Les Cahiers du CEDIMES
2024, Volume 19, Hors-série n° 2024, https://doi.org/10.69611/cahiers19-HS-32
ISSN 2110-6045

La gestion des risques liés à la digitalisation de l'enseignement supérieur dans une formation ouverte et à distance à l'Université d'Antananarivo

Pierre Benjamin RAKOTOMAHENINA

Professeur, Responsable de la Mention Gestion de la FEGS, Université d'Antananarivo, Antananarivo – Madagascar, netinfomanagement@yahoo.fr

Résumé : Dans le cadre de la révolution technologique et de ses enjeux, le présent article a pour objectif principal d'assurer le processus d'identification, d'analyse et de prévision des mesures de réduction des risques en rapport à la digitalisation au niveau de l'enseignement supérieur. La démarche qualitative à travers l'expérimentation dans une formation ouverte et à distance ou FOAD Gestion au sein de la Faculté d'Economie, de Gestion et de sociologie de l'Université d'Antananarivo – Madagascar – depuis son opérationnalité au cours de l'année universitaire 2015 jusqu'en 2023 constitue, en réalité, la zone d'étude empirique. Pour savoir ses expériences, les données ont été issues de l'observation participante et de l'enquête sous forme de sondage auprès d'environ 110 individus en tant qu'étudiants tous niveaux et parcours confondus, de la première année de licence jusqu'en deuxième année de master. Les données obtenues ont permis de découvrir des résultats sur la gestion de trois principaux risques sur la digitalisation, notamment le risque pédagogique marqué par la défaillance de la formation, le risque numérique entrainant au cyber risque et le risque opérationnel à travers l'inadéquation du système organisationnel de l'enseignement. Le processus de minimisation jusqu'au seuil d'acceptation de ces risques a été établi grâce aux actions de collaboration entre le personnel enseignant, les étudiants et le personnel administratif et technique au sein de la FOAD Gestion.

Mots-clés : Gestion des risques, Enseignement supérieur, Formation à distance, Digitalisation

Abstract : In the context of the new technological revolution and its challenges, the main objective of this article is to ensure the process of identification, analysis and forecasting of risk reduction measures in relation to digitalization at the level of the Higher Education. The qualitative approach through experimentation in open and distance learning or FOAD Gestion within the Faculty of Economics, Management and Sociology of the University of Antananarivo - Madagascar - since its operationality during the academic year 2015 through 2023 is, in fact, the area of empirical study. To find out about his experiences, the data was taken from participant observation and the survey in the form of a survey of around 110 individuals as students of all levels and backgrounds from the first year of a license to in the second year of a master. The data obtained made it possible to discover results on the management of three main risks on digitalization, in particular the educational risk marked by the failure of training, the digital risk leading to cybercrime and the operational risk through inadequacy and failure of the educational organizational system. The process of minimizing up to the acceptance threshold of these risks has been established thanks to collaborative actions between the teaching staff, the students and the administrative and technical staff within the FOAD Gestion.

Keywords : Risk management, Higher education, Distance learning, Digitalization

1. Introduction

Actuellement, les recherches sur l'amélioration du système d'enseignement face au développement des Technologies de l'Information et de la Communication (TIC) sont considérées comme une des priorités des décideurs si l'on considère l'objectif de développement durable des Nations Unies en 2030[1]. Dans cette optique, l'analyse de l'évolution de l'enseignement, en commençant par la formation en présentiel jusqu'à la conception du système de formation adapté aux TIC, constitue une orientation incontournable dans le monde universitaire, vue son expansion au niveau international (Batime, C. & Weber, E., 2007). Ce système de formation permet à un étudiant d'apprendre, seul ou en collaboration, avec des différents moyens de communication et des soutiens à distance de personnes – ressources (Gérin-Lajoie Serge, 2011). D'où l'apparition des termes « la Formation Ouverte et A Distance » (FOAD), équivalents du « e-learning » (Blandin Bernard, 1999). Pour cela, la définition donnée par l'AFNOR montre la FOAD comme un système de formation conçu pour permettre à des individus de se former sans se déplacer dans un lieu de formation et sans présence physique d'un formateur. La FOAD procure ainsi plusieurs avantages au profit des étudiants, du personnel enseignant et du personnel administratif et technique.

Mais force est de constater que ce dispositif de formation est exposé à des risques. D'une manière générale, un risque peut être défini comme un danger, un inconvénient plus ou moins probable auquel on est exposé (Dictionnaire Larousse) ou une éventualité d'un événement qui peut causer un dommage (Dictionnaire Le Robert). Le risque peut être perçu comme « objectif » (résultat d'une approche rationnelle non-interprétative du risque) ou « perçu » suivant la position de l'agent social dans son exposition au risque et compte tenu de sa psychologie (Godard et al., 2003). Pour Garel et Giard (2004), le risque concerne la possibilité qu'un projet ne s'exécute pas conformément aux prévisions de dates d'achèvement, de coûts, de spécifications ; ces écarts par rapport aux prévisions étant considérés comme difficilement acceptables, voire inacceptables. Le risque résulte ainsi d'un aléa ou d'une incertitude ou d'un imprévu. La question se pose alors : *Comment gérer les risques en rapport aux nouvelles révolutions technologiques, plus précisément, à la digitalisation au niveau de l'Enseignement Supérieur ?* En réalité, la digitalisation de l'enseignement supérieur constitue un sujet d'actualité qui suscite à la fois l'enthousiasme et la préoccupation au sein de la communauté éducative. Par ailleurs, les avantages potentiels de l'intégration des technologies numériques dans l'enseignement sont largement reconnus, la gestion des risques associés à cette transformation est devenue une priorité majeure. Cependant, aucune étude dans ce sens n'a pas encore été développée en Afrique subsaharienne, plus particulièrement à Madagascar, en tant que zone d'études.

A cet effet, l'objectif majeur de la présente recherche est de minimiser les risques rencontrés face à la digitalisation dans le domaine de l'enseignement supérieur. Dans cette optique, deux hypothèses de recherche ont été formulées. D'un côté, la maitrise des risques pédagogiques, numériques et communicationnels assure le bon fonctionnement de l'enseignement. De l'autre côté, les mesures correctives permettent d'arriver au seuil d'acceptation des risques liés à la digitalisation de l'enseignement supérieur.

Pour ce faire, le présent article est organisé en trois parties. Dans un premier temps seront explicités la revue de littérature et la méthodologie de gestion des risques. Par la suite, les résultats sur l'identification et l'analyse des risques de la formation à distance seront détaillés. Les mesures préventives y afférentes seront exposées au dernier temps.

[1] L'OMD vise à assurer une éducation inclusive et équitable de qualité et à promouvoir des possibilités d'apprentissage tout au long de la vie pour tous.

