

Infoturbekataloog

Tabel 1. Protsessimoodulid

Protsessimoodulid	
GRC. Turbehaldus	
GRC.1. Infoturbe haldus üldiselt	Esitada infoturbe halduse süsteemi rajamise ja täiustamise meetmed ning turbekontseptsiooni väljatöötamise juhised
GRC.2. Infoturbe korraldus	Esitada meetmed infoturbe korralduse sobitamiseks organisatsiooniga ning infoturbe haldamiseks. Käsitletakse infoturbeprotsesside haldust ja infoturbeülesandeid organisatsioonis
GRC.3. Varade haldus	Esitada meetmed, mis tagavad organisatsiooni varade kaitse ja halduse kogu vara elutsükli vältel ning toetavad varade tervikluse säilitamist ja asutuse turvalist toimimist
GRC.4. Isikuandmete kaitse	Esitada meetmed füüsilise isiku kui andmesubjekti põhiõiguste kaitseks isikuandmete töötlemisel
GRC.5. Krüptograafia	Esitada krüptograafilise vahendi kasutamise korralduslikud meetmed ning krüptokontseptsiooni koostamise juhised
GRC.6. Vastavuse haldus	Esitada organisatsiooni eesmärkidel, õigusaktidel, lepingutel ja poliitikatel põhinevate turvanõuete kehtestamise ja järgimise meetmed
GRC.7. Audit ja läbivaatus	Esitada infoturbe auditi ja sõltumatu läbivaatuse tegemise üldised juhised, et täiustada organisatsiooni infoturvet, vältida soovimatuid suundumusi valdkonnas ja optimeerida turvameetmeid ja -protsesse
ORP. Organisatsioon ja personal	
ORP.1. Identiteedi- ja õiguste haldus	
ORP.1.1. Identiteedi- ja õiguste haldus üldiselt	Esitada identiteedi- ja õiguste halduse korraldamise meetmed. Nii kasutajad kui infotehnoloogia (edaspidi <i>IT</i>) komponendid peavad saama juurdepääsu üksnes vajalikele IT-ressurssidele ja teabele
ORP.1.2. Sotsiaalmeediakonto haldus	Esitada meetmed, mis tagavad, et organisatsiooni ametlike sotsiaalmeediakontode loomine, haldamine ja kasutamine toimub turvaliselt ühtse korra alusel
ORP.2. Personali haldus	Esitada meetmed, mille abil personaliosakond ja juht tagavad, et nii oma kui ka välised töötajad tegutsevad organisatsiooni turvaeesmärke silmas pidades
ORP.3. Töötaja infoturvateadlikkuse tõstmine	Esitada töötaja turvateadlikkuse tõstmise ja töötaja koolitusplaani koostamise meetmed, arvestades organisatsiooni spetsiifikat ja töötaja vajalikke teadmisi ja oskusi

ORP.4. Välislähetuse infoturve	Esitada meetmed andmete turvalisuse tagamiseks töötaja välislähetuses viibimisel ning abistada vastutavaid isikuid välislähetuste turvameetmete kehtestamisel
ORP.5. Teabevahetus	Esitada organisatsiooni ja välise poole vahelise turvalise teabevahetuse meetmed
ORP.6. Kaugtöö	Esitada kaugtöö raames talletatava, töödeldava ja edastatava teabe kaitse meetmed
ORP.7. IT-vahendi turvaline kasutamine	
ORP.7.1. IT-vahendi kasutamine üldiselt	Esitada meetmed, et tagada organisatsiooni töövahendi turvaline kasutamine, mis on kooskõlas infoturvanõuetega
ORP.7.2. Isikliku seadme kasutamine	Esitada meetmed, et tagada organisatsioonis isikliku töövahendi (nt isiklik mobiiltelefon, tahvelarvuti, sülearvuti, nutikell, isiklikud kõrvaklapid) turvaline kasutamine, mis on kooskõlas infoturvanõuetega
ORP.7.3. Mobiiltelefoni kasutamine	Esitada meetmed mobiiltelefoni turvaliseks kasutamiseks
ORP.8. Raadioside turvaline kasutamine	
ORP.8.1. Raadioside kasutamine üldiselt	Esitada meetmed, et tagada organisatsioonis kasutatava raadiosidetehnoloogia (nt WiFi, Bluetooth, NFC, RFID ja muud lühimaa raadioside protokollid) turvaline kasutamine, vältides volitamata juurdepääsu, andmeside pealtkuulamist ja seadmete manipuleerimist
ORP.8.2. WiFi kasutamine	Esitada organisatsiooni WiFi-võrgu kavandamise ja turvalise käitamise meetmed, et vältida volitamata juurdepääsu sidevõrgule ja andmeleket
ORP.8.3. Lähiväljaside kasutamine	Esitada meetmed, et tagada organisatsioonis lähiväljaside tehnoloogia turvaline kasutamine, mis on kooskõlas organisatsiooni infoturvanõuetega
ORP.8.4. Bluetoothi kasutamine	Esitada meetmed, et tagada Bluetoothi tehnoloogia turvaline kasutamine organisatsioonis, vältides volitamata sidumisi, andmeleket, seadmete ülevõtmist ning muid lähiväljasidega seotud riske
OPS. IT haldus	
OPS.1. IT valdkonna põhitööd	
OPS.1.1. IT haldus üldiselt	Kehtestada infoturvameetmed lahutamatu osana kõigist IT halduse põhiaspektidest (IT-varade haldamine, IT-hanked, IT käitamine, muudatuste haldus, seire, intsidentide haldus ja IT-vahendite kasutusest kõrvaldamine)
OPS.1.2. Muudatusehaldus	Esitada organisatsiooni tarkvarauuendite ja IT-süsteemide muudatusehalduse protseduuri kohaldamise, juhtimise ja optimeerimise meetmed
OPS.1.3. Andmevarundus	Esitada organisatsioonis töödeldavate andmete varunduse korraldamise meetmed

