École d’été « Patrimoine et Numérique »

Gouvernance informationnelle : enjeux et perspectives

# Contexte

## Révolution numérique

Bien qu'elle trouve ses racines dans les débuts de l'automatisation au xviiie siècle, la révolution numérique débute véritablement à partir du milieu du xxe siècle avec le développement de l'informatique et des télécommunications (Révolution numérique 2021).

Au cours des années 2000, une étape supplémentaire est franchie avec la volonté de transformation numérique des institutions et de la société.

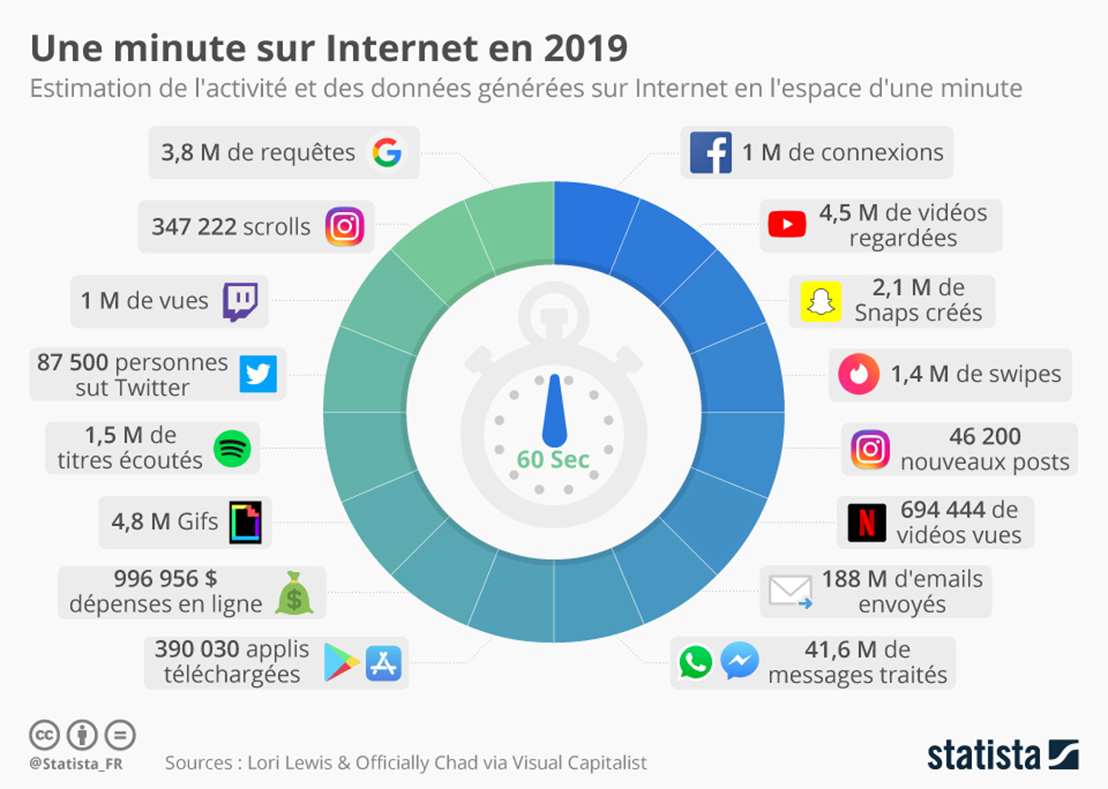
### Exemples

L'un des objectifs du programme *Action publique 2022* du Gouvernement français est une dématérialisation de l'ensemble (100 %) des services publics en 2022 (Texier 2019 ; Gouvernement français 2021).

En Suisse, la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) a lancé le projet *Justitia 4.0* qui vise à offrir un portail central hautement sécurisé par lequel transiteront les dossiers judiciaires entre les parties et les autorités (Foucault-Dumas 2019).

Cette transformation numérique a un coût énergétique. Hugues Ferreboeuf (2018, pp. 15-16) et son équipe estiment que « la consommation énergétique du Numérique dans le monde augmente d’environ 9% par an (période 2015 à 2020) » et que « [l]a part du Numérique dans la consommation finale d’énergie (elle-même en croissance de 1,5% par an) aura ainsi augmenté de presque 70% entre 2013 et 2020 ». Le Bitcoin consommerait plus d'électricité que la Suisse (Gaudiaut 2019).

## Infobésité



(Jenik 2019)

Un rapport de Deloitte estimerait la taille de l'univers numérique en 2020 à 44 zettabytes, soit 44 milliards de téra-octets, dont un grand nombre de données ne seront pas structurées (Boittiaux 2017).

## Sécurité de l’information

Durant la dernière décennie, le nombre de fuites de données et de "records" exposés a crû jusqu’en 2017, avant de se calmer un peu (Clement 2021).

