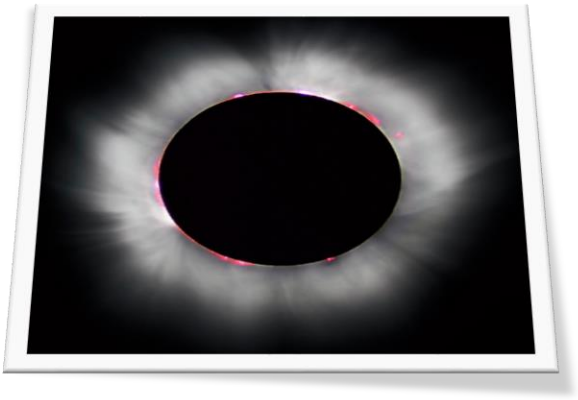
THÈSE PROFESSIONNELLE

SHADOW CLOUD IT
CONSERVER LA MAITRISE DU SI



Thèse soutenue le 27 février 2020

CVO-EUROPE
LIFE SCIENCES CONSULTANCY

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Tuteur : **GIRARD Olivier**

Pilotes : **GRIOL Gaël**

CONTI Patrice

ECHEVERRIA Sébastien

sebastien.echeverria@free.fr

Cycle : **Manager des Systèmes d'Information option sécurité**

Promotion : **MSSI (2018-2020)**

CC BY NC SA

Mots clé : Shadow IT, métiers, cloud, système d'information, gouvernance.

Fiche de confidentialité

FICHE DE CONFIDENTIALITE

DES RAPPORTS, MEMOIRES, THESES ET SOUTENANCES PROFESSIONNELS

Formation/qualification préparée : Manager des systèmes d'information – Option sécurité
Nom-Prénom du stagiaire : ...ECHEVERRIA Sébastien.....
Titre du dossier professionnel : ...Shadow cloud IT : conserver la maîtrise du SI.....
Date de la soutenance : 27 février 2020

Nom de l'entreprise : ...CVO-EUROPE.....
Nom et qualité du représentant de l'entreprise : ...GIRARD Olivier...Responsable infrastructure.....

Noms, entreprises et fonctions des membres de jury :

Nom-Prénom	Entreprise	Fonction

Mode de diffusion autorisé
(Cocher la case correspondante)

✓ Diffusion libre
Le dossier est conservé en archives au CESI, il peut être librement consulté et reproduit. Il peut être utilisé par les destinataires, les études peuvent faire l'objet de publication....

□ **Diffusion limitée au CESI**
Les membres du jury rendent leur exemplaire au stagiaire à la fin de la soutenance. Le stagiaire est responsable de cette restitution. Un exemplaire est conservé en archives au CESI. Le dossier peut être consulté pour exemple ou illustration par les stagiaires des promotions suivantes mais il ne peut être ni sorti du CESI, ni reproduit, sauf autorisation expresse de l'auteur et de son entreprise. La mention « Diffusion limitée au CESI, reproduction interdite » doit figurer sur la page de garde.

□ **Diffusion interdite**
Les membres du jury rendent leur exemplaire au stagiaire à la fin de la soutenance. Le stagiaire est responsable de cette restitution. Un exemplaire est conservé au CESI, à titre de preuve dans le dossier pédagogique du stagiaire. Le dossier ne peut être ni consulté, ni sorti du CESI, ni reproduit, sauf autorisation expresse de l'auteur et de son entreprise. La mention « Diffusion et reproduction interdites » doit figurer sur la page de garde.

Signatures

Pour l'entreprise
O. GIRARD

Le stagiaire
SE

Le CESI

BY NC SA

Remerciements

Je tiens à remercier l'équipe pédagogique du CESI de nous avoir formés et suivis pendant ces 18 mois et plus. J'ai particulièrement apprécié l'accueil, la qualité des intervenants et de la formation.

Je remercie Gaël GRIOL et Yoan ISSARTEL pour leur accompagnement pendant toutes ces années.

Je remercie mes compagnons de formation Mathieu BUCQUOY, Nathan MAY et, Jonathan CORDELOIS pour leur investissement et leur état d'esprit.

Je tiens également à remercier l'ensemble du personnel du groupe CVO-EUROPE, plus particulièrement Mr Olivier GIRARD ainsi que le service informatique de m'avoir fait confiance et permis d'intégrer l'équipe durant ma formation.

Je remercie aussi Mr Olivier GIRARD, Mr Quentin DUBOUX, Mr Cédric MARCEAU et Mr François LAGARDE pour leur disponibilité, leur patience et leur pédagogie.

Je remercie Alexis MARTIN-PINSON et Anne-Julie ROBINEAU pour leur aide et leurs conseils sur la thèse.

Je remercie également les différentes promotions de CESI avec lesquelles j'ai évolué et échangé tout au long de ma formation au CESI.

Je voudrais exprimer ma gratitude à toutes les personnes qui m'ont aidé avec la thèse.

Et enfin, je remercie ma famille et mes amis de m'avoir soutenu et encouragé durant toute la formation.

Droit de diffusion

Cette thèse est sous la licence Creative Commons avec les options suivantes :

	ATTRIBUTION (BY) : Oblige ceux qui utilisent les éléments sous cette option à créditer de la manière dont l'auteur le demande, sans pour autant suggérer une apparition de leur utilisation ou leur donner votre aval ou votre soutien.
	PAS D'UTILISATION COMMERCIALE (NC) : Autorise les autres à reproduire, à diffuser et à modifier, pour toute utilisation autre que commerciale.
	PARTAGE DANS LES MEMES CONDITIONS (SA) : Autorise les autres à reproduire, diffuser et modifier votre œuvre, à condition qu'ils publient toute adaptation sous les mêmes conditions. Toute publication d'une adaptation sous d'autres conditions doit obtenir une autorisation préalable.

Les descriptions sont extraites du site : https://creativecommons.org/licenses

J'ai souhaité utiliser ce type de licence, car elle me permet :

- De partager et faciliter l'utilisation pour tout le monde.
- D'autoriser gratuitement la reproduction et la diffusion.
- De faire évoluer ma thèse et de l'enrichir.

Ces options sont répertoriées dans le pied de page du document avec le logo suivant :

Notice de lecture

En lisant cette thèse, vous trouverez quatre types de paragraphes, chacun avec des couleurs différentes.

Ce code couleur existe pour distinguer les informations présentes dans ce document. Pour vous accompagner, veuillez vous référer à la notice de lecture suivante :

- Les cadres en pointillés de couleur verte : les définitions tirées de sites internet ou de documents :

- Les cadres en pointillés de couleur bleue : les passages de textes copiés depuis des sites internet ou documents.

- Les cadres en pointillés de couleur grise : les explications de termes utilisés dans la thèse.

- Les tableaux de couleur orange et grise : un résumé des informations importantes à retenir.

Résumé des informations importantes

Résumé

Le Shadow IT, un concept qui prévaut dans nos systèmes d'information, est la mise en œuvre ou l'utilisation de systèmes d'information ou de communication par les utilisateurs sans se référer au préalable ou sans en informer la direction des systèmes d'information (DSI). Les raisons sont nombreuses, comme la consumérisation ou la digitalisation. De plus, face à des besoins utilisateurs de plus en plus spécifiques, les DSI sont trop rigides ou trop longues dans leur temps de réponse.

Le marché actuel oblige les services métiers des entreprises à devenir de plus en plus réactifs, innovants et compétitifs pour ne pas perdre face à une concurrence grandissante. Si les DSI ne répondent pas à ces exigences, les utilisateurs prendront le risque de les court-circuiter malgré les problèmes de sécurité que cela peut entraîner. Ils se tourneront vers des fournisseurs externes qui leur proposent des solutions adaptées.

Le digital est devenu essentiel pour les entreprises aujourd'hui. Le développement des connaissances des utilisateurs leur a permis de s'adapter aux nouvelles technologies qui répondent à leurs besoins. Avec la croissance du Shadow IT ces dernières années, les DSI devront le considérer si elles ne veulent pas disparaître.

Cette tendance ne doit pas être éliminée ou simplement bloquée sans dialogue et remise en question. Le Shadow IT permettra de vous montrer vos faiblesses et d'évoluer avec vos services métiers. Votre gouvernance devra l'assimiler afin de réorienter vos choix et le fonctionnement du service.

Mots-clés : Shadow IT, métiers, cloud, système d'information, gouvernance, sécurité, digital, consumérisation.

Abstract

Shadow IT, a concept that prevails in our information systems, is the implementation or use of information or communication systems by users without prior reference or without informing the IT department.

There are many reasons for this, such as consumerisation or digitalisation. Moreover, faced with increasingly specific user needs, IT services management are too rigid or too long in their response time.

Today's market is forcing business departments to become increasingly responsive, innovative and competitive in order not to lose out in the face of growing competition.

If IT departments do not meet these requirements, users will take the risk of bypassing them despite the security issues that this may entail.

They will turn to external suppliers who offer them suitable solutions. Digital has become essential for businesses today. The development of users' knowledge has enabled them to adapt to new technologies that meet their needs.

With the growth of Shadow IT in recent years, IT departments will have to consider it if they do not want to disappear.

This trend must not be eliminated or blocked simply without dialog. Shadow It will allow you to show your weaknesses and evolve with your business services. Your IT governance will have to assimilate it in order to reorient your choices and the way the IT departement operates.

Keywords : Shadow IT, business services, cloud, information system, IT governance, security, digital, consumerization ..

Sommaire

Fiche de confidentialité **1**
Remerciements **2**
Droit de diffusion **3**
Notice de lecture **4**
Résumé **5**
Abstract **6**
Sommaire **7**
Liste des figures **9**
Liste des tableaux **10**
Introduction **11**
Cadrage **13**
I. Structure 13
II. Contexte et enjeux 14
III. Périmètre 14
Concepts et notions **15**
I. La consumérisation de l'informatique 15
II. Le Cloud 16
III. L'évolution des systèmes d'information 19
IV. RGPD 22
V. Problématique 24
État de l'art **26**
I. Définition 27
II. Terminologies 29
III. Caractéristiques 30
1. Notoriété 30
2. Travaux de recherches 31
3. Causes 32
IV. Pratiques du Shadow IT 34
1. Conséquences 35
V. Perception vs réalité 37
VI. Méthode d'évaluation Shadow IT 39
VII. Hypothèses 40
État des lieux **41**
I. Questionnaire sur le Shadow IT en entreprise 41
1. Objectifs 41
2. Méthode 41

A. Les profils informatiques 42
B. Les profils directions et métiers 43
C. Moyens de diffusion 44
3. Résultats du sondage 45
A. Les répondants et leur entreprise 45
B. Interprétation des résultats 47
II. Conclusions 61
1. La détection et le blocage du Shadow IT 61
2. La communication et la sensibilisation 62
3. Les capacités de la DSI 62
Conception de la démarche 64
I. Rappel 64
II. Axes de la démarche 64
1. Évolution technique du SI 65
2. Sensibilisation et communication 67
3. Organisation de la DSI 68
III. Guide méthodologique 72
Conclusion 74
I. Bilan de la thèse 74
Références webographies 75
Annexes 77
I. Glossaire 77
II. Stealth IT 81
III. Sondage 82
1. Profil DSI : 84
2. Profil Métier 86

Liste des figures

Figure 1. – Cadrage : Construction de la thèse 13
Figure 2. – Cloud : les différents modèles de service 17
Figure 3. – SI : Mode de fonctionnement classique 19
Figure 4. – SI : Mode de fonctionnement après le cloud et la consumérisation 19
Figure 5. – Projets informatiques : Participation aux projets 21
Figure 6. – Applications Cloud : GDPR-READY 23
Figure 7. – Représentation de l'ombre 26
Figure 8. – Google trends : Intérêt de la recherche sur le Shadow IT dans le monde 30
Figure 9. – SI : La relation entre le service informatique et les métiers 33
Figure 10. – Dangerosité du Shadow IT 35
Figure 11. – Évaluation : instances Shadow IT 40
Figure 12. – Questionnaire : Mind-map 41
Figure 13. – Sondage : Nombre de réponses par profil 45
Figure 14. – Sondage : Taille des entreprises 45
Figure 15. – Sondage : Secteurs d'activité 46
Figure 16. – Sondage : Expérience des répondants à leur poste 46
Figure 17. – Sondage : Conscience du Shadow IT des métiers 47
Figure 18. – Sondage : Définition du Shadow IT par le service informatique 48
Figure 19. – Sondage : Conscience du Shadow IT de la DSI 48
Figure 20. – Sondage : Exemples de Shadow IT 49
Figure 21. – Sondage : Communication sur l'utilisation des outils et matériels par la DSI 49
Figure 22. – Sondage : Communication sur la sécurité informatique par la DSI 50
Figure 23. – Sondage : Shadow IT : Menace ou opportunité ? vision de la DSI 51
Figure 24. – Sondage : Les menaces du Shadow IT par la DSI 52
Figure 25. – Sondage : Intégration du Shadow IT dans la gouvernance 53
Figure 26. – Sondage : Moyens face au Shadow IT 53
Figure 27. – Sondage : Actions contre le Shadow IT 54
Figure 28. – Sondage : Gouvernance du BYOD 55
Figure 29. – Sondage : Autorisation du BYOD et du BYOA par les managers 55
Figure 30. – Sondage : Relation entre l'IT et les métiers 57
Figure 31. – Sondage : Ratio d'implication de la DSI dans les projets métiers 57
Figure 32. – Sondage : Fréquence d'implication des services informatiques dans les projets métiers 58
Figure 33. – Sondage : La relation entre les DSI et les métiers durant les projets 58
Figure 34. – Sondage : Les problèmes majeurs des services informatiques par les métiers 59
Figure 35. – Sondage : Consommation du Shadow IT dans les entreprises 60
Figure 36. – Sondage : Le Shadow IT & les nouvelles générations 61
Figure 37. – Axes de la démarche 64
Figure 38. – Cartographie du SI : les différentes visions 65
Figure 39. – CASB : Marché des solutions 66
Figure 40. – Prévention du Shadow IT : Business Needs Manager 69
Figure 41. – Traitement : Actions face au Shadow IT 70
Figure 42. – Guide méthodologique : limitation de l'adoption du Shadow IT 72
Figure 43. – Illustration Stealth IT 81

Liste des tableaux

Tableau 1. – Concepts et notions : infos clé 25
Tableau 2. – Définition : Infos clé 29
Tableau 3. – Différentes terminologies : infos clé 30
Tableau 4. – Caractéristiques du Shadow IT : infos clé 34
Tableau 5. – Classification des ressources Shadow IT 34
Tableau 6. – Pratiques du Shadow IT : infos clé 37
Tableau 7. – Symantec : Top types des applications et services cloud 37
Tableau 8. – Symantec : Top des applications et services cloud 38
Tableau 9. – Cybersécurité : infos clé 39
Tableau 10. – Questionnaire : Questions génériques 42
Tableau 11. – Questionnaire : DSI – perception du répondant face au Shadow IT 42
Tableau 12. – Questionnaire : DSI – comportement du département informatique 43
Tableau 13. – Questionnaire : Métiers – vision et implication du répondant sur le Shadow IT. 43
Tableau 14. – Questionnaire : Métiers – le département informatique et les métiers 44
Tableau 15. – Sondage : Échelle de notation 56
Tableau 16. – Traitement : actions face à la pertinence et la qualité du Shadow IT 70
Tableau 17. – Méthodes de gestion de projet : Taux de réussite 71

Introduction

En quelques décennies, l'informatique et les télécommunications sont devenues les plus grands secteurs économiques mondiaux. Ces domaines ont connu des grandes avancées durant le XXe siècle.

Entre les années 1940 et 1980, les outils informatiques, essentiellement considérés comme des outils d'automatisation, ne remettent pas en cause la gestion organisationnelle traditionnelle de la logique pyramidale et des silos fonctionnels.

Le premier ordinateur entièrement électronique l'ENIAC[1] , servant à résoudre des problèmes de calcul, est apparu en 1946.

IBM annonce en 1953 la série des ordinateurs 650 qui seront utilisés, durant le reste de la décennie, pour des usages commerciaux et de correction de traitements.

La première grande avancée fut le réseau Arpanet[2] par l'armée américaine en 1969. Les ordinateurs devenaient un outil de communication.

Par conséquent, les 30 dernières années du XXe siècle ont été marquées par le développement rapide de l'informatisation commerciale.

Le marché du grand public a vu, à la fin des années 70, la commercialisation des ordinateurs d'Apple et d'IBM avec son premier ordinateur portable.

L'année 1989 marque la naissance du Web[3] créé par Tim Berners-Lee. C'est l'aspect le plus connu d'Internet aujourd'hui. Avec l'avènement d'Internet, nous avons assisté à la croissance explosive du numérique.

La course constante à l'innovation dans les domaines de l'électronique l'informatique et la communication font qu'ils deviennent le principal levier de modernisation et de compétitivité de l'économie moderne.

L'informatique domestique s'est métamorphosée par l'arrivée des tablettes tactiles et du Web 2.0 rendant internet plus simple et plus interactif. De nouvelles tendances comme le BYOD[4] font leur apparition. C'est l'utilisation d'appareils personnels dans le monde professionnel.

Le développement d'Internet a conduit à de nouvelles applications des technologies de l'information, comme le "cloud computing", qui permet l'utilisation à distance de ressources informatiques. D'autres tendances se dessinent, comme l'échange direct entre les prestataires informatiques et les services métiers des entreprises, court-circuitant les DSI.

[1] Numerical Integrator Analyser and Comuter
[2] Advanced Research Projects Agency Network
[3] World Wide *Web*
[4] Bring Your Own Device

L’explosion du numérique entraina la consumérisation de l'informatique. C’est le mélange d'utilisation personnelle et professionnelle d'applications et d'appareils technologiques.

J’ai décidé de présenter les différentes évolutions et pratiques de l’informatique car elles ont conduit à un usage appelé le « Shadow IT ». Ce phénomène est en constante augmentation dans le domaine professionnel. C’est une réelle problématique pour les directions des services informatiques et les entreprises. J’ai constaté lors de mes expériences professionnelles sa présence et son utilisation massive.

Pour ces raisons, j’ai décidé d’effectuer ma thèse sur ce sujet. Je souhaite aider les directions informatiques et les services métiers face à cette problématique peu documentée.

Ce thème doit être une priorité et être abordé par les directions des services informatiques, notamment dans le nouveau contexte du RGPD[5] et de l’explosion des applications cloud[6].

[5] Règlement Général sur la Protection des Données
[6] Cloud computing

I. Structure

Cette thèse professionnelle est divisée en quatre chapitres Je l'ai réalisé en suivant la méthode de la **figure 1**.

- Concepts et notions :
  J'expliquerai dans un premier temps les notions nécessaires pour la compréhension du Shadow IT. J'exposerai ma problématique.

- État de l'art :
  Je présenterai ensuite un résumé de mes recherches pour comprendre ce qu'est le Shadow IT. J'exposerai mes trois hypothèses.

- États des lieux :
  Je présenterai mon enquête et j'analyserai les réponses à mon sondage en étayant mes hypothèses.

- Conception de la démarche & proposition

  Le but du dernier chapitre est de présenter une démarche via un guide méthodologique qui me permettra de répondre à mes questions.

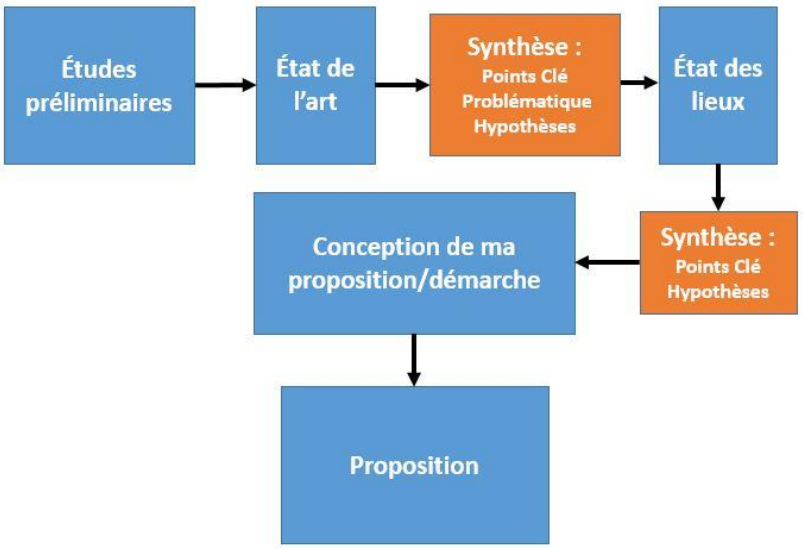


Figure 1. – Cadrage : Construction de la thèse

II. Contexte et enjeux

Aujourd'hui, le numérique a radicalement changé nos habitudes de travail et de vie.

L'avènement du cloud, les améliorations de l'informatique personnelle et la culture informatique prête à l'emploi sur Internet ont permis au Shadow IT de s'accroître.

Les directions des services Informatiques ont du mal à s'adapter aux besoins des utilisateurs en temps réel. Ils peinent à mettre en œuvre des solutions informatiques de plus en plus simples et rapides.

Le Shadow IT n'est pas sans risque, il vulnérabilise et met en péril le système d'information de l'entreprise.

Le RGPD est entré en vigueur le 25 mai 2018, il vise à harmoniser la collecte et le traitement des données personnelles des citoyens européens pour les protéger. Il est difficile pour les entreprises d'identifier un traitement ou des données dont elles n'ont pas conscience.

Dans ce contexte complexe, les enjeux sont de taille pour les entreprises européennes :

- La conformité au RGPD
- L'augmentation de la productivité
- La génération de valeurs
- La maitrise et la protection du système d'information
- Le maintien et l'amélioration de la communication entre les services informatiques et les services métiers
- La sensibilisation à la sécurité des collaborateurs
- L'augmentation de l'implication des collaborateurs
- Une meilleure prise de décisions
- L'amélioration du catalogue de service
- Le maintien et l'amélioration de l'image publique

III. Périmètre

J'ai choisi comme périmètre de ma thèse, les entreprises françaises de toute taille.

Je me suis concentré sur le Shadow IT et plus particulièrement sur sa nouvelle forme générée par les applications cloud.

Avant d'introduire le Shadow IT, je vais présenter des concepts comme la consumérisation de l'informatique et le cloud. Des pratiques que l'on doit comprendre car elles vont influencer le Shadow IT et les systèmes informatiques des entreprises. Ensuite, je vais introduire le nouveau règlement européen fortement lié au cloud. En conclusion de ce chapitre, j'annoncerai ma problématique.

I. La consumérisation de l'informatique

Je vais m'appuyer sur la définition du site Wikipédia sur la consumérisation (1) :

> Consumerization is the reorientation of product and service designs to focus on (and market to) the end user as an individual consumer, in contrast with an earlier era of only organization-oriented offerings (designed solely for business-to-business or business-to-government sales).

Cela décrit qu'il s'agit d'une redirection de produits vers de nouveaux consommateurs.

> The emergence of the individual consumer as the primary driver of product and service design is most commonly associated with the IT industry, as large business and government organizations dominated the early decades of computer usage and development. Thus the microcomputer revolution, in which electronic computing moved from exclusively enterprise and government use to include personal computing, is a cardinal example of consumerization. But many technology-based products, such as calculators and mobile phones, have also had their origins in business markets, and only over time did they become dominated by high-volume consumer usage, as these products commoditized and prices fell.

La définition nous décrit que la consumérisation est le plus souvent associée à l'industrie informatique.

Selon le cabinet Gartner[7], cette tendance remonte au moment où la bulle Internet a éclaté. Les budgets informatiques des entreprises ont été réduits et de nombreux fournisseurs informatiques se sont tournés vers un marché de l'informatique grand public potentiellement plus grand.

La tendance, des grandes entreprises et des organismes gouvernementaux à dominer les marchés des nouvelles technologies, s'est inversée. Les marchés traditionnels acquièrent souvent de nouvelles technologies avant d'entrer dans l'entreprise.

[7] Gartner est le leader mondial de la recherche et du conseil.

D’après la définition du site « riff.org » (2), la consumérisation est apparue dans les années 2000.

Tendance du marché informatique observée depuis les années 2000 à un renversement des priorités économiques : là où l’informatique du vingtième siècle était créée dans les laboratoires pour les usages militaires et professionnels, puis évoluait vers le marché domestique, la tendance « IT Consumerisation » voit des produits créés initialement pour les utilisateurs domestiques (téléphones, cartes vidéo) être rétroactivement adaptés au marché professionnel.

La consumérisation de l’informatique reflète l’adoption des matériels à usage privé par le monde professionnel, appelé le BYOD.

