FINANCIAL INCLUSION
GLOBAL INITIATIVE

Аюулгүй байдал, дэд бүтэц, итгэлцэлийн ажлын хэсэг

ДИЖИТАЛ САНХҮҮГИЙН ҮЙЛЧИЛГЭЭНИЙ АЮУЛГҮЙ БАЙДЛЫН АУДИТЫН УДИРДАМЖ

03/2021

АНХААРУУЛГА

Санхүүгийн үйлчилгээний хүртээмжийг нэмэгдүүлэх олон улсын санаачлага (FIGI)-ын хүрээнд Дэлхийн банк (WBG), Төлбөр тооцоо болон зах зээлийн дэд бүтэцийн хороо (CPMI)-ны хамтарсан 3 жилийн хөтөлбөр юм.

Дэлхий даяарх санхүүгийн үйлчилгээний хүртээмж 2050 үндсэн зорилтод хүрхийн тулд улс орон бүрийн санхүүгийн үйлчилгээний хүртээмжийг нэмэгдүүлэх зорилтод дэмжлэг үзүүлэх зорилгоор Билл ба Мелинда Гейтсийн сан (BMGF), Олон улсын цахилгаан холбооны байгууллага (ITU) хамтран тус арга хэмжээнд дэмлэг туслалцаа үзүүлэн хамтран ажилладаг бөгөөд тус сангаас Бүгд найрамдах Хятад Ард Улс, Египт, Мексик зэрэг улсуудтай хамтран ажиллаж байна. Хамтын ажиллагаа болон ерөнхий зохион байгуулалтын хувьд (1) Цахим төлбөр тооцоог нутагшуулах ажлын хэсэг (ДБАА удирдлагаар), (2) Дижитал санхүүгийн үйлчилгээн дэх танилт бүртгэл, хаяг ID -н ажлын хэсэг (ДБАА удирдлагаар), (3) Дэд бүтэц аюулгүй бадлыг бэхжүүлэх ажлын хэсэг (ОУЦХБ удирдлагаар) үүд ажиллаж тухайн улсын бодлого, зохицуулалтын байгууллага болон хувийн хэвшил, олон нийтийн санаа, санаачлагыг тусган уялдуулж хамтран ажиллаж байна.

Үндэсний эрх баригчид, хувийн хэвшил, олон нийтийн холбогдох сэдвүүдээр ажлын хэсэг болон улс орны хөтөлбөрүүдийн шинэ санааг хуваалцах зорилгоор жил бүр гурван симпозиум зохион байгуулдаг.

Энэхүү тайлан нь Олон улсын цахилгаан холбооны байгууллагаар ахлуулсан FIGI аюулгүй байдал, дэд бүтэц, итгэлцлийн ажлын хэсгийн бүтээгдэхүүн юм.

Энэхүү тайланд илэрхийлсэн дүгнэлт, тайлбар, дүгнэлтүүд нь Төлбөр ба зах зээлийн дэд бүтцийн хороо, Билл ба Мелинда Гейтсийн сан, Олон улсын цахилгаан холбооны байгууллага, Дэлхийн банк зэрэг Санхүүгийн хүртээмжийг дэмжих санаачилгыг идэвхижүүлэгчдийн шууд санал санаачлагын хүрээнд гарсан зүйлс бөгөөд шууд ашиглах, баримт бичигт тусгах албагүй.

Мөн тодорхой компаниуд эсвэл тодорхой үйлдвэрлэгчдийн бүтээгдэхүүнийг дурьдсан нь тэдгээрийг дурдаагүй ижил төстэй шинж чанартай бусад бүтээгдэхүүнээс илүү, ОУЦХБ-аас зөвшөөрсөн эсвэл санал болгосон гэсэн үг биш юм.

FIGI-ийн түншүүд энэ ажилд орсон мэдээллийн үнэн зөвийг баталгаажуулахгүй бөгөөд хил хязгаар, өнгө, нэр томъёо болон бусад мэдээлэл нь аливаа улс орон, нутаг дэвсгэр, хот, бүс нутгийн эрх зүйн байдлын талаарх FIGI-ийн түншүүдийн дүгнэлт, түүний эрх бүхий байгууллагуудын дүгнэлтийг илэрхийлэхгүй мөн анхаарна уу.

Энэ тайлангийн талаар

Энэхүү тайланг хэвлэлд бэлтгэх ажлыг Флоридагийн их сургуулийн Кевин Батлер гүйцэтгэсэн бөгөөд хянаж, засварлахад чиглүүлж, туусалсан ОУЦХБ-ын Вижай Маури, Арнольд Кибуука, Пакистаны Төрийн банкны Рехан Масуд нарт талархал илэрхийлье. Мөн FIGI Аюулгүй байдлын дэд бүтэц, итгэлцлийн ажлын хэсгийн гишүүдэд оруулсан хувь нэмэр, санал хүсэлтэд талархал илэрхийлье.

Хэрэв та нэмэлт мэдээлэл өгөхийг хүсвэл tsbfigisit@ itu .int хаягаар Вижай Моритэй холбогдоно уу .

Агуулга

(үргэлжлэл)

Товчлол:

API	Application Programming Interface
DFS	Digital Financial Services
DMZ	Demilitarized Zone
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
MD	Message Digest
MFA	Multi-Factor Authentication
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number
NTP	Network Time Protocol
OTP	One Time Password
PKI	Public Key Infrastructure
POS	Point of Sale
RBAC	Role-Based Access Control
SD	Security Dimension
SHA	Secure Hash Algorithms
Secure Element	A formally certified, tamper-resistant, stand-alone integrated SE circuit often referred to as a "chip" as defined by the European Payments Council or other recognized standards authority.
SIM	Subscriber Identity Module
SMS	Short Messaging Service
STK	SIM Toolkit
XML	Extensible Markup Language
USSD	Unstructured Supplementary Service Data

Орчуулга тайлбар:

API - хэрэглээний програмчлалын интерфейс
DFS - Дижитал санхүүгийн үйлчилгээ
DMZ - нийтийн интернетээс тусгаарладаг физик эсвэл логик дэд сүлжээ
IMEI - нь гар утас бүрт өгдөг 15-17 оронтой код юм. Энэ дугаарыг үйлчилгээ үзүүлэгчид хүчинтэй төхөөрөмжүүдийг ялган танихад ашигладаг.
IMSI- Энэ нь Мобайл Сүлжээний Операторууд (MNOs) хувь хүн хэрэглэгчийг танихад ашигладаг бөгөөд энэ нь Subscriber Identity Module (SIM) профайлын гол бүрэлдэхүүн хэсэг юм.
MD - мессеж задлах алгоритм
MFA - хэрэглэгчдээс өөрийн данс руугаа нэвтрэхийн тулд хоёр ба түүнээс дээш баталгаажуулах хүчин зүйл шаардаж, фишинг, мэдээлэл зөрчих зэрэг кибер халдлагад өртөх магадлалыг бууруулж, аюулгүй байдлын нэмэлт давхаргаар хангадаг арга хэлбэрийн нэр.
MNO -Мобайл сүлжээний үйлчилгээ эрхлэгч
MSISDN - Мобайл станцын олон улсын захиалагчийн лавлах дугаар
NTP сүлжээний цагийн протокол
OTP нэг удаагийн нууц үг
PKI нийтийн түлхүүрийн дэд бүтэц
POS борлуулалтын цэг
RBAC Үүрэгт суурилсан хандалтын хяналт
SD аюулгүй байдлын хэмжээс (баримт бичигт “АБХ”- гэж ашиглаж явна)
SHA хамгаалалт, аюулгүй байдлын хаш алгоритмууд
Secure Element - Албан ёсоор баталгаажсан, хөндлөнгийн хамгаалалттай, бие даасан нэгдсэн хэлхээг Европын төлбөрийн зөвлөл эсвэл бусад хүлээн зөвшөөрөгдсөн стандарт эрх бүхий байгууллагаас тодорхойлсон "чип" гэж нэрлэдэг. (Ерөнхий тодорхойлолт нь дизайны хувьд зөвшөөрөлгүй хандалтаас хамгаалагдсан чип бөгөөд хязгаарлагдмал багц програмуудыг ажиллуулах, түүнчлэн нууц болон криптограф өгөгдлийг хадгалахад ашигладаг.)
SIM захиалагчийн таних модуль
SMS богино үсэгт мэдээний үйлчилгээ
STK SIM хэрэгслийн хэрэгсэл
XML өргөтгөх тэмдэглэгээний хэл (нь дурын өгөгдлийг хадгалах, дамжуулах, сэргээхэд зориулагдсан тэмдэглэгээний хэл ба файлын формат юм.
USSD бүтэцгүй нэмэлт үйлчилгээний өгөгдөл Бүтэцлэгдээгүй нэмэлт үйлчилгээний өгөгдөл (USSD), заримдаа 'хурдан кодууд' эсвэл 'онцлог нэршсэн кодууд' гэж нэрлэдэг

Дижитал санхүүгийн үйлчилгээний аюулгүй байдлын аудитын удирдамж

1 ОРШИЛ

Энэхүү зөвлөмж нь дижитал санхүүгийн үйлчилгээ эрхлэхэд оролцогч талуудад аюулгүй байдын аудитын дутагдалтай хэсгийг тодорхойлох. ДСҮ-ний аюулгүй байдал, баталгааны тогтолцоо нь аюул заналхийлэл, эмзэг байдлыг тодорхойлох аюулгүй байдал эрсдлийн удирдлагын нэгдсэн системтэй үйл явцад үндэслэдэг.

ДСҮ-ний аюулгүй байдлын баталгааны хүрээнд ДСҮ-ний үйлчилгээ үзүүлэгч, үүрэн холбооны оператор болон экосистемд оролцогч гуравдагч этгээдүүд нэгэн зэрэг аюулгүй байдлын хяналтын арга хэмжээг хэрэгжүүлэх үүрэгтэй.

ДСҮ-ний хувьд үйлчилгээ авч буй этгээдийн хувийн нууц, өгөгдөлд хандах, үйлчилгээний нууцлал, хэрэглэгчийн баталгаажуулалт, нэвтрэх болон үйлчилгээ авах зөвшөөрөл зэрэг мөн сүлжээний аюулгүй байдал, залилан хуурах(гадаад болон дотоод) зэрэг эрсдэл учирч болзошгүй байдаг.

Энэ хүрээнд хяналт, баталгаажуулалтын хуудсыг ДСҮ-г зохицуулагч, үйлчилгээ үзүүлэгч болон дамжуулагч оператор дундаа үүсгэн ашиглах ёстой бөгөөд энэ нь хяналтын тогтолцоог үнэлэх боломжийг бүрдүүлж, хяналт тавьж ажиллахад ашиглагдах юм.

2 ДСҮ АЮУЛГҮЙ БАЙДЛЫН АУДИТЫН УДИРДАМЖ

ДСҮ-ний аюулгүй байдлын аудитын удирдамжийг зургаан бүлэгт ангилах бөгөөд зохицуулагч дотоод болон хөндлөнгийн аюулгүй байдлын аудитор, мобайл сүлжээний үйлчилгээ эрхлэгч эсвэл дижитал санхүүгийн үйлчилгээ үзүүлэгчийн үйлчилгээний аюулгүй байдлыг үнэлэхэд ашиглаж болно. Бүлэг тус бүр дээрх асуудлуудыг дижитал санхүүгийн үйлчилгээ, дэд бүтэцийн аюулгүй байдлын аудитын хяналтын хуудас болгон цуврал асуулгуудыг ашиглаж болно.

Дижитал санхүүгийн үйлчилгээний аюулгүй байдлын аудитын удирдамжийг дараах бүлгүүдэд ангилдаг:

i) **Хандалтын хяналт /Access control/**

Энэ бүлгийн аудитын удирдамж нь дижитал санхүүгийн үйлчилгээтэй холбоотой систем, үйлчилгээ, нөөц, хандалтад хяналт хийх, сүлжээний нөөцийг ашиглах, хамгаалах баталгааг хангах хэсэг.

ii) **Танилт, баталгаажуулалт /Authentication/**

Энэ бүлгийн аудитын удирдамж нь дижитал санхүүгийн үйлчилгээний програмын хэрэглэгчийг жинхэнэ хувь хүн болохыг нь баталгаажуулах чадварыг үнэлдэг.

iii) **Бэлэн байдал / Availability/**

Энэ бүлгийн аудитын удирдамж нь дижитал санхүүгийн үйлчилгээний дэд бүтэц, програмын найдвартай байдал, эрх бүхий ДСҮ-ний хэрэглэгчдэд цаг тухайд нь хандах боломжийг, боломжтой байдлыг үнэлдэг. Аппликейшн болон дэд бүтэц нь үйлчилгээ үзүүлэхээс татгалзах халдлаг (DoS)-д тэсвэртэй, хамгаалагдсан байдлыг үнэлдэг.

iv) **Луйврыг илрүүлэх / Fraud detection/**

Энэ бүлгийн аудитын удирдамж нь дижитал санхүүгийн үйлчилгээний системээс хэрэглэгчийн хувийн мэдээллийг олж авах, хөрөнгө завших, хулгайлах зорилгоор дотоод болон гадаад байгууллагууд хууль бусаар хөндлөнгөөс оролцохыг илрүүлэх систем дэх хяналтыг үнэлэх зорилготой.

v) **Сүлжээний аюулгүй байдал / Network security/**

Энэ бүлгийн аудитын удирдамж нь үндсэн сүлжээний дэд бүтцэд зөвшөөрөлгүй нэвтрэх, буруу ашиглах, буруу ажиллуулах, өөрчлөх, устгах, зохисгүй байдлаар задруулхаас хамгаалах хяналтыг үнэлдэг. Эдгээрийг мөн мэдээлэл шилжүүлэх эсвэл хөндлөнгөөс оролцохгүйгээр зөвхөн зөвшөөрөгдсөн цэгүүдийн хооронд мэдээлэл дамжуулж байгаа эсэхийг шалгахад ашиглаж болно..

vi) **Хувийн мэдээлэл ба нууцлал / Privacy and confidentiality/**

(үргэлжлэл)

Энэ бүлгийн аудитын удирдамж нь дижитал санхүүгийн үйлчилгээнд оролцогч/хэрэглэгчийн мэдээллийг зөвшөөрөлгүй задруулахаас хамгаалах хяналтыг үнэлдэг бөгөөд энд сүлжээний үйл ажиллагааг ажиглах явцад үүсэж болзошгүй өгөгдөл хамаалалтай холбоотой үүсэж болзошгүй асуудлуудыг оруулна.

Дижитал санхүүгийн үйлчилгээний аюулгүй байдлын аудитын удирдамж нь дараах форматаар хийгдсэн:

Нөлөөлөлд өртсөн тал	**Бүлэг**	**Эрсдэл ба эмзэг байдал**	**Хяналт**	**Аюулгүй байдлын аудитын асуулт**	**Холбогдох бодлого эсвэл журам**

Дээрх хүснэгтэд ДСҮ-ний аюулгүй байдлын эрсдэл, эмзэг байдал, тэдгээр эрсдэлд өртсөн ДСҮ-ний байгууллагууд, эрсдэлийг бууруулах хяналт, аудиторын асуух аюулгүй байдлын аудитын асуулт, холбогдох бодлого, журмыг хамруулав.

- "Нөлөөлөлд өртсөн тал" баганад Дижитал санхүүгийн үйлчилгээний экосистемийн эрсдэл болон эмзэг байдалд өртсөн аж ахуйн нэгжийн жагсаалтуудыг авч үзнэ.
- "Эрсдэл ба эмзэг байдал" баганад дижитал санхүүгийн үйлчилгээний орчин дахь аюулгүй байдлын найман үндсэн хэмжигдхүүний хүрээнд аж ахуйн нэгжид учирч болох аюул заналыг тоймлон харуулав (**АБХ**-аюулгүй байдлын хэмжээсүүд).
- “Хяналт” баганад дижитал санхүүгийн үйлчилгээний орчинд хэрэглэгдэх дижитал санхүүгийн үйлчилгээний хяналтуудыг тусган харуулав.
- "Аюулгүй байдлын аудитын асуулт" баганад тусгай хяналтын нийцлийг шалгах аудиторын асуултыг тоймлон харуулав.
- "Холбогдох бодлого эсвэл журам" баганад ISO/IEC 27001- Мэдээллийн аюулгүй байдлын менежментэд суурилсан тухайн байгууллагын өдөр тутмын үйл ажиллагаа, стратегийг чиглүүлдэг холбогдох бодлого, журмын баримт бичгүүдийг санал болгодог.

Дээрх бүтцийн хүснэгтийг 3-р хэсэгт боловсруулсан бөгөөд ДСҮ-ний аюулгүй байдлын баталгаажуулалтын тогтолцооны бүх аюулгүй байдлын хяналтын аудитын нарийвчилсан хяналтын хуудсыг багтаасан болно.