OPS.1.4. Andmete digitaalne arhiveerimine	Esitada digitaalsete dokumentide muutumatul kujul pikaajalise, turvalise ja ennistatavalt säilitamise meetmed
OPS.1.5. Turvasündmus logimine	Esitada logiandmete turvalise kogumise, talletamise ja nõuetekohase analüüsimise ja kõrvaldamise meetmed
OPS.1.6. Tarkvara testimine ja kasutuselevõtt	Esitada mistahes tarkvararakenduse või -süsteemi testimise ja kasutuselevõtu meetmed
OPS.1.7. Arvutikellade sünkroniseerimine	Esitada meetmed täpse ajaarvestuse tagamiseks IT-komponentide töös
OPS.1.8. IT-süsteemi kaughooldus	Esitada IT-süsteemi turvalise kaughoolduse korraldamise meetmed
OPS.1.9. Kaitse kahjurprogrammide eest	Esitada kahjurprogrammi vastase kaitse korraldamise meetmed
OPS.1.10. Turvanõrkuste haldus	Esitada infotehnoloogiliste turvanõrkuste haldamise protseduuride väljatöötamise meetmed koos juhistega, et minimeerida küberrünnete mõju
OPS.1.11. Andmete turvaline kustutamine	Esitada andmete turvalise kustutamise ja andmekandja hävitamise meetmed
OPS.2. IT haldus teenusena	
OPS.2.1. Väljasttellimine üldiselt	Esitada meetmed väljasttellitava teenuse turvaeesmärkide saavutamise tagamiseks kogu allhanke kestel
OPS.2.2. Pilvteenuse integratsioon äriprotsessiga	Esitada meetmed pilvteenuse kavandamiseks ja turvaliseks käitamiseks organisatsiooni äriprotsessi toetamise eesmärgil
OPS.2.3. Teenuseleping välise teenuseosutajaga	Esitada meetmed mistahes sisseostetava teenuse kvaliteedi tagamise lepete sätestamiseks teenuse osutamise lepingus (inglise keeles <i>service level agreement</i> , lühend SLA)
OPS.2.4. Tarneahela infoturbe	Esitada infoturbe haldamise meetmed tarneahela nõutava turvaseme hoidmiseks, lähtudes tarneahela osalistelt nõutavatest meetmetest
OPS.2.5. X-tee andmeteenus	Esitada X-tee andmeteenuse turvalise kasutamise ja kaitse meetmed. X-tee turvaserveriga liidestatud IT-süsteem ei tohi ohustada X-tee taristut ega sattuda X-teega liidestatuse tõttu ise haavatavasse olukorda. Samuti peab andmete liikumine eri organisatsioonide ja üksuste vahel põhinema selgetel õiguslikel alustel
OPS.3. Süsteemide haldus	
OPS.3.1. Süsteemi haldus üldiselt	Esitada mistahes süsteemina käsitatava keskkonna turvalise halduse meetmed. Kuna süsteemi haldamiseks on vaja eeliskontot, tuleb rakendada meetmeid selle võimaluse väärkasutuse tõkestamiseks
OPS.3.2. Mobiilseadmete keskhaldus	Esitada mobiilseadmete halduse kavandamise ja turvalise käitamise meetmed