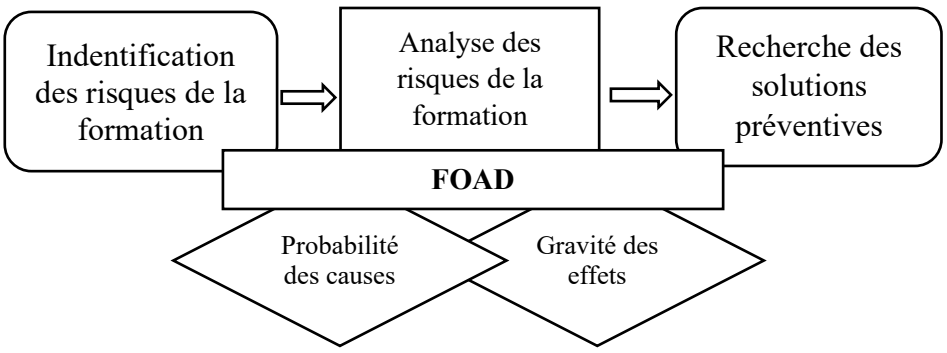
2. Revue de littérature et méthodologie

Pour asseoir la validité de la recherche, quelques investigations sur la gestion des risques sont nécessaires. Sur le plan théorique, le processus de gestion des risques selon Ferchaud (2004) peut se formaliser en cinq étapes essentielles : l'acceptabilité (définir les risques tolérés) ; l'identification (identifier les incertitudes et apprécier les risques associés) ; l'évaluation (évaluer et hiérarchiser leur impact) ; les actions sur les risques (définir et consolider les actions résultantes) ; la gestion des risques résiduels (suivre et contrôler l'application de ces actions). Alors que la gestion des risques selon Blondel et Gaultier-Gaillard (2006) comprend trois étapes classiques. La première concerne l'identification des risques. Cela permet de dresser la liste exhaustive de tous les événements susceptibles de handicaper le bon déroulement de l'innovation. La deuxième touche l'évaluation de l'impact possible des risques. En fonction du degré de gravité des conséquences et de la probabilité d'occurrence de chaque hypothèse, les risques sont hiérarchisés. La dernière étape est axée sur le traitement des risques. Il s'agit de la détermination d'un plan d'actions en fonction des priorités, puis de l'élaboration d'une veille stratégique destinée notamment à vérifier l'applicabilité et enfin, du suivi des traitements préconisés.

A partir de ces différentes approches, la reconfiguration de la démarche de gestion des risques, dans le cadre de la présente recherche au niveau de la FOAD, a permis de poser trois postulats sur l'identification des risques, la probabilité des causes et la gravité des effets des risques. Tout d'abord, la FOAD rencontre des risques au niveau pédagogique (Karsenti, 2006 ; Veyrié, 2014), numérique (Wolf, 2010), communicationnel (Racette et al., 2016) ; Vilches et Pirard, 2018), informationnel (Delbecque, 2006 ; Du Manoir de Juaye, 2014; Meneut, 2014), informatique (Denis, 2012 ; Boddaert, 2017), technique (Bertrand, 2003), administratif/opérationnel (Bon-Michel, 2010 ; Cherré et Dufour, 2015), financier (Aglietta et Scialom, 2002 ; Pesqueux, 2011), humain (Migeot et al., 2006 ; Carskadon et al., 1991) et qualité (Pesqueux, 2012). Ensuite, la défaillance de l'apprentissage, la non-maîtrise de la digitalisation, la défaillance d'interactions en ligne, la non-sécurisation des données, le défaut de traitement d'informations, la défaillance du logiciel, l'inadéquation/défaillance des procédures, la mauvaise opération financière, le manque de soin et la mauvaise qualité de service constituent les probabilités des causes des risques liés à la plateforme de FOAD. Et enfin, l'isolement/l'abandon de l'apprenant, le cyber risque, l'insuffisance de tutorat, la perte/fuite des données, le manque de traçabilité, l'interruption/non accès à la plateforme, la malversation, la perte financière, la maladie et la non-satisfaction constituent les gravités des effets des risques liés à la plateforme de FOAD.

En tenant compte de ces idées, le modèle de gestion des risques en FOAD se présente comme suit :

Schéma n°1 : Modèle de gestion des risques en FOAD



Source : Auteur

D'après ce modèle, l'identification de ces risques a pour objet de rechercher, reconnaître et décrire les risques qui peuvent empêcher le bon déroulement de la FOAD. Le risque se mesure par la multiplication de deux critères : la fréquence (ou probabilité) et la gravité (ou impact). La fréquence exprime la probabilité de survenance du risque. La gravité mesure l'importance des

impacts envisagés en cas de survenance du risque. Le résultat de cette multiplication est la criticité du risque. La recherche des solutions permettant d'arriver à l'acceptation des risques, au partage des risques avec une autre partie (comme le partage contractuel) et / ou le transfert de la gestion du risque à une tierce partie (assurance). En d'autres termes, la gestion des risques (Courtot, 1998) est le processus itératif appliqué tout au long d'un programme et qui regroupe les activités d'identification, d'estimation et de maîtrise des risques.

Dans le cadre du présent travail, l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC) a été adoptée en tant qu'une méthode d'analyse systématique utilisée dans la gestion des risques. Elle vise à identifier, évaluer et atténuer les risques associés aux défaillances du système suivant la norme AFNOR NF EN 60812 (2018). L'AMDEC comporte plusieurs étapes dans sa démarche. Elle commence par l'identification des modes de défaillance, puis se poursuit par l'évaluation des effets des défaillances. Cette étape implique l'identification des conséquences, des impacts et des risques associés à chaque défaillance. Ensuite, l'estimation de la gravité des effets permet de hiérarchiser les défaillances en fonction de leur impact sur le système. La prochaine étape consiste à analyser les causes de ces défaillances. Il revient ainsi d'examiner toutes les causes potentielles qui pourraient le déclencher. La détermination des mesures de préventions est la dernière étape de cette analyse par les Modes de Défaillance et leurs Effets. Les mesures ont été développées en fonction de leur nécessité face à la défaillance existante.

Pour ce faire, la démarche qualitative à travers l'expérimentation dans une formation ouverte et à distance ou FOAD Gestion au sein de la Faculté d'Economie, de Gestion et de Sociologie de l'Université d'Antananarivo – Madagascar – depuis son opérationnalité au cours de l'année universitaire 2015 jusqu'en 2023 constitue, en réalité, la zone d'étude empirique. Les données ont été collectées auprès de la FOAD proposée par l'Université d'Antananarivo. Cette organisation fait partie des pionniers de la formation à distance dans les universités publiques à Madagascar. Pour pouvoir tirer des conclusions globales des résultats obtenus, une enquête à l'aide d'un questionnaire plus structuré permettant d'éviter les erreurs dues aux questions ouvertes a été menée dans un échantillon significatif. Le questionnaire a été d'abord prétesté auprès de 10 individus. Par la suite, la version définitive du questionnaire a été envoyée aux 110 personnes légalement inscrites à ladite formation. Il est à noter que cet échantillon représente près de 10% des personnes poursuivant ce système de formation. Au cours de la descente sur le terrain, il a été demandé leurs idées sur les risques en matière de FOAD, puis les causes et les effets de ces risques. Les informations obtenues ont permis de dresser les tableaux montrant les probabilités de causes et les gravités d'effets des risques et d'établir le diagramme des risques. Ces différentes étapes sont finalisées par l'établissement de la fiche de risques.

