COUR DES COMPTES

RAPPORT N°95

DÉCEMBRE 2015

AUDIT DE GESTION

SÉCURITÉ DES SMARTPHONES

ÉTAT DE GENÈVE

Le contenu du présent rapport public
tient compte des intérêts publics et privés en jeu
en application de l'art. 43 al. 4 LSurv.

COUR DES COMPTES
RÉPUBLIQUE ET CANTON DE GENÈVE

LA COUR DES COMPTES

La Cour des comptes est chargée du contrôle indépendant et autonome des services et départements de l'administration cantonale, du pouvoir judiciaire, des institutions cantonales de droit public, des organismes subventionnés ainsi que des institutions communales. Elle a également pour tâche l'évaluation des politiques publiques.

La Cour des comptes vérifie d'office et selon son libre choix la **légalité** des activités et la **régularité** des recettes et des dépenses décrites dans les comptes, et s'assure du **bon emploi** des crédits, fonds et valeurs gérés par les entités visées par ses missions. La **Cour des comptes** peut également évaluer la **pertinence**, **l'efficacité** et **l'efficience** de l'action de l'État. Elle organise librement son travail et dispose de larges moyens d'investigation. Elle peut notamment requérir la production de documents, procéder à des auditions, à des expertises, se rendre dans les locaux des entités concernées.

Le champ d'application des missions de la Cour des comptes s'étend aux entités suivantes:

- L'administration cantonale comprenant les départements, la chancellerie d'État et leurs services ainsi que les organismes qui leur sont rattachés ou placés sous leur surveillance ;
- Les institutions cantonales de droit public ;
- Les entités subventionnées ;
- Les entités de droit public ou privé dans lesquelles l'État possède une participation majoritaire, à l'exception des entités cotées en bourse ;
- Le secrétariat général du Grand Conseil ;
- L'administration du pouvoir judiciaire ;
- Les autorités communales, les services et les institutions qui en dépendent, ainsi que les entités intercommunales.

Les rapports de la Cour des comptes sont rendus **publics:** ils consignent ses observations, les conclusions de ses investigations, les enseignements qu'il faut en tirer et les recommandations conséquentes. La Cour des comptes prévoit en outre de signaler dans ses rapports les cas de réticence et les refus de collaborer survenus au cours de ses missions.

La Cour des comptes publie également un **rapport annuel** comportant la liste des objets traités, celle de ceux qu'elle a écartés, celle des rapports rendus avec leurs conclusions et recommandations et les suites qui y ont été données. Les rapports restés sans effet ni suite sont également signalés.

Vous pouvez participer à l'amélioration de la gestion de l'État en prenant contact avec la Cour des comptes.
Toute personne, de même que les entités comprises dans son périmètre d'action, peuvent communiquer à la Cour des comptes des faits ou des pratiques qui pourraient être utiles à l'accomplissement des tâches de cette autorité.

Prenez contact avec la Cour par téléphone, courrier postal, fax ou courrier électronique.

Cour des comptes — Route de Chêne 54 — 1208 Genève
tél. 022 388 77 90 — fax 022 388 77 99
http://www.cdc-ge.ch/

SYNTHÈSE PUBLIQUE

Au cours des dix dernières années, l'utilisation des smartphones s'est largement répandue dans le cadre professionnel. Or, ces équipements mobiles sont particulièrement sensibles d'une part au risque de perte ou de vol en raison de leur faible taille et faible poids, et d'autre part au risque de virus, de maliciel (« malware »), d'espionnage du trafic internet en raison de leur facilité d'utilisation et de leur capacité technologique étendue avec un niveau de sécurité souvent problématique.

En cas de survenance de ces risques, un tiers pourrait avoir accès aux informations confidentielles suivantes :

- Documents professionnels ou personnels (par exemple : notes, courriels, calendrier, liste des contacts) ;
- Identifiants des comptes présents sur le smartphone tels que la messagerie ou les réseaux sociaux ;
- Applications qui enregistrent des informations personnelles ;
- Données de géolocalisation ;
- Paramètres du téléphone, permettant par exemple de créer des « trous sécuritaires» ou d'empêcher d'utiliser certaines fonctionnalités.

