

## Vabariigi Valimiskomisjoni infosüsteemi avaliku liidese tehniline audit

Koosataja andmed  
ASA Quality Services  
Ehitajate tee 108, Tallinn 12915  
[www.asaquality.ee](http://www.asaquality.ee)  
[kiri@asaquality.ee](mailto:kiri@asaquality.ee)

23.03.2011

1(6)

## Sisukord

1.	Sissejuhatus .....	2
2.	Lähteülesande kirjeldus .....	2
3.	Auditi meetoodika .....	2
4.	Auditi leiud .....	3
5.	Järeldused .....	4
6.	Soovitused edasisteks arendusprojektideks .....	5

23.03.2011

2(6)

## 1. Sissejuhatus

Antud auditi aluseks on Vabariigi Valimiskomisjoni pöördumine, kus valmiskomisjon soovib saada sõltumatult osapoolelt hinnagut valimistulemuse infosüsteemi avaliku liidese pooleteistunnise katkestuse põhjuste ja kriisi ohjamise pädevuse kohta 06. märtsil 2011. aastal.

Audit viidi läbi ajavahemikus 14. märts kuni 23. märts 2011.

## 2. Lähteülesande kirjeldus

Vastavalt Vabariigi Valimiskomisjoni soovile keskendus audit valimiskomisjoni infosüsteemi avaliku liidese töö tõrkele 2011. aasta 06. märtsi õhtul kella 20:55-22:35 vahel. Auditi ülesandeks on anda hinnang järgmistes küsimustes:

- Tõrke iseloomu kuuluvus arendus- või haldus/majutusprotsessi;
- Kas andmebaasiserverite seadistused vastasid seatud eesmärkidele;
- Andmebaasi ja infrastruktuuri administraatorite tegevuse adekvaatsus veaolukorras;
- Monitooringu võimekus tuvastada häireid infosüsteemi töös;
- Infosüsteemi testideks kavandatud ressursi piisavus arendaja AS Helmes poolt.

## 3. Auditi meetodika

Auditi meetodika baseerus intervjuudele nii AS Helmes kui ka Vabariigi Valimiskomisjoni töötajatega, kes osaleseid infosüsteemi arendamisel, testimisel ja haldamisel. Lisaks intervjuudele koguti auditi käigus mitmesugust tõendusmaterjali taastamiseks sündmuste käiku 06. märtsil 2011. Materjali hulka kuuluvad infosüsteemi komponentide seadistusfailid, mitmesugused logifailid, kriisiplaanid, osapoolte vaheline elektrooniline kirjavahetus ja arendustegevuse lepingud.

Auditi raportis toodud järeldused on tehtud ainult esitatud materjalide baasil.

23.03.2011

3(6)

## 4. Auditi leiud

### Oluliste sündmuste ahel 06. märtsi õhtul

#### 20:55

Vabariigi Valimiskomisjoni juurde valimispäeva õhtuks kogunenud töögrupp märkab, et valimiste infosüsteemi avaliku liidese kaudu edastatavad valimistulemused ei ole õigeaegselt uuenenud. Samal ajal avastab AS Helmes meeskond, et valimistulemuste aruanne ei ole õigeaegselt valminud.

#### 21:00

Helmese süsteemiadministraator tuvastab probleemi aruandegeneraatoris (audit selgitab, et tegemist on iseseisva Java EE rakendusega, mis on paigaldatud VIS valimiste infosüsteemist eraldi JBoss rakendusserverile ning mille funktsiooniks on valimistulemuste XML formaadis aruande perioodiline koostamine iga 3 minuti järel)

#### 21:06

Rakendusserverile tehakse algkäivitus.

#### 21:12

Helmese süsteemiadministraator edastab rakendusserveri logiväljavõtte vahemikust 21:06:40 kuni 21:11:41 arendajale. Otsustatakse, et arendus hakkab testima päringuid vastu varulokatsioonis olevat andmebaasi.