DER. Avastamine ja reageerimine	
DER.1. Turvaintsidendi avastamine	Esitada turvasündmusega seotud andmete kogumise, seostamise ja hindamise meetmed, et tagada turvaintsidendi terviklik ja õigeaegne avastamine
DER.2. Turvaintsidentide haldus	
DER.2.1. Turvaintsidendi käsitus	Esitada turvaintsidendi süstemaatilise käsitlemise meetmed
DER.2.2. IT-kriminalistika võimaldamine	Esitada meetmed infoturvaintsidendi kriminalistika võimaldamiseks oluliste ettevalmistuste kaudu IT-süsteemi projekteerimise ja käigushoiu etappides
DER.2.3. Ulatusliku turvaintsidendi lahendamine	Esitada ulatusliku turvaintsidendi lahendamise meetmed
DER.3. Turvatestimine ja õppus	Esitada infoturbe nõuetelevastavuse testimise ja infoturbeõppuse korraldamise meetmed
DER.4. Talitluspidevus	Esitada meetmed infoturbe ja talitluspidevuse tagamiseks avariiolukorras

Tabel 2. Süsteemimoodulid

Süsteemimoodulid	
INF. Taristu	
INF.1. Hoone	Esitada meetmed, mis käsitlevad organisatsiooni tüüphoone tehnilisi ja korralduslikke turvaaspekte
INF.2. Hoone ruumid	
INF.2.1. Bürooruum	Esitada infoturvameetmed, mis on kohaldatavad bürooruumile (nt kontor, ladu või muu ruum, kus asub arvutitöökoht) ja bürootöökohale
INF.2.2. Serveriruum ja andmekeskus	Esitada serveriruumi ja andmekeskuse turvaliste ja jätkusuutlike käidutingimuste loomise ja säilitamise meetmed
INF.2.3. Tehnilise taristu ruum	Esitada tehnilise taristu ruumi või tehnilise taristu kapi turvalisuse tagamise meetmed
INF.2.4. Arhiiviruum	Esitada andmekandjate arhiivi ja arhiveeritaval andmekandjal oleva teabe kaitse meetmed
INF.2.5. Koosoleku-, ürituse- ja koolitusruum	Esitada koosoleku-, ürituse- ja koolitusruumis töödeldava teabe ja neis ruumides olevate IT-seadmete kaitse meetmed
INF.3. Mobiilne töökoht	Esitada mobiilsele töökohale kohaldatavad korralduslikud, tehnilised ja personali käsitlevad meetmed, mida arvestatakse ja täidetakse siis, kui töötaja töötab väljaspool organisatsiooni ruume
INF.4. Kodutöökoht	Esitada meetmed organisatsiooni teabe kaitseks ja turvalise taristu rajamiseks kodutöökohas
INF.5. Sõiduki IT-komponendid	Esitada organisatsiooni mehitatud ja mehitamata, sh iseseisva sõiduki infoturvameetmed juhul, kui sõiduk (nt mootor-, vee- või õhusõiduk) on varustatud tänapäevaste infotehnoloogiliste komponentidega
INF.6. Elektriikaabeldus	Esitada meetmed hoone elektritoite kaitseks rikete, häirete ja manipuleerimise eest
INF.7. Tehnosüsteemid	
INF.7.1. Hoone tehnosüsteemide haldus üldiselt	Esitada hoone või hoonete tehnoseadmete ja -süsteemide (nt kütte-, jahutus-, ventilatsiooni-, konditsioneerimis-, vee-, valgustus-, tulekaitse- ja nõrkvoolusüsteemid; inglise keeles <i>technical building management</i> , lühend TBM) kavandamise ja turvalise käitamise meetmed
INF.7.2. Hooneautomaatikasüsteem	Esitada hooneautomaatikasüsteemi (inglise keeles <i>building automation and control system</i> , lühend BACS) kavandamise ja turvalise käitamise meetmed
INF.7.3. Puhvertoiteallikas	Esitada puhvertoiteallika kavandamise ja turvalise käitamise meetmed