Il appartient à la Cour de s'assurer notamment de l'efficacité, de l'efficience et de la qualité de l'action publique dans le respect des principes de la performance publique (art. 38 al. 1 LSurv).

Plusieurs informations confidentielles en mains de magistrats ou collaborateurs de l'État étant considérées comme cruciales pour la sécurité de l'État (par exemple : opérations de police, transferts de détenus, contacts protocolaires avec la Genève internationale) et par voie de conséquence pour la qualité et l'efficacité de l'action publique, la Cour a choisi, à l'été 2015, d'ouvrir une mission d'audit sur la sécurité des smartphones au sein de l'État de Genève.

Afin de déterminer si la sécurité des smartphones est adaptée au niveau de confidentialité des informations communiquées, la Cour a entrepris une démarche d'audit en deux temps, avec le concours d'un expert externe reconnu dans le domaine de la sécurité informatique :

- Une revue documentaire afin d'apprécier la qualité des règles, normes de sécurité et procédures appliquées par l'État de Genève relativement à l'utilisation et à la gestion des smartphones ;
- Des tests d'intrusion à l'égard de collaborateurs de l'administration gérant des données sensibles.

La méthodologie utilisée par la Cour se base sur :

- Les bonnes pratiques reconnues en matière de sécurité (ISO 27002 *« Code de bonnes pratiques pour le management de la sécurité de l'information »*). Cette norme comprend un ensemble de 133 mesures dites de « bonnes pratiques ». Le chapitre 6.2 de la norme traite plus spécifiquement de la communication par équipements mobiles et prévoit 14 points de contrôles spécifiques ;
- La liste des risques mobiles identifiés par l'agence de l'Union Européenne pour la sécurité des réseaux et de l'information (ENISA - European Union Agency for Network and Information Security). En effet, la norme ISO 27002 n'a pas pour objectif d'identifier et donc de fournir une liste des principaux risques de sécurité liés à l'utilisation des équipements mobiles. Ainsi, pour les besoins de cet audit, l'expert s'est basé sur la liste des 10 risques principaux établie par l'ENISA pour effectuer ses analyses de la conformité de l'État de Genève par rapport aux 14 points de contrôle prévus par la norme ISO.

Les analyses de la Cour l'ont amenée à adresser, au département de la sécurité et de l'économie, six recommandations conclusives à mettre en œuvre de manière coordonnée, étant précisé que ces dernières n'impliquent pas nécessairement des charges supplémentaires. Le département a accepté toutes les recommandations de la Cour, qu''il s'est engagé à mettre en œuvre dans les meilleurs délais.

Comme le veut la pratique en matière de sécurité informatique et conformément à l'art. 43 al. 4 LSurv[1], la Cour a choisi de ne pas rendre public le présent rapport, hormis cette synthèse, la table des matières, quelques rubriques du tableau de suivi des recommandations et le chapitre Divers. Un seul exemplaire du rapport complet a été remis par la Cour au conseiller d'État en charge du DSE.

[1] La Cour *« détermine l'étendue des informations contenues dans ses rapports en tenant compte des intérêts publics et privés susceptibles de s'opposer à la divulgation de certaines informations. »*