Хүснэгтэнд нийцэж байгаа эсэхийг шалгахын тулд ДСҮ-ний үйлчилгээ үзүүлэгч болон үүрэн холбооны операторын түвшинд хийх шаардлагатай янз бүрийн аюулгүй байдлын шалгалтуудыг тоймлон харуулав.

Энэ хүснэгтийг харилцаа холбооны болон санхүүгийн үйлчилгээний зохицуулагчид, аюулгүй байдлын аудиторууд, ДСҮ-ний үйлчилгээ үзүүлэгчид дотоод болон гадаад аюулгүй байдлын аудитын удирдамж болгон ашиглаж болно.

4-р бүлэгт аюулгүй байдлын аудиторуудын зөвлөмж болгох үүднээс 1-р хүснэгтээс ангиллаар нь бүлэглэсэн хэд хэдэн асуултыг тоймлон харуулав.

ДСҮ-ний аюулгүй байдал баталгаажуулалт, хяналтын аудитын удирдамж

Удирдамжид аудиторын аюулгүй байдлын хяналтыг үнэлэхэд ашиглаж болох асуултууд бүхий жагсаалтыг оруулсан.

Нөлөөлөлд өртсөн тал	Бүлэг	Эрсдэл ба эмзэг байдал	Хяналт	Аюулгүй байдлын аудитын асуулт	Холбогдох бодлого эсвэл журам
ДСҮ үзүүлэгч	Хандалтын хяналт	- Хэрэглэгчийн холбогдох хяналт хангалтгүй (АБХ: Хандалтын хяналт)	С1: ДСҮ-ний програмууд дээр автоматаар түр гаргах бүр гаргах хэрэглэгчийн хэсгийг тохируулах (логик хэсэг). Аппликешн дотор нууц үгтэй холбоотой зохицуулалт хийх (серверээс хэрэгжүүлсэн), амжилтгүй нэвтрэх оролдлого их хийгдэх, нууц үгийн түүх, дахин ашиглах хугацаа, акаунтыг хаах хугацааг боломжийн хамгийн бага утгаар тохируулж, офлайн халдлагыг багасгах.	ДСҮ-ний хэрэглэгчийн хэсэгт дараах тохиргоог хийхтэй холбоотой асуудал	Нэвтрэх хяналтын бодлого - Систем, хэрэглээний нэвтрэх хяналт
				i) нэвтрэлтээс автоматаар гаргах, цаг тохируулах асуудал	
				ii) Олон дахин нэвтрэх оролдлого(алдаатай нууц үг)-д хариу үзүүлэх	
				iii) Нууц үг болон ПИН кодын талаарх асуудал.	
				iv) Нууц үг/ПИН кодыг дахин ашиглах хугацаа	
ДСҮ үзүүлэгч	Хандалтын хяналт	- Хэрэглэгчийн идэвхигүй дансны хяналт хангалтгүй (АБХ: Танилт, баталгаажуулалт)	С2: Хэрэглэгчийн дансыг дахин идэвхжүүлэхийн өмнө идэвхгүй байгаа хэрэглэгчийг таних баталгаажуулалтыг шаардах.	Хэрэглэгчийн идвэхигүй байсан дансуудыг идэвхжүүлэхийн өмнө хэрэглэгчийн хувийн мэдээллийг баталгаажуулах хангалттай арга бий юу? Жишээ нь: Биометрик баталгаажуулалт.	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалтын удирдлага
ДСҮ үзүүлэгч	Хандалтын хяналт	- Газарзүйн байршлын баталгаажуулалтыг хийж чадаагүй (АБХ: Харилцаа холбооны аюулгүй байдал)	С3: ДСҮ дээр суурилсан хэрэглэгчийн байршилд хязгаарлалт хийх(жишээ нь хэрэглэгч танилт болон богино үсэгт мэдээний гэрээт агентад холбогдсон USSD код роаминг үйлчилгээ авсан.) Боломжтой бол мөнгө таталт болон байршуулж буй хэрэглэгч болон ДСҮ ний агент нэг бүс нутагт байгааг баталгаажуулж байх	ДСҮ-ний систем нь хэрэглэгчийн бүртгэл мэдээлэлд үндэслэн загвараас гадуур гүйлгээг илрүүлэх чадвартай юу?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт
				Жишээ нь: ДСҮ үйлчилгээ үзүүлэгч нь байршилд суурилсан гүйлгээний баталгаажуулалтыг ашиглан гүйлгээний жинхэнэ эсэхийг шалгадаг уу, жишээлбэл, газарзүйн хувьд холбогдож буй хурдыг хянах замаар эсвэл бусад хэрэгслээр дамжуулан?	
ДСҮ үзүүлэгч	Хандалтын хяналт	- ДСҮ-ний үйлчилгээнд зориулсан хэрэглэгчийн харилцааны сувгуудын хэрэглэгчийн баталгаажуулалт хангалтгүй (АБХ: Харилцаа холбооны аюулгүй байдал)	С4: Харилцаа холбооны сувгаар ДСҮ-г хязгаарлах (бүртгэлийн үед хэрэглэгчид үйлчилгээний хандалтын суваг, зөвхөн USSD, зөвхөн STK, зөвхөн апп эсвэл хосолмол хувилбарыг сонгох ёстой) сонгосон сувгуудаар дамжуулан ДСҮ эрхлэгч хандалт хийх оролдогыг тодорхойлох, тэмдэглэх болгоно.	ДСҮ үзүүлэгч нь хэрэглэгчийн нэгэн зэрэг нэвтрэх эрхийг хязгаарлаж, хэрэглэгчдэд бусад нэвтрэх сувгуудыг сонгох боломжийг олгосон уу?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт
				Жишээлбэл, USSD ашигладаг хэрэглэгчид энэ сувгаар нэвтрэх эрхийг идэвхжүүлэхээс өмнө өөр сувгийг сонгох боломжтой юу?	
ДСҮ үзүүлэгч	Баталгаажуулалт	- дахин илгээгдсэн хүсэлтэд хариу үзүүлэх (АБХ: Харилцаа холбооны аюулгүй байдал).	С5: ДСҮ-ний систем нь үйлчлүүлэгчийн баталгаажуулалт эсвэл эвшээрлийн мэдэгдэлд итгэх ёсгүй; хандалтын хүсэлтийн баталгаажуулалтыг сервер талд хийх ёстой.	ДСҮ үзүүлэгч нь бүх нэвтрэх хүсэл тийг сервер дээр суурилсан баталгаажуулалтынзарчимаар шийдвэрлэдэг үү?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт
ДСҮ үзүүлэгч	Хувийн мэдээлэл, нууцлал	-Нууц үг хадгалахад зориулсан шифэрлэлтийн алгоритмууд (АБХ: Өгөгдөл, нууцлал)	С6: Хүчэтгэсэн криптограф хаш алгоритм ашиглан ДСҮ хэрэглэгчийн нууц үгийг хадгалах.	Энэ үйл ажиллагаа нь өгөгдөл шифэрлэгдсэн үү, найдвартай хадгалагдсан уу?	Өгөгдлийн аюулгүй байдал болон мэдээлэл алдагдахаас урьдчилан сэргийлэх стандарт
Үүрэн сүлжээний оператор	Хандалтын хяналт	- ДСҮ-үйлчилгээ авхаар нэвтэрсэн холболтыг түр салгах	С7: USSD, STK апликейшин болон вэб д суурилан үйлчилгээ авах холболтод түр салгалт хийдэг.	ДСҮ үзүүлэгч нь USSD болон STK аар дамжин холбогдсон дижитал санхүүгийн үйлчилгээний хэрэглэгч идвэхгүй болсон тохиолдолд холболтыг салгадаг уу?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт
Үүрэн сүлжээний оператор	Хандалтын хяналт	- хэрэглэгчийн итгэмлэлийг богино үсэгт мэдээлэл болон агентуудаар дамжуулан баталгаажуулах (АБХ: Өгөгдөл, нууцлал)	С8: Боломжтой бол ДСҮ-ний хэрэглэгчид бүртгүүлэхдээ нууц үгээ тохируулж, систем рүү дамжуулах явцад шифрлэгдсэн байх ёстой. Хэрэглэгчдэд анх удаа итгэмжлэл илгээсэн тохиолдолд ДСҮ-ний програмын итгэмжлэлийг гуравдагч этгээд/агентгүйгээр шууд хэрэглэгчдэд илгээсэн эсэхийг шалгаарай. Хэрэглэгчид анх удаа нэвтэрсний дараа шинэ нууц үг оруулах шаардлагатай болно.	Нууц үг найдвартай дамжуулагдсан уу? Хэрэглэгч анх удаа нэвтэрсний дараа нууц үгээ солих шаардлагатай юу?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
	Хандалтын хяналт	- Нэвтрэх хяналтыг хийгээгүйгээс системийг гадны халдлагад өртөмтгий болгож байна (АБХ: хандалтын хяналт)	С12: ДСҮ-ний систем дээр хэрэглэгчдэд зориулсан данс руу нэвтрэх оролдлогын дээд хэмжээг бүх түвшинд (хэрэглэгч, гэрээт этгээд, агент, эцсийн хэрэглэгч) тохируулах, хэрэгжүүлэх. (өгөгдлийн сан, үйлдлийн систем, апликейшин)	Амжилтгүй нэвтрэх оролдлогын дээд хязгаар болон нэвтрэх эрх болон бүртгэлийг түгжих тохиргоо хийгдсэн үү?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт
Үүрэн сүлжээний оператор	Баталгаажуулалт	-Хэрэглэгчийн итгэмжлэлийг найдвартай шилжүүлэх (АБХ: хандалтын хяналт)	С14: ДСҮ эрхлэгчдэд хэрэглэгчийн баталгаажуулалтыг тусгай хамгаалагдсан аюулгүй ялгаатай сувгуудаар дамжуулдаг байх.	ДСҮ-ний хэрэглэгчийн баталгаажуулалтын итгэмжлэлүүдийг илгээдэг ялгаатай сувгуудыг сонгосон эсэх. (жишээ нь хэрэв дансны тохиргоог USSD сувгаар хийсэн бол нэг удаагын нууц үгийг е-майл болон дуудлагаарр дамжуулдаг уу?)	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт

(үргэлжлэл)

Нөлөөлөлд өртсөн тал	Бүлэг	Эрсдэл ба эмзэг байдал	Хяналт	Аюулгүй байдлын аудитын асуулт	Холбогдох бодлого эсвэл журам
Үүрэн сүлжээний оператор	Сүлжээний аюулгүй байдал	- Дотоод сүлжээн дэх гадны нөлөөг хязгаарлах, илрүүлэх. (АБХ: Хандалтын хяналт)	С15: ДСУ-ний сүлжээнд гадны нөлөөллийг хязгаарлах, илрүүлэх үүднээс NAT ашиглах буюу сүлжээний хягжилт хөрвүүлэх шаардлагатай.	ДСУ-ний системийн дотоод үйл ажиллагаанд зориулсан хаягуудын (өгөгдлийн сангийн IP хаяг гэх мэт) өртөлтийг хязгаарлах техникийн хяналт байдаг уу?	Харилцаа холбооны аюулгүй байдлын бодлого - Сүлжээний аюулгүй байдлын удирдлага
ДСУ эрхлэгч	Сүлжээний аюулгүй байдал	- Дотоот системийн халдлагаас хамгаалагдсан байдал (АБХ: Хандалтын хяналт)	С16: ДСУний системийг бусад бүх дотоод болон гадаад системүүдээс логикоор тусгаарладаг DMZ-ийг тохируулснаар системийг гадны халдлагад өртхөөс сэргийлэх.	Бусад бүх системээс ДСУ системд нэвтрэх боломжийг хязгаарласан логик хил хязгаар байдаг уу? (Жишээ нь, ДСУ-ний хэрэглэгчид ДСУ-ний систем болон боловсруулах системд хандах, хандалт хийх эрх хязгаарлагдмал байдаг)	Харилцаа холбооны аюулгүй байдлын бодлого - Сүлжээний аюулгүй байдлын удирдлага
ДСУ эрхлэгч	Хувийн нууц, нууцлал	- ДСУ-ний програмын үйлдлийн системүүдийн санал болгож буй аюулгүй байдлын сангууд (АБХ: Харилцаа холбооны аюулгүй байдал)	С17: Үйлдлийн системийн аюулгүй байдал түүнийг дэмжин ажиллаж буй шифрийн иж бүрдэл(Cryptographic Library) санг хангалттай зохион байгуулан ажиллаж буй эсэхийг шалгаарай.	Үйлдлийн систем эсвэл програмд ашигладаг криптографийн сангуудыг программд холбож зохион байгуулсан эсэх мөн түүнд тогтмол шинэчлэл хийдэг эсэх? Криптографийн сангууд хүчтэй криптографийн шифрийг дэмждэг үү, сул шифрийг ашиглахаас сэргийлдэг үү? Хэрэглээгүй хэш алгоритмууд ашиглагдаж байгаа бөгөөд хангалттай хэллэгийн уртыг дэмждэг үү? (Өнөөдөр SHA512-оос бага бол сул гэж тооцогддог. MD5 болон SHA1 ажиллахгүй байгаа.)	Криптографийн бодлого - Криптографийн хяналт
				Тэгш хэмтэй шифрлэлтийн шифрүүдийн хувьд хүчтэй шифрийг ашигладаг уу, түлхүүрийн хангалттай уртыг дэмждэг үү? (Жишээ нь, SWEET-32 халдлагын улмаас 3-DES нь илүүд үздэг шифр байхаа больсон байхад AES нь аюулгүй гэж тооцогддог бөгөөд үүнийг аль болох хурдан AES руу шилжүүлэхийг зөвлөж байна.) - Нийтийн түлхүүрийн хувьд Шифрлэлт, түлхүүрийн уртыг ашиглаж буй нийтийн түлхүүрийн алгоритмд тохирох хэмжээгээр сонгосон уу?	
				Криптографийн алгоритм болон түлхүүрийн хэмжээг сонгохдоо олон нийтийн болон сайтар шалгасан стандартад тулгуурласан шалгуурыг ашигладаг уу? (Жишээ нь, NIST 800-57 тусгай хэвлэлд алгоритм бүрийн хамгийн бага түлхүүрийн хэмжээ болон энэ түлхүүрийн хэмжээ хэр удаан ажиллах талаар зааварчилгаа байдаг)	
Үүрэн сүлжээний оператор	Хувийн нууц, нууцлал	- SMS, USSD (АБХ: харилцааны аюулгүй байдал) гэх мэт аюулгүйн сувгуудаар шифрлэлтийн сул практик эсвэл нууц мэдээллийг тодорхой текстээр илгээх.	С18: Сүлжээгээр дамжин өнгөрөх болон өгөгдөл амарч байх үед хэрэглэгчийн нууц үг болон PIN зэрэг бүх нууц мэдээллийг шифрлэсэн эсэхийг шалгаарай.	Бүх эмзэг хэрэглэгчийн өгөгдлийг програм эсвэл үйлдлийн системээр шифрлэсэн үү? Өгөгдлийн шифрлэгдээгүй хувилбаруудыг төхөөрөмжид, жишээлбэл, түр зуурын буфер эсвэл санах ойд хандах боломжтой юу? Сүлжээний холболтоор илгээсэн бүх мэдээлэл хүчтэй шифрлэлтийн шифрээр шифрлэгдсэн үү? (Хүчтэй шифрлэлтийн шифрт юу багтдаг талаар дэлгэрэнгүй ярилцахыг хүсвэл С17-г үзнэ үү.)	Криптографийн бодлого - Криптографийн хяналт
ДСУ үзүүлэгч ба гуравдагч талын үйлчилгээ үзүүлэгч	Луйвар Илрүүлэлт	- Өгөгдөл хамаалалтын хяналт хангалтгүй (АБХ: хувийн нууц)	С19: Хэрэглэгчийн мэдрэмтгий өгөгдлийг үл мөрийн бүртгэлээс устгана уу. Хасах ёстой өгөгдлийн жишээнд бэлэн мөнгө авах эрхийн бичгийн код, банкны дансны дугаар, итгэмжлэл орно. Үүний оронд боломжтой бол энэ өгөгдлийг бүртгэлд харуулахын тулд орлуулагчийг ашиглана уу.	Мөшгих бүртгэлүүд болон үйл явдлын өгөгдлийн бүртгэл нь хэрэглэгчийн эмзэг мэдээллийг авч/хадгалдаг уу? (жишээ нь EDR-д хадгалагдсан хэрэглэгчийн ПИН кодууд)	Үйл ажиллагааны аюулгүй байдал -Бүртгэл, хяналт
ДСУ үзүүлэгч ба гуравдагч талын үйлчилгээ үзүүлэгч	Хувийн нууц, нууцлал	- Гүйлгээ хийх явцад эсвэл API-ээр дамжуулан харилцагчийн эмзэг мэдээллийг ил гаргах (АБХ: хувийн нууц)	С20: ДСУ үзүүлэгчид хэрэглэгчдийнхээ мэдээллийг гуравдагч этгээд болон үйлчилгээ үзүүлэгчтэй хийх үйлдэлд хуваалцахдаа хамгийн бага хэмжээгээр хязгаарлах ёстой.	Гуравдагч этгээдтэй гүйлгээ хийх явцад хуваалцсан хэрэглэгчийн нууц мэдээлэлд хязгаарлалт байгаа юу? (жишээ нь: зөвхөн гүйлгээг боловсруулахад шаардлагатай мэдээллийг гуравдагч этгээдтэй хуваалцана)	Үйл ажиллагааны аюулгүй байдлын бодлого - Үйл ажиллагааны журам, үүрэг хариуцлага