NET. Andme- ja kõneside	
NET.1. Arvutivõrk	
NET.1.1. Võrguhaldus üldiselt	Esitada turvalise võrguhalduse rajamise ja käigus hoidmise ning turvalise andmeside tagamise meetmed
NET.1.2. Kohtvõrk	Esitada võrgu arhitektuuri ja võrgulahenduse infoturvameetmed
NET.1.3. Raadiokohtvõrk	Esitada raadiokohtvõrgu rajamise ja turvalise käitamise juhised
NET.1.4. Virtuaalne privaatvõrk	Esitada virtuaalse privaatvõrgu kavandamise ja turvalise käitamise meetmed
NET.2. Sidevõrgu kaabeldus	Esitada meetmed sidekaabelduse kaitseks rikete, häirete ja manipuleerimise eest
NET.3. Võrgukomponendid	
NET.3.1. Võrgukomponent üldiselt	Esitada arvutivõrgu mistahes komponendi turvalise käitamise meetmed
NET.3.2. Tulemüür	Esitada tulemüüri või tulemüürisüsteemi turvalise hankimise, rajamise, konfigureerimise ja käitamise meetmed
NET.3.3. Marsruuter	Esitada ruuteri turvalise käitamise meetmed
NET.3.4. Kommutaator	Esitada kommutaatori turvalise käitamise meetmed
NET.3.5. Raadiokohtvõrgu pääsupunkt	Esitada raadiokohtvõrgu komponendi turvalise käitamise meetmed
NET.4. Võrguühenduse automaatne seadistus	Esitada võrguseadme turvalise konfigureerimise ja käitamise meetmed
NET.5. Võrkupääsu reguleerimise süsteem	Esitada meetmed arvutivõrgu klientseadme võrkupääsu reguleerimise (inglise keeles <i>network access control</i> , lühend NAC) süsteemi kavandamise ja turvalise käitamise meetmed
SYS. IT-süsteemid	
SYS.1. Serverid	
SYS.1.1. Server üldiselt	Esitada serverina kasutatavas IT-komponendis töödeldavate andmete ning sellega seotud rakenduste kaitse meetmed
SYS.1.2. Microsoft Windowsi server	Esitada Microsoft Windowsi operatsioonisüsteemiga serveri turvalise käitamise ja serverisüsteemis töödeldavate andmete ning protsesside kaitsmise meetmed
SYS.1.3. Linuxi server	Esitada Linuxi ja UNIXi operatsioonisüsteeme kasutava serverisüsteemi ja selles töödeldavate andmete ning protsesside kaitse meetmed
SYS.1.4. Riistvaraline server	Esitada riistvaralise serverisüsteemi turvalise käitamise meetmed
SYS.1.5. Virtuaalserver	Esitada virtualiseeritud serverisüsteemi turvalise käitamise meetmed
SYS.1.6. Konteinerdus	Esitada konteinertehnoloogia kavandamise ja turvalise käitamise meetmed
SYS.1.7. Kubernetes	Esitada meetmed konteinerduse haldamiseks ja andmete kaitsmiseks Kubernetesi keskkonnas

