Strictement Confidentiel

Projet d'Audit du Registre Electoral 2014

Phase Synthèse de la mission

Rapport de Synthèse de la Mission d'Audit

(Destiné au Conseil de l'ISIE)

Livrable - Rapport de Synthèse Finale

Septembre 2015

Mr Elyes Khemiri, **(Chef de Projet – IT Security Consultant)** Auditeur Certifié ISO 27001-Lead Auditor auprès de LSTI Accrédité par le COFRAC en France, Certifié ISMS auprès du TUV-Allemagne, Certifié ANSI

1- Objectif de la mission & Références normatives / Outils & méthodes d'audit

Objectif :

L'objectif de cette mission est d'auditer le registre électoral 2014 en vérifiant en premier lieu le processus d'importation du registre électoral 2011, en second lieu en évaluant l'état de la sécurité du Registre Electorale 2014 et en réalisant par la suite un ensemble de tests de performance de l'environnement support de l'exploitation du registre électoral 2014.

Références normatives & Méthodes et Outils:

Références normative : Norma ISO 27002:2013 (14 Chapitres, 35 Objectifs de sécurité, 113 mesures)

Outils et Benchmarks pour les tests de performances : PGbench (Tests performances Base de données), iPerf (Réseau), Stress et Jmeter (tests de perfmances applicatif et système)

Les Méthodes d'Audit du processus d'importation et de la sécurité du registre électorale seront décrites dans la section suivante.

2- Modalités de Réalisation et périmètre d'Audit

2.1 Modalités de réalisation

L'audit a été réalisé durant la période du 17 Août 2015 au 11 Septembre 2015.

Les conclusions présentées dans notre rapport reposent sur les entretiens menés auprès des différents interlocuteurs, l'analyse de la documentation et la réalisation de tests et de contrôles sur le registre électoral 2014.

2.2 Périmètre des travaux

Les travaux d'audit ont pris en compte le périmètre défini dans le cahier des clauses techniques particulières du cahier des charges pour l'audit du registre électoral 2014. L'intervention est limitée par les documents qu'ont été fournis aux auditeurs et par l'accès qui leur a été donné sur les systèmes contrôlés.

Des tests techniques (partie performances) ainsi que des vérifications physiques et documentaires ont été effectués au niveau des locaux du CNI (Hébergeur de la plateforme).

3- Equipe d'Audit

Mr Elyes Khemiri, Chef de Projet, Expert Senior en Sécurité des SI, Certifié ISO 27001-Lead Auditor

Mr Mohamed Basti, Membre Auditeur, Expert d'Audit informatique , Certifié CISA/CISM, ISO 27001 Lead Auditor

Mr Aymen Belkhiria, Membre Auditeur, Expert d'Audit des performances

4- Synthèse des Constats d'Audit du Registre Electoral 2014

4.1 - Partie : Tests de performance du SGBD et de l'environnement Réseau, Système et applicatif support du Registre électoral 2014

Constats des tests de performance et du choix du noyau SGBD

Le benchmark de la base de données a démontré qu'une machine physique peut supporter qu'une seule Machine Virtuelle base de données (Limite CPU atteint 80%) donc il est recommandé d'allouer toute une machine physique pour la Machine virtuelle base de données (ceci afin d'éviter des problèmes d'atteinte à la disponibilité du noyau de base de données / problèmes de performances de la base).

En outre, pour les applications WEB, il est préférable d'utiliser une base de données MySQL, pour tous les benchmarks réalisés Mysql est plus rapide et stable que Postgress. Pour le cas des applications ISIE, nous avons constaté qu' il n'existe pas des avantages pour l'utilisation de Postgress. en effet pour l'architecture couramment utilisé par l'ISIE, il est possible d'avoir une réplication Actif/Actif --> avec chaque 2 Serveurs Web pointent sur une des bases de données.

Constats des tests du remontée des charges (Système) et tests de performance réseau

En faisant les testes de remonté des charges IO/CPU/Memory, nous avons détecté que 80% d'une Machine virtuelle (VM) est plus 25% CPU de la machine physique, cad avec 12 Machines avec 80% CPU peuvent occuper toutes les ressources CPU des machines physiques, En effet le risque de perdre une machine physique pourra affecter toute la plateforme. Par conséquent et du point de vue architecture il est recommandé d'ajouter une autre machine physique dans le Blade (Infra) des serveurs Applicatif et base de données

Pour les testes qu'ont été effectués sur le réseaux avec une seule machine en action, nous avons montré que la totalité de la bande passante est de 533 Mbits/s, avec plus de 15 machines actives, le réseau est la maille faible dans le cluster des machines virtuelles (VMs). Il est ainsi recommandé d'améliorer la bande passante réseau.