(үргэлжлэл)

Нөлөөлөлд өртсөн тал	Бүлэг	Эрсдэл ба эмзэг байдал	Хяналт	Аюулгүй байдлын аудитын асуулт	Холбогдох бодлого эсвэл журам
ДСУ үзүүлэгч ба гуравдагч талын үйлчилгээ үзүүлэгч	Луйвар Илрүүлэлт	- Хэрэглээний програмчлалын интерфейс дээрх шифэрлэлт хангалтгүй. (АБХ: хувийн нууц)	С21: API-ийн хэрэглээг хянаж, гуравдагч этгээдтэй хуваалцсан бүх өгөгдлийг шифрлэх. Нэмж дурдахад, мэдээлэл/өгөгдлийг алдхаас зайлсхийхийн тулд төлбөрийн үйлчилгээ үзүүлэгч нартай нууц задруулахгүй байх гэрээнд гарын үсэг зурсан гэх мэт өгөгдлийн удирдлагын журам, хяналтыг хэрэгжүүлнэ үү.	Хэрэглээний програмчлалын интерфейсээр хийгдсэн гүйлгээг хянах хангалттай механизм бий юу?	Үйл ажиллагааны аюулгүй байдлын бодлого - Бүртгэл, хяналт
				ДСУ үзүүлэгч нь гуравдагч этгээдтэй хэрэглэгчийн нууц мэдээллийг задруулахгүй байх гэрээтэй юу?	
				Гуравдагч этгээдтэй өгөгдөл дамжуулахад хүчирхэг криптографийн алгоритмууд байдаг уу?	
Үүрэн сүлжээний оператор	Бэлэн байдал	- Сүлжээний хүчин чадал хангалтгүй эсвэл засвар үйлчилгээ, дизайнаас үүдэлтэй сүлжээний доголдол (АБХ: бэлэн байдал)	С22: Үүрэн сүлжээний оператор нь USSD, SMS, интернетээр дамжуулан ДСУ үйлчилгээнд нэвтрэх боломжийг олгохын тулд сүлжээний өндөр хүртээмжийг хангах арга хэмжээ авах ёстой.	Үйлчилгээний хүртээмжийг хангах систем бий юу? Жишээ (үйлчилгээний нөөц давхар систем)	Мэдээллийн аюулгүй байдал, ослын менежмент - Нөөц
				Системийн хариу өгөх хугацаа болон ажиллахгүй байх хугацаат хэмжих тайлан, хэрэгслүүд байдаг уу?	
YCO	Бэлэн байдал	- Сүлжээний хүчин чадал, засвар үйлчилгээ, дизайнаас үүдэлтэй сүлжээний доголдол (АБХ:бэлэн байдал	С23: YCO нь системийн тасралтгүй ажиллагаа хангахын тулд хэрэглэгчийн тоо, хүлээгдэж буй өсөлт, хүлээгдэж буй гүйлгээний тоо, хүлээгдэж буй оргил үе зэрэгт үндэслэн техникийн чадавхийн туршилт хийх ёстой.	Үйлчилгээний чанар, туршлагын чанарыг хэмжих систем байдаг уу?	Системийн ашиглалт, хөгжүүлэлт, засвар үйлчилгээ хийх - Аюулгүй байдлыг дэмжих, хөгжүүлэх үйл явц
				QoS болон QoE нь ДСУ-ний стандартад нийцэж байгаа эсэх?	
ДСУ эрхлэгч	Сүлжээний аюулгүй байдал	- Сүлжээний траффик болон бие даасан сүлжээний багцын хяналт дутмаг (АБХ: бэлэн байдал, харилцааны холбооны аюулгүй байдал)	С24: ДСУ үзүүлэгч нь галт хана, траффик шүүлтүүр ашиглан сүлжээний халдлагаас хамгаалж, САРТСНА гэх мэт сүлжээнд нэвтрэх арга техник, механизмаар сэжигтэй урсгалыг сорьж ДСУ-ний дэд бүтцийг болзошгүй эрсдлээс хамгаалах ёстой.	Тохиромжтой тохиргоотой галт хана, ачааллын шүүлтүүр зэрэг сүлжээний халдлагаас хамгаалах хангалттай хамгаалалт байгаа юу?	Аюулгүй байдлын зарчим - хортой прогармаас хамгаалах
ДСУ эрхлэгч	Сүлжээний аюулгүй байдал	- шаардлагүй үйлчилгээг идвэхжүүлэх (АБХ: Өгөгдөл нууцлал)	С25: Интернетийн орох талын урсгалыг хязгаарлаж, байнга хянаж байх ёстой.	ДСУ-ний програмуудаас интернэтрүү чигэлсэн ачааллын хяналт хангалттай хийгддэг үү?	Аюулгүй байдлын зарчим - хортой прогармаас хамгаалах
ДСУ эрхлэгч	Сүлжээний аюулгүй байдал	- Шаардлагүй үйлчилгээг идэвхижүүлэх (АБХ: Өгөгдөл нууцлал)	С26: Хязгаарлагдмал галт ханын дүрмийг анхдагчаар тохируулж, портын зөвшөөрөгдсөн жагсаалтыг ашиглах, пакет шүүлтүүр ашиглах, зөвшөөрөгдсөн/зөвшөөрөгдсөн портууд болон IP-д хандах хандалтыг тасралтгүй хянах.	Галт ханын дүрмийг зохих ёсоор тохируулсан уу? Жишээ нь, портын цагаан жагсаалт, пакет шүүлтүүр	Аюулгүй байдлын зарчим - хортой прогармаас хамгаалах
ДСУ эрхлэгч	Луйвар илрүүлэлт	- Чухал үйл ажиллагааны дотоод хяналт хангалтгүй (АБХ: хандалтын хяналт)	С27: Боломжтой бол администратор өөр администраторын бүртгэл үүсгэх, өөрчлөх, устгах, хавсаргах, салгах зэрэг чухал үйлдлүүдэд (гэхдээ үүгээр хязгаарлагдахгүй) дөрвөн нүдний зарчмыг ашиглан чухал өөрчлөлтүүдийг хязгаарлана уу. Гар утасны дугаар/хэрэглэгчийн ID-аас ДСУ-ний данс, гүйлгээг бүцаах.	Дансны эгзэгтэй өөрчлөлтийг хянаж, батлах хангалттай хяналт байгаа юу? Жишээ нь, өөрчлөлт хийхээс өмнө үйлдвэрлэгч шалгагч, батлах үйл явц байдаг уу?	Нэвтрэх хяналтын бодлого – систем болон аппликейшинд нэвтрэх хяналт
ДСУ эрхлэгч	Луйвар илрүүлэлт	- Өгөгдлийн оролтыг баталгаажуулаагүй (АБХ: мэдээллийн бүрэн бүтэн байдал)	С28: ДСУ үзүүлэгчид үйлдвэрлэгч-батлагчийн үүрэг хариуцлагыг хангалттай тусгаарлах ёстой; жишээ нь администраторт ДСУ-ний бүртгэл үүсгэх болон идэвхжүүлэх эрх байхгүй байж болно.	ДСУ-ийн чухал ажлыг гүйцэтгэх нэгээс олон хүн шаардлагатай юу?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт
ДСУ эрхлэгч	Нэвтрэлт хяналт	Тусгай эрхийн удирдлага хангалтгүй (АБХ: хандалтын хяналт)	С29:ДСУ-ний эмзэг дэд бүтцэд физик хандалтыг хязгаарлах, хянах. Бусад дэд бүтцээс ДСУ дэд бүтцэд саад болох логик болон физик саад тотгорыг физикийн хувьд тусгаарлаж, байрлуулна. Эрх бүхий хүмүүст урьдчилан сэргийлэх зорилгоор нэвтрэх боломжийг олгох, илрүүлэх, хэрэгжүүлэх арга замаар (жишээ нь албадан тохиолдолд дохиолол) солих хамгийн бага давуу эрх бүхий техникийг ашиглах. Бүх хандалтыг бүртгэх замаар системийн үйл ажиллагааг хянах (жишээлбэл, хэн хандсан, юунд хандсан, хаанаас хандсан, хэзээ хандсан).	ДСУ-ний дэд бүтцэд хандах хандалтыг хязгаарлахад хангалттай физик болон логик саад бэрхшээл бий юу?	Тоног төхөөрөмж болон програм хангамжийн хувьд. - Аюулгүй байдлын орчин

(үргэлжлэл)

Нөлөөлөлд өртсөн тал	Бүлэг	Эрсдэл ба эмзэг байдал	Хяналт	Аюулгүй байдлын аудитын асуулт	Холбогдох бодлого эсвэл журам
ДСУ үзүүлэгч	Сүлжээний аюулгүй байдал	- Туршилтын өгөгдлийг үйлдвэрлэлийн өгөгдөлд нэмэх (АБХ: мэдээллийн бүрэн бүтэн байдал)	С30 ДСУүзүүлэгч нь гадна талын үйлчилгээнүүдэд хязгаараас гадуурх утгууд болон зөвшөөрөгдөөгүй тэмдэгтүүдийг шалгаж, оролтыг хязгаарлах замаар найдвартай оролтын баталгаажуулалтын горимуудыг ашиглах ёстой. Оролтын баталгаажуулалтыг аль болох эрт хийх ёстой бөгөөд үйлчлүүлэгч болон серверийн аль алинд нь хийх ёстой, гэхдээ сервер нь зөвхөн үйлчлүүлэгчийн баталгаажуулалтад найдах ёсгүй. Нэмж дурдахад вэб үйлчилгээний тайлбар хэл (WSDL) болон схемийг зөрчсөн бүх хүсэлтийг блоклож, бүртгэж, хянана.	ДСУ үзүүлэгч оролтын баталгаажуулалтын шалгалт хийж байна уу?	Системийг бий болгох, хөгжүүлэх, засвар үйлчилгээ хийх Хөгжүүлэх, дэмжих үйл явц дахь аюулгүй байдал
ДСУ Үйлчилгээ үзүүлэгч	Залилан илрүүлэх	- Туршилтын өгөгдлийг үйлдвэрлэлийн өгөгдөлд нэмэх (АБХ: мэдээллийн бүрэн бүтэн байдал)	С31: Мэдээллийн сангийн хурууны хээг ашиглан өгөгдөл хадгалагдсаны дараа хөндлөнгөөс оролцох, өөрчлөхийг илрүүлэх	Өгөгдлийн санд өөрчлөлт оруулах, өөрчлөхийг илрүүлэх механизм бий юу?	Үйл ажиллагааны аюулгүй байдал - Бүртгэл, хяналт
ДСУ Үйлчилгээ үзүүлэгч		- Туршилтын өгөгдлийг үйлдвэрлэлийн өгөгдөлд нэмэх (АБХ: мэдээллийн бүрэн бүтэн байдал)	С32: Бүх туршилтын өгөгдлийг үйлдвэрлэлийн орчинд шилжүүлэхээс өмнө кодоос устгасан эсэхийг шалгаарай.	Туршилтын өгөгдөл болон туршилтын хэрэглэгчийн бүртгэлийг үйлдвэрлэлийн орчноос устгасан уу?	Системийг олж авах, хөгжүүлэх, засвар үйлчилгээ хийх - Туршилтын өгөгдөл
ДСУ Үйлчилгээ үзүүлэгч	Залилан илрүүлэх	- Бүртгэл байхгүй, бүртгэлийг өөрчлөх чадваргүй, бүртгэл дэх мэдээлэл ханагалтгүй (АБХ: үгүйсгэхгүй)	С33: ДСУ системүүд нь хэрэглэгчийн үйлдлийн гарал үүслийг олж авах эсвэл чухал үйлдлүүдийг хөндлөнгийн хамгаалалттай хадгалах санд бүртгэх, ДСУ системийн бүртгэлийг хөндлөнгөөс оролцох, засварлах, устгах, зогсоохоос хамгаалах зэрэг бүртгэлийн механизмуудыг ашиглах ёстой.	ДСУ бүртгэлийг хөндлөнгийн хамгаалалттай модульд найдвартай хадгалдаг уу? жишээ нь, SIEM	Үйл ажиллагааны аюулгүй байдал - Бүртгэл, хяналт
ДСУ Үйлчилгээ үзүүлэгч	Сүлжээний аюулгүй байдал	- Нарийвчлалгүй, синхрончлогдоогүй цаг (АБХ: мэдээллийн бүрэн бүтэн байдал)	С34: ДСУ системд холбогдсон бүх систем дээр цагийн нарийвчлалын синхрончлолыг баталгаажуулах. Сүлжээний цагийн протокол(NTP) болон SNTP нь үнэн зөв цагийг синхрончлоход ашигладаг зарим протоколууд юм; Гэсэн хэдий ч эдгээрийг найдвартай байрлуулах ёстой.	ДСУ экосистемийн цаг синхрончлогдсон уу?	Үйл ажиллагааны аюулгүй байдал - Үйл ажиллагааны журам, үүрэг хариуцлага
Үүрэн холбооны үйлчилгээ эрхлэгч	Сүлжээний аюулгүй байдал	- Агаараар дамжуулах сул шифрлэлт (АБХ: холбооны аюулгүй байдал)	С38: A5/0, A5/1, болон A5/2 GSM шифрлэлтийн шифрийг ашиглахгүй байх. A5/3 болон A5/4-ийг эвдэх боломж, хялбар байдлын талаар аюулгүй байдлын болон криптографийн нийгэмлэгийн үр дүнг сайтар хянаж, илүү хүчтэй шифрүүдийг авч үзэх хэрэгтэй. Эдгээр шинэ шифрүүдэд байршуулах стратегийг бэлэн болго.	Мэдэгдэж байгаа сул шифрүүдийн хэрэглээг зогсоосон уу? Шинэ шифрүүдэд байршуулалтыг бэлтгэсэн үү?	Харилцаа холбооны аюулгүй байдал: Мэдээлэл дамжуулах
MNO	Залилан илрүүлэх	- Дуудлагын шугам сул байна Таних шүүлтүүр (АБХ: холбооны аюулгүй байдал)	С39: YCO нь ДСУ үйлчилгээ үзүүлэгчийн дуудлага шиг хуурамчаар үйлдэгдэж болзошгүй дуудлага, мессежийг илрүүлэхийн тулд дуудлага/ SMS-д CLI шинжилгээ хийх ёстой.	SMS болон дуудлагын хуурамч байдлыг илрүүлэх механизм байдаг уу? Жишээлбэл, CLI шинжилгээ?	Харилцаа холбооны аюулгүй байдал: Мэдээлэл дамжуулах
ДСУ Үйлчилгээ үзүүлэгч	Баталгаажуулалт	- Дансны тохиргоо болон зөвшөөрлийн хяналт дутуу/хангалтгүй байна (АБХ: баталгаажуулалт)	С40: Өндөр эрсдэлтэй дансны өөрчлөлт, гүйлгээний хувьд хэрэглэгчийн нэвтрэлт танилт, зөвшөөрлийг шаардаж, төхөөрөмж нэвтэрсэн байсан ч ПИН эсвэл нууц үгийн талаарх мэдлэгийг харуулах хүртэл гүйлгээ хийхээс татгалзах.	ДСУ хэрэглэгчийн дансанд өндөр дүнтэй гүйлгээ, өөрчлөлт хийх нэмэлт зөвшөөрөл, баталгаажуулалт байгаа юу? Жишээлбэл, гүйлгээний хязгаарыг нэмэгдүүлэхэд ямар нэмэлт шалгалт хийдэг вэ?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
Гуравдагч этгээдийн үйлчилгээ үзүүлэгчид	Нууцлал ба нууцлал	- Төхөөрөмжид хадгалагдсан өгөгдөл болон дамжуулагдсан өгөгдөлд ашигладаг сул шифрлэлтийн алгоритмууд (АБХ: нууцлал)	С41: Хөдөлгөөнт аппликейшн доторх өгөгдлийг хамгаалах, арын ДСУ системтэй харилцах аль алинд нь хангалттай аюулгүй шифрлэлтийг ашиглах ёстой бөгөөд боломжтой бол хэрэглэгчийн нууц мэдээллийг далдлах, тайрах, өөрчлөх шаардлагатай.	Хүчтэй шифрлэлтийн шифр, мессежийн баталгаажуулалтын код зэрэг бүрэн бүтэн байдлыг хамгаалах механизмыг төхөөрөмж дээр хадгалагдсан өгөгдөл болон өгөгдлийг арын ДСУ системд дамжуулах үед ашигласан уу? (Хүчтэй шифрлэлтийн алгоритмуудын талаар ярилцахыг С17-г үзнэ үү.) Хэрэглэгчийн нууц мэдээллийн хариу үйлдлийг баталгаажуулах бодлого бий юу?	Криптографийн бодлого - Криптографийн хяналт
Гуравдагч этгээдийн үйлчилгээ үзүүлэгчид	Нууцлал ба нууцлал	- Харилцаа холбооны шифрлэлт дутмаг (АБХ – Харилцаа холбооны аюулгүй байдал)	С42: Гүйлгээ хийх үед ДСУ системд холбогдсон гуравдагч этгээдийг тодорхойлохын тулд тоон гарын үсгийг ашиглана.	ДСУ системд холбогдсон гуравдагч талын үйлчилгээ үзүүлэгчдийг тодорхойлоход тоон гарын үсгийг ашигладаг уу?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт

