Revue Internationale du Chercheur
ISSN: 2726-5889
Volume 4 : Numéro 3

Vers une meilleure adoption des normes de sécurité des systèmes d'information au Burkina Faso

Toward a better adoption of information systems security standards in Burkina Faso

LAMIEN Salia
Docteur
Sciences de gestion
Aube Nouvelle
Laboratoire de systèmes d'information, de gestion de l'environnement et du développement durable (LSI-GEDD)
Burkina Faso
lam.sal1150@gmail.com

Date de soumission : 12/07/2023

Date d'acceptation : 02/09/2023

Pour citer cet article :

LAMIEN S. (2023) «Vers une meilleure adoption des normes de sécurité des systèmes d'information au Burkina Faso», Revue Internationale du Chercheur «Volume 4 : Numéro 3» pp : 820 – 844

Résumé

L'objectif principal de cet article est de comprendre pourquoi certaines entreprises ont du mal à adopter la norme « ISO/CEI 27001 ». Cette recherche se propose donc d'éclairer ces réticences théoriquement et empiriquement à travers l'analyse de l'acceptation de cette norme au Burkina Faso. Pour répondre à la problématique dans le cadre d'un paradigme positivisme, la « Théorie Unifiée de l'Acceptation et de l'Utilisation de la Technologie (TUAUT) » est le modèle théorique utilisé et testé sur un échantillon de 185 organisations. Cette démarche quantitative confirmatoire mobilise deux méthodes d'analyse des données collectées : l'analyse factorielle en composantes principales (ACP) utilisant l'indicateur alpha de Cronbach et l'analyse par la méthode de la régression multiple. Les résultats sont en substance la confirmation que le comportement d'adoption des normes de sécurité des systèmes d'information peut être amélioré en agissant conséquemment sur les variables explicatives que sont : la performance attendue, l'effort attendu, l'influence sociale et les conditions de facilitation. Aussi, des solutions à l'absence de personnel qualifié, au manque de connaissances et à l'insuffisance de budget du système d'information peuvent favoriser la mise en conformité des systèmes d'information et par suite améliorer la performance et la résilience des organisations.

Mots clés : systèmes d'information ; normalisation ; sécurité ; performance ; résilience.

Abstract

The main purpose of this article is to understand why some companies are struggling to adopt the ISO/CEI 27001 standard. This research aims to shed light on these reservations theoretically and empirically through the analysis of the acceptance of this standard in Burkina Faso. To answer the problem in the context of a positivism paradigm, the "Unified Theory of Acceptance and Use of Technology (TUAUT)" is the theoretical model used and tested on a sample of 185 organizations. This quantitative confirmatory approach mobilizes two methods of analysis of the data collected: factor-based principal component analysis (PCA) using the cronbach alpha indicator and analysis by the multiple regression method. The results are essentially confirmation that the adoption behavior of information systems (SI) security standards can be improved by acting accordingly on the explanatory variables which are: expected performance, expected effort, social influence and facilitating conditions. Also, solutions to the lack of qualified personnel, lack of knowledge and insufficient budget of the information system can promote the compliance of information systems and consequently improve the performance and resilience of organizations.

Keywords: information systems; standard; security; performance; resilience.

Introduction

Les systèmes d'information (SI) jouent davantage un rôle essentiel tout au long de la vie d'une entreprise. Dans de nombreuses entreprises, l'utilisation des systèmes d'information combinés aux technologies Internet est devenue une condition de fonctionnement et de développement, voire de survie. Ainsi, presque tous les secteurs d'activités dépendent de l'utilisation des systèmes d'information, notamment le commerce électronique, les secteurs des services, les secteurs industriels, etc. En effet, y sont consignés dans ces systèmes d'information, des informations qui sont parfois très sensibles dont la gestion est aussi problématique : "les informations, c'est ce qu'il y a de plus difficile à obtenir, c'est ce qu'il y a de plus dangereux à fournir". Un défi est donc livré en permanence entre la protection et la convoitise. Mais parfois le second l'emporte comme l'ANSSI au Burkina Faso l'indique : "en mai 2017 des hackers ont attaqué une dizaine de sites web du gouvernement et des institutions" (ANSSI, 2017). Ainsi, dans un environnement des affaires, qui n'a guère été aussi concurrentiel, les entreprises se doivent d'accroitre leur compétitivité pour faire face à cette concurrence, c'est alors que les systèmes d'information (SI) s'imposent de plus en plus comme un élément clé dans la stratégie de celles-ci. Les systèmes d'information acquièrent également un nouveau statut, celui de bien de consommation de plus en plus aligné aux objectifs des entreprises ou organisations. En effet, même si pour mieux juguler les crises de la concurrence, les entreprises font parfois recours aux opérations de fusion, d'acquisition, ou d'OPA (Offre Publique d'Achat), la possession d'une information stratégique de tiers compte cependant pour beaucoup. Si le désire d'obtenir des informations stratégiques d'autres entreprises existe, la question récurrente reste comment protéger ses propres informations stratégiques ou globalement son système d'information ?

Sécuriser des données et des échanges, anticiper les risques d'intrusion et de piratage, fiabiliser le système d'information, assurer la continuité des services stratégiques, et bien d'autres enjeux conduisent donc de nombreuses organisations à définir et mettre en œuvre des politiques de sécurité, parfois formalisées, parfois empiriques. Cependant, une étude ISO 2019 sur la certification à la conformité aux normes de système de management ISO (International Organization for Standardization), montre que la répartition de certifications ISO/CEI 27001 par pays semble fortement disparate (ISO, 2020). Par exemples parmi les trois premiers pays ayant obtenus le plus de certificats au cours de l'année 2019 se retrouvent la Chine, le Japon, et les Royaumes Unis avec respectivement 8356, 5245 et 2818 certificats. En revanche la France est à la 20^{èm} position avec 351 certificats, et les pays africains comptent

parmi les derniers avec moins de 5 certificats pour la plus part. Comme le Benin, le Niger ou le Tchad, le Burkina Faso n'a obtenu aucun certificat. Au regard de cette propension des entreprises au Burkina Faso à aller vers la certification ISO/CEI 27001 (Organisation Internationale de normalisation / commission électrotechnique internationale 27001), la question de recherche se décline comme suit : **Dans quelle mesure les cas d'entreprises rechignées à adopter les normes de sécurité peuvent-ils être résorbés ?**

Toute entreprise est concernée par la sécurité de son information ou peut être sollicitée sur ce sujet par ses partenaires économiques. Ainsi, la pertinence de cette recherche se traduit par la capacité de résilience de l'information au sein des entreprises au Burkina Faso. Aussi, d'une part les résultats pourront servir à l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) à mieux cadrer l'élaboration des exigences en vue de l'établissement, de la mise en œuvre, de la tenue à jour et de l'amélioration continue des systèmes de management de la sécurité de l'information des entreprises privées et publiques. D'autre part sur le plan scientifique l'article s'adresse aux apprenants, aux professionnels du domaine, et contribue à enrichir la littérature sur la thématique de la sécurité des systèmes d'information au Burkina. L'intérêt de cette étude se noue donc avec l'objectif général qui est de : résorber les cas d'entreprises rechignées à adopter les normes de sécurité. Les objectifs spécifiques sont les suivants :

- Aider les entreprises au Burkina Faso à obtenir de meilleures performances, à réduire les risques et à se développer de façon durable.
- Identifier et évaluer les freins à la conformité aux normes de sécurité des systèmes d'information.
- Elaborer un ensemble de recommandations aux responsables des systèmes d'information et aux décideurs des entreprises pour renforcer la capacité des entreprises à répondre à leurs propres exigences en matière de sécurité de l'information.

Le positionnement épistémologique adopté est le positivisme. La méthodologie de cette recherche hypothético-déductive est une étude quantitative afin de confirmer ou infirmer les cinq hypothèses du modèle TUAUT (Théorie Unifiée de l'Acceptation et de l'Utilisation de la Technologie) de la recherche. À cet effet, une enquête quantitative sur la base d'un questionnaire est administrée à un échantillon de départ (240) d'une population mère estimée à 3142 organisations disposant d'un système d'information et œuvrant dans les secteurs d'activités banque-assurances, commerce, industries-BTP, services, transport-télécoms.

