AUDIT DES SI ET SÉCURITÉ : NOTIONS DE BASE

PRÉSENTATION

COUR DES COMPTES – 26 AVRIL 2016

© Genève Tourisme

COUR DES COMPTES
RÉPUBLIQUE ET CANTON DE GENÈVE

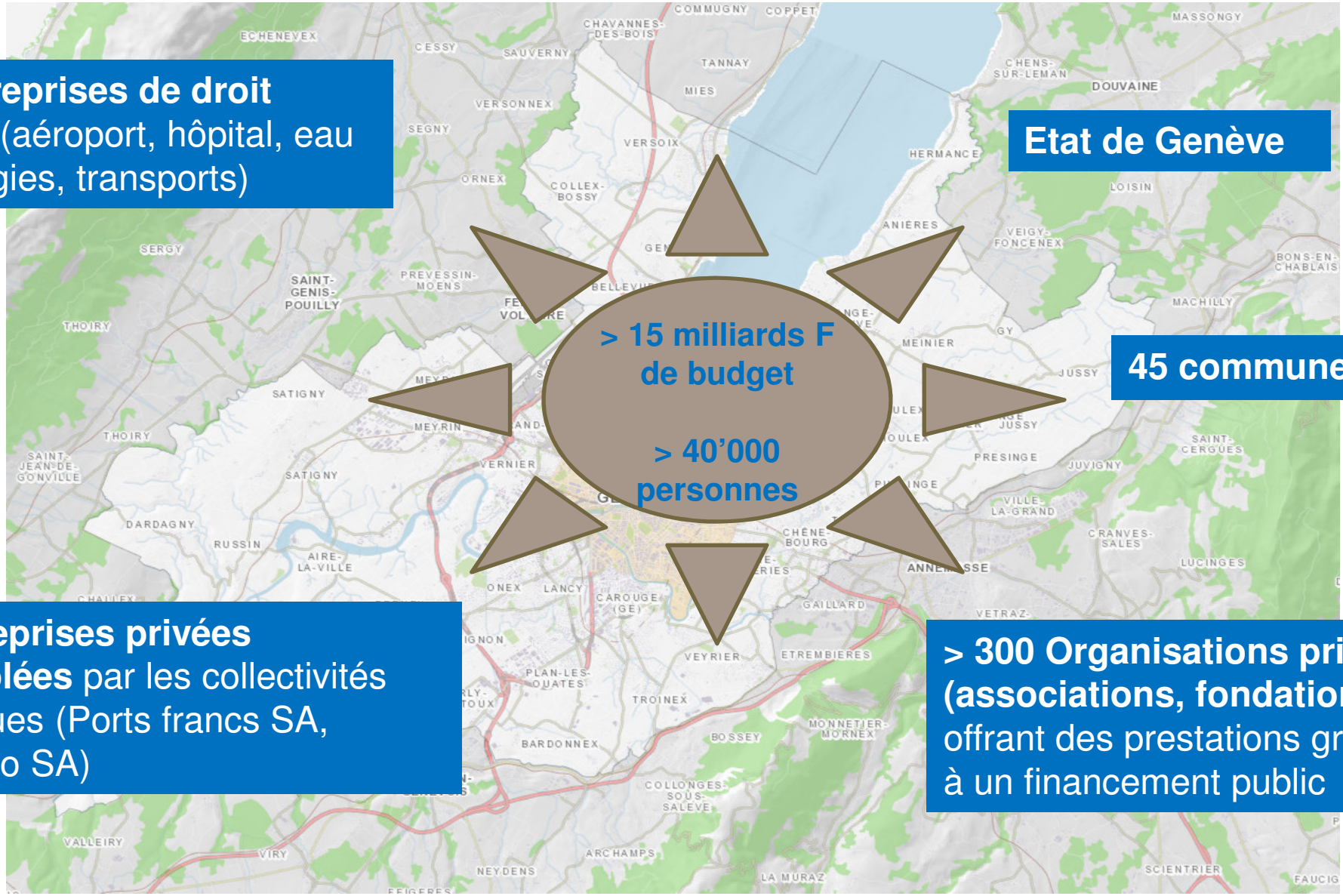
Objectifs de la présentation

- Principales caractéristiques de la Cour des comptes
- Clarification de la notion de «données personnelles»
- Brève présentation de l'audit des SI, des référentiels et du lien avec la protection des «données personnelles»

«Rendre l'administration publique plus efficiente, plus respectueuse du principe de responsabilité, plus efficace et plus transparente en renforçant les institutions supérieures de contrôle des finances publiques.»