Il est à noter que l'objectif principal de l'enquête est de prévoir certains phénomènes étudiés en connaissant la nature des relations entre les causes et les effets. Pour le questionnaire, l'approche par échelles de Likert a été optée pour différentes possibilités de réponses, par exemples « Tout à fait d'accord », « D'accord », « En désaccord » et « En total désaccord ». La première question a été de savoir s'ils sont d'accord aux 10 risques suivants en matière de FOAD. Il s'agit de risques pédagogique (R1), numérique (R2), communicationnel (R3), informationnel (R4), informatique (R5), technique (R6), administratif/opérationnel (R7), financier (R8), humain (R9) et qualité (R10). Pour cette question, l'enquêté peut répondre soit « tout à fait d'accord », soit « d'accord », soit « en désaccord », soit « en total désaccord ». La deuxième question concerne leurs idées sur les degrés de causes des risques sur la défaillance de l'apprentissage (C1), le système numérique non-maitrisé (C2), la défaillance d'interactions en ligne(C3), la défaillance des opérations techniques et administratives (C4), le défaut de traitement d'informations (C5), la défaillance du logiciel (C6), l'inadéquation/défaillance des procédures (C7), la mauvaise opération financière (C8), le manque de soin (C9) et la mauvaise qualité de service (C10). Dans ce cas, l'enquêté a été invité à choisir une des quatre propositions à chaque cause de risque : soit « Très faible », soit « Faible », soit « Grande », soit « Très Grande ». Puis, il a été demandé le degré des effets de risques sur l'incompétence/abandon de l'apprenant **(**E1), le cyber risque (E2), la lenteur administrative (E3), la

perte/fuite des données(E4), le manque de traçabilité (E5), l'interruption/non accès à la plateforme (E6), la malversation (E7), la perte financière (E8) la maladie (E9) et la non-satisfaction (E10). Parmi les quatre propositions, chaque enquêté choisit une alternative à chaque effet. Il suffit de marquer le choix selon la perception de la personne enquêtée.

La détermination des systèmes de réductions des risques a été, par la suite, l'objet de l'étude. De ce fait, le système de détection des risques a été observé au niveau des enquêtés. Ce système consiste à déterminer et à identifier le risque à un temps donné. Il s'agit de la consultation des résultats d'examen (D1), l'observation du cahier de texte numérique (D2), l'observation de la plateforme (D3), l'observation du cahier des charges (D4), l'observation des systèmes et réseaux (D5), l'observation sur terrain (D6), l'analyse du tableau de bord (D7), l'analyse des états financiers (D8), la consultation de la fiche individuelle (D9) et le sondage sur la satisfaction (D10). Enfin, les enquêtés ont été priés de citer un ou deux principal(aux) acteur(s) avec leurs actions respectives permettant de réduire le risque en question le plus convenablement tels que le personnel enseignant (PE), le personnel administratif et technique (PAT) et l'étudiant (E). Il a été exigé de préciser, dans le cas où il existe, encore d'autre(s) cas possible(s).

Les informations obtenues auprès des enquêtés ont été classées selon leurs catégories. Les dépouillements ont été réalisés à la suite de l'arrivée du dernier questionnaire rempli par les enquêtés. L'utilisation du « Tableur » a été suffisante pour traiter les nombres de réponses fournies. La transcription des réponses a été réalisée en faisant l'addition des chiffres dans les tableaux de réponses. A cet effet, il a été facile de déterminer les différents pourcentages à chaque type de réponse. Dans toutes les échelles de réponses (« tout à fait d'accord », « d'accord », « en désaccord », « en total désaccord »), le pourcentage le plus élevé a été considéré comme l'affirmation d'une question soumise aux enquêtés.

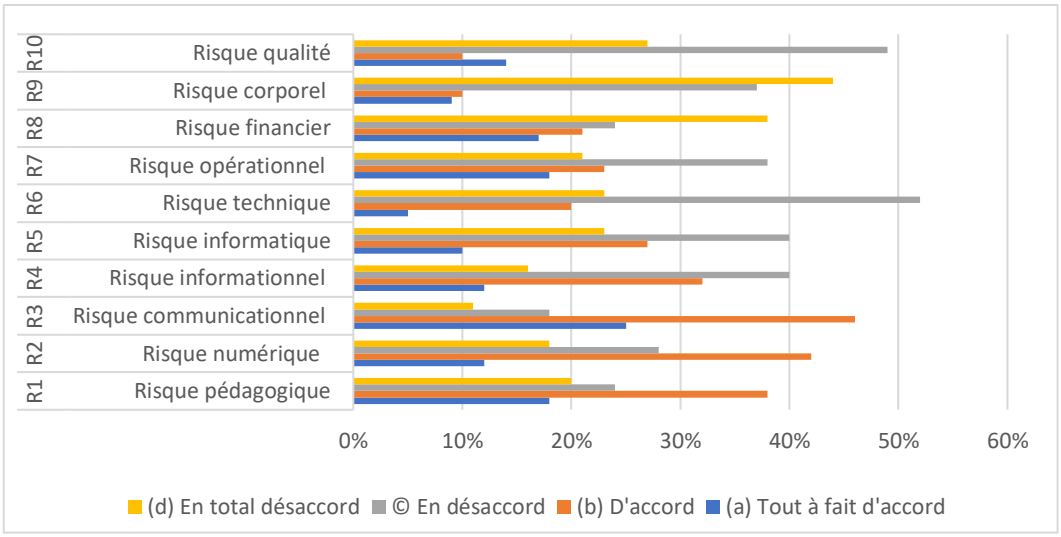
Pour obtenir les résultats de recherche, la démarche générique d'Analyse des Risques d'un Projet par Estimation des Gravités et des Effets (ARPEGE) a été utilisée (Cadet, B. & Kouabénan, D., 2005). Cette méthode consiste d'abord à transformer des risques qualitatifs en valeurs pondérées, ensuite à permettre l'acceptation ou non de chaque risque par un critère simple et enfin, en cas de risque inacceptable, à définir une solution préventive ou de secours ramenant le risque au seuil d'acceptation. Par ailleurs, l'évaluation des risques selon Pesqueux (2012) repose sur l'application de techniques utilisées dans le but de quantifier les effets et de mieux analyser les causes à partir d'échelles de gravité. La classification de la gravité et de la probabilité à l'aide de quatre qualificatifs : « Très faible, Faible, Grand et Très Grand » a permis de fournir la disposition des risques. Chaque qualificatif correspond à une zone codée en puissance de 2, soit 2^0, 2^1, 2^2, 2^3, c'est-à-dire 1, 2, 4, 8. Le risque correspond au produit P x G. Les diagonales descendantes du tableau représentent des zones à risque constant. On peut définir deux types, dont le risque faible avec PG maxi = 4 et le risque moyen avec PG maxi = 8. Les démarches d'analyses des risques suivies ont été de définir le type de risque, « Risque faible » ou « Risque moyen », de lister les risques importants en définissant leurs causes et leurs effets (on retiendra uniquement ceux pour lesquels la Gravité ou la Probabilité d'existence est estimée Grande ou Très Grande), d'estimer la probabilité d'occurrence des risques et la gravité de leurs effets (Très faible, Faible, Grande et Très grande). Si P x G est supérieur à 4 (risque faible) ou à 8 (risque moyen), il faut trouver des solutions pour réduire le risque par prévention ou par secours. Le but de l'utilisation de la démarche « ARPEGE » n'est pas de lister une grande quantité de risques majeurs, ce qui aura un caractère démotivant, mais considérer uniquement les risques importants. Par « risque important », il a été retenu tout risque dont l'effet peut être considéré comme Grave ou Très Grave ou dont la Probabilité semble Grande ou Très Grande.