Cette recherche s'articule en trois phases que sont :
une phase d'exploration de la littérature mettant en exergue les différents enjeux de la sécurité du système d'information, l'analyse et la gestion des risques, et la démarche vers la normalisation ; une phase d'élaboration d'une méthodologie de recherche applicable au terrain (cible) de recherche et permettant de parvenir à des résultats scientifiquement qualifiés ; et une phase d'analyse des résultats issus de la collecte de données du terrain suivie d'une discussion scientifique qui imbrique étroitement le cadre théorique et le matériau empirique.

1. Revue de la littérature

1.1. Enjeux de la sécurité du système d'information : quel impact sur la résilience d'une organisation ?

Pour comprendre les enjeux de la sécurité du système d'information quelques notions de mots clés sont nécessaires. Dans la littérature, les systèmes d'information sont généralement définis soit à partir de leurs attributs, soit à partir de leurs fonctions (Ein-Dor, et al., 1978). Ainsi, les tentatives de définition restent centrées sur ce que le système fait, ou sur ce que le système est ou encore sur ceux de quoi le système est fait. Le système d'information peut alors être compris comme un ensemble de moyens matériels et humains organisés permettant la collecte, le traitement et la diffusion des informations (Aldosa, et al., 2003). L'une des plus récentes définitions est celle de Robert REIX dans une approche de gestion des systèmes d'information : « *un système d'information est un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures permettant d'acquérir, de traiter, stocker, communiquer des informations (sous forme de données, textes, images, sons) dans des organisations* » (REIX, 2002). Défini de manière plus large, le système d'information est un ensemble de composants inter-reliés. Ceux-ci recueillent, traitent, stockent et diffusent de l'information afin d'aider à la prise de décision, à la coordination, au contrôle, à l'analyse et aux capacités de représentation de situations au sein d'une entreprise.
Les processus de traitement, de stockage et de diffusion de l'information ne peuvent réellement contribuer à l'amélioration de l'efficacité et de la résilience d'une organisation que s'ils sont entièrement sécurités. Sécuriser l'information ou le flux d'informations dans une organisation est donc un enjeu qui intègre globalement la notion de sécurité du système d'information. La sécurité du système d'information est souvent définie à partir de ses enjeux étroitement liés aux quatre critères fondamentaux de la valeur d'une information (Godart,

2002) : la disponibilité, l'intégrité, la confidentialité, la preuve/contrôle (la non-répudiation ou l'irrévocabilité/"auditabilité"). À ces quatre critères fondamentaux s'ajoutent très souvent l'authentification, l'autorisation et la journalisation qui s'apparentent à la preuve/contrôle.

Très souvent des auteurs traitant de la sécurité des systèmes d'information considèrent certains de ces critères fondamentaux comme des objectifs de la sécurité des systèmes d'information. Dans les organisations les objectifs de la sécurité des systèmes d'information dépendent à priori des enjeux. En effet, les enjeux de performance commerciale sont étroitement en lien avec le système d'information (TRAORE, et al., 2023), dont l'acquisition est un investissement majeur (ZEROUAL, et al., 2021) surtout dans un contexte où la question des perceptions des acteurs de l'organisation sur son rôle véritable reste posée.

1.1.1. Quelles perceptions les acteurs des entreprises ont-ils de la sécurité du système d'information (SSI) ?

D'après la théorie de la contingence de Mintzberg les acteurs d'une entreprise selon les différents types de configurations organisationnelles n'ont pas le même degré de responsabilité (Mintzberg, 1982), conduisant ainsi à des relations différentes avec l'entreprise et donc avec le système d'information. La perception, qu'un responsable au sommet stratégique se fait de la sécurité du système d'information, ne peut être la même avec celle d'un employé du centre opérationnel au bas de la hiérarchie. Le directeur du système d'information (DSI) en collaboration très souvent avec le responsable à la sécurité du système d'information (RSSI), qui doit œuvrer à la stratégie du système d'information et élaborer une politique de sécurité de l'information (PSI), a une perception différente (de la SSI) de celle d'un autre salarié qui attend d'être sensibilisé sur la question de la sécurité. De même la perception (de la SSI) du directeur général de l'entreprise se situe dans une autre vision que celle des autres. En effet, tout directeur général doit jouer un rôle fondamental face aux multiples enjeux qui sont faillibles en cas d'attaque. Selon une publication de l'ANSSI France en 2016, la portée financière dépasse de très loin des postes informatiques à remplacer ou des systèmes à repenser intégralement. Dénis de service, défigurations, exfiltrations et divulgations de données, prises de contrôle d'un système informatique, mettent en jeu la crédibilité de l'organisation victime.

Au Burkina Faso les systèmes d'information sont une ressource porteuse pour l'émergence et le développement de capitaux au sein des organisations qui sont contraintes à faire face au marché concurrentiel et à la dématérialisation de plus en plus réelle dans un environnement

mondial où l'économie traditionnelle se transforme progressivement en économie immatérielle. Des enjeux qui passent également forcement par le défi sécuritaire des systèmes d'information. Ces enjeux sur la valeur du système d'information, associés à ceux sécuritaires sont malheureusement souvent mal pris en compte dans la stratégie globale des entreprises. Ce gap semble désormais en être une préoccupation bien comprise par les plus hautes autorités du Burkina Faso. En effet, depuis trois ans au Burkina Faso un forum national (FNSI) est initié par le ministère du développement de l'économie numérique et des postes au profit des directeurs des systèmes d'information. L'édition 2019 était placée sous le thème « modernisation du système d'information de l'administration burkinabè : quelle démarche globale pour les directions en charge du système d'information (DSI) ? ». Un double objectif était visé à ce forum de 2019 : accorder une attention particulière à l'évolution du système d'information de l'administration publique burkinabè, et permettre aux acteurs du numérique de s'accorder nécessairement sur une démarche globale pour créer un système cohérent, interopérable, fédérateur de l'ensemble des actifs et bien maîtrisé. Pour le premier responsable il s'agit là « d'un cadre d'échange d'idées et d'expériences permettant de créer diverses énergies, de renforcer la veille technologique, de comprendre les nouveaux enjeux du métier et défis des directions des systèmes informatique (DSI) ». Mais, parvenir à un encrage des structures en charge des services informatiques au sein de l'administration publique et privée burkinabè semble opportun. De ce fait, les questions telles que la carrière des informaticiens, la sécurité, la stratégie pour l'élaboration d'un schéma directeur et les meilleures pratiques en matière de gestion de projet informatique devront être traitées convenablement.

1.1.2. Sécurité du système d'information (SSI) et résilience d'une organisation

Le système d'information jusqu'ici considéré comme simple moyen d'informer l'ensemble des acteurs impliqués dans le fonctionnement de l'entreprise, grâce à des procédures de collecte, de traitement, de stockage et de diffusion des données bien établies, ne permet pas d'avoir une connaissance précise des capacités internes de l'entreprise et de l'environnement en mutation permanente. Une insuffisance qui trouve une réponse d'abord avec les travaux de recherches de Charles Wiseman qui donne une vision stratégique au système d'information (Rackoff, et al., 1985) (Wiseman, 1988). Plus tard Hubert Tardieu et Bernard Guthmann abordent dans la même approche le système d'information comme support à la stratégie de l'entreprise ou levier de l'avantage concurrentiel de l'entreprise (Guthmann, et al., 1991). Si le système d'information présente un avantage concurrentiel, la maîtrise d'une information de

qualité est aussi d'un intérêt stratégique et donc la question quant aux enjeux de sa sécurité reste préoccupante. En effet, les organisations devraient réfléchir aux conséquences financières sur leurs activités, leurs ventes de produits et services, d'une interruption totale de tous leurs systèmes, voire de la simple perte de données sensibles (données clients). Des conséquences qui sans doute affecteraient la résilience de l'organisation en termes de capacité à se développer bien, à continuer à se projeter dans l'avenir en dépit d'évènements déstabilisants, de conditions de vie difficiles, de traumatismes parfois sévères. Fort est de savoir que la contribution du système d'information à la résilience aux autres actifs de l'entreprise dépend de l'apport de l'utilisation d'une application ou d'un service informatique en termes de : la réduction de temps de travail, la diminution de litiges et de pertes d'affaires grâce à des informations plus fiables, l'obtention de chiffres d'affaires, l'amélioration d'une image de marque.

