h e g

Haute école de gestion
Genève

h e g
Haute école de gestion
Genève

Congrès AAQ, 26 mai 2022

RISQUES INFORMATIONNELS DANS LES ORGANISATIONS PATRIMONIALES : OUTILS ET MÉTHODE D'IDENTIFICATION ET DE PILOTAGE *RIO*

Dr. Basma Makhlouf Shabou

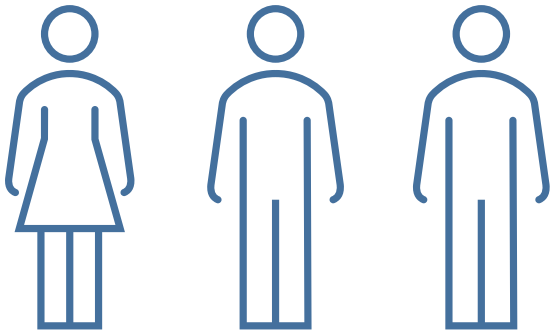
Prof. Resp. de la filière Master en Sciences de l'information de la Haute école de gestion de Genève

Hes·so GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

Plan

- **Équipe du projet**
- **Objectifs**
- **Méthodologie**
- **Résultats**
  0. Etat de l'art
  1. Cadre conceptuel et typologique des RI
  2. Cartographie des RI par type d'institution
  3. Études de cas auprès d'institution
  4. Processus, outils, indicateurs de suivi, mesures et contrôle d'impact
  5. Tableau de bord
  6. Spécifications pour l'outil de pilotage (software)

Équipe du projet RIO



Assistant-e-s :

S. Meroni, S. Krug

L. Ramalho

Cheffe de projet

B. Makhlouf Shabou

Trois étudiantes de la HEG

Elia DESHAYES

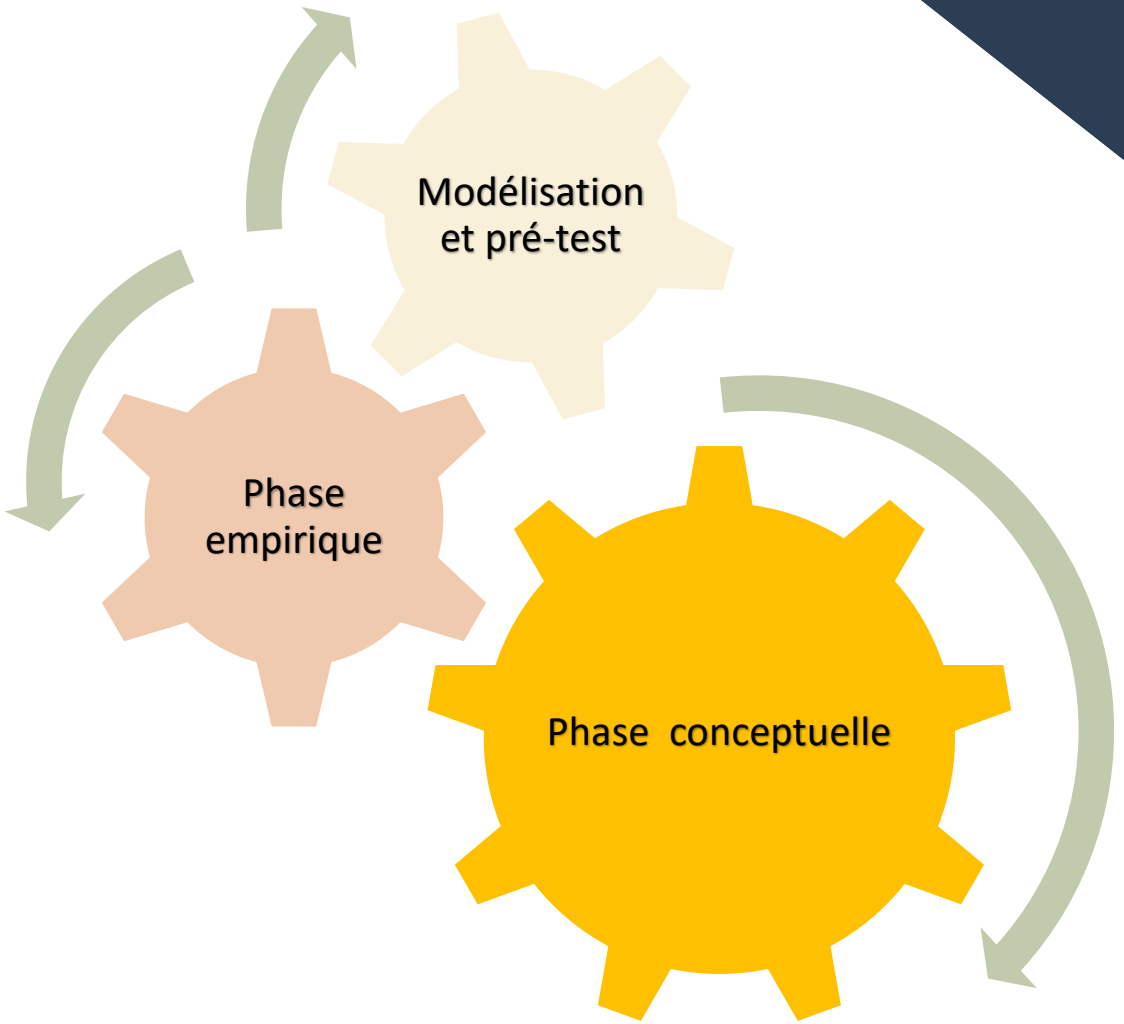
Aysha GUL

et Cloé ROBERT

2021-2021

- **Trois phases & un processus holistique**
  (24 mois: 02.2019-01.2021)

- **Approche qualitative descriptive**



Partenaires

Fondation Martin Bodmer

Comité international de la Croix-rouge

Archives d'Etat du Valais

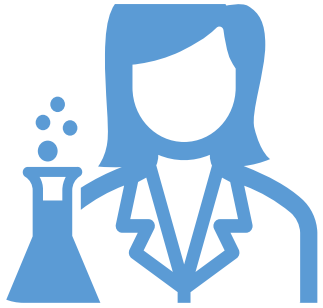
Ville de Genève

Objectifs

Objectif général

Définir **la nature, les principales caractéristiques et la typologie des risques informationnels (RI)** ainsi que les **indicateurs appropriés** permettant de les mesurer afin de proposer un modèle de gouvernance et des outils de pilotage appropriés aux RI.

