Ville de Lausanne
Contrôle des finances
case postale 6904 – 1002 Lausanne

RAPPORT D'AUDIT INTERNE

Technologies matérielles et logicielles gérées hors du SOI (Shadow IT)

Audit informatique

Destinataires :

Municipalité

Madame la Cheffe du service d'organisation et d'informatique

Extrait de la directive municipale sur le Contrôle des finances de la Ville de Lausanne[1]

Art. 18 – Rapports d'audit interne et recommandations

1. Le mandat d'audit débute par un entretien de lancement avec l'audité.
2. Le CFL émet le rapport en version définitive aux destinataires prévus uniquement après la finalisation des étapes suivantes :
   a. Le CFL présente ses conclusions d'audit et recommandations dans un projet de rapport qu'il adresse avant la réunion de clôture à l'audité.
   b. Lors de la réunion de clôture, l'audité fait part de ses éventuelles remarques sur les constats et recommandations du projet de rapport.
   c. A l'issue de cette réunion, le CFL émet une version du projet adressée à l'-aux audité-s et au-x directeurs concerné-s pour prise de position.
   d. L'audité a 60 jours ouvrés pour faire adopter une note à la Municipalité comprenant :
      i. sa position pour chaque recommandation. Si une recommandation s'adresse à un tiers, le CFL adresse séparément sa demande de positionnement à ce dernier ;
      ii. une note de synthèse de suivi des recommandations de l'audité ;
      iii. l'indication des éléments considérés comme étant confidentiels ainsi que les motifs afin que la Ville puisse en tenir compte lors de la publication du rapport.

      Lorsque l'audité n'est pas une entité rattachée à l'administration communale, le service de tutelle doit soumettre la note à la Municipalité, qui en prendra acte.
   e. Le délai de 60 jours écoulé, le CFL émet le rapport final aux destinataires prévus à l'art. 19 al. 1. Celui-ci inclut les prises de position et la note de synthèse de suivi des recommandations de l'audité.
3. En cas de désaccord au sujet des recommandations à mettre en œuvre, le CFL saisit le comité d'audit, qui statue définitivement.
4. Lorsque l'audité n'a pas donné, dans le délai imparti, une suite appropriée aux recommandations du CFL, celui-ci soumet le cas au comité d'audit qui prend les dispositions nécessaires.

Art. 19 - Diffusions des rapports

1. Les rapports d'audit interne sont adressés :
   a. A l'audité ;
   b. Au service subventionnant concerné, lorsque l'audité n'est pas une entité rattachée à l'administration communale ;
   c. A la direction concernée ;
   d. A la Municipalité ;
2. Sous réserve des dispositions de l'art. 16 LInfo, les rapports d'audit interne sont rendus publics dès qu'ils sont achevés au sens de l'article 9 alinéa 1er LInfo, soit dès que le rapport final a été émis par le CFL.
3. Les noms des collaborateurs ne sont pas mentionnés dans le rapport publié.

Remarque

« Les informations contenues dans le présent document (le « Document ») sont destinées aux seuls besoins internes de l'audité et de la Ville de Lausanne. L'utilisation directe ou indirecte par un tiers de tout ou partie du Document s'effectuera sous sa seule responsabilité. Le Document s'appuie sur les faits et circonstances bien particuliers tels qu'ils ont été présentés au Contrôle des finances au moment de sa rédaction et n'a pas vocation à valoir pour le futur. Les destinataires seront seuls compétents et responsables pour la mise en œuvre des recommandations. »

[1] Directive municipale sur le Contrôle des finances de la Ville de Lausanne du 14 janvier 2021 et entrée en vigueur le 14 janvier 2021 : Directive municipale sur le CFL

Synthèse

Le Service d'organisation et d'informatique (SOI) est en charge de l'administration et de la mise en place des solutions informatiques de la Ville de Lausanne. De par ses compétences, il garantit une maintenance et une sécurité des solutions technologiques utilisées. Le contexte de la Ville étant un peu particulier de par son grand nombre de métiers différents, il est un terreau fertile à l'apparition de l'informatique grise (shadow IT) au sein du système d'information.

Le shadow IT désigne tout système d'information mis en œuvre au sein d'une organisation sans l'approbation de sa direction des systèmes d'information (DSI). Le SOI occupe ce rôle et ne peut garantir la sécurité et la fiabilité des solutions shadow IT car elles lui sont, par définition, inconnues.

L'objectif principal de cet audit est de déterminer si les politiques et contrôles mis en place permettent d'encadrer le shadow IT au sein de la Ville et d'en réduire les risques à un niveau acceptable.

Plusieurs constats émanent de cet audit réalisé par le CFL sur les thèmes de la gouvernance et de la gestion opérationnelle :

- Gouvernance :
    - Il n'existe pas de gouvernance stratégique encadrant l'utilisation du shadow IT ;
    - Aucune formation et sensibilisation au shadow IT n'est effectuée auprès des collaborateurs de la Ville ;
    - Aucun contrôle formalisé n'est présent au sein des équipes techniques, défavorisant le bon respect du processus de gestion de la demande ;
    - Les catalogues de prestations, matériels et logiciels ne sont ni exhaustifs, ni attractifs, ni orientés utilisateur.
- Gestion opérationnelle :
    - Il n'existe pas de catalogue de petits matériels informatiques consommables élaboré en concertation avec les différents référents informatiques, puis négocié et mis à disposition par le Service achat et logistique Ville ;
    - Des contrôles liés à la sécurité de navigation internet existent mais aucun contrôles du trafic internet lié à la détection de shadow IT ou à l'utilisation d'applications sur le cloud[2] n'est effectué ;
    - A ce jour, l'outil d'inventaire commun Easyvista ne regroupe pas toutes les solutions informatiques métiers utilisées dans les services ;
    - Il existe un besoin fort de créer une nouvelle plateforme technique transverse répondant aux besoins des différents services, aujourd'hui compensés par des solutions stratégiques shadow IT individuelles.