Constats des tests de l'applicatif WEB

Il est à signaler que suite à l'interview avec l'équipe responsable du projet coté de l'ISIE , la valeur maximale des connexions simultanées est 300 connections simultanés pour une instance.

Nous avons constaté lors des tests avec l'outil Jmeter que la ressource CPU dans l'instance Glassfish (instance Applicatif - Machine virtuelle) atteint 100% d'utilisation dés le lancement du stress test et que le temps de réponse au moyenne est de 13 sec.

Cette grande utilisation dans le CPU pourra conduire à un crash de la Machine virtuelle. Ce problème pourra être résolu par un tunning coté application (JSF) /OS(Redhat) /GlassFish.

Synthèse des Constats : Existence des problèmes de performances Base de données, Système, Réseau et applicatif au niveau de l'architecture existante de la plateforme d'inscription des électeurs (une refonte de l'architecture est fortement recommandée afin d'assurer le bon dimensionnement matérielle, choix du noyau SGBD/applicatif/WEB ainsi que l'étude de mise en place de l'infrastructure virtuelle et réseau).

Il est à signaler en outre, le Tunning et le Hardering des environnements Open Source (Postgresql, GlassFish, Apache,RedHat) nécessitent un support permanant et des compétences justifiés et maitrise de ces environnements durant la période d'inscription/élection ce qui devra pris en compte en cas de continuation avec la même plateforme.

4.2 - **Partie** : Audit du Processus d'importation du Registre électoral 2011

Pour s'assurer du bon déroulement des opérations de passation et d'importation du registre électoral 2011, nous avons procédé à :

- La vérification de la procédure adoptée pour la passation et l'importation du registre électoral 2011 au sein du nouveau registre d'électeurs 2014 et,
- L'examen croisé du registre électoral 2011 et du registre électoral 2014.

La vérification de la procédure comporte la compréhension des différentes phases d'importation et l'évaluation des contrôles automatiques et manuels effectués.

L'examen croisé porte sur des échantillons de tailles optimales et représentatives des populations mères. Les populations mères définies représentent l'ensemble des électeurs inscrits volontairement lors des élections 2011 par circonscription.

La méthode d'échantillonnage probabiliste choisie est le sondage aléatoire simple avec une marge d'erreur de plus ou moins 5%.

Résultats de la vérification de la procédure

Le processus adopté pour la passation et l'importation du registre électoral 2011 au sein du nouveau registre d'électeurs 2014 s'est basée sur des jobs de migration de l'ETL (Extract, Transform, Load)Talend: logiciel Open Source spécialisé dans l'intégration et la gestion des données.

Cet outil a permit la planification des contrôles automatiques pour respecter les contrôles d'intégrité dans la base électorale 2014 et garantir l'intégrité des données sources lors de l'opération d'importation.

En plus de ces contrôles automatiques, des contrôles manuels ont été implémentés pour s'assurer de l'exhaustivité et la fiabilité des données importées :

- Vérification de nombre des lignes insérés dans la base de données cible par rapport au nombre des lignes des bases de données source.
- Examen de la fiabilité des données notamment la longueur des CIN doit être égale à 8.

Constats :

1. L'ISIE n'a pas développée une procédure formalisée d'importation du registre électoral 2011 définissant le QUI (intervenants), le QUOI (tâches, activités et contrôles), le COMMENT (instruction spécifique ou mode opératoire) et le QUAND (enchainement des tâches et activités).
2. L'ISIE n'a pas développé une procédure formalisée de gestion des incidents et des problèmes. Les incidents et les problèmes ne sont pas répertoriés.

Résultats de l'examen croisé du registre électoral 2011 et du registre électoral 2014

Pour les circonscriptions locales, l'examen croisé a permis d'identifier, que sur les 10 216 électeurs sélectionnés dans l'échantillon, 176 électeurs (1,7%) inscrits volontairement lors des élections 2011 ne se retrouvent pas au niveau du registre électoral 2014.

Toutefois, ces écarts ont été, tous, justifiés suite à notre vérification avec l'équipe de l'ISIE comme suit:

- 15 électeurs appartiennent à la Force de Sécurité Intérieure (FSI),
- 17 électeurs à la Défense,
- 6 électeurs sont en pénitentiaire,
- 137 électeurs sont décédés,
- 1 électeur avec un numéro CIN n'existant pas dans la base du ministère intérieur

Pour les circonscriptions à l'étranger, l'examen croisé a permis d'identifier, que sur les 2 287 électeurs sélectionnés dans l'échantillon, 1 166 électeurs (50,98%) inscrits volontairement lors des élections 2011 ne se retrouvent pas au niveau du registre électoral 2014.