Méthodologie



Recherche appliquée

Approche qualitative

Focus group

Analyse des documents et autres contenus

Revue systématique de la littérature

Décembre 2021 – juillet 2022

Méthodologie

Objectif scientifique

RIO : Typologies et natures

- L1 : Cadre conceptuel et typologie des RI
- L2 : Cartographie des RI par type d'institution

Objectif méthodologique

RIO patrimoniales: Méthode & dispositifs de contrôle

- L3 : Etudes de cas
- L4 : Processus, outils, indicateurs de suivi, mesures et contrôle d'impact

Objectif technique

RIO patrimoniales: tests des indicateurs et métriques

- L3 : Etudes de cas
- L5 : Tableau de bord
- L6 : Spécifications de l'outil de pilotage

Résultats

0. Etat de l'art – grille de lecture

	Litt. Académique	Litt. Professionnelle	Normes, lois et règlement	Remarques
Définitions				
Cadre général				
Gestion des risques liés à la sécurité de l'information				
Gestion des risques liés à la sécurité de l'information - Evaluation				
Outils / Métriques /Nomenclatures / Typologies				
Patrimoine				

Résultats

0. Etat de l'art – nature

- Le risque informationnel
  - **… n'est pas toujours négatif**
  - **… n'est pas réel, c'est la probabilité qu'un évènement non planifié survienne**
  - **… peut être contrôlé et réduit, mais le « risque zéro » n'existera jamais**
  - **… est souvent associé au processus de traitement des données et de l'information au sein du système d'information**
- Son impact est associé au ralentissement et/ou à l'interruption de l'activité institutionnelle.
- Son importance est un consensus chez les managers
- Sa gestion se fait en fonction d'un cycle, elle se focalise sur la protection des documents d'activité.
- Sa perception est subjective et est en fonction de facteurs sociaux, politiques, économiques …
- Les normes et les études sur l'analyse des risques existent → pas suffisamment de travaux sur les risques informationnels

ISO

ISO 24143:2022

Information et documentation – Gouvernance de l'information – Concept et principes

Principe n 11 dédié au RI

ISO 24143:2022

Information et documentation — Gouvernance de l'information — Concept et principes

5 Principles of Information Governance

- 5.1 Recognising information as a corporate, strategic asset
- 5.2 Designing Information Governance as a key element of corporate strategy
- 5.3 Integrating Information Governance into the organisation's governance frameworks
- 5.4 Securing senior management's leadership and commitment
- 5.5 Building Information Governance in a collaborative way
- 5.6 Ensuring Information Governance supports legal compliance and any mandatory requirements
- 5.7 Aligning Information Governance to business objectives
- 5.8 Ensuring Information Governance supports information security and privacy
- 5.9 Ensuring Information Governance supports information quality and integrity
- 5.10 Fostering a collaboration and knowledge sharing culture
- 5.11 Adopting a risk-based approach
- 5.12 Ensuring the availability and accessibility of information to authorised stakeholder
- 5.13 Governing information throughout its information lifecycle
- 5.14 Supporting corporate culture
- 5.15 Supporting sustainability

