Revue Internationale de la Recherche Scientifique et de l'Innovation (Revue-IRSI)
ISSN: 2960-2823
Vol. 3, No. 3, Mai 2025

Les Systèmes d'Information des Ressources Humaines (SIRH) et risques cybernétiques : Un cadre intégré de contrôle interne, de résilience opérationnelle et de conformité légale

MIRDASSE Samir

Docteur en sciences économiques et gestion
Université Ibn Zohr, Agadir - Maroc
https://orcid.org/0000-0002-3100-5416

Résumé: Les Systèmes d'Information des Ressources Humaines (SIRH) jouent un rôle central dans la gestion moderne des RH, centralisant des données sensibles d'employés et automatisant des processus critiques. Cependant, leur sophistication technologique accroît leur exposition à des risques cybernétiques croissants, tels que les violations de données ou les rançongiciels, menaçant la continuité opérationnelle, la stabilité financière et la conformité réglementaire. Bien que la littérature existante aborde isolément la cybersécurité, le contrôle interne, la résilience opérationnelle et la conformité légale, une lacune majeure persiste : l'absence d'un cadre intégré unissant ces dimensions spécifiquement pour les SIRH. Cet article théorique propose un modèle conceptuel novateur comblant cette lacune en clarifiant les interactions entre les contrôles de cybersécurité, la culture organisationnelle, les systèmes de contrôle interne, la résilience opérationnelle et la conformité légale. À travers une revue systématique de la littérature, l'étude synthétise des recherches fragmentées pour élaborer un cadre holistique. Le modèle postule que des mesures de cybersécurité robustes et une culture organisationnelle proactive renforcent l'efficacité des mécanismes de contrôle interne, qui médiatisent à leur tour les améliorations de la résilience des SIRH et du respect des obligations légales. En intégrant des dimensions techniques, culturelles, gouvernantes et opérationnelles, le cadre offre une approche unifiée pour atténuer les cyberrisques dans les SIRH. La recherche enrichit le discours académique en fournissant une perspective interdisciplinaire pour appréhender la cybersécurité des SIRH, tout en proposant aux praticiens des recommandations pratiques pour aligner les investissements technologiques avec les stratégies de gouvernance et de conformité. Une validation empirique future est recommandée pour tester l'applicabilité du modèle dans divers contextes organisationnels, avec des implications pour affiner les protocoles de sécurité des SIRH et promouvoir une résilience adaptative dans un paysage numérique de plus en plus hostile.

Mots-clés : Systèmes d'Information des Ressources Humaines (SIRH) ; risques cybernétiques ; contrôle interne ; résilience opérationnelle ; conformité légale.

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**15480861**

1 Introduction

Les Systèmes d'Information des Ressources Humaines (SIRH) occupent une place centrale dans la gestion contemporaine des RH, en automatisant des processus essentiels tels que la gestion de la paie, le recrutement, ou encore l'évaluation des performances. Ces systèmes permettent de centraliser une masse considérable de données sensibles, incluant les informations personnelles des employés (noms, adresses, numéros de sécurité sociale), les dossiers médicaux, ainsi que les historiques professionnels. Cette centralisation, bien qu'elle optimise l'efficacité opérationnelle des départements RH, accroît leur exposition aux risques cybernétiques

(Carlson et al., 2025). Les cyberattaques, telles que les violations de données, les ransomwares ou les intrusions malveillantes, constituent une menace croissante : une étude de Balaouras et al. (2018) révèle que 55 % des entreprises ont subi une violation de données au cours des 12 derniers mois, souvent liée à des failles humaines ou technologiques (Zielinski, 2019). Les impacts de ces incidents sont significatifs : interruptions des opérations (à l'exemple d'un arrêt du traitement de la paie), pertes financières (amendes, coûts de remédiation) et atteinte à la réputation organisationnelle (perte de confiance des employés et des partenaires). Dans ce contexte, trois piliers émergent comme fondamentaux pour protéger les SIRH : le contrôle interne, la résilience opérationnelle et la conformité légale. Le contrôle interne, basé sur le cadre COSO (2013), fournit une structure pour sécuriser les données et garantir la fiabilité des processus RH. La résilience opérationnelle, conceptualisée par le NIST (National Institute of Standards and Technology) en 2018, vise à maintenir la continuité des fonctions critiques face aux perturbations cybernétiques (Cybersecurity, 2018). Enfin, la conformité légale, notamment avec le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne (European Union, 2016), impose des obligations strictes pour protéger les données personnelles, sous peine de sanctions sévères. Ces trois dimensions, interdépendantes, sont essentielles pour assurer la pérennité des opérations RH dans un environnement numérique de plus en plus hostile.

Malgré l'importance stratégique des SIRH Mirdasse et Jaouhari (2021), et la montée des cybermenaces, la littérature scientifique souffre d'une lacune majeure : l'absence de cadres intégrés combinant le contrôle interne, la résilience opérationnelle et la conformité légale pour gérer les risques cybernétiques spécifiques à ces systèmes. Les travaux existants tendent à traiter ces aspects de manière isolée. A titre d'illustration, Kavanagh et Johnson (2017) se concentrent sur les fonctionnalités des SIRH sans aborder leur sécurité, tandis que le cadre COSO (2015) adapte le contrôle interne à la cybersécurité, mais sans application directe aux SIRH. De même, les recherches sur la résilience opérationnelle (Cybersecurity, 2018) et la conformité légale (European Union, 2016) manquent d'une articulation cohérente dans une perspective globale. Cette fragmentation limite la capacité des organisations à élaborer des stratégies unifiées et efficaces pour protéger leurs SIRH contre les cyberrisques. Ainsi, la problématique centrale de cette étude peut être formulée comme suit : comment les contrôles de cybersécurité, la culture organisationnelle, le contrôle interne, la résilience opérationnelle et la conformité légale interagissent-ils pour sécuriser les SIRH face aux menaces cybernétiques, et comment ces interactions peuvent-elles être conceptualisées dans un cadre intégré ? Cette question vise à dépasser les approches parcellaires pour offrir une vision holistique de la gestion des risques dans ce domaine.

L'objectif principal de cet article est de proposer un modèle conceptuel théorique qui articule les relations entre les contrôles de cybersécurité, la culture organisationnelle, le contrôle interne, la résilience opérationnelle et la conformité légale dans le contexte des SIRH. Ce modèle cherche à combler les lacunes identifiées dans la littérature en intégrant ces dimensions dans une approche cohérente et unifiée, offrant ainsi une nouvelle perspective sur la gestion des cyberrisques. Plus précisément, l'étude poursuit trois sous-objectifs : (1) définir et contextualiser les concepts clés en lien avec les SIRH et les cybermenaces ; (2) formuler des hypothèses sur les interactions entre ces variables, en s'appuyant sur les travaux existants (COSO, 2013 ; Cybersecurity, 2018 ; Kavanagh & Johnson, 2017) ; et (3) développer un cadre théorique permettant aux chercheurs et aux praticiens de mieux comprendre et gérer les risques cybernétiques dans les SIRH. En combinant des dimensions techniques (contrôles de cybersécurité), culturelles (culture organisationnelle), gouvernantes (contrôle interne) et opérationnelles (résilience et conformité), cet article ambitionne de jeter les bases d'une gestion proactive et intégrée des risques dans un domaine devenu critique pour les organisations modernes.

L'article est structuré en quatre sections principales pour répondre aux objectifs fixés. La section 2, intitulée Revue de littérature, explore les concepts fondamentaux (SIRH, risques cybernétiques, contrôle interne, résilience opérationnelle, conformité légale) et met en lumière les insuffisances des recherches actuelles. La section 3, Cadre conceptuel, présente le modèle théorique proposé, en détaillant les variables explicatives, médiatrices et à expliquer, ainsi que les hypothèses qui sous-tendent leurs relations. La section 4, Discussion, examine les implications théoriques et pratiques de ce modèle, tout en reconnaissant ses limites et en suggérant des orientations pour des recherches futures. Enfin, la section 5, Conclusion, récapitule les contributions de l'étude et souligne son importance pour la recherche académique et la pratique professionnelle dans le domaine de la cybersécurité des SIRH.

2 Revue de littérature

2.1 SIRH : Définition et fonctionnalités

Le SIRH, ou Human Resource Information System (HRIS) en anglais, est une plateforme numérique conçue pour automatiser les processus de gestion des ressources humaines (GRH), centraliser les données sensibles des employés et soutenir la prise de décision stratégique dans les organisations modernes. Selon Broderick et Boudreau (1992), un SIRH est défini comme « the composite of databases, computer applications, and hardware and software necessary to collect/record, store, manage, deliver, present, and manipulate data for human

resources ». Cette définition met en évidence la capacité du SIRH à intégrer diverses fonctions RH dans un système unifié, facilitant ainsi la gestion efficace des informations et des processus (Mirdasse, 2024b). Historiquement, les SIRH étaient principalement utilisés pour des tâches administratives comme la gestion de la paie ou le suivi des absences, mais leur rôle s'est élargi avec l'évolution des technologies numériques (Mirdasse, 2024c). Aujourd'hui, ils englobent des fonctionnalités avancées qui répondent aux besoins opérationnels, tactiques et stratégiques des organisations (Bondarouk & Ruël, 2013).