(үргэлжлэл)

Нөлөөлөлд өртсөн тал	Бүлэг	Эрсдэл ба эмзэг байдал	Хяналт	Аюулгүй байдлын аудитын асуулт	Холбогдох бодлого эсвэл журам
Гуравдагч этгээдийн үйлчилгээ үзүүлэгчид	Нууцлал ба нууцлал	- Сертификат эсвэл гол материалын менежмент хангалтгүй (АБХ: хандалтын хяналт)	С43: ДСУ үйлчилгээ үзүүлэгч болон гуравдагч этгээдийн хооронд өгөгдөл солилцохыг зөвшөөрөхийн тулд итгэмжлэгдсэн түлхүүр, гэрчилгээг ашиглах ба тэдгээрийг задруулахаас хамгаална.	Хувийн болон нууц түлхүүрүүдийн найдвартай байдал, хамгаалалтыг баталгаажуулах журам бий юу? Сертификат болон бусад криптограф мэдээлэл нь үйлдлийн системийн хяналтаар хамгаалагдсан уу?	Хандалтын хяналтын бодлого - Систем болон программын хандалтын хяналт
Гуравдагч этгээдийн үйлчилгээ үзүүлэгчид	Бэлэн байдал	- ДСУ үйлчилгээ үзүүлэгч эсвэл MNO системийн алдаа нь агентууд/гуравдагч этгээдүүдийг оффлайн процесс руу буцаахад хүргэдэг (АБХ: бэлэн байдал)	С44: Холбогдох үйлчилгээ үзүүлэгчтэй систем сул зогсолтын үед үр дүнтэй удирдах процедурын болон техникийн хяналтыг тохируулна уу. Жишээлбэл, ДСУ системд нэвтрэх тасалдалтай үед офлайн гүйлгээг (жишээ нь, SIM солих) удирдах хяналтыг тохируулна уу. ДСУ систем эсвэл гуравдагч талын системийн хандалт тасалдсан үед мөнгөн гүйвүүлэг болон гуравдагч этгээдийн төлбөрийг шалгах нэмэлт шалгалт хийнэ үү.	Системийн сул зогсолтын үед менежментийг баталгаажуулах бодлого бий юу?	Үйл ажиллагааны аюулгүй байдал - Үйл ажиллагааны журам, үүрэг хариуцлага
ДСУ Үйлчилгээ үзүүлэгч	Баталгаажуулалт	- Хэрэглэгчийн акаунт дээрх аюулгүй, хангалтгүй хандалтын хяналт (АБХ: хандалтын хяналт)	С45: ДСУ бүртгэлд хандахын тулд олон хүчин зүйлтэй эсвэл олон загварын баталгаажуулалтыг ашиглана уу.	ДСУ бүртгэлтэй холбогдох үед олон хүчин зүйлийн баталгаажуулалтыг ашигладаг уу?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
	Хандалтын хяналт	- Туршилтанд ороогүй сэргээн засварлах арга (АБХ: бэлэн байдал)	С46: Үйлдвэрлэлийн ДСУ системтэй харьцдаг мэдээллийн сан, программ, үйлдлийн систем болон бусад хандалтын интерфейсээс анхдагч бүртгэл, итгэмжлэлийг идэвхгүй болгож, устгана.	ДСУ систем болон ДСУ системд холбогдсон бүх системээс анхдагч системийн бүртгэлүүдийг устгасан уу?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
ДСУ Үйлчилгээ үзүүлэгч	Хандалтын хяналт	- Туршилтанд ороогүй сэргээн засварлах арга (АБХ: бэлэн байдал)	С47: Суурилуулалт, борлуулагч, дэмжлэгийн бүртгэл, ДСУ систем болон дэд бүтцэд нэвтрэх цэгүүдийг шалгана уу. Эдгээр бүх бүртгэлийг идэвхгүй болгох эсвэл зохих хэрэглэгчийн профайлыг өгөх ёстой.	Дэмжлэгийн ажил дууссаны дараа ДСУ борлуулагч болон түсламжийн системийн данс идэвхгүй болсон уу?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
ДСУ Үйлчилгээ үзүүлэгч	Бэлэн байдал	- Гүйлгээний атомын шинж чанарыг хэрэгжүүлэхгүй байх, тэдгээрийг хэсэгчлэн дууссан төлөвт байлгах зэрэг мэдээллийн хангалтгүй хяналт (АБХ: мэдээллийн бүрэн бүтэн байдал)	С48: ДСУ, MNO, SP болон гуравдагч этгээдийн системд гарсан аливаа өөрчлөлтийн дараа төгсгөл хоорондын туршилтыг хийж, регресс болон хүчин чадлын туршилтыг хүлээн авах туршилтанд оруулна. Түүнчлэн, буцаах/харах төлөвлөгөө байгаа эсэхийг шалгаарай.	ДСУ системд өөрчлөлт, шинэчлэлт хийсний дараа эцсийн туршилтыг хийсэн үү? Төгсгөлийн туршилтууд нь хүчин чадлын туршилт, аюулгүй байдлын туршилт, үйлчилгээний чанарын туршилт, хэрэглэгчийн хүлээн авах тест гэх мэт байж болно.	Системийг олж авах, хөгжүүлэх, засвар үйлчилгээ хийх - Хөгжүүлэх, дэмжих үйл явц дахь аюулгүй байдал
ДСУ Үйлчилгээ үзүүлэгч	Бэлэн байдал	- Гүйлгээний атомын шинж чанарыг хэрэгжүүлэхгүй байх, тэдгээрийг хэсэгчлэн дууссан төлөвт байлгах зэрэг мэдээллийн хангалтгүй хяналт (АБХ: мэдээллийн бүрэн бүтэн байдал)	С49: ДСУ системүүдийн хуваарьтай, тогтмол нөөцлөлттэй байх. Нөөцлөлтийг офлайн болон сайтаас гадуур шифрлэгдсэн хэлбэрээр тогтмол туршиж, найдвартай хадгалаарай.	ДСУ үйлчилгээ үзүүлэгч байнгын хуваарьт нөөцлөлттэй юу? Нөөцлөлтүүд нь шифрлэгдсэн бөгөөд гаднах байршилд хадгалагддаг уу?	Үйл ажиллагааны аюулгүй байдал - Нөөцлөх бодлого
ДСУ Үйлчилгээ үзүүлэгч		- Гүйлгээний атомын шинж чанарыг хэрэгжүүлэхгүй байх, тэдгээрийг хэсэгчлэн дууссан төлөвт байлгах зэрэг мэдээллийн хангалтгүй хяналт (АБХ: мэдээллийн бүрэн бүтэн байдал)	С50: Гүйлгээний бүрэн бүтэн байдлыг хангахын тулд мэдээллийн сангийн стандарт ACID (Atomicity, Consistency, тусгаарлах, бат бөх чанар) функцийг ашиглана уу. ДСУ үйлдлүүд нь бүрэн амжилттай эсвэл бүрмөсөн бүтэлгүйтэх ёстой. ДСУ үйлчилгээ үзүүлэгч нь давхардсан гүйлгээг (өвөрмөц гүйлгээний ID, цагийн тэмдэг, криптографийн бүс ашиглах) урьдчилан сэргийлэх шалгалт байгаа эсэхийг баталгаажуулах ёстой.	ДСУ системд хүлээгдэж буй гүйлгээ, давхардсан гүйлгээ байгаа юу? Гүйлгээ бүрэн хийгдсэн үү?	Үйл ажиллагааны аюулгүй байдал - Үйл ажиллагааны журам, үүрэг хариуцлага
Гуравдагч этгээдийн үйлчилгээ үзүүлэгч	Нууцлал ба нууцлал	- Өгөгдлийн бүрэн бүтэн байдлыг хангах механизм хангалтгүй, гадаад итгэлцлийн зангуунд хэт найдах (АБХ: үгүйсгэхгүй)	С51: ДСУ програмууд / гуравдагч талууд тоон гарын үсгийн хэрэглээг дэмжих ёстой; найдвартай дижитал гарын үсэг нь гүйлгээний гарал үүслийн няцаашгүй нотлох баримтыг өгдөг. Дижитал гарын үсэг нь PKI-д халдаагүй тохиолдолд л хүчинтэй бөгөөд авхаалж самбаагаа баталгаажуулах төлөвлөгөөний дагуу турших ёстой. Гарын үсэг зурах түлхүүрүүд нь үндсэн түлхүүр хүртэл зохих ёсоор хамгаалагдсан гэдгийг харуулснаар ДСУ үйлчилгээ үзүүлэгч нь тодорхой хэрэглэгч болон маргаантай гүйлгээний жинхэнэ байдлын талаарх хууль эрх зүйн сорилтуудыг даван туулж чадна.	Тоон гарын үсгийг ДСУ програмууд эсвэл гуравдагч талын үйлчилгээ үзүүлэгчид ашигладаг уу? Тоон гарын үсэг нь хангалттай хүчтэй криптограф алгоритм, түлхүүрийн хэмжээн дээр суурилсан уу? Криптографийн алгоритмуудын хэрэгжилт найдвартай, шинэчлэгдсэн эсэх, тэдгээр нь хангалттай санамсаргүй байдлыг хангаж чадаж байна уу? (Жишээ нь, хүчирхэг дижитал гарын үсгийн алгоритмд RSA, DSA, ECDSA орно. Зууван муруй криптограф алгоритмууд нь бусад шифртэй дүйцэхүйц аюулгүй байдлыг хангахын тулд богино түлхүүрүүдийг ашиглаж болно.)	Хандалтын хяналтын бодлого - Систем болон программын хандалтын хяналт

(үргэлжлэл)

Нөлөөлөлд өртсөн тал	Бүлэг	Эрсдэл ба эмзэг байдал	Хяналт	Аюулгүй байдлын аудитын асуулт	Холбогдох бодлого эсвэл журам
YCO (MNO)	Баталгаажуулалт	- SIM солих, дахин ашиглахаас өмнө хэрэглэгчийн таних, баталгаажуулах хяналт хангалтгүй (АБХ: Баталгаажуулалт)	C52: YCO нь SIM солихын өмнө хэн болохыг баталгаажуулах үйл явц байгаа эсэхийг баталгаажуулах ёстой.	SIM солих үйлдлээс өмнө хэн болохыг баталгаажуулах үйл явц, бодлого байгаа юу? SIM солихыг баталгаажуулах хүртэл мэдээлэл алдагдах, дамжуулахаас урьдчилан сэргийлэх техникийн механизм бий юу?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
YCO	Баталгаажуулалт	- SIM солих, дахин ашиглахаас өмнө хэрэглэгчийн таних, баталгаажуулах хяналт хангалтгүй (АБХ: Баталгаажуулалт)	C53: Хэрэглэгчийн хэн болохыг өөрт байгаа зүйл, түүнд байгаа зүйл эсвэл мэддэг зүйлсийн хослолыг ашиглан баталгаажуулах ёстой. Жишээлбэл, SIM солих/Сим солихын өмнө хүчинтэй ID, биометрийн баталгаажуулалт, ДСУ дансны дэлгэрэнгүй мэдээллийг танилцуулах.	Үүрэн сүлжээний оператор SIM солих эсвэл SIM солихын өмнө биометрийн баталгаажуулалтыг хийдэг үү?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
YCO	Баталгаажуулалт	- SIM солих, дахин ашиглахаас өмнө хэрэглэгчийн таних, баталгаажуулах хяналт хангалтгүй (АБХ: Баталгаажуулалт)	C54: ДСУ болон Төлбөрийн үйлчилгээ үзүүлэгч нь ДСУ үйлчилгээ бүхий SIM картыг солих эсвэл солих бүрийг бодит цаг хугацаанд нь илрүүлэх боломжтой байх ёстой. Мөн шинэ SIM картаар өндөр дүнтэй гүйлгээ хийх эсвэл дансны өөрчлөлт оруулахаас өмнө нэмэлт баталгаажуулалт хийнэ үү.	ДСУ үйлчилгээ үзүүлэгч нь ДСУ дансны SIM солих эсвэл SIM солихыг илрүүлэх боломжтой юу?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт
YCO	Баталгаажуулалт	- SIM солих, дахин ашиглахаас өмнө хэрэглэгчийн таних, баталгаажуулах хяналт хангалтгүй (АБХ: Баталгаажуулалт)	C55: YCO нь IMSI болон SIM нууц түлхүүрийн утгууд (Kl утгууд) зэрэг SIM өгөгдлийг хамгаалж, найдвартай хадгалах ёстой.	Мобайл сүлжээний оператор нь IMSI, Kc, Ki зэрэг SIM өгөгдлийг найдвартай хадгалдаг уу?	Хөрөнгийн менежмент - Хэвлэл мэдээллийн хэрэгсэлтэй харьцах
YCO	Баталгаажуулалт	- SIM солих, дахин ашиглахаас өмнө хэрэглэгчийн таних, баталгаажуулах хяналт хангалтгүй (АБХ: Баталгаажуулалт)	C56: Мобайл захиалагчийн таних дугаар (MSIDN)-ийг хаах эсвэл дахин боловсруулах талаар ДСУ үйлчилгээ үзүүлэгчидтэй харилцахтай холбоотой гар утасны дугаарыг дахин боловсруулах үйл явц байх ёстой. (энэ хүрээнд: дугаарын дахин боловсруулалт гэдэг нь YCO идэвхтэй/идэвхгүй байгаа гар утасны захиалагчийн дугаарыг (MSISDN) шинэ хэрэглэгч рүү дахин хуваарилах явдал юм). SIM картыг дахин ашиглах үед гар утасны оператор холбогдох дансны утасны дугаарын шинэ IMSI-г мэдээлэх болно. ДСУ үйлчилгээ үзүүлэгч нь SIM картыг эзэмшиж буй шинэ хүний данс эзэмшигч болохыг баталгаажуулах хүртэл дансыг хаах ёстой.	ДСУ үйлчилгээ үзүүлэгч нь ДСУ дансны SIM дахин боловсруулах үйл явцад оролцдог уу?	Хөрөнгийн менежмент - Хэвлэл мэдээллийн хэрэгсэлтэй харьцах
	Нууцлал ба нууцлал	- Мобайл төхөөрөмжийн хулгай (АБХ: мэдээллийн нууцлал)	C57: ДСУ-ийн хэрэглэгчид гар утасны төхөөрөмж дээр алсын зайнаас арчих, төхөөрөмж алдагдсан эсвэл хулгайлагдсан тохиолдолд мэдээллээ шифрлэх чадвартай байх ёстой.	Аппликейшн эсвэл үндсэн үйлдлийн систем нь ДСУ өгөгдөл эсвэл мобайл төхөөрөмжийг алсаас устгахад дэмжлэг үзүүлдэг үү, мөн төхөөрөмж алдагдсан эсвэл хулгайлагдсан тохиолдолд өгөгдлийг шифрлэх механизм байгаа юу?	Үйл ажиллагааны аюулгүй байдал - Үйл ажиллагааны журам, үүрэг хариуцлага
ДСУ Үйлчилгээ үзүүлэгч	Хандалтын хяналт	солих болон дахин боловсруулах үйл явцын хангалтгүй байдал [ii] (АБХ: мэдээллийн бүрэн бүтэн байдал)	C58: ДСУ үйлчилгээ үзүүлэгчид сэжигтэй SIM солих болон SIM дахин боловсруулалтыг илрүүлэх, урьдчилан сэргийлэх журамтай байх ёстой:	ДСУ үйлчилгээ үзүүлэгчээс сэжигтэй SIM солихыг илрүүлэх журам байдаг уу SIM дахин боловсруулах уу?	Үйл ажиллагааны аюулгүй байдал - Үйл ажиллагааны журам, үүрэг хариуцлага
			а) Утасны дугаартай холбоотой IMSI өөрчлөгдсөн эсэхийг шалгана уу, энэ нь SIM солих шинж тэмдэг юм.		
			б) Хэрэв SIM солих шинж тэмдэг байгаа бол SIM барьж буй утасны IMEI-г шалгана уу. Хэрэв IMEI нь өөрчлөгдсөн бол SIM солих магадлал өндөр байна. Энэ тохиолдолд ДСУ үйлчилгээ үзүүлэгч нь жишээлбэл дуут дуудлага эсвэл агентаар дамжуулан данс баталгаажуулах процедурыг гүйцэтгэх хүртэл дансыг блоклох ёстой.		