Toutefois, ces écarts ont été, tous, justifiés suite à notre vérification avec l'équipe de l'ISIE comme suit:

- 698 électeurs sont déjà inscrits par CIN,
- 398 électeurs sont inscrits par un nouveau Passeport,
- 3 électeurs ont une date de naissance inférieure à 18 ans,
- 5 électeurs sont inéligibles,
- 17 électeurs sont inscrits dans des centres de vote fermés.

Remarque : Les détails des examens croisés ont été présentés dans la Partie 2 du Rapport détaillé d'Audit.

4.3 - Partie : Audit Sécurité du Registre électoral 2014

Afin de vérifier la pertinence des données existantes et les mesures utilisées pour assurer la sécurité des informations relatives aux électeurs, nous avons procédé aux vérifications suivantes :

- Vérification de la procédure de collecte et de mises à jour des données auprès des institutions tunisiennes,
- Vérification des procédures de traitement des doublons dans le registre électoral,
- Vérification des procédures de publication des listes électorales et examen croisé du registre et des listes électorales,
- Evaluation de l'état de la sécurité du Registre Electorale 2014 en conformité aux bonnes pratiques (tel que les règles/mesures de la Norme ISO 27002:2013) en matière de la sécurité des Systèmes d'information (plus précisément - Focalisation sur le Périmètre d'Audit : Le contenu du Registre électorale 2014)

Résultats de l'audit

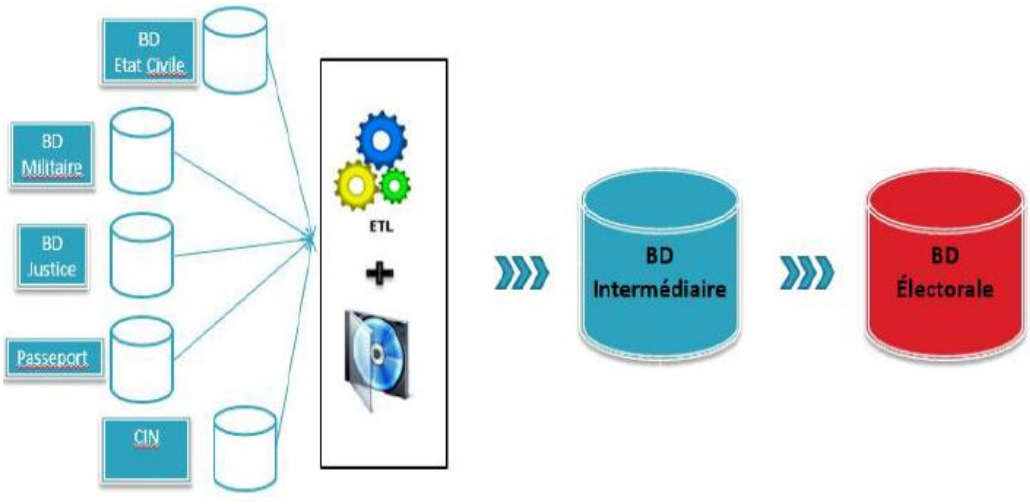
4.3.1 Résultats de la vérification de la procédure de collecte et mises à jour des données

La collecte et la mise à jour des données au niveau de la base de données électorale 2014 sont assurées par la synchronisation avec une base de données intermédiaire appelée SandBox.

La constitution et la mise à jour de la base de données intermédiaire (SandBox) a été confié au Centre National Informatique (CNI) dans le cadre d'une convention avec l'ISIE.

Cette base de données intermédiaire est constituée et mise à jour à partir des différentes données, sous différents formats de fichiers (Excel, Word, texte, papier), communiqués officiellement au CNI par les différentes institutions tunisiennes.

Le schéma suivant décrit de façon synthétique le processus de collecte et de mise à jour des données :



Durant le processus de collecte des données auprès des institutions tunisiennes, le CNI exécute des contrôles automatiques pour respecter les contrôles d'intégrité de la base intermédiaire et des contrôles manuels pour s'assurer de l'exhaustivité et la fiabilité des données importées.

En cas de rejets ou de détection d'erreurs, le CNI déclare officiellement l'incident à l'institution concernée pour la corriger avant de l'introduire dans la base de données intermédiaire.

Un champ de contrôle (IDX) est utilisé pour s'assurer du bon déroulement de l'opération de synchronisation entre la base électorale 2014 et la base intermédiaire SandBox et notamment pour assurer la migration seulement des électeurs éligibles vers la base électorale 2014.