Sur la base de ces constats, le CFL a formulé huit recommandations ayant pour but d'augmenter le niveau de maitrise du système d'information de la Ville.

[2] Cloud : Technologie en nuage, des services utilisés dans des centres de données ex situ.

Tableau des recommandations

N°	Année	Sujet	Responsables	Risques	Priorité
R1	**2021**	Mise en place d'une stratégie de gouvernance encadrant le shadow IT	SOI	Gouvernance	Elevée
R2	**2021**	Campagne de formation et sensibilisation au shadow IT	SOI	Gouvernance	Moyenne
R3	**2021**	Mise en place de contrôles en parallèle de la gestion de la demande	SOI	Gouvernance Opérationnel	Moyenne
R4	**2021**	Refonte des catalogues de prestations, matériels et logiciels	SOI	Gouvernance Management	Moyenne
R5	**2021**	Création d'un catalogue de petit matériel IT	SOI SALV	Gouvernance	Elevée
R6	**2021**	Système de contrôle du trafic web	SOI	Opérationnel	Elevée
R7	**2021**	Inventaire des solutions présentes dans les services	SOI	Management Opérationnel	Moyenne
R8	**2021**	Plateforme technique transverse encadrant le shadow IT stratégique	SOI SIL EAU MAP CADA	Gouvernance Management	Elevée

SOI : Service d'organisation et d'informatique
SALV : Service achat et logistique Ville
SIL : Services industriels de Lausanne
EAU : Service de l'eau
MAP : Service de la mobilité et de l'aménagement des espaces publics
CADA : Service du cadastre

Note de synthèse du suivi des recommandations (élaborée par l'audité)

Prise de position générale (facultatif)

Le Service d'organisation et d'informatique (SOI) remercie le Contrôle des finances pour le travail effectué et reconnaît que le shadow IT représente un risque pour la sécurité de la Ville.

La situation est encore plus critique lorsque les logiciels sont installés en mode SAAS (dans le Cloud) sans tenir compte de la loi sur la protection des données et des risques de sécurité. Le fait que les services puissent facilement s'abonner à ce type de logiciels fait que le SOI perd aussi la possibilité de rationaliser le nombre de solutions existant au sein de la Ville.

L'audit du CFL a permis de confirmer plusieurs pistes afin d'augmenter le niveau de maîtrise du système d'information de la Ville. Une partie des recommandations faites par le CFL a déjà été ou est en cours de mise en œuvre, notamment : l'élaboration d'un programme de sensibilisation et de formation, d'une stratégie Cloud, la mise en place d'un nouveau catalogue de services, les commandes de petit matériel IT sur LausaShop, la mise en place de systèmes de contrôle plus performants, la révision des processus au sein d'EasyVista et l'architecture d'un socle technique.

Pour les aspects financiers, il est clair que le Service des finances est également d'avis que consolider les budgets informatiques et donner la responsabilité de la gestion de ces lignes budgétaires et des contrats associés au SOI augmenterait grandement la visibilité de ce qui se passe en termes d'achats informatiques au sein de la Ville et réduirait la quantité de shadow IT.

Table des matières

1. Introduction

1.1 Préambule

Le contenu de ce rapport a fait l'objet d'une revue complète par l'audité avant la réunion de clôture le 25 août 2022. Les constats tels que repris dans ce rapport ont été validés lors de cette séance. Les recommandations, relevant quant à elles de l'opinion du CFL, ont été présentées et discutées avec l'audité.

A compter de la date d'émission du présent rapport dans sa version projet, l'audité disposera de 60 jours ouvrables pour prendre position sur les recommandations, élaborer la note de synthèse du suivi des recommandations et se déterminer sur la publication du rapport. A l'issue de ce délai, le rapport sera émis sous sa forme définitive et envoyé notamment à la Municipalité. Sous réserve des dispositions de l'art. 16 LInfo, le rapport d'audit interne sera rendu public.

Lettre de mission	4 février 2022
Réunion d'ouverture	15 décembre 2021
Remise du projet de rapport	19 juillet 2022
Réunion de clôture	25 août 2022
Rapport en version projet avant réponses de l'audité	22 septembre 2022
Remise des réponses de l'audité aux recommandations	6 juillet 2023

Le CFL tient à remercier l'ensemble des collaborateurs du service pour leur disponibilité et leur coopération lors de nos travaux d'audit.

1.2 Définition du shadow IT

Le shadow IT désigne tout système informatique en place sans que le SOI n'en ait la connaissance ou la gestion. La gestion de certaines solutions informatiques métiers peut être confiée à des services mais le SOI doit être au courant afin d'en valider les normes de sécurité, d'exploitation et de maintenance.