(үргэлжлэл)

Нөлөөлөлд өртсөн тал	Бүлэг	Эрсдэл ба эмзэг байдал	Хяналт	Аюулгүй байдлын аудитын асуулт	Холбогдох бодлого эсвэл журам
ДСҮ үйлчилгээ үзүүлэгч	Луйвар Илрүүлэх	- Системийн тохиргоо болон бүртгэлийн файл, өгөгдөлд зөвшөөрөлгүй өөрчлөлт оруулах (АБХ: Өгөгдлийн бүрэн бүтэн байдал)	С59: Хулгайлахаас хамгаалж, зөвхөн онлайн гүйлгээг зөвшөөрөх а) ДСҮ програмын файлуудыг шалгах, тоон гарын үсгийг баталгаажуулах зэргээр файлын бүрэн бүтэн байдлын хяналтыг ашиглан хөндлөнгийн оролцоо, өөрчлөлтөөс хамгаалж, хянах. б) Бодлогын дагуу ДСҮ үйлчилгээ үзүүлэгч эсвэл худалдаачин гар утасны төлбөрийн шийдлийг офлайнаар гүйлгээг зөвшөөрөх эсвэл дараа нь дамжуулах зорилгоор гүйлгээг хадгалахгүй байх ёстой.	Апп нь дараа нь дамжуулах гүйлгээг хадгалдаг уу?	Үйл ажиллагааны аюулгүй байдал: Үйл ажиллагааны журам, үүрэг хариуцлага
ДСҮ үйлчилгээ үзүүлэгч	Баталгаажуулалт	- Хэрэглэгчийн хандалтын баталгаажуулалт эсвэл хэрэглэгчийн оруулсан баталгаажуулалт хангалтгүй (АБХ: Баталгаажуулалт)	С60: Хэрэглэгч болон гуравдагч талын үйлчилгээ үзүүлэгчийн ДСҮ системд хандахын тулд хүчирхэг олон хүчин зүйлийн баталгаажуулалтыг ашиглах жишээ нь токен эсвэл биометр, системийн хэрэглэгчдийг баталгаажуулахын тулд олон хүчин зүйлийн баталгаажуулалтыг ашиглах нь гарал үүслийг үгүйсгэхгүй байдлыг нэмэгдүүлдэг.	Хэрэглэгчийг баталгаажуулахад олон хүчин зүйлийг ашигладаг уу?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт
ДСҮ үйлчилгээ үзүүлэгч	Баталгаажуулалт	- Хэрэглэгчийн хандалтын баталгаажуулалт эсвэл хэрэглэгчийн оруулсан баталгаажуулалт хангалтгүй (АБХ: Баталгаажуулалт)	С61: Хүлээгдэж буй өгөгдлийг API-тай холбоотой өгөгдлийн схемийн хүлээгдэж буй утгуудтай харьцуулж USSD-д шалгах, XML баталгаажуулалтыг хийх.	ДСҮ үйлчилгээ үзүүлэгч API болон USSD хүсэлтээр өгөгдөлд XML баталгаажуулалт хийж байна уу? Жишээлбэл, оролтын баталгаажуулалт, дүн, дүнгийн түсгай тэмдэгт, валютын чек гэх мэт.	Харилцаа холбоо аюулгүй байдал - Мэдээлэл дамжуулах
ДСҮ үйлчилгээ үзүүлэгч	Баталгаажуулалт	- Хэрэглэгчийн хандалтын баталгаажуулалт эсвэл хэрэглэгчийн оруулсан баталгаажуулалт хангалтгүй (АБХ: Баталгаажуулалт)	С62: Хэрэглэгчийн гүйлгээ хоорондын хурд, өдрийн гүйлгээний цагийг шалгахын тулд аналитик системийг ашиглан зөвшөөрлийн баталгаажуулалтын нэмэлт шалгалтыг ашиглана уу.	ДСҮ систем нь хэрэглэгчийн профайл дээр тулгуурлан загвараас гадуур гүйлгээг илрүүлэх чадвартай юу? ДСҮ үйлчилгээ үзүүлэгч нь хэрэглэгчийн гүйлгээний профайлд үндэслэн шалгалт хийж байна уу? Жишээлбэл, агент дэлгүүрүүд хожимдсон гүйлгээ, ДСҮ хэрэглэгчид хоёр өөр байршилд гүйлгээ хийдэг үү?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт
ДСҮ үйлчилгээ үзүүлэгч	Баталгаажуулалт	- Хэрэглэгчийн хандалтын баталгаажуулалт эсвэл хэрэглэгчийн оруулсан баталгаажуулалт хангалтгүй (АБХ: Баталгаажуулалт)	С63: Баримт бичгийг (и-мэйл, SMS эсвэл хавсаргасан хэвлэгч гэх мэт) гаргахад ашигладаг аргаас үл хамааран уг арга нь холбогдох хууль тогтоомж, дүрэм журам, төлбөрийн картын бодлогыг дэмжих үүднээс Үндсэн дансны дугаарыг (PAN) далдлах ёстой. Бодлого, практикийн дагуу ДСҮ Үйлчилгээ үзүүлэгч/худалдаачин нь PAN эсвэл Мэдрэмжтэй баталгаажуулалтын өгөгдөл (SAD) илгээхийн тулд и-мэйл, SMS зэрэг аюулгүй бус сувгуудыг ашиглахыг зөвшөөрөх ёсгүй.	ДСҮ програм нь хувийн дансны дугаар/мэдрэмжтэй баталгаажуулалтын өгөгдлийг SMS/имэйлээр энгийн текстээр хадгалдаг уу?	Хөрөнгийн менежмент - Хэвлэл мэдээллийн хэрэгсэлтэй харьцах
YCO	Сүлжээний аюулгүй байдал	- SS7-ийн хамгаалалтын сул тал[iii] (АБХ: Харилцаа холбоо Аюулгүй байдал)	С70: ПИН код, нууц үг зэрэг хэрэглэгчийн бүх эмзэг өгөгдлийг дотоод сүлжээн дэх хүчтэй шифрлэлтийн алгоритмаар найдвартай хадгалж, энэ өгөгдлийн эсрэг дотоод аюулыг багасгахын тулд амарч байгаа эсэхийг шалгаарай.	Ашигласан шифрлэлтийн алгоритмууд болон түлхүүрүүд нь хэрэглэгчийн ПИН код болон өгөгдлийг хамгаалахад хангалттай хүчтэй юу?	Криптографи - Криптографийн хяналт
YCO	Сүлжээний аюулгүй байдал	- SS7-ийн хамгаалалтын сул тал[iii] (АБХ: Харилцаа холбоо Аюулгүй байдал)	С71: SS7-ийн аюулгүй байдлын алдаан дээр үндэслэн халдлагыг илрүүлэх, хязгаарлахын тулд галт хана ашиглана уу.	YCO -д гадны SS7-д суурилсан халдлагыг илрүүлэх, хамгаалах галт хана байдаг уу? Жишээлбэл (захиалагчийн траффик саатуулах, зөвшөөрөлгүй USSD болон SM ашиглахаас хамгаалах галт хана)	Харилцаа холбооны аюулгүй байдал - Сүлжээний аюулгүй байдал удирдлага
YCO	Хандалтын хяналт	- YCO -USSD гүйлгээг саатуулах (АБХ: Харилцаа холбоо Аюулгүй байдал)	С72: Гүйлгээ хийж буй төхөөрөмжийн IMEI нь данс эзэмшигчийн утасны бүртгэлтэй IMEI-тэй таарч байгаа эсэхийг шалгана уу (MITM систем нь SIM-г өөр IMEI-ээр хуулбарлаж болно)	ДСҮ үйлчилгээ үзүүлэгч нь гүйлгээг боловсруулахаас өмнө бодит цагийн төхөөрөмжийн баталгаажуулалтыг хийж байна уу?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт
YCO	Сүлжээний аюулгүй байдал	- Хамгаалалтгүй эмзэг траффик ба шифрлэлтийн сул практик (АБХ: Харилцаа холбоо	С73: Гүйлгээ хийхэд ашигласан утасны байршлыг утасны хамгийн сүүлд мэдээлэгдсэн байршилтай (хамгийн сүүлд ирсэн/гарсан SMS эсвэл дуудлага) харьцуулж хэрэглэгчийн хурдыг хяна.	ДСҮ үйлчилгээ үзүүлэгч нь гүйлгээг боловсруулахаас өмнө хэрэглэгчийн гүйлгээний гео хурдыг шалгадаг уу?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт

(үргэлжлэл)

		Аюулгүй байдал)			
YCO	Сүлжээний аюулгүй байдал	- Хамгаалалтгүй эмзэг траффик ба шифрлэлтийн сул практик (АБХ: Харилцаа холбоо Аюулгүй байдал)	С74: Хөдөлгөөнт төхөөрөмж алдагдсан, хулгайлагдсан тохиолдолд нэмэлт аюулгүй байдлын үүднээс YCO нь SIM карт дээрх Хувийн түгжээг тайлах түлхүүрийг (PUK) ашиглах ёстой.	MNO нь ДСҮ-д ашигладаг хулгайлагдсан SIM карттай холбоотой эрсдлийг бууруулахын тулд SIM картууд дээр Хувийн түгжээ тайлах түлхүүрийг ашигладаг уу?	Харилцаа холбоо аюулгүй байдал - Мэдээлэл дамжуулах
YCO	Сүлжээний аюулгүй байдал	- Хамгаалалтгүй эмзэг траффик ба шифрлэлтийн сул практик (АБХ: Харилцаа холбоо Аюулгүй байдал)	С75: USSD дээр MSC MAP мөрдөх болон протокол анализаторын ашиглалтыг хянах, хянах, энгийн текст SMS болон дамжин өнгөрөх USSD урсгалыг дотоод хязгаарлах SMS дэд бүтэц	YCO нь дотоод сүлжээнд MAP мөрдөх, протоколын анализатор ашиглах, хандалтыг хязгаарлах хяналттай юу? (SMS болон USSD мессежийг MAP протоколд энгийн текстээр дамжуулдаг)	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
YCO	Сүлжээний аюулгүй байдал	- Хамгаалалтгүй эмзэг траффик ба шифрлэлтийн сул практик (АБХ: Харилцаа холбоо Аюулгүй байдал)	С76: Гүйлгээний хуудыг ёсны эсэхийг шалгахын тулд 2 талын Secure OTP-г эх үтасны дугаар руу нь ашиглана уу [iv]	Гүйлгээний баталгаажуулалтыг найдвартай OTP ашиглан хийдэг үү?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
YCO	Нууцлал ба нууцлал	- Хамгаалалтгүй эмзэг траффик ба шифрлэлтийн сул практик (АБХ: Харилцаа холбоо Аюулгүй байдал)	С77: Мэдээллийг ДСҮ үйлчилгээ үзүүлэгчийн сүлжээнд нэвтэрч, энэ орчинд боловсруулж, хадгалах үед нууцлал, бүрэн бүтэн байдлыг хангахын тулд хүчтэй криптографийн туршлагыг ашигла.	Ашигласан шифрлэлтийн алгоритмууд болон түлхүүрүүд нь хэрэглэгчийн ПИН код болон өгөгдлийг хамгаалахад хангалттай хүчтэй юу?	Криптограф - Криптографийн хяналт
YCO	Хандалтын хяналт	- Хамгаалалтгүй эмзэг траффик ба шифрлэлтийн сул практик (АБХ: Харилцаа холбоо Аюулгүй байдал)	С78: Хэрэглэгч бүрт ДСҮ сессийн тоог хязгаарлах. Хандалтын сувгаас (STK, USSD, эсвэл https) үл хамааран хэрэглэгч бүрт нэг сесс хийхийг зөвшөөрөх; ДСҮ хэрэглэгчийн бүртгэл нь олон сувгийг нэгэн зэрэг ашиглах боломжгүй байх ёстой.	Олон сувгаар нэгэн зэрэг нэвтэрч орохоос сэргийлэх хяналт байдаг уу?	Хандалтын хяналтын бодлого - Систем болон програмын хандалтын хяналт
				ДСҮ үйлчилгээ үзүүлэгч нь ДСҮ сүлжээнд холбогдохын тулд нэг удаад зөвхөн нэг сессийг зөвшөөрдөг үү? (өөр өөр сувгаар олон сесс хийх нь зөрчлийн шинж тэмдэг байж болно)	
YCO	Сүлжээний аюулгүй байдал	- Хамгаалалтгүй эмзэг траффик ба шифрлэлтийн сул практик (АБХ: Харилцаа холбоо Аюулгүй байдал)	С79: Мобайл оператор нь SS7 халдлагын улмаас үүсэх аюулыг хязгаарлахын тулд GSMA (FS.11, FS.07, IR.82, болон IR.88)-д заасан SS7 болон диаметрийн дохиоллын аюулгүй байдлын хяналтыг байрлуулах ёстой [3]	MNO нь SS7-ийн эмзэг байдлаас хамгаалахын тулд SS7 болон диаметрийн дохионы хяналтыг хэрэгжүүлсэн үү?	Харилцаа холбоо аюулгүй байдал - Сүлжээний аюулгүй байдал удирдлага
ДСҮ Үйлчилгээ үзүүлэгч	Нууцлал ба нууцлал	- ДСҮ хэрэглэгчийн бүртгэлийн мэдээллийн хамгаалалт хангалтгүй. (АБХ: Баталгаажуулалт)	С80: ДСҮ бүртгэлд ашигладаг хэрэглэгчийн өгөгдлийг хамгаалах, хамгаалах, физик хэлбэрийг ашиглах, өгөгдлийг найдвартай хадгалах, дамжуулах.	RBAC, өгөгдлийн шифрлэлт гэх мэт аливаа мэдээлэл алдагдахаас урьдчилан сэргийлэхийн тулд хэрэглэгчийн бүртгэлд ашигладаг ДСҮ өгөгдөл, маягтуудыг найдвартай хадгалж, дамжуулж, хадгалдаг уу?	Хөрөнгийн менежмент - Хэвлэл мэдээллийн хэрэгсэлтэй харьцах
ДСҮ Үйлчилгээ үзүүлэгч	Сүлжээний аюулгүй байдал	- Сул шифрлэлт ашиглах. (АБХ: Харилцаа холбоо Аюулгүй байдал)	С81: API харилцааны хувьд TLS шифрлэлт v1.2 болон түүнээс дээш зэрэг хүчтэй шифрлэлтийн стандартыг ашиглана уу.	TLS шифрлэлтийг аюулгүй ашигладаг уу? өөрөөр хэлбэл, v.12 буюу түүнээс дээш (2020 оны 7-р сар)	Харилцаа холбоо аюулгүй байдал - Мэдээлэл дамжуулах
				Апп нь TLS-ийн хамгийн сүүлийн хувилбарыг ашигладаг уу?	
				Апп нь хуучирсан TLS хувилбарыг ашигладаг уу?	
ДСҮ Үйлчилгээ үзүүлэгч	Сүлжээний аюулгүй байдал	- ДСҮ хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (АБХ: Хандалтын хяналт)	С82: API-тай холбоотой аюул заналыг тодорхой тусгах зорилгоор аюул илрүүлэхийг өргөтгөх.	API-тай холбоотой аюулыг илрүүлэх үйл ажиллагааны хяналт байдаг уу?	Үйл ажиллагааны аюулгүй байдал - Техникийн эмзэг байдлын менежмент
				Rouge/хорлонтой API-г илрүүлэх хяналт байгаа юу?	
ДСҮ Үйлчилгээ үзүүлэгч	Хандалтын хяналт	- ДСҮ хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (АБХ: Хандалтын хяналт)	С83: Алсын зайнаас нэвтрэх хандалтыг хязгаарлаж, арын ДСҮ системд алсаас нэвтрэх сешнүүдийн эрхийг багасгах.	Ялангуяа алсаас нэвтэрдэг хэрэглэгчдийн хувьд ДСҮ системд хандах хандалтыг хязгаарлах хяналт байдаг уу?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
ДСҮ Үйлчилгээ үзүүлэгч	Нууцлал ба нууцлал	- ДСҮ хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (АБХ: Хандалтын хяналт)	С84: TLS гэрчилгээний ашиглалтын хугацааг 825 хоногоор хязгаарлах.	TLS насан туршийн гэрчилгээ шинэчлэгдсэн үү? Өөрөөр хэлбэл гэрчилгээний нас 825 хоногоос бага байх ёстой	Харилцаа холбоо-tions security - Сүлжээний аюулгүй байдал удирдлага