3. Résultats et discussions

3.1. Identification et analyse des risques

Les réponses fournies par les personnes enquêtées, relatives à la question « En tant qu'étudiant, êtes-vous d'accord avec les risques suivants dans le cadre de la FOAD ? », sont montrées de la manière suivante :

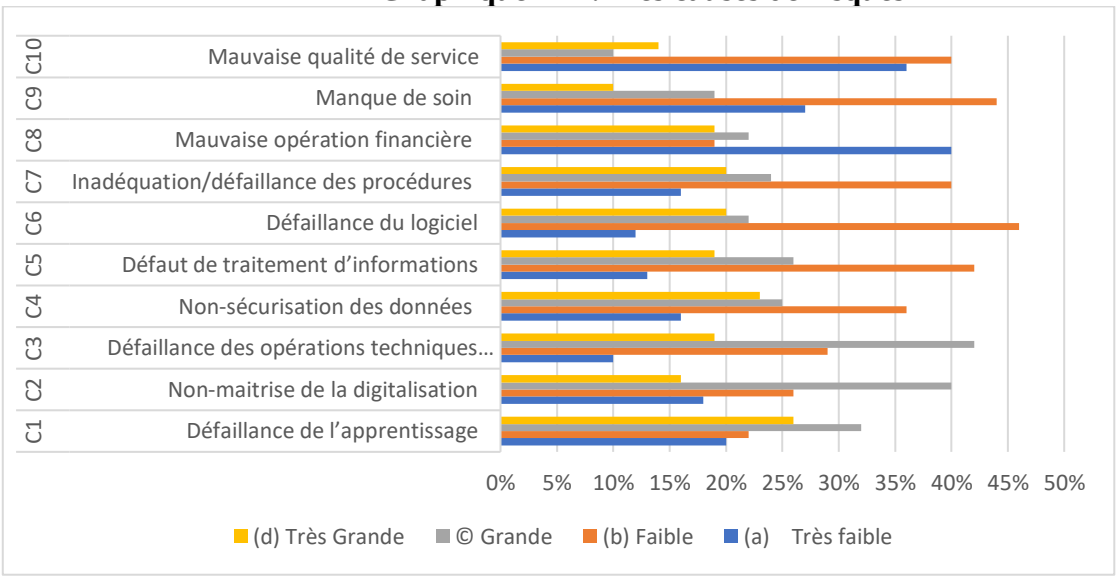
Graphique n°1 : Perceptions sur les risques



Source : Auteur

Les individus enquêtés, d'après les informations acquises, ont donné leurs réponses explicites – d'accord – de l'ordre de 38 % pour le « Risque de pédagogique », 40 % pour le risque numérique et 46 % pour le « Risque communicationnel ». Ce sont les principaux risques en matière de FOAD selon les enquêtés. En revanche, les autres risques sont catégoriquement rejetés. « En poursuivant la FOAD, montrez le degré des causes de risques suivants ? ». Telle est la question posée aux étudiants pour déterminer leurs idées relatives à la probabilité des causes des risques et en voici leurs résultats.

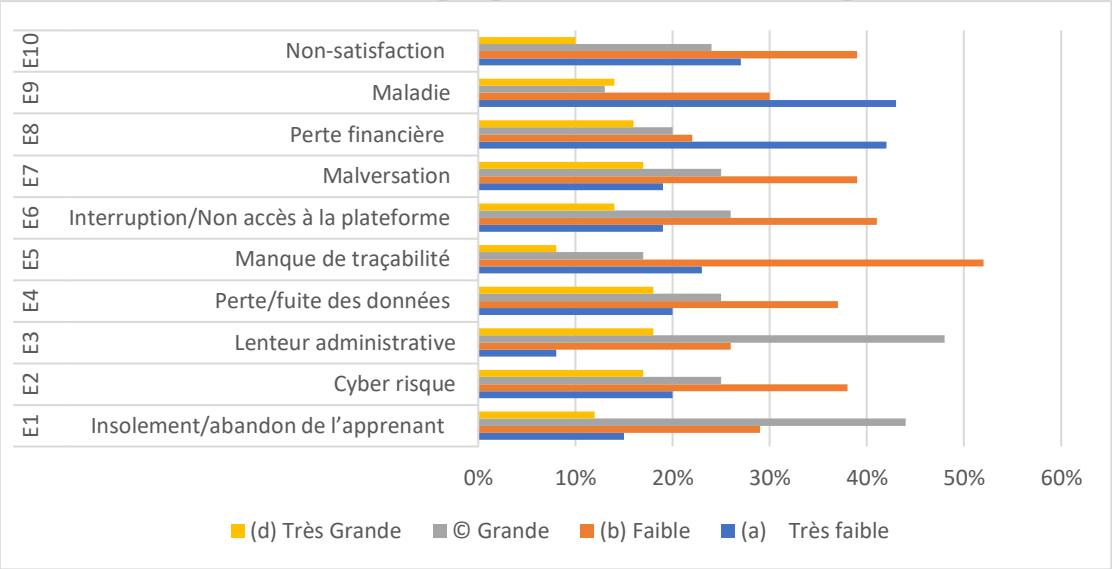
Graphique n°2 : Les causes de risques



(a) Source : Auteur

Les réponses obtenues permettent de connaitre que les probabilités des causes de risques N°1 (32 %), N°2 (40 %) et N°3 (42 %) sont élevées tandis que les autres sont marquées faibles voire très faibles. Par la suite, les avis des enquêtés relatifs aux effets des risques sur la FOAD sont montrés dans le graphique ci-après.

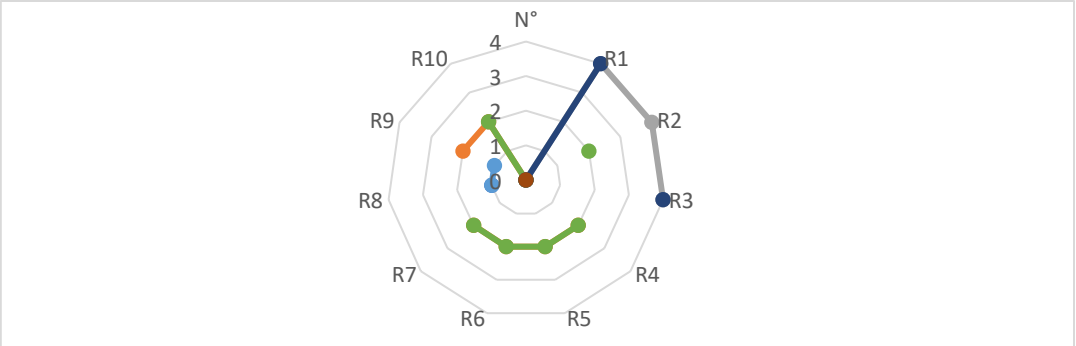
Graphique n°3 : Les effets de risques



Source : Auteur

L'abandon de l'apprenant (effet du risque pédagogique) et l'insuffisance de tutorat (effet du risque communicationnel) constituent des conséquences élevées selon les enquêtés. En contrepartie, les autres risques sont classés dans les probabilités des effets des risques faibles et mêmes très fables. Compte tenu de l'approche par l'ARPEGE, les pourcentages les plus élevés indiquent les classements de probabilités des causes et de gravité des effets risques à 1 pour les « Très faibles », 2 pour les « Faibles », 4 « Grandes » et 8 « Très Grandes ».

Graphique n°4 : Positionnement des risques de FOAD



Source : Auteur

A l'issue de cette matrice de probabilités, les perceptions des enquêtés concernant les risques en matière de FOAD sont montrées dans le Graphique ci-dessus.

3.2. Analyse des risques

L'existence des risques liés à la FOAD suscite, en effet, des débats aussi bien sur le plan théorique qu'au niveau empirique. En partant des résultats de recherche menée auprès de la FOAD Gestion de l'Université d'Antananarivo, des points de vue peuvent être analysés afin d'offrir une piste de réflexion face à l'acceptabilité ou non des risques attachés à la digitalisation.