ONU, Résolution 66/209 adoptée par l'Assemblée générale le 22 décembre 2011

82 entreprises de droit public (aéroport, hôpital, eau & énergies, transports)



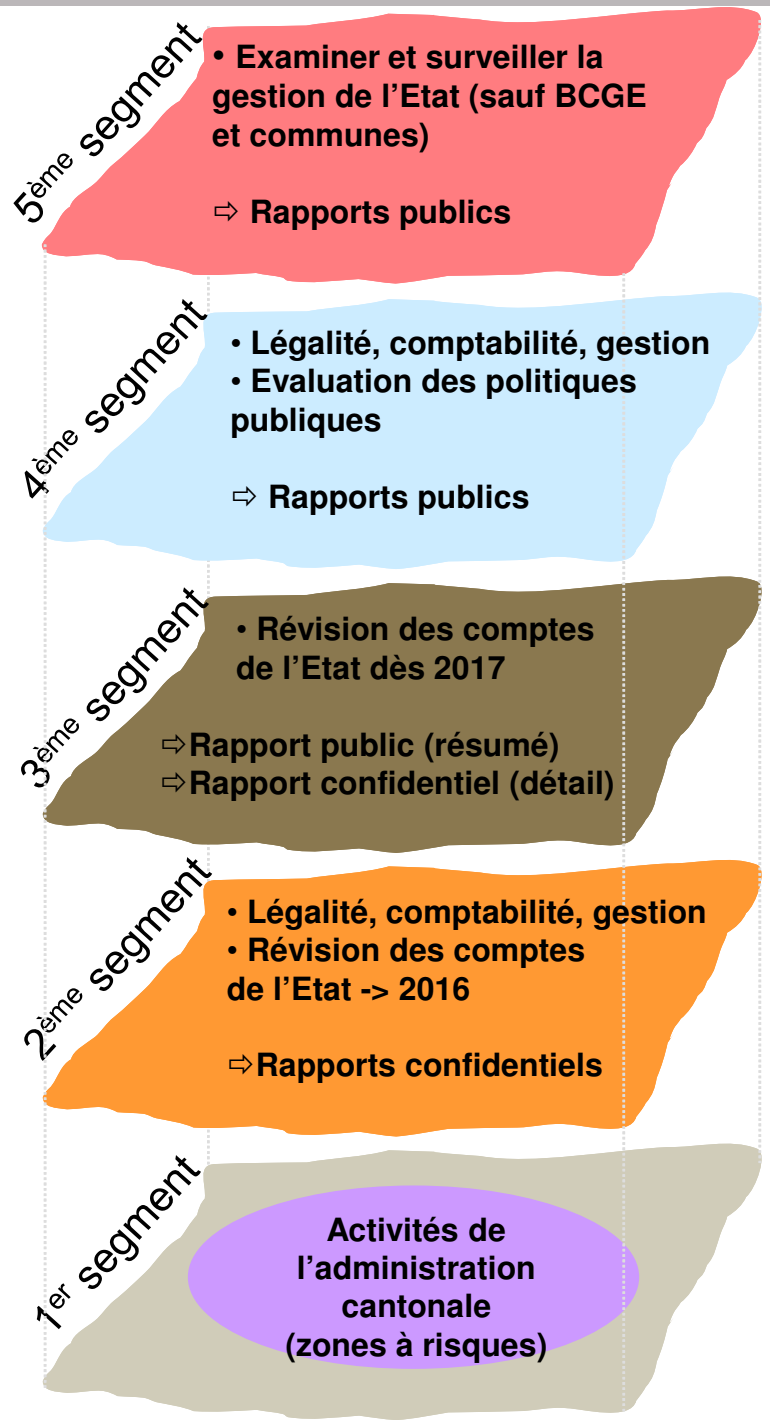
Etat de Genève

45 communes

9 entreprises privées contrôlées par les collectivités publiques (Ports francs SA, Palexpo SA)

> 300 Organisations privées (associations, fondations) offrant des prestations grâce à un financement public

SURVEILLANCE DÈS 2014 – ADMINISTRATION CANTONALE



Commission parlementaire de contrôle de gestion :

- 15 députés au Grand Conseil + 1 secrétaire scientifique + avis d'experts
- Budget annuel : ~ 0.4 millions
- Ne disposant d'aucun pouvoir juridictionnel ni de moyens de contrainte.