Observations :

1. L'ISIE n'a pas développé une procédure formalisée de collecte et de mise à jour des données définissant le QUI (intervenants), le QUOI (tâches, activités et contrôles), le COMMENT (instruction spécifique ou mode opératoire) et le QUAND (enchainement des tâches et activités).
2. L'ISIE n'a pas développé une procédure formalisée de gestion des incidents et des problèmes de collecte et mise à jour des données. Les incidents et les problèmes ne sont pas répertoriés.

4.3.2 Résultats de la vérification de la procédure de traitement des doublons dans le registre électoral

Les doublons identifiés et traités sont définis comme suit :

- Les doublons résultant des inscriptions par CIN et par Passeport, dans ce cas l'identification des doublons revient faire le groupement : cin_passport = le numéro de la carte d'identité nationale et même date de naissance.
- Les doublons résultant des inscriptions par un ancien et un nouveau passeport, dans ce cas l'identification du doublon revient faire le groupement : cin_passport = le numéro de la carte d'identité nationale qui correspond au ancien passeport et même date de naissance.

L'examen porté sur des échantillons de tailles optimales et représentatives de la base électorale 2014 n'a pas résulté à la détection de doublons.

4.3.3 Résultats de la vérification des procédures de publication des listes électorales et examen croisé du registre et des listes électorales

La tâche d'impression des listes électorales a été confiée au CNI dans le cadre d'une convention avec l'ISIE.

Le CNI a procédé à :

- L'élaboration des différents modèles des listes électorales à éditer sur la base du registre électoral 2014.
- Aménagement des deux salles réservées à l'édition des listes
- Installation, configuration et test de l'environnement d'édition (postes de travail et imprimantes)
- Participation aux contrôles et à l'analyse de la base de données électorale et au développement des scripts nécessaires
- Développement des modules d'édition des listes électorales et des états annexes

- Génération et contrôle des différentes listes à éditer et des listes à publier sur le site WEB de l'ISIE
- Conduite et suivi de la chaine d'édition des différentes listes électorales :
    - Impression des listes
    - Découpage des listes en volumes
    - Vérification des états édités
    - Façonnage
    - Contrôle, validation et livraison à l'ISIE des listes électorales.

L'examen croisé du registre électoral et des listes électorales publiées s'est porté sur un échantillon de taille optimale et représentative de la population mère. La population mère définie représente l'ensemble des bureaux de vote.

La méthode d'échantillonnage probabiliste choisie est le sondage aléatoire simple avec une marge d'erreur de plus ou moins 5%.

L'échantillon choisi comprend 372 bureaux de vote local et 195 bureaux de vote étranger.

Cet examen croisé du registre électoral et des listes électorales n'a pas identifié d'écarts**.**

4.3.4 Résultats de l'Audit de Conformité ISO 27002:2013

Synthèse des principaux Constats d'Audit:

✓ Il n'existe pas un Document de politique de sécurité SI-ISIE englobant les principes fondamentaux de la sécurité du SI et les règles d'administration & procédures opérationnelles spécifiques pour la sécurisation de la plateforme support du registre électoral 2014

✓ Il n'existe pas une définition d'une organisation de la sécurité du SI-ISIE : inexistence d'un comité de sécurité, inexistence d'une nomination formelle d'un RSSI + inexistence d'une définition formelle des responsabilités/attributions en matière de la Sécurité SI

✓ Il existe une description des composants de l'infrastructure matérielle (sous forme d'une liste des composants serveurs physiques + virtuelles) ainsi que les versions logicielles déployées au niveau de la plateforme support du registre électoral 2014

✓ Inexistence d'un document formel d'Appréciation des Risques IT de la plateforme support du registre électoral 2014

✓ Existence d'une Architecture Réseau & Sécurité de la plateforme d'inscription des électeurs --> Architecture modulaire formé par un système de filtrage frontal et interne : Protection du périmètre externe/WAN de la plateforme d'inscription qu'est accessible aux public via Internet (en couplage avec un système WAF "Barracuda") ainsi que Protection et filtrage d'accès aux ressources Serveurs interne de la plateforme d'inscription électorale (Firewalls du Module Hébergement + Firewalls du Module Infra)

✓ Filtrage et restriction d'accès aux données de nature confidentielle (2 Personnes uniquement ayant les comptes et les privilèges d'accès en mode super-utilisateur / Administrateur aux serveurs supports des données de nature confidentielles)