New

Mai 2022

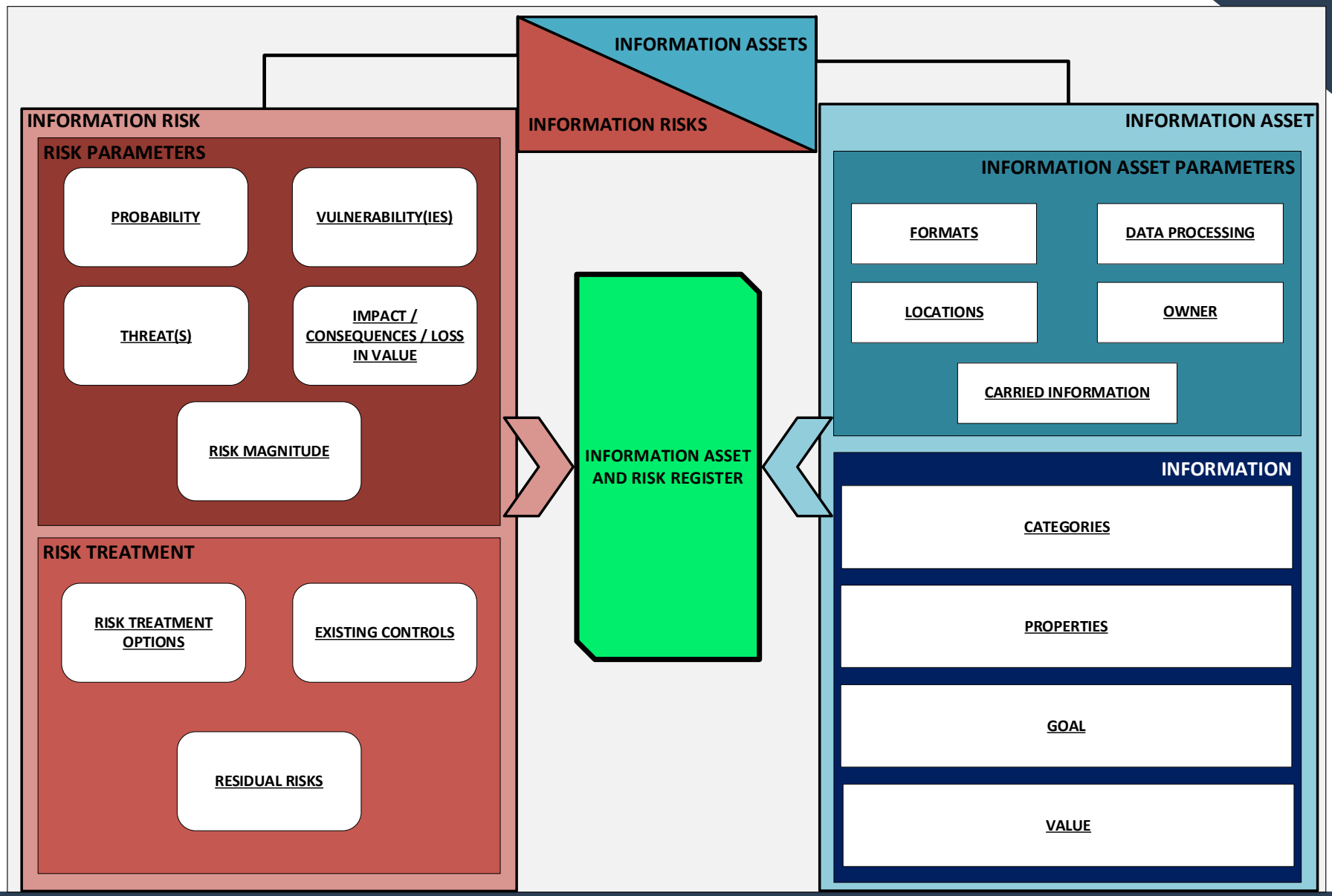
Résultats

0. Etat de l'art – typologies de RI basées sur …

Secteurs d'activités des institutions (Smallwood, 2014)	**Types de données/informations** (Vallès, 2015)	**Types de supports et formats de données**	**Niveaux de confidentialité**	**Nature des dommages** (Léger 2015)	**Types d'évènements imprévus** (Vermeys 2009)
• Administration publique, hôpitaux, banques, universités, …	• technique, scientifique, stratégique, opérationnel, …	• Données web, données électroniques, documents papiers, …	• Données ouvertes, confidentielles, …	• Dommage matériel (accidents, vandalisme) et immatériel (erreur, fraude, cyber crime)	• Dommage physique • Interaction humaine • Défaillance technique • Attaques internes et externes • Abus de données • Perte de données • Erreurs logicielles