#### 21:14

Andmebaasiserverisse logib sisse kogu intsidendi ajal esimest korda juurkasutaja (root).

#### 21:17

Andmebaasiserverisse logib sisse baasiadministraator.

#### 21:19

Rakendusserverile tehakse algkäivitus.

#### 21:20

Helmese süsteemiadministraator annab arendusele teada, et andmebaas varulokatsioonis on olemas ja et see on seal kogu aeg olemas olnud.

#### 21:34

Rakendusserverile tehakse algkäivitus.

#### 21:40

Helmese andmebaasiadministraator alustab intsidendi lahendamist.

#### 21:44

Helmese andmebaasiadministraator edastab arendusele probleemse päringu.

23.03.2011

4(6)

**21:53**

Audit tuvastas andmebaasiserverile edastatud käskude ajaloo põhjal, et käsitsi baasistatistika uuendamise ja seeläbi probleemi lahendamiseni jõudis Helmese meeskond pärast seda kellaaega.

**22:12**

Rakendusserverile tehakse algkäivitus.

**22:31**

Rakendusserveris toimub viimast korda transaktsiooni tagasikerimine. Rakenduse normaalne töö on taastunud.

## 5. Järeldused

Tutvunud logifailide ja kirjavahetusega järeltab audit järgmist:

**Tõrke iseloomu kuuluvus arendus- või haldus/majutusprotsessi;**

Audit tuvastas, et antud intsidendi lahendamine kuulub halduse pädevusse, sest:

- Andmebaasi nõuetekohase toimimise tagamine on majutusteenuse lepingu osa;
- Valimiste infosüsteem töötas enne intsidenti, intsidendi ajal ja pärast intsidenti muutmata kujul toodangukeskkonnas.

Neid kahte asjaolu arvestades ei saa antud intsidenti lugeda arendusega seotud probleemiks.

**Kas andmebaasiserverite seadistused vastasid seatud eesmärkidele;**

Audit leiab, et andmebaasiserver oli seadistatud konfiguratsioonis, mis sobis antud andmemahtude töötlemiseks. Intsidendi tekitas ebaefektiivne päringuplaan, mis ei uuenenud vastavalt andmebaasi salvestatavate andmete kasvule. Automaatne andmebaasistatistika uuendamine oli AS Helmes poolt teadlikult andmebaasi seadistustes välja lülitatud, mis on aktsepteeritav ja hea tava. Baasistatistika uuendamine oli manuaalse protseduurina AS Helmese tegevusplaanis ette nähtud, kuid seda ei rakendatud enne kella **21:53**. Mainitud manuaalse protseduuri käivitamine oli andmebaasiadministraatori pädevuses.

**Andmebaasi ja infrastruktuuri administraatorite tegevuse adekvaatsus veaolukorras;**

Audit leiab, et andmebaasi administraatori tegevused ei olnud adekvaatsed. Infrastruktuur toimis laitmatult. AS Helmes poolne intsidendihaldus polnud koordineeritud. Viited tõrke põhjuse kohta oleks saanud välja lugeda aruandegeneraatori logifailist tõrke tekkimise hetkel. Sellele järgnev opeatiivne ja koordineeritud tegutsemine oleks võimaldanud tõrke õigeaegselt likvideerida. Paraku otsiti potentsiaalset viga rakenduse seni toimunud ärioloogikast, millele kulutati rohkem kui lepingujärgselt lubatud 15 minutit infosüsteemi avaliku liidese mittetoimimise aega.

**Monitooringu võimekus tuvastada häireid infosüsteemi töös;**

Audit leiab, et monitooringusüsteemi võimekus infosüsteemi töös esinevaid võimalikke häireid tuvastada oli piiratud ainult serverite mälu-, ketta- ja protsessorikasutuse

23.03.2011

5(6)

jälgimisega. Monitooring ei pööratud piisavalt tähelepanu rakenduse oluliste komponentide logidele.