✓ Il y a eu un déploiement d'une solution antivirale réseau (Agents pour Serveurs et pour postes de travail) de type Symantec Endpoint Protection 12.1.4 [Il y a eu en outre une application de plusieurs type de politiques de sécurité au niveau de la solution afin d'assurer une protection des

stations contre les différents type d'attaques par malwares/code malveillants et/ou protection contre les risques liés à l'usage des supports amovibles]

✓ Réalisation des opérations de périodique de sauvegarde des données sous Postgresql (Base de données électorale) [opération planifiée d'une manière journalière via des scripts semi-automatiques] : copie en format DUMP de la Base vers un Serveur de sauvegarde puis externalisation sur des supports amovibles

✓ Les opérations de sauvegarde ne s'articule pas sur une politique formelle définissant le type et les méthodes de réalisation des opérations de sauvegarde, la périodicité, les supports de stockage, leur protection ainsi que la planification des tests de restauration

✓ Les copies de sauvegardes de données sont stockées en locale sur un Serveur backup ainsi que sur des supports externes (Disques externes) et qui sont par la suite transfères aux locaux du Site Siège de l'ISIE sous la responsabilité de l'Administrateur sécurité opérationnelle et l'Administrateur Système

✓ Les dossiers applicatifs, code sources et les fichiers de configurations des serveurs WEB, d'applications, fichiers de configuration des équipements réseau & sécurité et le fichier de configuration du noyau base de données (Postgresql) ont été sauvegardées (d'une manière manuelle) et aussi à chaque modification effectuée de type mise à jour de version, amélioration et renforcement de la sécurité des configurations ou corrections appliquées sur le code

✓ Un full Backup est effectuée pour l'ensemble des composants de la plateforme d'exploitation du registre électorale (selon une périodicité aléatoire)

✓ Un seul test de restauration a été effectué (sans être documenté)

✓ Inexistence d'une procédure de gestion de vulnérabilité technique permettant de vérifier que les configurations et le paramétrage des systèmes, réseaux, bases de données et applicatifs sont conformes aux stratégies de sécurité de l'ISIE par un audit technique interne qui pourra mettre en évidence une inadéquation entre l'objectif de sécurité et les moyens mis en œuvre (tests de vulnérabilités+tests de conformité technique) --> réalisation uniquement d'Audit de Sécurité et performances de la base de données électorale de l'ISIE + Tests de vulnérabilités et tests intrusifs de la plateforme d'inscription électorale par un Bureau externe - Mai/Juin 2014

✓ Il y a eu une mise en place d'une solution de collecte des journaux de logs de la base de données électorale sous Postgresql via l'outil open source de type OSSIM (Solution exploitée d'une manière manuelle/semi-automatique en cas d'un incident) + une solution d'administration et supervision de l'activité des équipements Réseaux et Serveurs via des outils open source tel que NAGIOS

✓ Il n'existe pas un outil de gestion & de corrélation des journaux de logs systèmes, réseaux, applicatifs et base de données pour l'environnement d'exploitation du registre électoral 2014 + inexistence des procédures d'analyse techniques des journaux de logs des systèmes Linux, de la base de données Postgresql et les journaux logs des équipements réseau & sécurité

✓ Il n'existe pas une procédure de gestion de changement ou une exigence de sécurité pour la gestion de changement/modification qui sera apportés sur les actifs de la plateforme d'exploitation du registre électoral 2014

✓ Il existe des mesures d'assurance de la continuité d'activité pour la plateforme support du registre électorale (redondance physique des actifs de type technique, mise en place d'une infrastructure virtuelle des serveurs de données et d'application, réalisation des opérations de sauvegarde périodique des données et images systèmes, secours des liaisons réseau WAN) + Existence des contrats de maintenance pour les actifs de type technique

✓ Il n'existe pas une organisation interne pour la continuité d'activité + un Document formel PCA « Plan de continuité d'activité pour la plateforme support du registre électoral 2014" + Inexistence d'une Plateforme de secours dans un site éloigné du Site d'hébergement au CNI.

