Uuringu „Infoturbe meetmete rakendused digitaalsetes arhiivides“ toetava küsitluse lühikokkuvõte

I. Eesmärk

Kaugem eesmärk – mõõta digiarhiivide usaldusväärsust nende endi hinnangul, arvestades pikaajalise säilitamise printsiipi. Et tagada säilitatava ainestu käideldavus, terviklikkus ja konfidentsiaalsus tuli uurida, kui suured on selles valdkonnas teadmiste, soovide ja tegelikkuse vahelised käärid.

Riigiti rakendatakse mäluasutustes nii kohustuslikke infoturbe reegleid ja standardeid kui ka oma valitud meetmeid. Lisaks erinevatele põhimõtetele, eesmärkidele ja poliitikale on uurimist väärt kahtlemata suur ühisosa, mida mäluautused teevad ühtemoodi.

Eesti Rahvusraamatukogu uuringu *"Infoturbe meetmete rakendused digitaalsetes arhiivides"* eesmärk on kaardistada infoturbe põhimõtted erinevate riikide mäluasutuste digitaalarhiivides, analüüsida ja võrrelda olukorda kultuuriväärtuste turvalisuse vallas ning rakendatud infoturbe meetmeid.

- I. etapp (2010): millised tingimused on selleks loodud (seadustik jm dokumentatsioon, kasutusel olevad infoturbe ja süsteemi auditeerimis-meetodid, hinnang riskidele, arengustrateegiad ja tegevusplaanid jm)
- II. etapp (2011) kevad: problemaatika mäluasutuste digitaalsete arhiivide riskidest Raivo Ruusalepalt auditeerimiste tulemusel saadud loetelu põhjal (ISO 14721:2002 standard)

II. Osalejad

Mihkel Reial – RR tehnoloogiadirektor, töörühma juht
Raivo Ruusalepp – Tallinna Ülikooli Infoteaduste instituut; Eesti Äriarhiivi OÜ
Kai Idarand – RR teadus- ja arenduskeskuse juhtiv spetsialist

III. Ressursid

hõlmavad olemasolevat tööjõudu, kommunikatsioonikulu jm vahendeid RR eelarve piires.

IV. Ülesanded (I. etapp)

- uurida usaldusväärsust **põhiliselt riskihalduse seisukohalt** ning koostöö võimalikkust;
- infoturvameetmete hindamine jms II-s etapis;
- ülevaade riiklikest, valdkonna või asutuse arenguprogrammidest;
- milliseid rahvusvahelisi, asutuse vm standardeid järgitakse, ja miks just neid;
- kas ja milliseid auditeid digitaalarhiivid on kasutanud;
- millistest allikatest finantseeritakse ja kelle ülesandeks (institutsionaalselt) on;
- infoturbe meetmete tõhususe hindamine järgmiste riskifaktorite vähendamisel:
  - tehnoloogia ja tehnilise keskkonna vananemine;
  - füüsiline kriisisituatsioon;
  - küberrünnak ja häkkimine;
  - IT arendustega seotud riskid;
  - andmevargus ja autoriõigusega seotud problemaatika;
- prognoos tuleviku infoturbepoliitika probleemide ja koostööhuvide kohta.

V. Meetod

Uurimusel on rakenduslik ja kirjeldav iseloom. Kasutati **ülevaateuurimuse** strateegiat, kus materjal koguti põhiliselt lahtiste ja osaliselt struktureeritud küsimustega. II. etapis kasutatakse intervjuusid spetsialistidega põhjalikuma teabe saamiseks.

VI. Küsimustik

17 küsimust Eesti ja Läänemeremaade mäluasutuste juhtidele, kes vastasid ise või edastasid vastava valdkonnaga tegelevale töötajale. Välismaa vastajatele kirjeldati näitena RR kogemust.

VII. Valim

Uuring keskendus Eesti ja Läänemere-äärsetele riikide rahvus- või selles staatuses olevatele raamatukogudele, arhiividele jt mäluasutustele. Uuringu ankeedid saadeti 23 mäluasutuse juhile. Vastused laekusid 14-lt (6 Eestist ja 8 välismaalt).
Seega analüüsitakse:

- lisaks Eesti Rahvusraamatukogu enda vastustele
- Tartu Ülikooli Raamatukogu,
- Eesti Rahvusarhiivi Ajalooarhiivi,
- Eesti Kirjandusmuuseumi,
- Eesti Rahva Muuseumi
- Ennistuskoja KANUT
- ja Eesti Rahvusringhäälingu,
- Läti Rahvusraamatukogu,
- Leedu Rahvusraamatukogu,
- Leedu Arhiiviameti,
- Helsingi Ülikooli Raamatukogu,
- Rootsi Kuningliku (Rahvus-) Raamatukogu,
- Rootsi Rahvusarhiivi,
- Taani Rahvusarhiivi
- ja Taani Riikliku Raamatukogu ankeedivastuseid. Kokku **15** respondenti.