Tableau n°1 : Positionnement des risques

Gravité de l'effet					
	Très Grande	8	16	32	64
	Grande	4	8	16 (R1, R3)	32
	Faible	2 (R9)	4 (R4, R5, R6, R7, R10)	8 (R2)	16
	Très faible	1 (R8)	2	4	8
		Très faible	Faible	Grande	Très Grande
		Probabilité de la cause			

Source : Auteur

Le tableau ci-dessus fait sortir sept (7) risques considérés comme acceptables dans le cadre de la FOAD. Il s'agit du risque financier (R8 $\Rightarrow$ 1), du risque humain (R9 $\Rightarrow$ 2) et des autres risques (R4, R5, R6, R7 et R10 $\Rightarrow$ 4). Ils sont acceptables, étant donné que leurs criticités sont évaluées respectivement de 1, 2 et de 4.

Premièrement, le concept de risque informationnel (R4) est généralement relié à l'intelligence économique et au domaine juridique. Pour réduire le risque inhérent à l'information, Delbecque (2006) trouve l'importance de l'intelligence économique. Cette dernière, qui est considérée comme savoir-faire, s'organise autour de la croissance de la société de l'information, de la révolution que constitue la gestion offensive de ladite information et du défi que constitue la production de connaissances. La gestion du risque informationnel met en avant une approche informationnelle et communicationnelle du risque en multipliant les collectes et remontées d'information. Or, il est important de noter combien une approche informationnelle du risque est conditionnée par une représentation a priori. Du point de vue juridique, Du Manoir de Juaye (2014) évoque, dans son article sur « Le risque informationnel au filtre du droit », que les individus peuvent être victimes de rumeurs et de l'absence du droit à l'oubli mais aussi des atteintes au droit d'auteur ou de surveillance exacerbée, tandis que les entreprises peuvent voir leurs données volées et leurs secrets des affaires dévoilés. Ainsi, le niveau du risque informationnel est le produit de la probabilité des attaques et de la gravité des pertes (Meneut, 2014).

Deuxièmement, l'informatique (R5), considérée comme étant un élément essentiel en FOAD, constitue la première porte d'entrée aux intrusions ou erreurs pouvant mettre en péril le dispositif de formation. D'autant plus, tout le monde n'est jamais certain d'être à l'abri des risques de façon pérenne en matière informatique, même s'il existe des innovations quotidiennes (Boddaert, 2017). Dans cette optique, trois types de risque ont ainsi été mis en avant (Denis, 2012) : les premiers s'appuient sur la désignation d'un espace extérieur, potentiellement dangereux, les seconds se présentent au contraire comme des risques internes liés à certaines pratiques qu'il faut chercher à encadrer, enfin, les troisièmes renvoient aux vulnérabilités matérielles des outils informatiques. Des recherches ont montré que les risques informatiques les plus courants portent essentiellement sur les virus et malwares (programmes malveillants), les courriels frauduleux, le piratage, l'espionnage industriel, la malversation, la perte d'informations confidentielles, l'erreur de manipulation et le risque de panne, d'incendie ou de vol.

Troisièmement, l'idée de risque technique (R6), dans le domaine de la FOAD, repose sur les dispositifs de formation et notamment sur la plateforme de la formation. Bertrand (2003) rend compte de trois éléments liés à ce type de risque. Il s'agit, respectivement, de la structure accueillant les dispositifs, mettant ainsi en lumière des incompatibilités structurelles à l'utilisation de tels dispositifs, de l'incompatibilité des dispositifs FOAD avec les normes pédagogiques et culturelles et de la complexité de sa mise en œuvre.

Quatrièmement, pour le risque opérationnel (R7), le comité de Bâle définit le risque opérationnel comme « le risque de pertes dues à une inadéquation ou à une défaillance des procédures, des personnels, des systèmes internes ou à des évènements extérieurs » (BCBS, 2003). Cependant, Bon-Michel (2010) a porté une attention particulière sur l'impact de l'identification du risque opérationnel au niveau du système d'apprentissage. D'après Cherré et Dufour (2015), l'une des dimensions sensibles de la fonction de gestion du risque opérationnel est d'ordre intentionnel et concerne la mauvaise foi que peuvent rencontrer les fonctions de gestion des risques. Cette mauvaise foi se caractérise par le refus d'adhérer à une démarche effective de gestion des risques en dissimulant la réalité des risques dans l'organisation.

Cinquièmement, pour le risque financier (R8), il relève de la problématique plus générale du risque économique sur la base du raisonnement en dualité entre la rentabilité et le risque **(**Pesqueux, 2011). Dans ce cas, la rentabilité peut être considérée comme la juste rémunération du risque. Par ailleurs, le risque financier prend la forme de risque de crédit ou de risque de marché associé aux activités bancaires **(**Pesqueux, 2012). Dans cette optique, Aglietta, et Scialom (2002) placent le risque financier au niveau des systèmes bancaires électroniques. Le risque se présente, de manière frauduleuse, à travers l'accès aux données d'authentification des comptes des clients ou le vol des cartes de stockage de valeur monétaire. La monnaie électronique au sens étroit est elle-même exposée au risque de contrefaçon criminelle et les banques peuvent être considérées comme responsables pour le montant de monnaie électronique falsifiée.

Sixièmement, la notion de risque humain (R9) touche tous les acteurs au niveau de la FOAD tels que les apprenants, le personnel enseignant et le personnel administratif et technique. Elle prend en compte la santé de ces acteurs, notamment les étudiants. L'amélioration des connaissances des jeunes sur les risques pour leur santé constitue ainsi une nécessité. La recherche menée par Migeot et al. (2006) sur les comportements de santé des étudiants au sein d'une université en France montre que la population estudiantine se caractérise par un bon état de santé avec, paradoxalement, une fréquence élevée de comportements dits « à risque ». Les risques de maladie que les étudiants craignaient le plus pour eux-mêmes étaient les accidents de la circulation, le cancer, le sida et les maladies sexuellement transmissibles. Cependant, les étudiants travailleurs qui sont probablement beaucoup plus nombreux en FOAD que ceux en présentiel sont exposés au risque de somnolence excessive. Ce risque est associé à d'autres risques selon Carskadon et al. (1991), comme le risque plus élevé de difficultés pédagogiques et de troubles de l'humeur. Une étude effectuée en Brésil confirme également que les étudiants qui travaillent le jour et fréquentent l'établissement le soir sont exposés à la douleur corporelle, une durée de sommeil réduite les jours de semaine et un nombre plus élevé d'accidents de travail (Fischer et al., 2005).

En dernier, il s'agit du risque qualité (R10). Selon Pesqueux (2012), gérer la qualité, c'est gérer le risque et vice versa, c'est-à-dire, le Total Quality Management correspond au miroir du Total Risk Management. Suivant cette perspective, l'appréciation du risque se définit comme un processus général d'analyse et d'évaluation. De ce fait, la détermination du risque sur la qualité au niveau de la FOAD concerne l'effet de l'incertitude sur un résultat escompté par les acteurs, notamment les étudiants. Etant donné la flexibilité dans le temps et dans l'espace de la FOAD, les étudiants exigent des services de qualité supérieure correspondant à leurs besoins.