Il existe au sein de la Ville plusieurs réseaux informatiques, pour simplifier il y a le réseau bureautique sur lequel sont connectés la majorité des ordinateurs de travail. Il y a ensuite un réseau isolé pour les serveurs et un autre pour la partie technique, industrielle.

Nous avons défini le shadow IT à la Ville comme ceci : « toutes les solutions informatiques non connues ou connues mais non validées par le SOI et présentes sur le réseau bureautique ». Il peut prendre plusieurs formes :

- Du matériel non standard acheté et installé sans l'aval du SOI ;
- Des serveurs connectés au réseau bureautique délivrant des services aux collaborateurs ;
- Des solutions cloud pour l'hébergement ou le stockage ;
- Des applications pour la gestion de projet, tâches spécifiques, ressources ;
- Du shadow IT stratégique, c'est-à-dire qui impacterait des fonctions vitales du système d'information de la Ville en cas de coupure, piratage ou défaillance.

Le shadow IT peut avoir une origine historique, c'est-à-dire qu'il a été mis en place il y a plusieurs années et répondait, à l'époque, à un besoin non couvert par la DSI. Il a pris ou non de l'importance et perdure sur des technologies parfois obsolètes.

Il existe également du shadow IT plus récent, lié à la fois à la facilité de mise en œuvre et à son coût peu élevé mais aussi favorisé par la profusion de solutions gratuites mise à disposition sur internet.

1.3 Contexte et périmètre d'audit

Le SOI est en charge de la surveillance, la maintenance, l'exploitation, et le développement de l'informatique de la Ville de Lausanne. Il assure également un service de veille informatique afin de se tenir au courant des dernières innovations.

Dans un but de sécurisation et de maitrise du système d'information de la Ville de Lausanne, le CFL a souhaité auditer un phénomène grandissant dans les entreprises, le shadow IT. Du fait de ses activités hétérogènes et du cloisonnement de ses services, la Ville de Lausanne semble propice à un tel phénomène.

L'objectif principal de cet audit est de déterminer si les mécanismes de gouvernance mis en place pour la gestion et l'encadrement du shadow IT au sein de la Ville de Lausanne sont suffisants pour réduire les risques liés à ce dernier à un niveau acceptable.

Deuxièmement, le processus achat a été analysé afin d'évaluer si les contrôles en place permettent d'encadrer ou de réduire le shadow IT.

Finalement, le CFL a évalué, sans en recenser l'exhaustivité, l'ampleur et les risques du shadow IT au sein de la Ville en se concentrant sur le shadow IT dit stratégique. Cela concerne les applications remplissant des fonctions stratégiques pour la Ville mais considérées comme du shadow IT car inconnues ou non validées par le SOI.

En relation avec les objectifs mentionnés ci-dessus, le CFL a notamment examiné les éléments suivants :

- Gouvernance :
    - Les politiques en place concernant l'utilisation de matériels, logiciels et applications shadow IT ;
    - La formation et la sensibilisation au shadow IT au sein de la Ville ;
    - La détection du shadow IT en parallèle de la gestion de la demande ;
    - Les catalogues de prestations, matériels et logiciels.
- Gestion opérationnelle :
    - La commande et mise à disposition du petit matériel IT (consommable) ;
    - Le système de contrôle du trafic web ;
    - La tenue d'un inventaire unique et transverse de toutes les solutions de la Ville ;
    - La mise en œuvre d'une plateforme technique transverse répondant aux besoins stratégiques actuels non couverts.

Le matériel et les logiciels présents sur le réseau technique (industriel) ou serveurs ont été exclus du périmètre d'audit car bien trop spécifiques.

1.4 Liste des risques

Les différents risques liés au shadow IT vont dépendre de sa forme, de son ampleur et de sa raison d'être. Voici les principaux enjeux liés au shadow IT :

- Risque de sécurité : Le principal risque du shadow IT est le risque de sécurité. Les logiciels et le matériel approuvés par le SOI font l'objet d'importantes mesures de sécurité, ce qui n'est pas le cas des logiciels et matériels non approuvés. La Ville serait plus sujette aux cyberattaques menées avec succès prenant comme cible son shadow IT.
- Fuite, perte, vol ou corruption de données : certaines applications telles que les services de partage ou de stockage de données comme Google Docs[3] ou DropBox[4] peuvent engendrer des fuites de données sensibles, stratégiques ou financières. Cela peut également créer une porte d'entrée dérobée et avoir pour conséquence la perte, le vol ou la corruption de données.
- Réputation : la réputation de la Ville peut être grandement perturbée par des attaques ciblées fructueuses sur des solutions non gérées par le SOI et accompagnées d'une perte de crédibilité et de confiance de ses citoyens.
- Non-conformité : ces applications représentent aussi un risque concernant la conformité aux lois et règlements telle que la Loi fédérale sur la protection des données personnelles.
- Coûts cachés : si ce n'est pas le SOI qui effectue ou participe aux phases de développement ou d'intégration, l'utilisateur le fera dans ses heures de travail durant lesquelles il ne réalisera pas les tâches pour lesquelles il est rémunéré.
- Capacité de la bande passante[5] : des outils et des applications utilisés sans le consentement du SOI peuvent affecter la bande passante disponible par une consommation accrue et s'avérer nuisibles pour les autres utilisateurs.