II. Le Cloud

Le cloud est le parfait exemple de consumérisation de l’informatique. Ci-dessous, la définition du site Wikipédia sur le cloud (3) :

Le cloud computing, en français l'informatique en nuage, consiste à utiliser des serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet, pour stocker des données ou les exploiter.

Le cloud se résume à l’utilisation de ressources informatique à distance.

Le cloud computing se caractérise par sa grande souplesse : selon le niveau de compétence de l'utilisateur client, il est possible de gérer soi-même son serveur ou de se contenter d'utiliser des applicatifs distants.

Le cloud démocratise, facilite et simplifie l’utilisation de l’informatique dans tous les domaines.

Les principaux services proposés en cloud computing sont le SaaS (Software as a Service), le PaaS (Platform as a Service) et le IaaS (Infrastructure as a Service). En fonction du service, les systèmes d'exploitation, les logiciels d'infrastructure et les logiciels applicatifs seront de la responsabilité soit du fournisseur soit du client.

La représentation graphique des responsabilités des modèles de service du cloud de Wikipédia est très explicite :

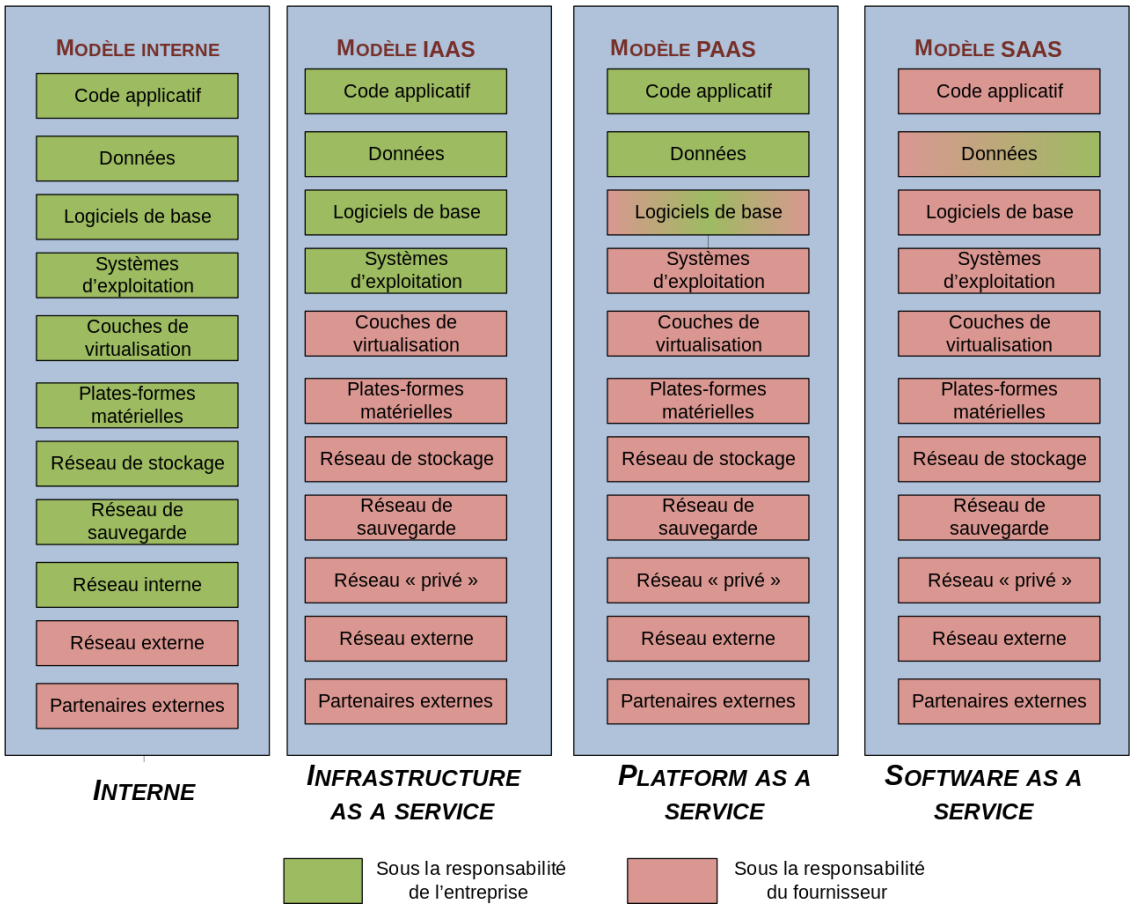


Figure 2. – Cloud : les différents modèles de service

L'offre SAAS [8] est la fourniture de logiciel ou d'application en ligne. Les données sont sous la responsabilité de l'utilisateur et du fournisseur. Elle est la plus connue et accessible par tout le monde. Les solutions « O365 » de Microsoft et « GoogleApps » de Google sont des applications SaaS.

L'offre PAAS[9], c'est la fourniture d'une plateforme de développement d'applications en ligne comme « GoogleApp engine » de Google. Elle est destinée à des personnes avec un profil informatique, comme les développeurs.

L'offre IAAS[10] est la fourniture d'infrastructures de calcul et de stockage en ligne tel qu' « Amazon Web service » d'Amazon. Elle est orientée vers les personnes avec un profil informatique tels que les administrateurs systèmes et réseaux.

[8] Software as a Service
[9] Platform as a Service
[10] Infrastructure as a Service

Ces différents modèles peuvent se déployer et s'utiliser de différentes façons :

- « **Public** » quand un service est partagé et mutualisé entre de nombreux clients, les ressources sont mises à disposition par des fournisseurs depuis leurs plateformes Cloud respectives. Ils délivrent de la capacité informatique comme un service, la partageant avec plusieurs utilisateurs en fonction de leurs besoins. Favorisant les économies d'échelle, le Cloud public est le modèle le plus accessible.
- « **Privé** » quand le Cloud est dédié à un client. Celui-ci peut choisir de gérer le Cloud en interne lui-même, ou charger un fournisseur externe de lui délivrer les ressources d'un Datacenter[11].
- « **Communautaire** » quand le Cloud est partagé par plusieurs entreprises qui ont des intérêts communs.
- « **Hybride** » quand un service est partiellement dans un Cloud public et partiellement dans un Cloud privé. Dans ce cas, nous considérons que le service peut être étudié comme deux traitements interconnectés.

D'après une étude de Markess by exaegis[12] (4), le marché français du cloud a augmenté de 20% pour atteindre les 12 milliards d'euros en 2019. Avec un franc succès pour le cloud public. Peu d'entreprises ont fait part de leur volonté de migrer l'intégralité de leurs systèmes informatiques vers le cloud public comme Veolia.

La moyenne de l'objectif est de 48% pour 2020, révèle Emmanuelle Olivié-Paul. Pour 25% des entreprises interrogées, l'objectif atteint même 75%.

Les systèmes d'informations des entreprises ne sont plus cloisonnés en interne. Ils s'ouvrent vers l'extérieure.

La démocratisation du cloud, par sa simplicité et son agilité, touche le grand public les entreprises et leurs employés. La consumérisation de ces nouvelles applications est la cause de nouvelles tendances au sein des entreprises. L'utilisation de matériels privés s'étend aux logiciels. Le BYOD se décline en BYOA[13].

[11] Centre de données basique regroupant des ressources informatiques
[12] Société d'études indépendante spécialisée dans l'analyse des marchés du numérique
[13] Bring Your Own Applications

III. L'évolution des systèmes d'information

Le système d'information a été touché par la consumérisation, modifiant son mode de fonctionnement. La Direction des services informatiques n'est plus la seule avec les connaissances nécessaires pour l'exploiter. Benoît FILOCAMO représente dans son ouvrage le mode de fonctionnement classique d'un système d'information avant l'arrivée du cloud et de la consumérisation (5).

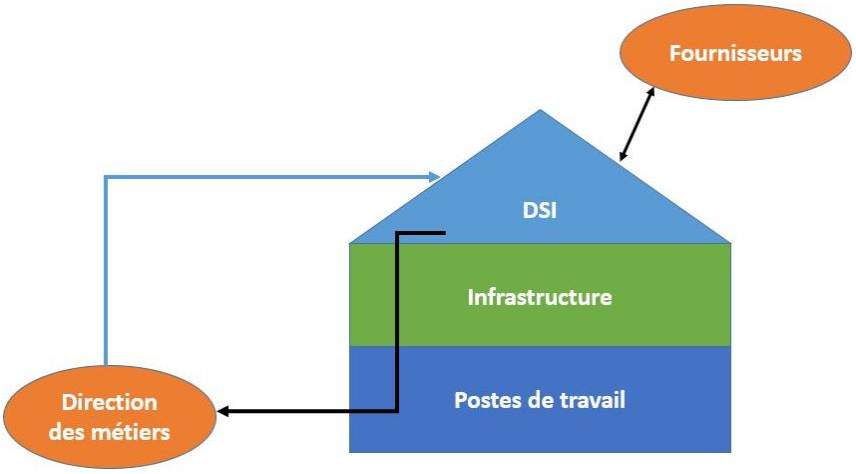


Figure 3. – SI : Mode de fonctionnement classique

Les métiers n'ayant pas la connaissance étaient tributaires de la direction des services informatiques pour leurs demandes. Les fournisseurs échangeaient uniquement avec la DSI.

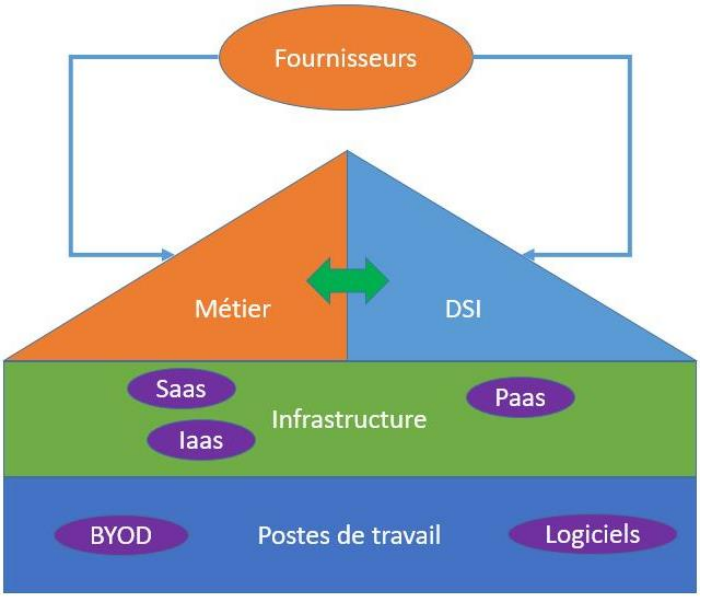


Figure 4. – SI : Mode de fonctionnement après le cloud et la consumérisation

Extraie du même ouvrage, cette représentation graphique montre l'évolution du système d'information après l'arrivée des solutions cloud et de la consumérisation.

Les fournisseurs s'adressent directement aux services métiers et à la direction des services informatique. Le marché « Business to Business » évolue en « Business to Consumer ».

Les métiers deviennent consommateurs de produits flexibles et agiles répondant à leur besoins. La DSI ne peut pas concurrencer leur rapidité de mise en place et leur agilité.

De nouveaux logiciels SaaS intègrent le système d'information comme Google drive, Dropbox, Discord, Slack ou des solutions IaaS proposées par OVH et Amazon.

La DSI n'a pas forcément conscience de ces applications. Par conséquent, l'utilisation de ces solutions fantômes et leurs sécurités n'ont pas été validées. Cet usage alimente le Shadow IT.

La société IDC[14] a mené une étude auprès d'une centaine de services informatiques et décideurs en 2016 pour comprendre le taux d'allocation budgétaire des projets informatiques dans l'entreprise (6). IDC a identifié 5 situations de mise en œuvre de projets informatiques :

- **Financés et gouvernés par l'IT seul**. Les DSI financent les projets à partir des budgets informatiques alloués par l'entreprise et sont gouvernés en intégralité par la direction informatique.
- **Financés par l'IT et gouvernés conjointement par l'IT et les métiers**. Dans ce contexte, les métiers prennent part à la mise en place du projet informatique et participent à la définition des besoins, au bornage des frontières du projet, au suivi des étapes etc
- **Financés par les métiers, gouvernés conjointement par l'IT et les métiers**. Dans cette situation, chaque direction métier gère les coûts du projet en fonction des budgets dont elle dispose.
- **Financés et gouvernés par les métiers, sans le concours de la DSI**. Ce contexte ne correspond pas à ce qu'IDC qualifie de Shadow IT, dans la mesure où les directions informatiques restent conscientes de la mise en place des projets.
- **Enfin, financés et gouvernés par les métiers sans le concours de la DSI**, et sans que celle-ci n'en soit informée. IDC qualifie alors ce contexte de Shadow IT.

[14] International Data Corporation (IDC) est le premier groupe mondial de conseil et d'études sur les marchés des technologies de l'information

Dans ce sondage, les directions métiers et les directions des services informatiques devaient répondre à cette question :

Pouvez-vous répartir votre rôle dans le financement et la gouvernance des projets IT ?

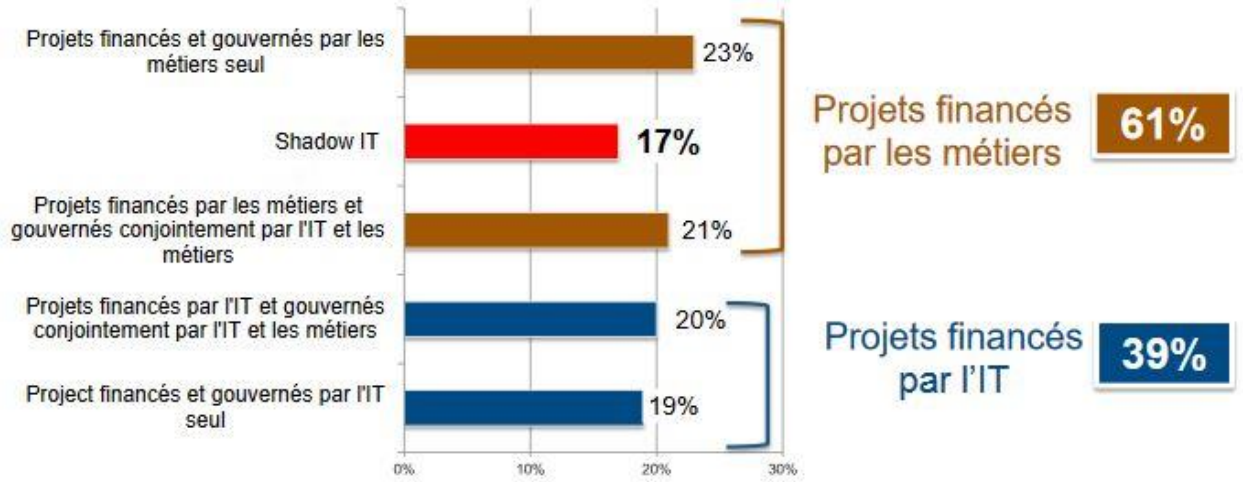


Figure 5. – Projets informatiques : Participation aux projets

L'étude a montré que la consumérisation a bien affecté le mode de fonctionnement des systèmes d'information. Seulement 39 % des projets sont financés par le département informatique contre 61% pour les services métiers.

Parmi tous les projets, le département informatique n'a pas conscience de 17% d'entre eux. Ces projets fantômes engendrent des risques pour l'entreprise et sont qualifiés de Shadow IT.

IV. RGPD

Pour définir le RGPD[15], je vais m'appuyer sur la définition du site Wikipédia (7) :

> Le règlement no 2016/679, dit règlement général sur la protection des données (RGPD, ou encore GDPR, de l'anglais General Data Protection Regulation), est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

Ce nouveau règlement concerne les données à caractère personnel des citoyens européens. Une donnée à caractère personnel permet d'identifier une personne, comme son nom, son numéro de téléphone, sa plaque d'immatriculation, son numéro de sécurité sociale, etc.

> Après quatre années de négociations législatives, ce règlement a été définitivement adopté par le Parlement européen le 27 avril 2016. Ses dispositions sont directement applicables dans l'ensemble des 28 États membres de l'Union européenne à compter du 25 mai 2018.

Le parlement européen a laissé deux ans aux entreprises traitant des données personnelles de citoyens européens pour se mettre en conformité.

> Ce règlement remplace la directive sur la protection des données personnelles (95/46/CE) adoptée en 1995 (article 94 du règlement).

C'est une grande évolution de la législation informatique européenne.

> Les principaux objectifs du RGPD sont d'accroître à la fois la protection des personnes concernées par un traitement de leurs données à caractère personnel et la responsabilisation des acteurs de ce traitement. Ces principes pourront être appliqués grâce à l'augmentation du pouvoir des autorités de contrôle

Le RGPD responsabilise les entreprises et leur traitement des données personnelles sous peine de sanction financière allant jusqu'à 4 % du chiffre d'affaires annuel mondial.

L'organisation des DSI évolue par ce règlement en intégrant un délégué à la protection des données (DPO[16]). Il est chargé d'accompagner et de conseiller son organisation dans sa conformité.

[15] Règlement Général sur la Protection des Données
[16] Data Protection Officer

Le concept « GDPR-READY » fait son apparition dans la course à la conformité.

Le GDPR-READY fait référence au règlement européen vis-à-vis des applications Cloud. Il indique le respect des niveaux de sécurité des données et de contrôle sur la confidentialité.

Le rapport de l'entreprise Netskope[17](8), au cours du premier trimestre de 2017 sur l'utilisation et les tendances des applications Cloud en entreprise, indique que plus de 75 % de ces solutions ne sont pas GDPR-READY.

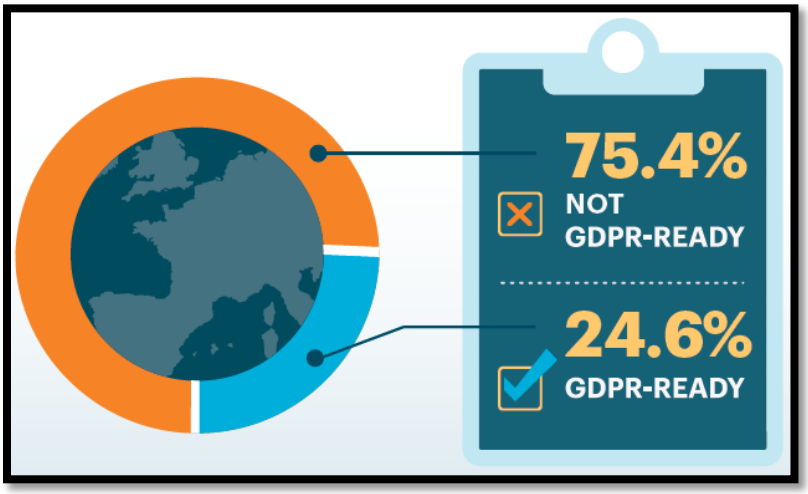


Figure 6. – Applications Cloud : GDPR-READY

Parmi ces applications non conformes :

- **11.6** % ne prennent pas en charge l'exportation des données à la fin du service.
- **46.4** % conservent les données plus longtemps qu'une semaine à la fin du service
- **62.3** % ne précisent pas que le client est propriétaire des données dans leurs conditions de service

Les employés ont utilisé, en moyenne, 935 applications dans le cloud. Les applications marketing sont en tête suivie par les applications collaborative et comptable.

Avec le RGPD, les entreprises doivent découvrir les applications Cloud utilisées dans leur organisation et s'assurer que ces applications répondent aux exigences du règlement.

[17] Leader dans la sécurité du cloud

V. Problématique

Le but de cette thèse est d'aider les entreprises face au Shadow IT et de limiter son utilisation.

La problématique qui s'en dégage est la suivante :

« **Quels sont les moyens et méthodes nécessaires afin de limiter l'adoption du Shadow IT dans l'entreprise**? »

.

Résumé des informations importantes

• La consumérisation de l'informatique génère le Shadow IT.
• Le cloud a démocratisé les applications et les connaissances informatiques.
• La consumérisation et le cloud ont modifié le mode de fonctionnement de nos systèmes d'information :
  ○ Perte de la dominance de la DSI sur le SI.
  ○ Les métiers ont les connaissances et le budget.
  ○ Évolution du marché en « Business to Consumer ».
 	
• 61% des projets IT sont financés par les services métiers
  ○ Dont 17% sont du Shadow IT
  ○ Dont 23% sont financés et gouvernés par les métiers
• Toutes les données pouvant être liées directement ou indirectement à un citoyen européen sont considérées comme des données personnelles.
• 75 % des applications Cloud en 2017 ne sont pas GDPR-READY
• Problématique : Quels sont les méthodes et moyens nécessaires afin de limiter l'adoption du Shadow IT dans l'entreprise?

Tableau 1. – Concepts et notions : infos clé

Si l'on cherche sur Google le terme « Shadow IT », on obtient 1 490 000 000 résultats. Il est important de bien le définir et le comprendre.

Il est difficile de déterminer la naissance exacte de ce concept. Le terme français le plus courant pour le Shadow IT est «l'Informatique de l'ombre». En informatique, nous empruntons le terme des anglo-saxons.

Quand vous vous promenez votre ombre vous suit, c'est similaire avec l'informatique et le Shadow IT, Ils sont indissociables. Le Shadow IT est produit par l'informatique. Et plus avez d'éléments informatiques, plus votre ombre est grande.

Pour l'ombre, le site Wikipédia (9) nous donne la définition suivante :

> Une ombre est une zone sombre créée par l'interposition d'un objet opaque entre une source de lumière et une surface qu'éclaire cette lumière. Elle se matérialise par une silhouette sans épaisseur.
>
> L'ombre propre d'un objet est la partie que la lumière principale n'atteint pas en plein, et qui est donc plus sombre. L'ombre portée est la partie d'un autre objet que celui qui fait écran prive de lumière.

Cette définition nous indique qu'une ombre est générée par trois acteurs :

- Une source de lumière
- Un objet
- Une surface de projection

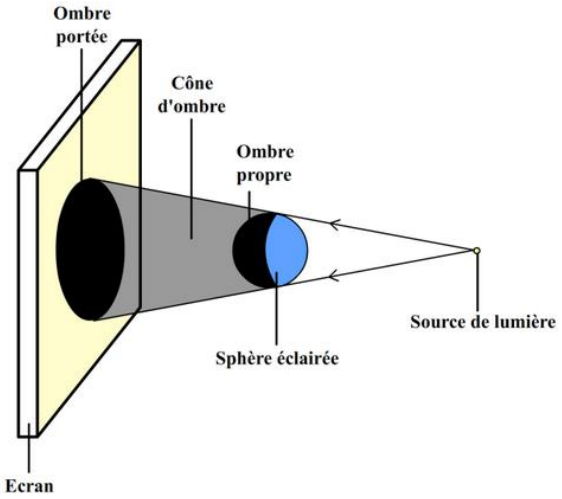


Figure 7. – Représentation de l'ombre

Afin de pouvoir transposer l'ombre sur l'informatique, nous devons le définir. L'informatique en entreprise se désigne par le terme « système d'information ».

Le site itsocial.fr (10) nous donne la définition suivante :

> Le système d'information (SI) c'est l'ensemble des ressources de l'entreprise qui permettent la gestion de l'information. Le SI est généralement associé aux technologies (matériel, logiciel et communication), aux processus qui les accompagnent, et aux hommes qui les supportent. D'abord simplement appelé informatique, cet ensemble a pris le nom de SI avec l'arrivée des nouvelles technologies qui ont élargi son domaine.

L'informatique en entreprise est un outil de travail qui permet de traiter l'information. Elle est utilisée par les employés de l'entreprise et gérée par la DSI.

Avec ces deux définitions, nous pouvons interpréter l'ombre sur l'informatique en entreprise :

- Les sources de lumière sont les utilisateurs du système d'information, les employés.
- L'objet est représenté par le système d'information de l'entreprise.
- La surface de projection devient l'entreprise.

L'informatique de l'ombre ou Shadow IT est la zone d'ombre qui se projette sur l'entreprise.

Je vais dans un premier temps définir le Shadow IT en informatique, puis ses différentes appellations afin d'identifier ses caractéristiques. Ensuite, je vous présenterai les recherches et études pertinentes sur le sujet. En conclusion, je finirai avec mes hypothèses.

I. Définition

Plusieurs sources donnent des définitions constructives sur le Shadow IT.

Celle de Technopédia.com (11), nous donne :

> Shadow IT is used to describe IT solutions and systems created and applied inside companies and organizations without their authorization. This is considered a vital foundation for technological advancement and innovation because these efforts can become potential prototypes for IT solutions that are approved in the future. Even though these solutions can help in the advancement of IT innovations, they may not conform to the company's requirements in terms of reliability, documentation, control, security and more.