Les fonctionnalités clés d'un SIRH incluent la gestion des données des employés, le traitement de la paie, l'administration des avantages sociaux, le recrutement et le suivi des candidatures, la gestion de la performance, la formation et le développement, le suivi du temps et des présences, ainsi que la gestion de la conformité. A cet égard, la gestion des données des employés permet de stocker des informations telles que les coordonnées personnelles, l'historique d'emploi et les évaluations de performance, assurant un accès rapide et sécurisé à ces données. Le traitement de la paie automatise le calcul des salaires, des impôts et des déductions, réduisant les erreurs humaines et améliorant l'efficacité (Carlson et al. (2025). De même, les modules de recrutement facilitent la publication d'offres d'emploi, la gestion des candidatures et la planification des entretiens, tandis que les outils de gestion de la performance permettent de suivre les objectifs et de fournir des retours continus aux employés. Les fonctionnalités de reporting et d'analyse de données sont particulièrement stratégiques, car elles permettent aux dirigeants RH d'identifier des tendances, comme les taux de turnover, et de prendre des décisions basées sur des données probantes (Bondarouk & Ruël, 2013). Pour illustrer ce propos, un tableau de bord analytique peut révéler des lacunes en compétences, orientant ainsi les programmes de formation pour aligner les ressources humaines sur les objectifs organisationnels. En centralisant les données sensibles et en automatisant les processus, le SIRH devient un outil indispensable pour les organisations cherchant à optimiser leurs opérations RH tout en répondant aux exigences de conformité et de performance dans un environnement numérique complexe (Mirdasse, 2024a).

2.2 Risques cybernétiques dans les SIRH

Les SIRH, en raison de la nature sensible des données qu'ils contiennent – telles que les numéros de sécurité sociale, les informations bancaires et les dossiers médicaux des employés – sont des cibles privilégiées pour les cyberattaques. Les risques cybernétiques affectant ces systèmes incluent les violations de données, les attaques par rançongiciel (ransomware), les menaces internes, les attaques de phishing et les vulnérabilités liées aux tiers. Ces menaces ont des impacts financiers, opérationnels et réputationnels significatifs, et leur prévalence est en augmentation, rendant la cybersécurité des SIRH une priorité stratégique pour les organisations.

Les violations de données constituent l'un des risques les plus graves pour les SIRH. Une violation peut entraîner l'accès non autorisé à des données personnelles, exposant les employés au vol d'identité et les organisations à des amendes pour non-conformité aux réglementations comme le RGPD. Comme en témoigne une étude de Balaouras et al. (2018) a révélé que 55 % des décideurs en sécurité des réseaux d'entreprise ont signalé au moins une violation de données au cours des 12 derniers mois, 44 % de ces violations étant causées par des employés exposant des données sensibles, intentionnellement ou non (Zielinski, 2019). Les attaques par rançongiciel sont une autre menace croissante, où des cybercriminels chiffrent les données du SIRH et exigent une rançon pour leur déverrouillage. Ces attaques peuvent paralyser des fonctions critiques comme le traitement de la paie, entraînant des perturbations opérationnelles majeures et des coûts financiers élevés (Foxall, 2024). Les menaces internes, qu'elles soient intentionnelles (telles qu'un employé mécontent volant des données) ou accidentelles (à l'image d'un employé cliquant sur un lien malveillant), représentent une part significative des incidents. Selon ISACA (2021), environ 60 % des violations de données sont attribuables à des menaces internes, soulignant l'importance des contrôles d'accès et de la formation des employés (Foxall, 2024). Les attaques de phishing visent à tromper les employés pour qu'ils divulguent leurs identifiants, permettant aux attaquants d'accéder au SIRH. Enfin, les risques liés aux tiers, tels que les fournisseurs de services cloud ou les plateformes de gestion des avantages sociaux, introduisent des vulnérabilités si leurs mesures de sécurité sont inadéquates (Story, 2024).

La prévalence croissante de ces risques est exacerbée par la dépendance accrue aux technologies numériques et par l'intégration des SIRH avec d'autres systèmes d'entreprise, ce qui élargit la surface d'attaque. Une étude de McLennan (2020) a révélé que 62 % des dirigeants considèrent le non-respect par les employés des règles de sécurité des données comme la principale menace à la cybersécurité, surpassant les pirates ou les fournisseurs. Ces impacts – financiers (amendes, coûts de remédiation), opérationnels (interruptions des processus RH) et réputationnels (perte de confiance des employés et des parties prenantes) – soulignent l'urgence de développer des stratégies robustes pour protéger les SIRH contre les cybermenaces.

2.3 Contrôle interne et cybersécurité

Le contrôle interne est un processus structuré visant à garantir la fiabilité des opérations, la conformité aux réglementations et l'atteinte des objectifs organisationnels. Le cadre du Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2013) est une référence mondiale pour la conception et l'évaluation des

systèmes de contrôle interne, comprenant cinq composantes interdépendantes : l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication, et la surveillance. Dans le contexte de la cybersécurité, ce cadre peut être adapté pour gérer les risques cybernétiques affectant les systèmes d'information, y compris les SIRH, en intégrant des mesures spécifiques pour protéger les données et assurer la continuité des opérations.

En réponse à l'escalade des cybermenaces, COSO a publié des orientations spécifiques, notamment « COSO in the Cyber Age » (2015), qui explique comment appliquer le cadre de contrôle interne à la gestion des cyberrisques. L'environnement de contrôle établit le ton organisationnel en matière de cybersécurité, comme en témoigne la promotion d'une culture où la protection des données RH est une priorité, soutenue par des politiques claires et l'engagement de la direction (COSO, 2015). L'évaluation des risques implique l'identification des menaces cybernétiques spécifiques au SIRH, telles que les violations de données ou les attaques par rançongiciel, et l'analyse de leur impact potentiel sur les opérations RH et la conformité légale. Les activités de contrôle englobent des mesures techniques, comme le chiffrement des données et l'authentification multi-facteurs (MFA), ainsi que des mesures procédurales, comme des audits réguliers de sécurité pour détecter les vulnérabilités dans le SIRH (Moeller, 2016). L'information et la communication garantissent que les politiques de cybersécurité sont clairement diffusées aux employés, avec des canaux pour signaler les incidents, tandis que la surveillance implique une évaluation continue de l'efficacité des contrôles à travers des revues périodiques et des tests de pénétration (COSO, 2015).

Dans le contexte des SIRH, le cadre COSO est particulièrement pertinent en raison de la sensibilité des données gérées. A titre d'illustration, les activités de contrôle peuvent inclure des contrôles d'accès basés sur les rôles (RBAC) pour limiter l'accès aux données RH aux seuls employés autorisés, réduisant ainsi le risque de menaces internes (Foxall, 2024). De plus, l'intégration des SIRH avec d'autres systèmes d'entreprise, comme les systèmes de gestion financière, nécessite des contrôles inter-systèmes pour prévenir les vulnérabilités croisées. En appliquant le cadre COSO, les organisations peuvent structurer leurs processus de cybersécurité pour protéger les SIRH, garantissant ainsi la fiabilité des données et la conformité aux exigences réglementaires.

2.4 Résilience opérationnelle

La résilience opérationnelle est définie comme la capacité d'une organisation à maintenir ses fonctions critiques face à des perturbations, y compris les cyberattaques, et à récupérer rapidement après un incident. Dans le contexte des SIRH, la résilience opérationnelle implique de s'assurer que des fonctions RH essentielles, telles que le traitement de la paie, la gestion des dossiers des employés et le recrutement, peuvent continuer ou être restaurées rapidement après un cyberincident. Cette capacité est cruciale pour minimiser les interruptions opérationnelles et maintenir la confiance des employés et des parties prenantes.