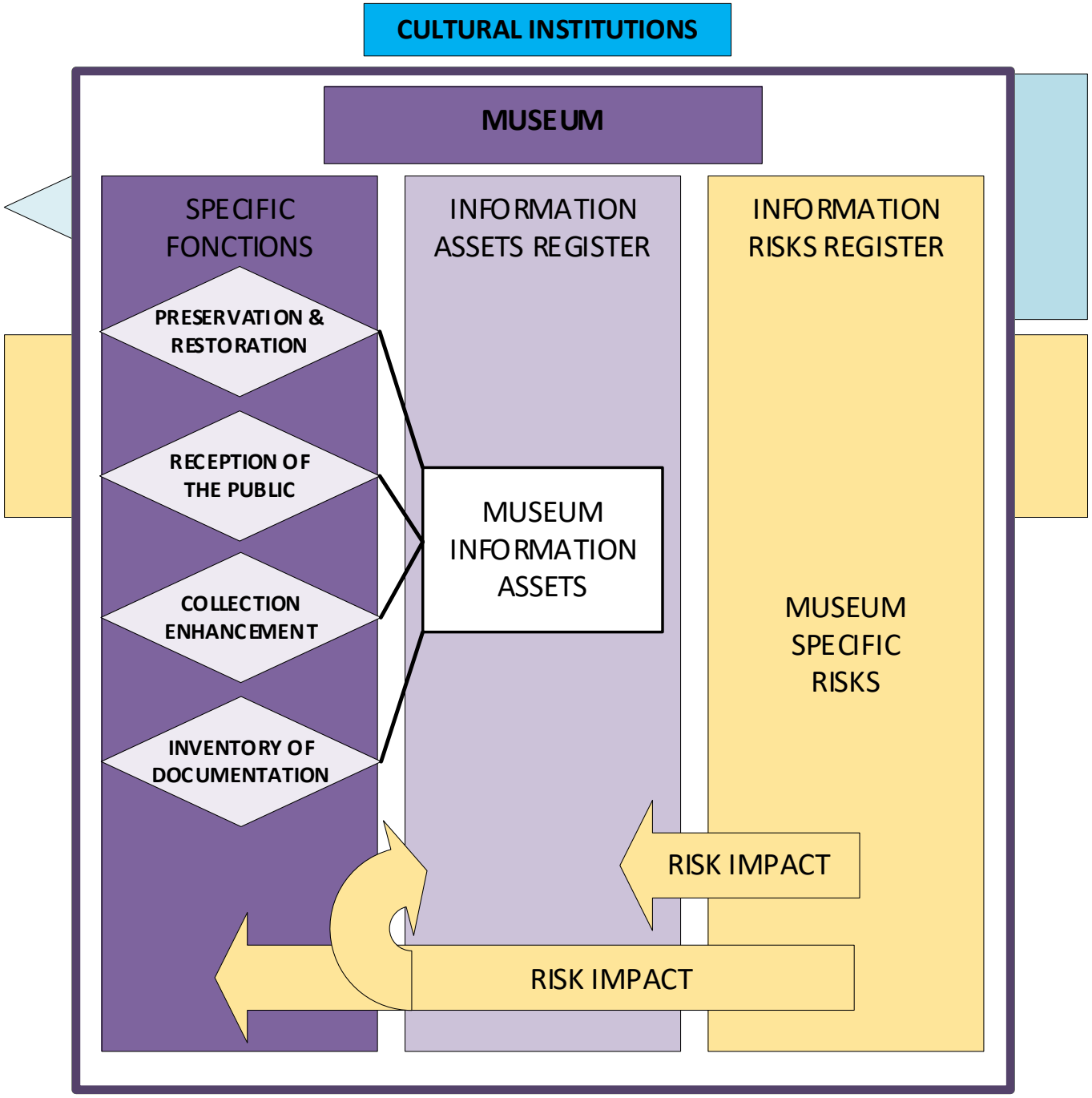
Résultats

1. Cadre conceptuel et typologique des RI



Résultats

2. Cartographie des RI par type d'institution



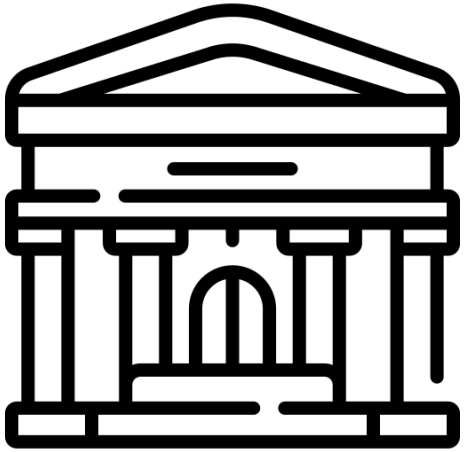
Résultats

3. Études de cas auprès d'institution

Trois études de cas

Archives publiques d'une ville

Archives publiques d'une région

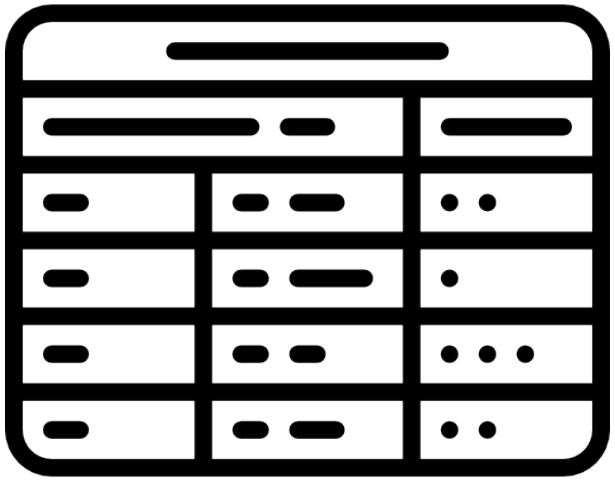


Musée privé

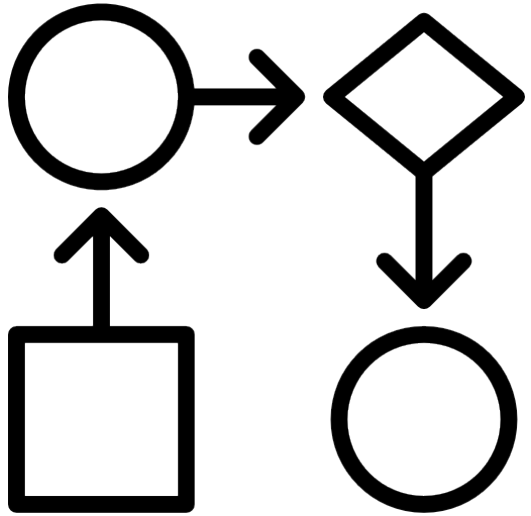
Résultats

3. Études de cas auprès d'institution

Résultats



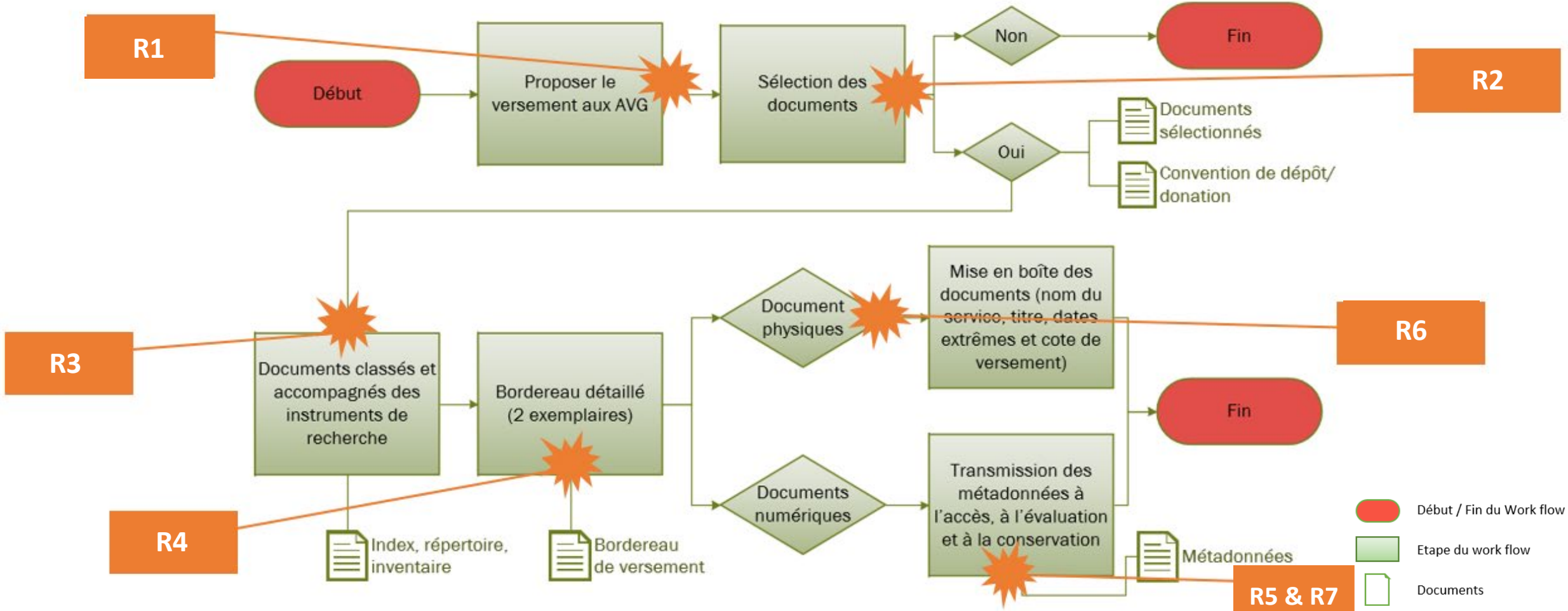
Tableaux détaillés des différents risques et des actifs informationnels