Cour des comptes :

- 3 magistrats titulaires à plein temps + 3 suppléants + 15 collaborateurs
- Budget annuel : ~ 4 millions
- Exerce un contrôle indépendant et autonome de l'administration cantonale, des institutions cantonales et communales, des établissements de droit public et des organismes subventionnés.
- Ne disposant d'aucun pouvoir juridictionnel ni de moyens de contrainte.
- Saisie possible par tout citoyen et libre choix de donner suite.
- Recommandations non obligatoires

Cour des comptes (dès les états financiers 2017)

Service d'audit interne (anc. Inspection cantonale des finances) :

- ~ 26 fonctionnaires
- Budget annuel : ~ 5 millions
- Exerce un contrôle indépendant de l'administration cantonale, des institutions cantonales, des établissements de droit public qui n'ont pas d'audit interne et des organismes subventionnés (sauf demande CE).
- Recommandations obligatoires; si divergence: arbitrage du comité d'audit (délégation CE).

Contrôle interne :

- Tous les départements (environ 20 EPT « référents »)
- Budget annuel « petit Etat » : ~ 3 millions

LES LIMITES

- Absence de force contraignante
- Absence de suivi des recommandations rejetées
- Plus de suivi au-delà de trois ans
- Inadéquation du périmètre d'action cantonal au regard d'enjeux inter-cantonaux, voire transfrontaliers

CHIFFRES-CLÉS APRÈS 8 ANS D'ACTIVITÉ (CUMUL - 5 AVRIL 2016)

- Rapports : 103 rapports distincts
- Origine des 103 rapports : 50% autosaisines, 20% citoyens, 30% autorités
- 103 rapports contenant 1'450 recommandations :
  - Acceptées à 98%
  - Mises en œuvre : 70% lors du dernier suivi de la Cour
- Economies proposées: somme de 96.3 millions, dont 23 uniques et 73.3 récurrentes. Valeur potentielle 2007 (avril 2016) : 266.3 millions

QUELQUES PISTES DE RÉFLEXION SUR LES GRANDES ÉVOLUTIONS

- Tendance générale vers une baisse des coûts de traitement et de conservation des données.

- Simultanément, la quantité des informations disponibles ne cesse d'augmenter.

- En outre le développement des «***big data***» ou «mégadonnées».

QUELQUES PISTES DE RÉFLEXION SUR LES GRANDES ÉVOLUTIONS

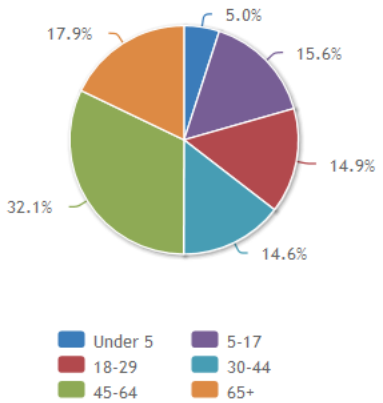
OVERVIEW | NEIGHBORS & DEMOGRAPHICS | REAL ESTATE | PUBLIC SCHOOLS | CRIME RATES | FIND AN AGENT

NEIGHBORS & DEMOGRAPHICS

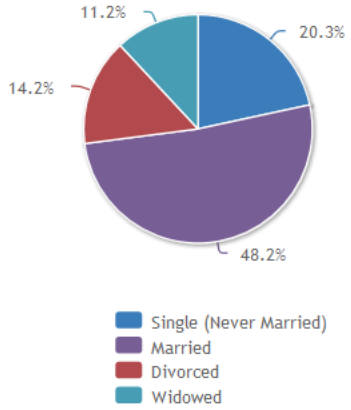
SPECIAL CHARACTER

Hip & Trendy	51.2%
Urban Sophisticates	21.6%
Walkable	1.1%
Quiet	95.0%
Nautical	0.0%