**Infosüsteemi testideks kavandatud ressursi piisavus arendaja AS Helmes poolt;**

Audit leiab, et funktsionaalsete testide osas oli AS Helmese kavandatud resurss piisav. Mittefunktsionaalsete testides pöörati tähelepanu taristu töökindlusele, kuid ei testitud infosüsteemi käitumist maksimaalse andmemahu korral.

## 6. Soovitused edasisteks arendusprojektideks

Antud süsteemi kontekstis ei rakendanud Vabariigi Valimiskomisjon piisaval määral projekti järelvalvet. Projekti otsused jäid dokumenteerimata ning edastati suusõnaliselt. Seetõttu jäid nendest otsustest tekkivad potentsiaalsed riskid kaardistamata. AS Helmes hindas andmebaasi serveri tõrget madala esinemistõenäosusega keskmiseks riskiks. Andmebaasiserveri riskina oli kaardistatud risk juhuks, kui server lakkab töötamast ning maanduseks oli ette valmistatud võimalus suunata rakendusserverite päringud ümber teise andmebaasiserverisse, mis on majutaja seisukohast adekvaatselt hinnatud ja maandatud risk. Projekti juhtrühm peaks projekti kestel läbi viima „mis siis kui“ koosolekuid, et leida ja kaardistada uusi riske (nii äri-, kui ka arendusriske), et vältida sarnaseid olukordi. Samuti on mõistlik kaasata järelvalveekspert, kui tellija projektijuhil ei jätku piisavalt aega loetletud tegevuste tegemiseks.

Projektis eksisteeris küll kriisiohjamismeeskond, mis koosnes nii Vabariigi Valimiskomisjoni kui AS Helmes esindajatest, kuid auditi läbiviijale ei esitatud kriisimeeskonna detailseid tegevusjuhiseid ega riskiplaane, mistõttu võib järeldada, et AS Helmese meeskonna liikmetel puudusid konkreetsed tegevusjuhised erinevate tarkvaraliste veaolukordade lahendamiseks. Vabariigi Valitsuskomisjonil eksisteeris äririski maandamiseks varuplaan (tulemusi hakati edastama alternatiivkanalite kaudu), mille käikuandmisega viivitati, sest AS Helmes kinnitas Vabariigi Valimiskomisjoni esindajale kogu intsidendi jooksul probleemi peatsest lahendumisest. Selliste olukordade vältimiseks on tulevikus mõistlik laia kõlapida omavate süsteemide rakendamisel määrata rakendamispäeval üks kriisijuht (olenemata kriisijuhi organisatoorsest kuuluvusest või tavaelu alluvussuhetest), kes võtab kriisiohjamise täielikult enda valdusse ning kelle käskude ja korralduste järgi kogu kriisimeeskond edasi tegutseks. Samuti peavad olema kriisijuhil kindlad tegevuskavad, et teenuse käideldavus ei langeks alla kokkulepitud normi olenemata, kas probleemi põhjus peitub tarkvaras või taristus. Ühe kindla kriisijuhi puudumine (sisuliselt oli kaks kriisimeeskonda) viis kriisi tekkimisel peataolekuni ning AS Helmese meeskond tegutses juhuslikult. Vabariigi Valimiskomisjoni esindajatel puudus üheselt võimalus kriisi ohjata, sest kommunikatsioon tarkvara haldusega käis AS Helmese projektijuhi kaudu. Kõikide nende asjaolude kokkulangemine tingis avaliku liidese liiga pikaajalise mittetoimimise. Samuti on soovitatav läbi mängida „mis siis kui“ koosolekutelt tekkinud riskistsenaariumid ja veenduda, et kogu meeskond suudab plaani järgi toimida.

23.03.2011

6(6)

Ülari Ainjärv  
Süsteemiarhitekt  
[dokument on digitaalselt allkirjastatud]

Tanel Nargla  
Infosüsteemide audiitor  
[dokument on digitaalselt allkirjastatud]

Sander Vallaots  
ASA Quality Services  
[dokument on digitaalselt allkirjastatud]