(үргэлжлэл)

ДСУ Үйлчилгээ үзүүлэгч	Баталгаажуулалт	- ДСУ хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (АБХ: Хандалтын хяналт)	С85: ДСУ системд холбогдсон бүх давуу эрхтэй хэрэглэгчид, агентууд болон худалдаачдын хэрэглэгчийн IP, төхөөрөмж болон нэвтрэх цагийг баталгаажуулна уу. Жишээлбэл, худалдаачин болон төлөөлөгчийн ДСУ системд хандах хандалтыг зөвхөн арилжааны нээлттэй цагаар ашиглах боломжтой байхаар тохируулаарай.	Давуу эрхтэй хэрэглэгчдийг баталгаажуулах хяналт байдаг уу? Жишээлбэл, IP баталгаажуулалт, нэвтрэх хугацааг шалгах замаар?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
ДСУ Үйлчилгээ үзүүлэгч	Сүлжээний аюулгүй байдал	- ДСУ хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (АБХ: Хандалтын хяналт)	С86: Үйлдвэрлэлийн платформ руу шилжихийн өмнө код болон өөрчлөлтийг туршилтын орчинд туршиж үзэх шаардлагатай; туршилтын орчин нь үйлдвэрлэлийн орчноос физик болон логикийн хувьд тусгаарлагдсан байх ёстой.	Кодын өөрчлөлтийг үйлдвэрлэлд шилжүүлэхээс өмнө туршиж, баталгаажуулсан уу? Жишээлбэл, кодыг туршиж үзсэн хэрэглэгчийн болон дотоод хүлээн авах гэрчилгээ.	Системийг олж авах, хөгжүүлэх, засвар үйлчилгээ хийх - Хөгжүүлэлт ба дэмжих үйл явц дахь аюулгүй байдал

Нөлөөлөлд өртсөн тал	Бүлэг	Эрсдэл ба эмзэг байдал	Хяналт	Аюулгүй байдлын аудитын асуулт	Холбогдох бодлого эсвэл журам
ДСУ Үйлчилгээ үзүүлэгч	Сүлжээний аюулгүй байдал	- ДСУ хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (АБХ: Хандалтын хяналт)	С87: Аюулгүй байдлыг сайжруулахын тулд хэрэглэгчийн ПИН код, гүйлгээ, жетон, мөнгөний эрхийн бичгийг хамгаалахын тулд процессыг найдвартай удирдаж, криптограф түлхүүрүүдийг хадгалахын тулд Тоног төхөөрөмжийн аюулгүй байдлын модуль (HSM) гэх мэт хөндлөнгийн хамгаалалттай төхөөрөмжийг ашиглана уу.	ДСУ үйлчилгээ үзүүлэгч нь криптограф түлхүүрүүдийг найдвартай хадгалах механизмтай юу?	Криптограф - Криптографийн хяналт
ДСУ Үйлчилгээ үзүүлэгч	Хандалтын хяналт	- ДСУ хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (АБХ: Хандалтын хяналт)	С88: Хамгийн бага давуу эрхийн зарчимд тулгуурлан хандалтын эрхийг тодорхойлохын тулд хэрэглэгчийн үүргийг тохируулна.	ДСУ үйлчилгээ үзүүлэгч нь дүрд суурилсан хандалтын хяналтыг ашигладаг уу?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
ДСУ Үйлчилгээ үзүүлэгч	Хандалтын хяналт	- ДСУ хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (АБХ: Хандалтын хяналт)	С89: Хэрэглэгч, төлөөлөгч, худалдаачин, төлбөрийн үйлчилгээ үзүүлэгч эсвэл гуравдагч этгээдийн үйл ажиллагааг дуусгавар болгосны дараа холбогдох бүртгэлийг идэвхгүй болгох/идэвхгүй болгох	Дууссан ДСУ администраторууд, агентууд болон хэрэглэгчдийн нэвтрэх үнэмлэх идэвхгүй болсон уу? Унтсан ДСУ дансууд идэвхгүй болсон уу?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
ДСУ Үйлчилгээ үзүүлэгч	Хандалтын хяналт	- ДСУ хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (АБХ: Хандалтын хяналт)	С90: Бүртгэлийн зогсолтын хугацааг тогтоож, зогсолттой байгаа дансыг хугацаа дуусахад идэвхгүй болгоно.	ДСУ үйлчилгээ үзүүлэгч нь идэвхгүй админ акаунтуудыг идэвхгүй болгох үнтрах хугацааг тогтоосон уу? Идэвхгүй байгаа бүх дотоод ажилтнууд болон API дансууд идэвхгүй болсон уу?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
ДСУ Үйлчилгээ үзүүлэгч	Залилан илрүүлэх	- ДСУ хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (АБХ: Хандалтын хяналт)	С91: ДСУ-ийн үүрэг дээр үндэслэн нэвтрэх болон сессийн хязгаарлалтуудын хуваарийг тохируулах. (сессийн хязгаарлалт нь дүрд үндэслэн өдөрт хамгийн их буцаах тоог багтааж болно)	ДСУ үйлчилгээ үзүүлэгч нь дүрд суурилсан хандалтын хяналтыг хэрэгжүүлдэг үү?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
ДСУ Үйлчилгээ үзүүлэгч	Залилан илрүүлэх	- ДСУ хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (АБХ: Хандалтын хяналт)	С92: Хэрэглэгч нэмэх, өөрчлөх, устгах зэрэг ДСУ системд нэвтрэх эрхийг хязгаарлах, хянах, үе үе хянах.	Захиргааны эрх ямбаны эрхийг шалгах механизм бий юу?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
ДСУ Үйлчилгээ үзүүлэгч	Нууцлал ба нууцлал	- ДСУ хэрэглэгчийн хандалтын хяналт, хяналт хангалтгүй. (АБХ: Хандалтын хяналт)	С93: API-ийн хэрэглээг хянах, гуравдагч этгээдтэй хуваалцсан бүх өгөгдлийг шифрлэх, мэдээлэл/мэдээлэл алдагдахаас зайлсхийхийн тулд төлбөрийн үйлчилгээ үзүүлэгчтэй байгуулсан нууцлалын гэрээ гэх мэт мэдээллийн удирдлагын журам, хяналтыг бий болгох.	API-ээр дамжуулан өгөгдөл солилцохыг хянах хяналтын механизм байгаа юу?	Харилцаа холбоо-tions security - Сүлжээний аюулгүй байдал удирдлага
				Мэдээлэл алдагдахаас сэргийлэх хяналт байдаг уу?	
ДСУ Үйлчилгээ үзүүлэгч	Сүлжээний аюулгүй байдал	- Утасгүй сүлжээний хяналт хангалтгүй (АБХ: Мэдээллийн нууцлал)	С94: PCI DSS шаардлагын дагуу утасгүй дамжуулалтыг хамгаална. Хяналтад дараахь зүйлийг багтаах ёстой, гэхдээ үүгээр хязгаарлагдахгүй.	Сүүлгах үед шифрлэлтийн түлхүүрүүдийг анхдагчаас өөрчилсөн үү? Өгөгдмөл SNMP мөрүүд өөрчлөгдсөн үү?	Харилцаа холбоо-tions security - Сүлжээний аюулгүй байдал удирдлага
			- Үйлдвэрлэгчийн өгөгдмөл шифрлэлтийн түлхүүр, нууц үг, SNMP нийгэмлэгийн мөрүүдийг өөрчилсөн эсэхийг шалгаарай.		
			- Баталгаажуулах, дамжуулахад хүчтэй шифрлэлтийг хэрэгжүүлэхийн тулд салбарын шилдэг туршлагыг ашиглахад дэмжлэг үзүүлэх.		

(үргэлжлэл)

			- Интернэтэд холбогдсон сервер дээр тодорхой бичвэртэй дансны өгөгдөл хадгалагдахгүй байхыг баталгаажуулах.		
Гуравдагч этгээд	Нууцлал ба нууцлал	- Төхөөрөмжийг устгахаас өмнө өгөгдлийг устгах/устгах явцад алдаа гарсан (АБХ: Нууцлал)	С95: ДСҮ үйлчилгээ үзүүлэгч/худалдаачид хүүчин төхөөрөмжүүдээ тогтмол устгаж байх ёстой. Шийдэл нийлүүлэгч зааварчилгаа өгөх үед худалдаачин үүнийг дагаж мөрдөх ёстой. Зарим зүйлийг анхаарч үзэх хэрэгтэй:	ДСҮ-тэй холбоотой өгөгдлийг устгахдаа аюулгүй байдлын удирдамжийг дагаж мөрддөг үү?	Үйл ажиллагааны аюулгүй байдал - Хортой программаас хамгаалах
			- Бүх шошго болон бизнесийн танигчийг устгана уу.		
			- Боломжтой бол цахим материал, эд ангиудыг найдвартай устгахад туслах эрх бүхий борлуулагчтай гэрээ байгуул.		
			- Өөрийн бизнестэй холбоотой төхөөрөмжийг хогийн сав, хогийн саванд бүү хая.		

Нөлөөлөлд өртсөн тал	Бүлэг	Эрсдэл ба эмзэг байдал	Хяналт	Аюулгүй байдлын аудитын асуулт	Холбогдох бодлого эсвэл журам
Гуравдагч этгээд, ДСҮ Үйлчилгээ үзүүлэгч	Сүлжээний аюулгүй байдал	- Худалдан авсан гар утасны төхөөрөмжийн аюулгүй байдлын талаар шийдэл нийлүүлэгчтэй хангалтгүй хамтын ажиллагаа (АБХ: Боломж ба Нууцлал)	С99: Худалдаачид болон ДСҮ үйлчилгээ үзүүлэгчид шийдэл нийлүүлэгчээсээ дараахь зүйлийг шаардах ёстой.	Програм хангамжийн шинэчлэлтийг хянах журам байдаг уу, шинэчлэлтүүдийг аюулгүйгээр суулгасан уу ?	Үйл ажиллагааны аюулгүй байдал - Техникийн эмзэг байдлын менежмент
			- Шийдэл нийлүүлэгч нь төлбөрийн програмаа тогтмол шинэчилж, шинэчлэлтүүд бэлэн байгаа бөгөөд суулгахад аюулгүй гэдгийг худалдаачдад зааж өгөх ёстой.		
			- Шийдэл нийлүүлэгч нь зөвхөн зөвшөөрөгдсөн програм хангамжийг ажиллуулж байгаа төхөөрөмж дээр ажиллахын тулд төлбөрийн програмдаа хязгаарлалт тавих ёстой.		
			- Шийдэл нийлүүлэгч нь худалдаачны дагаж мөрдөх шаардлагатай шинэчлэлтийн жүрмыг нарийвчлан харуулсан баримт бичгийг нийлүүлэх ёстой.		
			- ДСҮ шийдлийн үйлчилгээ үзүүлэгч нь ДСҮ үйлчилгээ үзүүлэгчтэй харилцаж, төлбөр хүлээн авах шийдэлд шинээр илэрсэн сул талуудын талаар тэдэнд мэдэгдэх ёстой. Нэмж дурдахад, шийдлийн үйлчилгээ үзүүлэгч нь шинэ эмзэг байдал илэрсэн үед худалдаачдыг удирдан чиглүүлэхээс гадна эдгээр эмзэг байдлын аль нэгийг шалгасан засваруудыг өгөх ёстой.		
Гуравдагч этгээд, ДСҮ Үйлчилгээ үзүүлэгч	Залилан илрүүлэх	- Илрүүлээгүй системийн програмын сул талуудыг нээх (АБХ: Өгөгдөл Нууцлал)	С100: Худалдаач нь аливаа аудит эсвэл бүртгэл хөтлөх чадварыг идэвхжүүлэхийн тулд шийдэл нийлүүлэгчтэйгээ хамтран ажиллах ёстой. Шийдэл нийлүүлэгч нь хэвийн бус үйл явдлуудыг илрүүлэх хангалттай нарийвчлалтайгаар бүртгэл хөтлөх чадвартай эсэхийг баталгаажуулах ёстой.	Өгөгдсөн аудитын бүртгэлүүд нь ДСҮ үйлчилгээнд нөлөөлж буй ДСҮ систем эсвэл MNO систем дээрх бүх өөрчлөлтийг хангалттай хянаж чадаж байна уу?	Үйл ажиллагааны аюулгүй байдал - Техникийн эмзэг байдлын менежмент
			Шийдэл нийлүүлэгч нь бүртгэлийг шалгахын тулд худалдаачны хариуцлагын талаар худалдаачинд чиглүүлэх ёстой. Нэмж дурдахад системийн бүртгэл, тайланг хэвийн бус үйл ажиллагаатай эсэхийг тогтмол шалгана. Хэрэв хэвийн бус үйл ажиллагаа сэжиглэгдсэн эсвэл илэрсэн бол асуудлыг шийдэж дуустал мобайл төхөөрөмж болон түүний төлбөрийн аппликейшнд хандахыг зогсооно уу. Хэвийн бус үйлдлүүд нь зөвшөөрөлгүй нэвтрэх оролдлого, өргөжүүлсэн эрх, программ хангамж эсвэл програм хангамжийн зөвшөөрөлгүй шинэчлэлтүүд орно, гэхдээ үүгээр хязгаарлагдахгүй.		