Dans le cadre de la présente recherche, trois principaux risques sont supposés non acceptables vue la criticité évaluée à 8 et plus. Il s'agit du risque pédagogique (1 $\Rightarrow$ 16), du risque numérique (2 $\Rightarrow$ 8) et du risque communicationnel (3 $\Rightarrow$ 16).

Tout d'abord, la littérature sur la FOAD montre généralement des avantages considérables de la formation à distance par rapport à la formation classique en présentiel pour ne citer que la flexibilité, l'accessibilité et la variété des modes d'enseignement et d'apprentissage. Cependant, plusieurs études évoquent une situation inquiétante face aux taux de succès dans les formations totalement ou partiellement à distance (formations hybrides), variant de 20 à 45 % et le fort taux d'abandons affichés par les universités. De plus, les réticences de nombreux formateurs et professeurs sont encore trop présentes (Karsenti, 2006). Cela constitue un risque pédagogique

comme il y a un manque de savoir encore non connu, une connaissance non encore acquise et un apprentissage non encore assimilé.

Ensuite, le numérique constitue un dispositif essentiel dans le cadre de l'évolution incessante de la technologie. Pourtant, cet essor numérique s'est accompagné d'un développement de nombreux risques dans plusieurs facettes. A ce titre, Wolf (2010) trouve des nouvelles formes de criminalité allant des actions quotidiennes du cyber-vandalisme ou du cyber-crime dont l'appât du gain est le moteur principal, aux modes d'actions cachées de la cyberguerre ou de l'espionnage économique bien plus difficiles à caractériser ou à reconnaître. Sur le plan juridique, la technologie numérique favorise également la réalisation d'activités délinquantes, ce que l'on appelle les infractions commises dans l'environnement numérique et les cyber-délinquants utilisent tous les moyens pour parvenir à leurs fins en procédant par exemple à des attaques informatiques de natures et de modalités différentes (Quéméner, 2011). Sur le plan pédagogique, la technologie numérique expose au risque de non-respect d'autrui, de la vie privée des enseignants, du personnel de l'éducation ou celle des apprenants. Les situations dites de « cyberharcèlement » ou cybercriminalité via les outils du web 2.0 sont aussi des problèmes que les éducateurs ont à gérer. Selon les Nations Unies, la cybercriminalité recouvre tout comportement illégal, faisant intervenir des opérateurs électroniques qui visent la sécurité des systèmes informatiques des données. Les pratiques numériques des jeunes sont d'autant plus complexes qu'elles mêlent la créativité, l'intimité et l'exposition de soi. Au niveau de la FOAD en particulier, Henda, (2016) rend dans son étude que la numérisation des cours constitue un risque conduisant à la démotivation des enseignants. C'est fondamentalement crucial et complexe pour plusieurs considérations : économiques, législatives et déontologiques.

Enfin, le système de FOAD qui se fait avec un minimum de contraintes d'horaire ou de déplacement, à l'exception des contraintes requises pour les évaluations sommatives des apprentissages, permet à un étudiant d'apprendre seul ou en situation de collaboration, avec du matériel didactique approprié et avec le soutien à distance de personnes- ressources (Gérin-Lajoie et Potvin, 2011). Toutefois, les travaux physiquement à distance des acteurs concernés tels que les apprenants, le personnel enseignant ainsi que le personnel technique et administratif peuvent faire face au risque de communication à travers les interactions aussi bien synchrones qu'asynchrones. Les résultats de la recherche réalisée par Racette et al. (2016) montrent que, dans la majorité des cas, les acteurs de la FOAD n'obtiennent pas et ne fournissent pas les informations nécessaires au bon fonctionnement des cours, contraignant la collaboration entre eux. En outre, Vilches et Pirard (2018) trouvent que le risque lié à la communication se focalise sur l'incompréhension du tutorat due aux non-dits et aux implicites dans les propos du tuteur, que les apprenants ont du mal à décoder.

4. Recherche des solutions préventives

La recherche des solutions préventives, permettant de réduire à la fois le risque pédagogique, le risque numérique et le risque communicationnel, nécessite l'intervention des trois principaux acteurs en FOAD.

4.1. L'exploitation de l'espace numériques de travail

L'espace numérique de travail ou ENT désigne un portail qui ouvre l'accès aux services numériques. Il met des outils informatiques à la disposition de tous les acteurs de la communauté éducative de l'Enseignement Supérieur. Pour le cas de la FOAD au sein de l'Université d'Antananarivo, l'existence du centre ENT depuis des années et peu exploité conduit à ce projet de structuration. Il s'agit, dans ce cas, d'effectuer des formations et d'instaurer un lieu de partage des compétences.

À la suite des analyses de l'environnement interne et externe, le problème réside dans le manque de compétences et de formations adéquates. Dans ce cas, l'Espace Numérique de Travail sert à considérer comme le quartier général pour effectuer des formations. Cette activité est disponible pour tous les étudiants de la FOAD. Cet espace est aménagé et dispose des outils informatiques tels que des ordinateurs et un ensemble d'équipements de projection. Les matériels informatiques permettent d'effectuer une formation pratique sur des outils réels. De plus, l'utilisation fréquente des nouvelles technologies développe les compétences de chaque étudiant et de chaque personnel.

Les compétences informatiques ne s'acquièrent guère sans les échanges et le partage. Certes la pratique est indispensable dans la gestion des nouvelles technologies, pourtant la volatilité de ce secteur conduit à des informations variées chaque jour. Ainsi, les séances de partage permettent d'échanger sur les nouveautés dans le secteur. Avec une connexion internet haut débit, la réalisation des recherches constitue un moyen efficace pour augmenter les compétences. Ensuite, l'étudiant partage ses acquis avec d'autres, ce qui conduit à un effet de boule de neige. Finalement, le monde de la digitalisation au niveau de l'Enseignement Supérieur n'a plus beaucoup de secret pour tous les étudiants et le personnel. La totalité n'est pas acquise vu l'évolution rapide de la technologie mais le concept et l'utilisation en général sont assimilés. De ce fait, la fiche de risque numérique est montrée dans le tableau ci-après.

Tableau n°2 : Risque numérique

<table>
<tr><th colspan="2">Eléments</th><th colspan="2">Causes</th><th colspan="2">Effets</th></tr>
<tr><td colspan="2">R2 : Risque numérique</td><td colspan="2" rowspan="2">Système numérique non-maitrisé
⇓</td><td colspan="2" rowspan="2">Cyber risque
⇓</td></tr>
<tr><td>Type</td><td>Solution préventive</td></tr>
<tr><td>Détection</td><td>Observation du cahier de texte numérique</td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>Actions</td><td>Actions de prévention</td><td colspan="4" rowspan="2">Exploitation de l'espace numériques de travail</td></tr>
<tr><td>R2=PG</td><td>32 ⇒4</td></tr>
<tr><td>Acceptabilité :</td><td>NON ⇒ OUI</td><td>Probabilité P=</td><td>8⇒2</td><td>Gravité G=</td><td>4⇒2</td></tr>
</table>

Source : Auteur

L'exploitation d'un Espace Numérique de travail permet de maîtriser le risque numérique au niveau de l'enseignement. Il passe par l'apprentissage en mode réel grâce à des outils informatiques. De plus, l'ENT met en place un système de partage et d'échange pour augmenter les compétences de chaque utilisateur. Dans ce cadre, des suggestions d'amélioration du système digital présentent les collaborations avec les différents partenaires.