Des cadres comme le Framework de Cybersécurité du National Institute of Standards and Technology (Cybersecurity, 2018) offrent une approche structurée pour atteindre la résilience opérationnelle, avec cinq fonctions principales : Identifier, Protéger, Détecter, Répondre et Récupérer. Pour les SIRH, l'identification consiste à déterminer les fonctions RH critiques qui doivent être prioritaires, comme la paie ou la gestion des avantages sociaux. La protection implique la mise en place de mesures telles que des sauvegardes régulières, des systèmes redondants et des contrôles d'accès pour sécuriser ces fonctions. La détection nécessite des outils pour identifier rapidement les anomalies, comme des tentatives d'accès non autorisées au SIRH. La réponse inclut des plans pour isoler les systèmes affectés, communiquer avec les parties prenantes et limiter les dommages, tandis que la récupération vise à restaurer les opérations normales en utilisant des sauvegardes ou des processus alternatifs (Cybersecurity, 2018). De même, la norme ISO 27001, qui définit les exigences pour un système de gestion de la sécurité de l'information, inclut des dispositions pour la continuité des activités, applicables aux SIRH (ISO, 2013).

La résilience opérationnelle des SIRH repose également sur une préparation organisationnelle (Mirdasse, 2025). Les plans de continuité d'activité (BCP) spécifiques aux RH doivent inclure des procédures pour maintenir les opérations critiques pendant une perturbation. Pour illustrer ce propos, en cas d'attaque par rançongiciel rendant le SIRH inaccessible, une organisation peut recourir à des processus manuels pour traiter la paie ou utiliser des systèmes alternatifs pour gérer les absences (Brown, 2024). De plus, les départements RH jouent un rôle clé dans la communication pendant les crises, informant les employés des mesures prises et maintenant la confiance (Bravanti, 2023). En intégrant la résilience opérationnelle dans leurs stratégies, les organisations peuvent non seulement protéger leurs SIRH contre les cybermenaces, mais aussi garantir la continuité des services RH essentiels.

2.5 Conformité légale des données RH

La conformité légale des données RH est un enjeu majeur pour les organisations, en raison des réglementations strictes sur la protection des données personnelles, telles que le RGPD dans l'Union européenne et le California Consumer Privacy Act (CCPA) aux États-Unis. Ces lois imposent des obligations rigoureuses pour la collecte, le

traitement et la sécurisation des données des employés, qui sont particulièrement sensibles dans les SIRH en raison de leur contenu (ex. : numéros de sécurité sociale, informations médicales).
Le RGPD, entré en vigueur en 2018, exige que les organisations aient une base légale pour traiter les données personnelles, comme la nécessité contractuelle ou le consentement, et accorde aux employés des droits tels que l'accès, la rectification, l'effacement et la portabilité de leurs données (European Union, 2016). Les SIRH doivent être configurés pour faciliter ces droits, à l'appui de cette exigence, en permettant aux employés de consulter leurs données via un portail sécurisé ou en automatisant la suppression des données à la fin d'un contrat. De plus, le RGPD mandate des mesures de sécurité robustes, comme le chiffrement et les contrôles d'accès, et exige la notification des violations de données dans les 72 heures. Le non-respect peut entraîner des amendes allant jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial (Morris, 2025). Le CCPA, applicable aux résidents de Californie, impose des exigences similaires, bien que moins strictes, notamment le droit de savoir quelles données sont collectées et de demander leur suppression (California State Legislature, 2018). Pour les organisations multinationales, la gestion des données RH à travers différentes juridictions représente un défi majeur, car les exigences légales varient d'un pays à l'autre.
Les SIRH doivent également gérer les risques liés aux tiers, comme les fournisseurs de services cloud, qui doivent eux-mêmes être conformes aux réglementations (BasuMallick, 2024). Les défis incluent la mise à jour constante des systèmes pour répondre aux évolutions réglementaires, la formation des employés pour éviter les erreurs de conformité et la coordination avec les équipes juridiques pour auditer les processus. En intégrant des fonctionnalités de conformité, comme des journaux d'audit et des outils de gestion des droits des données, les SIRH peuvent aider les organisations à respecter ces obligations tout en minimisant les risques juridiques.

2.6 Lacunes dans la littérature

Malgré les avancées dans la recherche sur les SIRH, la cybersécurité, le contrôle interne, la résilience opérationnelle et la conformité légale, il existe une lacune significative dans la littérature concernant un cadre théorique intégré qui combine ces dimensions pour gérer les risques cybernétiques dans les SIRH. Les études existantes se concentrent souvent sur des aspects isolés : les fonctionnalités des SIRH sont bien documentées Kavanagh et Johnson (2017), les cadres de contrôle interne comme COSO sont appliqués à la cybersécurité (COSO, 2015), et les exigences légales comme le RGPD sont largement analysées (Morris, 2025). Cependant, peu de travaux articulent ces éléments dans un modèle unifié spécifique aux SIRH, qui tiennent compte de leurs interconnexions et de leur impact collectif sur la gestion des cyberrisques.
A ce titre, bien que des guides existent pour sécuriser les SIRH (Ungashick, 2024), ils se concentrent principalement sur les mesures techniques sans intégrer les aspects de résilience opérationnelle ou de contrôle interne. De même, les recherches sur la résilience opérationnelle abordent souvent des contextes généraux, sans application spécifique aux systèmes RH (Cybersecurity, 2018). Cette fragmentation limite la capacité des organisations à développer des stratégies cohérentes qui exploitent les synergies entre la technologie, la gouvernance et la conformité pour protéger les données RH et assurer la continuité des opérations. En outre, l'absence de modèles théoriques intégrés freine l'innovation dans les pratiques RH, car les organisations manquent de cadres clairs pour aligner leurs investissements technologiques avec leurs objectifs de cybersécurité et de conformité. Cette étude vise à combler cette lacune en proposant un cadre conceptuel qui articule les relations entre ces dimensions, offrant ainsi des perspectives théoriques et pratiques pour renforcer la gestion des risques cybernétiques dans les SIRH.

3 Cadre conceptuel de la recherche

3.1 Définitions des concepts clés

Pour poser une base théorique robuste, cette section définit les concepts centraux de l'étude : le SIRH, les risques cybernétiques, le contrôle interne, la résilience opérationnelle et la conformité légale. Ces définitions, ancrées dans la littérature scientifique récente, sont contextualisées pour éclairer leurs rôles et interactions dans la gestion des cyberrisques spécifiques aux SIRH.

3.1.1 Système d'Information des Ressources Humaines (SIRH)

Le SIRH est un système numérique intégré conçu pour automatiser et gérer les processus RH, tels que la gestion de la paie, le recrutement, la formation, et la gestion des talents, tout en centralisant les données sensibles des employés (Kavanagh & Johnson, 2017, Mirdasse, 2024e). Les SIRH modernes vont au-delà des tâches administratives traditionnelles : ils incluent des fonctionnalités avancées comme les portails en libre-service pour les employés, l'intégration avec les systèmes ERP (Enterprise Resource Planning), et des outils analytiques pour la prise de décision stratégique (Bondarouk & Ruël, 2013). Ces systèmes sont devenus des actifs critiques pour les organisations, car ils optimisent l'efficacité opérationnelle tout en soutenant les objectifs stratégiques, tels que l'alignement des compétences sur les besoins futurs (Strohmeier, 2020). Pour preuve, un portail en libre-service permet aux employés de mettre à jour leurs informations personnelles directement, réduisant la charge

administrative tout en augmentant l'autonomie (Mirdasse, 2024d). Cependant, leur dépendance croissante aux technologies numériques et leur interconnexion avec d'autres systèmes organisationnels (comme les bases de données financières) augmentent leur exposition aux cybermenaces (Adejumo & Ogburie, 2025). Une étude récente montre que les SIRH cloud, bien que flexibles, sont particulièrement vulnérables aux attaques en raison de leur accessibilité à distance (Gartner, 2022, 2025). Ainsi, la sécurité des SIRH est cruciale non seulement pour protéger les données personnelles, mais aussi pour garantir la continuité des opérations RH face aux perturbations potentielles.

3.1.2 Risques cybernétiques

Les risques cybernétiques englobent les menaces et vulnérabilités technologiques qui compromettent la confidentialité, l'intégrité ou la disponibilité des données et des systèmes d'information (Von Solms & Van Niekerk, 2013). Dans le contexte des SIRH, ces risques incluent une gamme variée de cybermenaces : les cyberattaques comme les ransomwares, qui peuvent paralyser les systèmes RH en chiffrant les données critiques (Choi & al., 2023) ; les violations de données, qui exposent les informations personnelles des employés à des acteurs malveillants (Aghaunor & al., 2025) ; et les erreurs humaines, telles que les clics sur des liens de phishing ou l'utilisation de mots de passe faibles, qui représentent une cause majeure de failles de sécurité (Willie, 2023). Comme en atteste l'exemple suivant, une attaque par hameçonnage ciblant un employé RH peut compromettre des identifiants d'accès, offrant aux attaquants une entrée dans le SIRH. Les SIRH sont particulièrement vulnérables en raison de la nature sensible des données qu'ils contiennent (numéros de sécurité sociale, informations bancaires, dossiers médicaux), et leur compromission peut entraîner des pertes financières substantielles, des interruptions opérationnelles critiques (comme l'incapacité à traiter la paie ou à gérer les absences), et des violations des réglementations sur la protection des données (Boyens & al., 2022). Une étude récente de Vorecol (2024a) indique que 60 % des organisations ont subi au moins une cyberattaque ciblant leurs systèmes RH au cours des deux dernières années, tandis que Verizon (2024) rapporte que les incidents liés aux SIRH ont augmenté de 25 % en 2023, soulignant l'urgence de renforcer leur sécurité face à des menaces comme les vulnérabilités zero-day ou les attaques par ingénierie sociale.