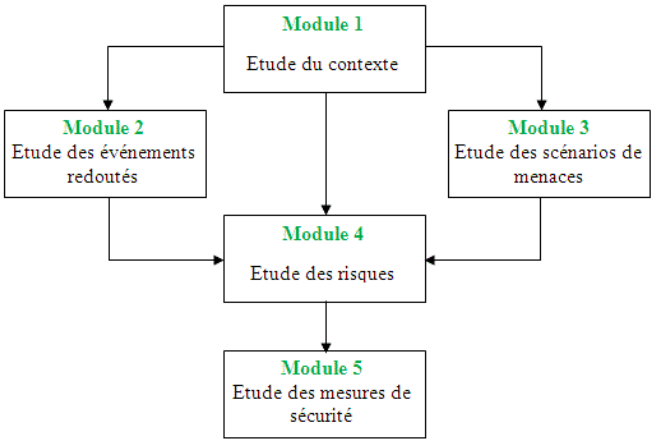
1.2. Analyse et gestion des risques : démarche vers la normalisation

1.2.1. Analyse et gestion des risques

Les objectifs de sécurité sont identifiés par l'analyse et la gestion des risques qui pèsent sur les ressources à protéger. Ces objectifs de sécurité visent donc à proposer des solutions organisationnelles et ou techniques susceptibles de protéger les actifs de valeur (données ou informations stockées, traitées, partagées, transmises ou extraites à partir d'un support électronique) contre les menaces qui conduisent à la perte, l'inaccessibilité, l'altération ou la divulgation inappropriée. Du fait des risques d'attaque du système d'information, les entreprises et les États s'investissent à une quête permanente de solutions proactives. Parmi ces solutions, se trouvent les méthodes d'analyse des risques sur le système d'information. Les méthodes les plus utilisées sont :

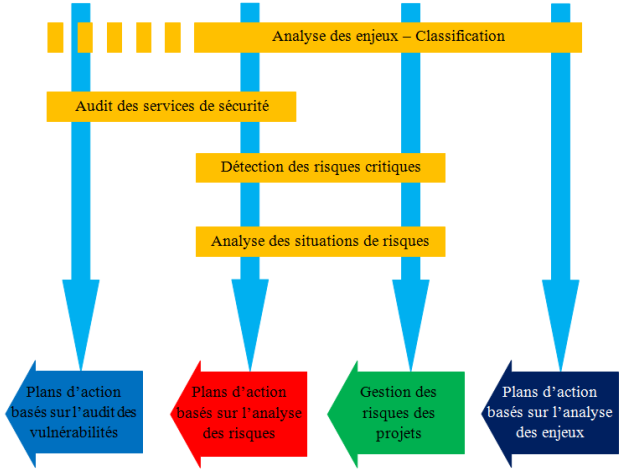
- EBIOS (expression des besoins et identification des objectifs de sécurité) développée par l'agence nationale de la sécurité des systèmes d'information (ANSSI).
- MEHARI (méthode harmonisée d'analyse des risques) développée par le club de la sécurité de l'information français (CLUSIF).
- CRAMM (CCTA Risk Analysis and Management Method) développée par l'organisation du gouvernement britannique ACTC (agence centrale de communication et des télécommunications).
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), développée par l'université de Carnegie Mellon aux États-Unis.

Figure 1 : Démarche globale EBIOS



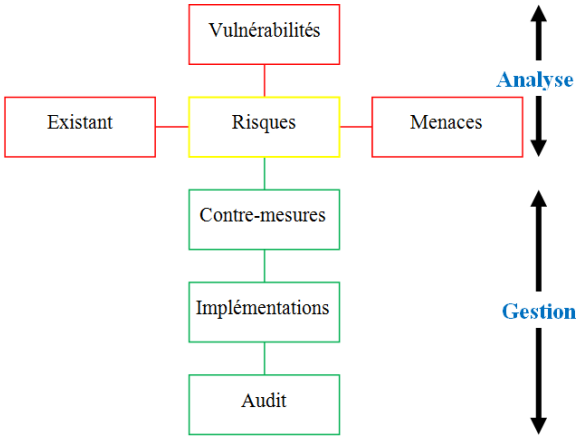
Source : ANSSI France (traduit du guide de la méthodologie EBIOS)

Figure 2 : Démarche globale de la méthode MEHARI



Source : Traduit de CLUSIF

Figure 3 : Démarche globale de la méthode CRAMM



Source : Traduit de CRAMM (Mayer, 2009)

Figure 4 : Démarche globale de la méthode OCTAVE

Source : Traduit de Software engineering Institute (Caralli, et al., 2007)

Ces méthodes sont appuyées des sensibilisations proposées par des organisations nationales aussi bien qu'internationales et des règlements ou lois étatiques. Dans de nombreux pays francophones la création d'une agence nationale de la sécurité des systèmes d'information (ANSSI) marque un engagement à la problématique de la sécurité de l'information. Toutefois, pour mener une offensive commune de protection de l'information, l'ISO recommande la norme ISO/CEI 27001 rendue publique en 2005. Si la norme ISO/CEI 27001, est désormais le référentiel pour tout acteur dans l'élaboration d'une politique de sécurité d'un système d'information, beaucoup d'incompréhensions demeurent en suspens quant à son adoption.

1.2.2. Démarche vers la normalisation

La norme est définie par ISO (International Organization for Standardization) comme suit : *« document établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné »* (ISO/CEI, 2011). La famille **ISO/CEI 27000** est composée de normes relatives à la gestion de la sécurité de l'information, actuellement au nombre de quatre : ISO/CEI 27001 : 2005, ISO/CEI 27002 : 2005, ISO/CEI 27005 : 2008, ISO/CEI 27006 : 2007.
L'ISO/CEI 27001 est conçu pour s'aligner ou s'intégrer au mieux avec les systèmes de gestion connexes au sein de l'organisation (qualité ISO 9001, ISO 14001). Pour aller vers la normalisation (approche globale, approche progressive) de son système de sécurité, une organisation se doit de mettre en œuvre son système de management du système d'information (SMSI) ou de l'amélioration en répondant aux éléments suivants :

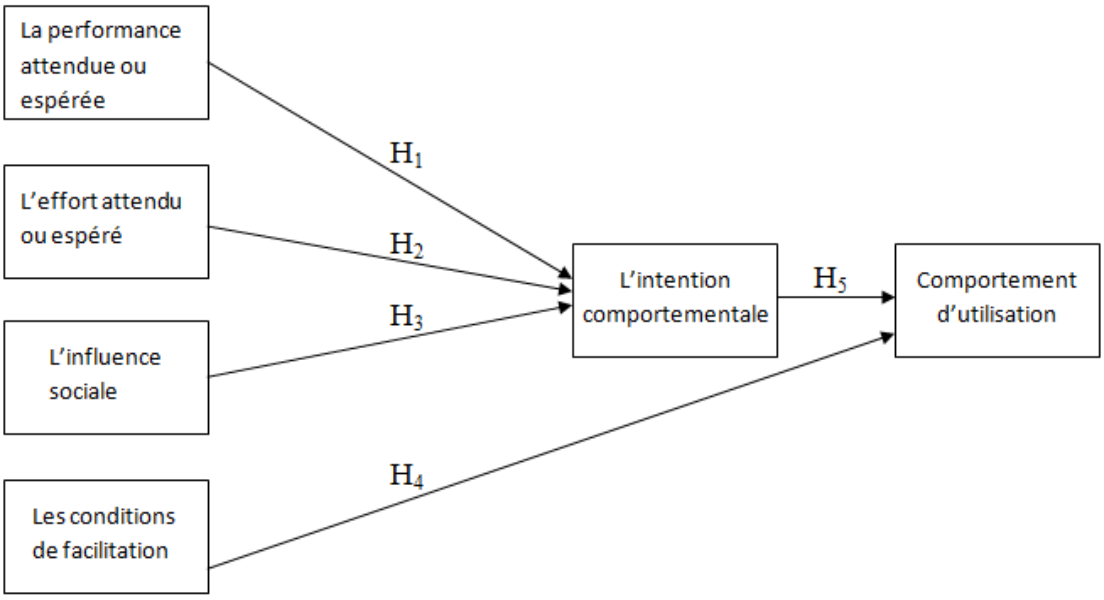
- Etablir un projet de mise en œuvre du SMSI, avec une méthode d'amélioration continue (Planifier, Déployer, Contrôler, Agir (PDCA)),
- Déterminer la motivation de la haute direction (hiérarchie), et définir une politique de sécurité de l'information et la répartition des fonctions et responsabilités,
- Evaluer par approche systémique des risques et des critères d'acceptation des risques, et évaluer les risques sur les actifs d'information importants de l'organisation,
- Identifier et évaluer les options concernant le traitement de ces risques (sélection des objectifs de contrôle et les contrôles à mettre en œuvre au besoin),
- Préparer une déclaration d'applicabilité et un plan de traitement des risques et mettre en œuvre le plan de traitement des risques et les contrôles prévus,
- Offrir une formation appropriée et des programmes de sensibilisation au personnel concerné,
- Gérer les opérations et les ressources conformément au SMSI et mettre en œuvre des procédures permettant la détection rapide des incidents de sécurité et les réponses à y apporter,