Neli mäluasutust küsimustikule ei vastanud, kuid e-kirjavahetust nendega on võimalik kokkuvõtvas analüüsis kasutada (Eesti Kunstimuuseum KUMU, Soome Rahvusgalerii (Valtion taidemuseo), Jeltsini nim Venemaa Presidendiraamatukogu ja Norra Arhiivide, Raamatukogude ja Muuseumide Amet).
Norra Rahvusraamatukogu ja Rahvusarhiivi, Läti ja Soome Rahvusarhiivi ning Taani Kuningliku (Rahvus-)raamatukogu vastuseid ei laekunud.

VIII. Tulemuste analüüs

- uuringu käiku tutvustati ja küsimustikku kasutati osaliselt rühmatöös käesoleva aasta teadusseminaril Palmses;
- küsitluse tulemusi võib kasutada teaduslike ettekannete ja artiklite koostamiseks;
- uuringu tulemusi tutvustatakse rahvusvahelisel konverentsil „**Aligning National Approaches to Digital Preservation**“, mille Eesti Rahvusraamatukogu korraldab 2011 aasta maikuus koostöös USA Kongressi raamatukogu ja Educopia instituudiga.

IX. Ajakava

- ajakavast ei suudetud kinni pidada, sest lisaks Ajalooarhiivile ja Kirjandusmuuseumile oodati Soome Rahvusraamatukogust prooviküsitluse vastuseid, mida õigel ajal ei saadud ja ajagraafik nihkus kuu võrra edasi – aprillikuust mai lõppu. Augustis saime enamus vastuseid, kuid neid ootasime veel septembris ja oktoobriski. Viimane vastaja Rootsi Riigiarhiiv saatis vastused 1. novembril.
- 2. etapi edasilükkamine 2011. aasta kevadesse.

X. Mõned järeldused

1. : ei taheta tunnistada ega veel vähem avalikustada riskide olemasolu digitaalsete objektide turvalisusele

Fakt, et paljud küsimustiku saanud Läänemeremaade mäluasutused sellele ei vastanud või vastasid üldsõnaliselt, võis olla tingitud järgmistest **põhjustest**:

1. Digitaalsete kogude turvalisusele pole veel suurt ohtu tekkinud ja poliitika väljatöötamise vajadust ei ole tajutud või on nende mäluasutuste juhtkonna tegevus antud valdkonnas olnud nõrk. Näiteks Eestis on asutud hoogsalt digiteerima, et kaitsta kultuuriväärtusi hävimise eest, kõigele kaasnevale pole sageli aega olnud mõeldagi, rääkimata sammudest.
2. Väljatöötatud ankeet oli liialt töömahukas, samas tulemust oli võimatu ennustada, st kasuteguri suurus ei paistnud piisavalt suur. Näiteks Soome ja Norra aeglase tagasiside taktika, Läti soov, et ankeet oleks võinud olla vaid plussidega tabeli täitmine jms.
3. Tähtsaim põhjus võib olla aga selles, et ei taheta tunnistada ega veel vähem avalikustada riskide olemasolu digitaalsete objektide turvalisusele, mis tähendaks turvaaukude tunnistamist ja digitaalsete kollektsioonide haavatavust. Näiteks Venemaal loetakse infosüsteemide turvalisus osaks erilisest, rahvuslikku turvalisust puudutavast infost ja sellepärast pole taolise teabe avalikustamine lubatud.

