Põhilised küsimused ja eeldused nelja-faasilise mudeli erinevate faaside rakendamisel

Poliitilised eeldused	Õiguslikud eeldused	Tehnilised eeldused	Organisatsioonilised eeldused	Eeldused ametnikkonnas	Eeldused kodanikkonnas	Finantsressurss	Põhilised ohud
1. faas - internetileht Soov ja arusaam, et infot tuleb anda. Õigus infole.	Otsesed eeldused puuduvad. Internet on vaba keskkond.	Internetiühenduse ja -teenuse olemasolu.	-Vastutavad inimesed on kindlaks määratud. - Organisatsioonisisese info liikumise korraldamine.	-Valmisolek kasutada internetilehte kui võimalust mitte kui kohustust. -Piisavad IKT oskused.	Valmisolek, piisavad IKT oskused, juurdepääs.	Operaatori tasu. 0-25 000 kr.	-Info ei ole aktuaalne, info ebaselgus. -Ebaselge vastutus andmete õigsuse eest. -Isikuandmete ja kontrollimata info ülespanek. -Sissetung ja andmete muutmine. -Ebapiisav juurdepääs.
2. faas- online päringud Soov lihtsustada kodanikele info saamist, parandada sellele juurdepääsu	-Andmekogust andmete väljastamise korra ja avaliku/mitteavaliku info reguleerimine. -*Online* andmebaasi ja päringute õigusliku olemuse määratlemine (informatiivsed või avalikult usaldatavad). -Info õigsust ja vormi puudutavate nõuete olemasolu ning selle eest vastutuse määratlemine. -Kohustus pidada andmebaasi elektrooniliselt -Andmekogu põhimääruse olemasolu. Isikuandmete kaitse ja riigisaladuse reguleerimine. Pakkuja sertifitseerimine (Urmas)???	Internetiühendus. Viiruskontrolliga elektroonilised andmekogud. Toimiv infosüsteem, andmebaasiserver, andmebaasirealisatsioon veebiväljundiga. Andmebaasi teenuse pakkuja sertifitseerimine. Lihtne ja informatiivne otsingusüsteem. Andmete sisetaja ja sisestamise aja tuvastamise süsteem. Süsteemide turvalisus.	Teadlik ja selge infosüsteemide ja IKT juhtimispoliitika, selge organisatsioonisisene ülesannete jaotus (sh. info uuendamine ja liikumine). Koostöö IKT osakonna ja andmebaasi haldaja vahel.	-Arusaam, et on vaja kodanikele info saamist lihtsustada. -Valmisolek ja tahe kasutada IKT-d paberkandja alternatiivina. -IKT kasutamise, andmete töötlemise ja uuendamise oskus. -Valmidus teha esialgu topelttööd (pidada netiandmebaasi + suhelda endiselt vahetult kodanikega, kes teevad oma päringud endistviisi).	-Tahe, huvi, juurdepääs IKT-le. -Piisavad IKT kasutamise oskused. - teadlikkus registrites oleva info ja *online*-päringu võimaluste kohta, vajadus nende järele.-Valmisolek elektrooniliseks infovahetuseks ametiasutustega ja elektroonilise info usaldamine.	Üksikute isikute koolitus (registriamet); andmekogude pidamine; püsiühendus (Daimar). Vähe: 50 – 300 000 (tegemisel) (Urmas). Serverid; turvastruktuur (Ivo). Ei peaks olema väga kallis (Virgo). Pidajatasu, võimalik tasu andmete töötlemise eest, kulud koostöö käigus jne (Einar).	-Inimeste ebavõrdsus tulenevalt juurdepääsuvõimalustest ja kasutamisoskustest. -Keerulised otsingumootorid. -Suutmatus ja soovimatus andmeid korras hoida. Ebaselgelt määratletud vastutus andmete õigsuse eest. -Vananenud, väärad või ebaolulised andmed, nende usaldamisest tekkiv kahju.. - Puudulik isikuandmete kaitse.
3. faas- andmete sisestamine Soov hoida kokku asjaajamisel, teadlikkus ja arusaam tehnika võimalustest.. Valmisolek teha esialgu lisakulutusi.	Digitaaldokumentide reguleerimine, digitaaldokumendi võrdsustamine paberdokumendiga. -Isiku identifitseerimise reguleerimine. -Isikuandmete kaitse reguleerimine. -Eel- ja järelkontrolli vajalikkuse ja suhte reguleerimine -Pideva järelkontrolli sätestamine andmete õigsuse kindlustamiseks.	Isiku identifitseerimine digitaalallkirja vms abil/ jooksev kontroll (Nele, Ivo, Virgo, Külli, Maarja). Autoriseerimist võimaldav riist ja tarkvara, suurem võimsus ja mälu kui 2. faasis (Daimar). Sertifitseerimise infrastruktuur; toimiv infosüsteem; andmebaasiserver; standardid (Urmas). Sisestatud andmete automatiseeritud töötlemine (võrdlemine olemasolevatega) tarbimisformaati (Virgo). Kasutamine peab olema võimalikulu lihtne ja mugav	-Teadlik ja selge IKT juhtimine, IKT kui organisatsiooni strateegiline komponent. -Selge sisetatud andmete kontrollimise struktuur, kindel vastutusstruktuur, ligipääsukontroll ametkonnasiseselt. -Kontrolli teostava poole seostatus andmekogujatega. -Süsteemi tehniliste ja sisuliste haldajate koordineeritud koostöö.	-Oskused ja väljaõpe IKT kasutamiseks. -Teadlikkus turvalisuse ohtudest ja õiguslikest küsimustest (andmekaitse, isikuandmed, riigisaladus jne). -Oskus integreerida IKT lahendusi olemasolevatesse tööprotsessidesse. -Valmisolek aktsepteerida elektrooniliselt saadud infot, kodanike ja tehnoloogia usaldamine. -Ametnike aktiivne osavõtt andmete kontrollimisel ja töötlemisel.	-IKT kasutamise oskused, juurdepääs ja huvi. -Valmisolek elektrooniliseks infovahetuseks ametiasutustega ja elektroonilise info usaldamine. -Usaldus süsteemi töökindluse suhtes. -Soov anda oma andmeid.	Finantsressursid digiallkirja kasutusele võtmiseks (Nele). Kulutused kaasaegsele turvatehnoloogiale, personalile, tekstikoostamisele, autentimisele (Daimar). Keskmine: 0,5 – 1 milj (tegemisel) (Urmas). Lõppkasutaja liidese, kasutajatuvast. Ja andmete töötlemise süst. On päris kallis (Virgo). Administreerimiskulud (Einar). Koolitus; turvasüsteem (Maarja).	-Vajadus suhelda otse inimesega, mitte arvuti vahendusel. Takistuseks harjumuslik arusaam, et paberil on kindlam, elektroonilise info usaldamise puudulikkus. -Kontrollimata ja hindamata info avaldamine ja kasutamine. -IKT-le vähene juurdepääs. Ebapiisavad IKT kasutamise oskused. -Andmete sisestaja identifitseerimissüsteemi puudulikkus. Vigade oht andmete sisestamisel. Andmete kuritarvitamine ja kuritahtlik muutmine väljastpoolt ja ametnikkonna sees. -Puudulik turvalisus ja kontrollisuutlikkus.