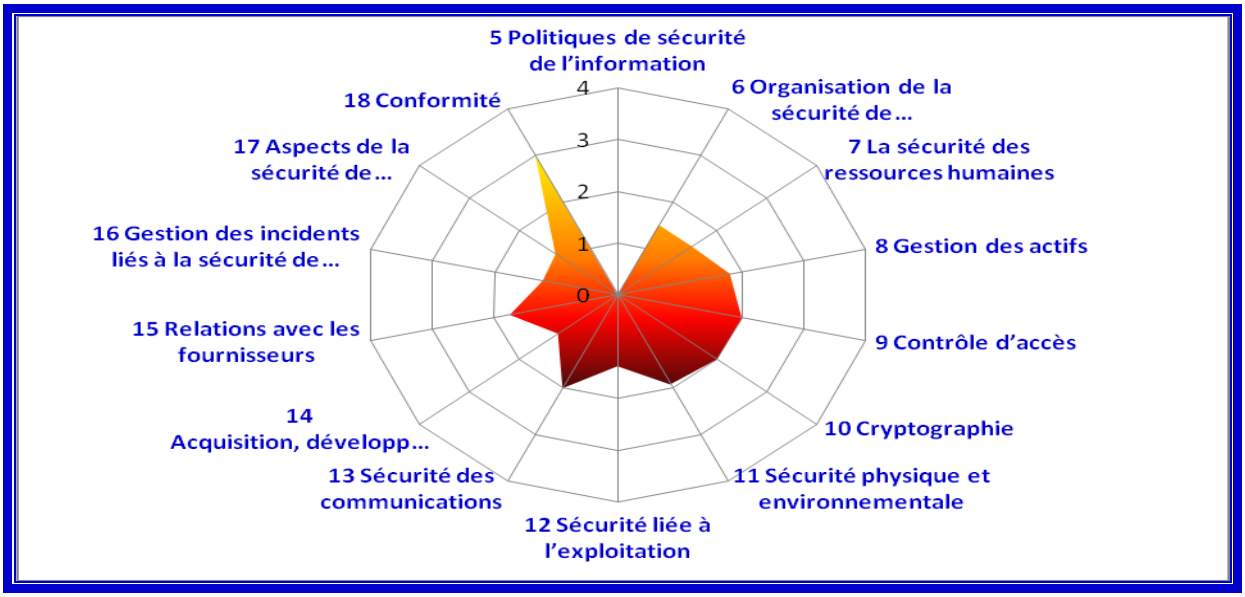
Synthèse de l'évaluation du niveau de la sécurité du Registre Electoral 2014 en conformité aux bonnes pratiques (Norme ISO 27002:2013)

Note Globale 1,56 et un pourcentage de conformité de 38,9%

Politiques de sécurité de l'information	0,00
Organisation de la sécurité de l'information	1,50
La sécurité des ressources humaines	1,50
Gestion des actifs	1,82
Contrôle d'accès	2,01
Cryptographie	2,00
Sécurité physique et environnementale	1,92
Sécurité liée à l'exploitation	1,38
Sécurité des communications	2,00
Acquisition, développement et maintenance des systèmes d'information	1,20
Relations avec les fournisseurs	1,74
Gestion des incidents liés à la sécurité de l'information	1,21
Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	1,25
Conformité	3,00
Note Globale	1,56
Poucentage %	38,90

Le niveau de sécurité actuel du périmètre audité, qu'est a été évalué par rapport aux exigences de la norme ISO 27002 : 2013 devra être renforcé par des mesures de sécurité à appliquer en urgence sur les plans organisationnels, physiques, procédurales et techniques (voir Plan d'action dans le Rapport de Synthèse).

Rosace de niveau de conformité ISO 27002:2013



Nous constatons que le seuil de maturité (valeur 3) n'est pas atteint par la plupart des objectifs des différents chapitres du référentiel de sécurité (**la Norme ISO 27002,** version 2013), par conséquent l'état actuel de la sécurité du Registre électoral présente des points des vulnérabilités au niveau organisationnel ,physique, procédurales et techniques dont il faut appliquer les actions correctives adéquates.

5- Plan d'action pour le Management et la maîtrise des Risques

Synthèse globale des importantes mesures organisationnelles, procédurales, physiques et techniques préconisés dans l'immédiat et sur le moyen terme (Plan d'action pour le Management des Risques)

Synthèse : Plan d'action

Actions d'ordre organisationnel, Procédurale, physique et Techniques à planifier la réalisation dans l'immédiat & à court terme (4ème Trimestre 2015 / Début 2016)

Cette section du plan d'action englobe les actions correctives à appliquer (dans l'immédiat et à court terme) sous forme d'identification des mesures de sécurité permettant de réduire les risques à un niveau acceptable.