Cette définition nous précise, tout d'abord, le périmètre et le lieu de vie du Shadow IT.

Les solutions et les systèmes informatiques représentent le périmètre; l'entreprise et l'organisation sont le lieu de vie du Shadow IT.

On remarque la notion d'autorisation mais elle n'est pas clairement ciblée.

Dans la définition de Wikipédia ci-dessous (12), on constate des précisions :

> Shadow IT (parfois Rogue IT) est un terme fréquemment utilisé pour désigner des systèmes d'information et de communication réalisés et mis en œuvre au sein d'organisations sans approbation de la direction des systèmes d'information.

La direction des systèmes d'information est responsable du système d'information et de sa gouvernance, elle le gouverne. La direction de l'entreprise a délégué ces responsabilités à la DSI. Le Shadow IT est une application ou solution informatique inconnue de la DSI.

Dans sa version anglaise, Wikipédia apporte un complément d'information (13) :

> Some people consider shadow IT an important source of innovation, and such systems may become prototypes for future approved IT solutions. On the other hand, shadow IT solutions are not very often in line with organizational requirements for control, documentation, security, reliability, etc.

Le Shadow IT pourrait être un facteur de développement de l'innovation mais il génère des données incompatibles avec les lois ou les modèles de gouvernance en vigueur dans les entreprises.

Est-ce que le Shadow IT est une menace ou une opportunité ? C'est une question qui divise le monde des entreprises.

Une source universitaire complémentaire provenant de Konstanz (14), où le professeur Rentrop et Stefan Zimmerman, nous donnent la définition suivante :

The term Shadow IT describes business process supporting IT Systems, IT service processes and IT staff that are used independently within businessdepartmentsandby ITusers. Thereby, theShadow-IT entities are involved neither technically nor strategically in the IT service management of the organization and, therefore, neither included in the asset and configuration management nor in the service portfolio.

Ils expliquent que c'est un acte technologique opérant hors de la stratégie de l'entreprise. Ils précisent également que ces solutions ne font pas partie des éléments référencés dans le SI ou le catalogue de services de l'entreprise.

Je vais synthétiser, ci-dessous, mes analyses.

Résumé des informations importantes
Le service informatique appelle ce concept le Shadow IT. Il représente l'utilisation d'applications, de solutions, de technologies ou de matériels sans la validation de la direction des systèmes d'information. Il n'est pas référencé dans le système d'information de l'entreprise. Il est parfois considéré comme encourageant pour l'innovation mais génère des sources de menaces.

Tableau 2. – Définition : Infos clé

II. Terminologies

Il existe d'autres terminologies pour désigner le Shadow IT, même si c'est le terme le plus couramment utilisé. Nous utiliserons la désignation Shadow IT dans cette thèse.

Shadow System

Le terme « Shadow System » est ancien, il date des années 2000. On le retrouve dans des travaux de recherche comme par exemple « *Why Shadow Systems exist after an ERP implemantation* » de Sandy BEHRENS et Wasana SEDERA paru en 2004 (15).

Il fait référence aux solutions informatiques qui subsistaient alors que les entreprises venaient de mettre en place un ERP[18]. Cette terminologie est moins vaste que le Shadow IT car elle désigne uniquement cette pratique. Il est très rare aujourd'hui d'utiliser ce terme.

Invisible IT

Le terme « Invisible IT » ne désigne pas le Shadow IT. Il représente l'informatique informelle en entreprise qui n'est ni tracée ni répertoriée. Par exemple, une demande faite à la machine à café ou dans un couloir qui n'est pas traitée de façon officielle.

Cette pratique est réelle en entreprise mais ne concerne pas le Shadow IT.

[18] Enterprise Resource Planning

Rogue IT et Stealth IT

Ces terminologies sont les plus populaires après le Shadow IT.

Le terme «rogue IT» signifie en français «informatique de voyou». Il est parfois utilisé pour soutenir le Shadow IT et pour souligner les critiques de cette approche. Il accuse des comportements qui ne respectent pas les règles.

Le terme « Stealth IT » ou « informatique furtive » associe les utilisateurs de cette pratique à des ninjas en entreprise. Les employés se transforment en ninjas armés de matériels Shadow IT. Cette représentation humoristique du Shadow IT est utilisée par la société wikibon.org, vous la trouverez en annexe [2].

Résumé des informations importantes
• Le terme Shadow IT est le plus couramment utilisé • Rogue IT et Stealth IT sont des synonymes

Tableau 3. – Différentes terminologies : infos clé

III. Caractéristiques

1. Notoriété

Une analyse avec Google trends permet de se rendre compte de la notoriété du Shadow IT dans le monde depuis 2004.

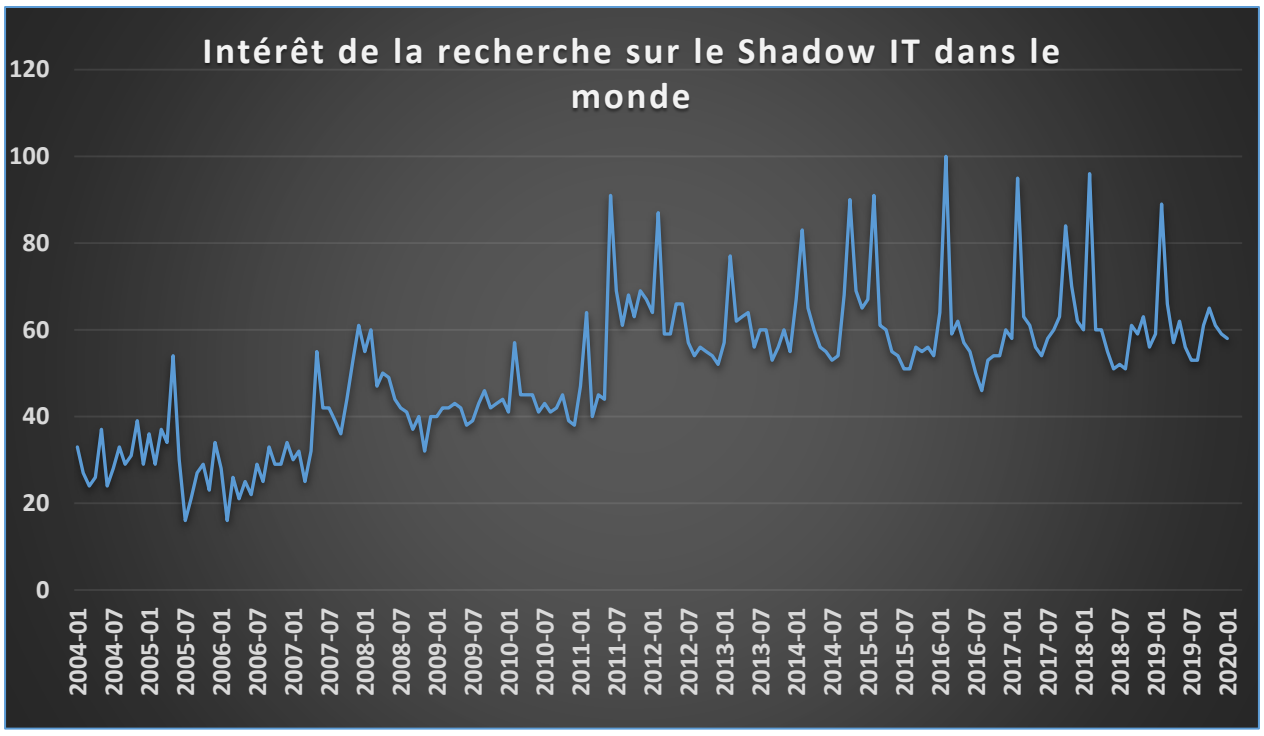


Figure 8. – Google trends : Intérêt de la recherche sur le Shadow IT dans le monde

La courbe se résume en des pics d'intérêts successifs qui correspondent à l'apparition de travaux de recherche. Le terme n'est pas beaucoup demandé en 2004. Il y a un premier pic d'intérêt en 2005 puis un second en 2007.La demande va progressivement croitre jusqu'à son pic de 2011. La plus grande demande fut pendant l'année 2016. Sa notoriété n'est pas à la hauteur de sa popularité en entreprise.

2. Travaux de recherches

Durant mes recherches, j'ai trouvé plusieurs études sur le Shadow IT.

Le professeur Rentrop et Stefan Zimmerman ont effectué plusieurs recherches sur le sujet durant ces dernières années. Ils sont considérés comme des experts dans ce domaine.

Leur première étude se nomme « Shadow IT » et date de 2010. Elle fournit une méthode pour le management du Shadow IT. De leur étude précurseuse a découlé les travaux suivants :

- En 2012 : « Shadow IT – Management and control of unofficiall IT » (16) et « Shadow IT Evaluation model » (17).
- En 2014 : « On the Emergence of Shadow IT – A Transaction Cost-Based Approach » (18).
- En 2015 : « Managing Shadow IT instances – A method to control autonomous IT solutions in the business departements » (19).
- En 2016 : « Governing Identified Shadow IT by Allocating IT Task Responsibilities » (20).
- En 2017 : « The Influence of Shadow IT Systems on Enterprise Architecture Management Concerns » (21).
- En 2018 : « Shadow IT and Business-Managed IT: A Conceptual Framework and Empirical Illustration » (22) et « Conceptualizing Shadow IT Integration Drawbacks from a Systemic Viewpoint » (23).

Une étude de chercheurs suisse, « Exploring the Shadow : IT governance approaches to user-driven innovation » (24) parue en 2012, parle de l'innovation générée par les utilisateurs et le Shadow IT comme de la gouvernance pour la gérer.

Le Shadow IT fut le sujet de plusieurs thèses pour les étudiants. La thèse professionnelle en 2013 de Thomas Chejfec, « Shadow It de la menace à l'opportunité » (25), aborde le sujet en opposant la vision des services métiers à celle de la direction informatique.

Celle de Benoît FILOCAMO en 2016, « Shadow IT dans nos entreprises : Transformer la gouvernance de son SI afin d'en contrôler l'influence » (5), propose une démarche en trois étapes afin d'améliorer la gouvernance face au Shadow IT.

La publication de la thèse de Lucas et Emerich Imbart en 2018, « Digitalisation : nouvelle source de Shadow IT ? Comment la gérer ? » (26), introduit le citoyen développeur et le système d'information 3-tiers dans la gouvernance de l'entreprise pour limiter le Shadow IT.

En regardant les dates de parution de ces études, on remarque qu'elles correspondent aux pics d'intérêts sur la Figure 7 à la page 30.

3. Causes

Dans un monde et un marché en constante évolution, les services métiers sont amenés à être plus rapide, plus réactifs et plus compétitifs.

Comme vu précédemment, l'évolution des systèmes d'information a modifié leurs organisations et le comportement de ces utilisateurs. D'après une étude de Frost & Sullivan[19](27) en 2017, 80% des employés interrogés passent par le Shadow It.

Une liste des plus grandes raisons d'utilisation du Shadow IT est fournie par l'étude de Landesk[20] (28) :

1 : Easier to get technology from an app store or SaaS-based service (73%)

2 : IT doesn't have the specific solution expertise (44%)

3 : Certain teams or departments have technical expertise to implement technology solutions (41%)

4 : Business units have the budget to spend on whatever they need (22%)

5 : IT can't meet a department timeline due to IT resource constraints or procurement (9%)

On remarque que la facilité d'accès aux services Cloud SaaS est la première raison de ce classement. Le changement de stratégie des fournisseurs, Business to Customer, est bien réel.

[19] Frost & Sullivan est une société de recherche et de conseil
[20] LANDESK est un leader de la gestion des systèmes IT

L'expertise du département informatique est considérée comme insuffisante en deuxième place. Les personnes interrogées considèrent à 44% que leur DSI ne peut pas répondre à leurs besoins.

Le budget et le marché permettent aux services métiers, en quatrième place, d'utiliser des solutions Shadow IT. L'association ISACA[21], dans son livre blanc « Shadow IT Primer »(29) réagit à cette situation en disant :

> Aujourd'hui, les coûts d'accès à la technologie ont ouvert une voie royale au Shadow IT

Alan McSweeney, lors de sa présentation « Shadow IT And The Failure Of IT Architecture » (30) en 2019, représente la relation entre le service informatique et les services métiers par l'illustration suivante :

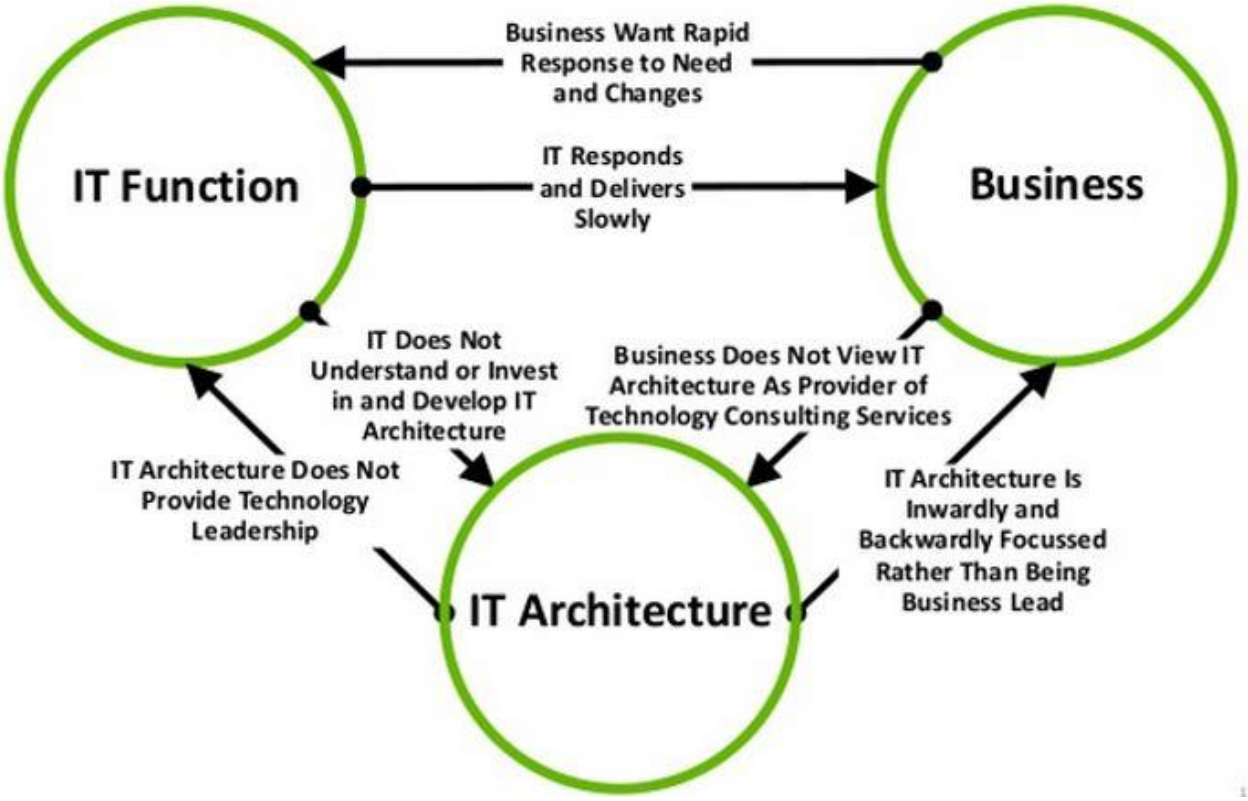


Figure 9. – SI : La relation entre le service informatique et les métiers

Les relations entre le service informatique et les services métiers se sont progressivement compliquées. La complexité des architectures des SI des entreprises, l'apparition du cloud et les besoins urgents des services métiers ont favorisé l'apparition du Shadow IT.

[21] L'ISACA est une association professionnelle internationale dont l'objectif est d'améliorer la gouvernance des systèmes d'information

Résumé des informations importantes
• La notoriété du Shadow IT n'est pas à la hauteur de sa popularité en entreprise • Des solutions informatiques sont utilisées sans l'aval de la DSI • Ce concept existe depuis longtemps et explose lors de l'apparition du Cloud • L'expertise de la DSI est considérée comme insuffisante • La rigidité de la DSI favorise le Shadow IT • Le marché exerce une pression sur les métiers

Tableau 4. – Caractéristiques du Shadow IT : infos clé

IV. Pratiques du Shadow IT

Au cours des parties précédentes, nous avons énoncé les acteurs du shadow :

- Les métiers, consommateurs principaux du shadow IT
- Les directions des systèmes d'information subissant le phénomène.
- Les fournisseurs de solutions informatiques avec le Business to Customer

Frédéric Hay, lors de son webinaire « Identifier et traiter le Shadow IT » (31), classifie les ressources du shadow IT par le tableau suivant :

Cas 1 à 4	Perso	Métiers	
		Usage interne uniquement	**Avec sorties de données**
1 Applications métiers		Application utilisateur Application achetée	Souscription SaaS Transfert de fichiers Support éditeur
2 Autres applications	Application de jeu Addon Navigateur	Addon navigateur	Drive
3 Matériels	NAS Streaming Téléphone Objets connectés Ordinateur/tablette	App sur téléphone perso	Email pro sur tel perso Box internet utilisateur
4 Service		Assistance sur site	Assistance à distance (VPN,PMAD)

Tableau 5. – Classification des ressources Shadow IT

On remarque que le BYOD est présent dans les ressources. Le support et les départements informatiques des fournisseurs sont aussi acteurs du Shadow IT avec leurs assistances.

Par exemple, l'armée américaine est revenue sur ses positions concernant le BYOD particulièrement sur la montre connectée utilisant l'application Strava[22]. En 2013, l'armée a lancé une campagne de fitness pour ses soldats à l'aide de ses montres connectées. Strava, fin 2017, publie une carte montrant le mouvement de ses usagers dans le monde entier. Cette publication dévoile les bases et les déplacements en zone de guerre de l'armée. L'armée a changé depuis sa politique sur les objets connectés et le BYOD en les interdisant.

Un autre exemple, une collectivité fut victime d'un consultant externe, prestataire « utilisateur » d'un de leur site distant. Il a modifié les mots de passe administrateur des machines, bloquant toute intervention de la DSI.

1. Conséquences

La compétitivité d'une entreprise est vitale. La mesure constante des performances des employés exerce une énorme pression. Les employés se tournent alors vers des applications plus flexibles et plus rapides à mettre en place qu'avec leur DSI, entrainant une augmentation du Shadow IT.

Thomas Chejfec dans son rapport, « résultats de l'enquête sur le phénomène du « Shadow IT » (32), illustre la dangerosité du Shadow IT :

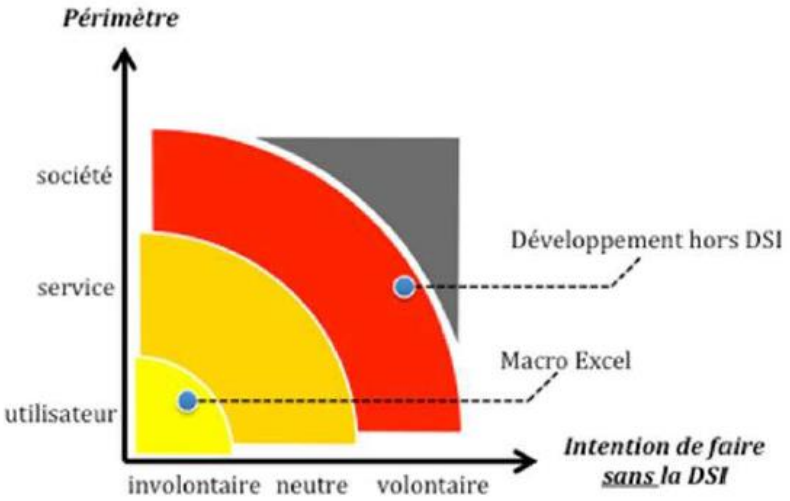


Figure 10. – Dangerosité du Shadow IT

L'illustration représente la dangerosité du Shadow IT pour l'entreprise en fonction de l'intention et du périmètre du consommateur.

[22] Strava est un site internet et une application mobile utilisée pour enregistrer des activités sportives via GPS

Un utilisateur non informé pratiquant le Shadow IT involontairement, avec une macro Excel, représente une dangerosité faible. A l'opposé, un service métier utilisant une application SaaS volontairement est extrêmement dangereuse pour l'entreprise.

L'intention et la sensibilisation des employés sont à prendre en compte dans le traitement du Shadow IT. La DSI doit être capable de répondre aux besoins des métiers avec efficacité pour limiter le Shadow IT. Selon une étude de Vanson Bourne[23] (33), l'innovation informatique est de plus en plus prise en charge par les métiers, pénalisant les directions des systèmes d'information.

L'étude européenne indique que 58% des personnes lancent de nouveaux produits et services plus rapidement de cette manière, tandis que 63% pensent que cela peut promouvoir l'innovation. Elle souligne également que cela permet à 57% des répondants de s'adapter plus efficacement au développement du marché. Les deux dernières raisons sont la satisfaction des employés à 56% et attirer des talents plus qualifiés à 56%.

Cependant, les répondants sont également conscients des limites de cette approche. Premièrement, la perte de contrôle et de responsabilité sur la technologie utilisée à 51% et l'augmentation des dépenses informatiques à 45%. 47% des répondants ont également mentionné l'achat d'une solution moins sécurisée. Les équipes informatiques souhaitent, à 54%, davantage de consultations et qu'elles devraient garder le contrôle sur des domaines souverains, tels que la sécurité et la conformité des réseaux.

Les entreprises renommées ont indiqué que pour leur DSI, les coûts représentaient 5% à 15% de leur budget, soit en moyenne 13 millions d'euros par an.

Le Shadow IT représente une menace réelle car il pose des problèmes de sécurité importants pour les données d'entreprise. La DSI ne peut pas suivre les données utilisées dans les applications non autorisées. Shadow IT ajoute des risques en termes de qualité, de fiabilité et de partage accidentel de données sensibles.

Shadow IT apporte un coût caché à l'entreprise, en particulier pour les licences de logiciels sous-utilisées ou même inutilisées. Les employés travaillent davantage sur d'autres applications métier et services cloud, ce qui nuit aux outils «officiels». En conséquence, le Shadow IT empêche les entreprises d'obtenir un retour sur investissement satisfaisant pour les outils commerciaux qu'elles achètent.

Shadow IT multiplie les logiciels et les applications utilisés par l'entreprise. Et plus il y a d'outils, plus les sources de conflits entre les données sont nombreuses: créer des doublons, des îlots de données, des flux d'informations entre plateformes.

La plupart des entreprises ont plusieurs règlements, lois et normes de l'industrie auxquels elles doivent se conformer. La présence de logiciels non gérés rend beaucoup plus difficile pour une entreprise de respecter ces normes.

[23] Prestataire spécialisé en études de marché

Résumé des informations importantes

• Les métiers, la DSI et les fournisseurs sont acteurs du Shadow IT
• Le Shadow IT touche toutes les entreprises et couvre un périmètre important de leur système d'information
• Des utilisateurs non informés utilisent le Shadow IT
• Le Shadow IT entraine :
  ○ Des augmentations budgétaires
  ○ Une perte de contrôle de la DSI
  ○ Une perte de temps de la DSI via la détection et des utilisateurs avec les conflits
  ○ Une augmentation des risques de sécurité et de perte de données
  ○ Des non-conformités et des amendes

Tableau 6. – Pratiques du Shadow IT : infos clé

V. Perception vs réalité

Les entreprises, leurs employés et les particuliers ont rapidement appris à tirer parti du cloud. L'entreprise Symantec[24], identifie en 2017, plus de 22 000 applications cloud qui ont des aspects « business » et permettent le partage d'informations.

Ce rapport, « Shadow IT France 2017 » (34), indique un écart très important entre la perception et la réalité des applications Cloud au sein des entreprises.

En moyenne, les DSI estiment entre 30 et 40 applications Cloud utilisées dans leur système d'information. En réalité, c'est environ **1700** « cloudapps ». Cet écart montre l'ampleur du Shadow IT en entreprise et la perception discutable de la DSI.

Parmi les types d'applications et de services Cloud, on retrouve :

Top	Par utilisateur	Par trafic Web
1	Réseaux Sociaux	**Moteurs de recherche**
2	Moteurs de recherche	**Réseaux Sociaux**
3	Partage de fichiers	**Partage de fichiers**
4	Messagerie	**Vidéos**
5	Vidéos	Messagerie

Tableau 7. – Symantec : Top types des applications et services cloud

Les 4 premiers, moteurs de recherche, réseaux sociaux, partage de fichiers et vidéos représentent 88% du trafic total.