SYS.2. Lõppkasutaja tööjaamad	
SYS.2.1. Tööjaam üldiselt	Esitada meetmed tööjaamas töödeldavate andmete kaitseks olenemata arvuti tüübist või selles kasutatavast operatsioonisüsteemist ning suurendada teadlikkust seadme spetsiifilistest ohtudest
SYS.2.2. Microsoft Windowsi tööjaam	Esitada Microsoft Windowsi operatsioonisüsteemi kasutava tööjaama andmete kaitse meetmed
SYS.2.3. Linuxi tööjaam	Esitada Linuxi operatsioonisüsteemi kasutava tööjaama andmete kaitse meetmed
SYS.2.4. Apple macOSi tööjaam	Esitada macOSi operatsioonisüsteemi kasutavas tööjaamas talletatud andmete kaitse meetmed
SYS.2.6. Sülearvuti	Esitada meetmed sülearvuti turvaliseks kasutamiseks organisatsioonis ja suurendada teadlikkust seadme spetsiifilistest ohtudest
SYS.2.7. Irdandmekandja	Esitada irdandmekandja (inglise keeles <i>removable media</i>) turvalise kasutamise meetmed
SYS.2.8. Failijagamisteenus	Esitada serverisõnumiploki (inglise keeles <i>server message block</i> , lühend SMB) andmesideprotokolli kavandamise ja turvalise käitamise meetmed
SYS.3. Mobiilseadmed	
SYS.3.1. Mobiilseade üldiselt	Esitada meetmed tööülesannete täitmiseks kasutatava nutitelefoniga ja tahvelarvuti jaoks
SYS.3.2. Google Android	Esitada Androidi operatsioonisüsteemiga mobiilseadme turvalise haldamise meetmed
SYS.3.3. Apple iOS	Esitada iOSi ja iPadOSi operatsioonisüsteemiga mobiilseadme turvalise haldamise meetmed
SYS.4. Muud võrgustatud seadmed	
SYS.4.1. Esemevõrgu seade üldiselt	Esitada esemevõrgu (inglise keeles <i>internet of things</i> , lühend IoT) seadme turvalise haldamise meetmed
SYS.4.2. Printer ja kontorikombain	Esitada võrgustatud printeri ja kontorikombaini turvalise haldamise ja kasutamise meetmed
SYS.4.3. Sardsüsteem	Esitada sardsüsteemi (inglise keeles <i>embedded system</i>) turvalise kasutamise meetmed
SYS.5. Serveriteenused	
SYS.5.1. Serveriteenus üldiselt	Esitada mistahes serveriteenuse turvalise seadistamise ja haldamise meetmed
SYS.5.2. Failiserver	Esitada failiserveri turvalise käitamise meetmed
SYS.5.3. Andmebaasiserver	Esitada andmebaasisüsteemi kavandamise ja turvalise käitamise ning andmebaasides töödeldava teabe kaitsmise meetmed
SYS.5.4. Veebirakendus	Esitada veebirakenduse turvalise töötamise ning töödeldava teabe kaitsmise meetmed

SYS.5.5. Ajaserveri teenus	Esitada meetmed ajaserveri turvaliseks seadistamiseks usaldusväärse ja täpse kellaaja tagamise eesmärgil kõigis seotud IT-süsteemides
SYS.5.6. Domeeninimesüsteem	Esitada organisatsioonis kasutatava domeeninimesüsteemi (inglise keeles <i>domain name system</i> , lühend DNS) serveriteenuste turvalise käitamise meetmed
SYS.5.7. Veebiserver	Esitada veebiserveri ja veebiserveri kaudu juurdepääsetava teabe kaitse meetmed
SYS.5.8. Andmesalvesti	Esitada andmesalvestilahenduse kavandamise, turvalise käitamise ja kasutuselt kõrvaldamise meetmed
SYS.5.9. Terminaliserver	Esitada terminaliserveri kavandamise ja turvalise käitamise meetmed
SYS.5.10. E-posti server	Esitada e-posti serveri turvalise seadistamise ja käitamise meetmed
SYS.5.11. Microsoft Exchange	Esitada Microsoft Exchange'i rühmatarkvaralahenduse kavandamise ja turvalise käitamise meetmed
SYS.5.12. Kataloogiteenus	Esitada kataloogiteenuse kavandamise, turvalise käitamise ja kõrvaldamise ning kataloogiteenuse andmete kaitsmise meetmed
SYS.5.13. Microsoft Active Directory Domain Services	Esitada meetmed Microsoft Active Directory Domain Services'i tavakasutuse turbeks, kui Active Directory teenust kasutatakse Microsoft Windowsi süsteemidest koosneva taristu ja keske autentimis- ja autoriseerimislahenduse haldamiseks
SYS.5.14. X-tee turvaserver	Esitada X-tee turvaserveri kaitse meetmed, et tagada andmevahetuse tõendusväärtus ja X-teega seotud äriprotsesside usaldusväärsus
SYS.5.15. Tehisarusüsteem	Esitada meetmed tehisarusüsteemi turvaliseks kasutuselevõtmiseks ja käitamiseks organisatsioonis
SYS.5.16. IP-telefonside server	Esitada VoIP-põhise sidesüsteemi komponendi ja IP-telefoni kõneedastuse turvalisuse tagamise meetmed
SYS.5.17. Virtualiseerimissüsteem	Esitada serveri virtualiseerimiskeskonna turvalisuse tagamise meetmed
SYS.5.18. Töölaua virtualiseerimine	Esitada virtuaaltöölaua taristu (inglise keeles <i>virtual desktop infrastructure</i> , lühend VDI) kavandamise ja turvalise käitamise meetmed
SYS.5.19. Elektrooniline arhiivisüsteem	Esitada digitaalsete andmete arhiveerimise süsteemi kavandamise ja turvalise käitamise meetmed
SYS.5.20. Keskne logitaristu	Esitada keske logitaristu kavandamise ja käitamise meetmed
SYS.6. Pilvandmetöötlus	
SYS.6.1. Pilvandmetöötlus üldiselt	Esitada pilvandmetöötluse kavandamise ja turvalise käitamise meetmed
SYS.6.2. Pilvrakendus	Esitada pilvrakenduse turvalise seadistamise ja käitamise meetmed