Réf.Action	Actions à entreprendre	Budget (Coût de réalisation)	Chargé de l'action (Charge interne + Charge assistance / prestation externe	Priorité de l'action / Date de mise en œuvre
Partie Architecture matérielle, logicielle & Performances				
1	Revoir le choix du noyau SGBD Postgresql comme support de données du registre électoral (vue que les tests/benchmarks ont montré qu'il n'est pas un choix optimal pour les applications ISIE). Dans la configuration existante (en cas de continuation avec la même plateforme --> Allocation recommandée de toute une machine physique pour la Machine virtuelle base de données). Avoir des licences d'utilisation du nouveau SGBD en cas d'une refonte et assurer le transfert de compétences pour les Administrateurs de Bases de données coté ISIE.	En interne + Prestation de service d'étude + Budget d'acquisition de nouveaux composants (Hard+soft) + Acquisition des licences d'utilisation valide et contrats support/maintenance **[Budget A étudier]**	**Comité de Sécurité SI-ISIE (à créer) + RSSI + Bureau d'étude (dimensionnement de l'infrastructure virtuelle) + Intégrateurs des solutions + Intégrateur Base de données**	**Très Urgent** 4ème Trimestre 2015
2	Amélioration des performances de l'architecture système et réseau existante : Ajout au moins d'une autre machine physique dans le Blade (Infra) des Serveurs de données et d'applications & d'augmenter la bande passante réseau (ceci selon une étude de dimensionnement système/réseau et de mise en place d'une nouvelle infrastructure virtuelle). Application des mesures de Tunning coté application (JSF) /OS(Redhat) /GlassFish (tel qu'a été décrit dans le Rapport des tests de performances) en cas de continuation avec la même plateforme. Remarque : Utilisation des environnements WEB/Applicatif optimums, justifiés selon le choix du noyau SGBD en cas d'une refonte de la plateforme support de données du	En interne + Prestation de service d'étude de l'infrastructure virtuelle + Budget d'acquisition de nouveaux composants (Hard+soft) **[Budget A étudier]**	**Comité de Sécurité SI-ISIE (à créer) + RSSI + Intégrateurs Systèmes / Applicatifs / Base de données**	**Très Urgent** 4ème Trimestre 2015

	registre électorale (Avec l'Action 1)			
Partie Sécurité Organisationnelle / Procédurale / Technique				
3	➢ Elaboration d'un Manuel de Politique de Sécurité du SI-ISIE englobant la Politique générale, les exigences liées à l'organisation de la sécurité ainsi que la définition des procédures opérationnelles de la sécurité de la plateforme d'inscription des électeurs : procédures de contrôle d'accès physique, les procédures techniques (procédure de contrôle d'accès réseau / Matrice des flux, Politique d'autorisation applicative, procédure de gestion de vulnérabilités technique, procédure de gestion d'incidents de nature logique, procédure de gestion des journaux logs,etc..] . Ce document doit être signé et approuvé par le comité à créer	En interne + Prestation de service (Experts en Sécurité) 10 000 DT	**Comité de Sécurité SI-ISIE (à créer) + RSSI + Bureau d'Audit & Conseil**	**Très Urgent** 4ème Trimestre 2015
4	➢ Elaboration d'une une procédure formelle d'importation du registre électoral 2011 et une procédure de collecte et de mise à jour des données définissant le QUI (intervenants), le QUOI (tâches, activités et contrôles), le COMMENT (instruction spécifique ou mode opératoire) et le QUAND (enchainement des tâches et activités) + une procédure formelle de gestion des incidents et des problèmes de collecte et mise à jour des données.	Avec l'action N°3	**Comité de Sécurité SI-ISIE (à créer) + RSSI + Bureau d'Audit & Conseil**	**Très Urgent** 4ème Trimestre 2015
5	➢ Création d'un Comité de Sécurité SI-ISIE + Nomination Formelle d'un RSSI ➢ Définition des attributions et les responsabilités en matière de la Sécurité de la plateforme d'inscription des électeurs au niveau du nouveau document de la PSSI-ISIE à élaborer → Avoir les fiches fonctions type RSSI, Administrateur Sécurité Système, Sécurité base de données, Sécurité Réseau , Sécurité opérationnelle et Sécurité applicative ➢ Renforcer la composante ressource humaine en matière de la sécurité SI-ISIE par le recrutement d'un Profil « Administrateur Sécurité opérationnelle "	En interne + Assistance Post-Audit + Budget alloué pour le recrutement "Fonction Administrateur Sec. Opérationnelle"	**Comité de Sécurité SI-ISIE (à créer) + RSSI + Bureau d'Audit & Conseil**	**Très Urgent** 4ème Trimestre 2015