2. : digitaalsete varade pikaajalisele turvalisele säilitamisele on seadusandlikult vähe tähelepanu pööratud

Eestis eraldi infosüsteemide kaitse seadust ei ole, enamus naaberriike on aga vastavate riiklike aktidega määratlenud nii infosüsteemide turvalisuse üldiselt kui avaliku sektori, sh riiklike institutsioonide IKT eraldi. Eestis on võrreldes naaberriikidega infosüsteemide turvalisusele seni killustatult lähenetud. Näiteks küberkuritegudest kui ühest riskiallikast küll räägitakse, kuid **andmete pikaajalisele säilitamisele on äärmiselt vähe tähelepanu pööratud.** Peale Eesti Informaatikanõukogu soovituste puudub infosüsteemide kaitse terviklik ja mitmekülgne, piisavalt laiaulatuslik, kuid samas kontsentreeritud seadus.
Igasuguste valdkonna arengukavade ja tegevusprogrammidega on Eestis tunduvalt paremad lood ja nende küsimustega tegelevad inimesed mõistavad sihipärase tegutsemise olulisust kaasaegses arengus. Vanade EU riikide mäluasutused mainisid mitmesuguseid arengukavu vähem. Nähtavasti kajastavad seadused neid tõhusamalt ja piisavalt.

3. : mäluasutuste digikogude spetsiifilisi turvanõuded ei ole piisavalt standardiseeritud

Pooled vastajaist nentisid, et nad ei kasuta infoturbe standardeid, vaid lähtuvad IT-osakonna töötajate kompetentsusest selles vallas ja riiklikest soovitustest. Samalaadsed asutused eri maades lähtuvad katusorganisatsiooni seadusest nagu näiteks ülikooliraamatukogud Eestis ja Soomes ülikooliseadusest või arhiivid arhiiviseadusest. Oma turvastandardi väljatöötamise vajadust arutatakse. Kõige omanäolisemana tundus Taani Infoturvalisuse standard DS 484, mis 2007. aastani on olnud Taani riiklikes institutsioonides kohustuslik, seega seaduse jõuga. Peaaegu ainsa riiklikult sätestatud soovitusena mainiti Eestis digitaalse kultuuripärandi metaandmeelementide standardloetelu.

4. : Eestis ollakse asjade seisuga kõige vähem rahul

Kõne all olnud riiklikult sätestatud seadused ja rahvusvaheliselt kinnitatud standardite olemasolu annab teistes Läänemere riikides rohkem põhjust rahuoluks kui Eestis. Meie riigis ollakse kriitilisemad, sest mäluasutused vastasid, et nad pigem ei ole asjade seisuga rahul. Skandinaavia mäluasutused Taani ja Soome näitel seevastu arvavad, et olemasolevad seadused ja muud regulatsioonid neid toetavad ja annavad raamistiku, milles mäluasutused ennast suhteliselt turvaliselt tunnevad.

Nii Leedus kui ka Lätis puudutavad raamatukogu-, arhiivi- ja muuseumiseadused ka digitaalsete kollektsioonide kaitse aspekte. Eesti Arhiiviseaduses (2010. redaktsioon) digitaalsete arhivaalide mõistet ega spetsiifikat ei rõhutata, juttu on „...mistahes teabekandjale jäädvustatud teabest“. Strateegiatest ja riiklikest programmidest mainiti Eesti infoühiskonna arengukava aastani 2013, mis andis raamistiku Eesti kultuuripärandi digitaalse säilitamise rahvusliku strateegia väljatöötamiseks ja arengukava „Digitaalne Kultuuripärand 2007-2010” väljatöötamiseks.

Mis puudutab mäluasutuste endi infoturbe meetodeid, siis lähtub enamus oma arengukavast või katusorganisatsiooni regulatsioonidest, milles on muuhulgas ära toodud arvutivõrgu turvalisust tagav kord. Paistab, et enamuses mäluasutustest on digitaalse säilitamise strateegia alles väljatöötamisfaasis.

Mäluasutused on vastustena märkinud olulisi dokumente, kus kollektsioonide kaitsmise põhimõtted küll kirjas, kuid digiteeritud kogude turvalisust otsesõnu mainitud ei ole. Loomulikult sisaldavad asutusesiseseid dokumendid, eeskirjad ja arenguplaanid rohkem vastavat materjali. Soomes näiteks on käimas Soome Digitaalse Raamatukogu projekt, kus saavad kajastuse ka andmekaitse turvalisust puudutavad sätted.

Puuduvatest strateegilistest ja juhisdokumentidest mainiti kõige sagemini (10 korda) vajakajäämisena oma asutuse infoturbepoliitika põhimõtete ja meetmete plaani. See tähendab, et kõik need asutused, kus veel seda dokumenti kinnitatud ei ole, tunnetavad sellise vajalikkust.