- Mettre en œuvre des procédures de surveillance, de réexamen, de test et d'audit, aussi mettre en œuvre des procédures pour l'examen du SMSI ainsi que des résultats de tests et audits en tenant compte d'un contexte de risque changeant, des nouvelles technologies ou de toute autre circonstance.

2. Méthodologie

Le choix de la méthodologie de recherche dans cet article est le positionnement épistémologique positivisme. Celui-ci est couplé avec une stratégie quantitative d'approche du terrain. Bien que TUAUT (Théorie Unifiée de l'Acceptation et de l'Utilisation de la Technologie) soit un modèle relativement récent (2003), plusieurs chercheurs ont été impressionnés entre autre de sa validité, sa consistance et de sa flexibilité à expliquer l'adoption des technologie dans divers domaines (Anderson, et al., 2006) (Carlsson, et al., 2006) (Li, et al., 2006) (Oshlyansky, et al., 2007) (Venkatesh, et al., 2003) (Wang, et al., 2005). D'où un choix approprié de ce modèle TUAUT pour analyser la conformité aux normes de sécurité des systèmes d'information des entreprises au Burkina Faso.

Figure 5 : Modèle TUAUT avec identification des hypothèses



Source : Traduit de UTAUT model (Venkatesh, et al., 2003)

Les variables du modèle TUAUT utilisées sont réparties en deux catégories : les variables dépendantes (VD) ou variables à expliquer (l'intention comportementale et le comportement d'utilisation) et les variables indépendantes (VI) ou variables explicatives (la performance attendue, l'effort attendu, l'influence sociale et les conditions de facilitation). Les hypothèses de recherche sont :

H_1 : la performance attendue influence positivement l'intention comportementale de normaliser la sécurité du système d'information. **H_2 :** l'effort attendu agit positivement sur l'intention comportementale dans la

formalisation de la sécurité de l'information. **H_3 :** l'influence sociale favorise l'intention comportementale d'adopter la norme de sécurité ISO/CEI 27001. **H_4 :** les conditions de facilitation influencent positivement le comportement d'utilisation de la norme de sécurité ISO/CEI 27001 du système d'information. **H_5 :** l'intention comportementale facilite le comportement d'utilisation des normes de sécurité des systèmes d'information. À partir de ce modèle de recherche des items sont formulés afin de pouvoir faciliter la vérification des différentes hypothèses sur le terrain.

Tableau 1 : Présentation des construits et items de la recherche

VARIABLES	ITEMS	SOURCES
La performance attendue ou espérée	**H_{1_1} :** La norme ISO/CEI 27001 permet de réduire les risques (de cyber sécurité) dans l'organisation **H_{1_2} :** La norme ISO/CEI 27001 inspire de la confiance au sein de l'organisation **H_{1_3} :** La norme ISO/CEI 27001 aide à la protection au sein de l'organisation **H_{1_4} :** La norme ISO/CEI 27001 aide à se conformer à la législation et à la règlementation **H_{1_5} :** La norme ISO/CEI 27001 permet d'accroitre le niveau de compétitivité **H_{1_6} :** La norme ISO/CEI 27001 permet de réduire les risques d'erreurs	(Davis, 1989) (Venkatesh, et al., 2000) (Venkatesh, et al., 2003)
L'effort attendu ou espéré	**H_{2_1} :** Les efforts d'implication des entités de l'organisation dans l'élaboration de la politique de sécurité de l'information (PSI) facilitent la formalisation de la sécurité de l'information. **H_{2_2} :** Le temps consacré dans le cadre des missions du RSSI aide à l'ancrage de la formalisation de la sécurité de l'information.	(Davis, 1989) (Venkatesh, et al., 2000) (Venkatesh, et al., 2003)
L'influence sociale	**H_{3_1} :** Le recours à l'infogérance et son suivi aide à l'adoption de la norme de sécurité ISO/CEI 27001 **H_{3_2} :** L'influence des collègues ou des supérieurs hiérarchiques exerce un effet significatif sur l'adoption de la norme ISO 27001 **H_{3_3} :** L'influence des collaborateurs ou des entreprises (ou institutions) partenaires exerce un effet significatif sur l'adoption de la norme ISO 27001 **H_{3_4} :** L'influence des clients exerce un effet significatif sur l'adoption de la norme ISO 27001 **H_{3_5} :** L'influence du gouvernement exerce un effet significatif sur l'adoption de la norme ISO 27001	(Moore, et al., 1991) (Venkatesh, et al., 2000) (Venkatesh, et al., 2003)
Les conditions de facilitation	**H_{4_1} :** L'existence d'une équipe permanente de veille à la sécurité de l'information est un soutien à l'adoption de la norme ISO 27001 **H_{4_2} :** L'existence de la fonction de responsable de la sécurité des systèmes d'information (RSSI) au sein de l'organisation facilite la normalisation de la sécurité de son système d'information. **H_{4_3} :** L'assistance technique facilite l'intention d'une organisation à normaliser la sécurité de son système d'information. **H_{4_4} :** L'évolution du degré de rattachement du RSI ou RSSI aux entités de l'organisation facilite la normalisation de la sécurité de son système d'information. **H_{4_5} :** La mise en place d'indicateurs et ou de tableau de bord de la sécurité des systèmes d'information (TBSSI) facilite la formalisation de la sécurité de l'information.	(Thompson, et al., 1991) (Venkatesh, et al., 2003)
L'intention comportementale	**H_{5_1} :** Le nombre d'audits ou de contrôles de sécurité du système d'information menés influence significativement le comportement d'adoption des normes de sécurité du système d'information. **H_{5_2} :** Le niveau de motivations qui déclenchent les audits est un aspect influençant sur le comportement d'adoption des normes de sécurité du système d'information.	(Fishbein, et al., 1975)

Source : auteur

Pour tester ce modèle sur le terrain, c'est-à-dire vérifier les différentes hypothèses, un questionnaire est administré principalement en ligne et quelquefois en copies aux responsables des systèmes d'information et autres décideurs au sein des entreprises. La population mère d'environ 3142 est constituée d'organisations disposant d'un système d'information et œuvrant dans les secteurs d'activités banque-assurances, commerce, industries-BTP, services, transport-télécoms. Puis la méthode d'échantillonnage utilisée est l'échantillonnage non probabiliste par convenance (c'est-à-dire une égalité de chance d'en faire partir). Aussi pour que l'échantillon soit représentatif, celui-ci dit échantillon théorique est fonction des paramètres suivants : p (proportion de la population mère ou probabilité de réalisation), t (coefficient de marge), e (marge d'erreur estimée), n (taille théorique de l'échantillon) et la formule ($\boldsymbol{n=pt^2(1-p)/e^2}$). Ainsi, selon les valeurs attribuées à ces paramètres (par exemple pour cette enquête $p=0.5$; $t=1.44$; $e=0.06$) est déduit l'échantillon théorique ($n=144$). Par souci de recouvrir au moins 144 répondants (correspondant à l'échantillon théorique), 240 entreprises ont été contactées soit en leurs envoyant le lien du questionnaire en ligne, soit simplement en leurs faisant parvenir une copie du questionnaire.