TABLE DES MATIÈRES

1. CADRE ET CONTEXTE

2. MODALITÉS ET DÉROULEMENT

3. CONTEXTE GÉNÉRAL

3.1. Sécurité des smartphones

3.1.1. Introduction

3.1.2. Norme ISO/IEC 27002

3.1.3. Risques identifiés par l'agence de l'Union Européenne pour la sécurité des réseaux et de l'information (ENISA)

3.1.4. La gestion de la sécurité à l'État de Genève

3.1.5. Utilisation du smartphone à l'État de Genève

4. ANALYSE : REVUE DOCUMENTAIRE

4.1. Enregistrement des smartphones

4.1.1. Contexte

4.1.2. Constats

4.2. Protection physique des smartphones

4.2.1. Contexte

4.2.2. Constats

4.3. Limitation des installations de logiciels sur les smartphones

4.3.1. Contexte

4.3.2. Constats

4.4. Gestion des versions du système d'exploitation et des mises à jour de sécurité

4.4.1. Contexte

4.4.2. Constats

4.5. Contrôle d'accès des smartphones

4.5.1. Contexte

4.5.2. Constats

4.6. Utilisation de techniques cryptographiques de protection

4.6.1. Contexte

4.6.2. Constats

4.7. Protection contre les maliciels

4.7.1. Contexte

4.7.2. Constats

4.8. Désactivation, effacement et blocage à distance

4.8.1. Contexte

4.8.2. Constats

4.9. Sauvegardes des données du smartphone

4.9.1. Contexte

4.9.2. Constats

4.10. Formation du personnel aux risques spécifiques des smartphones

4.10.1. Contexte

4.10.2. Constats

4.11. Séparation des données privées et professionnelles

4.11.1. Contexte

4.11.2. Constats

4.12. Document spécifique concernant l'utilisation d'un smartphone privé à des fins professionnelles

4.12.1. Contexte

4.12.2. Constats

5. ANALYSE : TESTS TECHNIQUES

5.1. Contexte

5.1.1. Introduction

5.2. Constats

6. CONCLUSION

6.1. Faits marquants de l'audit

6.2. Risques conclusifs

6.3. Recommandations conclusives

6.4. Observations de l'audité

7. TABLEAU DE SUIVI DES RECOMMANDATIONS ET ACTIONS

Réf.	Recommandation/Action	Mise en place (selon indications de l'audité)			
		Risque 4 = Majeur 3 = Significatif 2 = Modéré 1 = Mineur	**Responsable**	**Délai au**	**Fait le**
6	Recommandation n°1	2	DGSI	Juin 2016	
6	Recommandation n°2	3	DGSI	Fin 2017	
6	Recommandation n°3	2	DGSI	Juin 2016	
6	Recommandation n°4	3	DGSI	Fin 2017	
6	Recommandation n°5	3	DGSI	Fin 2017	
6	Recommandation n°6	3	DGSI	Juin 2016	

8. DIVERS

8.1. Glossaire des risques

Afin de définir une **typologie des risques pertinente aux institutions et entreprises soumises au contrôle de la Cour des comptes**, celle-ci s'est référée à la littérature économique récente en matière de gestion des risques et de système de contrôle interne, relative tant aux entreprises privées qu'au secteur public. En outre, aux fins de cohésion terminologique pour les entités auditées, la Cour s'est également inspirée du « Manuel du contrôle interne, partie I » de l'État de Genève (version du 13 décembre 2006).

Dans un contexte économique, le **risque** représente la « possibilité qu'un événement survienne et nuise à l'atteinte d'objectifs ». Ainsi, la Cour a identifié trois catégories de risques majeurs, à savoir ceux liés aux objectifs **opérationnels** (1), ceux liés aux objectifs **financiers** (2) et ceux liés aux objectifs de **conformité** (3).

1) Les risques liés aux objectifs opérationnels relèvent de constatations qui touchent à la structure, à l'organisation et au fonctionnement de l'État et de ses services ou entités, et dont les conséquences peuvent avoir une incidence notable sur la qualité des prestations fournies, sur l'activité courante, voire sur la poursuite de son activité.

Exemples :

- engagement de personnel dont les compétences ne sont pas en adéquation avec le cahier des charges ;
- mauvaise rédaction du cahier des charges débouchant sur l'engagement de personnel;
- mesures de protection des données entrantes et sortantes insuffisantes débouchant sur leur utilisation par des personnes non autorisées ;
- mauvaise organisation de la conservation et de l'entretien du parc informatique, absence de contrat de maintenance (pannes), dépendances critiques ;
- accident, pollution, risques environnementaux.

2) Les risques liés aux objectifs financiers relèvent de constatations qui touchent aux flux financiers gérés par l'État et ses services et dont les conséquences peuvent avoir une incidence significative sur les comptes, sur la qualité de l'information financière, sur le patrimoine de l'entité ainsi que sur la collecte des recettes, le volume des charges et des investissements ou le volume et coût de financement.

Exemples :

- insuffisance de couverture d'assurance entrainant un décaissement de l'État en cas de survenance du risque mal couvert ;
- sous-dimensionnement d'un projet, surestimation de sa profitabilité entraînant l'approbation du projet.