Modélisation des risques et des actifs informationnels dans des **workflows**

Résultats

3. Études de cas auprès de l'Archives publiques d'une ville



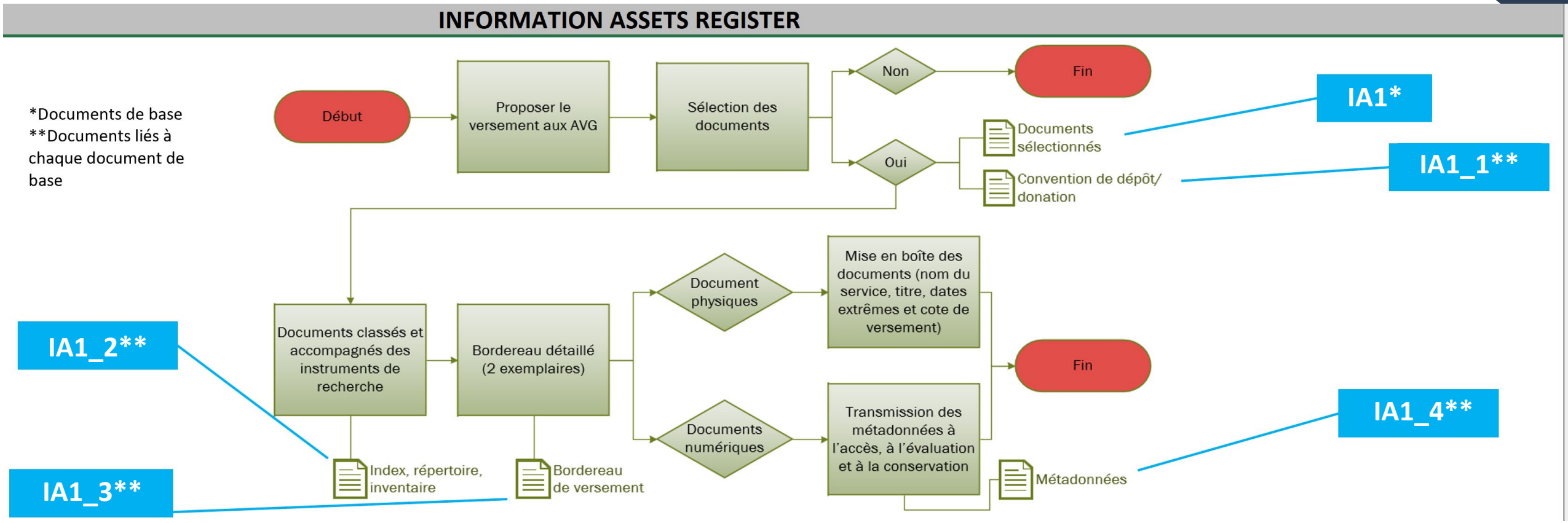
Résultats

3. Études de cas auprès de l'Archives publiques d'une ville

N°	Titre	Type	Vulnérabilités	Proba.	Impact	Ampleur du risque	Contrôle existant	Options de traitement des risques	Risques résiduels	Commen-taires
R1	Absence de prise en compte de demande de versement	Organi-sationnel	• Mauvaise définition des rôles • Employé en charge du traitement des versements en vacance et absence de remplaçant	Possible (2)	Modéré (2)	Moyen	-	Instaurer un rôle de remplacement lors d'absence ou de vacance de la personne ayant le rôle de traiter les demandes de versement		
R2	Erreur dans la sélection des documents à conserver / pas accepté	Erreur Humaine	• Inattention des employés en charge de la sélection	Possible (2)	Très élevé (4)	Majeur	Calendrier de conservation	Double vérification des documents lors du tri		
R3	Document classé dans un mauvais fonds	Erreur Humaine	• Inattention des employés en charge du classement	Possible (2)	Très élevé (4)	Majeur	Plan de classement	Double vérification des documents lors du classement		
R4	Perte du bordereau de versement	Erreur Humaine	• Inattention des employés en charge du versement	Possible (2)	Modéré (2)	Moyen	2 exemplaires du bordereau			
R5	Métadonnées incomplètes	Erreur Humaine	• Inattention des personnes qui versent	Probable (3)	Considérable (3)	Majeur	-	Instaurer une fiche de description des métadonnées qui sont impératives à fournir		
R6	Erreurs sur les informations indiquées lors de la mise en boîte des documents	Erreur Humaine	• Inattention des employés	Probable (3)	Très élevé (4)	Majeur	Calendrier de conservation	Double vérification des documents lors de la création des boîtes		

Résultats

3. Études de cas auprès d'institution



Résultats

3. Études de cas auprès d'institution

N° actif info.	N° document de base	Titres	Formats	Data processing	Locations	Owners	Categories of information	Goals	Commentaires
IA1		Documents sélectionnés	Papier, PDF, Excel	Retranscrit par le greffier lors de la séance du XX.XX.XXXX	Locale n°2	XXX	Engagente	Servir de preuve et d'aide mémoire pour les éléments discuté et les décisions prises lors de la séance du XX.XX.XXXX	
	IA1_1	Convention de dépôt / donation	Papier, PDF, Excel	Rempli par X le XX.XX.XXXX	Locale n°2	XXX			
	IA1_2	Index, répertoire, inventaire	Papier, PDF, Excel	Rempli par X le XX.XX.XXXX	Locale n°2	XXX			
	IA1_3	Bordereau de versement	Papier, PDF, Excel	Rempli par X le XX.XX.XXXX	Locale n°2	XXX			
	IA1_4	Métadonnées	Dublin Core, MARC21, XML, RDF…	Rempli par X le XX.XX.XXXX	Locale n°2	XXX			
…	…		…	…	…	…	…	…	…

Résultats

4. Processus, outils, indicateurs de suivi, mesures et contrôle d'impact

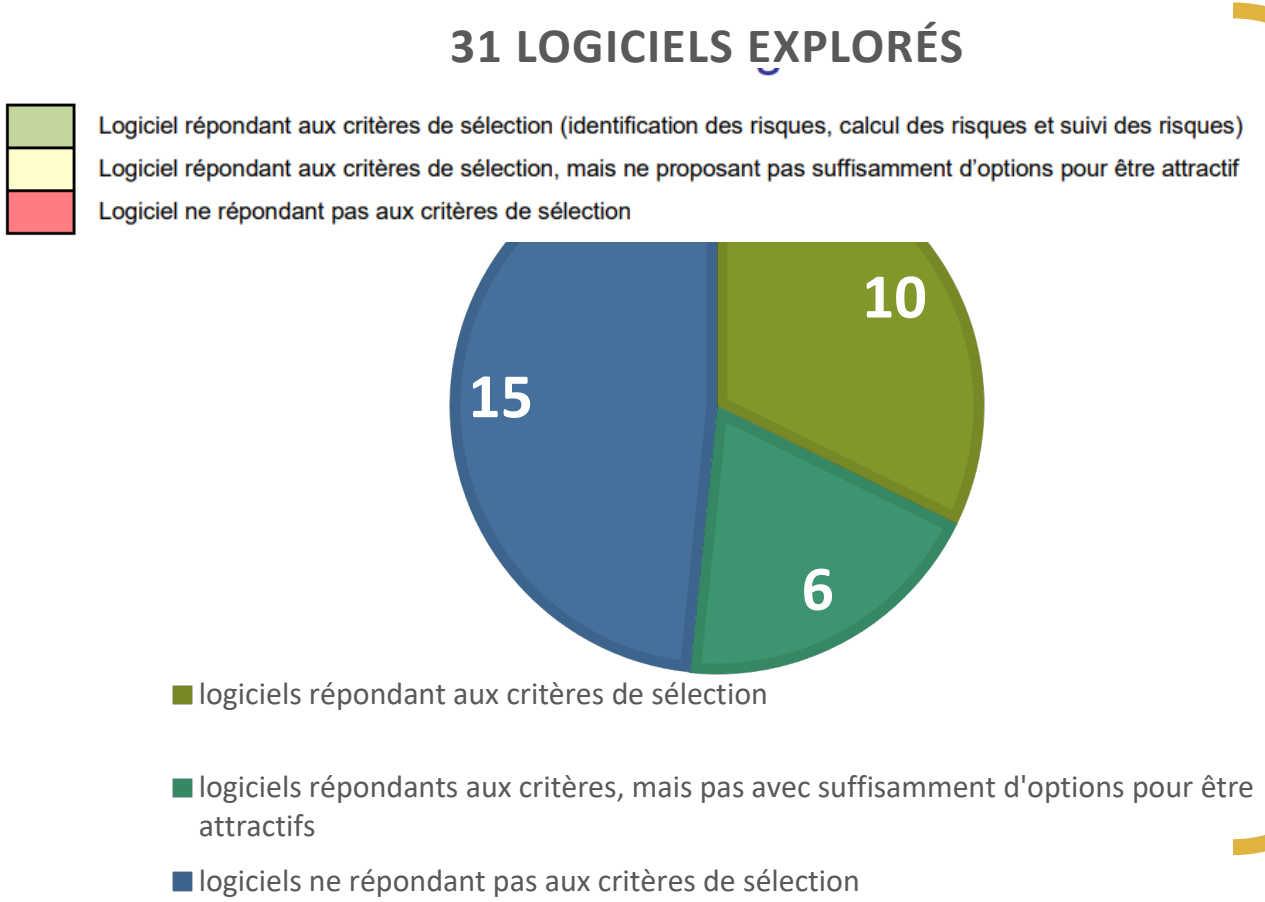
Indicateurs de suivi, les mesures et le contrôle d'impact (cf. tableau de bord)