Sur les 240 questionnaires administrés aux entreprises, 185 entreprises ont répondu : soit un taux de réponse de 77% (un taux un peu au dessus de celui préalablement estimé à 75% pour une représentativité acceptable). Parmi ces 185 réponses, 8 ont été invalidées pour les raisons suivantes : 7 invalidées pour un taux de remplissage aux questions en deçà de 50%, 1 invalidée car cette entreprise n'est pas régulièrement enregistrée sur la base des entreprises à la chambre du commerce et de l'industrie du Burkina Faso.

3. Présentation des résultats

L'analyse des données quantitatives est effectuée en trois grandes étapes : la création de variables, l'identification des variables aux données de l'échantillon, et la création de relations. De ce fait, ce sont les logiciels Sphinx iQ2 (tri à plat) et IBM SPSS Statistics 24 (statistiques descriptives, test-t, analyse factorielle et analyse de la fiabilité) qui sont utilisés dans cette analyse de données, parce qu'ils offrent une facilité et une qualité d'analyse des données. Dans cette étude deux méthodes d'analyse des données collectées sont mises en œuvre. La première méthode d'analyse est l'analyse factorielle en composantes principales (ACP) (tri croisé ou multi-varié) dont le but est la validation des échelles de mesure à travers la validité convergente et la fiabilité. L'indicateur utilisé à cet effet, est l'alpha de cronbach (Cronbach, 1951). La deuxième méthode d'analyse est l'analyse par la méthode de la régression multiple dont le but est d'expliquer (ou prédire) les relations entre les variables dépendantes et les variables indépendantes du modèle de recherche TUAUT utilisé. Cette méthode effectue des analyses déductives qui permettent de vérifier les hypothèses de la recherche. Le test de fiabilité des construits a donné le tableau récapitulatif suivant :

Tableau 2 : Récapitulatif de la fiabilité des construits

Construits			Statistique item	Analyse factorielle en composantes principales (ACP)		Fiabilité
Variables	**Items**		**Ecart type**	**Qualité de représentation**	**Variance expliquée**	**Alpha de Cronbach (α)**
H1 : performance attendue	H1_1	: (q6)	0,693	0,695	74,11%	0,820
	H1_2	: (q7)	0,640	0,758		
	H1_3	: (q8)	0,715	0,695		
	H1_4	: (q9)	0,806	0,580		
	H1_5	: (q10)	0,741	0,849		
	H1_6	: (q11)	0,684	0,869		
H2 : effort attendu	H2_1	: (q12)	0,542	0,666	61,878%	0,831
	H2_1	: (q13)	0,541	0,717		
	H2_1	: (q14)	0,987	0,515		
	H2_1	: (q15)	0,991	0,797		
	H2_1	: (q16)	0,991	0,827		
	H2_1	: (q17)	0,910	0,520		
	H2_2	: (q18)	0,590	0,672		
	H2_2	: (q19)	0,875	0,397		
	H2_2	: (q20)	0,611	0,652		
	H2_2	: (q21)	0,689	0,484		
	H2_2	: (q22)	0,746	0,558		
H3 : influence sociale	H3_1	: (q25)	0,273	0,905	71,578%	0,735
	H3_2	: (q26)	0,908	0,695		
	H3_3	: (q27)	0,878	0,760		
	H3_4	: (q28)	1,019	0,616		
	H3_5	: (q29)	0,712	0,602		
H4 : conditions de facilitation	H4_1	: (q30)	1,044	0,615	68,426%	0,865
	H4_3	: (q32)	0,621	0,856		
	H4_4	: (q33)	0,619	0,576		
	H4_4	: (q34)	0,874	0,697		
	H4_4	: (q35)	0,919	0,792		
	H4_4	: (q36)	0,845	0,601		
	H4_4	: (q37)	0,897	0,707		
	H4_4	: (q38)	0,915	0,762		
	H4_4	: (q39)	0,903	0,655		
	H4_5	: (q41)	0,093	0,855		
	H4_5	: (q42)	0,715	0,778		
	H4_5	: (q43)	0,719	0,682		
	H4_5	: (q44)	0,679	0,787		
	H4_5	: (q45)	0,769	0,591		
	H4_5	: (q46)	0,750	0,571		
	H4_5	: (q47)	0,760	0,746		
	H4_5	: (q48)	0,787	0,597		
	H4_5	: (q49)	0,651	0,695		
	H4_5	: (q50)	0,695	0,639		
	H4_5	: (q51)	0,793	0,572		
	H4_5	: (q52)	0,622	0,665		
	H4_5	: (q53)	0,598	0,614		
H5 : intention comportementale	H5_1	: (q54)	0,454	0,050	55,375%	0,553
	H5_2	: (q55)	0,120	0,566		
	H5_2	: (q56)	0,528	0,680		
	H5_2	: (q57)	1,011	0,499		
	H5_2	: (q58)	0,869	0,791		
	H5_2	: (q59)	0,878	0,736		

Source : auteur

Quant à la validité des hypothèses, elle a fourni les conclusions suivantes :

– Vérification de l'hypothèse **H_1**

Tableau 3 : Indicateurs de vérification de l'hypothèse H_1

	Indicateurs				
VI	**β**	**R^2**	**Coefficient de Ficher (F)**	**Signification de F (noté *p*)**	**VD**
H_{1_4}	0,232	0,159	16,087	0,000	H_{5_1} : (q54)
H_{1_5}	0,260				
H_{1_1}	-0,259	0,121	9,059	0,000	H_{5_2} : (q55)
H_{1_3}	0,432				
H_{1_4}	0,250	0,063	8,881	0,003	H_{5_2} : (q56)
H_{1_5}	0,365	0,133	20,464	0,000	H_{5_2} : (q58)
H_{1_3}	0,188	0,092	6,772	0,02	H_{5_2} : (q59)
H_{1_6}	0,205				

***β :** Coefficient des variables explicatives, **R^2 :** Indice de corrélation multiple R-deux*

Source : auteur

Avec (β<0 et p=0,000 ou p<0,05) la variable indépendante (VI) **H_{1_1}** est rejetée. Par contre les items **H_{1_3}** , **H_{1_4}** , **H_{1_5}** et **H_{1_6}** de l'hypothèse **H_1** sont acceptés. Donc une affirmation de l'hypothèse **H_1** c'est-à-dire que la performance attendue influence positivement l'intention comportementale de normaliser la sécurité du système d'information.

– Vérification de l'hypothèse **H_2**

Tableau 4 : Indicateurs de vérification de l'hypothèse H_2

	Indicateurs				
VI	**β**	**R^2**	**Coefficient de Ficher (F)**	**Signification de F (noté *p*)**	**VD**
H_{2_1} : (q14)	0,145	0,203	20,511	0,000	H_{5_1} : (q54)
H_{2_2} : (q20)	0,437				
H_{2_1} : (q12)	0,772	0,933	590,469	0,000	H_{5_2} : (q55)
H_{2_1} : (q13)	0,234				
H_{2_1} : (q17)	0,047				
H_{2_2} : (q18)	0,158	0,235	19,623	0,000	H_{5_2} : (q56)
H_{2_2} : (q20)	0,425				
H_{2_1} : (q16)	0,287	0,209	11,073	0,000	H_{5_2} : (q57)
H_{2_2} : (q19)	0,291				
H_{2_2} : (q21)	-0,197				
H_{2_1} : (q16)	0,442	0,196	31,125	0,000	H_{5_2} : (q58)
H_{2_1} : (q16)	0,439	0,265	23,024	0,000	H_{5_2} : (q59)
H_{2_2} : (q21)	0,160				

***β :** Coefficient des variables explicatives, **R^2 :** Indice de corrélation multiple R-deux*

Source : auteur

L'ensemble des items de l'hypothèse **H_2** retenus après filtrage par régression multiple SPSS sont acceptés ($\beta>0$ et $p<0,05$) à l'exception de **H_{2_2}** : (q21) ($\beta=-0,197$ et $p=0,000$) rejeté. Cela confirme **H_2** et donc l'effort attendu agit positivement sur l'intention comportementale dans la formalisation de la sécurité de l'information.