3.1.3 Contrôle interne

Le contrôle interne est un ensemble de processus, politiques et procédures mis en place par une organisation pour garantir la fiabilité des informations, la protection des actifs, et la conformité aux lois et réglementations (COSO, 2013). Dans le cadre des SIRH, le contrôle interne vise à structurer les mesures de cybersécurité pour prévenir les incidents, détecter les anomalies et assurer la qualité des données RH (Mirdasse, 2025 ; Moeller, 2016). Le cadre COSO, largement adopté, propose cinq composantes interdépendantes : l'environnement de contrôle (culture et gouvernance), l'évaluation des risques (identification des menaces), les activités de contrôle (mesures spécifiques), l'information et la communication (partage des bonnes pratiques), et la surveillance (évaluation continue) (COSO, 2013). Appliqué aux cyberrisques, ce cadre permet d'instaurer des mécanismes robustes, tels que des audits de sécurité réguliers, des contrôles d'accès basés sur les rôles (RBAC), ou des politiques de gestion des mots de passe (Komandla, 2023). Tel que le montre l'exemple suivant, une organisation peut limiter l'accès au SIRH aux seuls employés autorisés via des profils RBAC, réduisant ainsi les risques d'intrusion interne. De plus, une évaluation rigoureuse des risques peut identifier des vulnérabilités spécifiques, comme les intégrations mal sécurisées avec des systèmes tiers, et orienter la mise en place de contrôles adaptés (ISACA, 2021). Une étude récente montre que les organisations adoptant le cadre COSO pour leurs SIRH réduisent de 35 % les incidents liés à des erreurs de configuration (PwC, 2023).

3.1.4 Résilience opérationnelle

La résilience opérationnelle est définie comme la capacité d'une organisation à maintenir ou restaurer rapidement ses fonctions critiques face à des perturbations, y compris les cyberincidents (Cybersecurity, 2018). Pour les SIRH, elle implique de garantir la continuité des services RH essentiels, tels que le traitement de la paie, la gestion des absences, ou l'accès aux dossiers des employés, même en cas d'attaque ou de défaillance système (Willie, 2023). La résilience repose sur une planification proactive, incluant des sauvegardes régulières des données RH, des systèmes redondants pour éviter les points de défaillance uniques, et des plans de réponse aux incidents bien définis (BCI, 2022). Comme le démontre la pratique, une organisation peut mettre en place des processus manuels alternatifs pour la paie en cas de compromission du SIRH, ou utiliser des solutions cloud sécurisées avec des sauvegardes hors site pour assurer la disponibilité des données critiques (Vorecol, 2024b). La résilience opérationnelle ne se limite pas à la récupération technique : elle inclut également la capacité à communiquer efficacement avec les employés pendant une crise pour maintenir leur confiance (Choi & al., 2023). Une étude de Gartner (2022) révèle que les organisations résilientes réduisent de 40 % les pertes opérationnelles liées aux cyberincidents, soulignant l'importance d'une approche intégrée combinant technologie et gouvernance.

3.1.5 Conformité légale

La conformité légale se réfère au respect des lois et réglementations qui encadrent la gestion des données personnelles, comme le(RGP) dans l'Union européenne (European Union, 2016) ou le California Consumer Privacy Act (CCPA) aux États-Unis (California Department of Justice, 2018). Ces réglementations imposent des obligations strictes pour la collecte, le traitement, et la sécurisation des données RH, sous peine de sanctions sévères pouvant atteindre jusqu'à 4 % du chiffre d'affaires annuel mondial pour les violations du RGPD ou des amendes significatives sous le CCPA (European Union, 2016). Dans le contexte des SIRH, la conformité nécessite des mesures telles que le chiffrement des données sensibles, la gestion des consentements des employés pour le traitement de leurs données, et la capacité à répondre rapidement aux demandes d'accès ou de suppression des informations personnelles (Aghaunor & al., 2025). Comme le suggère le cas suivant, un employé peut exiger la suppression de ses données après son départ, ce qui oblige l'organisation à disposer de processus clairs pour localiser et effacer ces informations dans le SIRH. Les défis sont amplifiés par la complexité des flux de données transfrontaliers, notamment dans les multinationales, et par l'intégration des SIRH avec des systèmes tiers, nécessitant une vigilance constante pour éviter les infractions (Adejumo & Ogburie, 2025). Une analyse récente d'EY (2023) montre que 45 % des violations de conformité liées aux SIRH proviennent d'une mauvaise gestion des sous-traitants, soulignant le besoin de contrôles étendus.
Ces définitions enrichies forment une base théorique solide pour explorer les interactions entre ces concepts dans le modèle conceptuel proposé, en s'appuyant sur des exemples concrets et des références actualisées.

3.2 Proposition du modèle conceptuel

Le modèle conceptuel examine comment les contrôles de cybersécurité du SIRH et la culture de cybersécurité organisationnelle influencent l'efficacité du système de contrôle interne pour les risques cybernétiques, qui agit comme une variable médiatrice affectant la résilience opérationnelle du SIRH et la conformité légale des données RH. Chaque variable est détaillée avec des sous-dimensions et des indicateurs mesurables, enrichissant la compréhension de leurs rôles et interactions.

3.2.1 Variables explicatives

❖ Contrôles de cybersécurité du SIRH

Les contrôles de cybersécurité du SIRH englobent les mesures techniques et procédurales mises en place pour protéger le système contre les cybermenaces (Knapp & al., 2007). Ces contrôles peuvent être classés en trois catégories principales :

- **Contrôles préventifs :** Ils visent à empêcher les incidents avant qu'ils ne surviennent. Exemples : chiffrement des données pour protéger les informations sensibles, authentification multifactorielle (MFA) pour sécuriser les accès, pare-feux avancés pour bloquer les intrusions (Komandla, 2023).
- **Contrôles détectifs :** Ils identifient les anomalies ou les tentatives d'attaque en temps réel. Exemples : systèmes de détection d'intrusion (IDS) pour signaler les activités suspectes, journaux d'audit pour retracer les actions dans le SIRH (ISACA, 2021).
- **Contrôles correctifs :** Ils permettent de restaurer les systèmes après un incident. Exemples : sauvegardes régulières pour récupérer les données perdues, plans de reprise d'activité pour relancer les opérations RH (Vorecol, 2024a).

Ces contrôles sont essentiels pour sécuriser les données RH sensibles, comme les informations bancaires ou les dossiers médicaux, et prévenir les interruptions des services critiques, telles que la gestion de la paie (Aghaunor & al., 2025. Comme le démontrent les données, une étude de PwC (2023) montre que l'implémentation de l'authentification multifactorielle réduit de 70 % les risques d'accès non autorisés dans les SIRH, tandis que les audits réguliers permettent de détecter les vulnérabilités avant qu'elles ne soient exploitées par des attaquants (Willie, 2023).

❖ Culture de cybersécurité organisationnelle

La culture de cybersécurité organisationnelle reflète l'engagement collectif envers la sécurité des informations, mesuré par la sensibilisation des employés, le soutien de la direction, et l'existence de politiques claires (Hofstede & al., 2010). Elle peut être décomposée en plusieurs dimensions :

- **Sensibilisation et formation :** Programmes réguliers pour éduquer les employés sur les bonnes pratiques, comme la gestion sécurisée des mots de passe, la reconnaissance des emails de phishing, ou l'utilisation responsable des outils numériques (BCI, 2022).
- **Soutien de la direction :** Engagement visible des dirigeants à prioriser la cybersécurité, avec allocation de ressources financières et humaines pour soutenir les initiatives de sécurité (Choi & al., 2023).
- **Politiques et procédures :** Documents formalisant les attentes en matière de sécurité, comme les politiques d'accès strictes, les protocoles de réponse aux incidents, ou les simulations d'attaques pour tester les défenses (Boyens & al., 2022).