Üheksal juhul (9) tuntakse puudust digitaalse kultuuripärandi riiklikult sätestatud põhimõtetest ja meetmete plaanist. Seda tunnetavad nii Eesti mäluasutuste, teiste Baltimaade kui ka Taani ja Rootsi raamatukogud.

Tartu Ülikooli Raamatukogu meelest oleks aga hoopis vaja konkreetset plaani, mille alusel regulaarselt testitakse infosüsteemide reaalset turvalisust. Seda tegevust peab finantseerima riiklikult.

5. : riske teatakse, kuid kindel tegevuskava puudub

Paljude Eesti kultuuriasutuste tegutsemist kriisi puhul oma dokumentidega ei reguleeri. Eesti Rahvusraamatukogus ja Ennistuskojas KANUT on kinnitatud infoturbe poliitika põhimõtted ja kriisireguleerimise plaan. Paljudes asutustes on selle peale mõtlema hakatud ja tegevuskava dokument väljatöötamise järgus (nt Eesti Rahvusarhiivis) või on olemas visioon digikoopiate erinevatesse geograafilistesse asukohtadesse (hoidlatesse) paigaldamise kohta (Eesti Rahvusringhääling). Enamikes organisatsioonides Eestis, Lätis, Leedus jm see dokument veel puudub. Sellepärast **lepitakse üldiste või oma valdkonna reeglitega**.

Peaaegu kõigil mäluasutustel on teada riskid, mis digitaalseid varasid ohustavad ja millega oma töös arvestatakse. Näiteks Rootsis viiakse igal aastal läbi oletatavate riskide analüüs, mille tulemused esitatakse valitsusele.

Vastustest avatud küsimusele võib eritada 9 arvestatavat riskirühma (vastuste arvu järgi):

1. inimlik tegur

Kõige rohkem mainitud valdkond. Eestis ebakompetentsi otseselt ei tunnistatud, vaid viidati personali juhuslikele äpardustele (inimlikud vead tööoperatsioonide sooritamisel),

hooletusele, liigsele kiirustamise ja halduriõigustes töötajate vigadele. Nii Balti- kui Skandinaaviamaades mainiti kõige rohkem IT kompetentsi vähesust ja võtmepersonali puudumist. Tõdeti, et lisaks kogemusele ja kompetentsile on puudu ka teadmisest, millised võivad olla parimad lahendused.

2. organisatsioonilised nõrkused

Loogiliselt eelnevaga seotud. Üldistest riskidest mainiti majandusliku ja administratiivse külje nõrkust vähese kompetentsi, võimekuse, tehnilise mahajäämuse ja huvipuuduse tõttu. Kardetakse, et selline ebakindlus loob eeldused digiteerimise tsükli erinevate lülide kvaliteedi languseks (andmetöötlus, digiteerimine, metaandmete loomine, hoidlad, säilitamistingimused, juurdepääs). Konkreetse näitena võib tuua hoidlate ebapiisava mahutavuse.
Majanduslanguse tingimustes on mõnedes maades probleemiks ebaküllaldane rahastamine, mis ei ole piisav vajaliku IT vajadusteks, sh isegi elektri ja kommunikatsioonikulude katmisel.

3.IT halduse probleemid

IT süsteemide haldamisega seotud riskid võivad olla andmete või IT-infrastruktuuri puuduliku rahastamise tulemus, kui kasutusele võetakse odavad lahendused ning unikaalsed andmed hävinevad või riknevad.
Paar asutust mainis ka probleemi, et metaandmete hulk on ebapiisav pikaajalise säilitamise jaoks. Samuti võib tugi IT-süsteemide haldamise koostööfirmaga osutuda ebapiisavaks.

4.tehnilised rikked ja defektid

Eriti Eesti mäluasutuste mure. Mitmed välismaa vastajad mainisid ohtu andmekandjatele, põhjuseks elektrisüsteemi võnked ja elektri vms avariid koos riistvara rikkega.

5. füüsiline kriisisituatsioon

Seda riskide gruppi pidasid võimalikuks ohuks võrdselt Eesti ja Skandinaavia mäluasutused. Loodusõnnetuste (nt üleujutuse) eest pole täielikult keegi kaitstud. Minimeerida tuleb hädaolukordade (tuli, vesi) juhtumise võimalikkust. Välistatud pole ka muud füüsilise kahjustuse ohud, mis võivad juhtuda, kui geograafiliselt andmesüsteeme hajutatakse.