– Vérification de l'hypothèse **H_3**

Tableau 5 : Indicateurs de vérification de l'hypothèse H_3

	Indicateurs				
VI	**β**	**R^2**	**Coefficient de Ficher (F)**	**Signification de F (noté *p*)**	**VD**
H_{3_5} : (q29)	0,279	0,078	7,866	0,006	H_{5_1} : (q54)

***β :** Coefficient des variables explicatives, **R^2 :** Indice de corrélation multiple R-deux*

Source : auteur

L'analyse par régression linéaire de SPSS ne retient que l'item **H_{3_5}**, les quatre autres items (**H_{3_1}**, **H_{3_2}**, **H_{3_3}** ; **H_{3_4}**) étant filtrés (rejetés). Cela signifie que l'action du gouvernement impacte positivement une intention comportementale, à savoir le nombre d'audits ou de contrôles de sécurité du système d'information. D'où la confirmation de l'hypothèse **H_3** : l'influence sociale favorise l'intention comportementale d'adopter la norme de sécurité ISO/CEI 27001.

– Vérification de l'hypothèse **H_4**

Tableau 6 : Indicateurs de vérification de l'hypothèse H_4

	Indicateurs				
VI	**β**	**R^2**	**Coefficient de Ficher (F)**	**Signification de F (noté *p*)**	**VD**
H_{4_4} : (q33)	0,145	0,085	16,293	0,000	H_{5_1} : (q54)
H_{4_4} : (q33)	0,400	0,261	15,177	0,000	H_{5_2} : (q55)
H_{4_4} : (q37)	0,248				
H_{4_4} : (q38)	-0,196				
H_{5_2} : (q50)	-0,198				
H_{4_3} : (q32)	0,216	0,188	9,925	0,000	H_{5_2} : (q56)
H_{4_4} : (q34)	-0,131				
H_{4_4} : (q35)	-0,310				
H_{4_4} : (q38)	0,264				
H_{4_5} : (q52)	0,151				
H_{4_1} : (q30)	0,189	0,286	17,231	0,000	H_{5_2} : (q57)
H_{4_5} : (q44)	0,308				
H_{4_5} : (q46)	0,171				
H_{4_5} : (q51)	0,275				
H_{4_4} : (q35)	0,260	0,137	13,868	0,000	H_{5_2} : (q58)
H_{4_5} : (q51)	0,217				
H_{4_4} : (q35)	0,237	0,260	9,955	0,000	H_{5_2} : (q59)

H_{4_5} : (q42)	0,155				
H_{4_5} : (q44)	0,201				
H_{4_5} : (q46)	0,146				
H_{4_5} : (q51)	0,166				
H_{4_5} : (q52)	-0,244				

β : *Coefficient des variables explicatives,* ***R^2 :*** *Indice de corrélation multiple R-deux*

Source : auteur

Ce tableau de vérification des items de l'hypothèse **H_4** présente ceux identifiés comme prédicteurs suite à une analyse par régression linéaire. Parmi les vingt-deux (22) items (ou VI de **H_4**), treize (13) sont retenus et neuf (9) exclus par SPSS. Puis les variables indépendantes ayant obtenu un coefficient des variables explicatives négatif (β<0) sont rejetés et finalement onze (11) items sont acceptés. Cela permet de déduire que l'hypothèse **H_4** est confirmée et donc que les conditions de facilitation influencent positivement le comportement d'utilisation de la norme de sécurité ISO/CEI 27001 du système d'information.

– Vérification de l'hypothèse **H_5**

Selon le modèle TUAUT utilisé pour cette recherche, un lien d'influence existe entre l'intention comportementale et le comportement d'utilisation. D'autre part dans leurs travaux de recherche, des chercheurs tel que Ajzen conclut que l'intention comportementale influence directement le comportement d'adopter une technologie (Ajzen, 1991). En effet, de manière générale dans le cadre de cette étude, les variables intention comportementale et intention d'utilisation sont des variables exogènes peu nuancées. Ainsi, ces deux variables dépendantes, dans cette vérification des hypothèses peuvent être couplées en une seule variable. Les hypothèses H_1, H_2, H_3, H_4 étant confirmées, les variables dépendantes intention comportementale et intention d'utilisation peuvent être prédites par la combinaison des variables indépendantes : performance attendue, effort attendu, influence sociale et conditions de facilitation. Par conséquence l'hypothèse **H_5** est confirmée c'est-à-dire que l'intention comportementale facilite le comportement d'utilisation des normes de sécurité des systèmes d'information.

4. Discussion

4.1. Analyse de la validité des construits : sécurité et résilience du SI

Dans cet article le choix du positivisme comme posture épistémologique a permis d'élaborer un cadre théorique basé sur le modèle de recherche TUAUT dont les hypothèses sont vérifiées auprès des entreprises du Burkina Faso. À l'issue de cette confrontation du cadre analytique et du matériau empirique, la confirmation des différentes hypothèses est une conclusion de la recherche du terrain qui peut être discutée par approche avec la synthèse de la littérature. La validation de chaque hypothèse peut donc ainsi s'expliquer comme suit :

L'hypothèse **H_1** validée, signifie que la performance attendue influence positivement l'intention comportementale de normaliser la sécurité du système d'information. En effet, les articles (les paragraphes A5 à A15) de la norme ISO/CEI 270001 version 2005 décrivant les objectifs de sécurité et les mesures de sécurité, améliorent le niveau de sécurité lorsqu'ils sont bien implémentés par les principaux acteurs des organisations. De ce fait, le degré de responsabilité, tant bien que disparate selon Mintzberg (Mintzberg, 1982), de chaque acteur est également renforcé.

L'hypothèse **H_2** validée, signifie que l'effort attendu agit positivement sur l'intention comportementale dans la formalisation de la sécurité de l'information. En effet, selon Zeroual et Zeroualiuariti un système d'information est un investissement majeur (ZEROUAL, et al., 2021) qui peut donc permettre la formalisation de la sécurité de l'information. Aussi, la formalisation de la sécurité de l'information est facilitée par l'implication des entités de l'organisation dans l'élaboration de la politique de sécurité de l'information (PSI) sur divers aspects comme par exemples : la stratégie de la direction générale de mise à disposition de la DSI d'un budget conséquent, l'implication de la DRH par la mise à disposition de la DSI de personnel qualifié, l'intégration de modules sur la sécurité du système d'information dans les programmes de formation, la mise à niveau ou amélioration des compétences de tout les acteurs (personnel) de l'organisation.

L'hypothèse **H_3** est aussi validée c'est-à-dire que l'influence sociale favorise l'intention comportementale d'adopter la norme de sécurité ISO/CEI 27001. Cela s'explique grandement par l'influence du gouvernement sur l'adoption de la norme ISO 27001, notamment à travers les sensibilisations menées par ABNORM (Agence Burkinabé de Normalisation, de la Métrologie et de la Qualité), ANSSI (Agence Nationale de Sécurité des Systèmes d'Information), CIL (Commission de l'Informatique et des Libertés). Des actions qui peuvent éviter de stagner dans les tréfonds du classement comme le révèle une étude ISO 2019 sur la certification à la conformité aux normes ISO/CEI 27001 (ISO, 2020).

L'hypothèse **H_4** est confirmée et donc les conditions de facilitation influencent positivement le comportement d'utilisation de la norme de sécurité ISO/CEI 27001 du système d'information. En effet, la proposition d'un suivi technique ou une assistance technique, l'existence d'une équipe permanente de veille à la sécurité de l'information, ou encore l'existence de la fonction de responsable de la sécurité des systèmes d'information (RSSI), sont des dispositions que les dirigeants des organisations peuvent exiger ou observer pour aller vers la normalisation de la sécurité de leurs systèmes d'information. De sorte à s'aligner à cette vision de Rackoff, Wiseman ou Guthmann qui est d'en faire du système d'information un support à la stratégie de l'entreprise ou levier de l'avantage concurrentiel de l'entreprise (Rackoff, et al., 1985) (Wiseman, 1988) (Guthmann, et al., 1991).