Deux exemples plus appliqués permettent d'illustrer les risques susmentionnés :

- Un serveur shadow IT hébergé sur le réseau bureautique peut sembler ne représenter aucun risque car le service délivré n'est pas vital, comme des tableaux de bords par exemple. Cependant, sur un aspect sécuritaire, il peut très bien ne pas être à jour ou mal protégé et constituer une porte d'entrée pour un piratage.
- Une solution cloud de type gestion de projet va héberger des informations sur des ressources humaines ou financières mais les participants au projet n'auront peut-être pas tous la même sensibilisation sur le fait que les données sont stockées sur un cloud à l'étranger. Il existe un risque que des informations confidentielles soient téléchargées sur le cloud et fuitent un jour au grand public.

[3] Google Docs : solution d'hébergement de données sur le cloud de Google.
[4] DropBox : solution d'hébergement de données sur le cloud.
[5] Bande Passante : volume d'informations transitant simultanément sur un câble réseau.

2. Gouvernance

2.1 Politiques et directives en place

L'équipe gouvernance, sécurité et données du Service d'organisation et d'informatique (SOI) a pour mission d'élaborer, de maintenir et de diffuser les politiques et directives et autres règlements informatiques à appliquer à l'ensemble de la Ville de Lausanne.

Dans ce contexte-là, le CFL a analysé si les politiques en place étaient suffisamment à jour et en phase avec les technologies actuelles afin de cadrer l'utilisation du shadow IT ou d'en réduire l'usage.

Nous avons constaté qu'à ce jour, il n''existe pas de politique régissant les différents cas possibles d'utilisation de solutions de type cloud. La charte d'utilisation des moyens de traitement de l'information du 14 novembre 2019 présente des lacunes concernant les nouvelles technologies dites dans le cloud. Un seul paragraphe n'est pas suffisant pour cadrer toutes les nouveautés de ce nouveau domaine :

- Cloud Computing[6] ;
- Machine Learning[7] ;
- Hébergement cloud[8] ;
- Applications SAAS[9].

De plus, le règlement informatique en vigueur date de 2018 et ne comporte aucune mention liée au shadow IT. Les rôles et responsabilités face à ce problème ne sont ainsi pas définis au niveau de la gouvernance.

L'absence de politique formelle, donnant les règles générales d'encadrement du shadow IT au sein de la Ville de Lausanne, ne permet pas à ce jour au SOI d'intervenir de façon légitime dans les services. Ceci a pour conséquence de favoriser la possibilité d'utiliser ou de mettre en place de nouvelles solutions ne respectant pas les standards du SOI en matière de sécurité ou de protection des données.

R1. Mise en place d'une stratégie de gouvernance encadrant le shadow IT

Le CFL recommande de :

- Mettre en place une directive applicable à l'ensemble de la Ville encadrant l'utilisation et l'acquisition des applications hébergées dans des clouds et plus largement de type SAAS (Software As A Service) ou PAAS (Plateform As A Service).
- Mettre à jour le règlement informatique afin de tenir compte des problématiques de shadow IT et de définir les rôles et responsabilités de chacun des acteurs face à ce phénomène.

Risque	Responsable	Priorité
Gouvernance	SOI	Elevée

Position de l'audité	Acceptée	~~Contestée~~	
Eléments clés de la mise en œuvre : Le SOI travaille actuellement à sa stratégie cloud. Cette stratégie définit clairement l'usage acceptable de ce stockage au sein de la Ville de Lausanne et la gouvernance qui sera mise en place. Une nouvelle version du règlement informatique sera présentée cette année à la Municipalité pour approbation. Cette nouvelle version du règlement inclura les points de recommandation mentionnés, entre autres.			
Personne responsable de la recommandation	Chef du pôle GSD & adjoint à la Cheffe de service SOI	**Délai**	Fin 2023

[6] Cloud Computing : Utilisation de services hébergés sur des serveurs ex situ, dans le cloud.
[7] Machine Learning : Apprentissage automatique par des logiciels intelligents.
[8] Hébergement cloud : Stockage de données sur des serveurs distants.
[9] Applications SAAS : Applications Software As A Service : ce sont des logiciels mis à disposition via un simple navigateur web sans installation, prêts à l'emploi et hébergés dans le cloud.

2.2 Formation et sensibilisation au shadow IT

Le SOI dispense, sur demande uniquement, une formation à l'informatique aux nouveaux collaborateurs au travers de l'équipe support helpdesk. Cette formation est orientée utilisation des composants présents sur le poste de travail comme la messagerie, la suite Office, le VPN etc.

Cette formation inclut également une dimension sécuritaire, cela peut concerner une sensibilisation aux mails de hameçonnage ou sur la protection des données personnelles sur le poste.

A ce jour, aucune formation de l'ensemble des collaborateurs travaillant pour la Ville de Lausanne, sur le thème du shadow IT n'est effectuée. Les entretiens menés par le CFL au cours de l'audit confirment que ce sujet est encore méconnu et les risques associés complètement ignorés.

Une sensibilisation et une explication de ce sujet aurait un effet préventif et curatif dans la mesure où il pourrait être porté à l'attention du SOI puis encadré par la suite.