6. ründed

Ka otsesed ründed IKT süsteemidele ohustavad mäluasutusi. Seda tajutakse ohuna võrdselt füüsiliste riskidega.

7. IT infrastruktuur

Mäluasutused on riskidena maininud IT infrastruktuuri aegumist ja muid nõrkusi (sh ebasoodne asukoht, nõrk või amortiseerunud riist- ja tarkvara, andmekandjate vananemine).

8. IT arenduse, eriti tarkvaraga, seotud riske (riistvara areng, tarkvara või andmete struktuuri muudatuste käigus tekkiv info kvaliteedi kadu).

9. andmevargus ja autoriõigusega seotud probleemistik, eriti isikuandmete kaitse.

Strukturteeritud küsimuses loetletud riskidest võivad kõik üsna tõenäoliselt juhtuda, **lahter ”risk puudub” jäi tühjaks**.
Suhteliselt madalaks ja ebatõenäoliseks riskiks peetakse füüsilist kriisisituatsiooni (4 x) ning küberrünnakut ja häkkimist (3 x).
Kõige kõrgemaks hinnati nii Eesti kui naabermaade mäluasutuste poolt tehnoloogia ja tehnilise keskkonnaga seotud riske, mida mainisid erineva astme riskitõenäosusena erandita kõik vastanud mäluasutused. IT-arendusega seotud riskid said „teise koha“.
Üldist turvatunnet iseloomustab see, et riskide esinemise võimalikkust hinnati kõige rohkem **keskmiseks ehk mõõdukaks** (28 korda). Eesti ja välismaa mäluasutuste riskitunnetus on sarnane. Väike erinevus oli andmevarguse ja autoriõigusega seotud riskigrupis.
Avaldati muuhulgas arvamust, et turvalisuse nõuetest tingitud koopiate lokaliseerimine riigi eri paikadesse kujutab endast ilmselt riski, sest paigutatakse eri tasemel andmekandjatele.

6. : ideaalsed säilitustingimused eeldavad tööd laial tegevusskaalal

I. Hoiutingimused

Digiteeritud vara turvalise säilitamise tingimustest:
hoidla on usaldusväärne turvanõuetele vastav serveriruum,
kogu hoones on turvasüsteemid ja mehitatud valve,
töökorralduslikult on loodud IKT võimalike tõrgete juhtimise süsteem,
riskid lokaliseeritakse tugeva tarkvaralise tulemüüriga,
kasutatakse varutoiteallikaid (UPSid) jne.

II. Varundamine

kõigis mäluasutustes tehakse jõudu mööda tagavarakoopiaid, st käib pidev andmete varundamine,
oluliste andmekogude varundamine geograafiliselt kauges kohas. Rootsis, Taanis ja Soomes käib koopiafailide hajutamine juba ammu, teistes riikides on vastavate uuendustega algust tehtud.

III. Tarkvaravahendid on enamasti universaalsete programmide (nt FEDORA, IBM Tivoli, Microsoft, Radar) edasiarendused,
süsteemide kasutajad peavad ennast sisenemisel autentimina,
pidevalt käib töö riist- ja tarkvara uuendamisega.

IV. Auditeerimine

Kolmeteistkümnest mäluasutusest kuues ei ole infoturbe seisundit professionaalselt auditeeritud, enamuses piirdub audit asutusesisese kontrolliga. Nendes mäluasutustes, kus auditeerimine on tehtud, toimub see kas asutusesisese riskianalüüsina (näiteks kord aastas) või tellimustööna firmadelt.

V. Finantseerimise tagamine

Loomulikult finantseeritakse digitaalse arhiivi haldamist ja arengut põhiliselt iga maa eelarvest. Skandinaavia riigid rõhutasid, et see kuulub riigi kohustuste hulka ja muid allikaid mainiti väga vähe. Uute EU riikide arendusprojekte on rahastanud ka Euroopa Komisjon või rahvuslikud struktuurfondid.

VI. Sujuv töökorraldus

Digitaalsete arhiivide turvalisus on tagatud:

1) juhtimise tasand

Kõige kõrgemal tasemel juhib ja vastutab infoturbealase poliitika, vastavate nõuete rakendamise ja **töö korraldamise** eest asutuse direktor või asedirektor. Taani Rahvusarhiivis on olemas IT turvalisuse komitee (IT security committee), Soome Rahvusraamatukogus juhib tööd administratsiooni- ja arendusjuht (Head of Administration and Development Services), kes delegeerib ülesanded vastavatele osakondadele.