SYS.7. Käidutehnoloogia	
SYS.7.1. Käidutehnoloogia üldiselt	Esitada korralduslikud ja kontseptuaalsed meetmed käidutehnoloogia (inglise keeles <i>operational technology</i> , lühend OT) turvaliseks kasutamiseks organisatsioonis
SYS.7.2. Tööstusautomaatika	Esitada tööstusautomaatikasüsteemi (inglise keeles <i>industrial automation and control system</i>), sh protsessijuhtimissüsteemi (inglise keeles <i>industrial control system</i> , lühend ICS) ja SCADA-süsteemi komponentide turbe meetmed, olenemata komponentide valmistajast, arhitektuurist, otstarbest ja paigalduskohast
SYS.7.3. Autonoomnesüsteem	Esitada autonoomse süsteemi, sh nutika anduri, andurina töötava seadmestiku ja robotseadme turbe meetmed, olenemata selle valmistajast, otstarbest, arhitektuurist või asukohast
SYS.7.4. Ohutusautomaatika	Esitada infoturvameetmed ohutusautomaatika süsteemi turvaliseks kasutuselevõtmiseks ja käitamiseks
SYS.7.5. Programmeeritav kontrolleri	Esitada programmeeritava kontrolleri (inglise keeles <i>programmable logic controller</i> , lühend PLC) turvalise kasutuselevõtmise ja käitamise meetmed, olenemata nende valmistajast, otstarbest, arhitektuurist või asukohast
SYS.7.6. Käidutehnoloogia komponentide kaughooldus	Esitada käidutehnoloogia komponentide turvalise kaughoolduse meetmed. Käidutehnoloogia koosneb tavaliselt eri tootjate riistvara- ja tarkvarakomponentidest, mille käigushoidmiseks ja hooldamiseks tuleb tagada volitatud hoolduspersonali kaugjuurdepääs
APP. Lõppkasutaja rakendused	
APP.1. Tarkvara üldiselt	Esitada lõppkasutaja tööjaamas kasutatava tarkvara ja tarkvaraga töödeldavate andmete turbe meetmed, sh tarkvara kasutuselevõtmise, hankimise, kasutamise ja kasutuselt kõrvaldamise meetmed
APP.2. Veebilehitseja	Esitada meetmed andmete kaitsmiseks tööjaama veebilehitseja kaudu realiseeruda võivate ohtude eest, hõlmates nii tsentraalselt kui ka iseseisvalt hallatavaid töökeskkondi
APP.3. E-posti klient	Esitada e-posti kliendi töödeldavate andmete kaitse üldmeetmed
APP.4. Kontoritarkvara	Esitada kontoritarkvaras töödeldavate andmete kaitsmise ja kontoritarkvara turvalise haldamise meetmed
APP.5. Rühmatarkvara	Esitada ühendatud side- ja koostöölahenduse (inglise keeles <i>unified communication and collaboration</i> , lühend UCC) turvalise kasutamise meetmed
APP.6. Mobiilirakendus	Esitada äriprotsessi toetavas mobiilirakenduses töödeldavate andmete kaitse meetmed

DEV. Tarkvaraarendus	
DEV.1. Tarkvaraarendus üldiselt	Esitada organisatsiooni tellitud või organisatsioonis arendatava tarkvaralahenduse infoturbe haldamise ja tarkvara turvalisuse tagamise meetmed
DEV.2. Tarkvaraarendusprojekt	Esitada organisatsiooni individuaalseks kasutusotstarbeks välja töötatud või organisatsiooni tarbeks oluliselt kohandatud rakenduste projektipõhise arendamise meetmed
DEV.3. Veebirakenduse arendus	Esitada dünaamilise (muutuva sisuga) veebirakenduse turvalise arendamise ja veebirakenduses töödeldavate andmete kaitsmise meetmed
DEV.4. Integreerimine Eesti e-riigi teenustega	
DEV.4.1. eID komponent	Esitada meetmed elektroonilise identiteedi (eID) komponendi ja sellega seotud teenuste rakendamiseks organisatsioonis