L'hypothèse **H_5** est aussi confirmée et donc l'intention comportementale facilite le comportement d'utilisation des normes de sécurité des systèmes d'information. En effet, la DSI grâce à des audits fréquents ou à des contrôles réguliers de la sécurité du système d'information, en somme grâce à une élaboration d'une stratégie d'amélioration continue du management de la sécurité alliant la roue de Deming (PDCA) et le processus ITIL (Information Technology Infrastructure Library / ou Bibliothèque pour l'infrastructure des technologies de l'information) de gestion des incidents peut aller vers la normalisation de la sécurité et l'amélioration de la résilience de son système d'information. Cette veille de la sécurité permettra d'éviter des cas d'attaques comme celles évoquées par l'ANSSI en 2017 (ANSSI, 2017).

4.2. Freins à la conformité aux normes de sécurité des systèmes d'information

Le « test-t » pour l'échantillon unique est effectué avec le logiciel IBM SPSS Statistics 24 sur chacun des variables du questionnaire. Ce test permet de comparer pour chaque variable les moyennes de ses items à partir desquelles une moyenne de variable est générée. Ainsi, ce « test-t » a concerné également la troisième partie du questionnaire dont le but est de mieux focaliser les facteurs explicatifs à la réticence des entreprises dans l'application des normes de sécurité des systèmes d'information. Les résultats de ce « test-t » sur cette troisième partie, "freins à la conformité aux normes de sécurité des systèmes d'information" fournissent une moyenne minimale de 1,15 et une moyenne maximale de 2,93. La moyenne générale est 2,36. Trois éléments (freins) parmi la liste des 7 freins enquêtés ont leurs moyennes inférieures aux moyennes inférieures à la moyenne générale et les 4 autres freins ont leurs moyennes supérieures à la moyenne générale.

Tableau 7 : Niveau d'importance des principaux freins

	Peu importante	Importante	Très importante
Manque_de_connaissances	1,1%	5,2%	93,7%
Manque_personnel_qualifié	0,6%	6,3%	93,1%
Réticence_de_la_DSI	17,2%	64,9%	17,8%
Manque_de_budget	0,6%	10,3%	89,1%
Contraintes_organisationnelles	19,0%	67,8%	13,2%
Manque_de_temps	86,9%	10,9%	2,3%
Réticence_DG_utilisateurs	3,4%	28,2%	68,4%
Aucun			
Total	18,4%	27,6%	54,0%

Source : auteur

Interprétation : pour cette liste de freins proposés aux participants, 4 freins principaux ont focalisés leurs choix. Les moyennes de ces freins sont supérieures à la moyenne générale et donc ces freins sont identifiés comme étant les plus importants. Ainsi, leur classement par ordre d'importance est ci-dessous présenté :

- Manque de connaissances, assigné à la variable *manque_de_connaissances,* avec une moyenne de 2,93.
- Manque de personnel qualifié, assigné à la variable *manque_personnel_qualifié*, avec une moyenne de 2,93.
- Manque de budget, assigné à la variable *manque_de_budget*, avec une moyenne de 2,89.
- Réticence de la direction générale, des métiers ou des utilisateurs, assignés à la variable *réticence_DG_utilisateurs*, avec une moyenne de 2,65.

Les autres freins moins importants dont les moyennes sont inférieures à la moyenne générale, sont listés ci-dessous :

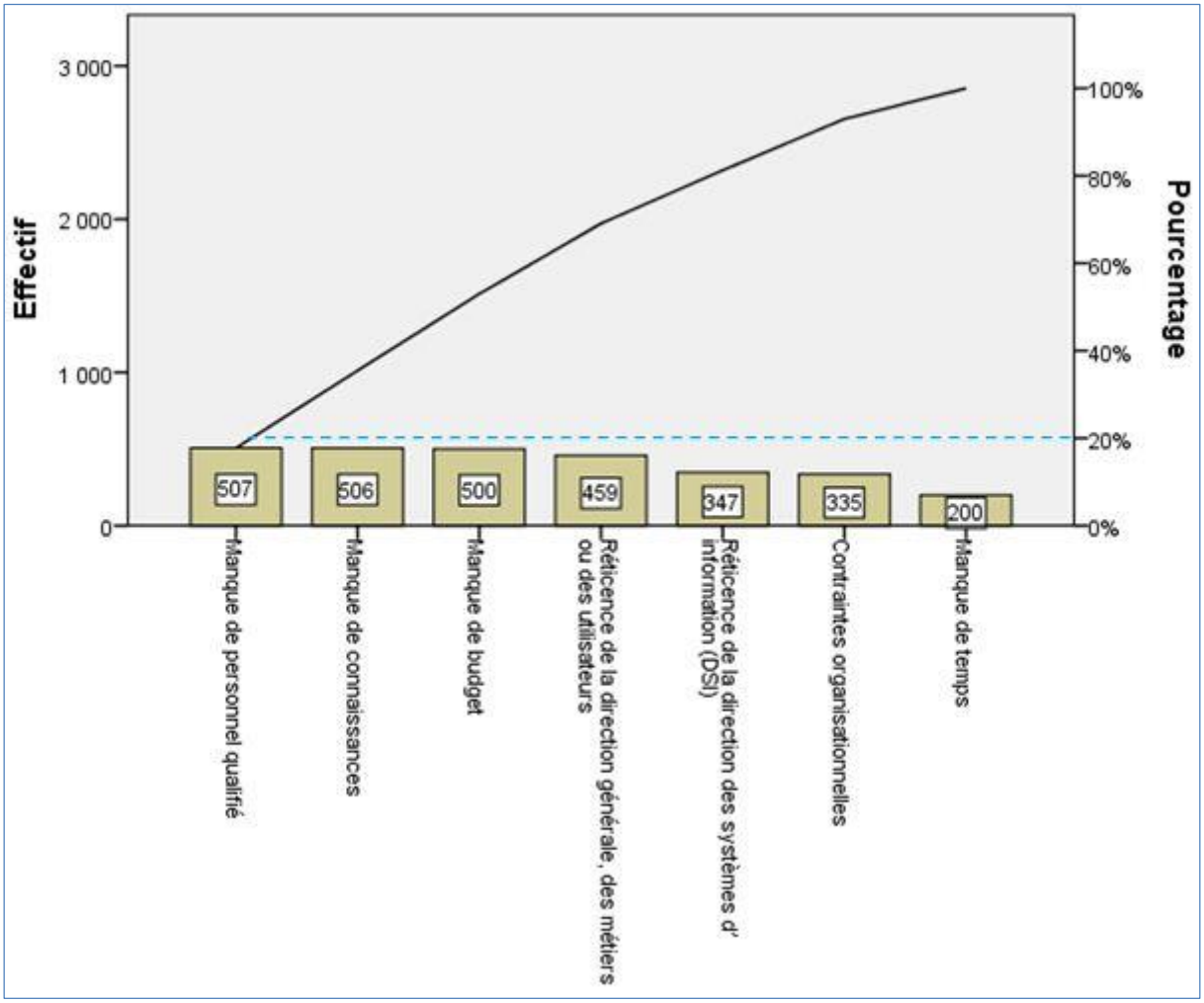
- Réticence de la direction des systèmes d'information (DSI), assigné à la variable *réticence_de_la_DSI*, avec une moyenne de 2,01.
- Contraintes organisationnelles, assigné à la variable *contraintes_organisationnelles,* avec une moyenne de 1,94.
- Manque de temps, assigné à la variable *manque_de_temps* avec une moyenne de 1,15.

Diagramme de Pareto :

L'analyse de la conformité aux normes de sécurité des systèmes d'information dans les entreprises au Burkina Faso, s'étend également à d'autres aspects tels que : les perceptions, les interprétations des acteurs faîtiers.

Quelles perceptions les acteurs des entreprises ont-ils de la sécurité du système d'information (SSI) ? Pour répondre à cette question, le recours au principe de Pareto permet de mettre en évidence les principaux freins à la conformité aux normes de sécurité des systèmes d'information dans les organisations au Burkina Faso.