2) täidesaatev tasand

Paljudes mäluasutustes on **funktsionaalse** taseme institutsiooniks, kes peab hea seisma digitaalsete kogude turvanõuete korraldamise eest arvutisüsteemide osakond või muu allüksus.

3) aluspõhjaline tasand

Kõik kollektsioonide (kogude) juhatajad täidavad tavaliselt ka turvalisust puudutavaid kohustusi ja ülesandeid oma **hallatava süsteemi või andmekogu piires**.
On ka neid mäluasutusi, kus vastutusahelat ei ole veel lõplikult paika pandud.

Enamasti on antud küsimusele vastajad rõhutanud, et **kõik töötajad** peavad seisma hea üldiste infosüsteemide turvalisuse nõuete eest, sest on läbinud vastava koolituse. Antud probleemistik on seotud info kättesaadavuse nõude ja kasutajatega.

7. : riskide hajutamiseks on otstarbekas teha koostööd

Grupeerides neid vastuseid, mis sisaldasid **tulevikuvaateid**, joonistusid välja järgmised jooned:

1.Tulevikus suureneb kindlasti progresseeruvalt digitaalarhiivide töömaht.
2.Määravaks võivad saada mõned sotsiaalsed põhjused (infovõltsingud, andmete jäljendamine ja andmevargused, poliitilised põhjused).
3.Suureneb digitaalarhiivide järjekindla ja läbimõeldud haldamise otsustav roll.
4.Probleeme põhjustab jätkuvalt uue tehnoloogia kasutamine: IT riist- ja tarkvara kiire areng, failiformaatide lootusetu vananemine ja mitmekesistumine, meedia areng.
5.Pikaajalisel säilitamisel võib digiteeritud informatsioon muutuda ja selle läbi toimuda materjali autentsuse kadu.

Turvalisus tähendab mitte niivõrd maksimaalset, aga **optimaalset** panustamist, sellepärast mõistetakse koostöö vajalikkust.
Mitmed vastajad rõhutasid just laiemat, sotsiaalset mõõdet ja selle tähtsust koostööprojektide juures. Nenditi, et infoturvalisuse alal töötavate inimeste ühisarutelud on vajalikud, olgu siis seminaride ja (video)konverentside, e-kirjavahetuse või foorumite vormis. Vajalik oleks nii parima praktika kui *know-how* teoreetlised teadmised. Need suurendavad lisaks otsesele praktilisele väärtusele ka avalikku huvi info turvalise säilitamise temaatikale.
Võimalikud ja vajalikud **ühised projektid**: andmesäilituskokkulepped, standardite ühtlustamise, andmevahetuse turvalisus, info säilitamise vormingute ühtlustamine, ühiste hoidlate loomine jpm.

Kokkuvõte. Digitaalarhiivi varade kaitse on tagatud mitmete seaduste ja määrustega, kuid riiklik regulatsioon jääb sageli üldsõnaliseks ja killustatuks. Valdkonna ja asutuse arengustrateegiad ning töökorraldusjuhendid (kui need olemas on) käsitlevad teemat täpsemalt, kuid neil puudub konsensuslik seaduse kate, et oleks kindlus mäluasutustele spetsiifilise, digiteeritud kultuuripärandi pikaajalise säilitamise ja turvalise juurdepääsu tagamise ühiste jõupingutuste osas.
Tagasi tulles jutu algusse teadmiste-soovide ja tegelikkuse vaheliste kääride kohta, siis eriti suurt vastuolu ei tunnetata. Kahjuks muutub turvalisus oluliseks sageli alles peale õnnetust ja alati on targem pigem karta kui kahetseda. Digitaalne säilitamine on suhteliselt uus võimalus kultuuripärandit säilitada ja puuduvad traditsioonid. Infoturbestandardid ja -meetodid vajavad kindlasti suuremat tähelepanu nii mäluasutustes kui laiemal tasemel, meetmed sätestamist ja rakendamist, valdkondlikud põhimõtted koostööd.

Kai Idarand
RR teadus- ja arenduskeskus
Kai.Idarand@nlib.ee , 630 7121
15.11.2010