LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Centre des technologies de l'information
de l'État

Luxembourg, le 18 OCT. 2016

Le Ministre de la Fonction publique
et de la Réforme administrative

Vu l'article 6 du règlement (UE) n° 211/2011 du Parlement européen et du Conseil relatif à l'initiative citoyenne ;

Vu l'article 1er du règlement d'exécution (UE) n° 1179/2011 de la Commission du 17 novembre 2011 établissant des spécifications techniques pour les systèmes de collecte en ligne conformément au règlement (UE) n° 211/2011 du Parlement européen et du Conseil relatif à l'initiative citoyenne ;

Vu l'article 1er de la loi du 23 mars 2012 relative à la mise en application du règlement (UE) n° 211/2011 du Parlement européen et du Conseil du 16 février 2011 relatif à l'initiative citoyenne ;

Vu les résultats de l'audit réalisé par le Centre des technologies de l'information de l'État sur le système de collecte en ligne https://ec.europa.eu/citizens-initiative/REQ-ECI-2016-000004/public utilisé pour la collecte des déclarations de soutien à *MORE THAN EDUCATION* ;

**Arrête:**

**Art. 1er** .- Le système de collecte en ligne https://ec.europa.eu/citizens-initiative/REQ-ECI-2016-000004/public utilisé pour la collecte des déclarations de soutien à *MORE THAN EDUCATION* est conforme aux dispositions pertinentes du règlement (UE) n° 211/2011.

**Art. 2** .- Le présent arrêté sera adressé à *MORE THAN EDUCATION* pour la collecte des déclarations de soutien par le biais du système de collecte en ligne https://ec.europa.eu/citizens-initiative/REQ-ECI-2016-000004/public. Ampliation en sera transmise au Centre des technologies de l'information de l'Etat.

Le Ministre de la Fonction publique
et de la Réforme administrative

Dan Kersch

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Centre des technologies de l'information
de l'État

# Note à l'attention de Monsieur le Ministre Dan Kersch

**Objet : Initiative citoyenne européenne « More than Education »**

Dans le contexte des initiatives citoyennes européennes, la loi du 23 mars 2012 établit que la certification des systèmes de collecte en ligne de signatures hébergés au Luxembourg incombe au ministre ayant les Technologies de l'information de l'État dans ses attributions. Depuis octobre 2012 vingt-et-un systèmes de collecte en ligne de signatures ont ainsi été certifiés au Luxembourg.

Le 25 septembre 2016, l'initiative « More than Education » nous a adressé une demande de certification de leur système de collecte en ligne.

Conformément à la procédure en place, le CTIE a entamé un audit du système de collecte en ligne de cette initiative afin d'évaluer sa conformité avec les exigences du règlement européen d'exécution EU 1179/2011. L'audit est terminé et n'a mis en lumière que les non-conformités mineures habituelles pour ce type d'audit, comme indiqué dans le draft de rapport d'audit en annexe. Cependant le rapport final d'audit n'est pas encore disponible, car le processus formel de validation du rapport vient seulement de commencer chez le prestataire.

Or conformément à l'article 6.3 du règlement européen EU 211/2011, le certificat doit être délivré aux organisateurs endéans un mois de la demande de certification. Bien que les résultats de l'audit soient déjà connus, le processus interne de validation du rapport chez le prestataire risque donc de mettre en danger le respect de notre obligation légale par rapport à l'article précité.

Au vu de ces éléments, je me permets de demander à Monsieur le Ministre de signer l'arrêté de certification en annexe en vue d'une délivrance aux organisateurs de l'initiative « More than Education ».

Luxembourg, le 13 octobre 2016

Deloitte.

# CTIE

## Compliance assessment of ECI "More than education" using OCS hosted at DIGIT

DRAFT VERSION

12th October, 2016
DRAFT Version

# Table of contents

# 1 Objectives, scope and approach

## 1.1 Context and objectives

In accordance with our engagement letter dated 25 October 2013, as amended, we have been appointed by the Centre des Technologies de l'Information de l'Etat (hereafter referred to as the CTIE) to carry out audits in order to allow the CTIE to certify the organisers of European Citizens Initiatives (hereafter referred to as ECI).