AGES



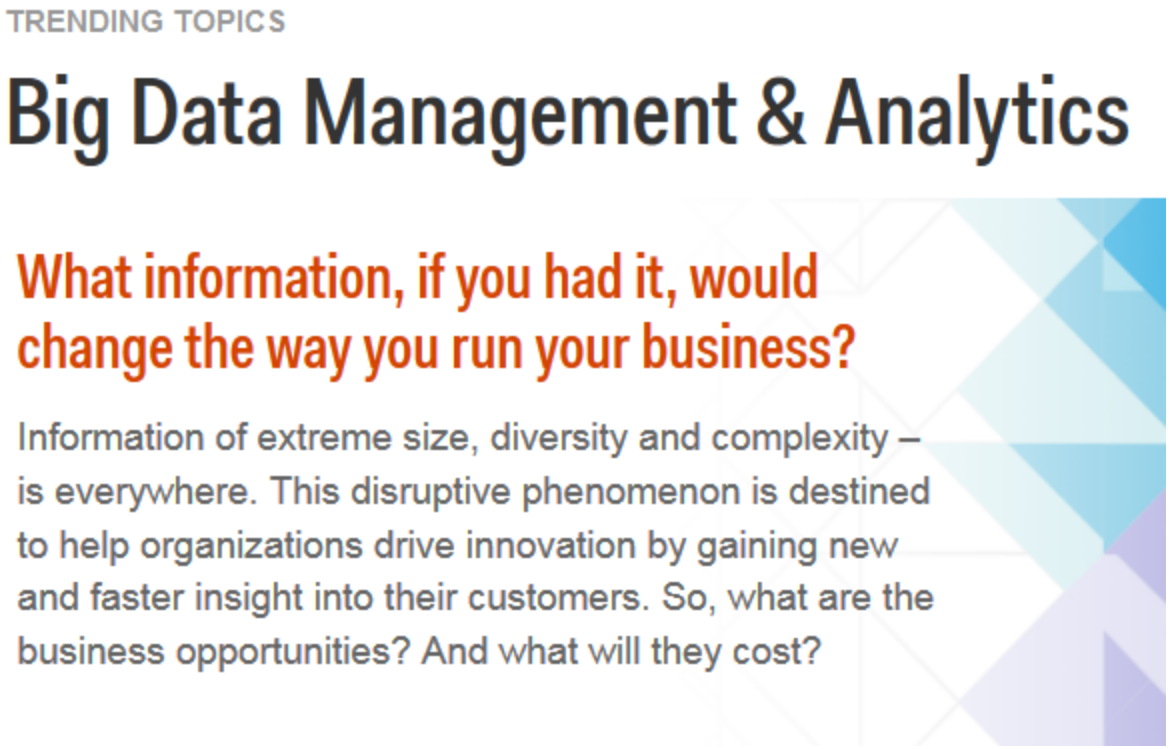
MARITAL STATUS



http://www.neighborhoodscout.com/ca/twenty nine-palms/

QUELQUES PISTES DE RÉFLEXION SUR LES GRANDES ÉVOLUTIONS EXEMPLES RÉCENTS EN SUISSE

- ✓ Il est conseillé aux petites et moyennes entreprises de conserver un maximum de données, même sans savoir à quoi elles pourraient servir (Prof. Kossmann, EPFZ, *NZZ*, 21 avril 2016 p. 27 : "*Laut Kossmann ist es zunehmend attraktiv, Daten zu sammeln, bevor man eigentlich weiss, was man damit machen will*."
- ✓ À l'avenir, il pourrait être profitable d'inciter les clients à de nouveaux achats sur la base d'une analyse de leurs achats antérieurs.
- ✓ Est-il admissible que *Swisscom* vende les données relatives à l'usage du téléphone mobile dans un espace donné (ex. *Bahnhofstrasse*) et qu'elles soient croisées avec des données sur l'âge (ex. trentenaires célibataires) et leur situation économique, qui peuvent être achetées librement ?



http://www.gartner.com/technology/topics/big-data.jsp?utm_source=gcom&utm_medium=interlink&utm_campaign=ITG


PERSONAL
DATA

Le droit suisse distingue les données ***personnelles***, qui se rapportent à une personne (physique ou morale) identifiée ou identifiable des données ***sensibles***, qui sont les données personnelles quant aux opinions, à la santé, la sphère intime et du ***profil de la personnalité***, qui est un assemblage de toutes ces données, concernant une personne physique.