[24] Symantec développe des produits et solutions de sécurité aux entreprises et particuliers

Les applications et services les plus populaires sont :

Top	Par utilisateur	Par trafic Web
1	Google	Google
2	Facebook	Facebook
3	MSN	YouTube
4	Bing	OneDrive
5	Twitter	Google Drive

Tableau 8. – Symantec : Top des applications et services cloud

On confirme la présence des applications de partage de fichiers, « Drive », de Microsoft et de Google dans le Top 5.

Il est nécessaire que la DSI soit capable d'identifier l'utilisation de ses applications au sein de son organisation.

Dans son rapport sur la cybersécurité en 2016 (35), le groupe Gartner prédit :

> En 2020, un tiers des attaques réussies vécues par les entreprises porteront sur leurs ressources en Shadow IT.

Ce constat alarmant sur la cybersécurité des entreprises montre l'importance, la croissance et la dangerosité du Shadow IT. Cette menace est en deuxième position dans le rapport.

En 2019, l'entreprise Gartner conseille aux responsables de la sécurité et de la gestion des risques de mettre en œuvre une liste de dix projets pour répondre aux besoins changeants en matière de cybersécurité (36).

Dans cette liste figure, en quatrième position, la mise en place de solutions CASB[25]. Les CASB fournissent un point de contrôle pour la visibilité et la gestion des organisations qui ont adopté plusieurs applications SaaS. Ces outils permettent d'évaluer si l'organisation a le contrôle et la visibilité des données sensibles utilisées et partagées par les applications SaaS.

Face à la croissance du Shadow IT, de nouveaux outils viennent aider la DSI à le détecter :

- Les solutions CASB
- Le Digital Asset Management (DAM). Il permet aux entreprises de stocker, d'organiser, d'enrichir et de partager des ressources numériques de manière intuitive, grâce à une source centralisée et sécurisée.
- L'évolution des solutions antivirus en solutions « Endpoint Detection and Response » (EDR). C'est une catégorie d'outils et de solutions qui détectent les activités suspectes directement sur les hôtes du système d'information.

[25] Cloud access security broker

Résumé des informations importantes
• Les DSI ne détecte pas l'intégralité du Shadow IT et l'importance de ce phénomène • Les métiers consomment les applications SaaS • Le Shadow IT est la deuxième menace de cybersécurité en 2016 • En 2020, 33% des attaques réussies contre les entreprises seront liées à leurs environnements Shadow IT • Le marché de la cybersécurité voit apparaître de nouvelles solutions pour détecter le Shadow IT

Tableau 9. – Cybersécurité : infos clé

VI. Méthode d'évaluation Shadow IT

Dans son étude, « Shadow IT Evaluation model »(17), le professeur Rentrop a publié une méthode d'évaluation pour le Shadow IT. Elle permet d'évaluer la criticité du Shadow IT et ainsi définir leur priorité de traitement. Les processus utilisant le Shadow IT doivent être évalués avec les critères suivants :

- La pertinence (Relevance) : Il indique son importance et sa signification pour l'entreprise. C'est la criticité et la pertinence stratégique du processus au sein de l'entreprise.

- La qualité (Quality) : Il représente la qualité de l'instance. Il observe la qualité du logiciel ou du matériel, la qualité des données et le respect des référentiels comme ITIL[26].

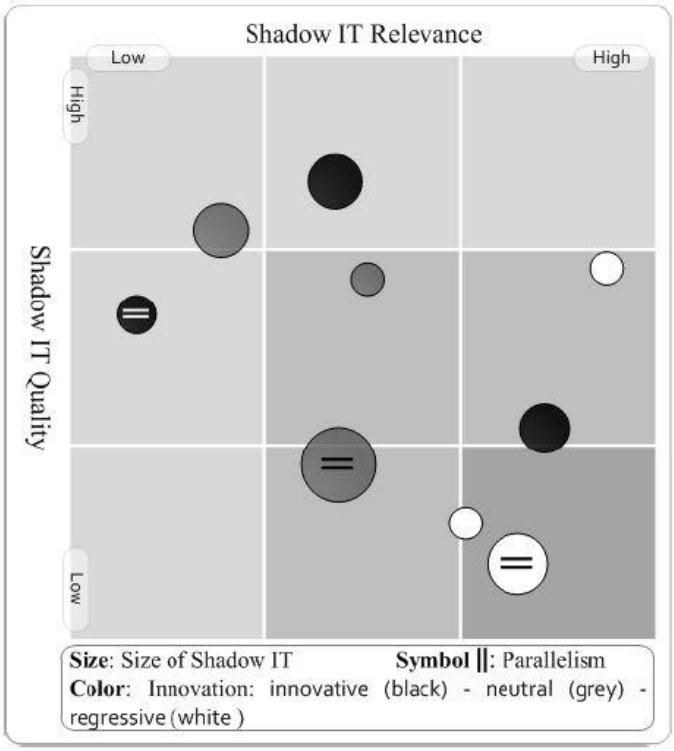
- La taille (Size) : Il représente le périmètre de l'instance. Il quantifie les personnes liées au processus.

- Le potentiel d'innovation (Innovative potential) : Il caractérise si l'instance peut être novatrice ou non dans l'entreprise.

- Parallélisme (Parallelism) : Il indique si d'autres instances ou solutions possèdent les mêmes fonctions et caractéristiques dans l'entreprise.

[26] ITIL est un ensemble d'ouvrages recensant les bonnes pratiques du management du système d'information

Ci-dessous, une représentation graphique d'instances Shadow IT :



La criticité de l'instance est à son niveau le plus bas dans le coin en bas à gauche.

Et à son niveau le plus haut dans le coin en haut à droite.

Cette méthode permet d'identifier et de traiter par priorité les instances Shadow IT mais aussi de permettre à l'entreprise d'identifier l'innovation de ses employés.

Elle nécessite en amont d'identifier tous les processus utilisant le Shadow IT.

Figure 11. – Évaluation : instances Shadow IT

VII. Hypothèses

Pour rappel ma problématique est :

« **Quels sont les moyens et méthodes nécessaires afin de limiter l'adoption du Shadow IT dans l'entreprise**? »

Suite aux parties précédentes, j'ai dégagé trois hypothèses pour répondre à ma problématique :

- Avoir une DSI possédant les capacités à répondre efficacement aux besoins métiers limite l'adoption du Shadow IT.
- Des utilisateurs/métiers avertis et conscients des risques/enjeux informatiques limitent l'adoption du Shadow IT.
- Une DSI capable de détecter et de bloquer les outils non validés par la politique de l'entreprise limite l'adoption du Shadow IT.

I. Questionnaire sur le Shadow IT en entreprise

1. Objectifs

J'ai souhaité avoir une étude de terrain concrète avec un sondage en ligne anonyme sur le Shadow IT. Cette enquête a pour but de répondre à mes questions et mes hypothèses. Vous pouvez consulter les questions du sondage en annexe [3].

Ce sondage avait plusieurs objectifs :

- Identifier la présence du Shadow IT en entreprise
- Comprendre le comportement du Shadow IT en entreprise
- Comprendre les relations du service informatique avec les métiers
- Identifier les moyens mis en place pour lutter contre le Shadow IT
- Avoir un retour d'expérience face au Shadow IT
- Comprendre la vision des services métiers.

2. Méthode

Je me suis aidé du logiciel libre « FreeMind » pour construire une carte du sondage. Il est très facile de prise en main par rapport à ses concurrents.

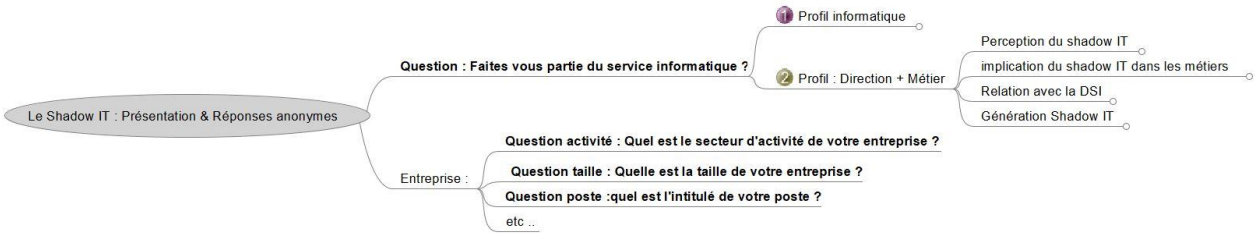


Figure 12. – Questionnaire : Mind-map

Cela m'a permis de définir rapidement des axes, profils et thématiques. La première partie du questionnaire se renseigne sur l'entreprise, le poste et l'expérience du répondant.

Elle est composée de 4 questions :

Questions	Objectifs
Question 1	Savoir la taille de l'entreprise
Question 2	Savoir le secteur d'activité de l'entreprise
Question 3	Savoir l'intitulé du poste du répondant
Question 4	Savoir l'expérience du répondant

Tableau 10. – Questionnaire : Questions génériques

Ensuite, La question numéro 5 permet d'identifier si le répondant à un profil informatique ou un profil direction/métiers

« Faites-vous partie du service informatique ? »

Un questionnaire spécifique est présenté pour :

- Les profils informatiques : questions numéro 6 à 20.
- Les profils directions et métiers : questions numéro 21 à 34.

A. Les profils informatiques

Le questionnaire, pour les profils informatiques, est composé de 15 questions avec deux thématiques.

La première thématique reflète la perception du répondant face au Shadow IT.

Questions	Objectifs
Question 6	Savoir si le répondant connait la définition du Shadow IT
Question 7	Savoir si le répondant considère le Shadow It comme une menace ou une opportunité
Question 8	Savoir quelles menaces a identifié le répondant
Question 9	Savoir si le répondant a été confronté au Shadow IT
Question 10	Avoir un exemple de Shadow IT dans l'entreprise du répondant

Tableau 11. – Questionnaire : DSI – perception du répondant face au Shadow IT

La seconde thématique concerne le département informatique avec le Shadow IT, les métiers et leurs projets.

Questions	Objectifs
Question 11	Savoir si le BYOD est pris en compte dans le management du SI
Question 12	Voir si le Shadow IT est encadré dans le management du SI
Question 13	Savoir les moyens mis en place
Question 14	Savoir les actions mises en place
Question 15	Connaître les relations entre le service informatique et les métiers
Question 16	Connaître les relations entre le service informatique et les métiers avec leurs projets
Question 17	Savoir si la DSI est systématiquement impliquée dans les projets métiers
Question 18	Savoir si la DSI a les capacités à gérer tous les projets
Question 19	Savoir si le répondant souhaite répondre à une interview
Question 20	Savoir si le répondant utilise des applications « Shadow IT »

Tableau 12. – Questionnaire : DSI – comportement du département informatique

B. Les profils directions et métiers

Le questionnaire, pour les profils directions et métiers, est composé de 14 questions avec deux thématiques.

La première thématique concerne le répondant avec sa vision et son implication sur le Shadow IT.

Questions	Objectifs
Question 21	Savoir si le répondant a été informé du Shadow IT
Question 22	Savoir si le répondant achète ou utilise des outils « Shadow IT »
Question 23	Connaître leurs fréquences d'utilisation
Question 24	Savoir le répondant communique avec des prestataires informatiques
Question 25	Connaître les raisons de cette communication

Tableau 13. – Questionnaire : Métiers – vision et implication du répondant sur le Shadow IT.

La seconde thématique concerne la communication, les relations et l'implication dans les projets entre le département informatique et les services métiers.

Questions	Objectifs
Question 26	Savoir si la DSI communique sur l'utilisation du SI
Question 27	Savoir si la DSI communique sur la sécurité du SI
Question 28	Connaître les relations entre le service informatique et les métiers
Question 29	Connaître la fréquence d'implication du service informatique dans les projets métiers
Question 30	Connaître les relations entre le service informatique et les métiers avec leurs projets
Question 31	Connaître les problèmes majeurs de la DSI
Question 32	Savoir si le BYOD est autorisé par leur manageur
Question 33	Voir si le répondant pense que les nouvelles générations sont sources de Shadow IT
Question 34	Savoir si le répondant souhaite répondre à une interview

Tableau 14. – Questionnaire : Métiers – le département informatique et les métiers

C. Moyens de diffusion

J'ai décidé ensuite d'utiliser la plateforme « Google Forms » pour la diffusion de ce sondage. Possédant déjà un compte Google, cet outil gratuit répondait à tous mes besoins.

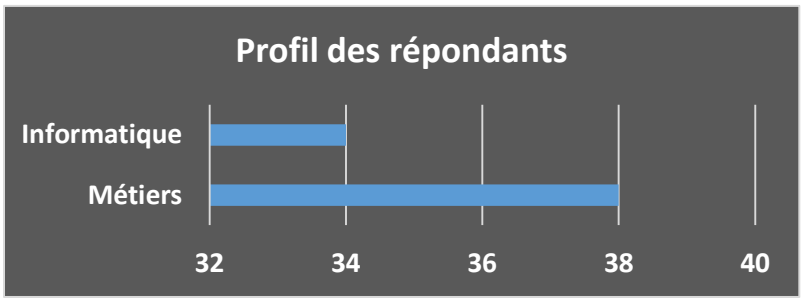
J'ai ciblé l'ensemble de mes contacts professionnels et personnels en leur demandant de le partager un maximum. Dans le but d'avoir un nombre de réponses conséquent.

Je l'ai diffusé :

- Par mail à mes collègues de travail
- Par mail à mes collègues de formation et mes connaissances du CESI de Lyon
- Sur le réseau social LinkedIn
- Sur le réseau social Facebook
- Sur le réseau social Twitter
- Par mail à mes connaissances professionnelles
- Par mail à ma famille et amis

3. Résultats du sondage

Mon sondage, avec les deux formulaires, a comptabilisé 72 réponses au total. Les graphiques ci-dessous indiquent le nombre et le pourcentage de répondants en fonction de chaque profil.



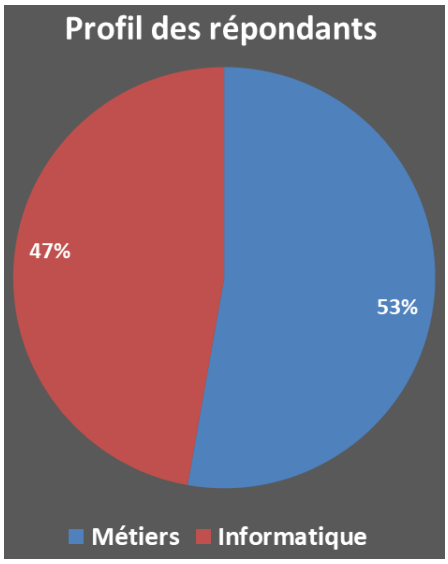


Figure 13. – Sondage : Nombre de réponses par profil

Les services métiers sont les plus nombreux à avoir répondu au sondage. Je présenterai tout d'abord les résultats de la partie générique du sondage. Dans une seconde partie, j'interpréterai les résultats en fonction de ma problématique et de mes hypothèses

A. Les répondants et leur entreprise

J'ai voulu savoir dans ce questionnaire, la taille des entreprises des répondants.

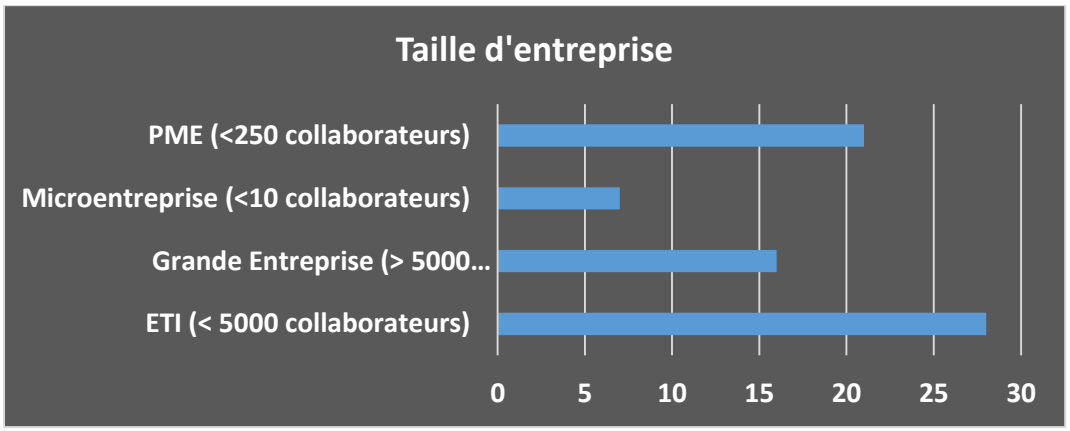


Figure 14. – Sondage : Taille des entreprises

J’ai obtenu des réponses de tous les types d’entreprises. Je vais pouvoir connaitre l’importance du Shadow IT dans chacune d’elles.

Il y a 13 secteurs d’activité qui ont participé au sondage. Le secteur de « l’informatique / Télécoms » est majoritaire suivi du secteur de la « Santé ».

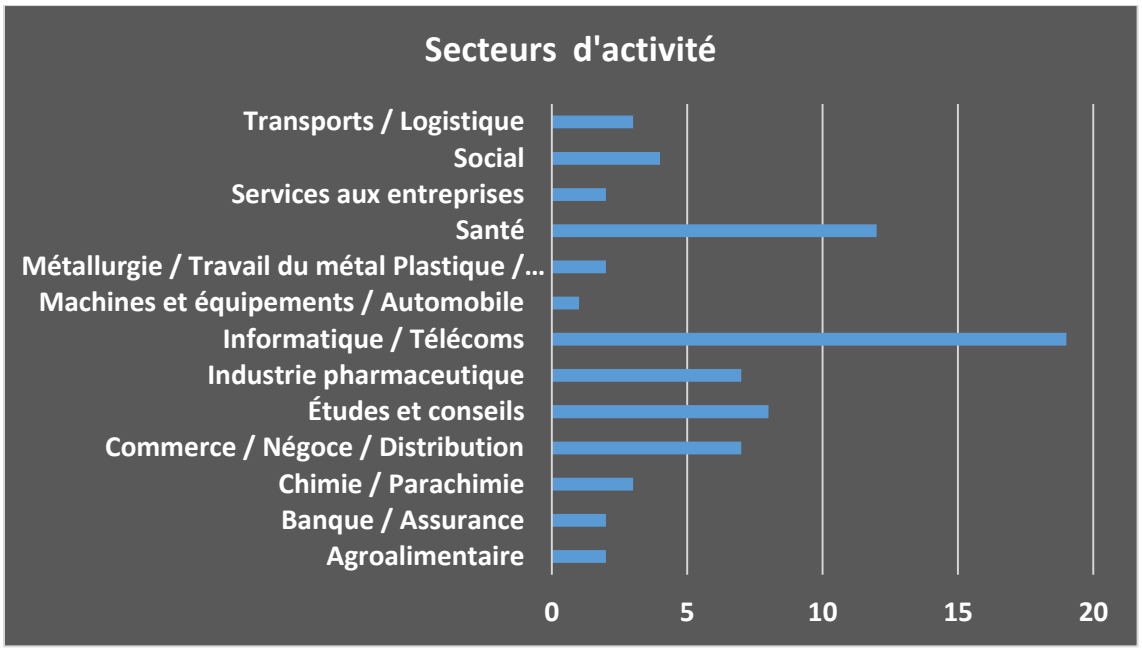


Figure 15. – Sondage : Secteurs d’activité

J’ai souhaité savoir l’expérience des répondants au poste qu’ils occupent. Une personne expérimentée connaît son entreprise et son travail.

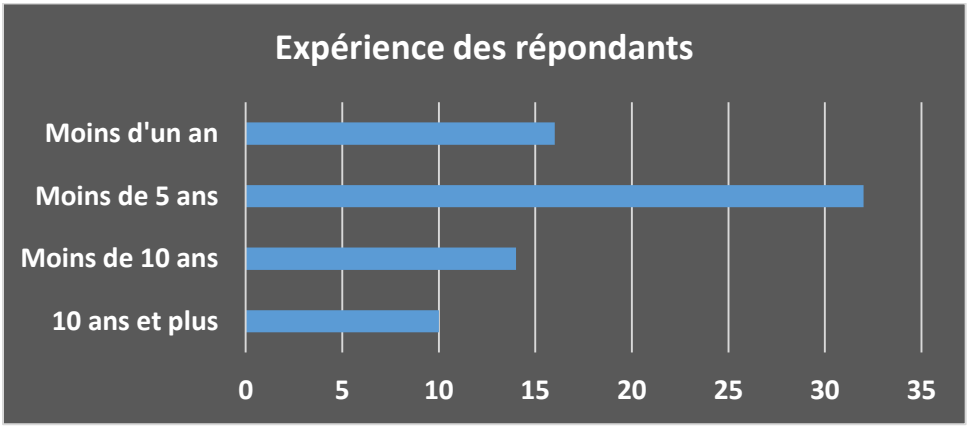


Figure 16. – Sondage : Expérience des répondants à leur poste

56 des répondants ont plus d’un an d’expérience à leur poste. Leur prise de recul sera bénéfique à la qualité du sondage.

B. Interprétation des résultats

Dans cette partie, je vais mettre en corrélation les avis des services métiers et des services informatiques sur le Shadow IT.

Cette étude me permettra d'avoir des éléments sur mes questions et mes hypothèses.

Conscience du Shadow IT en entreprise

Les métiers, utilisateurs d'applications et de solutions Shadow IT, n'ont pas nécessairement conscience de participer à ce phénomène. Le graphique, ci-dessous, nous indique que le Shadow IT est très peu connu des services métiers. Sur les 38 répondants, seuls 26% ont déjà entendu parler du Shadow IT.

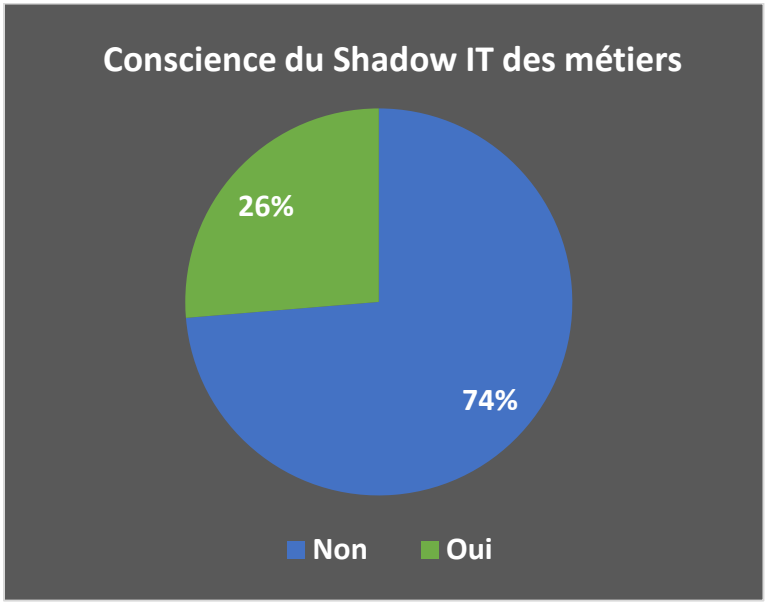


Figure 17. – Sondage : Conscience du Shadow IT des métiers

Les métiers, pour la majorité, ne savent pas ce que représente le Shadow IT. Ils peuvent l'utiliser sans en avoir conscience. Je suppose qu'ils n'ont pas été sensibilisés sur ce sujet.

Des questions se posent, qu'en est-il des services informatiques ? Savent-ils le définir avec exactitude ?

La figure 18 nous indique que sur les 34 répondants, seuls 15 savent définir avec exactitude le Shadow IT, soit 44 %. 66 % des répondants ne sont pas capables d'identifier et de définir le Shadow IT avec exactitude.

La sensibilisation et la connaissance informatique sont transmises par le service informatique. Les métiers ne peuvent pas être informés sur le Shadow IT si le service informatique ne maîtrise pas le sujet.

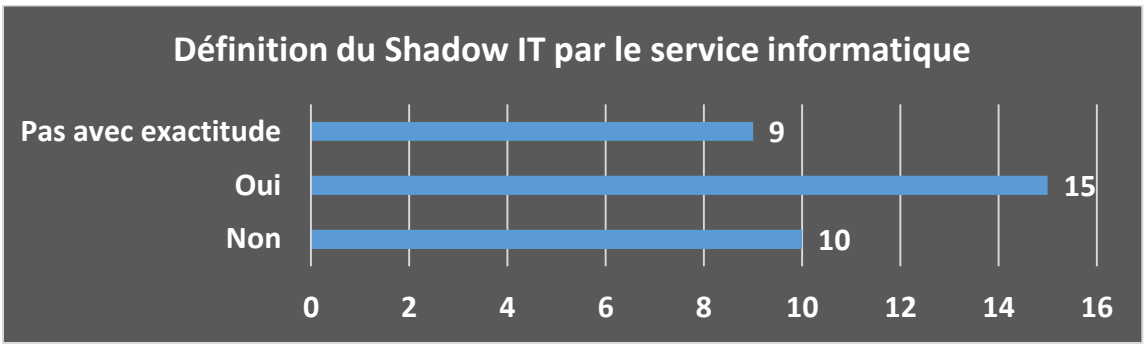


Figure 18. – Sondage : Définition du Shadow IT par le service informatique

Parmi les répondants des services informatiques, seulement 50 % ont constaté le Shadow IT dans leur entreprise.