Types de risque	Vulnérabilités	Probabilités	Impacts
Magnitude de risque	Contrôles existants	Options de traitement du risque	Risques résiduels

Résultats

4. Processus, outils, indicateurs de suivi, mesures et contrôle d'impact

Outils logiciels



Plusieurs constats :

- Absence de logiciel open source
- Peu de logiciels en langue française
- Logiciels principalement américains (6 sur les 16 logiciels répondant aux critères de sélection)
- Logiciels sous forme de modules ou packs
- Logiciels principalement sur mesure

Logiciel répondant aux critères de sélection (identification des risques, calcul des risques et suivi des risques)

Logiciel répondant aux critères de sélection, mais ne proposant pas suffisamment d'options pour être attractif

Logiciel ne répondant pas aux critères de sélection

Analyse générale → 10 logiciels

						User community			
N°	Nom du logiciel	Entreprise	Langues	Opensource	Pays	Share point	Clients	Site	Logiciel initiale
1	Enterprise Risk Management	Knowllence		non	France	oui	Centre de Gestion de la Fonction Publique Territoriale de la Guyane	https://www.knowllence.com/logiciel/logiciel-gestion-risque-entreprise.html	gestion des risques en entreprise
2	Resolver	Resolver	anglais	non	Canada	oui	Quebecor Media	https://www.resolver.com	sécurité d'entreprise, Gouvernance, risque et conformité, sécurité de l'information
3	CURA manage uncertainty	CURA		non	Singapour	oui	Kellogg's	https://www.curasoftware.com/enterprise-risk-management/	gestion des risques en entreprise
4	Corporate Business Management plateform	corporater	anglais	non	Norvège	non	Gassco	https://corporater.com/en/	gestion des risques en entreprise
5	HighBond	Galvanize	allemand, anglais, français	non	Canada	non	Coca-Cola	https://www.wegalvanize.com/highbond/	gestion des risques, de la conformité et de la sécurité des données
6	Optimiso	Integrum	allemand, anglais, français	non	Suisse	non		https://info.gartnerdigitalmarkets.com/integrum-gdm-lp?category=risk_mgmt&utm_source=capterra	gestion des risques en entreprise
7	Risk management Software enablon	Enablon	anglais	non	France	non	MOL Group	https://enablon.com/	risque et conformité, ingénierie et opérations, EHSQ et durabilité
8	BIC GRC	GB Tec	allemand, anglais, espagnol	non	Allemagne	non	Das Bundesarchiv	https://www.gbtec.com/	gestion des risques en entreprise
9	Qualios	Qualios	anglais, espagnol, français	non	France	oui	PnG, BNP	https://www.qualios.com/	gestion électronique de document
10	Tessi	Tessi	anglais, français	non	France	non		https://www.tessi.eu/fr/solution/technologies/edition-de-logiciels/securite-confiance-numerique/securite-documentaire/	sécurité documentaire
11	Xerox	Xerox	francais	oui	Congo	oui		https://www.xerox.com/fr-cg/logiciel-gestion-workflow	gestion de workflow
12	GRC Toolbox Pro	SwissGRC	allemand, anglais	non	Suisse	non	Confédération suisse	https://swissgrc.com/en/risk-management/	gestion des risques en entreprise
13	Logicgate Risk Cloud	Logicgate		non	Etats-Unis	non	Intradiem	https://www.logicgate.com/resources/enterprise-risk-management/	gestion des risques en entreprise
14	Fusion Framework System	Fusion Risk Management	anglais	non	Etats-Unis	oui	ETS	https://www.fusionrm.com/offerings/operational-risk-management/?dpm=51311	gestion des risques
15	Opture	Opture	allemand, anglais	non	Allemagne	non	Kantonsspital St-Gallen	https://www.opture.com/en/home.html	gestion des risques
16	ERM essential	Tracker Networks	anglais	non	Canada	non	pwc / kpmg	https://trackernetworks.com/essential-erm/	gestion des risques
17	Quantivate It risk management	Quantivate	anglais	non	Etats-Unis	non	Docufree	https://quantivate.com/solutions/it-risk-management-software/	gestion risques informationnels
18	ARC	Arcrisk	anglais	non	Royaume-Unis	non		https://www.arcrisk.com/	cybersécurité
19	Netwirx	Netwirx	allemand, anglais, espagnol, français	non	Etats-Unis	oui	Reading international, virgin, NHS	https://www.netwrix.com/it_risk_assessment.html?utm_source=capterra&utm_medium=cpc&utm_campaign=risk_management	data security
20	Tandem Information Security and Compilance Software	Tandem	anglais	non	Etats-Unis	non	Surtout des banques	https://tandem.app/	cybersécurité et gestion des risques informationnels
21	MetricStream IT and Cyber Risk Management	MetricStream	anglais	non	Etats-Unis	oui	Surtout des banques	https://www.metricstream.com/products/it-and-cyber-risk-management.htm	cybersécurité et gestion des risques informationnels
22	OneTrust GRC	OneTrust	allemand, anglais, espagnol, français, italien	non	Etats-Unis	non	La Mairie de Neuilly sur Seine	https://www.onetrust.com/solutions/grc-platform/	gestion des risques en entreprise
23	Document Control Software	MasterControl	allemand, anglais, français	non	Etats-Unis	non		https://www.mastercontrol.com/quality/document-control-software/	gestion des risques en entreprise avec une fonction dédiée aux documents
24	Zeenea	Zeenea	anglais, français	non	France	non	Societe générale, Renault Digital	https://zeenea.com/metadata-management-platform/	gestion des métadata
25	Rubrik	Rubrik	anglais, français	non	Etats-Unis	oui	HBO, Mazda, Honda, expedia	https://www.rubrik.com/en/lp/webinars/rubrik-product-demo?utm_source=capterra&utm_medium=display-ads&utm_content=display-nam-us-	back-up, management et securité de data