The European Union's («EU») treaty provides every citizen the right to participate on democratic life of the EU using a "European Citizens Initiative. This procedure gives the possibility for citizen to directly address the European Commission (hereafter referred to as EC) in order to present a request for a juridical act. Citizens can support such an initiative by completing a specific form given by the initiative's organizer. This form can be a paper form or an electronic form filled in via the Internet (i.e. a web site). The first step in the ECI process is for the organiser to declare their initiative to the Commission. If the initiative is authorised by the EC, the organiser can subsequently organise paper or electronic collection of forms. In order to be allowed to carry out electronic collection, certification of the collection system has to be obtained from the national certification authority, which is the CTIE for Luxembourg. After receiving a certification request, the CTIE has of one month to audit the online collection system and certify (or not) the concerned collection system. Online support collection can only start after certification. The CTIE has mandated Deloitte to carry out the ECI certification audits on behalf of the CTIE.

In order to certify ECI organisers, the organisers have to be found to be compliant with:

- Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative
- Commission Implementing Regulation (EU) No 1179/2011 of 17 November 2011 laying down technical specifications for online collection systems pursuant to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative

For this purpose, CTIE has validated and has made available an audit guide which take into account the above regulations and which has to be used by the IT auditor to carry out the audit.
Our audit activities were carried out based on ISACA *Standards for Information Systems Control Professionals*.

The ECI auditee for this report is "More than education", however as the initiative uses hosting of OCS at DIGIT (the EC) and as the majority of information assets are hosted by DIGIT, this also brings DIGIT into the audit scope. This document presents the audit activities that were carried from September 07th 2016 to October 12th 2016 in this context, i.e. the compliance audit of the organiser with the EU regulations, for both "More than education" and their service provider, DIGIT.

It is important to note that no testing was conducted by Deloitte and that the design adequacy testing activities were limited in the sense that some controls are documented but have not been operated yet, as operation of OCS can only start after certification. A significant part of our audit procedures was based on evidence provided by the auditees (DIGIT and "More than education"), including areas such as testing (e.g. running of scripts on server to be tested). All infrastructure testing activities were performed by DIGIT staff. The evaluation results provided by our audit procedures should therefore be considered in the light of these limitations on the nature and extent of evidence-gathering procedures performed.

## 1.2 Scope

The previously stated regulations do not specify how hosting may influence the requirements and the way the audit has to be carried out. Requirements for the ECI initiative and infrastructure on the other hand are clearly stated.

In the context of the hosting of the ECI infrastructure by DIGIT, two parties are involved in the ECI initiative. On one hand the organiser ("More than education") with limited systems and infrastructure on their side, used to consult and manage their ECI system instance and DIGIT on the other hand, hosting the ECI systems (i.e. multiple instances of ECI systems, one for each organiser), where the majority of information assets are located. The only possible interpretation of the regulations (in line with security standards and practices) is that both need to comply with the regulations in order for the CTIE to be able to certify an initiative involving both parties.

The audit guides foresee two different use cases, an ECI using OCS (publicly available software produced by the EC for ECI purposes) and an ECI not using OCS. This assessment concerns the use case of an ECI system using OCS and hence follows the workflow in the audit guide foreseen for this use case.

The following activities and assets have been involved in the assessment:

### 1.2.1 EC DIGIT ECI

- 1 - **Solaris**
- 2 - **Oracle Database**
- 3 - **Weblogic**
- 4 - **Ubuntu Live-DVD**
- 5 - **ISO 27002 Checklist**
- 6 - **Physical - network – encryption**
- 7 - **Risk Assessment SoA / RTP and supporting documentation**

### 1.2.2 More than education

- 8 - **ISO 27002 Checklist**
- 9 - **Risk Assessment SoA / RTP and supporting documentation**

## 1.3 Assessment activities approach

Based on the audit guide, the following activities have been performed in relation with the previously defined scope:

- Preparation of extraction scripts related to security controls for Solaris and Oracle Database as documented in the audit guide.
- Interviews, document/evidence request for controls as required by the audit guide.
- Execution of scripts by each concerned DIGIT team (after acceptance of the scripts by the DIGIT).
- Analysis of received evidence, documents and script results.
- Validation of audit points with the DIGIT/More than education

# 2 Assessment summary

## 2.1 Non conformity ratings definition

The following non conformity ratings have been used to evaluate conformity against the EC ECI regulations (see "1.1 Context and objectives")

| Non-conformity description | Level of non-conformity |
|---|---|
| Non conformities which have a high impact on the degree of compliance of the auditee with EC ECI regulations. A single non conformity of this level can cause the CTIE to find the ECI collection system is not compliant with relevant EC ECI regulations and hence cannot be operated until re-audited and found to be compliant. | Major |
| Non conformities which have a medium degree of impact on the compliance of the auditee with EC ECI regulations. A significant quantity of risks of this level can cause the CTIE to find the ECI collection system is not compliant with relevant EC ECI regulations and hence cannot be used until re-audited and found to be compliant. If the CTIE deems the amount of medium non conformity findings to be acceptable, the CTIE can agree to certification. | Medium |
| Non conformities which have a low degree of impact on the compliance of the auditee with EC ECI regulations. At this level, non-conformities are of "housekeeping" level that should ideally be resolved, but the non-conformities in themselves do not prevent certification. | Minor |

## 2.2 Summary of findings

The tables below present the findings for the assessment performed for the scope and objectives previously defined, and carried out as described in the audit guide:

Severity levels of non-conformities are distributed as follows:

- 4 Minor non-conformities
- 0 Medium non-conformity
- 0 Major non-conformity

The ID's in the findings below correspond to the relevant sections in the audit guides if applicable.

### 2.2.1 Solaris

| IDs | Non-conformity description | Level of non-conformity | Auditee(s) concerned |
|---|---|---|---|
| 4.5 | Solaris local terminal commands are not logged. | Minor | DIGIT |
| 6.6 | SSH Root connection is allowed. | Minor | DIGIT |

### 2.2.2 Oracle Database

| IDs | Non-conformity description | Level of non-conformity | Auditee(s) concerned |
|---|---|---|---|
| | No finding for this section. | | DIGIT |

### 2.2.3. Weblogic

| IDs | Non-conformity description | Level of non-conformity | Auditee(s) concerned |
|---|---|---|---|
| | Traffic between the reverse proxy and Weblogic is not encrypted. | Minor | DIGIT |

### 2.2.4. Ubuntu Live-DVD

| IDs | Non-conformity description | Level of non-conformity | Auditee(s) concerned |
|---|---|---|---|
| | No finding for this section. | | |

### 2.2.5. ISO 27002 Checklist

| IDs | Non-conformity description | Level of non-conformity | Auditee(s) concerned |
|---|---|---|---|
| | No finding for this section. | | |

### 2.2.6. Physical - network – encryption

| IDs | Non-conformity description | Level of non- | Auditee(s) |
|---|---|---|---|

| | | conformity | concerned |
|---|---|---|---|
| No finding for this section. | | | |

### 2.2.7. Risk Assessment SoA / RTP and supporting documentation

| IDs | Non-conformity description | Level of non-conformity | Auditee(s) concerned |
|---|---|---|---|
| | Lacks in the Business Impact Assessment formalisation | Minor | More than education |

### 2.2.8. New ECI installation procedures

| IDs | Non-conformity description | Level of non-conformity | Auditee(s) concerned |
|---|---|---|---|
| No finding for this section. | | | |

# 3 Detailed assessment findings

## 3.1 Solaris

### 3.1.1 Solaris local terminal commands are not logged (4.5) (Minor)

**Observation:**

There are no logs for commands entered via Solaris local terminal.

After an interview with Solaris team, there is no KVM allowing a distant access to Solaris local terminal's server.
For physical access, the server is located in a physically protected data center, each rack is secured by two different locks (one for front panel and the other for back panel).
Physical protections are mitigating the risk.