Cette donnée peut être la résultante de l'incapacité du service informatique à détecter et identifier le Shadow IT.

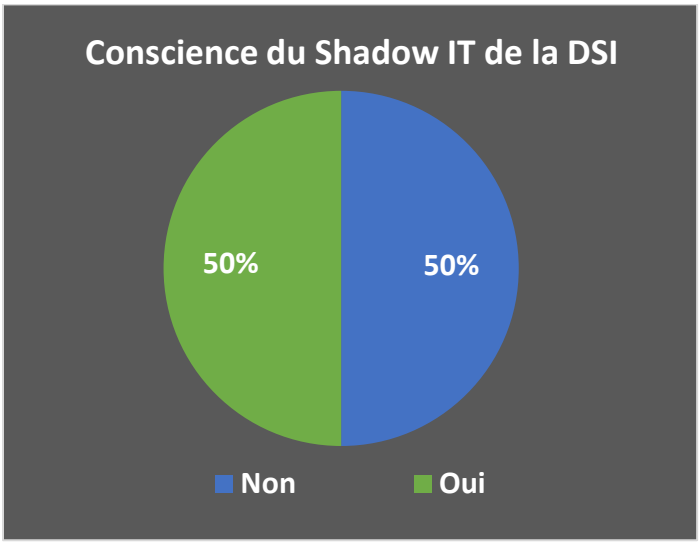


Figure 19. – Sondage : Conscience du Shadow IT de la DSI

A la suite de cette question, j'ai demandé un ou des exemples parmi ceux constatés. J'ai catégorisé leurs réponses sur la figure suivante.

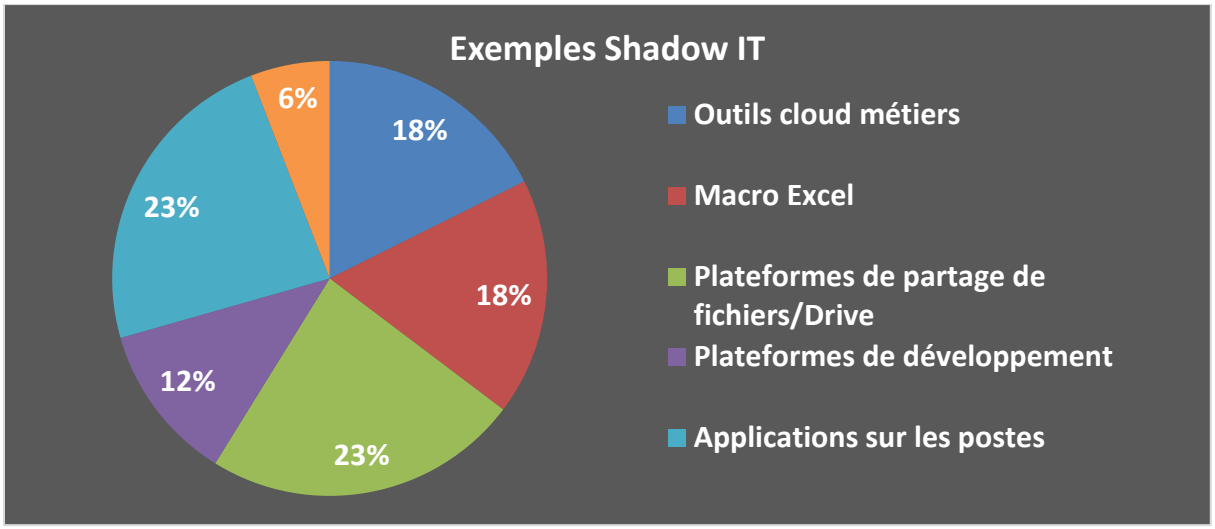


Figure 20. – Sondage : Exemples de Shadow IT

Nous constatons la forte présence des applications sur les postes des utilisateurs et des plateformes de partages de fichiers, « Drive », sans la validation de la DSI. Nous confirmons l'utilisation des applications Cloud et des macros Excel par les services métiers. Nous remarquons avec surprise que le service informatique utilise des applications Shadow IT avec les plateformes de développement. Le BYOD est légèrement présent et concerne principalement les téléphones portables personnels.

La conscience, la sensibilisation et le traitement du Shadow IT dans les entreprises ne pourront être possible que si les services informatiques maitrisent le sujet.

La communication de la DSI en entreprise

Le défaut de communication peut aussi être responsable de l'inconscience des services métiers par rapport au Shadow IT. Pour cette raison, j'ai demandé aux métiers si leur DSI communiquait sur différents sujets.

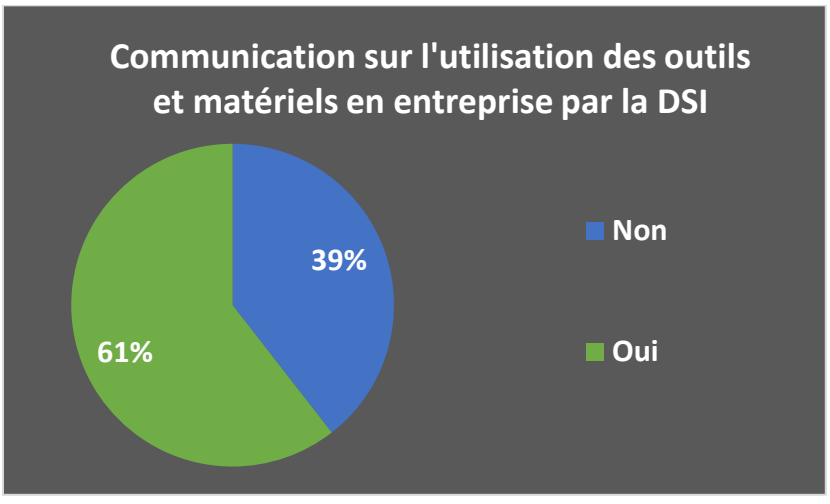


Figure 21. – Sondage : Communication sur l'utilisation des outils et matériels par la DSI

Pour 39 % des répondants, leur service informatique ne communique pas sur l'utilisation des outils et matériels en entreprise. Ils n'ont pas connaissance ou conscience des règles d'usage et d'utilisation du système d'information de l'entreprise. Ce manque de communication ou son manque d'efficacité freine la sensibilisation des utilisateurs du SI.

La sécurité informatique, sujet d'actualité, est importante et primordiale pour les entreprises. Tous les acteurs de l'entreprise doivent être conscients des risques de leurs outils informatiques de travail.

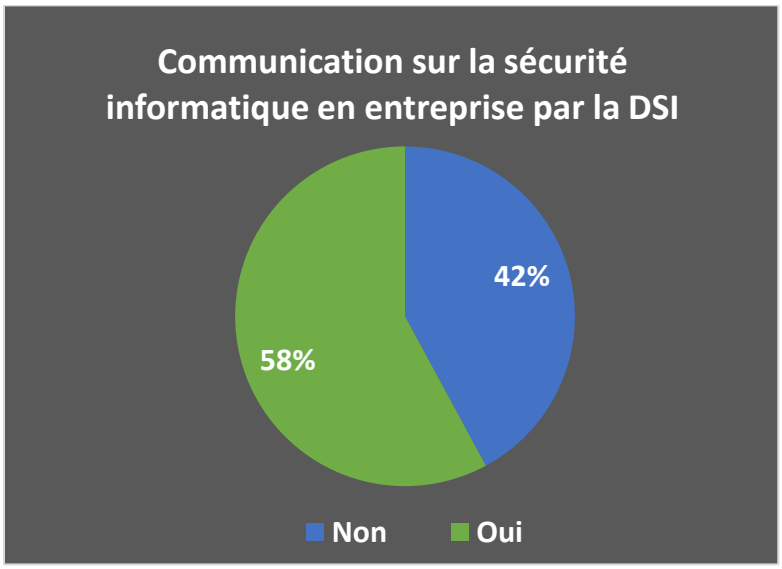


Figure 22. – Sondage : Communication sur la sécurité informatique par la DSI

42 % des répondants nous indiquent que leur DSI ne communique pas sur la sécurité informatique de leur entreprise. Ce chiffre est plus important que celui sur l'utilisation des outils et matériels. Les enjeux de la sécurité informatique ne sont pas transmis à l'ensemble des services métiers. 3 personnes sur 7, en moyenne, sont des menaces potentielles pour leur entreprise.

Nous avons constaté lors du point précédent que les métiers n'avaient pas conscience du Shadow IT en raison du manque de maitrise de leur DSI sur le sujet. Un manque ou l'inefficacité de la communication de la DSI sont des raisons à rajouter à ce constat. Une sensibilisation de l'ensemble des employés est obligatoire dans le contexte actuel.

Shadow IT, menace et/ou opportunité

Dans les parties précédentes, j'ai évoqué le Shadow IT pouvant être une opportunité. Les services métiers, sous pression et avec l'intention d'optimiser leurs processus, se tournent vers le Shadow IT. J'ai souhaité dans le questionnaire avoir l'avis des services informatiques sur ce constat.

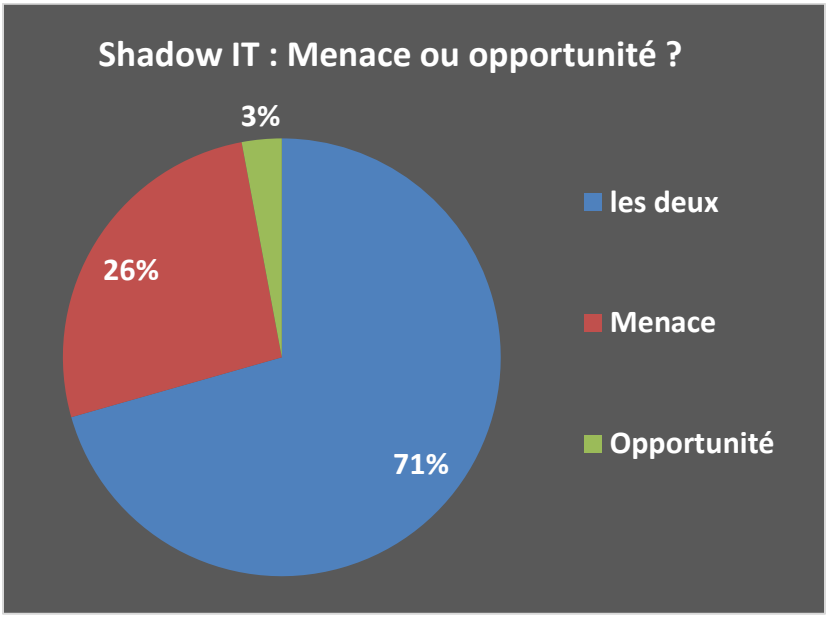


Figure 23. – Sondage : Shadow IT : Menace ou opportunité ? vision de la DSI

Les services informatiques pensent à 71 % que le Shadow IT est une menace tout comme une opportunité. 26 % des répondants envisagent le Shadow IT uniquement comme une menace.

Nous remarquons que des répondants, à hauteur de 3 %, ne perçoivent pas la menace dans le Shadow IT, seulement son opportunité. Ils sont une minorité.

Sur les 34 répondants, la menace est perçue au total à 97 % et l'opportunité à 74 %. La DSI aperçoit l'opportunité dans le Shadow IT, les métiers peuvent fournir des nouvelles méthodes, solutions et technologies qui ne sont pas proposées par leur direction. Ce phénomène comble les fonctionnalités manquantes des systèmes d'information.

L'avis des répondants sur les menaces générées par le Shadow IT est sans appel. Le shadow IT reste une menace. J'ai demandé aux membres des services informatiques d'identifier les menaces qu'ils associent au Shadow IT.

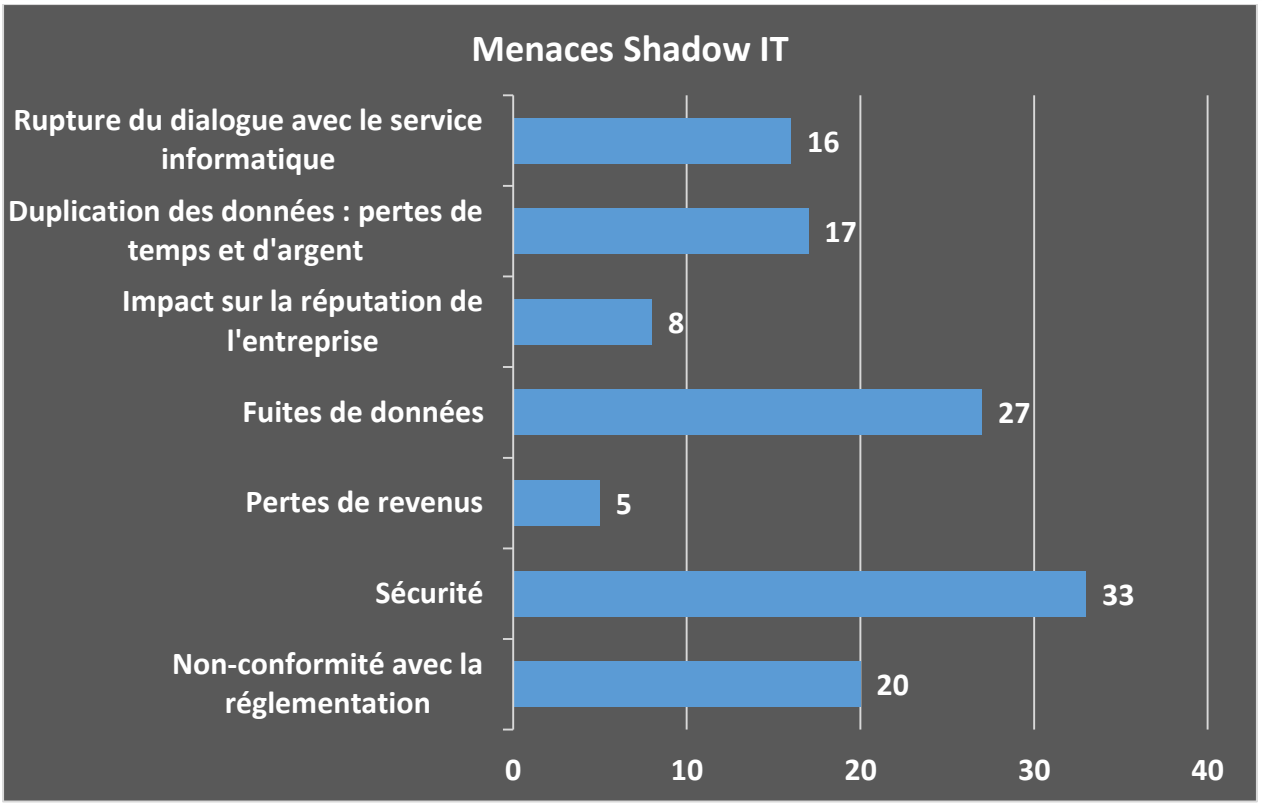


Figure 24. – Sondage : Les menaces du Shadow IT par la DSI

Les menaces du Shadow IT sont nombreuses et variées. Les répondants s'accordent à 97 % sur les menaces de sécurité de ce phénomène, suivi à 79% par les fuites de données. Les membres des services informatiques sont conscients de la non-conformité du Shadow IT avec les réglementations en vigueur. La duplication des données, avec ses conséquences, est constatée par 50 % des interrogés. Les répondants subissent à 47 % une rupture du dialogue avec leurs services métiers.

Le Shadow IT est à la fois une opportunité et une menace pour l'entreprise. Le potentiel d'innovation, la génération de valeurs et les menaces sont une réalité. Avec l'immense choix d'application cloud sur le marché, bloquer le Shadow IT ne suffit pas. Le consommateur peut se tourner vers d'autres solutions encore moins sécurisées et dangereuses pour l'entreprise.

Communiquer avec les consommateurs permet d'identifier leurs solutions Shadow IT, leurs besoins et de les sensibiliser. Le shadow IT doit être rapidement détecté et encadré.

Les DSI sont responsables de leur système d'information. Comme je l'ai évoqué durant les points précédents, ne pas prendre en compte le Shadow IT peut avoir des conséquences dévastatrices pour l'entreprise. Nous remarquons sur la figure ci-dessous, seulement 44 % des services informatiques prennent en compte le Shadow IT dans leur gouvernance.

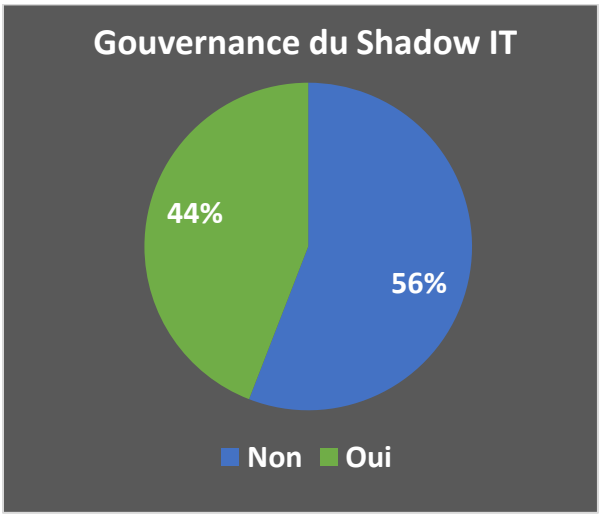


Figure 25. – Sondage : Intégration du Shadow IT dans la gouvernance

56 % des professionnels de l'IT interrogés n'ont pas encore pris en compte le Shadow IT dans leur gouvernance. Le phénomène n'étant pas géré, il prolifère au sein de ces entreprises. J'ai souhaité ensuite connaître les moyens et les actions mises en œuvre par les entreprises pour traiter le Shadow IT.

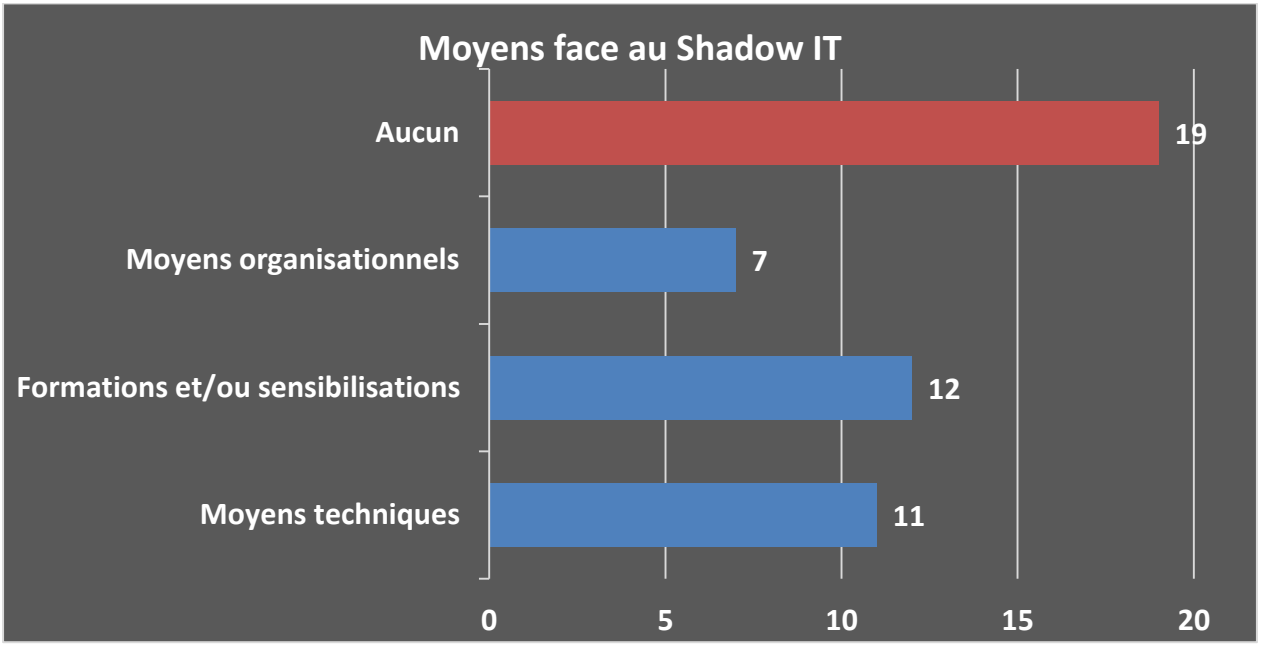


Figure 26. – Sondage : Moyens face au Shadow IT

Nous pouvons voir que le shadow IT ne se traite pas avec un seul et unique moyen. Le traitement passe par des moyens organisationnels, techniques et de sensibilisation. La sensibilisation et les outils techniques sont les méthodes les plus populaires.

La figure, ci-dessous, regroupe les actions des services informatiques contre le Shadow IT.

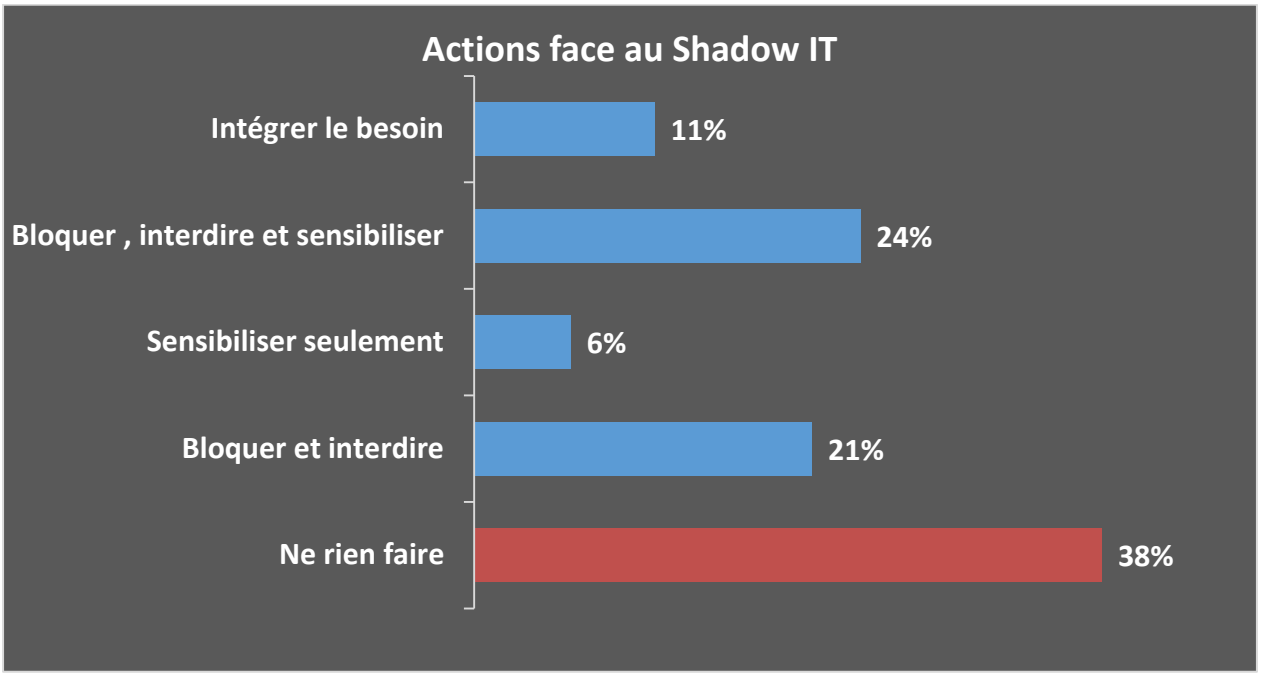


Figure 27. – Sondage : Actions contre le Shadow IT

Le blocage des solutions Shadow IT sans prendre en compte les besoins apparaît dans 45% des réponses. Les utilisateurs bloqués recherchent et utilisent en conséquence d'autres solutions Shadow IT accessibles. Ils jouent au jeu du chat et de la souris. Bloquer uniquement n'est pas efficace dans le temps.

La sensibilisation des services métiers est utilisée par 30 % des répondants. Cette communication permet de se rapprocher des utilisateurs et de renouer un lien de confiance avec eux. Cette étape permet de prendre en compte les besoins des services métiers.