R2. Campagne de formation et sensibilisation au shadow IT

Le CFL recommande, pour l'ensemble des collaborateurs travaillant pour la Ville de Lausanne :

- D'améliorer la formation informatique existante en ajoutant la notion de prévention et d'explication du shadow IT à des fins pédagogiques et préventives ;
- De mettre en place une campagne d'information et de sensibilisation sur la présence et les risques du shadow IT.

Risque	Responsable	Priorité
Gouvernance	SOI	Moyenne

Position de l'audité	Acceptée	~~Contestée~~	
Eléments clés de la mise en œuvre : Un programme de sensibilisation et de formation sur la sécurité informatique et la protection des données est prévu. Le SOI inclura le sujet du shadow IT dans ce programme.			
Personne responsable de la recommandation	Chef du pôle GSD & adjoint à la Cheffe de service SOI	**Délai**	Fin 2023

2.3 La détection du shadow IT

Une bonne pratique recommandée par ITIL[10] consiste en une gestion des processus et des workflows afin d'uniformiser le travail et de réduire les risques d'erreur. Cependant, il faut également mettre en place des contrôles réguliers, planifiés et aléatoires permettant de vérifier périodiquement l'exactitude des actions effectuées et de corriger les éventuelles anomalies identifiées.

Une équipe de gestion de la demande a été créée en novembre 2021 afin de centraliser les nouveaux besoins informatiques de l'ensemble des services de la Ville. L'introduction de cette nouvelle équipe contribue à la diminution du shadow IT mais il faut également coupler les actions de cette équipe avec la mise en place de contrôles réguliers permettant de monitorer l'activité informatique des collaborateurs de la Ville puis d'agir en fonction des anomalies identifiées.

Cet ensemble de contrôles réguliers doit être mis en place et opéré à chacun des niveaux de l'informatique, des créations de comptes aux achats de matériels, en passant par l'analyse du réseau, l'administration des postes de travail et serveurs ou la gestion de solutions. Par exemple :

- Achat : contrôles réguliers des écritures comptables liées à l'informatique permettant d'identifier les divergences entre les consignes budgétaires et la réalité des achats effectués ;
- Environnement numérique : mise en place de contrôles réguliers des applications tierces inconnues installées, utilisées ou autorisées et du matériel de type poste de travail ;
- Réseau et télécom : identification des équipements et serveurs non conformes sur le réseau bureautique ;
- Serveur : analyse régulière et formalisée des serveurs et machines virtuelles en production afin de s'assurer de la conformité de l'utilisation par rapport à la demande ;

[10] ITIL : Information Technology Infrastructure Library est un ensemble d'ouvrages recensant les bonnes pratiques du management du système d'information.

- Gestion des solutions : respect des étapes du processus projet pour la maintenance, les mises à jour et la documentation.

Ces dispositifs de maitrise des risques doivent prendre forme petit à petit afin d'éviter ou de réduire les erreurs commises et donc les failles de sécurité potentielles.

Si des contrôles réguliers ne sont pas en place, le shadow IT peut proliférer, contournant entièrement l'activité de l'équipe en charge de la gestion de la demande et par conséquent les normes de sécurité en vigueur.

R3. Mise en place de contrôles en parallèle de la gestion de la demande

Afin de se prémunir d'éventuels achats de matériels ou logiciels shadow IT, le CFL recommande que ces achats, ceux de services informatiques ainsi que les contrats de maintenance soient gérés par le SOI. En conséquence, les budgets liés à ces sujets devraient donc être transférés au budget du SOI.

Risque	Responsable	Priorité
Gouvernance Opérationnel	SOI SFIN	Moyenne

Position de l'audité	Acceptée	~~Contestée~~	
Eléments clés de la mise en œuvre : Le SOI lancera des réflexions au sein de la Ville au sujet de la centralisation de tels budgets. Il apparaît toutefois que, pour les entités commercialisées, cette solution n'est pas adéquate (refacturation interne, traitement de la TVA). Une solution pourrait être d'appliquer le modèle qui existe déjà sur l'achat de mobiliers (contrôle de la commande par l'entité centralisée mais pas de centralisation des budgets), accompagnée par une directive selon laquelle les achats ne respectant pas le processus ne sont pas pris en charge.			
Personne responsable de la recommandation	Chef de service SFIN Cheffe de service SOI	**Délai**	2024

2.4 Les catalogues de prestations, matériels et logiciels

Il existe au sein de la Ville de Lausanne un catalogue des prestations ainsi qu'un catalogue du matériel et des logiciels qui permettent de répondre aux besoins des collaborateurs de la Ville. De tels catalogues, s'ils sont clairs, intuitifs et incitatifs, permettent de réduire l'apparition du shadow IT.

Lors de notre audit nous avons constaté que l'intégralité des prestations de services du SOI n'était pas présente dans le catalogue mis à disposition sur le portail ServiceApps[11]. Cela ne met pas en valeur l'entièreté du champ de compétences du SOI et peut engendrer du shadow IT par les collaborateurs de la Ville qui considèrent dès lors que la prestation répondant à leur besoin n'est pas disponible.

Il en va de même pour le format du catalogue logiciel qui ne permet pas une lecture complète et aisée de l'ensemble des logiciels. Ce manque de visibilité entraine les collaborateurs à opter pour une nouvelle solution lors d'un nouveau besoin, qui pourrait parfois être mutualisé sur une solution existante.