4.2. La transformation digitale du système administratif

Une transformation digitale de tous les services revient à intégrer et utiliser les technologies numériques pour améliorer les processus de la digitalisation. Cette transformation implique une mise à jour au niveau du service de relevé des notes et au sein même de l'administration de la formation.

Tableau n°3 : Risque opérationnel et administratif

<table>
<tr><th colspan="2">Eléments</th><th>Causes</th><th>Effets</th></tr>
<tr><td colspan="2">R3 : Risque communicationnel</td><td rowspan="3">Défaillance des opérations techniques et administratives
⇓</td><td rowspan="3">Lenteur Administrative
⇓</td></tr>
<tr><td>Type</td><td>Solution préventive</td></tr>
<tr><td>Détection</td><td>Observation de la plateforme</td></tr>
<tr><td>Actions</td><td>Actions de</td><td colspan="2">Renfoncement de la transformation digitale du</td></tr>
</table>

	prévention	système administratif			
R3=PG	16 ⇒4				
Acceptabilité :	NON ⇒ OUI	Probabilité P=	4⇒2	Gravité G=	4⇒2

Source : Auteur

Pour maîtriser le risque communicationnel, la digitalisation doit être en adéquation avec l'automatisation du processus administratif, tels que l'inscription des étudiants, la gestion des programmes d'études, l'évaluation et les archives des données de chaque étudiant. Dans le cas d'une demande de liste des admis, le problème réside dans le système d'archivage des années précédentes qui est assez confus. La digitalisation du système fait gagner un temps considérable au lieu de perdre des journées entières à chercher une liste attestant le parcours d'un quelconque étudiant.

De plus, concernant la déclaration des vacations ou des heures complémentaires, la mise en place d'un programme sécurisé représente un atout pour l'Enseignement Supérieur. Cela permet de sauvegarder les informations concernant les heures effectuées par chaque enseignant, les pièces justificatives relatives aux informations et toutes les autres pièces jointes nécessaires pour valider le contenu de leur déclaration. D'un simple clic et entrant un mot de passe, un enseignant a la possibilité de consulter ses activités durant une année universitaire. Il est ensuite libre d'incorporer parmi les informations disponibles, les informations à insérer dans leur déclaration. La possibilité d'y insérer de nouvelles informations comme une nouvelle nomination ou un nouvel article publié est aussi envisageable. Cette digitalisation requiert tout de même une étroite collaboration avec les délégués de chaque niveau d'études. Ils effectueront le pointage des cours avec les enseignants à chaque séance.

La mise en place d'un système de notification électronique permet aux étudiants d'accéder plus rapidement à leur relevé de notes. Cette réforme consiste à insérer ou exporter les notes de chaque étudiant à partir des résultats définitifs des examens. Le service des notes est l'une des services les plus fréquentés à part le service diplôme. Qu'il soit en formation en présentiel ou en formation à distance, un étudiant passe par le service des relevés de notes pour complément de dossier. Pour respecter l'environnement et garantir la sécurité des données, aucun relevé de notes en version papier n'est livré au propriétaire. Il convient d'envoyer une photocopie certifiée des notes de l'étudiant à l'entité requérante. Ainsi, aucun relevé des notes n'est remis en main propre. Le problème majeur réside dans la difficulté à trouver les notes des années universitaires lointaines. La transformation digitale est une opportunité de renouveler le système d'archivage. Dans cette pratique, les informations sont plus accessibles et sont facile à traiter. En addition, les Procès-Verbal (PV) sont aussi touchés par cette transformation digitale.

En effet, les notes de chaque soutenance sont à vérifier auprès des PV de soutenance de chaque étudiant. Pourtant la recherche de ces PV est aussi source de gaspillage d'un temps considérable. Alors, une réforme dans le sens d'un système digital permettrait d'instaurer un classement plus flexible et une sauvegarde à long terme.

Ainsi, la transformation digitale des services regroupe essentiellement l'administration et le service de relevé de notes. Dans cette réforme, la mise en place de site sécurisé et fiable garantit une facilité de manipulation des données, ce qui conduit à la réorganisation du système de classement et d'archivage des données.

Chaque service digitalisé constitue alors un processus bien défini qui réduit les risques de communication. Le manque de processus claire et précis favorise les erreurs. Dans le cadre des nouvelles technologies, l'exploitation d'un espace numérique de travail représente ainsi un atout pour se familiariser avec le monde digitalisé.

Dans le cadre de la minimisation des risques pédagogiques, la collaboration avec des partenaires représente une suggestion d'amélioration dans le sens où elle permet de bâtir de nouvelles idées innovatrices et futuristes. La mise en place des infrastructures technologiques

repose sur les partenaires. En effet, ces derniers possèdent les ressources nécessaires dans la réalisation de projet de développement sur le plan pédagogique.

En collaborant avec des partenaires, tels que les entreprises technologiques ou d'autres entités, l'entité pourra être en mesure de bénéficier de leur expertise et des ressources supplémentaires. Cette collaboration inclut l'accès à des technologies de pointe, des connaissances spécialisées et des financements pour développer des solutions numériques innovantes. Les partenaires (entreprises, établissements publics, universités nationales et à l'étranger) doivent être en mesure de fournir des instruments et un service spécial dans le développement du système digital de l'Enseignement Supérieur. De plus, la collaboration avec des partenaires favorise le partage des meilleurs pratiques, notamment en sécurisation des données. Elles sont aussi en mesure de partager leurs expériences. Cela permet aux établissements d'apprendre les uns aux autres, d'identifier les approches les plus efficaces, et de s'inspirer des réussites des autres entités pour améliorer le système digital de l'Enseignement Supérieur.

Tableau n°4 : Risque pédagogique

<table>
<tr><th colspan="2">Eléments</th><th colspan="2">Causes</th><th colspan="2">Effets</th></tr>
<tr><td colspan="2">R1 : Risque pédagogique</td><td colspan="2" rowspan="2">Défaillance de la formation
⇓</td><td colspan="2" rowspan="2">Isolement et abandon des étudiants
⇓</td></tr>
<tr><td>Type</td><td>Solution préventive</td></tr>
<tr><td>Détection</td><td>Consultation des résultats d'examen</td><td colspan="4"></td></tr>
<tr><td>Actions</td><td>Actions de prévention</td><td colspan="4" rowspan="2">Collaboration des acteurs</td></tr>
<tr><td>R1=PG</td><td>16 ⇒4</td></tr>
<tr><td>Acceptabilité :</td><td>NON ⇒ OUI</td><td>Probabilité P=</td><td>4⇒2</td><td>Gravité G=</td><td>4⇒2</td></tr>
</table>

Source : Auteur

La collaboration avec des partenaires ouvre des portes en termes d'opportunité, de réseautage professionnel et de développement pour les enseignants, les étudiants, le personnel administratif. Elle se traduit par des échanges d'expériences, des formations conjointes, des conférences ou des évènements collaboratifs afin de contribuer au renforcement des compétences et des connaissances dans le domaine du numérique. Les partenaires apportent des idées novatrices pour développer des solutions numériques avancées. La sécurisation des données est l'une des principales sources de problème majeur au niveau de la digitalisation. Ainsi, la collaboration avec des partenaires stimule la recherche appliquée de solutions, facilite le transfert des connaissances et contribue à l'amélioration continue du système digital de l'Enseignement Supérieur.