Nous remarquons que seulement 11 % des services informatiques ont mis en place des processus qui permettent l'intégration des besoins métiers dans leur système d'information. Cette méthode chronophage est efficace mais nécessite des ressources et une organisation qui sont hors de portée pour la majorité des DSI interrogées.

Le BYOD est utilisé par les services métiers pour des raisons de performance et de facilité d'utilisation. Il est bien plus facile d'utiliser un seul téléphone plutôt que deux. Cette pratique du Shadow IT possède les mêmes menaces. Nous observons sur la figure, ci-dessous, que seulement 18 % des services informatiques interrogés possèdent une politique d'utilisation pour ces matériels au sein de leur entreprise.

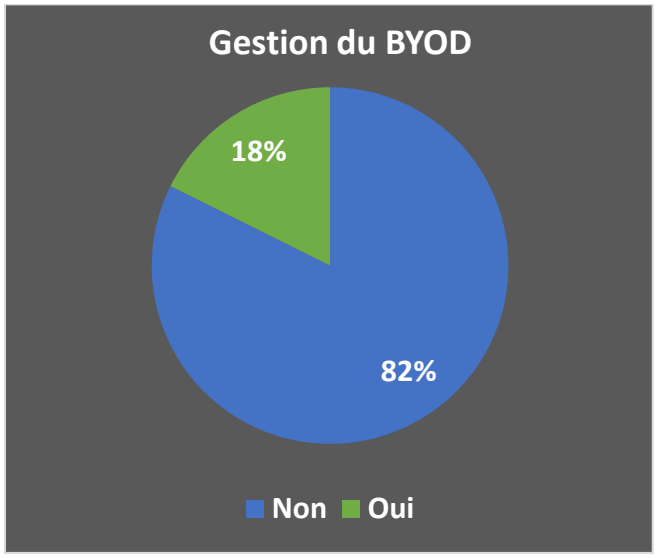


Figure 28. – Sondage : Gouvernance du BYOD

Les résultats de ce sondage indiquent un manque de prise en charge du Shadow IT par les DSI. Ce manque d'intérêt conduit à l'utilisation des outils BYOD et BYOA dans les entreprises.

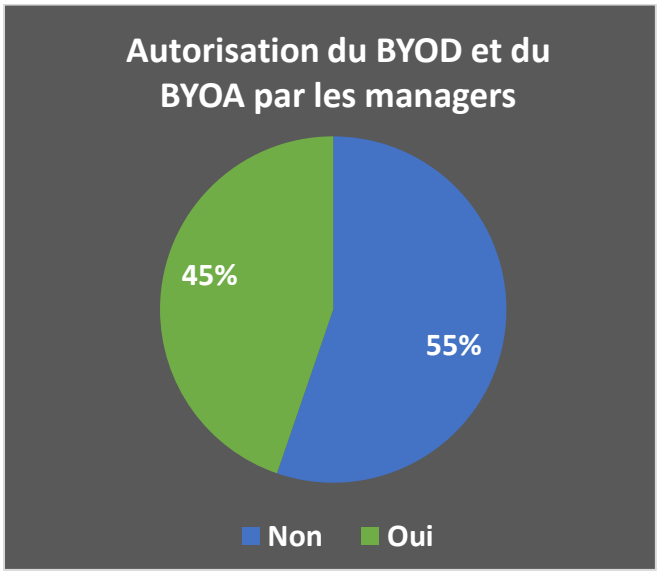


Figure 29. – Sondage : Autorisation du BYOD et du BYOA par les managers

45 % des répondants métiers indiquent que leur manager autorise l'utilisation d'application et de matériel personnel.

Ces chiffres alarmants révèlent que la gestion des applications et des matériels personnels est parfois assurée par les métiers et non par leur DSI. Cette population non qualifiée et non consciente des menaces met en danger les entreprises. La défaillance des DSI en est la cause.

Afin de réduire l'utilisation du Shadow IT, les directions des services informatiques doivent assurer leurs responsabilités et se concentrer sur trois points indissociables :

- Des moyens techniques pour détecter, alerter et bloquer
- La communication et la sensibilisation pour instaurer un dialogue, éduquer et informer les métiers
- Des moyens organisationnels pour suivre, répondre et intégrer les besoins des métiers dans le système d'information

Les relations entre les métiers et les services informatiques

Dans ce sondage, j'ai voulu mesurer et qualifier les relations entre les départements informatiques et les services métiers. Ce relationnel est vital pour les organisations. La qualité et la compréhension des échanges entre le service informatique et les services métiers dépendent de leur relation.

Dans un cadre général ou projet métier, quel est l'état des relations entre les services métiers et le département informatique ?

Veuillez-vous référer à l'échelle de notation pour l'interprétation des résultats :

Note	1	2	3	4	5
Qualité	Très Mauvaise	Plutôt Mauvaise	Moyenne	Plutôt Bonne	Très bonne
Fréquence	Jamais	Peu	Moyenne	Souvent	Tout le temps

Tableau 15. – Sondage : Échelle de notation

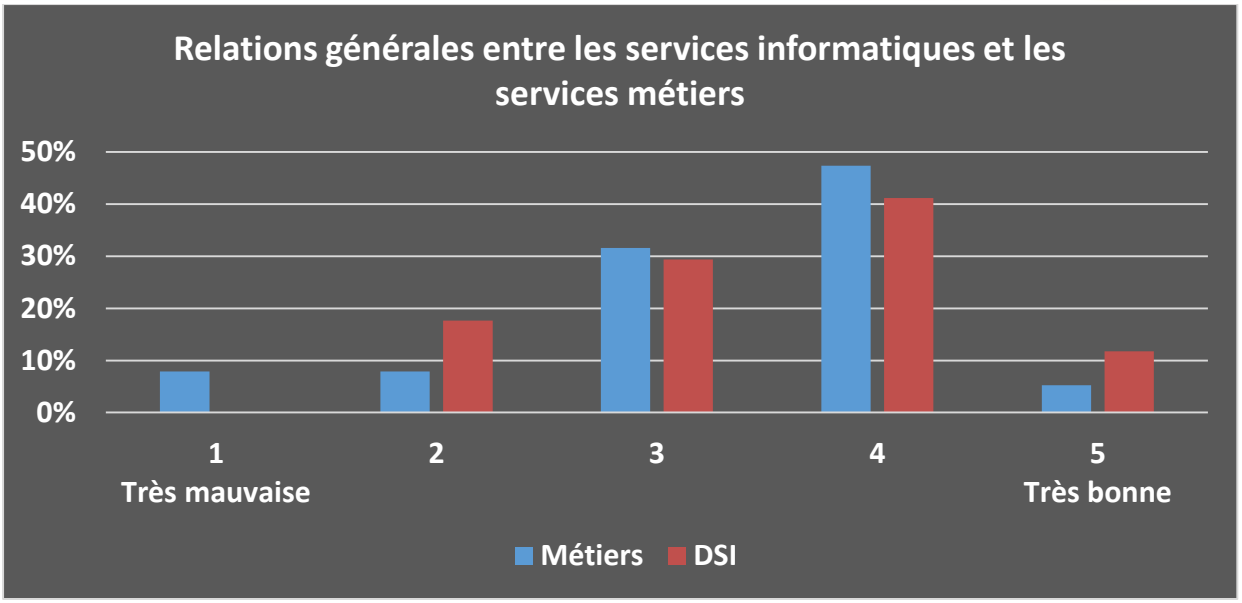


Figure 30. – Sondage : Relation entre l'IT et les métiers

Nous remarquons que plus de 40 % des répondants métiers et informatiques s'accordent à qualifier, dans un cadre général, la relation comme « plutôt bonne ». La qualité moyenne est partagée par environ 30 % des répondants métiers et informatiques. Les relations qualifiées de « mauvaise » rassemblent 16 % des profils métiers et 17 % des répondants informatiques.

La fréquence d'implication de la DSI dans les projets métiers nous donne un indice sur l'état de leur relation. J'ai demandé aux répondants informatiques si leur service était impliqué systématiquement dans les projets métiers.

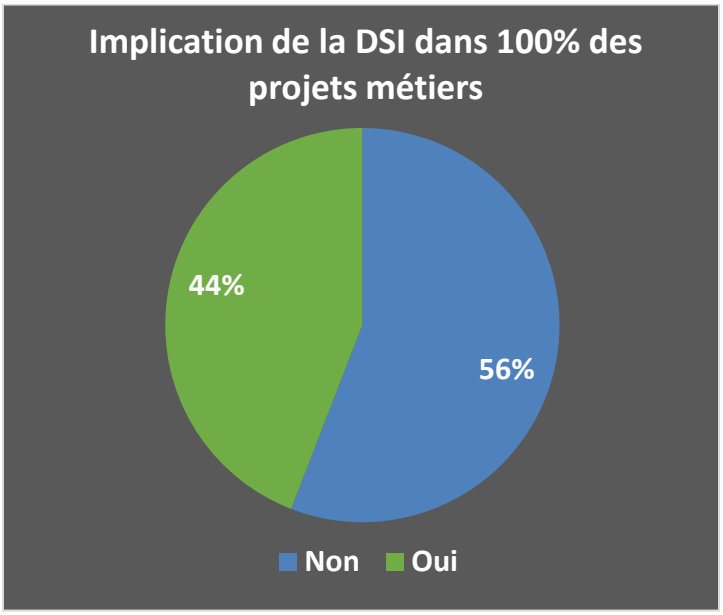


Figure 31. – Sondage : Ratio d'implication de la DSI dans les projets métiers

Seulement 44% des services informatiques sont impliqués systématiquement dans les projets métiers de leur entreprise. Certaines DSI ont perdu leur dominance sur les projets métiers impliquant leur système d'information.

La vision des répondants métiers nous précise la fréquence d'implication de la DSI dans leurs projets.

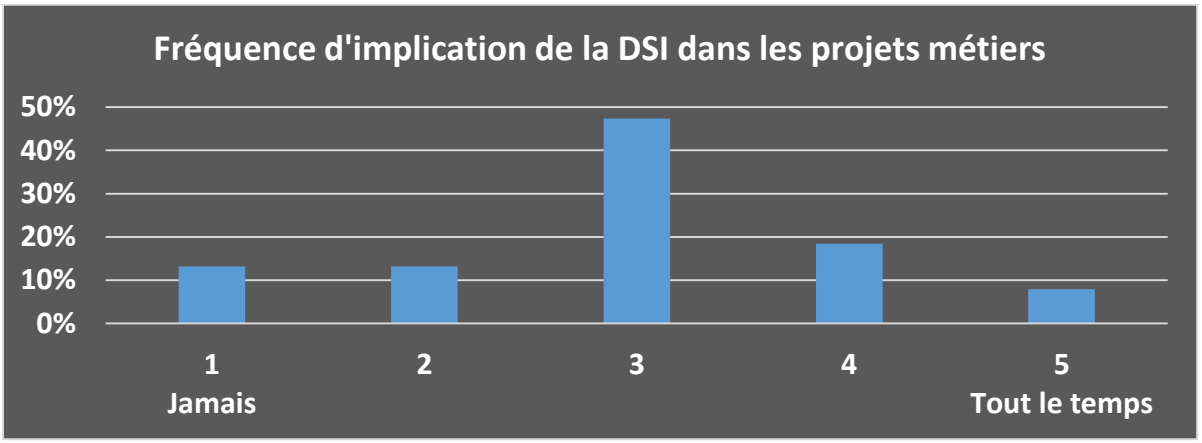


Figure 32. – Sondage : Fréquence d'implication des services informatiques dans les projets métiers

La majorité (47 %) des participants métiers du sondage indique que leur service informatique est impliqué avec une fréquence moyenne dans leurs projets. J'ai estimé la moyenne à un projet sur deux environ. Ce ratio montre l'émancipation des services métiers et la diminution de l'implication de la DSI dans ces projets. Les services travaillent et parlent moins entres eux.

Nous constatons une nette détérioration des relations entre les services informatiques et métiers dans le cadre des projets.

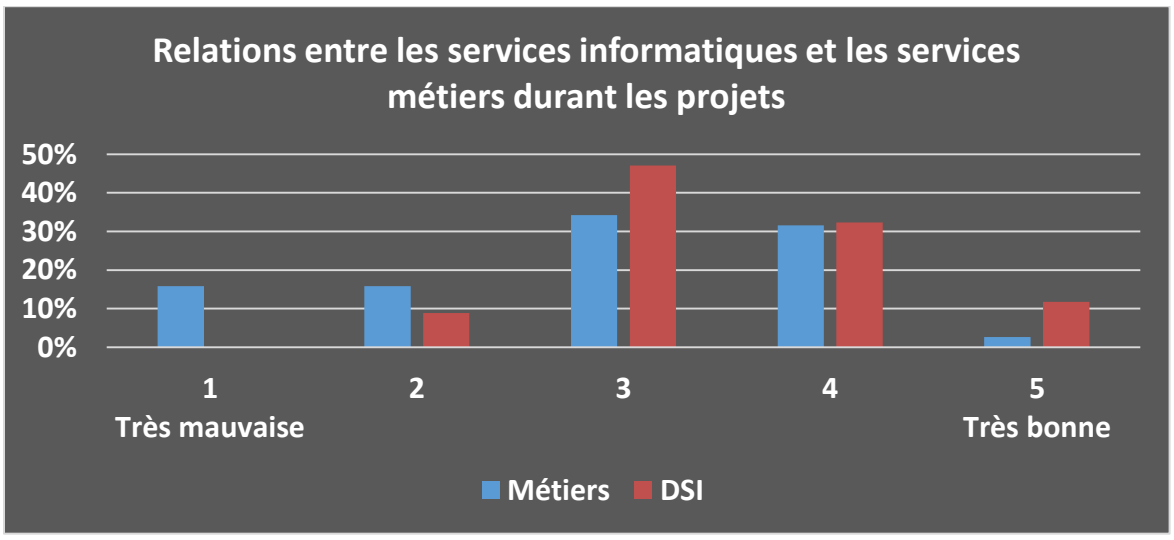


Figure 33. – Sondage : La relation entre les DSI et les métiers durant les projets

Les participants informatiques qualifient majoritairement à 47 % leur relation, avec les métiers dans un cadre projet, comme « Moyenne ». Les répondants métiers sont partagés entre une qualité moyenne à 34 % et une qualité « Plutôt bonne » à 31 %.

Nous remarquons que les relations qualifiées de « Mauvaise » rassemblent 32 % des profils métiers, soit le double par rapport au cadre général.

Les services métiers vivent et travaillent avec les défauts de leur DSI. Ces difficultés entrainent le mécontentement des services métiers. Les 38 répondants métiers ont identifié plusieurs de ces problèmes.

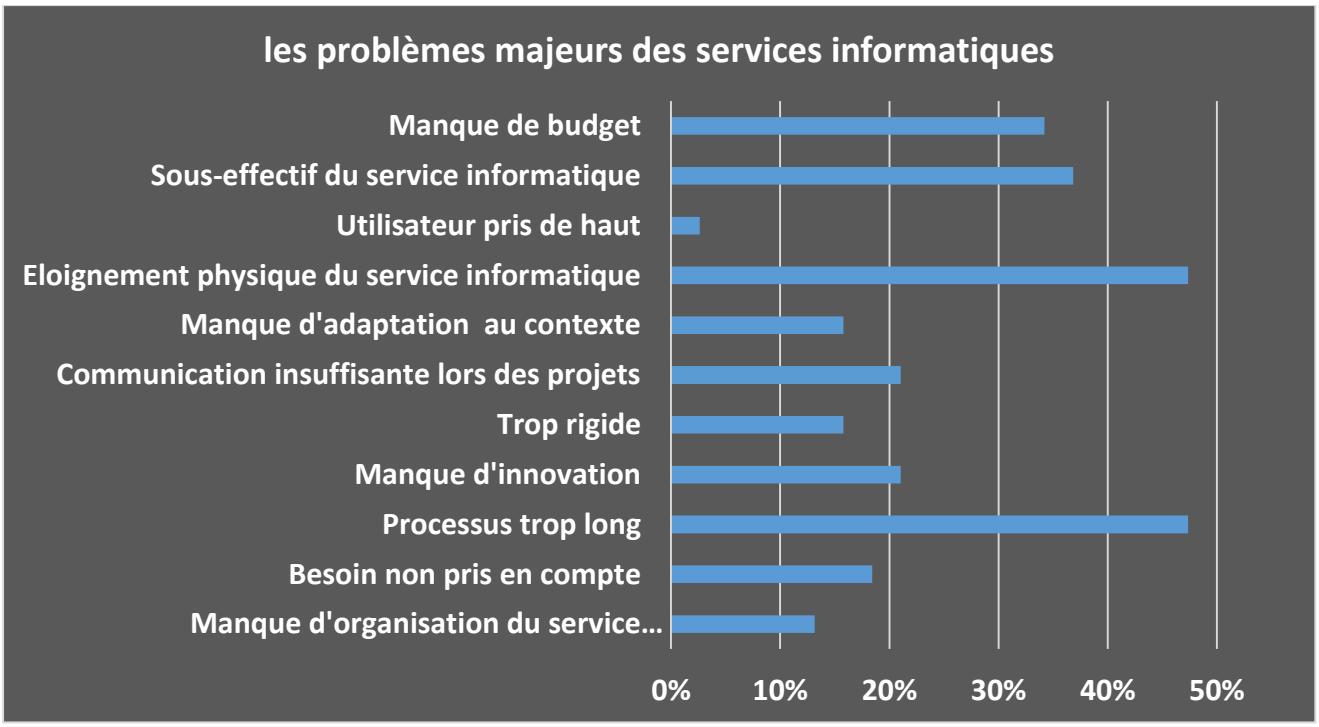


Figure 34. – Sondage : Les problèmes majeurs des services informatiques par les métiers

Les problèmes sont nombreux et variés. Les services informatiques sont considérés comme trop éloignés, les services métiers ont perdu leur proximité et en qualité d'écoute. Les processus de la DSI sont jugés comme trop longs voir obsolètes. Le sous-effectif et le manque de budget des services informatiques affectent leur qualité de service. Les métiers n'identifient plus la DSI comme un centre d'innovation. La rigidité et le manque de communication de la DSI font chuter sa popularité.

Les métiers souhaitent une écoute et une mise en place flexible de leurs besoins. Plus l'efficience de la DSI diminue plus le Shadow IT grandit.

Les raisons développées dans les parties précédentes entrainent une consommation d'outils et de matériels Shadow IT dans les entreprises. Les employés achètent et utilisent des solutions Shadow IT en dépit des risques qu'elles génèrent. La figure, ci-dessous, représente les consommateurs en fonction de chaque profil.

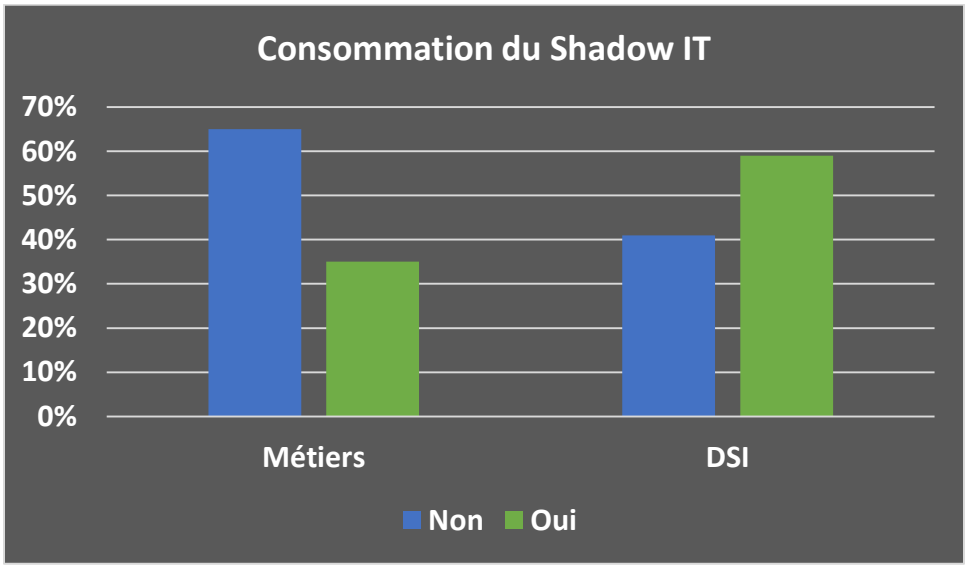


Figure 35. – Sondage : Consommation du Shadow IT dans les entreprises

Nous remarquons que 35 % des répondants métiers sont consommateurs de Shadow IT. Les services informatiques avouent à 59 % utiliser des outils et solutions Shadow IT. Ce phénomène a envahi toute l'entreprise même le service responsable de son système d'information. Les informaticiens rencontrent les mêmes problèmes de flexibilité que les métiers.

Depuis la création d'Internet aux États-Unis et son introduction en Europe, le développement de la technologie n'a jamais cessé. Les événements historiques, les innovations technologiques et les changements sociaux ont eu une influence significative sur les différentes générations.

La génération Z, née entre 1995 et 2010, est dominée par la technologie. La technologie gouverne cette génération dans sa vie quotidienne. Internet est leur principal outil de communication pour les interactions personnelles ou professionnelles. La génération Alpha, la plus jeune des générations, naîtra dans le numérique alors que la génération z est née avec. Elle intégrera les technologies « hyper-connectées » dans leur vie.

Ces générations dans les entreprises partageront leurs habitudes et technologies. Seront-ils vecteurs et consommateurs du Shadow IT en entreprise ?

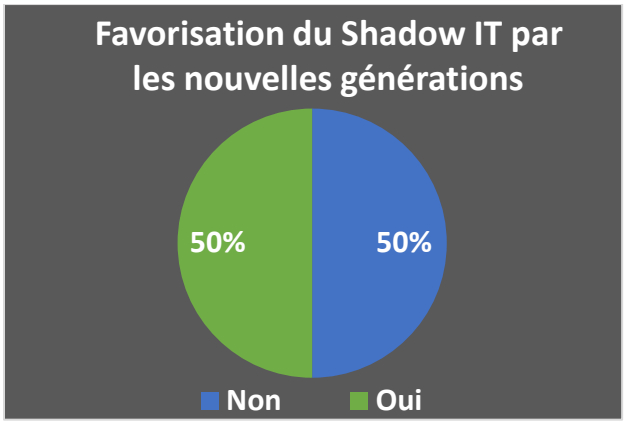


Figure 36. – Sondage : Le Shadow IT & les nouvelles générations

L'avis des répondants métiers est partagé sur ce sujet. La moitié des participants pensent que les nouvelles générations favoriseront le Shadow IT en entreprise. Ces nouvelles générations seront vectrices de Shadow IT mais surtout d'innovations. Les entreprises devront les encadrer et les écouter afin de capitaliser leur potentiel en valeur et ainsi réduire l'utilisation du Shadow IT.

II. Conclusions

Les articles et études existants m'ont permis d'analyser et de déchiffrer le sujet. Mon enquête de terrain m'a apporté la vision des services métiers et informatiques sur le Shadow IT en entreprise.

Les métiers, sous pression par le marché, se tournent vers le Shadow IT pour plus de compétitivité et de flexibilité. La DSI peine à répondre aux besoins des métiers à cause de son inflexibilité, son manque d'écoute, ses processus trop longs, son manque d'innovation et de communication. Le Shadow IT s'amplifie dans l'entreprise en fonction de l'inefficacité de la DSI. La DSI doit réagir afin de devenir un centre de profit et générer de la valeur pour ses services métiers.

Mon interprétation des résultats du sondage m'a permis d'étayer mes hypothèses, je vais synthétiser mes conclusions dans les parties suivantes.

1. La détection et le blocage du Shadow IT

Détecter et bloquer le Shadow IT limitent à court terme son adoption. Ces actions ne suffisent pas dans le temps. L'immense choix d'applications et de matériels proposé aux employés leur permet de se tourner vers d'autres solutions non bloquées et moins sécurisées.

La détection du Shadow IT permettra à la DSI de prendre conscience de l'étendue du phénomène au sein de son système d'information. C'est la première étape indispensable pour traiter et limiter l'usage du Shadow IT en entreprise.

Les moyens techniques et de communications permettront à la DSI de détecter, d'alerter, de bloquer et de limiter le Shadow IT. L'identification des applications, des matériels, des besoins et des consommateurs aidera la DSI dans l'encadrement, le traitement et la limitation du Shadow IT.

2. La communication et la sensibilisation

Les employés n'ont pas conscience d'utiliser des éléments Shadow IT car la DSI a failli dans sa mission. La communication de la DSI des règles d'utilisation du SI et des enjeux de la sécurité informatique sont absentes ou inefficaces auprès des utilisateurs.