Une culture forte réduit les erreurs humaines, qui représentent jusqu'à 80 % des incidents de sécurité selon Verizon (2024), et encourage des comportements proactifs, comme le signalement rapide des anomalies ou des emails suspects (Willie, 2023). Comme le confirment les études, des sessions de formation mensuelles sur le phishing peuvent diminuer de 50 % les clics sur des liens malveillants, renforçant ainsi la sécurité globale du SIRH (EY, 2023).

3.2.2 Variable médiatrice

❖ **Efficacité du système de contrôle interne pour les risques cybernétiques**

L'efficacité du système de contrôle interne évalue la capacité de l'organisation à gérer les cyberrisques via des processus alignés sur le cadre COSO (2015). Cette variable médiatrice est mesurée par l'application des cinq composantes du contrôle interne :

- **Environnement de contrôle :** Ton organisationnel favorisant la cybersécurité, avec des valeurs et une gouvernance claires (COSO, 2013).
- **Evaluation des risques :** Identification et analyse des cybermenaces spécifiques aux SIRH, comme les vulnérabilités des intégrations cloud (Komandla, 2023).
- **Activités de contrôle :** Mesures concrètes comme les contrôles d'accès, les audits de sécurité, ou les mises à jour régulières des logiciels (Moeller, 2016).
- **Information et communication :** Diffusion claire des politiques de sécurité à tous les niveaux de l'organisation (ISACA, 2021).
- **Surveillance :** Evaluation continue de l'efficacité des contrôles via des tests et des indicateurs de performance (Boyens & al., 2022).

Un système de contrôle interne efficace permet de structurer les efforts de cybersécurité, d'anticiper les menaces émergentes (comme les attaques par ransomware), et de garantir une gestion proactive des risques (COSO, 2015). A l'appui de cette assertion, des audits trimestriels peuvent révéler des failles dans les configurations du SIRH, permettant des corrections avant une exploitation malveillante (PwC, 2023).

3.2.3 Variables à expliquer

❖ **Résilience opérationnelle du SIRH**

La résilience opérationnelle du SIRH mesure la capacité du système à maintenir ses fonctions critiques (paie, gestion des talents, administration des avantages) pendant et après un cyberincident (Cybersecurity, 2018). Elle peut être évaluée par :

- **Temps de reprise :** Délai nécessaire pour restaurer les services après une perturbation, comme une attaque par ransomware (BCI, 2022).
- **Redondance des systèmes :** Existence de solutions alternatives, comme des serveurs miroirs ou des sauvegardes hors site, pour éviter les interruptions totales (Vorecol, 2024a).
- **Plans de continuité :** Stratégies détaillées pour maintenir les opérations en cas d'attaque, incluant des processus manuels ou des outils de secours (Willie, 2023).

Une résilience élevée limite les interruptions, réduit les pertes financières, et préserve la confiance des parties prenantes, notamment les employés qui dépendent du SIRH pour leurs salaires ou leurs avantages (Choi & al., 2023). Une étude de Gartner (2022) montre que les organisations avec des plans de continuité bien testés réduisent de 60 % les temps d'arrêt liés aux cyberincidents.

❖ **Conformité légale des données RH**

La conformité légale des données RH reflète l'adhésion aux réglementations comme le RGPD ou le CCPA dans la gestion des données personnelles via le SIRH (California Department of Justice, 2018 ; European Union, 2016). Elle inclut :

- **Protection des données :** Mesures comme le chiffrement des bases de données ou l'anonymisation des informations pour limiter les risques d'exposition (Aghaunor & al., 2025).
- **Gestion des droits :** Capacité à répondre aux demandes des employés, comme l'accès à leurs données ou leur suppression, dans les délais impartis par la loi (Adejumo & Ogburie, 2025).
- **Audits de conformité :** Vérifications régulières pour s'assurer que les processus du SIRH respectent les exigences légales, y compris la documentation des flux de données (Komandla, 2023).

Une conformité rigoureuse est essentielle pour éviter des sanctions financières et renforcer la crédibilité de l'organisation auprès des régulateurs et des employés (Boyens & al., 2022). Comme l'indiquent les données empiriques, un audit mal exécuté peut entraîner une amende de plusieurs millions d'euros sous le RGPD, tandis qu'une conformité proactive peut améliorer la réputation de l'entreprise (EY, 2023).

3.2.4 Schéma du modèle

Le modèle conceptuel peut être décrit textuellement comme suit : les contrôles de cybersécurité du SIRH et la culture de cybersécurité organisationnelle influencent directement l'efficacité du système de contrôle interne pour les risques cybernétiques. Cette efficacité, en tant que variable médiatrice, impacte positivement la résilience opérationnelle du SIRH et la conformité légale des données RH. De plus, la culture de cybersécurité organisationnelle influence directement la conformité légale, car une culture proactive favorise des pratiques alignées sur les réglementations, comme la gestion rigoureuse des consentements ou la réponse rapide aux demandes des employés. Ces relations sont étayées par des travaux récents sur la gestion des cyberrisques et la gouvernance organisationnelle (Choi & al., 2023 ; Aghaunor & al., 2025). Comme le mettent en évidence ces travaux, une culture forte peut amplifier l'efficacité des contrôles techniques en réduisant les erreurs humaines, créant ainsi un effet modérateur bénéfique sur la résilience et la conformité.

3.3 Hypothèses et justifications

Cinq hypothèses sont formulées pour articuler les relations entre les variables du modèle, chacune étayée par des études empiriques récentes, des rapports sectoriels, et des arguments logiques.

- **Hypothèse 1 (H1)**

En amont, de nombreuses recherches insistent sur le rôle central des mesures techniques et procédurales dans le renforcement du contrôle interne. En effet, le chiffrement des données et l'authentification multifactorielle (MFA) accroissent la robustesse des activités de contrôle et de surveillance, deux composantes clés du cadre COSO (2013). Par exemple, Komandla (2023) montre que la mise en œuvre de contrôles préventifs, tels que la MFA, réduit de 70 % les incidents de sécurité dans les systèmes d'information critiques, ce qui améliore significativement la capacité du contrôle interne à prévenir les menaces. De même Knapp et al. (2007) démontrent que des dispositifs tels que les pare-feux avancés permettent de détecter et d'atténuer les cyberrisques avant qu'ils n'engendrent des dommages significatifs (PwC, 2023).
A la lumière de ces éléments empiriques et conceptuels, nous formulons l'hypothèse suivante :
H1 : Les contrôles de cybersécurité du SIRH influencent positivement l'efficacité du système de contrôle interne pour les risques cybernétiques.

- **Hypothèse 2 (H2)**

Au regard des travaux existants, une culture organisationnelle axée sur la cybersécurité renforce significativement l'environnement de contrôle, une des composantes majeures du cadre COSO (2015). Hofstede et al. (2010) montrent que des valeurs pro-cybersécurité au sein de l'entreprise limitent les comportements à risque, tels que le partage non sécurisé de mots de passe ou le non-respect des mises à jour de sécurité. Par ailleurs, Willie (2023) révèle qu'une culture de sensibilisation accrue se traduit par une diminution de 40 % des incidents de sécurité liés aux erreurs humaines, optimisant dès lors la gestion des risques à travers des processus internes mieux appliqués (Verizon, 2024).
En conséquence de ces fondements théoriques et empiriques, nous énonçons l'hypothèse suivante :
H2 : La culture de cybersécurité organisationnelle influence positivement l'efficacité du système de contrôle interne pour les risques cybernétiques.

- **Hypothèse 3 (H3)**

Au préalable, un système de contrôle interne performant, intégrant des plans de réponse aux incidents et des mécanismes de surveillance, soutient la continuité des opérations en réduisant au maximum les temps d'arrêt après un cyberincident (Cybersecurity, 2018). En outre, Moeller (2016) souligne que des dispositifs proactifs, tels que les simulations de crises ou les tests de sauvegarde, fortifient la résilience en préparant les équipes à intervenir rapidement et efficacement. De surcroît, Vorecol (2024b) révèle que les organisations disposant de systèmes de contrôle interne matures parviennent à diminuer de 50 % leur délai de reprise post-cyberattaque, garantissant ainsi la disponibilité des fonctions RH critiques (Gartner, 2022).
Dès lors, nous posons l'hypothèse suivante :
H3 : L'efficacité du système de contrôle interne pour les risques cybernétiques influence positivement la résilience opérationnelle du SIRH.

- **Hypothèse 4 (H4)**

En amont, des processus rigoureux tels que les audits de conformité et les contrôles d'accès assurent un alignement constant avec les exigences réglementaires du RGPD et du CCPA (COSO, 2015). Par ailleurs, le RGPD prescrit explicitement la mise en œuvre de mesures techniques et organisationnelles appropriées, démarche facilitée par un système de contrôle interne intégrant le chiffrement des données et une gestion fine des droits d'accès (European Union, 2016). De surcroît, Aghaunor et ses collaborateurs (2025) montrent que les entreprises dotées de systèmes de contrôle interne robustes sont 60 % plus susceptibles de satisfaire aux

obligations légales sans rencontrer d'incidents, réduisant ainsi significativement les risques de sanctions (EY, 2023).
En conséquence, nous émettons l'hypothèse ci-après :
H4 : L'efficacité du système de contrôle interne pour les risques cybernétiques influence positivement la conformité légale des données RH.