Concernant le catalogue matériel, l'ergonomie n'est pas au rendez-vous, il est trop fonctionnel. Il doit être attractif, intuitif et surtout orienté utilisateur.

L'absence de clarté et d'attractivité des trois catalogues décourage les collaborateurs des différents services de la Ville de Lausanne à solliciter le SOI et les pousse à agir en silo, alimentant ainsi le volume de solutions shadow IT.

[11] ServiceApps : Interface utilisateur de ticketing de l'application Easyvista.

R4. Refonte des catalogues de prestations, matériels et logiciels

Afin de proposer aux collaborateurs de la Ville l'intégralité des prestations, matériels et logiciels à leur disposition, le CFL recommande de :

- Mettre à jour les différents catalogues existants ;
- Repenser et mettre en place des catalogues plus attractifs visuellement et orientés utilisateur. Par exemple, le collaborateur ne devrait pas se soucier de savoir si le logiciel qu'il demande est standard, métier, sans package, etc.

Risque	Responsable	Priorité
Gouvernance Management	SOI	Moyenne

Position de l'audité	Acceptée	~~Contestée~~
Eléments clés de la mise en œuvre : Le SOI est en train de repenser le catalogue de services en se basant sur une vision utilisateur. L'utilisatrice ou l'utilisateur effectuera une recherche en fonction d'un besoin et obtiendra en réponse les logiciels qui correspondront à ce besoin. La mise en place d'un nouveau catalogue de services nécessite l'investissement en temps de plusieurs équipes au sein du SOI. Une solution à analyser serait celle d'une directive que les achats ne respectant pas le processus ne sont pas pris en charge par la Ville.		
Personne responsable de la recommandation	Chef de pôle PCN	**Délai** Mi-2024

3. Gestion opérationnelle

3.1.1 Le processus achat informatique général

Le Partenariat Des Achats Informatiques Romands (PAIR) facilite grandement la négociation et l'achat du matériel IT de type poste de travail puisque les appels d'offres sont réalisés au sein de ce groupement public. Les appels d'offres ne sont pas réalisés par la Ville et permettent une réduction de prix du fait des grands volumes.

Nous avons constaté, via nos entretiens, que la politique d'achat du matériel et des logiciels est connue par tous les interlocuteurs dans les services et que des consignes budgétaires sont envoyées dans les services chaque année. Le seul bémol précisé à la recommandation trois est l'absence de contrôles permettant de vérifier que les consignes budgétaires sont bien suivies.

Des lignes budgétaires distinctes existent pour différencier les exercices, dépenses de fonctionnement ou d'investissement, et les interlocuteurs interviewés sont satisfaits du processus.

3.1.2 Le processus achat du petit matériel informatique

Le petit matériel IT est défini comme du matériel informatique, en général peu onéreux, non présent dans les dépenses d'investissement tel que les câbles, clés USB, casques audios, vidéoprojecteurs, écrans TV, etc. Pour se procurer ce type de matériel dit « consommable », il existe à minima quatre processus au sein de la Ville de Lausanne :

- Effectuer une demande au SOI puis être refacturé ;
- Contacter le helpdesk lors d'une intervention ou un dépannage ;
- Effectuer un achat puis une note de frais et se faire rembourser par la Ville ;
- Passer une commande via l'application Lausashop du SALV, ensuite imputée sur le budget du service.

Par conséquent, la Ville s'expose d'une part à une plus grande probabilité de ne pas respecter les procédures d'appel d'offres publics en raison des montants élevés des dépenses effectuées en consommables chez les fournisseurs de matériel informatique et d'autre part à une hétérogénéité des matériels utilisés à la Ville et donc à de plus grandes probabilités de pannes ou d'incidents.

Le CFL voit ici une réelle opportunité de se professionnaliser et d'industrialiser le processus d'acquisition de petit matériel informatique avec le Service achat et logistique Ville (SALV) qui travaille déjà avec Lausashop et propose plusieurs catalogues de matériels divers, élaborés via des groupes de travail regroupant plusieurs interlocuteurs au sein de la Ville.

R5. Création d'un catalogue de petit matériel IT

Le CFL recommande l'élaboration d'un catalogue de petit matériel IT répondant à la grande majorité des besoins des collaborateurs en concertation avec l'ensemble des représentants informatiques de la Ville afin d'assurer une cohérence entre l'offre et la demande.

Ce catalogue devrait ensuite être étudié avec le Service achat et logistique Ville afin de travailler conjointement à un encadrement et une mise à disposition simplifiée de ce matériel pour l'ensemble des collaborateurs de la Ville.

Risque	Responsable	Priorité
Opérationnel Gouvernance	SOI SALV	Elevée

Position de l'audité	Acceptée	~~Contestée~~

Eléments clés de la mise en œuvre :

Depuis le 1er février 2023, l'ensemble des collaboratrices et collaborateurs habilités à commander selon les autorisations par service peuvent accéder aux commandes de « petit » matériel IT sur Lausashop géré par le SALV :

- Clavier sans-fil
- Souris sans-fil
- Adaptateurs USB-C vers HDMI/VGA/Ethernet/USB-A (ex: Dell DA310)
- Chargeur USB-C secteur
- Chargeur USB-C allume-cigare
- Clés USB
- Webcam
- Casque téléphonique filaire et sans-fil
- Beamer
- Câbles Ethernet / HDMI
- Speaker de table en USB
- Système vidéo-conférence
- Filtre de confidentialité pour écran.