Art. 3 de la loi fédérale sur la protection des données du 19 juin 1992 (LPD – RS 235.1) – Quelques exemples tirés de la jurisprudence du Tribunal fédéral : ATF 138 II 346, 137 I 167, 136 II 508.

Le droit genevois a repris les mêmes notions que le droit fédéral : données personnelles, données sensibles et profil de la personnalité.

Art. 4 de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles du 5 octobre 2001 (LIPAD - A 2 08)

Les questions qui s'imposent sont de deux ordres :

a. Quelles sont les réponses des juristes pour interpréter une notion comme celle de «personne identifiable» ?

b. Ces réponses sont-elles pertinentes au regard des évolutions techniques ?

Un exemple tiré de la jurisprudence de la Chambre administrative de la Cour de justice (Genève) : ATA/528/2012 du 21 août 2012.

Comment résoudre les difficultés liées à la détention de données personnelles.

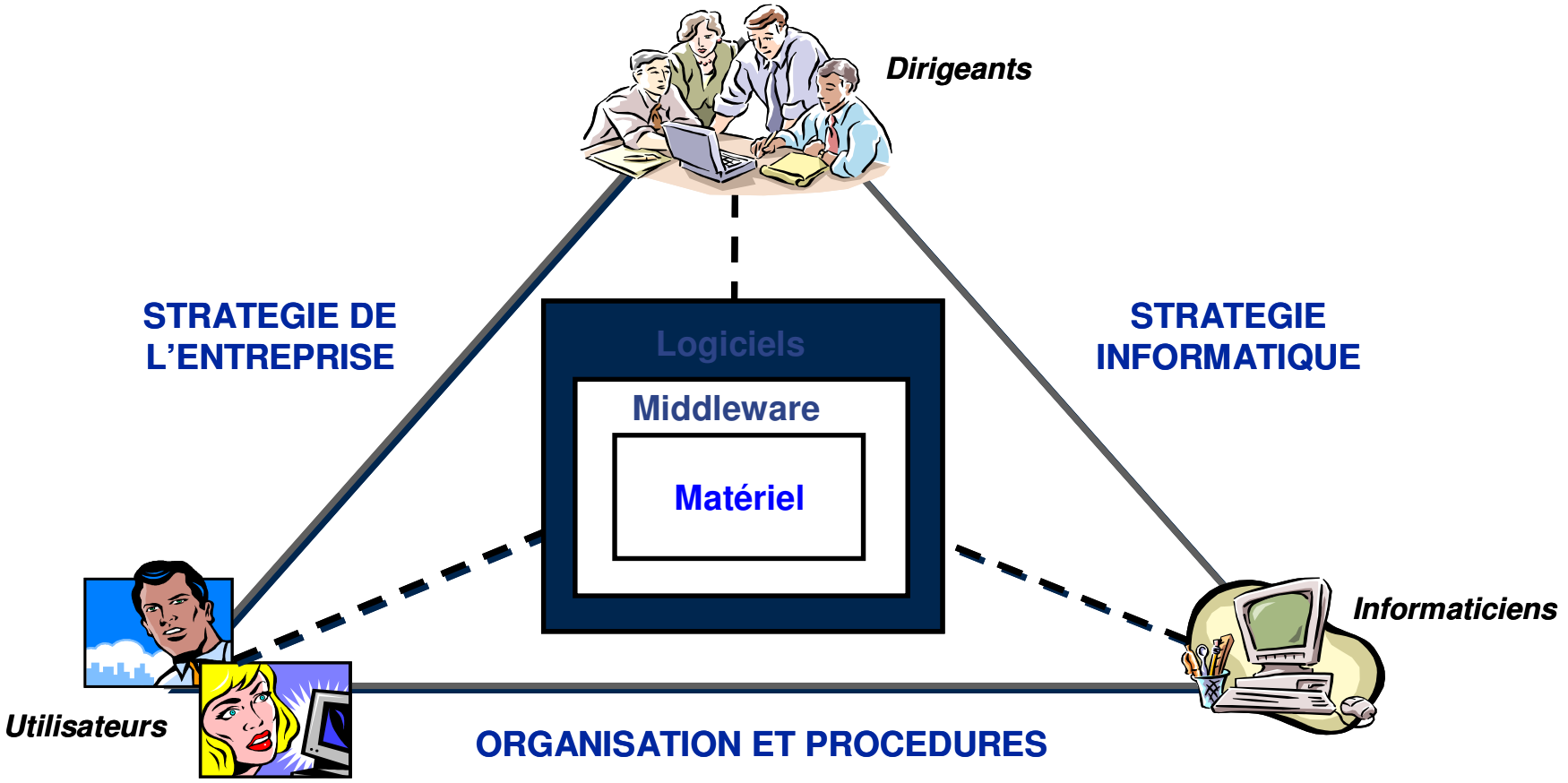
Deux exemples tirés de la pratique de la Cour:

- ✓ **Rapport n°87** : Données du SECO, de la Centrale de compensation, de l'Office cantonal de l'emploi, de l'Hospice général => création d'une clé de cryptage par la Centrale de compensation, donc d'un numéro anonyme : la Cour des comptes ne connaît ni les numéros AVS/AI, ni la clé de cryptage, ni les numéros anonymes (l'institution universitaire qui a analysé les cas ne connaît que le numéro anonyme et n'a livré que des données agrégées).
- ✓ **Rapport n°98** : Données fiscales => serment relatif au secret fiscal, consultation des données sur place, dossier accessible à un cercle limité de personnes.

Qu'est-ce que l'**informatique** et les **risques associés** dans une organisation ?

L' « Informatique » ?

- ✓ Un **processus** / une **fonction** de l'organisation
- ✓ et le **système d'information** supportant les activités de l'organisation



La notion de risques « informatiques » ?

- Les risques inhérents à la **fonction informatique** : stratégie, organisation, ressources humaines, compétences, méthodes, choix des technologies, modes de management et de fonctionnement, opérationnels (développement d'application, exploitation des systèmes), financiers
- Les risques propres au **système d'information**, outil au service de l'organisation, qui ont une incidence directe sur les processus opérationnels et décisionnels

Objectifs à atteindre en matière de SI

EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

efficacité	Atteinte des objectifs fixés initialement
efficience	Utilisation optimale des ressources
conformité	Respect des lois, réglementations et clauses contractuelles
intégrité	Exactitude, validité et intégralité des informations
confidentialité	Protection contre toute divulgation non autorisée
disponibilité	Disponibilité des systèmes, des ressources et des données
fiabilité	Mise à disposition d'informations fiables


Qu'est-ce que l'Audit de SI
au final ?

Les divers types d'audit informatique

- Audit de **gouvernance.**
- Audit **processus** : plan de continuité, gestion du changement, etc.
- Audit d'un **projet,** programme ou d'un projet particulier.
- Audit **technique** : firewall, gestion des identités et authentification dans un progiciel, revue de codes informatiques, paramétrage fonctionnel, application informatique, analyse de la qualité des données, etc.

Rrrrréférentiels …rrrrrr ?

Importance pour l'auditeur et l'audité

- Avantages :
  - Permet de se baser sur les bonnes pratiques reconnues (ce n'est pas que de la théorie) ;
  - Permet de disposer d'un document évolutif ;
  - Facilite l'accès à la formation (permet également d'avoir des intervenants certifiés) ;
  - Offre un langage commun non seulement pour les équipes projets, les opérationnels mais également avec l'auditeur : réduit les incompréhensions et clarifie les attentes de l'auditeur ;
  - Augmente la probabilité de succès d'un projet / d'une activité pérenne : n'est pas égal à une garantie de succès…

Les principaux référentiels

COBIT®
Gouvernance, Contrôle
et Audit *de l'* Information
et des Technologies Associées

AFAI®
Pour des systèmes d'information
de confiance et créateurs de valeur

The Institute of Internal Auditors

Practice Guides — GTAG®
Global Technology Audit Guides (GTAG)

GTAGs are written in straightforward business language and address timely issues related to information technology (IT) management, control, and security.