❖ **Hypothèse 5 (H5)**

Enfin, une culture proactive en cybersécurité incite à adopter des pratiques rigoureuses, telles que le respect des politiques de confidentialité et la formation continue sur les exigences réglementaires (Knapp & al., 2007). De surcroît, des employés régulièrement sensibilisés commettent moins d'erreurs coûteuses, par exemple le partage non autorisé de données ou le non-respect des protocoles de sécurité, ce qui limite les risques de violations (Adejumo & Ogburie, 2025). Par ailleurs, BCI (2022) rapporte que les organisations dotées d'une culture de cybersécurité forte observent 30 % moins de violations de données, renforçant ainsi leur conformité légale face à des cadres tels que le RGPD ou le CCPA (Verizon, 2024).
H5 : La culture de cybersécurité organisationnelle influence directement et positivement la conformité légale des données RH.
Le schéma présenté en Figure 1 synthétise les cinq hypothèses formulées et met en évidence les relations directes et médiées entre les variables explicatives (contrôles de cybersécurité et culture organisationnelle), la variable médiatrice (efficacité du contrôle interne) et les variables à expliquer (résilience opérationnelle et conformité légale).

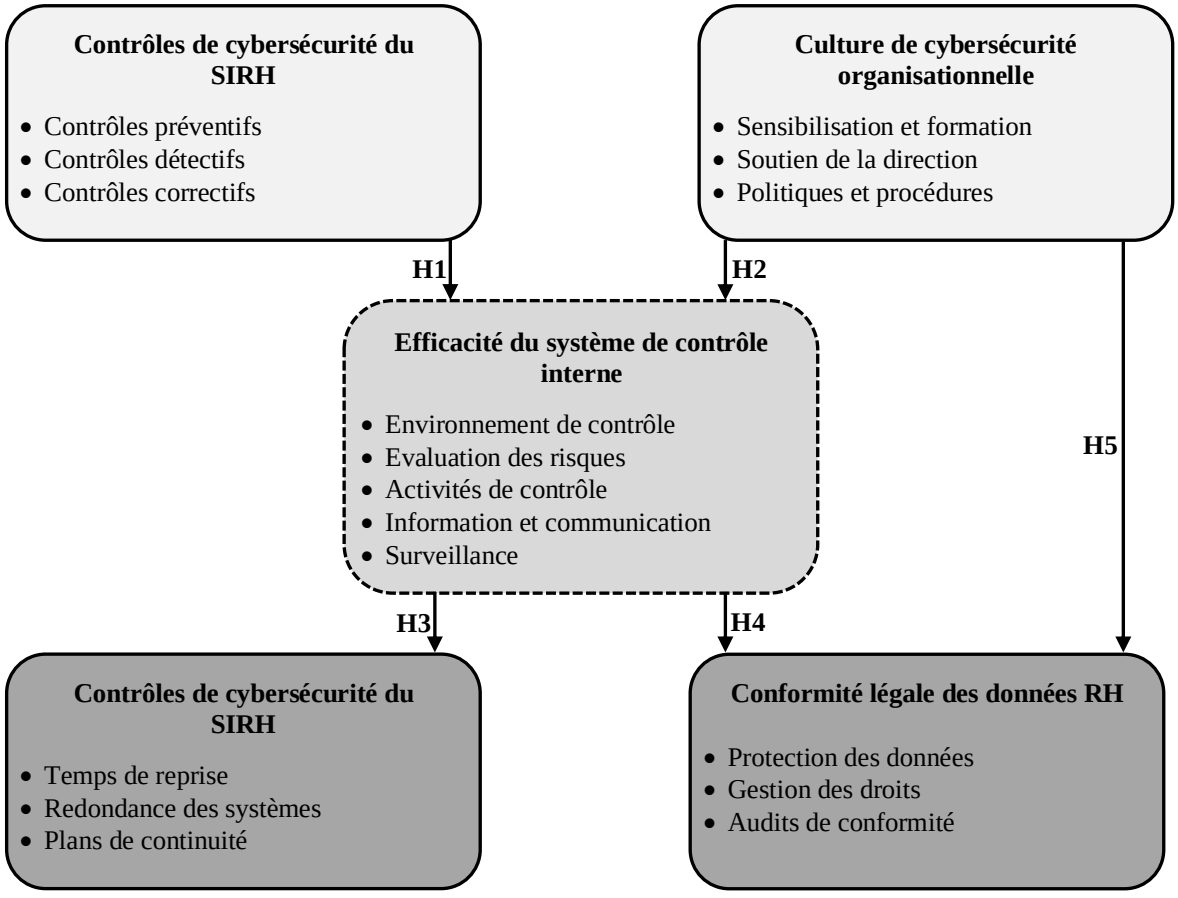

Figure 1 : Schéma du modèle conceptuel de la recherche.

4 Discussion

La présente section vise à analyser les apports du modèle conceptuel proposé sous trois angles : ses implications théoriques, ses implications pratiques et ses limites accompagnées de pistes pour des recherches futures. Structurée en trois sous-sections, cette discussion explore comment le modèle enrichit la littérature en intégrant des concepts clés, propose des recommandations concrètes pour les organisations et identifie les lacunes nécessitant une validation empirique et des investigations supplémentaires.

4.1 Implications théoriques

Le modèle conceptuel développé dans cette étude apporte une contribution notable à la littérature en intégrant des concepts jusque-là étudiés de manière fragmentée : les SIRH, la cybersécurité, le contrôle interne, la résilience opérationnelle et la conformité légale. En reliant ces domaines au sein d'un cadre unifié, il répond à une lacune significative dans les travaux existants, qui se concentrent souvent sur des aspects isolés sans en articuler les interactions. A l'examen des études antérieures, Kavanagh et Johnson (2017) explorent principalement les fonctionnalités des SIRH, tandis que le cadre COSO (2013) met l'accent sur les principes de contrôle interne, mais aucun ne propose une synthèse holistique englobant les risques cybernétiques dans ce contexte spécifique. Le modèle comble cette insuffisance en démontrant comment les contrôles de cybersécurité et la culture organisationnelle influencent l'efficacité du contrôle interne, qui agit comme une variable médiatrice renforçant la résilience opérationnelle et la conformité légale. Cette approche intégrée enrichit la compréhension théorique en soulignant les synergies entre ces dimensions, offrant ainsi une perspective plus complète de la gestion des cyberrisques dans les SIRH (Strohmeier, 2020).

Un apport particulièrement innovant réside dans l'intégration de la culture de cybersécurité comme variable explicative. Alors que les recherches antérieures privilégient souvent des solutions techniques (Knapp & al., 2007), ce modèle s'appuie sur les travaux de Hofstede et al. (2010) pour mettre en avant le rôle déterminant des facteurs humains et organisationnels dans la mitigation des risques. En reconnaissant que les comportements et les valeurs des employés façonnent l'efficacité des mesures de sécurité, il répond à un besoin croissant d'approches interdisciplinaires combinant gestion des ressources humaines, systèmes d'information et cybersécurité (Bondarouk & Ruël, 2013). De plus, en posant des hypothèses claires sur les relations entre ces variables, le modèle fournit une base solide pour des recherches futures, répondant ainsi aux appels de la communauté académique pour des cadres conceptuels intégrateurs capables de guider l'étude des cyberrisques dans un environnement numérique complexe et en évolution rapide (Moeller, 2016).

4.2 Implications pratiques

Le modèle offre des implications pratiques substantielles pour les organisations cherchant à sécuriser leurs SIRH face aux cybermenaces. Tout d'abord, il recommande d'optimiser les contrôles de cybersécurité au sein des SIRH par des mesures techniques et procédurales robustes. Parmi celles-ci, le chiffrement des données sensibles (au repos et en transit), l'authentification multifactorielle (MFA) et la mise en place de pare-feux avancés sont essentiels pour protéger les informations RH contre les intrusions (Knapp et al., 2007). Parallèlement, des audits réguliers et une gestion stricte des accès basée sur les rôles (RBAC) permettent de détecter et de corriger les vulnérabilités de manière proactive, renforçant ainsi l'efficacité du système de contrôle interne conformément au cadre COSO (2015). Ces mesures, lorsqu'elles sont bien exécutées, réduisent les risques de violations de données et améliorent la capacité de l'organisation à répondre aux incidents.