20 Critères spécifiques

1	Accessoire
2	Important
3	Indispensable

Numéro	Titre	Pondération
1	Mutlilingue	2
2	Accessible en ligne	3
3	Flexibilité et customisation	2
4	Convivialité	2
5	Important dans le marché	2
6	Suisse	1
7	Expertise domaine GLAM	2
8	Logiciel sur pc, android…	1
9	Compliance avec la norme ISO 31000 et éventuellement la 27005 et la 18128	3
10	Compliance légale et réglementaire	3
11	Identification des risques et classement risque interne et externe	3
12	Création d'une terminologie des risques	3
13	Création de rapport d'analyse	3
14	Création d'infographie des risques	3
15	CAPA (Corrective Action Preventive Action)	2
16	Gestion de la réponse aux risques	3
17	Registre de risques informationnels	3
18	Identification des données sensibles	2
19	Système d'alerte	2
20	Prise en compte du cyber risque	2
21	Base de données disponible hors ligne	1
22	Possibilité de créer une base d'actifs informationnels	1

Top cinq des logiciels pertinents

N°	Nom du logiciel	Entreprise	Site	Logiciel initial
1	Entreprise Risk Management	Knowllence	https://www.knowllence.com/logiciel/logiciel-gestion-risque-entreprise.html	Gestion des risques en entreprise
5	GRC Toolbox Pro	SwissGRC	https://swissgrc.com/en/risk-management/	Gestion des risques en entreprise
8	Quantivate	Quantivate	https://quantivate.com/solutions/it-risk-management-software/	Gestion des risques informationnels
9	Tandem Information Security and Compliance Software	Tandem	https://tandem.app/	Cybersécurité et gestion des risques informationnels
10	Protech.ERM	Protech	https://www.protechtgroup.com/en-au/enterprise-risk-management-for-risk-professionals	Gestion des risques en entreprise

Résultats

4. Processus, outils et indicateurs de suivi

Logiciels	Avantages	Inconvénients
Tandem	un bon support client Fondé en 2008, donc a beaucoup d'ancienneté Connu pour être simple d'utilisation modules compatibles Les différents événements sont facilement planifiables, et des accès à différents niveaux peuvent être attribués aux utilisateurs	Le logiciel est spécialisé dans les institutions financières, par conséquent, les normes et les outils correspondent davantage à ce type de structure Selon *Capterra*, les risques juridiques ne sont pas pris en compte dans la gestion de risques

Résultats

4. Processus, outils et indicateurs de suivi

Logiciels	Avantages	Inconvénients
Swiss GRC	Logiciel Suisse Compliance management (ISO 19600) Gestion des risques (identification & analyse)	Difficile de trouver l'information Manque une base des risques Pas une clientèle GLAM Ne gère pas l'information sensible Pas de conformité avec les normes ISO 27005 et ISO 18128

Résultats

4. Processus, outils et indicateurs de suivi

Logiciels	Avantages	Inconvénients
Quantivate	Tableau de bord et rapport customisable "what if" → scénario Applications supplémentaires possibles	Risques des répétitions si plusieurs modules sont mis ensemble Pas les normes 31000, 27005 ou 18128 Pas d'information sur la fusion des différents modules Surtout adapté pour les banques et assurances (risques de ne pas être customisable)

Résultats

4. Processus, outils et indicateurs de suivi

Logiciels	Avantages	Inconvénients
Protech. ERM	Analyse de risques Base de risque disponible Auto-évaluation de risque & contrôle Possibilité de personnaliser les formulaires papier ou électroniques. Dashboard de risques	Disponible uniquement en anglais N'identifie pas les données sensibles

Résultats

4. Processus, outils et indicateurs de suivi

Logiciels	Avantages	Inconvénients
Enterprise Risk Management (Knowllence)	Possibilité de cartographier Possibilité de créer un plan d'urgence Plus que le modèle SWOT pour l'analyse Module entier sur la RGPD avec une approche macro Création depuis 2001 Module entier pour la bonne synchronisation et la possibilité de coupler avec d'autres modules pas en lien avec la gestion des risques	Peu d'information hors du site web officiel Surtout adapté pour les lois françaises Pas les normes 31000, 27005 ou 18128 Uniquement 3 modules pour la gestion des risques

Résultats

5. Tableau de bord

Identification du risque				Gestion du risques			Traitement du risques			
Identifiant du risque	Titre	Type de risque	Vulnérabilités	Probabilités	Impact	Ampleur du risque	Contrôle existant	Options de traitement des risques	Risques résiduels	Commentaires
R1	…	…	…	…	…	…	…	…	…	…
R2	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…

Résultats

6. Spécifications pour l'outil de pilotage (software)

Fonctionnalités génériques

Fonctionnalités

Risque informationnel

Fonctionnalités Actif informationnel

Résultats

6. Spécifications pour l'outil de pilotage (software)

Fonctionnalités génériques

- Accessible en ligne
- Flexible et personnalisable
- *User-friendly*
- Conforme aux lois et règlementations