5. Conclusion

La gestion des risques liés à la digitalisation de l'enseignement à Madagascar représente un défi complexe et crucial à l'intersection de l'innovation technologique et de la recherche pédagogique. C'est dans ce cadre que le présent article tient débout, étant donné que ce type de formation n'est pas exempt de risques. La démarche de gestion des risques adoptée a permis de procéder à l'analyse et à la proposition de réduction des risques inhérents à la FOAD. Les postulats de départ sur l'identification des risques, l'analyse de la probabilité des causes et l'analyse de la gravité des effets de ces risques ont été étudiés dans un dispositif de FOAD déjà opérationnel dans l'université d'Antananarivo à Madagascar. L'analyse des risques par estimation de gravité et de probabilité a fait sortir l'acceptabilité ou non de chaque risque. Les résultats obtenus affichent trois principaux risques supposés non acceptables dans le domaine de la FOAD tels que le risque pédagogique, le risque numérique et le risque communicationnel. Dans cette optique, les hypothèses sont validées. Cependant, il faut admettre que l'évaluation de l'acceptabilité d'un risque ne peut être laissée à la science et à l'expertise du fait de l'aspect collectif qui est associé au risque avant qu'il

ne devienne acceptable. L'acceptabilité résulte d'une construction mentale, sociale et culturelle où l'aspect affectif entre en ligne de compte (Noiville, 2003). Pour ces risques inacceptables, les solutions préventives ramenant le risque au seuil d'acceptation dépendent de la réalisation effective des actions des étudiants, du personnel enseignant et du personnel administratif et technique, en tant que principaux acteurs de la FOAD. La gestion des risques liés à la FOAD constitue, par conséquent, une piste de discussions sur l'amélioration du système de formation aussi bien dans les pays développés que dans les pays en voie de développement.

Ainsi, cette recherche a permis d'établir le lien entre la gestion des risques et la digitalisation de l'Enseignement Supérieur. Cependant une question demeure existante : Comment les acteurs au niveau de l'enseignement supérieur doivent-ils agir face à l'intelligence artificielle ?

Bibliographie

1. AFNOR (2018), Norme NF EN 60812 : Analyse des modes de défaillance et de leurs effets (AMDE et AMDEC).
2. Aglietta, M. & Scialom, L. (2002), Les risques de la monnaie électronique, *L'Économie politique*, 14(2), 82-95.
3. Bon-Michel, B. (2010), Identification du risque opérationnel et apprentissage organisationnel : étude d'un établissement de crédit, le groupe Société Générale. Gestion et management. Conservatoire national des arts et métiers – CNAM.
4. Bertrand, I. (2003), Les dispositifs de FOAD dans les établissements d'enseignement supérieur : transfert ou intégration ? *Distances et savoirs*, 1(1), 61-78.
5. Blondel, F. & Gaultier-Gaillard, S. (2006), Comment une entreprise peut-elle maîtriser les risques induits par l'innovation ? *Vie & sciences de l'entreprise*, 172(3), 10-23.
6. Boddaert, G. (2017), Sécurité informatique : de la résistance à la résilience. I2D, *Information, données & documents*, 3(54), 42-43.
7. Cadet, B. & Kouabénan, D. (2005), Évaluer et modéliser les risques : apports et limites de différents paradigmes dans le diagnostic de sécurité. Le travail humain, 68(1), 7-35.
8. Carskadon, M. A., . Seifer, R, Davis S. S. & Acebo C. (1991), Sleep, Sleepiness, and Mood in College-Bound High School Seniors, *Sleep Research*, 21.
9. Cherré, B. & Dufour, N. (2015), Le contrôle en dualité, entre aliénation et autonomie. Le cas du management éthique appliqué aux risques opérationnels. *Recherches en Sciences de Gestion*, 108(3), 159-178.
10. Courtot H. (1998), *La Gestion des risques dans les projets*, Économica, Paris.
11. Delbecque, É. (2006), *L'intelligence économique : une nouvelle culture pour un nouveau monde*, France : Presses Universitaires de France.
12. Denis, J. (2012), L'informatique et sa sécurité : Le souci de la fragilité technique. *Réseaux*, 171(1), 161-187.
13. Du Manoir de Juaye, T. (2014), Le risque informationnel au filtre du droit, *Documentaliste-Sciences de l'Information*, 51(3), 37-40.
14. Ferchaud, B. (2004), Journée d'étude ADBS : Gestion de l'information et gestion des risques, *Documentaliste-Sciences de l'Information*, 41(3), 187-189.
15. Fischer, F. M., Oliveira, D. C., Nagai, R., Teixeira, L. R., Lombardi Jr, M.., DO Latorre, M. do R. & Cooper S. P.. (2005). Job Control, Job Demands, Social Support at Work and Health Among Adolescent Workers, *Revista de Saúde Pública*, 39(2), 245-253.
16. Garel, G & Giard, V, Midler, C. (2004). *Faire de la recherche en management de projet*, Vuibert-FNEGE.
17. Godard O., Henry C., Lagadec P. & Michel-Kerjean E. (2003). *Traité des nouveaux risques*, Gallimard : Paris.
18. Makosso, B. (2006), La crise de l'enseignement supérieur en Afrique francophone : Une analyse pour les cas du Burkina Faso, du Cameroun, du Congo, et de la Côte d'Ivoire, *Journal of Higher Education in Africa*, 4(1), 69-86.
19. Meneut, E. (2014). Le risque informationnel vu depuis la Chine : vers un basculement ? *Documentaliste-Sciences de l'Information*, 51(3), 62-64.

20. Migeot, V., Ingrand, I., Defossez, G., Salardaine, F., Lahorgue, M., Poupin, C. & Ingrand, P. (2006), Comportements de santé des étudiants d'IUT de l'Université de Poitiers, *Santé Publique*, 18(2), 195-205.
21. Henda, M.B. (2016), Formation à distance et outils numériques pour l'enseignement supérieur et la recherche en Asie-Pacifique (Cambodge, Laos, Vietnam). Partie 01: État des lieux, *Agence Universitaire de la Francophonie*, Bureau Asie-Pacifique.
22. Pesqueux, Y. (2011), Pour une épistémologie du risque. *Management & Avenir*, 43(3), 460-475.
23. Pesqueux, Y. (2012). La gestion du risque : une question d'expert ? *Prospective et stratégie*, 2-3(1), 243-265.
24. Quéméner, M. (2011), Concilier la lutte contre la cybercriminalité et l'éthique de liberté, *Sécurité et stratégie*, 5(1), 56-67.
25. Racette, N., Poellhuber, B. & Bourdages-Sylvain, M.-P. (2016). La communication entre tuteurs et équipes de conception, dans quatre établissements de formation à distance, incite-t-elle à la collaboration? *Revue internationale des technologies en pédagogie universitaire / International Journal of Technologies in Higher Education*, 13 (1), 6–16.
26. Gérin-Lajoie, S., Potvin C. (2011). Évolution de la formation à distance dans une université bimodale, *Distances et savoirs*, 3(9), 349-374.
27. Karsenti, T. (2006). *Comment favoriser la réussite des étudiants d'Afrique dans les formations ouvertes et à distance (foad)* : principes pédagogiques, Montréal, QC : Université de Montréal.
28. Veyrié, N. (2014), Quelle pédagogie pour quelle prise de risque ? *Le sociographe*, 45(1), 73-81.
29. Vilches, V. A. & Pirard, F. (2018). Le tutorat dans les métiers de l'interaction humaine, *Formation emploi*, 1(141), 27-44
30. Wolf, P. (2010), Les menaces numériques aujourd'hui. *Sécurité et stratégie*, 3(1), 44-46.