(үргэлжлэл)

Гуравдагч этгээд, ДСУ үйлчилгээ үзүүлэгч	Сүлжээний аюулгүй байдал	- Сүлжээнд гадны халдлагад өртөх (АБХ: Боломж)	С101: ДСУ програмууд нь аюулгүй байдлын нэвтрэлтийн сканнер, нэвтрэлтийн шалгалтанд тогтмол хамрагдах ёстой. Ялангуяа программууд нь фишинг программ хангамжийн эсрэг бат бөх байхаар бүтээгдсэн байх ёстой.	ДСУ системийн нэвтрэлтийн туршилтыг тогтмол хийдэг үү?	Үйл ажиллагааны аюулгүй байдал - Техникийн эмзэг байдлын менежмент
MNO	Бэлэн байдал	- Сүлжээнд гадны халдлагад өртөх (АБХ: Боломж)	С107: Системийн хүртээмжид нөлөөлж болзошгүй халдлагад өртөх эсэхийг шалгахын тулд MNO дэд бүтцийн эмзэг байдлын сканнер болон нэвтрэлтийн тестийг тогтмол хийнэ.	ДСУ систем дээр тогтмол эмзэг байдлын скан хийдэг үү?	Үйл ажиллагааны аюулгүй байдал - Техникийн эмзэг байдлын менежмент
MNO	Сүлжээний аюулгүй байдал	- Сүлжээнд гадны халдлагад өртөх (АБХ: Боломж)	С108: Хамгийн сүүлийн үеийн вирусын эсрэг программ хангамжийг (хэрэв байгаа бол) суулгаж, тогтмол шинэчилж, үүнийг эцсийн хэрэглэгчид ашиглах боломжтой болго. Хортой программ хангамж, программ хангамжаас урьдчилан сэргийлэх, үстгах зорилгоор MDM (Мобайл төхөөрөмжийн менежмент) шийдэлтэй хамт хэрэглэж болох програмын багцыг авч үзье.	ДСУ системийг шинэ аюулаас хамгаалахын тулд хамгийн сүүлийн хувилбар болгон шинэчилсэн үү?	Үйл ажиллагааны аюулгүй байдал - Хортой програмаас хамгаалах
YCO, ДСУ үйлчилгээ үзүүлэгчид болон гуравдагч этгээдүүд	Сүлжээний аюулгүй байдал	- Байршуулсан системийн эсрэг шинэ мөлжлөгүүдийг илрүүлэх, эдгээр мөлжлөгийн эсрэг шийдлийг ашиглах боломжгүй байх (АБХ: Өгөгдлийн нууцлал, Хандалтын хяналт, Боломжтой байдал)	С109: YCO -ууд ДСУ үйлчилгээ үзүүлэгч болон төлбөрийн үйлчилгээ үзүүлэгчдийн хамт хүүчин эмзэг байдлаас үүссэн халдлагаас хамгаалахын тулд борлуулагчаас өгсөн хамгийн сүүлийн үеийн хувилбарт системийг нөхөх ёстой.	ДСУ системүүд нь мэдэгдэж бүй эмзэг байдлын эсрэг засвар хийгдсэн үү?	Үйл ажиллагааны аюулгүй байдал - Техникийн эмзэг байдал
MNO, ДСУ үйлчилгээ үзүүлэгчид болон гуравдагч этгээдүүд	Хандалтын хяналт	- Байршуулсан системийн эсрэг шинэ мөлжлөгүүдийг илрүүлэх, эдгээр мөлжлөгийн эсрэг шийдлийг ашиглах боломжгүй байх (АБХ: Өгөгдлийн нууцлал, Хандалтын хяналт, Боломжтой байдал)	С110: Зэрлэг байгальд тэг өдрийн халдлага илэрсэн тохиолдолд үйлчилгээ үзүүлэгч болон MYO-ууд засвар үйлчилгээ хийх, системийн засварыг хурдан шуурхай авахын тулд борлуулагчидтай хамтран гэнэтийн төлөвлөгөөтэй байх ёстой. Энэхүү стратегийн нэг хэсэг нь нөөцлөлтийг зөв ашиглах явдал юм.	ДСУ системд шинэ аюул заналхийлэл, халдлагыг удирдах бодлого, үйл явц байгаа юу?	Үйл ажиллагааны аюулгүй байдал - Техникийн эмзэг байдлын менежмент
YCO	Сүлжээний аюулгүй байдал	- ДСУ дэд бүтцэд холбогдсон аюулгүй төхөөрөмжүүд (АБХ: Өгөгдлийн бүрэн бүтэн байдал)	С111: YCO нь ДСУ системд холбогдох эсвэл өөр аргаар хандахад ашигладаг төхөөрөмжүүдийг хянаж байх ёстой бөгөөд эдгээр төхөөрөмжүүд нь хамгийн сүүлийн үеийн засварууд, шинэчлэгдсэн вирусын эсрэг программ хангамж, rootkit болон түлхүүр бүртгэгчид сканнердсан, сүлжээ өргөтгөгчийг дэмждэггүй эсэхийг шалгах ёстой.	ДСУ системд холбогдоход ашигладаг бүх төхөөрөмжийг аюул заналхийлсэн эсэхийг шалгаж, хамгийн сүүлийн үеийн програм хангамжийн засваруудыг шалгасан уу?	Үйл ажиллагааны аюулгүй байдал - Техникийн эмзэг байдлын менежмент
	Баталгаажуулалт	- ДСУ дэд бүтцэд хэт зөвшөөрөгдсөн хандалт (АБХ: Баталгаажуулалт)	С115: ДСУ хэрэглэгчдийг баталгаажуулахын өмнө боломжтой бол хэрэглэгчийн IMSI, төхөөрөмж, байршил, IP хаягийг баталгаажуулж, сүлжээний дэд бүтцэд зөвшөөрөлгүй нэвтрэхээс сэргийлж, тэдний таних тэмдэгийг тогтооно.	ДСУ үйлчилгээ үзүүлэгч нь SIM солихоос хамгаалахын тулд ДСУ гүйлгээнд ашигладаг гар утасны дугааруудын IMSI-г шалгаж байна уу?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
Гуравдагч этгээдийн үйлчилгээ үзүүлэгч	Залилан илрүүлэх	- Гүйлгээний баталгаажуулалт хангалтгүй (АБХ: Татгалзахгүй)	С116: Төлбөрийн үйлчилгээ үзүүлэгч нь ДСУ данстай холбогдсон ерөнхий зориулалтын дахин цэнэглэх боломжтой картууд нь ПИН код эсвэл биометр зэрэг карт эзэмшигчийн баталгаажуулалтын арга бүхий EMV чип ашиглахыг шаардлагатай бол бүх гүйлгээний үр дүнд харилцагчдад анхааруулга өгөх ёстой.	ДСУ-ийн хэрэглэгчид өөрсдийн дансанд ДСУ гүйлгээ хийх үед анхааруулга авдаг уу?	Хандалтын хяналтын бодлого - Хэрэглэгчийн хандалт удирдлага
ДСУ Үйлчилгээ үзүүлэгч	Нууцлал ба нууцлал	- Туршилтын орчин дахь хяналт, хяналт хангалтгүй (АБХ: нууцлал)	С117: ДСУ үйлчилгээ үзүүлэгчид шилдэг туршлагын дагуу нэрээ нууцлахаас бусад тохиолдолд үйлдвэрлэлийн орчин дахь хэрэглэгчийн өгөгдлийг туршилтын орчинд ашиглахгүй байхыг баталгаажуулах ёстой. Үүний эсрэгээр, туршилтын өгөгдлийг бүтээгдэхүүн рүү шилжүүлж болохгүй.	Туршилт болон үйлдвэрлэлийн орчинд хэрэгжсэн өгөгдлийг зөв тусгаарлах боломжтой юу? Туршилтын зорилгоор хэрэглэгчийн өгөгдлийг ашиглахыг хязгаарласан үйл явц байдаг уу? Өгөгдлийн нэргүй болгох гэх мэт.	Хөрөнгийн менежмент - Хэвлэл мэдээллийн хэрэгсэлтэй харьцах

(үргэлжлэл)

Гуравдагч этгээдийн үйлчилгээ үзүүлэгч	Нууцлал ба нууцлал	- Хэрэглэгчийн мэдрэмтгий мэдээллийг гүйлгээ эсвэл API-ээр дамжуулан ил гаргах (АБХ: нууцлал)	C118: Гуравдагч талын үйлчилгээ үзүүлэгчид төлбөрийн үйлчилгээ үзүүлэгч болон ДСУ үйлчилгээ үзүүлэгч зэрэг бусад талуудтай мэдээлэл хуваалцахыг гүйлгээний бүрэн бүтэн байдлыг хангахад шаардагдах хамгийн бага хэмжээнд хязгаарлах ёстой.	Гүйлгээ хийгдэж байх үед гуравдагч этгээдтэй хуваалцах өгөгдлийг хязгаарласан процессууд байдаг уу?	Хөрөнгийн менежмент - Хэвлэл мэдээллийн хэрэгсэлтэй харьцах
Гуравдагч этгээдийн үйлчилгээ үзүүлэгч	Нууцлал ба нууцлал	- Мэдээлэл хамгаалах хяналт хангалтгүй (АБХ: нууцлал)	C119: Үйлчилгээ үзүүлэгч нар хэрэглэгчийн мэдрэмтгий өгөгдлийг үл мөрийн бүртгэл (жишээлбэл, бэлэн мөнгө авах эрхийн бичгийн код, банкны дансны дугаар, итгэмжлэл) зэрэг орчноос устгасан байх ёстой. Бүртгэлийн файлд энэ өгөгдлийг харуулахын тулд боломжтой бол газар эзэмшигчийг ашиглана уу.	Үйл явдлын бүртгэлд PIN гэх мэт хэрэглэгчийн мэдрэмтгий өгөгдөл агуулагддаг уу?	Үйл ажиллагааны аюулгүй байдал - Бүртгэл, хяналт

Дээрх мэдээллийг бүтнээр нь дараах холбоосоор татаж авах боломжтой:
https:// itu .int/ en/ ITU -T/ extcoop/figisymposium/ Documents/Digital %20Financial %20Services %20security %20audit %20checklist .xlsm

4. АЮУЛГҮЙ БАЙДЛЫН АУДИТЫН ШАЛГАЛТЫН ЖАГСААЛТ

4.1. Хандалтын хяналт

4.1.1. Дууссан ДСҮ администраторууд, агентууд болон хэрэглэгчдийн нэвтрэх үнэмлэх идэвхгүй болсон уу. ДСҮ дансууд идэвхгүй болсон уу?

4.1.2. ДСҮ систем болон ДСҮ системд холбогдсон бүх системээс анхдагч системийн бүртгэлүүд хасагдсан уу?

4.1.3. Дэмжлэгийн ажил дууссаны дараа ДСҮ борлуулагч болон туслах системийн данс идэвхгүй болсон уу?

4.1.4. ДСҮ хэрэглэгчийн сессүүдэд дараах логик хяналтуудыг тохируулсан уу: i) автоматаар гарах нэг удаагийн нэвтрэлтийн хугацаа дуусах ii) нууц үгээр нэвтрэх хамгийн их амжилтгүй оролдлого iii) Нууц үг болон ПИН-ийн нарийн төвөгтэй байдал. Iv) Нууц үг/ПИН кодыг дахин ашиглах хугацаа

4.1.5. ДСҮ үйлчилгээ үзүүлэгчийн хувьд сэжигтэй SIM солих болон SIM дахин боловсруулалтыг илрүүлэх журам байдаг уу?

4.1.6. Олон сувгаар нэгэн зэрэг нэвтэрч орохоос сэргийлэх хяналт байдаг уу? ДСҮ үйлчилгээ үзүүлэгч нь ДСҮ сүлжээнд холбогдохын тулд нэг удаад зөвхөн нэг сессийг зөвшөөрдөг үү? (өөр өөр сувгаар олон сесс хийх нь зөрчлийн шинж тэмдэг байж болно)

4.1.7. Ялангуяа алсаас нэвтэрдэг хэрэглэгчдийн хувьд ДСҮ системд хандах хандалтыг хязгаарлах хяналт байдаг уу?

4.1.8. ДСҮ системд шинэ аюул заналхийлэл, халдлагыг удирдах бодлого, үйл явц байгаа юу?

4.1.9. ДСҮ дэд бүтцэд нэвтрэх эрхийг хязгаарлахад хангалттай физик болон логик саад бэрхшээл бий юу?

4.1.10. ДСҮ үйлчилгээ үзүүлэгч нь дүрд суурилсан хандалтын хяналтыг ашигладаг уу?

4.1.11. ДСҮ систем нь хэрэглэгчийн профайл дээр тулгуурлан загвараас гадуур гүйлгээг илрүүлэх чадвартай юу? Жишээ нь: ДСҮ үйлчилгээ үзүүлэгч нь байршилд суурилсан гүйлгээний баталгаажуулалтыг ашиглан гүйлгээний жинхэнэ эсэхийг шалгадаг уу, жишээлбэл, гео хурдыг хянах эсвэл бусад хэрэгслээр дамжуулан?

4.1.12. ДСҮ үйлчилгээ үзүүлэгч нь хэрэглэгчийн нэгэн зэрэг нэвтрэх эрхийг хязгаарлаж, хэрэглэгчдэд бусад нэвтрэх сувгуудыг сонгох боломжийг олгосон уу? Жишээлбэл, USSD ашигладаг хэрэглэгчид ДСҮ үйлчилгээ үзүүлэгч энэ сувгаар нэвтрэх эрхийг идэвхжүүлэхээс өмнө ДСҮ програмын сувгийг сонгох боломжтой юу?

4.1.13. ДСҮ үйлчилгээ үзүүлэгч нь идэвхгүй админ акаунтуудыг идэвхгүй болгох унтрах хугацааг тогтоосон уу? Идэвхгүй байгаа бүх дотоод ажилтнууд болон API дансууд идэвхгүй болсон уу?

4.1.14. ДСҮ үйлчилгээ үзүүлэгч USSD болон STK ДСҮ сешнүүдийг хэрэглэгч тодорхой хугацаанд идэвхгүй байх үед автоматаар салгахаар тохируулсан уу?

4.1.15. ДСҮ үйлчилгээ үзүүлэгч нь гүйлгээг боловсруулахаас өмнө бодит цагийн төхөөрөмжийн баталгаажуулалтыг хийж байна уу?

4.1.16. Нууц үг найдвартай дамжуулагдсан уу? Хэрэглэгч анх удаа нэвтэрсний дараа нууц үгээ солих шаардлагатай юу?

4.1.17. Бүртгэл түгжигдэхээс өмнө амжилтгүй нэвтрэх оролдлогын дээд хязгаар бий юу?

4.1.18. Биометрийн баталгаажуулалт гэх мэт өмнө нь идэвхгүй байсан дансуудыг идэвхжүүлэхийн өмнө хэрэглэгчийн хувийн мэдээллийг баталгаажуулах хангалттай арга бий юу?

4.2. Баталгаажуулалт

4.2.1. SIM солих үйлдлээс өмнө хэн болохыг баталгаажуулах үйл явц, бодлого хэрэгжиж байна уу? SIM солихыг баталгаажуулах хүртэл мэдээлэл алдагдах, дамжуулахаас урьдчилан сэргийлэх техникийн механизм бий юу?

4.2.2. ДСҮ хэрэглэгчийн баталгаажуулалтын итгэмжлэлүүд өөр сувгаар/хамтаас гадуур дамждаг уу? (жишээ нь, хэрэв дансны тохиргоог USSD сувгаар хийсэн бол цахим шуудан эсвэл дүут дуудлагаар дамжуулдаг нэг удаагийн нууц үг үү?)

4.2.3. Зөвшөөрөгдсөн хэрэглэгчдийг шалгах хяналт байгаа юу? Жишээлбэл, IP баталгаажуулалт, нэвтрэх хугацааг шалгах замаар?

4.2.4. ДСҮ аппликейшн нь хувийн дансны дугаар/мэдрэмжтэй баталгаажуулалтын өгөгдлийг SMS/имэйлээр энгийн текст хэлбэрээр хадгалдаг уу?

4.2.5. ДСҮ үйлчилгээ үзүүлэгч нь бүх хандалтын хүсэлтэд серверт суурилсан нэвтрэлт танилтыг хэрэгжүүлдэг үү?

4.2.6. Мобайл сүлжээний оператор SIM солих эсвэл SIM солихын өмнө биометрийн баталгаажуулалтыг хийдэг үү?

4.2.7. Мобайл сүлжээний оператор нь IMSI, Kc, Ki гэх мэт SIM өгөгдлийг найдвартай хадгалдаг уу?

4.2.8. Хэрэглэгчийг баталгаажуулахад олон хүчин зүйлийг ашигладаг уу?

4.2.9. ДСҮ бүртгэлтэй холбогдох үед олон хүчин зүйлийн баталгаажуулалтыг ашигладаг уу?

4.2.10. ДСҮ үйлчилгээ үзүүлэгч нь ДСҮ дансны SIM солих эсвэл SIM солихыг илрүүлэх боломжтой юу?

4.2.11. ДСҮ үйлчилгээ үзүүлэгч нь SIM солихоос хамгаалахын тулд ДСҮ гүйлгээнд ашигладаг гар утасны дугаарууудын IMSI-г шалгаж байна уу?

4.2.12. ДСҮ үйлчилгээ үзүүлэгч нь ДСҮ дансны SIM картыг дахин боловсруулах үйл явцад оролцдог уу?

4.2.13. ДСҮ үйлчилгээ үзүүлэгч API болон USSD хүсэлтээр өгөгдөлд XML баталгаажуулалт хийж байна уу? Жишээлбэл, оролтын баталгаажуулалт, дүн, дүнгийн тусгай тэмдэгт, валютын чек гэх мэт

4.2.14. ДСҮ хэрэглэгчийн дансанд өндөр дүнтэй гүйлгээ, өөрчлөлт хийх нэмэлт зөвшөөрөл, баталгаажуулалт байгаа юу? Жишээлбэл, гүйлгээний хязгаарыг нэмэгдүүлэхэд ямар нэмэлт шалгалт хийдэг вэ?

4.2.15. ДСҮ систем нь хэрэглэгчийн профайл дээр тулгуурлан загвараас гадуур гүйлгээг илрүүлэх чадвартай юу? ДСҮ үйлчилгээ үзүүлэгч нь хэрэглэгчийн гүйлгээний профайлд үндэслэн шалгалт хийж байна уу? Жишээлбэл, агент дэлгүүрүүд хожуу гүйлгээ хийдэг, ДСҮ хэрэглэгчид хоёр өөр байршилд гүйлгээ хийдэг үү?

4.3. Боломжтой байдал

4.3.1. Системийн сул зогсолтын үед менежментийг баталгаажуулах бодлого бий юу?

4.3.2. ДСҮ системд өөрчлөлт, шинэчлэлт хийсний дараа төгсгөл хүртэлх туршилтууд хийгдсэн үү? Төгсгөлийн туршилтууд нь хүчин чадлын туршилт, аюулгүй байдлын тест, QoS тест, хэрэглэгчийн хүлээн авах тест гэх мэтийг агуулж болно.

