүнд:

	a) энэхүү сайжруулалтад хүрэхийн тулд дараах хэрэгжүүлэлтийг боловсруулдаг бөгөөд зөвхөн үүгээр хязгаарлагдахгүй: 1) эрсдэл, боломжуудыг шийдвэрлэх арга хэмжээ авах (ISO/IEC 27001:2013, 6.1-ийг үзнэ үү); 2) зорилтуудыг тодорхойлох (ISO/IEC 27001:2013, 6.2-ыг үзнэ үү); 3) шинэ технологи, арга, мэдээллийг харгалзан үйл ажиллагааны хяналтыг сайжруулах (ISO/IEC 27001:2013, 8.1-ийг үзнэ үү); 4) гүйцэтгэлд дүн шинжилгээ хийх, үнэлэх (ISO/IEC 27001:2013, 9.1-ийг үзнэ үү); b) дотоод аудит хийдэг (ISO/IEC 27001:2013, 9.2-ыг үзнэ үү); c) удирдлагын үнэлгээг хийдэг (ISO/IEC 27001:2013, 9.3-ыг үзнэ үү); d) Үл тохирол(ууд)-ыг илрүүлж, засч залруулах арга хэмжээг хэрэгжүүлдэг (ISO/IEC 27001:2013, 10.1-ийг үзнэ үү); e) Эрсдэл, боломжийн зорилтуудыг шийдвэрлэх арга хэмжээ (ISO/IEC 27001:2013, 6.1), түүнд хүрэх төлөвлөлт (ISO/IEC 27001:2013, 6.1), үйл ажиллагааны төлөвлөлт, хяналттай (ISO/IEC 27001:2013, 8.1) уялдуулан сайжруулах боломжуудыг тодорхойлж, зохих арга хэмжээг төлөвлөхийн тулд хяналт-шинжилгээ, хэмжилт, дүн шинжилгээ, үнэлгээ (ISO/IEC 27001:2013, 9.1) болон дотоод аудит (ISO/IEC 27001:2013, 9.2) , удирдлагын хянан шалгалтын (ISO/IEC 27001:2013, 9.3) шаардлагын дагуу МАБУТ-гоо үе үе үнэлж, хянаж байдаг.

Ном зүй

[1] ISO/IEC 17021-1:2015, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

[2] ISO/IEC 17024, *Conformity assessment — General requirements for bodies operating certification of persons*

[3] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[4] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[5] ISO/IEC 27003:2017, *Information technology — Security techniques — Information security management systems — Guidance*

[6] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[7] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[8] ISO/IEC 27006:2015, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[9] ISO/IEC TS 27008, *Information technology — Security techniques — Guidelines for the assessment of information security controls*

[10] ISO/IEC 27021:2017, *Information technology — Security techniques — Competence requirements for information security management systems professionals*

[11] ISO 31000:2018, *Risk management — Guidelines*

[12] IAF MD1, 2018, IAF Mandatory Document for the Audit and Certification of a Management system Operated by Multi-Site Organization, International Accreditation Forum. [viewed 2019-01-01]. Available at https:// www .iaf .nu/ articles/ Mandatory _Documents _/ 38 ©