Deleted: ¶

		(Einar).					
4. faas- aktiivne-teadlik ristkasutus Soov muuta haldusprotseduure võimalikult lihtsaks. Valmisolek loobuda senisest andmehõive sektoraalsest kasutusest ja kontrollist. Ristkasutuse aktsepteerimine. Tugev ja teadlik koordineeritud areng, IKT arendamine kui prioriteet.	-Volitus andmete ristkasutuseks. -Isikuandmete kaitse reguleerimine. -Riikliku ja regionaalse tasandi koostöö ning pädevuse delegeerimise võimalused ja tingimused on sätestatud.-E-seadusandluse olemasolu ja korrastatus (ühtne aadresside ja kohanimede süsteem, ühtne klassifikaatorite süsteem, infosüsteemide turvameetmete süsteem, ruumiandmete asukoha määramise e. geodeediline süsteem). -Andmetele juurdepääsu ja vastutuse reguleerimine.	Vastav liides; andmekaitse (Nele). Ühilduvad arvuti ja tarkvarasüsteemid (Daimar, Ivo). Korralikud sidekanalid (Daimar). Toimiv infosüsteem; võimsad andmebaasiserverid; riigi andmekogude ristkasutus; standardid (Urmas, Külli). Igast liigutusest peab jääma jälg; üksnes soovitud andmete edastamine eraldatud teistest; asutuste ühtlane tehniline tase (Virgo). Autentimine ja autoriseerimine; PKI (Maarja). Autoriseerimissüsteem paigas ja kontroll selle üle (Daimar).	-Teadlik IKT juhtimine, IKT kui organisatsiooni orgaaniline osa. -Asutusesisene ja asutustevaheline koostöö andmete sisestamiseks ja kasutamiseks. -Andmete kasutamise kord ja kontroll. -Korrastatud andmekogude süsteem.	-Valmisolek ja oskused IKT kasutamiseks ning info jagamiseks -Teadlikkus ning arusaam ohtudest (andmekaitse) ja nende vältimisest. -Tahe asutusesiseseks ja asutustevaheliseks koostööks.. -Vastutustundlikkus ja usaldusväärsus .	-Ristkasutuse ja tekkiva lisaväärtuse??? aktsepteerimine. -Piisavad IKT oskused ja valmisolek. -Soov anda oma andmeid. -Usaldus süsteemi töökindluse suhtes.	Sektoraalselt eelarvelt üleminek eesmärgipärasele (Nele). Kulutused koolitusele, turvalisusele (Daimar). Palju: 0,5-2 milj (tegemisel), aga siin ei saa ühe organisatsiooni kaupa läheneda (Urmas). Serverid; koolitus (Ivo, Maarja. Asutuste tehnilise taseme ühtlustamine ja selle hoidmine nõuab päris palju finantse (Virgo). Andmebaaside ja koostöö halduskulud (Einar).	-IKT oskuste ja juurdepääsu puudulikkus. -Andmekaitse puudulikkus, süsteemi haavatavus. -Valede ja aegunud andmete kasutamine ning levik. -Andmete mitte-eesmärgipärane kasutamine. -Ristkasutuse kontrollija poolt oma seisundi kuritarvitamine. -Inimestel ülevaate ja kindlustunde puudumine andmete kasutajate ja kasutamise otstarbe kohta. -Kasutajaliidesed pole loogilised ja erihuvidele vastavad. -Teenuste sisu nõrkus -Soovimatus loobuda teenustasudest. -Arusaam, et andmed kuuluvad asutusele kui takistus ristkasutuseks. -Autentimis- ja autoriseerimissüsteemi nõrkus ja/või ebaotstarbekus/läbimõtlematus ning sellega kaasnev võimu koondumise oht. -Liigne info kontsentreerumine, superandmebaasi tekkimise oht, oht riiklikule julgeolekule.