Résultats

6. Spécifications pour l'outil de pilotage (software)

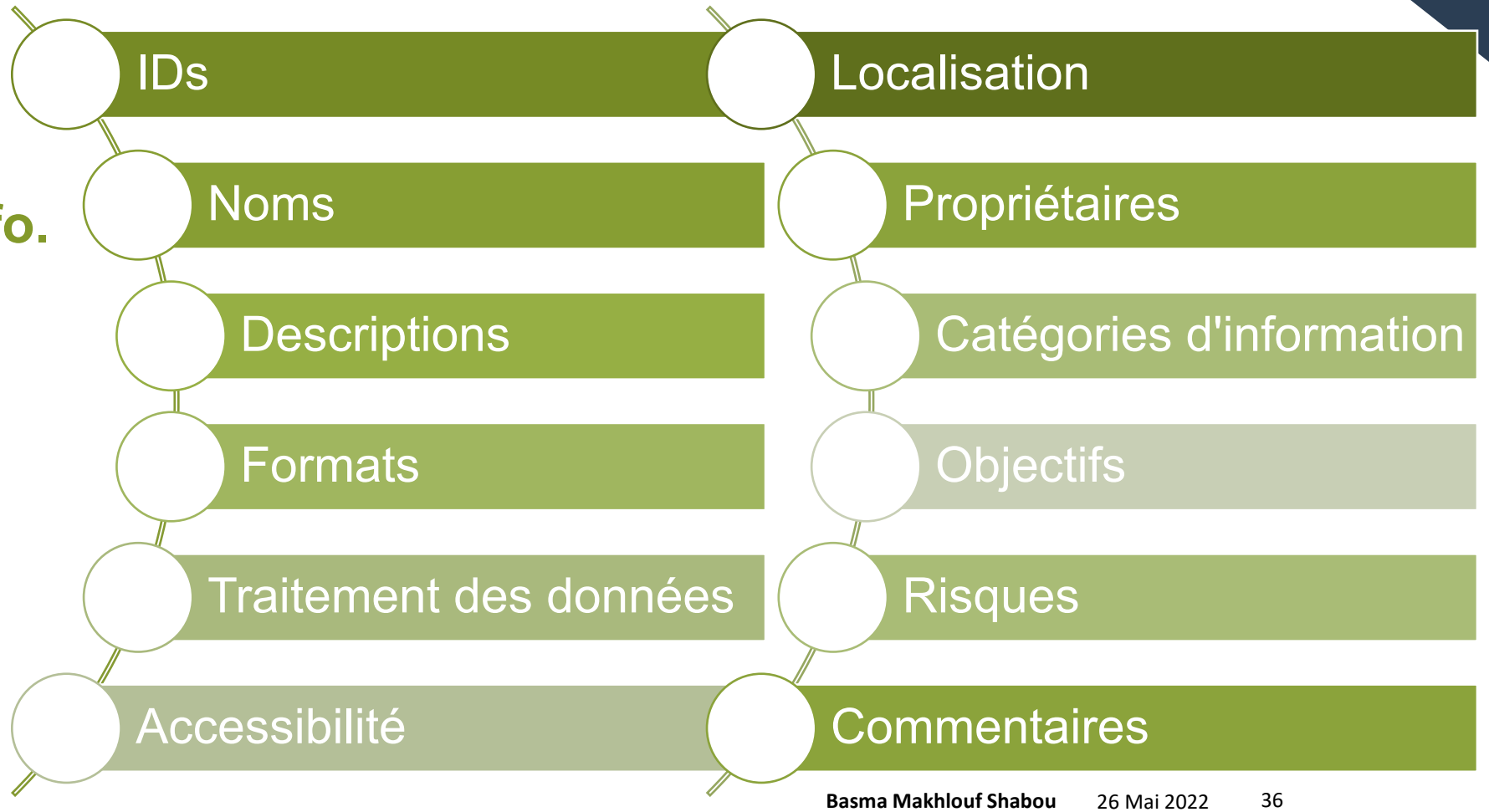
Fonctionnalités RI

- Identification et classification des risques internes et externes
- Création d'une terminologie des risques
- Création de rapports d'analyse
- Création d'infographies sur les risques
- Gestion de la réponse aux risques
- Système d'alerte
- Prise en compte du cyber risque

Résultats

6. Spécifications pour l'outil de pilotage (software)

Fonctionnalités Actif Info.



- L1 : Cadre conceptuel et typologie des RI (10/2019)
- L2 : Cartographie des RI par type d'institution (02/2020)
- L3 : Etudes de cas (10/2020)
- L4 : Processus, outils, indicateurs de suivi (10/2020)
- L5 : Tableau de bord (10/2020)
- L6 : Spécifications de l'outil de pilotage (01/2021)

Valorisation des résultats

- Master IS (HEG) :
  - Le contenu de cette recherche a été présenté et réutilisé dans le cadre de deux cours du Master IS sur 1) la méthodologie de la recherche et sur 2) la gouvernance des données (2020) .
- Licence et Master RM à la Sorbonne Paris- Abu Dhabi
  - Le contenu de cette recherche a été présentée et réutilisé dans le cadre des cours de Master et de Licence en records management de l'Université de la Sorbonne Paris Abu Dhabi (2021-2022)

Références

- SMALLWOOD, Robert F., 2014. *Information governance: concepts, strategies and best practices*. Hoboken : Wiley. Wiley CIO series. ISBN 9781118218303.
- LÉGER, Marc-André, 2015. Typologie des risques informationnels. *Le site de Marc-André Léger* [en ligne]. 23 octobre 2015. [Consulté le 24 mai 2022]. Disponible à l'adresse : http://web.archive.org/web/20200927222001/http://www.leger.ca/2015/10/23/typologie-des-risques-informationnels/
- VALLÈS, Lyonel, 2015. Le risque informationnel et l'urgence de le gérer de façon adéquate. *Lyonel Vallès, CISA, CRISC* [en ligne]. 20 décembre 2015. [Consulté le 24 mai 2022]. Disponible à l'adresse : http://lyonelvalles.com/2015/12/20/le-risque-informationnel-et-lurgence-de-le-gerer-de-facon-adequate/
- VERMEYS, Nicolas, 2009. *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile* [en ligne]. Montréal : Université de Montréal. Thèse. [Consulté le 24 mai 2022]. Disponible à l'adresse : https://papyrus.bib.umontreal.ca/xmlui/handle/1866/3663

Merci !

basma.makhlouf-shabou@hesge.ch