Prévoir une obligation de passer par Lausashop pourrait compléter le dispositif.

Personne responsable de la recommandation	Cheffe de service SOI Cheffe de service SALV	Délai	Février 2023

3.2 Système de contrôle du trafic web

La notion de trafic internet et les outils techniques de filtrage et de contrôle ont beaucoup évolué ces dernières années. Les nouvelles technologies liées au trafic internet rendent plus difficile l'analyse du contenu échangé lors de la navigation. Par ailleurs, l'offre proposée sur internet, en constante augmentation en termes de volume mais aussi de technologies nouvelles, impose un meilleur encadrement de ce trafic plus adapté aux enjeux actuels.

Le SOI dispose actuellement des technologies nécessaires au bon contrôle du trafic internet mais des améliorations peuvent cependant être apportées :

- Le choix d'autoriser des applications d'hébergement cloud plutôt que de disposer d'un cloud local mis à dispositions des utilisateurs internes ou externes est discutable du point de vue de la sécurité sachant que le volume et le contenu des données échangées ne sont pas contrôlés ;
- Une solution de type CASB[12] peut être mise en place afin de faciliter le management et les contrôles du trafic web. Des analyses comportementales peuvent être opérées avec des alertes ainsi que la détection de shadow IT.

[12] CASB : Solution de contrôle des flux et accès aux applications cloud.

- Un serveur de log[13] Syslog[14] permettant de regrouper les nombreux journaux d'évènements des différents firewalls est en place mais est sous utilisé. Avec plus de ressources et de temps, il permettrait une analyse plus fine du trafic web afin de mieux suivre l'utilisation faite par les collaborateurs de la Ville.

R6. Système de contrôle du trafic web

Le CFL recommande de :

- Mettre en place des solutions de filtrages web et de contrôle du trafic web améliorées afin d'empêcher ou d'encadrer le plus possible l'utilisation d'applications de type Software As A Service (Cloud) ;
- Instaurer des contrôles réguliers du trafic web afin de vérifier l'utilisation de ce service fourni aux collaborateurs à travers les divers moyens d'accès au réseau ;
- Optimiser l'usage du serveur Syslog afin de permettre une meilleure analyse du trafic web ;
- Etudier la mise en place d'un cloud local Ville de Lausanne ou sa réalisation conjointement avec d'autres administrations publiques.

Risque	Responsable	Priorité
Opérationnel	SOI	Elevée

Position de l'audité	Acceptée partiellement	~~Contestée~~	
Eléments clés de la mise en œuvre Le SOI soumettra des propositions à la Municipalité afin de mettre en place des systèmes de contrôle plus performants. Une stratégie Cloud pour les besoins de la Ville de Lausanne sera soumise prochainement à la Municipalité. Dans cette stratégie, il est prévu que la Ville approche de façon proactive les projets de Swiss Cloud ou Cloud souverain, afin de voir dans quelle mesure il est possible de rejoindre l'un d'entre eux le plus rapidement possible.			
Personne responsable de la recommandation	Chef du pôle GSD & adjoint à la Cheffe de service SOI	**Délai**	Fin 2024

3.3 Un inventaire commun et exhaustif des logiciels

L'outil d'inventaire des logiciels du SOI, Easyvista, est à jour en ce qui concerne le périmètre du SOI. Depuis plus de cinq ans déjà, les exigences relatives à la documentation, hébergées sur le Sharepoint se sont améliorées et les nouvelles solutions répondent aux exigences de qualité.

Le CFL a obtenu plusieurs extractions de logiciels :

- Les logiciels présents dans l'outil d'inventaire Easyvista ;
- Les logiciels installables sur les postes ;
- Les logiciels installés sur les postes ;
- Les logiciels réellement utilisés.

Les logiciels recensés dans Easyvista doivent être les mêmes que dans les trois dernières extractions. Nous avons donc effectué diverses vérifications sur la base de ces extractions et avons constaté les points suivants :

- Certains logiciels sont présents sur les postes mais pas dans l'inventaire. Parmi ces logiciels absents de l'inventaire, certains ont pourtant été autorisés sur les outils de sécurité ;
- Des solutions techniques ou métiers sont utilisées sur le réseau bureautique alors qu'elles ne devraient être installées et utilisées que sur le réseau technique ;
- Des solutions cloud, non visibles sur les postes de travail sont directement utilisées grâce à un navigateur internet.

Après plusieurs entretiens avec des responsables informatiques, tous sont favorables à partager les connaissances informatiques avec le SOI. Cela n'empêche pas de garder la gestion opérationnelle au sein des services mais favoriserait les synergies interservices grâce à un niveau d'informations mutualisé.

[13] Log : Journal d'évènements informatiques d'un ordinateur ou d'un serveur.
[14] Syslog : Serveur dédié au regroupement et à la mise en forme des logs pour faire ressortir les informations pertinentes.

Le niveau de maturité, de documentation, de technologie utilisée et de sécurité informatique demandés aux services pour leurs solutions informatiques ne peut être garanti que par le SOI, seul service en charge de mettre en œuvre le programme de législature concernant la sécurité informatique.