La sensibilisation à la sécurité informatique est un des moyens utilisés pour informer les employés des risques de leurs outils de travail et de leurs responsabilités. C'est un outil indispensable de communication pour les entreprises dans un contexte RGPD et de cybersécurité actuel.

Afin de limiter les comportements dangereux, il est nécessaire d'éduquer en permanence et de tenir informés les employés des enjeux de la sécurité informatique. La sensibilisation et la prise de conscience des employés permettront de réduire considérablement les risques liés à la sécurité informatique et de limiter l'adoption du Shadow IT.

Communiquer avec les consommateurs permet d'identifier leurs solutions Shadow IT, leurs besoins et de les sensibiliser. L'encadrement du Shadow IT passe par la communication et la sensibilisation.

Un service informatique à l'écoute des utilisateurs permettra de répondre efficacement à leurs besoins et d'améliorer son relationnel.

L'hypothèse suivante est donc vraie. Des utilisateurs/métiers avertis et conscients des risques/enjeux informatiques limitent l'adoption du Shadow IT.

3. Les capacités de la DSI

L'évolution accélérée des activités métiers et les exigences de conformité changent le rôle du service informatique au sein de l'entreprise. Leurs responsabilités et leurs missions ont grandement augmenté ces dernières années. Les services informatiques assurent avec difficulté leurs devoirs.

Les métiers recherchent des solutions innovantes et répondant à leurs besoins de compétitivité. La DSI ne parvient pas à satisfaire pleinement ses utilisateurs. Plus l'efficience de la DSI diminue plus le Shadow IT grandit. Pouvoir répondre aux besoins et satisfaire les métiers doit être une priorité pour les DSI.

Ses capacités à s'adapter, communiquer, prendre en compte, et intégrer les besoins des métiers sont la clé pour limiter l'adoption du Shadow IT dans l'entreprise. Sans la maîtrise et la connaissance de leur système d'information et des technologies, les DSI ne peuvent pas s'adapter aux demandes des métiers. Leur budget et leur effectif jouent un rôle déterminant dans leur qualité de service. La capacité de la DSI à détecter le Shadow IT est vitale pour sa limitation.

La prise de conscience, la sensibilisation et le traitement du Shadow IT dans les entreprises ne pourront être possibles que si les services informatiques maitrisent le sujet.

Des moyens organisationnels pour encadrer le Shadow IT et intégrer les besoins métiers dans le système d'information seront nécessaires. Cet encadrement transformera le Shadow IT en innovation et générera de la valeur pour l'entreprise.

L'hypothèse suivante est donc vraie. Avoir une DSI possédant les capacités à répondre efficacement aux besoins métiers limite l'adoption du Shadow IT.

I. Rappel

Ma problématique est la suivante :

« **Quels sont les moyens et méthodes nécessaires afin de limiter l'adoption du Shadow IT dans l'entreprise**? »

Aujourd'hui, il n'existe pas de méthodes ou de moyens spécifiques pour traiter et limiter le Shadow IT. Les référentiels, les démarches et les bonnes pratiques existants, tels que ITIL (37), COBIT[27] (38), l'urbanisation des SI (39), n'offrent pas de solutions propres en matière de Shadow IT. Ils apportent cependant des mécanismes sur lesquels nous pouvons nous appuyer.

Pour développer une démarche cohérente sur ce sujet, Je vais tout d'abord introduire les moyens et méthodes en relation avec mes hypothèses. Je proposerai ensuite un guide méthodologique pour la limitation de l'adoption dans les entreprises. Je finirai par ma conclusion.

II. Axes de la démarche

Ma réflexion sur la limitation de l'adoption du Shadow IT porte sur 3 axes.

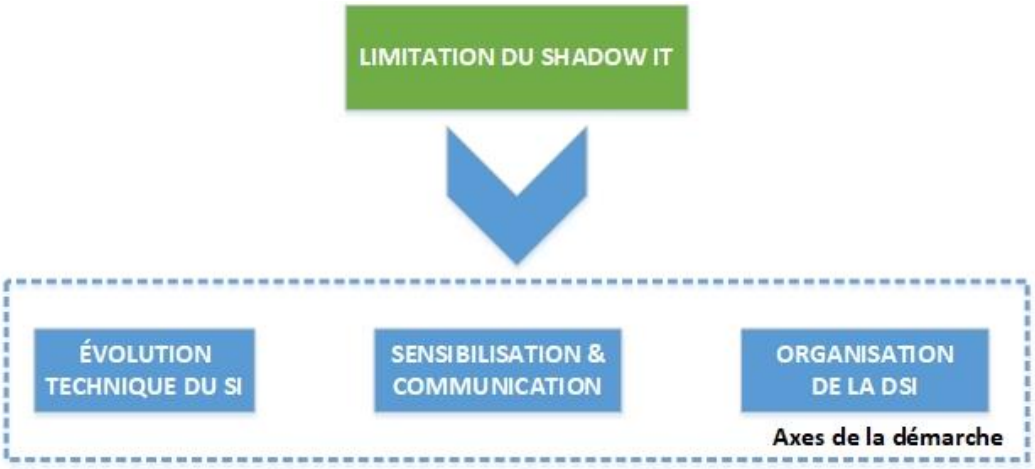


Figure 37. – Axes de la démarche

[27] Control Objectives for Information and related Technology est un référentiel de bonnes pratiques d'audit informatique et de gouvernance des systèmes d'information d'origine américaine.

1. Évolution technique du SI

La maîtrise du SI

Aujourd'hui, le système d'information est au cœur du fonctionnement de toute organisation et son efficacité détermine sa performance. Le développement continu de métiers et des technologies ont compliqué la gestion du système.

Il est donc important pour les entreprises de maîtriser puis de gérer de manière stricte et cohérente leurs SI. La cartographie du SI est une méthode indispensable pour sa maîtrise. Elle permet aux organisations de comprendre tous les éléments du SI et d'obtenir une meilleure vision en le montrant sous différentes vues.

L'élaboration de cartes fait partie de la démarche d'urbanisation des systèmes d'information (39). La cartographie du SI d'information est d'ailleurs encouragée par l'ANSSI[28] à l'aide d'un guide d'élaboration consultable sur leur site. La réalisation d'une cartographie du SI améliorera la flexibilité du SI et le temps de réponse du service informatique, grâce à leur maitrise. Cette démarche aidera à capitaliser et intégrer le Shadow IT dans le SI et ainsi le limiter.

L'accessibilité de la cartographie du SI par les métiers renforcera leur implication et facilitera l'interprétation de leurs besoins. Le site bpms.info (40) illustre les différentes visions par la figure ci-dessous :

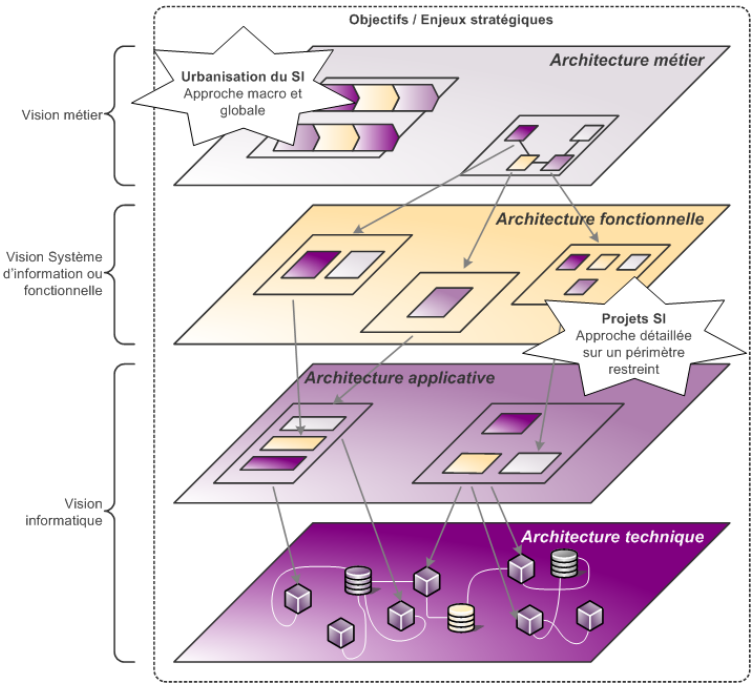


Figure 38. – Cartographie du SI : les différentes visions

[28] Agence National de la sécurité des systèmes d'information

La détection

Comme nous avons pu voir dans les parties précédentes l'identification du Shadow IT dans sa pratique permet son traitement et sa limitation. Les moyens de détection à l'aide de solutions techniques sont apparus récemment sur le marché.

Les solutions CASB répondent au besoin de visibilité sur les applications cloud et à la protection des données dans l'entreprise, réclamée par le GDPR. Le CASB deviendra un moyen capital pour les entreprises face à l'utilisation massive d'application cloud non validée des métiers.

Le CASB est un outil avec de nombreuses fonctionnalités et son périmètre n'est pas limité au cloud. Sa surveillance du réseau, des postes de travail, des accès et du cloud font de lui une solution de détection et de protection modèle contre le Shadow IT.

Le choix d'une solution CASB dépend des besoins identifiés, du budget et de l'architecture de l'entreprise. La société Gartner a synthétisé en 2019 le marché des solutions CASB (41). Les solutions sont comparées en fonction de leur capacité d'adaptation et leurs fonctionnalités. Cinq entreprises sont leaders du marché dont Microsoft.

Figure 39. – CASB : Marché des solutions

La mise en place d'une solution CASB permettra aux entreprises d'obtenir une visibilité sur le Shadow IT et de le limiter par la suite.

La protection

Des évolutions techniques du SI augmentent sa sécurité en protégeant les données ou les matériels de l'entreprise. La mise en place du standard 802.1X empêche les matériels BYOD non autorisés d'accéder au réseau de l'entreprise, limitant ainsi l'utilisation du Shadow IT. Le Digital Asset Management (DAM) est un moyen de centraliser et de sécuriser les données permettant aux entreprises de monitorer et contrôler l'accès à ses données classifiées. L'utilisation ou l'extraction de données non autorisée est interdite, limitant ainsi l'adoption du Shadow IT.

Ces évolutions techniques limiteront le Shadow IT en apportant une protection et une meilleure gestion du système d'information aux entreprises.

2. Sensibilisation et communication

La sensibilisation

La première étape de la sensibilisation est la rédaction et la communication d'une charte informatique ainsi que d'une charte d'administrateur. Tous les employés doivent être informés et accepter les règles d'utilisation du SI. Joindre la charte au contrat de travail permet d'informer et de sensibiliser les nouveaux arrivants.

La seconde étape est l'organisation de séances de formation et de sensibilisation à la sécurité de l'information. Ces modules devront être adaptés par rapport aux objectifs stratégiques du programme et aux connaissances des utilisateurs. Ces séances peuvent prendre différentes formes. Pour leur efficacité, il est préférable d'opter pour des formes participatives telles que :

- des Ateliers
- des situations ludiques : Escape Game
- des Quiz
- des mises en situation

Il faudra ensuite évaluer le succès de votre campagne de sensibilisation, soit à l'aide d'un test soit d'une simulation en relation avec les objectifs. En comparant les objectifs aux résultats, vous pourrez adapter vos prochaines séances pour plus d'efficacité. C'est inspiré du cycle d'amélioration continue du référentiel d'ITIL (37).

Afin d'intégrer et mémoriser les enjeux de la sécurité informatique, il est conseillé de relancer votre campagne tous les 6 mois. Un rappel cyclique, par courriel, des objectifs de la campagne peut être effectué.

Sensibiliser les utilisateurs permettra de réduire les risques liés à la sécurité informatique et de limiter l'adoption du Shadow IT.

La formation des employés

La constante évolution des technologies complexifie leur maîtrise et leur application. Le service informatique a besoin de se former pour combler ses lacunes et pour intégrer les technologies innovantes. Un service informatique compétent et efficient sera plus productif et compétitif pour l'entreprise.

Le manque de connaissances et l'utilisation approximative des applications de l'entreprise peuvent être un frein à leur popularité. Mettre en place un plan de formation avec le soutien des services des ressources humaines, reposant sur du e-learning, facilitera la maîtrise des employés. La popularité des applications influe sur l'usage du Shadow IT.

La communication

Les communications internes maitrisées sont synonymes d'une organisation qui avance selon une stratégie commune. Les services informatiques doivent sortir de leur isolement et adopter une méthode de communication plus adaptée. Le marketing de la DSI est une démarche interne visant à rapprocher les métiers et le service informatique. Elle a comme objectifs de :

- Comprendre les besoins des métiers
- Construire des offres pertinentes liées aux enjeux métiers
- Renforcer la confiance des métiers envers la DSI
- Consolider la visibilité des offres et leur utilisation
- Assister les métiers à la prise en main des nouvelles offres du catalogue de service
- Assurer une gestion parfaite des offres et de l'innovation

La DSI et le marketing travailleront ensemble pour réaliser ces objectifs. Cette démarche ciblant les métiers et leur vision de la DSI effectue un marketing stratégique tout en analysant les retours. Le service informatique pourra mettre en évidence leur rôle central dans la transformation digitale de l'entreprise.

La communication de la DSI via cette démarche sera plus efficace sur les métiers. Les campagnes de communication comme les règles d'utilisation du SI et la sécurité informatique en entreprise pourront s'appuyer sur cette méthode. La communication régulière des règles, des outils disponibles en entreprise et leur utilisation permettront de réduire l'utilisation du Shadow IT.

3. Organisation de la DSI

L'analyse du Shadow IT

Après l'avoir détecté, la DSI devra qualifier le Shadow IT afin de différencier les innovations des utilisations dangereuses pour l'entreprise. Le modèle d'évaluation des instances Shadow IT du professeur Rentrop évalue leur criticité et définit leur priorité de traitement en se basant sur les principes d'ITIL (37).

Veuillez vous référer à la page 39 pour une explication du modèle. La DSI devra s'organiser et mettre en œuvre cette méthode. Elle facilitera la prise de décision et les actions à entreprendre contre les instances Shadow IT de l'entreprise. Les innovations ainsi détectées seront des sources de valeur pour l'organisation; elles pourront être intégrées dans sa gouvernance du SI. L'analyse du Shadow IT contribue indirectement à sa limitation.

La prévention

La DSI doit prévenir l'arrivée de nouveaux besoins provoquant l'adoption du Shadow IT. Le recrutement d'une personne qualifiée pour effectuer régulièrement cette prévention auprès des métiers sera nécessaire. Il fera partie de la DSI mais sera proche des métiers et du marketing. Il sera désigné comme le « Business Needs Manager » (BNM), le responsable des besoins métiers.

Il aura comme missions de :

- Mettre en place un planning de rencontre et d'écoute avec les métiers.
- Informer et sensibiliser les métiers
- Participer aux campagnes de communication
- Analyser les retours
- Qualifier les besoins métiers listés durant les campagnes marketing de la DSI.
- Retranscrire les besoins en projet.
- Valider et présenter ses actions et résultats à la DSI
- Présenter un plan d'action aux métiers

Si l'entreprise n'a pas le budget pour recruter ce profil, elle peut désigner une ou des personnes volontaires de la DSI pour réaliser ces missions. La qualité et l'efficacité de la prévention seront amoindries.

Figure 40. – Prévention du Shadow IT : Business Needs Manager

Une DSI plus réactive et plus proche des métiers lui donnera un avantage stratégique dans sa mission de création de valeurs. La prévention sera un vrai moteur d'innovation pour l'entreprise et permettra de réduire l'adoption du Shadow IT.

Le traitement

Après avoir évalué le Shadow IT avec la méthode Rentrop, plusieurs choix s'offrent à l'entreprise. Je propose les actions suivantes afin de capitaliser sur le long terme et de limiter l'utilisation du Shadow IT.

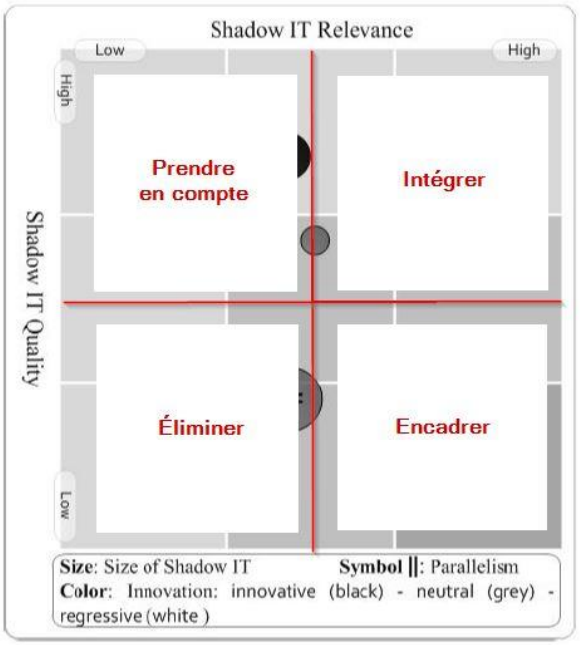


Figure 41. – Traitement : Actions face au Shadow IT

Pertinence	Qualité	Actions
Haute	Haute	**Intégrer** : L'application Shadow IT est de qualité et représente un fort besoin pour le métier. Il faudra l'intégrer dans le SI en respectant les exigences de sécurité (GDPR-READY), sinon il faudra l'encadrer.
Haute	Basse	**Encadrer** : Application dangereuse pour l'entreprise à cause de sa qualité et de la criticité du processus qu'elle touche. Fournir une solution équivalente aux métiers et planifier le blocage.
Basse	Haute	**Prendre en compte** : Application de qualité qui répond à un besoin non critique. Planifier son intégration en priorité basse.
Basse	Basse	**Éliminer** : Application non nécessaire et dangereuse. Sensibiliser et bloquer.

Tableau 16. – Traitement : actions face à la pertinence et la qualité du Shadow IT

La gestion de projet

L'échec d'un projet est dû en général à une mauvaise communication, un planning sous-estimé et des besoins qui évoluent dans le temps. Il existe plusieurs méthodes de gestion de projets utilisées dans les entreprises. Parmi les plus populaires, il y a la « traditionnelle », nommée Waterfall, et la « flexible », nommée Agile. En termes de retour d'expérience, le Standish Group Chaos Study a publié en 2019 les chiffres suivants (42):

Méthode	Réussi	Contesté	Échoué
Agile	42 %	50 %	8 %
Waterfall	26 %	53 %	21 %

Tableau 17. – Méthodes de gestion de projet : Taux de réussite

Ces chiffres indiquent que les méthodes agiles apportent plus de réussite. Utiliser les méthodes agiles pour la gestion de projets informatique de la DSI permettra de gagner en efficience bien qu'elles ne garantissent pas une réussite à 100%. Elles apportent aussi plus de communication et de retours avec les intéressés, ce qui entrainera une meilleure implication des parties prenantes et un meilleur relationnel.

L'implication de la DSI

Le rôle du département informatique va bien au-delà de la gestion de la technologie utilisée dans l'entreprise, il doit apporter de manière proactive de nouvelles applications qui prennent en charge la transformation numérique de l'entreprise.

La DSI n'est plus un centre de coûts, mais un fournisseur d'applications innovantes qui peuvent accroître les affaires des métiers de l'entreprise. Elle est le cœur d'une organisation complexe qu'elle doit rendre simple et agile pour tous les utilisateurs. Le service informatique doit être plus proche des métiers pour s'adapter à leur langage et répondre à leurs attentes.

Afin de mener à bien ce projet, la DSI devra travailler en étroite collaboration avec des sponsors. Le premier sponsor du projet sera le CODIR[29]. Le soutien de la direction sera révélateur des enjeux stratégiques liés au rôle de l'informatique. L'implication de la DSI dans les projets métiers informatiques génèrera de la valeur pour l'entreprise. Sa communication et son implication seront demandées et reconnues par les métiers. Les capacités et l'efficacité du département informatique lui permettront de proposer des innovations à ses sponsors.

Le niveau d'implication du département informatique détermine ses possibilités et ses capacités. Il se doit d'être géré et piloté afin d'apporter un rôle actif à la création de valeur.

[29] Comité de Direction

III. Guide méthodologique

Mon guide méthodologique a pour but d'aider les entreprises à limiter l'adoption du Shadow IT en s'appuyant sur les axes de ma démarche. Il est composé de trois étapes et d'un pilier.

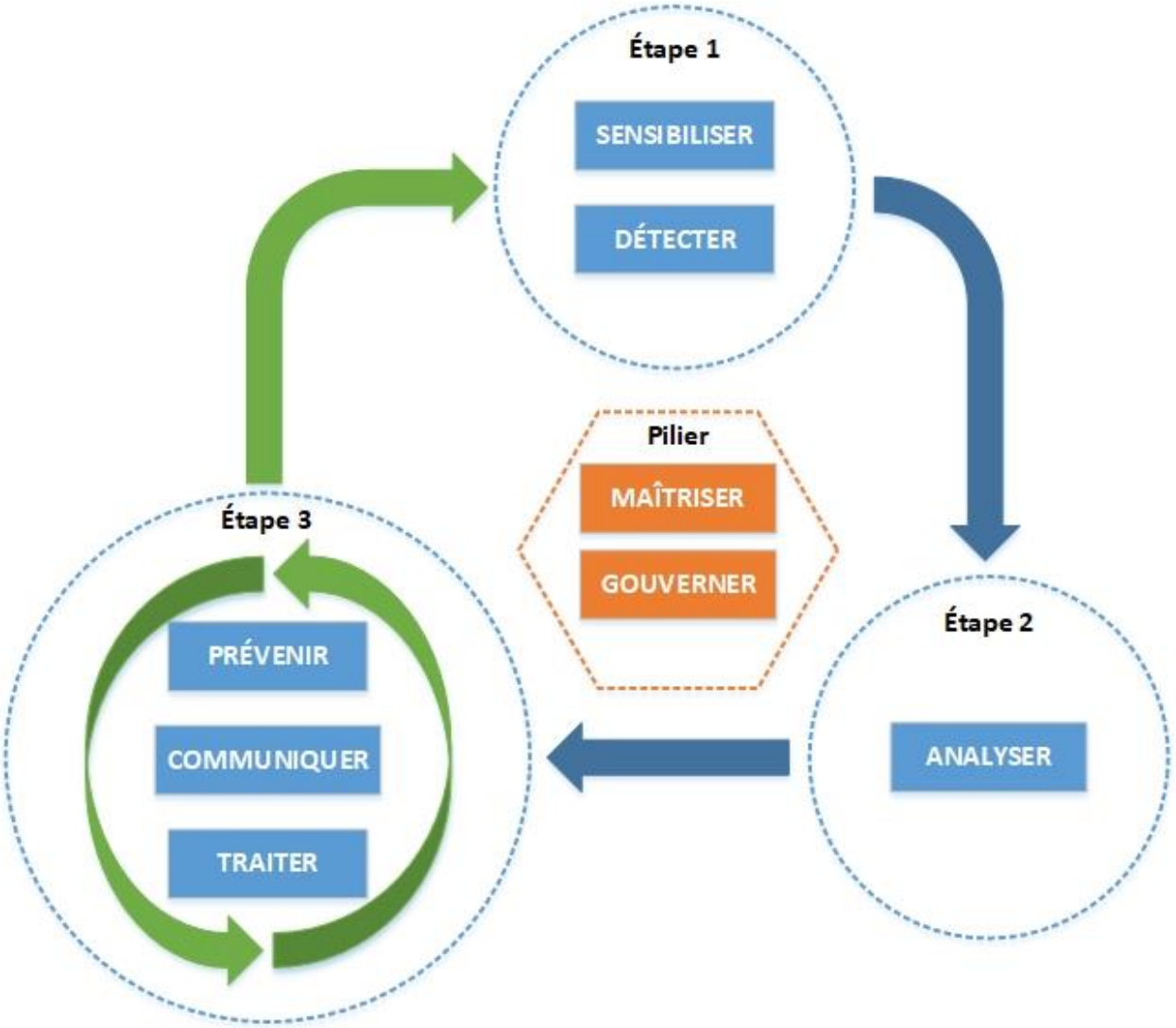


Figure 42. – Guide méthodologique : limitation de l'adoption du Shadow IT

Les étapes se suivent et reposent sur un pilier.

Étape 1

Elle consiste à détecter et sensibiliser. L'identification du Shadow IT permettra de prendre conscience de son ampleur et d'identifier ses caractéristiques. La sensibilisation supportera l'identification et la réduction du Shadow IT par la responsabilisation des employés et leur compréhension des enjeux de la sécurité informatique.

Étape 2

L'analyse du Shadow IT avec la méthode du professeur Rentrop permettra de le qualifier. L'analyse des observations et résultats de la sensibilisation permettront de mettre en place des plans d'action.

Étape 3

L'étape 3 est un travail perpétuel et intègre l'amélioration continue représentée par les flèches verte.