Ensuite, le modèle met en lumière l'importance de renforcer la culture de cybersécurité organisationnelle. Les entreprises devraient investir dans des programmes de formation continue pour sensibiliser les employés aux bonnes pratiques, telles que l'utilisation de mots de passe complexes et la détection des tentatives de phishing (Hofstede & al., 2010). Le soutien de la direction est tout aussi crucial : les dirigeants doivent promouvoir une culture où la sécurité est une priorité collective, en allouant des ressources et en intégrant la cybersécurité dans les objectifs stratégiques. Des simulations d'attaques, comme des campagnes de phishing contrôlées, peuvent également être déployées pour tester et améliorer la vigilance du personnel, réduisant ainsi les erreurs humaines, souvent à l'origine des failles de sécurité (Knapp & al., 2007). Ces efforts culturels complètent les contrôles techniques en créant un environnement où la sécurité est ancrée dans les comportements quotidiens.

Enfin, le modèle préconise un alignement des systèmes de contrôle interne sur les cadres réglementaires, tels que le Règlement Général sur la Protection des Données (RGPD). Cela nécessite de cartographier les flux de données dans le SIRH, d'identifier les points de vulnérabilité et d'instaurer des processus d'évaluation des risques et de surveillance continue (COSO, 2015). Les organisations peuvent automatiser certaines fonctions de conformité, comme la gestion des consentements ou la suppression des données en fin de contrat, pour minimiser les erreurs. Des audits internes réguliers, combinés à des revues juridiques, garantissent que les pratiques restent conformes aux évolutions réglementaires. En intégrant ces recommandations, les organisations transforment leurs SIRH en outils résilients et conformes, capables de résister aux cybermenaces tout en respectant les obligations légales.

4.3 Limites et pistes de recherche futures

Malgré ses apports, le modèle présente des limites inhérentes à son caractère théorique. Premièrement, il n'a pas été validé empiriquement, ce qui restreint sa capacité à être généralisé sans tests concrets. Les relations hypothétiques entre les contrôles de cybersécurité, la culture organisationnelle, l'efficacité du contrôle interne, la résilience opérationnelle et la conformité légale doivent être examinées dans des contextes réels pour en confirmer la robustesse (Strohmeier, 2020). Deuxièmement, le modèle se limite à un ensemble restreint de variables, omettant des facteurs potentiellement influents comme le leadership en cybersécurité ou les

spécificités technologiques des SIRH (Bondarouk & Ruël, 2013). Pour illustrer cette lacune, un leadership proactif pourrait amplifier l'efficacité des contrôles, mais cette dimension reste inexplorée ici. Enfin, le modèle ne prend pas en compte les variations contextuelles, telles que les différences entre PME et multinationales ou entre secteurs public et privé, qui pourraient modifier les dynamiques proposées.

Ces limites ouvrent des perspectives pour des recherches futures. Des études empiriques, combinant analyses quantitatives (notamment, régressions pour évaluer les relations entre variables) et qualitatives (à l'exemple des entretiens pour explorer les perceptions des parties prenantes), sont nécessaires pour tester les hypothèses du modèle. Ces investigations pourraient être menées dans divers contextes organisationnels, comme les PME versus les multinationales, afin d'identifier comment la taille ou la structure influence les résultats (Knapp et al., 2007). De plus, l'exploration de variables supplémentaires, telles que le leadership en cybersécurité, pourrait enrichir le cadre conceptuel. Une étude pourrait, à titre d'exemple, analyser comment un style de leadership transformationnel favorise une culture de sécurité proactive. Enfin, des recherches comparatives entre secteurs pourraient révéler des spécificités contextuelles, offrant des recommandations adaptées. Ces travaux futurs permettront de valider et d'affiner le modèle, contribuant ainsi à une gestion plus efficace et nuancée des cyberrisques dans les SIRH.

5 Conclusion

5.1 Synthèse des points clés

Cette étude visait à examiner comment les SIRH peuvent être protégés contre les cybermenaces en intégrant les notions de contrôle interne, de résilience opérationnelle et de conformité légale dans un cadre conceptuel cohérent. Une revue de littérature exhaustive a permis de poser les bases théoriques, en définissant le SIRH comme un outil essentiel à la gestion des données RH, mais exposé à des risques tels que les violations de données ou les attaques par rançongiciel (Carlson & al., 2025). Le contrôle interne, inspiré du cadre COSO (2013), a été identifié comme un mécanisme clé pour structurer la gestion de ces risques, tandis que la résilience opérationnelle, alignée sur les recommandations du Cybersecurity (2018), garantit la continuité des fonctions RH critiques face aux perturbations. Par ailleurs, la conformité légale, notamment avec le RGPD (European Union, 2016), s'impose comme une exigence incontournable pour sécuriser les données personnelles des employés. La littérature existante, bien qu'abondante sur ces thèmes individuellement, manque d'approches intégrées, une lacune que ce travail cherche à combler.

Le modèle conceptuel proposé établit des liens entre les variables explicatives (contrôles de cybersécurité du SIRH et culture organisationnelle de cybersécurité), une variable médiatrice (efficacité du contrôle interne face aux cyberrisques) et les variables dépendantes (résilience opérationnelle et conformité légale). Ce cadre postule que des contrôles techniques robustes, combinés à une culture proactive, renforcent le contrôle interne, qui améliore à son tour la résilience et la conformité (COSO, 2015 ; Hofstede & al., 2010). En offrant une perspective unifiée, ce modèle répond aux besoins d'interdisciplinarité dans la gestion des cyberrisques appliquée aux SIRH, comme le soulignent certains auteurs (Strohmeier, 2020).

5.2 Réaffirmation de la contribution

Le modèle conceptuel développé dans cette étude constitue une avancée notable tant pour la recherche académique que pour les praticiens. Sur le plan académique, il comble un vide théorique en réunissant des concepts souvent étudiés isolément – SIRH, cybersécurité, contrôle interne, résilience et conformité – dans une approche intégrative. Cette synthèse répond à un appel croissant pour des cadres holistiques dans la littérature, comme le note Strohmeier (2020), et enrichit la compréhension des interactions entre technologie, gouvernance et culture organisationnelle. Pour les praticiens, le modèle offre un outil pratique pour renforcer la sécurité des SIRH, en proposant des recommandations concrètes : optimiser les contrôles techniques, promouvoir une culture de cybersécurité et aligner les processus sur les exigences réglementaires (Knapp & al., 2007). Ainsi, les organisations peuvent non seulement réduire leurs vulnérabilités face aux cybermenaces, mais aussi améliorer la résilience et la performance globale de leurs systèmes RH, transformant un point de faiblesse potentiel en un atout stratégique.

5.3 Perspectives

Bien que ce modèle pose une fondation théorique solide, sa validation empirique reste une étape cruciale. Des recherches futures, combinant analyses quantitatives et études de cas qualitatives dans divers contextes (PME, grandes entreprises, secteurs publics ou privés), permettraient de tester les hypothèses formulées et d'affiner les relations entre les variables. L'intégration de dimensions supplémentaires, telles que le rôle du leadership en cybersécurité, pourrait également enrichir le cadre conceptuel. Sur le plan pratique, les organisations sont invitées à mettre en œuvre ce modèle pour sécuriser leurs SIRH, en investissant dans des technologies avancées (comme les outils de détection des intrusions) et en développant une culture de sensibilisation aux risques cybernétiques. Ces initiatives favoriseraient une gestion proactive des cyberrisques, tout en assurant une

conformité aux normes légales et une résilience face aux imprévus, contribuant ainsi à une transformation durable des pratiques RH.

REFERENCES

[1] Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. World Journal of Advanced Research and Reviews, 25(03), 1542-1556. https://doi.org/10.30574/wjarr.2025.25.3.0909

[2] Aghaunor, C. T., Eshua, P., Obah, T., & Aromokeye, O. (2025). Data security strategies to avoid data breaches in modern information systems. 25(01), 827-849. https://doi.org/10.30574/wjarr.2025.25.1.3906

[3] Balaouras, S., Cunningham, C., & Cerrato, P. (2018). Five Steps to a Zero Trust Model. Forrester Research, 1. www.forrester.com/report/Five+Steps+To+A+Zero+Trust+Network/-/E-RES120510, consulté le 21/03/2025.