R7. Inventaire des solutions présentes dans les services

Le CFL recommande au SOI de mettre en place, à l'attention de chaque référent informatique de service, un dispositif de mise à jour de leurs différentes solutions technologiques respectives sur l'outil d'inventaire unique Easyvista.

Les modèles de documentation doivent également être remplis sur la plateforme Sharepoint, permettant de garantir un niveau correct d'informations sur les solutions existantes dans le système d'information de la Ville.

Risque	Responsable	Priorité
Management Opérationnel	SOI	Elevée

Position de l'audité	Acceptée partiellement	~~Contestée~~

Eléments clés de la mise en œuvre :
Le SOI est en train de revoir les processus au sein d'EasyVista et les droits nécessaires pour chaque acteur. L'accès à la CMDB qui contient les informations concernant les applications sera inclus dans cette révision.
La documentation des solutions gérées par le SOI est maintenue à jour par les responsables solutions.

Personne responsable de la recommandation	Chef de pôle PCN	Délai	2024

3.4 Le shadow IT stratégique

Le shadow IT est presque impossible à éviter dans une organisation, surtout à la Ville de Lausanne où le contexte est un peu particulier du fait du grand nombre de métiers différents qui implique une hétérogénéité dans les applications mises à disposition et donc un environnement plus propice au shadow IT.

Le CFL s'est concentré sur cette partie dite stratégique, c'est-à-dire du shadow IT qui, s'il ne fonctionnait pas, impacterait le fonctionnement de toute la Ville, d'un service ou d'une équipe.

Notre travail ne peut être exhaustif car le shadow IT est par essence invisible mais au cours de nos entretiens et de notre analyse des serveurs présents sur le réseau bureautique, nous avons identifié du shadow IT stratégique dans plusieurs services :

- Le Service EAU possède un intranet, hébergé sur sa propre infrastructure physique et mis à disposition de ses collaborateurs par ses informaticiens. Au fil des années, cet intranet a pris de l'ampleur et constitue aujourd'hui une véritable solution technique indispensable gérant les formations, les éléments variables de paie, les rapports d'analyse du laboratoire, etc. ;
- Le Service du cadastre (CADA) héberge la solution Goéland, utilisée initialement pour des publications et flux de documents puis rapidement devenu hautement stratégique et utilisée dans tous les services de l'Administration communale par plusieurs centaines de collaborateurs.
- Le Service partagés des SiL (SPAR), qui comporte une division informatique avec des chefs de projet et des développeurs, a créé des solutions sur mesure pour répondre aux besoins métiers des différents services composant les Services industriels de Lausanne (SiL) comme de la gestion de projet interfacée avec SAP[15] ou des outils de gestion du réseau fibre de la Ville.

Le dénominateur commun de ces solutions réside en plusieurs points :

- La rapidité de mise en œuvre ;
- La facilité du processus décisionnel ;
- Le coût généralement faible car provenant de solutions libres ;
- Des ressources humaines ayant du temps dédié et des compétences informatiques.

[15] SAP : Logiciel de gestion d'entreprise utilisé par les SIL.

Un des risques de sécurité identifié est le retard de la mise en place du Network Access Control (NAC), un dispositif technique permettant de contrôler et bloquer tout équipement informatique qui se connecterait au réseau de la Ville sans autorisation du SOI.

Ces solutions, et potentiellement bien d'autres, peuvent ou non être connues du SOI mais en tout cas ne sont ni gérées, ni documentées, ni sécurisées selon les standards du SOI. Parfois, le niveau est plus exigeant que celui du SOI, parfois plus bas et la robustesse d'une chaine se mesure à son maillon le plus faible.

R8. Plateforme technique transverse encadrant le shadow IT stratégique

Le CFL recommande :

- D'effectuer une récolte des besoins métiers de tous les services, pouvant être réunis sur un socle technique transverse afin de former un projet dédié à l'harmonisation de ces solutions ;
- De mettre en conformité technologique et sécuritaire toutes les solutions stratégiques évoquées ci-dessus au travers d'une technologie commune ;
- D'uniformiser les solutions techniques shadow IT stratégiques au sein d'une plateforme technique transverse.

Risque	Responsable	Priorité
Gouvernance Opérationnelle	SOI SIL EAU CADA	Elevée

Position de l'audité	Acceptée partiellement	~~Contestée~~	
Eléments clés de la mise en œuvre : Les services collaborent actuellement sur l'architecture des socles techniques. Ces nouvelles architectures seront présentées à la Municipalité pour approbation.			
Personne responsable de la recommandation	Chef du pôle GSD & adjoint à la Cheffe de service SOI Responsable division IT SIL Responsable gestion des données EAU Resp. Goéland et GC & adjoint au Chef de service CADA	**Délai**	Note à la Municipalité fin 2023

Compte tenu des remarques et recommandations figurant dans le corps du présent rapport, et tout en formulant les réserves d'usage pour le cas où des documents, des renseignements ou des faits susceptibles de modifier nos considérations n'auraient pas été portés à notre connaissance au cours de nos travaux, cet audit n'appelle pas d'autre commentaire de notre part.

Lausanne, le 24 juillet 2023

Contrôle des finances de la Ville de Lausanne

Yves Tritten

2023-07-24 12:06

Signé électroniquement par Yves Tritten

Yves Tritten
Chef de service