**Standard:** 1179/2011 2.16. All system activity logs are in place.
The system makes sure that audit logs recording exceptions and other security-relevant events listed below may be produced and kept until the data is destroyed in accordance with Article 12(3) or (5) of Regulation (EU) No 211/2011. Logs are adequately protected, for instance by storage on encrypted media. Organisers/administrators regularly check the logs for suspicious activity. Log contents include at least:

(a) dates and times for log-on and log-off by organisers/administrators;

(b) performed backups;

(c) all database administrator changes and updates.

**Risk:** Minor

**Recommendation:**
Activate logs for commands entered via Solaris local terminal (loginlog).
Regularly check data center logs and verify that only authorized accesses are done.

**Comments from Management (DIGIT):**

- Agree/ Disagree :
- Action to be taken :
- Person responsible :
- Time frame :

### 3.1.2 SSH Root connection is allowed (6.6) (Minor)

**Observation:**

The "PermitRootLogin" parameter specifies if the root user can log in using ssh. The default value is "no".
The root user must be restricted from directly logging in from any location other than the terminal.

Deloitte's script detected that this parameter is enabled:
"`PermitRootLogin without-password`" is defined in SSHD configuration file.

Solaris operators are using SSH root access via private key to administrate servers.

The use of private key is mitigating the risk as it is not directly possible to launch brute force attacks against known root login.

**Standard:** Best practices on Operating Systems

**Risk:** Minor

**Recommendation:**
Root access should not be use remotely, it is possible to grant exceptional root permission using "sudo" commands or it could also be possible to log as normal user and request root access using "su" command.

**Comments from Management (DIGIT):**

- Agree/ Disagree :
- Action to be taken :
- Person responsible :
- Time frame :

## 3.2 Oracle Database

No finding for this section.

## 3.3 Weblogic

### 3.3.1 Traffic between the reverse proxy and Weblogic is not encrypted (Minor)

**Observation:**

The traffic between the client and the reverse proxy is encrypted using HTTPS protocol.

The traffic between Weblogic and Oracle Database is encrypted by Weblogic.

However, the traffic between the reverse proxy in a DMZ and the Weblogic server is not encrypted.

**Standard:** 1179/2011 2.7.7. (in particular point A) The system provides for encryption of data as follows:

(a) personal data in electronic format is encrypted when stored or transferred to the competent authorities of the Member States in accordance with Article 8(1) of Regulation (EU) No 211/2011, the keys being managed and backed up separately;

**Risk:** Minor

**Recommendation:**
Establish a secure link between the reverse proxy and the Weblogic server; this can be done by using encryption or by using a separate network zone (VLAN for example).

**Comments from Management (DIGIT):**

- Agree/ Disagree :
- Action to be taken :
- Person responsible :
- Time frame :

## 3.4 Ubuntu Live-DVD

No finding for this section.

## 3.5 ISO 27002 Checklist

No finding for this section.

## 3.6 Physical - network – encryption

No finding for this section.

## 3.7 Risk Assessment SoA / RTP and supporting documentation

### 3.7.1 Lacks in the Business Impact Assessment formalisation (Minor)

**Observation:**

There are some formalisation lacks in the Business Impact Assessment document:

- In the section "Document History, the date mentioned for the version v1.0 is "03/09/2012", which is erroneous.

**Standard:** 1179/2011 2.2. Organisers choose security controls based on the risk analysis in 2.1(a) from the following standards: (1) ISO/IEC 27002.
From ISO/IEC 27002, point A.5.1.1 Information security policy document:
An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.

**Risk:** Minor

**Recommendation:**

- Confirm the correct date for the version v1.0 of the Business Impact Assessment document and formalise it in the document.

**Comments from Management (More than education):**

- Agree/ Disagree :
- Action to be taken :
- Person responsible :
- Time frame :

## 3.8 New ECI installation procedures

No finding for this section.

**www.deloitte.lu**

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in 150 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's 200,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other, and strength from cultural diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.