Sécurité ????
??? Référentiels

Objectifs à atteindre en matière de SI

EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

efficacité	Atteinte des objectifs fixés initialement
efficience	Utilisation optimale des ressources
conformité	Respect des lois, réglementations et clauses contractuelles
intégrité	Exactitude, validité et intégralité des informations
confidentialité	Protection contre toute divulgation non autorisée
disponibilité	Disponibilité des systèmes, des ressources et des données
fiabilité	Mise à disposition d'informations fiables

Protection des données personnelles - smartphones

Points de contrôle	Description
L'enregistrement des smartphones.	Enregistrement, « dés-enregistrement » des utilisateurs et des smartphones; vérification de la conformité des smartphones avant enregistrement.
La protection physique des smartphones.	Mesures de protection contre la perte, le vol, entre autres.
L'installation de logiciels sur les smartphones.	Contrôle et autorisation pour l'installation de logiciels tiers sur les smartphones.
La gestion des versions du système d'exploitation et les mises à jour de sécurité.	Contrôle, déploiement et gestion des versions des systèmes d'exploitation et des mises à jour.
La connexion aux systèmes d'information.	Contrôle et restriction des connexions aux systèmes d'information.
Les contrôles d'accès aux smartphones.	Verrouillage des smartphones.

Protection des données personnelles - smartphones

Points de contrôle	Description
Les techniques cryptographiques.	Utilisation du chiffrement pour protéger les données.
La protection contre les maliciels.	Installation d'un antivirus sur les smartphones.
La désactivation, l'effacement et le blocage à distance.	Blocage, désactivation et effacement à distance en cas de perte ou de vol.
Les sauvegardes.	Sauvegarde des données du smartphone.
L'utilisation des services web et des applications web.	Contrôle et restriction des applications accessibles depuis le smartphone.
Les formations spécifiques.	Mise en œuvre de formations spécifiques couvrant les risques liés à l'utilisation des smartphones.
Séparation entre l'utilisation privée et professionnelle	Ségrégation et cryptage des données, procédures spécifiques (mise en place de logiciel de gestion).
Utilisation de smartphones privés dans le cadre professionnel	Contrat spécifique d'utilisation du smartphone.

Protection des données personnelles - smartphones

Numéro	Risque	Description	Niveau de risque
1	Fuite de données à la suite d'un vol ou de la perte d'un smartphone	Le smartphone est volé ou perdu sans protection adéquate des données.	Elevé
2	Divulgation involontaire de données	L'utilisateur divulgue des données du smartphone de manière involontaire.	Elevé
3	Attaques sur un smartphone déclassé	Les données d'un smartphone décommissionné[1] sont volées.	Elevé
4	Hameçonnage (phishing)	Des renseignements personnels sont soutirés à l'utilisateur (mot de passe, code pin, entre autres). Ces attaques peuvent par exemple être réalisées au travers de SMS ou courriel.	Moyen
5	Attaque de logiciels espions (spyware)	Un logiciel malveillant est installé dans le smartphone dans le but de collecter, déduire des données sensibles par recoupement de données non sensibles, entre autres.	Moyen
6	Attaque par usurpation de réseau	Un point d'interconnexion internet malveillant est installé et les utilisateurs s'y connectent avec leur smartphone. Cette attaque peut ensuite être utilisée pour lancer d'autres attaques, par exemple par hameçonnage.	Moyen
7	Attaque par surveillance	Une personne spécifique est surveillée au travers de son smartphone.	Moyen
8	Attaque par vol d'argent (« Diallerware »)	Il s'agit d'un logiciel malveillant installé sur le smartphone qui effectuera automatiquement et à l'insu de l'utilisateur des appels payants ou enverra des SMS à des numéros surtaxés.	Moyen
9	Attaque par maliciel financier	Il s'agit d'un logiciel malveillant installé sur le smartphone qui vise spécifiquement à dérober des numéros de carte de crédit, les identifiants de ebanking, entre autres	Moyen
10	Congestion du réseau	Il s'agit d'un type d'attaque qui vise à surcharger le réseau afin que l'utilisateur ne puisse pas utiliser son smartphone.	Faible

Protection des données personnelles - smartphones

- Exemples de mesures minimales à prendre :
  - Mise à jour ;
  - Cryptage du smartphone ;
  - Code de verrouillage ;
  - Verrouillage automatiques ;
  - Fonctions spéciales ;
  - Sauvegardes nuagiques ;
  - Messages d'erreur.

Questions ?