La prévention par le Business Needs Manager anticipera l'adoption du Shadow IT par les métiers. Son travail collaboratif avec le service Marketing identifiera les besoins et améliorera la relation du département informatique avec les services métiers.

Le marketing de la DSI appuiera efficacement la communication informatique. Elle est le point essentiel des actions, informations et relations de la DSI.

Le traitement représente les actions du département informatique pour la limitation du Shadow IT. Le Shadow IT sera traité en fonction de sa qualification via ma proposition. Les mises en place de plans d'action et de projets répondront aux besoins des services métiers.

La flèche verte allant de l'étape 3 à l'étape 1 représente la répétition et l'amélioration continue de la démarche.

Pilier

La démarche est réalisable si elle repose sur les éléments composant le pilier.

Le département informatique doit maîtriser le SI à l'aide de son urbanisation et de ses formations.

La direction et la gouvernance du SI doit accompagner et supporter cette démarche.

Conclusion

Cette thèse aborde plusieurs sujets comme la consumérisation, le cloud, l'évolution des systèmes d'information et le RGPD avant d'introduire le Shadow IT.

Hormis le RGPD, ces évolutions ont permis la croissance du Shadow IT reflétant la perte de contrôle du département informatique. La pression exercée sur les métiers a amplifié le phénomène au sein des entreprises.

La rigidité des directions des systèmes d'information est en cause. Le Shadow IT devient une menace pour les entreprises.

Les évolutions du SI et du département informatique limitent l'adoption du Shadow IT. Le rapprochement des métiers, l'implication de la DSI et l'amélioration de ses capacités permettent même son traitement et sa prévention. Une communication efficace renoue le dialogue avec les services métiers.

La capitalisation des innovations du Shadow IT et sa limitation sont possibles en appliquant mon guide méthodologique. Le but de cette thèse n'est pas d'apporter une réponse cartésienne ultime au phénomène mais bien d'ouvrir les débats et les réflexions sur les moyens et méthodes de limiter l'adoption du Shadow IT dans les entreprises.

I. Bilan de la thèse

La rédaction de cette thèse m'a permis d'étudier et de prendre du recul sur un sujet très intéressant.

La partie, que j'ai le plus apprécié, était l'analyse et l'interprétation du sondage. Pouvoir confronter l'avis des services métiers à ceux des services informatiques fut très enrichissant. La vision du phénomène sous différents angles m'a vraiment plu.

La synthétisation de la thèse et plus particulièrement de l'état de l'art fut la plus grande difficulté. L'énorme quantité d'informations intéressantes rend l'opération complexe.

Le sujet est large et permet des pistes d'approfondissement, comme l'amélioration de mon guide et de sa mise en place.

Références webographies

- 1. Web-Wikipédia https://en.wikipedia.org/wiki/Consumerization
- 2. Web-Riffnews https://labo-microsoft.supinfo.com/articles/consumit/
- 3. Web-Wikipédia : https://fr.wikipedia.org/wiki/Cloud_computing
- 4. Web-Markess : http://blog.markess.com/2019/07/quelles-perspectives-a-2021-pour-lecosysteme-cloud-en-france-barometre/
- 5 Livre : Benoît FILOCAMO, « Shadow IT dans nos entreprises : Transformer la gouvernance de son système d'information »
- 6. Livre : Karim BAHLOUL « IDC-Faire face aux enjeux du Shadow IT »
- 7.Web-Wikipédia : https://fr.wikipedia.org/wiki/R%C3%A8glement_g%C3%A9n%C3%A9ral_sur_la_protection_des_donn%C3%A9es
- 8.Livre-Netskope : « cloud report 3 out of 4 cloud apps in use not ready forgeneral data protection regulation »
- 9. Web Wikipédia https://fr.wikipedia.org/wiki/Ombre
- 10.Web-itsocial : https://itsocial.fr/enjeux/infrastructure/datacenter/quest-systeme-dinformation-5-meilleurs-articles-systeme-dinformation/
- 11.Web-Techopedia : https://www.techopedia.com/definition/28621/shadow-it
- 12.Web-Wikipédia : https://fr.wikipedia.org/wiki/Shadow_IT
- 13.Web-Wikipédia : https://en.wikipedia.org/wiki/Shadow_IT
- 14.Livre-Rentrop : « Praxis der Wirtschaflsinformatik »
- 15.Livre- Sandy BEHRENS & Wasana SEDERA : « Why Shadow Systems exist after an ERP implemantation »
- 16.Livre-Rentrop : « Shadow IT – Management and control of unofficiall IT »
- 17.Livre-Rentrop : « Shadow IT Evaluation model »
- 18.Livre-Rentrop : « On the Emergence of Shadow IT – A Transaction Cost-Based Approach »
- 19.Livre-Rentrop : « Managing Shadow IT instances – A method to control autonomous IT solutions in the business departements »
- 20.Livre-Rentrop : « Governing Identified Shadow IT by Allocating IT Task Responsibilities »
- 21.Livre- Rentrop : « The Influence of Shadow IT Systems on Enterprise Architecture Management Concerns »
- 22.Livre-Rentrop : « Shadow IT and Business-Managed IT: A Conceptual Framework and Empirical Illustration »
- 23.Livre-Rentrop : « Conceptualizing Shadow IT Integration Drawbacks from a Systemic Viewpoint »
- 24.Livre-Györy, Andreas Antonius Béla; Cleven, Anne; Uebernickel, Falk & Brenner, Walter : « Exploring the Shadow : IT governance approaches to user-driven innovation »
- 25-Livre-Thomas Chejfec : « Shadow It de la menace à l'opportunité »
- 26-Livre-Lucas Girardin et Emerich Imbart : « Digitalisation : nouvelle source de Shadow IT ? Comment la gérer? »

- 27-Web-Frost & Sullivan : https://www.zdnet.fr/actualites/le-shadow-it-un-risque-reel-pour-les-donnees-39850274.htm
- 28-Web-Landeck : https://www.ivanti.com/blog/survey-results-role-shadow-organization
- 29-Livre-ISACA : « Shadow IT Primer »
- 30-Webinaire-Alan McSweeney : « Shadow IT And The Failure Of IT Architecture »
- 31-Webinaire-Frédéric Hay : « Identifier et traiter le Shadow IT »
- 32-Livre- Thomas Chejfec : « résultats de l'enquête sur le phénomène du « shadow IT »
- 33-Web-Vanson Bourne : https://www.cio-online.com/actualites/lire-le-shadow-it-ne-se-cache-plus-9133.html
- 34-Livre-Symantec : « Shadow IT France 2017 »
- 35-Web-Gartner : https://itsocial.fr/partenaires/insight/avis-expert-insight/cloud-hybrid/top-10-previsions-gartner-cybersecurite/
- 36-Web-Gatner : https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2019/
- 37-Livre-AXELOS : ITIL® Foundation, ITIL 4 edition
- 38-Livre-Longépé Christophe : Le projet d'urbanisation du S.I. - 4ème édition - Cas concret d'architecture d'entreprise
- 39-Livre- Desfray Philippe & Raymond Gilbert : TOGAF, Archimate, UML et BPMN - 3e édition
- 40-WEB-BPMS : https://www.bpms.info/architecture-d-entreprise-la-tour-de-babel/
- 41-WEB-Gartner : https://www.microsoft.com/security/blog/2019/10/29/gartner-microsoft-leader-2019-cloud-access-security-broker-casb-magic-quadrant/
- 42-Web-Standish Group Chaos Study : https://vitalitychicago.com/blog/agile-projects-are-more-successful-traditional-projects/

I. Glossaire

- - A - -

Architecture d'entreprise : Démarche de transformation du SI qui consiste à aligner les services et composants du SI sur les besoins métiers tout en le rendant plus agile et plus performant.

Arpanet : Advanced Research Projects Agency Network, est le premier réseau développé aux États-Unis, c'est l'ancêtre du réseau internet.

- - B - -

BYOA : Bring Your Own Applications, utilisation d'une application personnel dans le cadre du travail.

BYOD : Bring Your Own Device, utilisation d'un appareil personnel dans le cadre du travail.

- - C - -

Cloud computing : L'informatique en nuage consiste à exploiter la puissance de calcul ou et de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet.

COBIT : Control Objectives for Information and related Technology est un référentiel pour la gouvernance des systèmes d'information

- - D - -

Digitalisation : Transformation d'une entreprise pour intégrer de plus en plus de nouvelles tendances de l'informatique dans ses processus et dans sa relation client (Big data, application mobile, IOT)

DPO : Data Protection Officer, personne chargée de la protection des données au sein d'une organisation.

DSI : La direction des systèmes d'information est l'organisation qui est responsable dans une entreprise de la gestion et du bon fonctionnement du système d'information, elle est en charge des données et de l'informatique.

- - E - -

ENIAC : Numerical Integrator Analyser and Computer, c'est le premier ordinateur entièrement électronique.

ERP : Entreprise Resource Planning, Il s'agit d'un système d'information qui gère et surveille quotidiennement toutes les informations et les services opérationnels de l'entreprise.

- - F - -

Framework : Le Cadre est une structure réelle ou conceptuelle destinée à servir de support ou de guide pour la construction de quelque chose.

- - H - -

Hosting : Le fait d'héberger des ressources cloud du client.

Housing : Le fait d'héberger des équipements appartenant au client, non à l'hébergeur.

- - I - -

IaaS : L'infrastructure en tant que service ou, en anglais, infrastructure as a service est un modèle où l'entreprise dispose sur abonnement payant d'une infrastructure informatique (serveurs, stockage, sauvegarde, réseau) qui se trouve physiquement chez le fournisseur.

Infraction : L'infraction est une violation d'une loi ou d'une réglementation.

Infrastructure informatique : L'infrastructure désigne les équipements informatiques matériels : matériel informatique ; réseau informatique. L'infrastructure est un élément-clé pour réaliser une bonne interopérabilité entre les éléments des systèmes d'information, comme les logiciels.

IOT : Objet intelligent connecté à internet.

ISO 9001 : Série d'exigences concernant la mise en place d'un système de gestion de la qualité dans un organisme.

ISO 27001 : Série d'exigences internationale sur la sécurité des systèmes d'information. Elle définit les exigences pour la mise en place d'un système de management de la sécurité de l'information.

ITIL : Information Technology Infrastructure Library est un ensemble de livres sur les bonnes pratiques du management du système d'information

- - L - -

LAN : Un réseau local, Local Area Network, est un réseau informatique à une échelle géographique relativement restreinte, par exemple une salle informatique, une habitation particulière, un bâtiment ou un site d'entreprise.

- - P - -

PaaS : Plate-forme en tant que service, de l'anglais platform as a service, permet de mettre à disposition des entreprises un environnement d'exécution rapidement disponible, en leur laissant la maîtrise des applications qu'elles peuvent installer, configurer et utiliser elles-mêmes.

Problématique : elle est la présentation d'un problème sous différents aspects. La problématique représente un cheminement regroupant un thème, des interrogations évoquées par ce thème, une question précise et l'hypothèse que l'on en fait.

Processus : c'est la chaîne de valeur fournissant un bien ou un service à un client interne ou externe à l'entreprise, à partir d'un évènement de gestion initiateur. Cette chaîne de valeur est décrite par une séquence d'activités de transformation, indépendante de l'organisation, exécutée dans des conditions de délai et de qualité.

- - R - -

Référentiel : Base de données servant de source de vérité lorsqu'il s'agit de connaitre la valeur de certaines données

RGPD : Règlement Général sur la Protection des Données, c'est un règlement de l'UE pour la protection données à caractère personnel des citoyens européens

- - S - -

SaaS : Le logiciel en tant que service ou software as a service (SaaS) est un modèle de distribution de logiciel à travers le Cloud. Les applications sont hébergées par le fournisseur de service.

Scalabilité : Elle désigne la capacité d'un produit à s'adapter à un changement d'ordre de grandeur de la demande (montée en charge), en particulier sa capacité à maintenir ses fonctionnalités et ses performances en cas de forte demande.

Service Informatique : Service interne de l'entreprise qui gère le parc informatique.

Shadow IT : Ressource informatique qui compose le système d'information d'une entreprise sans l'accord de son responsable, la DSI.

SLA : Le service-level agreement est un document qui définit la qualité de service requise entre un prestataire et un client.

Système d'information : noté SI, il représente l'ensemble des éléments participant à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'entreprise.

- - T - -

Transformation numérique : désigne le processus qui consiste, pour une organisation, à intégrer pleinement les technologies digitales dans l'ensemble de ses activités.

Time-to-market : c'est le délai de mise sur le marché d'un produit ou d'une fonctionnalité.

- - U - -

Urbanisation des SI : L'urbanisation des SI est l'acte d'urbaniser les SI: cette démarche ou méthode fournit des principes et des règles, ainsi qu'un cadre cohérent, stable et modulaire, qui peut être référencé par différents organes décisionnels de l'organisation pour gagner en gestion avec l'organisation sur les décisions d'investissement pertinentes du SI.

- - V - -

VLAN : Un réseau local virtuel, communément appelé VLAN (Virtual LAN), est un réseau informatique logique indépendant permettant d'isoler logiquement un ensemble de machines sur le réseau.

VPN : Un réseau privé virtuel, communément appelé VPN (Virtual Private Network), est un système permettant de créer un lien direct entre des ordinateurs distants. La connexion entre les machines est gérée de façon transparente par le logiciel de VPN, créant un tunnel entre eux.

- - W - -

WAN : Un réseau étendu, (Wide Area Network), est un réseau informatique ou un réseau de télécommunications couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, ou de la planète entière. Le plus grand WAN est le réseau Internet.

WEB : World Wide Web, le réseau mondial est un système hypertexte public fonctionnant sur Internet.

II. Stealth IT

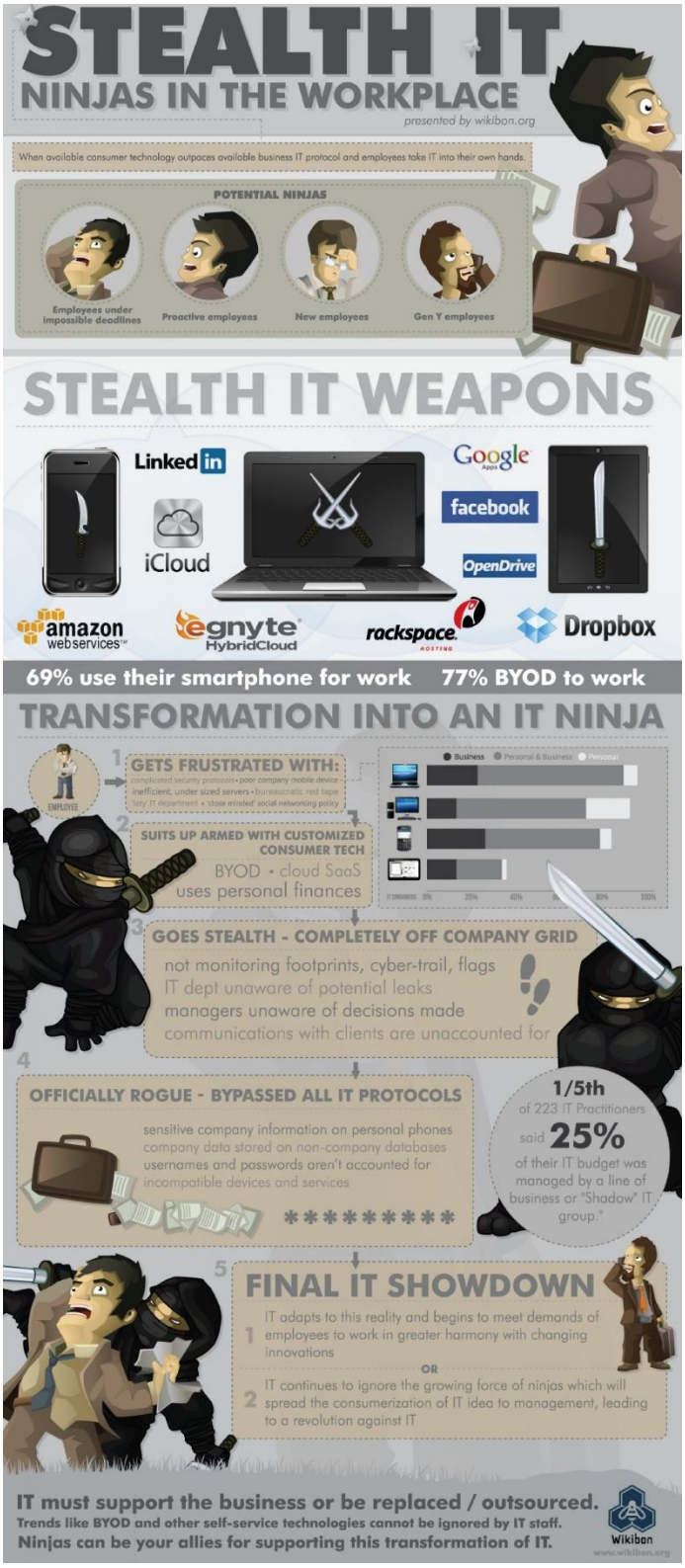


Figure 43. – Illustration Stealth IT

III. Sondage

Lien :
https://docs.google.com/forms/d/e/1FAIpQLSdIbZyHyKJBSJ1izUkJb1qTGXYy6tdFrQ69NO90iaRtOqMxgQ/viewform

Sondage Shadow IT

Ce sondage est anonyme et sera intégré à ma thèse : "Shadow cloud IT : conserver la maitrise du SI"

Au sein d'une entreprise, le terme "Shadow IT" désigne l'utilisation de systèmes informatiques, d'appareils, de logiciels, d'application et de service sans l'approbation explicite du département informatique.

Depuis quelques années les technologies numériques font une entrée fracassante dans les entreprises et les organisations publiques. On les retrouve dans tous les corps de métiers. Plébiscité par de nombreux collaborateurs pour leur simplicité d'usage et souvent disponibles gratuitement dans leur version de base, les services Cloud sont particulièrement représentés.

Cette pratique peut permettre de stimuler l'innovation et la productivité des employés, mais elle induit aussi des risques de sécurité.

Votre vision sur ce phénomène et vos réponses me permettrons d'obtenir une photographie plus claire de la réalité du terrain et m'aideront dans mon travail de recherche sur ce sujet.

Ce sondage dure 5 minutes.

Qu'est ce que le Shadow IT (Anglais) ?

Quelle est la taille de votre entreprise ? *

- ○ Microentreprise (<10 collaborateurs)
- ○ PME (<250 collaborateurs)
- ○ ETI (< 5000 collaborateurs)
- ○ Grande Entreprise (> 5000 collaborateurs)
- ○ Autre...

Quel est le secteur d'activité de votre entreprise *

- ○ Agroalimentaire
- ○ Banque / Assurance
- ○ Bois / Papier / Carton / Imprimerie
- ○ BTP / Matériaux de construction
- ○ Chimie / Parachimie
- ○ Commerce / Négoce / Distribution
- ○ Édition / Communication / Multimédia
- ○ Électronique / Électricité
- ○ Études et conseils
- ○ Industrie pharmaceutique
- ○ Informatique / Télécoms
- ○ Machines et équipements / Automobile
- ○ Métallurgie / Travail du métal Plastique / Caoutchouc
- ○ Services aux entreprises
- ○ Textile / Habillement / Chaussures
- ○ Transports / Logistique
- ○ Santé
- ○ Social

Quel poste occupez-vous ? *

Réponse courte

Depuis combien d'années occupez-vous ce poste ? *

- ○ Moins d'un an
- ○ Moins de 5 ans
- ○ Moins de 10 ans
- ○ 10 ans et plus

Faites vous partie du service informatique ? *

- ○ Oui
- ○ Non

1. Profil DSI :

Saviez-vous définir le shadow IT avant ce sondage ? *

- ○ Oui
- ○ Non
- ○ Pas avec exactitude

Pour vous, est ce que le shadow It est une menace ou une opportunité ? *

- ○ Menace
- ○ Opportunité
- ○ les deux

Pour vous, quelles sont les menaces générées par le shadow IT ? *

- ☐ Non-conformité avec la réglementation
- ☐ Sécurité
- ☐ Pertes de revenus
- ☐ Fuites de données
- ☐ Impact sur la réputation de l'entreprise
- ☐ Duplication des données : pertes de temps et d'argents
- ☐ Rupture du dialogue avec le service informatique
- ☐ Autre...

Avez-vous été confronté au shadow IT dans votre entreprise ? *

- ○ Oui
- ○ Non

Si oui, pouvez-vous donner un exemple de Shadow IT ?

Réponse courte

Est-ce qu'une politique d'utilisation du BYOD (Bring Your Own Device) est en place au sein de votre organisation ?

- ○ Oui
- ○ Non

Est-ce que le shadow IT est pris en compte dans votre management du Système d'information ? *

- ○ Oui
- ○ Non

Quelle sont les moyens mis en place face au shadow IT dans votre entreprise ? *

- ☐ Moyens techniques
- ☐ Formations et/ou sensibilisations
- ☐ Moyens organisationnels
- ☐ Aucun

Quelles sont les actions mises en place face au shadow IT dans votre entreprise ? *

- ○ Ne rien faire
- ○ Bloquer et interdire
- ○ Bloquer , interdire et sensibiliser
- ○ Autre...

Au sein de votre entreprise, comment évaluez-vous les relations entre le service informatique et les services métiers ? *

	1	2	3	4	5	
Très mauvaise	○	○	○	○	○	Très bonne

Au sein de votre entreprise, comment évaluez-vous la relation de la DSI dans les projets des directions métiers ? *

	1	2	3	4	5	
Très mauvaise	○	○	○	○	○	Très bonne

CC BY NC SA

Au sein de votre entreprise, la DSI est elle impliquée systématiquement dans les projets des directions métier ? *

- Oui
- Non

Considérez-vous que votre DSI possède les capacités et l'organisation pour répondre à tous les projets de l'entreprise ? *

- Oui
- Non

Souhaitez-vous me partager votre expérience face au shadow IT au cours d'une interview (10 min) ? *

- Oui
- Non

Si oui, merci de me transmettre votre e-mail :

Réponse courte

Utilisez-vous des outils ou logiciels non validés par la DSI ? *

- Oui
- Non

2. Profil Métier

Aviez-vous déjà entendu parler du shadow IT ou de l'informatique de l'ombre ? *

- Oui
- Non

Achetez-vous ou utilisez-vous des outils ou logiciels à l'insu de votre direction du système d'information (service informatique) ? *

- Oui
- Non
- Pas de système d'information (SI) ou pas de direction du système d'information (DSI)

Quelle est la fréquence d'achat ou d'utilisation de ces outils ou logiciels ? *

	0	1	2	3	4	5	
Jamais	○	○	○	○	○	○	Très souvent

Avez-vous déjà été en contact avec un fournisseur de service informatique ? *

- Oui
- Non

Si oui, pour quel besoin avez-vous contacté ce fournisseur ?

Réponse courte

CC BY NC SA

Est-ce que votre service informatique communique sur l'utilisation des outils et matériels de votre entreprise ? *

- ○ Oui
- ○ Non

Est-ce que votre service informatique communique sur la sécurité du système d'information ou la sécurité informatique ? *

- ○ Oui
- ○ Non

Comment évaluez-vous les relations en général entre vous et le service informatique ? *

	1	2	3	4	5	
Très Mauvaise	○	○	○	○	○	Très Bonne

Comment évaluez-vous la fréquence d'implication du service informatique dans vos projets métiers ? *

	1	2	3	4	5	
Jamais	○	○	○	○	○	Tout le temps

Comment évaluez-vous la relation entre le service informatique et vos projets métiers ? *

	1	2	3	4	5	
Très mauvaise	○	○	○	○	○	Très bonne

D'après-vous, quels sont les problèmes majeurs de votre service informatique (4 max) ? *

- ☐ Manque d'organisation du service informatique
- ☐ Besoin non pris en compte
- ☐ Processus trop long
- ☐ Manque d'innovation
- ☐ Trop rigide
- ☐ Communication insuffisante lors des projets
- ☐ Manque d'adaptation au contexte
- ☐ Eloignement physique du service informatique
- ☐ Utilisateur pris de haut
- ☐ Sous-effectif du service informatique
- ☐ Manque de budget

CC BY NC SA

Les outils ou logiciels ou matériels personnels sont ils autorisés par votre manager ? *

- Oui
- Non

Pensez-vous que les nouvelles générations présentent dans votre entreprise sont acteurs du shadow IT ? *

- Oui
- Non

Souhaitez-vous me partager votre expérience face au shadow IT au cours d'une interview (10 min) ?

- Oui
- Non

Si oui, merci de me transmettre votre e-mail :

Réponse courte

BY NC SA