Figure 6 : Diagramme de Pareto des principaux freins



Source : auteur

Le diagramme de Pareto ci-dessus (ou diagramme de causes à effets) permet de hiérarchiser les freins (ou problèmes) à la conformité aux normes de sécurité des systèmes d'information. Cette hiérarchisation est fonction du nombre d'occurrences et permet ainsi de définir des priorités dans le traitement des freins (ou problèmes). Ainsi, les répondants au questionnaire considèrent que le *manque de personnel qualifié* constitue le plus important frein. En revanche le *manque de temps* est selon ces répondants un frein peu important. La loi de Pareto est aussi l'application du principe des « quatre-vingts/vingt » (80-20 ou encore 80% des effets sont le produit de 20% des causes). Puisque dans cette étude 20% du cumule des valeurs des freins (cumule=2854) correspondent à 570,8 donc en conclusion apporter des solutions au *manque de personnel qualifié* et au *manque de connaissances* contribuerait à résoudre 80% du problème de la conformité aux normes de sécurité des systèmes d'information dans les organisations au Burkina Faso.

Conclusion

La concurrence et l'intégration des systèmes sont désormais des phénomènes incontournables pour les entreprises ou organisations. Leur acceptation nécessite d'apporter des solutions à leurs corolaires que sont principalement : la recherche de l'information stratégique, les attaques de systèmes d'information. Dans cet article un paradigme de recherche hypothético-déductive de type positivisme visait à déterminer l'acceptation des normes de sécurité des systèmes d'information au Burkina Faso. Les travaux de recherche empirique se sont focalisés autour du modèle de recherche "Théorie Unifiée de l'Acceptation et de l'Utilisation de la Technologie (TUAUT)". Un modèle simplifié qui est adapté à cette recherche basée sur cinq variables ou déterminants directs de comportement des individus par rapport à leurs intentions et usages de la technologie. Dans cette étude deux méthodes d'analyse des données collectées sont mises en œuvre. La première méthode d'analyse, est l'analyse factorielle en composantes principales (ACP) dont l'indicateur est l'alpha de cronbach (α). La deuxième méthode d'analyse, est l'analyse par la méthode de la régression multiple. Ces analyses de données sont effectuées avec les logiciels Sphinx iQ2 et IBM SPSS Statistics 24. La substance des résultats de cette étude montre que des facteurs tels que : la performance attendue, l'effort attendu, l'influence sociale notamment l'action du gouvernement, l'influence des conditions de facilitation, et l'intention comportementale, influencent le comportement d'adoption des normes de sécurité des systèmes d'information dans les entreprises ou organisations au Burkina Faso. Les décideurs et les responsables des systèmes d'information peuvent donc aller vers une meilleure adoption de la norme ISO/CEI 27001 en intégrant pas à pas ces facteurs d'une part grâce au processus d'amélioration continue (cycle de Deming) du système de management de la sécurité de l'information (SMSI) et d'autre part en apportant des solutions au manque de personnel qualifié et au manque de connaissances. Une démarche qui contribue également à améliorer la perception qu'ont les acteurs du système d'information sur la norme ISO/CEI 27001. Enfin, cet article vient mettre en exergue une analyse verticale et transversale d'adoption d'une norme au Burkina Faso en utilisant le modèle TUAUT couplé à l'analyse par la méthode de la régression multiple que propose IBM SPSS. En revanche, cette étude comporte quelques limites inhérentes au modèle TUAUT qui est simplifié des variables modératrices (âge, sexe, expérience et caractère obligatoire ou volontaire), dont une prise en compte pourrait renforcer le modèle, par suite élargir le champ de diversité du corpus et donc mieux préciser les résultats obtenus.

BIBLIOGRAPHIE

Ajzen, I. (1991). *The theory of planned behaviour, Organizational Behavior and Human Decision Processes.* (50:2), pp.179-211.

Aldosa, N., Le Bihan, M., & Monin, M. (2003). *Information, communication, organisation.* Bréal Rosny ; 2ème édition ; pp. 159 .

Anderson, J., Schwagner, P., & Kerns, R. (2006). The drivers for acceptance of tablet PCs by faculty in a college of business. *Journal of Information Systems Education, 17 (4)* , pp. 429-440.

ANSSI. (2017). *Plusieurs institutions visées par une importante cyberattaque.* Ouagadougou .

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process.* Carnegie Mellon: Software Ingineering Institute, Technical report ESC-TR-2007-012; pp.2-4 .

Carlsson, C., Carlsson, J., Hyvonen, K., Puhakainen, J., & Walden, P. (2006). Adoption of mobile devices / services : Searching for answers with the UTAUT. *Proceedings of the 39th Hawaii International Conference on Systems* , pp. 1-10.

Cronbach, L. (1951). *Coefficient alpha and the internal structure of test.* Psychometrika, 16, 3, pp. 297-334 .

Davis, F. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology.* MIS Quarterly, Vol. 13, pp. 319-339.

Ein-Dor, P., & Segev, E. (1978). *A classification of information systems: analysis and interpretation.* Tel-Aviv : Information Systems Research, vol 4, pp 166-204 .

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behaviour : an introduction to theory and research.* Addison-Wesley, Reading, MA.

Godart, D. (2002). *Sécurité informatique : risques, stratégies et solutions : échec au cyber-ro.* Edipro, pp.18 .

Guthmann, B., & Tardieu, H. (1991). *Le triangle stratégique : stratégie, structure et technologie de l'information.* les éditions d'organisation.

ISO. (2020). *Organisation internationale de normalisation*. Retrieved Décembre 12, 2020, from Organisation internationale de normalisation: https://www.iso.org/fr/the-iso-survey.html

ISO/CEI, D. (2011). *Règles de structure et de rédaction des Normes internationales.* Guide ISO, 6è édition, définition 3.1.1.

Li, J., & Kishore, R. (2006). How robust is the UTAUT instrument? Amultigroup invariance analysis in the context of acceptance and use of online community weblog systems. *Proceedings of the 2006 ACM SIGMIS CPR conference on Computer Personnel Research* , pp. 183-189.

Mayer, N. (2009, 07 08). Model-based Management of Information System. *https://theses.hal.science/tel-00402996* . University of Namur , Belgique: HAL, open science; pp. 43-44.

Mintzberg, H. (1982). *Structure et dynamique des organisations.* Paris: Les Editions d'Organisation, Montréal Les Editions Agence d'Arc .

Moore, G., & Benbasat, I. (1991). *Development of an instrument to measure the perceptions of adopting an information technology innovation, information systems research.* Vol. 2, pp 192-222 .

Oshlyansky, L., Cairns, P., & Thimbleby, H. (2007). Validating the unified theory of acceptance and use of technology (UTAUT) tool croos-culturally. In D. Ramduny-Ellis & D. Rachivides (Eds.). *Proceedings of the HCI 2007 , 2, BCS* , pp. 83-86.

Rackoff, N., Wiseman, C., & Ullrich, W. A. (1985). Information Systems for Competitive Advantage: Implementation of a Planning Process. *Academic Journal , 9* (4), pp. 285-294.

REIX, R. (2002). *systèmes d'information et management des organisations.* Paris: Vuibert, ed4, pp.67.

Thompson, R., Higgins, C., & Howell, J. (1991). *Personal computing: toward a conceptual model of utilization.* MIS Quarterly, (15:1), pp.124-143.

TRAORE, S., SIDIBE, A., & KAKA, Z. (2023). Effets des systèmes d'informations sur la performance commerciale des petites et moyennes entreprises (PME) au Mali: cas du district de Bamako. *Revue Internationale du chercheur. 4, 2* , pp. 465-484.

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). *User acceptance of information technology : toward a unified view.* MIS Quarterly, 27(3), pp. 425-478.

Venkatesh, V.; Davis, F.D. (2000). *A theoretical extension of the technology acceptance model: four longitudinal studies.* Management Science, 46 (2); pp. 186-204.

Wang, H., & Yang, H. (2005). The role of personality traits in UTAUT model under online stocking. *Contemporary Management Research, l(1)* , pp. 69-82.

Wiseman, C. (1988). *Strategic Information Systems.* McGraw-Hill Professional .

ZEROUAL, L., & ZEROUALIUARITI, O. (2021). Les systèmes d'information comme leviers de la performance logistique. *Revue Internationale des Sciences de Gestion. 3, 2* , pp. 711-730.