6	➢ Réalisation d'une mission d'appréciation des Risques IT de la plateforme d'inscription des électeurs englobant les phases d'élaboration d'inventaire & Classification des actifs, d'étude d'impact haut niveau / bas niveau ainsi qu'un Plan de traitement des Risques en s'appuyant sur les méthodologies et/ou approches inspirées de la norme ISO 27005	En interne + Prestation de service (Experts en Sécurité) 10 000 DT	**Comité de Sécurité SI-ISIE (à créer) + RSSI + Bureau d'Audit & Conseil**	**Très Urgent** 4ème Trimestre 2015
7	➢ Avoir une documentation formelle de l'Architecture Réseau & Sécurité englobant outre le schéma de l'existant, la politique de filtrage implantée autour de la plateforme d'inscription des électeurs sous forme des matrices de contrôle des flux réseau LAN/WAN	Avec l'Action 3	**Comité de Sécurité SI-ISIE (à créer) + RSSI + Bureau d'Audit & Conseil**	**Très Urgent** 4ème Trimestre 2015
8	➢ Avoir une documentation formelle de l'Architecture Système et applicative déployée permettant ainsi d'avoir les interactions entre les différents couches applicatifs de la plateforme d'inscription électorale et de définir l'infrastructure d'exécution des modules applicatifs	Avec l'Action 3	**Comité de Sécurité SI-ISIE (à créer) + RSSI + Bureau d'Audit & Conseil**	**Très Urgent** 4ème Trimestre 2015
9	➢ Avoir une procédure de gestion de changement ou une exigence de sécurité pour la gestion de changement/modification qui seront apportés sur les actifs la plateforme de l'inscription électorale	Avec l'Action 3	**Comité de Sécurité SI-ISIE (à créer) + RSSI + Bureau d'Audit & Conseil**	**Très Urgent** 4ème Trimestre 2015
10	➢ Elaboration d'une procédure de gestion d'incidents + procéder à l'implémentation des mesures de gestion d'incidents et collecte des éléments de preuve, traçabilité permettant d'identifier les origines des incidents + Elaboration d'une procédure formelle de signalement des failles de sécurité, ainsi qu'une procédure de remontée d'informations et de réponse en cas de détection d'un incident lié à une attaque logique (gestion des incidents de nature logique / attaques expertes)	Avec l'Action 3	**Comité de Sécurité SI-ISIE (à créer) + RSSI + Bureau d'Audit & Conseil**	**Très Urgent** 4ème Trimestre 2015
11	➢ Acquisition d'un Système d'Analyse & Corrélation des journaux permettant la consolidation et la corrélation des journaux de log système, applicatifs, réseau et base de données : Renforcement et d'amélioration de la traçabilité ainsi que la gestion sophistiquée des incidents de sécurité	60 000 DT	**Comité de Sécurité SI-ISIE (à créer) + RSSI + Administrateurs Techniques de l'ISIE + intégrateur de la solution d'analyse et corrélation des logs**	**Urgent** Début 2016

	➢ Elaboration d'une politique de sauvegarde de l'environnement d'exploitation du registre électorale décrivant l'opération, responsabilité, vérification périodique des supports de sauvegarde, réalisation des opérations de test de recours et de test d'exploitation ainsi que la définition des cycles de conservation des sauvegardes, détermination de la période de conservation et les exigences de sécurité des copies d'archive ➢ Acquisition d'une armoire anti-feu pour la protection en local des supports de sauvegarde des données de la plateforme	Avec l'Action 3 + Budget d'acquisition d'une armoire anti-feu (10 000 DT)	**Comité de Sécurité SI-ISIE (à créer) + RSSI + Bureau d'Audit & Conseil + Intégrateur de la solution de sauvegarde**	**Très Urgent** 4ème Trimestre 2015
12	➢ Création d'un comité PCA qu'aura pour mission la mise en place d'une stratégie de continuité d'activité pour la plateforme support du registre électorale et le suivi d'élaboration et mise en place du processus de gestion de continuité d'activité pour (dès la planification, cahier des charges, élaboration et l'implémentation du manuel PCA et la réalisation des tests PCA) ➢ Avoir une plateforme de secours de l'environnement d'exploitation du registre électorale dans un site éloigné	40 000 DT	**Comité de Sécurité SI-ISIE (à créer) + Comité PCA (à créer) + RSSI + Bureau d'Audit & Conseil [Mission d'élaboration d'un PCA pour l'ISIE]**	**Très Urgent** 4ème Trimestre 2015
13	Elaboration d'une procédure permettant de définir des actions de gestion des vulnérabilités techniques et qui sera implémentée via l'acquisition et la mise en place d'un système d'Audit & Scan	Avec l'Action 3 + Budget d'acquisition d'un Système d'Audit & Scan} (20 000 DT)	**Comité de Sécurité SI-ISIE (à créer) + Administrateurs Techniques de l'ISIE + Intégrateur de la Solution d'Audit & Scan**	**Urgent** Début 2016