3) Les risques liés aux objectifs de conformité (« compliance ») relèvent de constatations qui touchent au non-respect des dispositions légales, réglementaires, statutaires ou tout autre document de référence auquel l'entité est soumise et dont les conséquences peuvent avoir une incidence sur le plan juridique, financier ou opérationnel.

Exemples :

- dépassement de crédit d'investissement sans information aux instances prévues ;
- tenue de comptabilité et présentation des états financiers hors du cadre légal prescrit (comptabilité d'encaissement au lieu de comptabilité d'engagement, non-respect de normes comptables, etc.) ;
- absence de tenue d'un registre des actifs immobilisés ;
- paiement de factures sans les approbations requises, acquisition de matériel sans appliquer les procédures habituelles ;

À ces trois risques majeurs peuvent s'ajouter trois autres risques spécifiques qui sont les risques de **contrôle** (4), de **fraude** (5) et **d'image** (6).

4) Le risque de contrôle relève de constatations qui touchent à une utilisation inadéquate ou à l'absence de procédures et de documents de supervision et de contrôle ainsi que de fixation d'objectifs. Ses conséquences peuvent avoir une incidence sur la réalisation des objectifs opérationnels, financiers et de conformité.

Exemples :

- absence de tableau de bord débouchant sur la consommation des moyens disponibles sans s'en apercevoir ;
- procédures de contrôle interne non appliquées débouchant sur des actions qui n'auraient pas dû être entreprises ;
- absence de décision, d'action, de sanction débouchant sur une paralysie ou des prestations de moindre qualité.

5) Le risque de fraude relève de constatations qui touchent aux vols, aux détournements, aux abus de confiance ou à la corruption. Ses conséquences peuvent avoir une incidence sur la réalisation des objectifs opérationnels, financiers et de conformité.

Exemples :

- organisation mise en place ne permettant pas de détecter le vol d'argent ou de marchandises ;
- création d'emplois fictifs ;
- adjudications arbitraires liées à l'octroi d'avantages ou à des liens d'intérêt ;
- présentation d'informations financières sciemment erronées, par exemple sous-estimer les pertes, surestimer les recettes ou ignorer et ne pas signaler les dépassements de budget, en vue de maintenir ou obtenir des avantages personnels, dont le salaire.

6) Le risque d'image (également connu sous « risque de réputation ») relève de constatations qui touchent à la capacité de l'État et de ses services ou entités à être crédible et à mobiliser des ressources financières, humaines ou sociales. Ses conséquences peuvent avoir une incidence sur la réalisation des objectifs opérationnels, financiers et de conformité.

Exemples :

- absence de contrôle sur les bénéficiaires de prestations de l'État;
- bonne ou mauvaise réputation des acheteurs et impact sur les prix,
- porter à la connaissance du public la mauvaise utilisation de fonds entraînant la possible réduction ou la suppression de subventions et donations.

8.2. Remarques

La Cour remercie l'ensemble des collaborateurs qui lui ont consacré du temps durant cet audit et tout particulièrement le DSE pour sa diligence et sa collaboration particulièrement constructive.

L'audit a été terminé en novembre 2015. Le rapport complet a été transmis au conseiller d'État en charge du DSE le 27 novembre 2015, dont les observations ont été dûment reproduites dans le rapport complet.

Genève, le 18 décembre 2015

Isabelle Terrier	François Paychère	Stanislas Zuin
Présidente	Magistrat titulaire	Magistrat titulaire

9. ANNEXE

Vous pouvez participer à l'amélioration de la gestion de l'État en prenant contact avec la Cour des comptes.

Toute personne, de même que les entités comprises dans son périmètre d'action, peut communiquer à la Cour des comptes des faits ou des pratiques qui pourraient être utiles à l'accomplissement des tâches de cette autorité.

La Cour des comptes garantit l'anonymat des personnes qui lui transmettent des informations, mais n'accepte pas de communication anonyme.

Vous pouvez prendre contact avec la Cour des comptes par téléphone, courrier postal, fax ou courrier électronique.

Cour des comptes — Route de Chêne 54 — 1208 Genève
tél. 022 388 77 90 — fax 022 388 77 99
http://www.cdc-ge.ch

Cour des comptes — Route de Chêne 54 — 1208 Genève
tél. 022 388 77 90 — fax 022 388 77 99
http://www.cdc-ge.ch