[4] BasuMallick, C. (2024). TechFunnel. Ensuring GDPR Compliance: A Guide for HR Tech Systems. https://www.techfunnel.com/hr-tech/guide-for-hr-tech-systems/, consulté le 26.03.2025

[5] Bondarouk, T., & Ruël, H. (2013). The strategic value of e-HRM: Results from an exploratory study in a governmental organization. The International Journal of Human Resource Management, 24(2), 391-414. https://doi.org/10.1080/09585192.2012.675142

[6] Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). Cybersecurity supply chain risk management practices for systems and organizations (No. NIST Special Publication (SP) 800-161 Rev. 1 (Withdrawn)). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1

[7] Bravanti (2023). https://bravanti.com/hr-role-in-business-continuity-planning/, consulté le 25.03.2025

[8] Broderick, R., & Boudreau, J. W. (1992). Human resource management, information technology, and the competitive edge. Academy of Management Perspectives, 6(2), 7-17. https://doi.org/10.5465/ame.1992.4274391

[9] Brown, B. (2024). What is a business continuity plan and how can HR support it? MOOREPAY. https://www.moorepay.co.uk/blog/what-is-a-business-continuity-plan-and-how-can-hr-support-it/, consulté le 25.03.2025

[10] Business Continuity Institute (BCI). (2022). BCI launches Continuity & Resilience Report 2022. https://www.thebci.org/news/continuity-resilience-report-2022-launch.html, consulté le 30.03.2025

[11] California State Legislature (2018). California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4., consulté le 25.03.2025

[12] Carlson, K. D, Kavanagh, M. J., & Johnson, R. D. (Eds.). (2025). Human Resource Information Systems: Basics, Applications, and Future Directions. Etats-Unis: SAGE Publications, Incorporated.

[13] Choi, S. H., Youn, J., Kim, K., Lee, S., Kwon, O. J., & Shin, D. (2023). Cyber-resilience evaluation methods focusing on response time to cyber infringement. Sustainability, 15(18), 13404. https://doi.org/10.3390/su151813404

[14] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal Control — Integrated Framework. COSO. KPMG Assets

[15] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2015). Governance and Internal Control. COSO in the Cyber Age.

[16] Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. Cybersecurity Framework Version 1.1. National Institute of Standards and Technology, URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP, 4162018(7).

[17] European Union. (2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. Official Journal of the European Union, L119, 1-88. https://natlex.ilo.org/dyn/natlex2/natlex2/files/download/101947/EEU-101947%20(EN).pdf

[18] EY. (2023). How can reimagined mobility help organizations see reward and not risk? https://www.ey.com/en_gl/insights/workforce/how-can-reimagined-mobility-help-organizations-see-reward-and-not-risk, consulté le 01.04.2025

[19] Foxall, D. (2024). Six basic HR data security threats in 2025. HRMS World. https://www.hrmsworld.com/hr-data-security-threats.html, consulté le 24.03.2025

[20] Gartner. (2022). Security Leaders Must Evolve Strategies to Protect an Expanding Digital Footprint Against Emerging Threats. https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022, consulté le 02.04.2025

[21] Gartner. (2025). Analysts to Explore Cybersecurity Trends During Gartner Security & Risk Management Summit, March 3-4 in Sydney. https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025, consulté le 02.04.2025

[22] Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). Cultures and organizations: Software of the mind, 3rd McGraw Hill. New York.

[23] International Organization for Standardization. (2013). ISO 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements (ISO 27001:2013). https://www.iso.org/standard/54534.html

[24] ISACA. (2021). State of Cybersecurity 2021. Information Systems Audit and Control Association, https://www.isaca.org/resources/infographics/state-of-cybersecurity-2021-infographic, consulté le 28.03.2024

[25] Kavanagh, M. J., & Johnson, R. D. (Eds.). (2017). Human Resource Information Systems: Basics, Applications, and Future Directions. Etats-Unis: SAGE Publications.

[26] Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., & Ford, F. N. (2007). Information security effectiveness: Conceptualization and validation of a theory. International Journal of Information Security and Privacy (IJISP), 1(2), 37-60. https://doi.org/10.4018/jisp.2007040103

[27] Komandla, V. (2023). Critical Features and Functionalities of Secure Password Vaults for Fintech: An In-Depth Analysis of Encryption Standards, Access Controls, and Integration Capabilities. Access Controls, and Integration Capabilities; 12(1), 1366-1373. https://dx.doi.org/10.21275/SR24913162137

[28] McLennan, M. (2020). MMC Cyber Handbook 2020 Advancing Cyber Resilience. file:///C:/Users/HP-USER/Downloads/mmc-cyber-handbook-2020.pdf, consulté le 24.03.2025

[29] Mirdasse, S. (2024a). Digitalization and Performance Management: A Conceptual Framework for HR Governance. Journal of Economics, Finance and Management (JEFM), 3(3), 642-664. https://doi.org/10.5281/zenodo.11234574

[30] Mirdasse, S. (2024b). Modèle conceptuel intégratif pour la prédiction de l'utilisation du système d'information ressources humaines dans l'entreprise: Une approche combinée des cadres d'ajustement humain-organisation-technologie et technologie organisation-environnement. Revue Internationale du Chercheur, 5(2), 233-256. https://doi.org/10.5281/zenodo.11417521

[31] Mirdasse, S. (2024c). Prédiction du comportement d'utilisation du SIRH dans l'entreprise: Vers un modèle conceptuel basé sur une extension du cadre technologie-organisation-environnement (TOE). International Journal of Accounting, Finance, Auditing, Management and Economics, 5(4), 634-659. https://doi.org/10.5281/zenodo.11079327

[32] Mirdasse, S. (2024d). Fondements théoriques d'utilisation des technologies de l'information et des systèmes d'information. Proposition d'un cadre intégrateur de groupe de variables clés. International Journal of Strategic Management and Economic Studies (IJSMES), 3(2), 719-738. https://doi.org/10.5281/zenodo.11073448

[33] Mirdasse, S. (2024e). Prévision d'utilisation du système d'information des ressources humaines (SIRH) dans l'entreprise. Elaboration d'un modèle conceptuel centré sur une extension du cadre d'ajustement Humain-Organisation-Technologie (HOT-fit). Revue Internationale des Sciences de Gestion, 7(2). 495-520. https://doi.org/10.5281/zenodo.11075671

[34] Mirdasse, S. (2025). Utilisation du SIRH dans le renforcement du dispositif de contrôle interne : Proposition d'un modèle conceptuel pour la gestion des risques RH. Revue Internationale De La Recherche Scientifique (Revue-IRS), 3(2), 2152–2165. https://doi.org/10.5281/zenodo.15337790

[35] Mirdasse, S., & Lhassane, J. (2021). Le Système d'Information Ressources Humaines (SIRH)-outil incontournable au service des organisations: Une analyse théorique. International Journal of Accounting, Finance, Auditing, Management and Economics-IJAFAME, 2(3), 109-132. https://doi.org/10.5281/zenodo.4785662

[36] Moeller, R. R. (2016). Brink's Modern Internal Auditing: A Common Body of Knowledge. Royaume-Uni: Wiley.

[37] Morris A. (2025). GDPR for HR. DavidsonMorris. https://www.davidsonmorris.com/gdpr-for-hr/, consulté le 25.03.2025

[38] PwC. (2023). Global Cybersecurity Outlook 2023. Insight Report January 2023. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf, consulté le 29.03.2025

[39] Story B. (2024). Top 5 Cybersecurity Concerns for HR Professionals: How to Safeguard Your Organisation. The HR World. https://www.thehrworld.co.uk/hr-tech-data-ai/top-5-cybersecurity-concerns-for-hr-professionals-how-to-safeguard-your-organisation/, consulté le 24.03.2025

[40] Strohmeier, S. (2020). Digital human resource management: A conceptual clarification. German Journal of Human Resource Management, 34(3), 345-365. https://doi.org/10.1177/2397002220921131

[41] Ungashick, B. (2024). HRIS System Security: A Comprehensive Guide, OutSail HRIS Advisor. https://www.outsail.co/post/hris-system-security-what-you-need-to-know-a-comprehensive-guide, consulté le 25.03.2025

[42] Verizon (2024). 2024 Data Breach Investigations Report, https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf, consulté le 28.03.24

[43] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

[44] Vorecol (2024a). Ensuring Data Security in Automated HR Processes, https://vorecol.com/blogs/blog-ensuring-data-security-in-automated-hr-processes-10731, consulté le 27.03.2025

[45] Vorecol (2024b). Cybersecurity challenges in digital HR management. https://vorecol.com/blogs/blog-cybersecurity-challenges-in-digital-hr-management-9316, consulté le 30.03.2025

[46] Willie, M. M. (2023). The role of organizational culture in cybersecurity: building a security-first culture. Journal of Research, Innovation and Technologies, 2(2 (4)), 179-198. https://doi.org/10.57017/jorit.v2.2(4).05

[47] Zielinski, D. (2019). 5 Top Cybersecurity Concerns for HR in 2019, shrm.org. https://www.shrm.org/topics-tools/news/technology/5-top-cybersecurity-concerns-hr-2019, consulté le 21//2025.