4.3.3. ДСҮ систем дээр тогтмол эмзэг байдлын скан хийдэг үү?

4.3.4. Үйлчилгээний хүртээмжийг хангах систем бий юу? Жишээ (үйлчилгээний илүүдэл) Системийн хариу өгөх хугацаа болон ажиллахгүй байх хугацааг хэмжих тайлан, хэрэгслүүд байдаг уу?

4.3.5. Үйлчилгээний чанар, туршлагын чанарыг хэмжих систем байдаг уу? QoS болон QoE нь ДСҮ-ийн стандартад нийцэж байна уу?

4.3.6. ДСҮ үйлчилгээ үзүүлэгч байгын хуваарьт нөөцлөлттэй юу? Нөөцлөлтүүд нь шифрлэгдсэн бөгөөд гаднах байршилд хадгалагддаг уу?

4.4. Залилан илрүүлэх

4.4.1. ДСҮ бүртгэлийг хөндлөнгийн хамгаалалттай модульд найдвартай хадгалдаг уу? Жишээлбэл, SIEM

4.4.2. Өгөгдлийн санд өөрчлөлт оруулах, өөрчлөхийг илрүүлэх механизм бий юу?

4.4.3. SMS болон дуудлагын хуурамч байдлыг илрүүлэх механизм бий юу? Жишээлбэл, CLI шинжилгээ?

4.4.4. Дансны эгзэгтэй өөрчлөлтийг хянаж, батлах хангалттай хяналт байгаа юу? Жишээ нь, өөрчлөлт хийхээс өмнө үйлдвэрлэгч шалгагч, батлах процесс байдаг уу?

4.4.5. Төлбөрийн API-ээр дамжуулан хийгдсэн гүйлгээг хянах хангалттай механизм бий юу? ДСҮ үйлчилгээ үзүүлэгч нь гуравдагч этгээдтэй хэрэглэгчийн нууц мэдээллийг задруулахгүй байх гэрээтэй юу? Гуравдагч этгээдтэй өгөгдөл дамжуулахад хүчирхэг криптографийн алгоритмууд байдаг уу?

4.4.6. Өгөгдсөн аудитын бүртгэлүүд нь ДСҮ үйлчилгээнд нөлөөлж буй ДСҮ систем эсвэл MNO систем дээрх бүх өөрчлөлтийг хангалттай хянаж чадаж байна уу?

4.4.7. ДСҮ-ийн хэрэглэгчид өөрсдийн дансанд ДСҮ гүйлгээ хийх үед анхааруулга авдаг уу?

4.4.8. Бүртгэлийн бүртгэл болон үйл явдлын өгөгдлийн бүртгэл нь хэрэглэгчийн мэдрэмтгий өгөгдлийг авах/хадгалах уу? (жишээ нь, EDR-д хадгалагдсан хэрэглэгчийн ПИН кодууд)

4.4.9. Апп нь дараа нь дамжуулах гүйлгээг хадгалдаг уу?

4.4.10. ДСҮ үйлчилгээ үзүүлэгч нь дүрд суурилсан хандалтын хяналтыг хэрэгжүүлдэг үү?

4.4.11. Захиргааны эрхийг шалгах механизм бий юу?

4.4.12. ДСҮ-ийн чухал ажлыг гүйцэтгэхэд нэгээс олон хүн шаардлагатай юу?

4.5. Сүлжээний аюулгүй байдал

4.5.1. ДСҮ системд холбогдоход ашигладаг бүх төхөөрөмжийг аюул заналхийлсэн эсэхийг шалгаж, хамгийн сүүлийн үеийн програм хангамжийн засваруудыг шалгасан уу?

4.5.2. Кодын өөрчлөлтийг үйлдвэрлэлд шилжүүлэхээс өмнө туршиж, баталсан уу? Жишээлбэл, кодыг туршиж үзсэн хэрэглэгчийн болон дотоод хүлээн авах гэрчилгээ.

4.5.3. Суулгах үед шифрлэлтийн түлхүүрүүдийг анхдагчаас өөрчилсөн үү? Өгөгдмөл SNMP мөрүүд өөрчлөгдсөн үү?

4.5.4. .ДСУ экосистемийн цаг синхрончлогдсон уу?

4.5.5. ДСУ системүүд нь мэдэгдэж буй эмзэг байдлын эсрэг засвар хийгдсэн үү?

4.5.6. ДСУ системийг шинэ аюулаас хамгаалахын тулд хамгийн сүүлийн хувилбар болгон шинэчилсэн үү?

4.5.7. Ашигласан шифрлэлтийн алгоритмууд болон түлхүүрүүд нь хэрэглэгчийн ПИН код болон өгөгдлийг хамгаалахад хангалттай хүчтэй юу?

4.5.8. Галт ханын дүрмийг зохих ёсоор тохируулсан уу? Жишээ нь портын цагаан жагсаалт, пакет шүүлтүүр

4.5.9. Зохих тохиргоотой галт хана, замын хөдөлгөөний шүүлтүүр зэрэг сүлжээний халдлагаас хамгаалах хангалттай хамгаалалт байгаа юу?

4.5.10. Бусад бүх системээс ДСУ системд хандах хандалтыг хязгаарлах логик хил хязгаар бий юу? (Жишээ нь, бусад зөвшөөрөлгүй дотоод хэрэглэгчид сүлжээнд ДСУ боловсруулах системд хандах нь логик болон/бие махбодийн хувьд хязгаарлагдмал байдаг)

4.5.11. API-тай холбоотой аюулыг илрүүлэх үйл ажиллагааны хяналт байдаг уу? Rouge/хорлонтой API-г илрүүлэх хяналт байгаа юу?

4.5.12. ДСУ системд хүлээгдэж буй гүйлгээ, давхардсан гүйлгээ байгаа юу? Гүйлгээ бүрэн хийгдсэн үү?

4.5.13. Програм хангамжийн шинэчлэлтийг хянах журам байгаа эсэх, шинэчлэлтүүдийг найдвартай суулгасан уу?

4.5.14. Дотоод ДСУ системийн хаягуудын (өгөгдлийн сангийн IP хаяг гэх мэт) өртөлтийг хязгаарлах техникийн хяналт байдаг уу?

4.5.15. ДСУ үйлчилгээ үзүүлэгч нь криптограф түлхүүрүүдийг найдвартай хадгалах механизмтай юу?

4.5.16. ДСУ-д ашигладаг хулгайлагдсан SIM карттай холбоотой эрсдлийг бууруулахын тулд MNO нь SIM картууд дээр Хувийн түгжээ тайлах түлхүүрийг ашиглахыг шаарддаг уу?

4.5.17. MNO нь гадны SS7-д суурилсан халдлагыг илрүүлэх, хамгаалах галт ханатай юу? Жишээлбэл (захиалагчийн траффик саатуулах, зөвшөөрөлгүй USSD болон SM ашиглахаас хамгаалах галт хана)

4.5.18. MNO оператор нь дотоод сүлжээн дэх MAP мөрдөх болон протоколын анализаторын хэрэглээг хязгаарлах хяналттай юу? (SMS болон USSD мессежийг MAP протоколд энгийн текстээр дамжуулдаг)

4.5.19. MNO нь SS7-ийн эмзэг байдлаас хамгаалахын тулд SS7 болон диаметрийн дохионы хяналтыг хэрэгжүүлсэн үү?

4.5.20. Мэдэгдэж байгаа сул шифрүүдийн хэрэглээг зогсоосон уу? Шинэ шифрүүдэд байршуулалтыг бэлтгэсэн үү?

4.5.21. ДСУ үйлчилгээ үзүүлэгч оролтын баталгаажуулалтын шалгалт хийж байна уу?

4.5.22. ДСУ үйлчилгээ үзүүлэгч нь гүйлгээг боловсруулахаас өмнө хэрэглэгчийн гүйлгээний гео хурдыг шалгадаг уу?

4.5.23. Интернэт рүү чиглэсэн ДСУ програмуудын хөдөлгөөний хангалттай хяналт байгаа юу?

4.5.24. ДСУ системийн нэвтрэлтийн туршилтыг тогтмол хийдэг үү?

4.5.25. TLS шифрлэлтийг аюулгүй ашиглаж байна уу? Өөрөөр хэлбэл, v.12 буюу түүнээс дээш (2020 оны 7-р сар) Апп нь TLS-ийн хамгийн сүүлийн хувилбарыг ашигладаг уу? Апп нь хуучирсан TLS хувилбарыг ашигладаг уу?

4.5.26. Гүйлгээний баталгаажуулалтыг найдвартай OTP ашиглан хийж байна уу?

4.6. Хувь хүний нууц ба нууцлал

4.6.1. Дижитал гарын үсгийг ДСУ програмууд эсвэл гуравдагч талын үйлчилгээ үзүүлэгчид ашигладаг уу? Тоон гарын үсэг нь хангалттай хүчтэй криптограф алгоритм, түлхүүрийн хэмжээн дээр суурилсан уу? Криптографийн алгоритмуудын хэрэгжилт найдвартай, шинэчлэгдсэн эсэх, тэдгээр нь хангалттай санамсаргүй байдлыг хангаж чадаж байна уу? (Жишээ нь, хүчирхэг дижитал гарын үсгийн алгоритмд RSA, DSA, ECDSA орно. Зуйван муруй криптограф алгоритмууд нь бусад шифртэй дүйцэхүйц аюулгүй байдлыг хангахын тулд богино түлхүүрүүдийг ашиглаж болно.)

4.6.2. Хувийн болон нууц түлхүүрүүдийн найдвартай байдал, хамгаалалтыг баталгаажуулах журам байдаг уу. ? Сертификат болон бусад криптограф мэдээлэл нь үйлдлийн системийн хяналтаар хамгаалагдсан уу?

4.6.3. ДСУ системд холбогдсон гуравдагч талын үйлчилгээ үзүүлэгчдийг танихад тоон гарын үсгийг ашигладаг уу?

4.6.4. Үйлдлийн систем эсвэл програмын ашигладаг криптографийн сангуудыг зөв боловсруулж, хэрэгжүүлсэн эсэх, шинэчлэгдсэн эсэх? Криптографийн сангууд хүчтэй криптографийн шифрийг дэмждэг үү, сул шифрийг ашиглахаас сэргийлдэг үү? Хэрэглээгүй хэш алгоритмууд ашиглагдаж байгаа бөгөөд хангалттай хэллэгийн уртыг дэмждэг үү? (Өнөөдөр SHA512-оос бага зүйлийг сул гэж үздэг. MD5 болон SHA1 эвдэрсэн.) Тэгш хэмт шифрлэлтийн шифрүүдийн хувьд хүчтэй шифрийг ашигладаг бөгөөд хангалттай түлхүүрийн уртыг дэмждэг үү? (Жишээ нь, SWEET-32 халдлагын улмаас 3-DES нь илүүд үздэг шифр байхаа больсон байхад AES нь аюулгүй гэж тооцогддог бөгөөд үүнийг аль болох хурдан AES руу шилжүүлэхийг зөвлөж байна.) – Нийтийн түлхүүрийн хувьд Шифрлэлт, түлхүүрийн уртыг ашиглаж буй нийтийн түлхүүрийн алгоритмд тохирох хэмжээгээр сонгосон уу? Криптографийн алгоритм болон түлхүүрийн хэмжээг сонгохдоо олон нийтийн болон сайтар шалгасан стандартад тулгуурласан шалгуурыг ашигладаг уу? (Жишээ нь, NIST 800-57 тусгай хэвлэлд алгоритм бүрийн хамгийн бага түлхүүрийн хэмжээ болон энэ түлхүүрийн хэмжээ хэр удаан ажиллах талаар зааварчилгаа байдаг)

4.6.5. Ашигласан шифрлэлтийн алгоритмууд болон түлхүүрүүд нь хэрэглэгчийн ПИН код болон өгөгдлийг хамгаалахад хангалттай хүчтэй юу?

4.6.6. Гүйлгээ хийгдэж байх үед гуравдагч этгээдтэй хуваалцах өгөгдлийг хязгаарласан процессууд байдаг уу?

4.6.7. ДСУ-тэй холбоотой өгөгдлийг устгахдаа аюулгүй байдлын удирдамжийг дагаж мөрддөг үү?

4.6.8. Үйл явдлын бүртгэлд PIN гэх мэт хэрэглэгчийн мэдрэмтгий өгөгдөл агуулагддаг уу?

4.6.9. Аппликейшн эсвэл үндсэн үйлдлийн систем нь ДСҮ өгөгдөл эсвэл хөдөлгөөнт төхөөрөмжийг алсаас устгахад дэмжлэг үзүүлдэг үү, мөн төхөөрөмж алдагдсан эсвэл хулгайлагдсан тохиолдолд өгөгдлийг шифрлэх механизм бий юу?

4.6.10. Хэрэглээний бүх эмзэг мэдээллийг програм эсвэл үйлдлийн системээр шифрлэсэн үү? Өгөгдлийн шифрлэгдээгүй хувилбарууд нь төхөөрөмжид, жишээлбэл, түр зуурын бүфер эсвэл санах ойд хандах боломжтой юу? Сүлжээний холболтоор илгээсэн бүх мэдээлэл хүчтэй шифрлэлтийн шифрээр шифрлэгдсэн үү? (Хүчтэй шифрлэлтийн шифр гэж юу болох талаар дэлгэрэнгүй ярихыг хүсвэл С17-г үзнэ үү.)

4.6.11. Хүчтэй шифрлэлтийн шифр, мессежийн баталгаажуулалтын код зэрэг бүрэн бүтэн байдлыг хамгаалах механизмыг төхөөрөмж дээр хадгалагдсан өгөгдөл болон арын ДСҮ системд дамжуулах үед ашигласан уу? (Хүчтэй шифрлэлтийн алгоритмуудын талаар ярилцахыг С17-г үзнэ үү.) Хэрэглэгчийн нууц мэдээллийн хариу үйлдлийг баталгаажуулах бодлого бий юу?

4.6.12. Туршилтын өгөгдөл болон туршилтын хэрэглэгчийн бүртгэлийг прогомын ажиллах орчноос устгасан уу?

4.6.13. Хэрэглэгчийн бүртгэлд ашигладаг ДСҮ өгөгдөл, маягтуудыг RBAC, өгөгдлийн шифрлэлт гэх мэт мэдээллийн алдагдлаас урьдчилан сэргийлэхийн тулд найдвартай хадгалж, дамжуулж, хадгалдаг уу?

4.6.14. TLS насан туршийн гэрчилгээ шинэчлэгдсэн үү? Өөрөөр хэлбэл, гэрчилгээний нас 825 хоногоос бага байх ёстой.

4.6.15. Амралт байгаа өгөгдлийг шифрлэж, найдвартай хадгалах механизм бий юу?

4.6.16. API-уудаар дамжуулан өгөгдөл хуваалцахыг хянах хяналтын механизм байгаа юу? Мэдээлэл алдагдахаас сэргийлэх хяналт байдаг уу?

4.6.17. Гуравдагч этгээдтэй гүйлгээ хийх явцад хуваалцсан хэрэглэгчийн нууц мэдээлэлд хязгаарлалт байгаа юу? (жишээ нь: Зөвхөн гүйлгээг боловсруулахад шаардлагатай мэдээллийг гуравдагч этгээдтэй хуваалцана)

4.6.18. Туршилт болон үйлдвэрлэлийн орчинд хэрэгжсэн өгөгдлийг зөв тусгаарласан уу? Туршилтын зорилгоор хэрэглэгчийн өгөгдлийг ашиглахыг хязгаарласан үйл явц байдаг уу? Өгөгдлийн нэргүй болгох гэх мэт.

6 BIBLIOGRAPHY

[1] K. Butler and V. Mauree, “Digital Financial Service Security Assurance Framework,” https:// www .itu .int/ en/ ITU -T/ extcoop/ figisymposium/ Documents/ ITU _SIT _WG _Technical %20report %20on %20Digital %20Financial %20Services %20Security %20Assurance %20Framework _f .pdf.

[2] “Information Security Management” https:// www .iso .org/ isoiec -27001 -information -security .html .

[3] A. Klinger, "SS7 vulnerabilities and mitigation measures for Digital Financial Services transaction," http:// itu .int/ en/ ITU -T/ extcoop/ figisymposium/ Documents/ ITU _SIT _WG _Technical %20report %20on %20the %20SS7 %20vulnerabilities %20and %20their %20impact %20on %20ДСУ %20transactions _f .pdf .

[4] "Digital Financial Services audit checklist,"https:// itu .int/ en/ ITU -T/ extcoop/ figisymposium/ Documents/ Digital %20Financial %20Services %20security %20audit %20checklist .xlsm.