Gartner estime que les dépenses investies dans la sécurité de l'information dépasseront les 124 milliards de dollars en 2019. (Moore, Keen 2018).

# Terminologie

Il est important de différencier les notions de gouvernance des données et de gouvernance de l’information. Pour cela, il faut s’intéresser aux concepts qui composent ces deux notions.

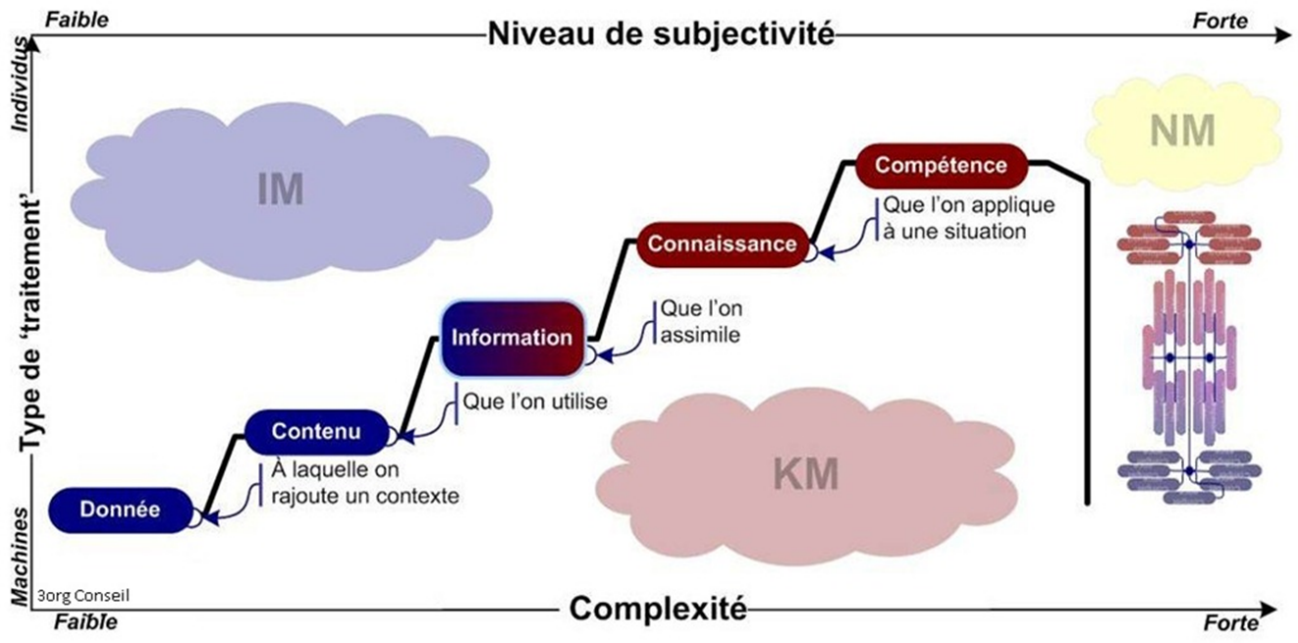
## Gouvernance

« A senior-level administrative structure that sets strategy for an organization by identifying roles, responsibilities, decision-making processes, policies, and procedures and that monitors outcomes and compliance » (InterPARES Trust 2018a)

## Donnée & Information

“An assemblage of data intended for communication either through space or across time” (InterPARES Trust 2018b)

“Whereas data connotes facts or ideas in their most atomized form, information refers to more complex concepts made up of multiple data elements. Information may take many forms, including words, sounds, images, and formulas” (Society of American Archivists [s. d.]))



Perrein 2010

IM = *Information management* : regroupe les principes et techniques pour traiter, stocker, récupérer, manipuler et contrôler l'accès à l'information permettant aux utilisateurs de trouver l'information dont ils ont besoin (Society of American Archivists [s. d.])

KM = *Knowledge management* : « ensemble de modes d'organisation visant à créer, collecter, organiser, stocker, diffuser, utiliser et transférer » (Cigref 2000, p. 12) les connaissances (documents ou expériences des collaborateurs) dans une organisation

NM = *Network management* : « ensemble des disciplines avec une orientation outils, qui permettent de conceptualiser, déployer et développer les environnements de réseaux sociaux » (Perrein 2011b)

## Actifs informationnels

“(…) An asset is any data, device, or other component of the environment that supports information-related activities. (…) Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization” (InterPARES, 2018c)

## Gouvernance des données

« Data governance is a newer, hybrid quality control discipline that includes elements of data quality, data management, IG policy development, business process improvement, and compliance and risk management. » (Smallwood 2014b, p. 16)

## Gouvernance de l’information

« IG is a subset of corporate governance, and includes key concepts from records management, content management, IT and data governance, information security, data privacy, risk management, litigation readiness, regulatory compliance, long-term digital preservation, and even business intelligence. » (Smallwood 2014b, p. 5)

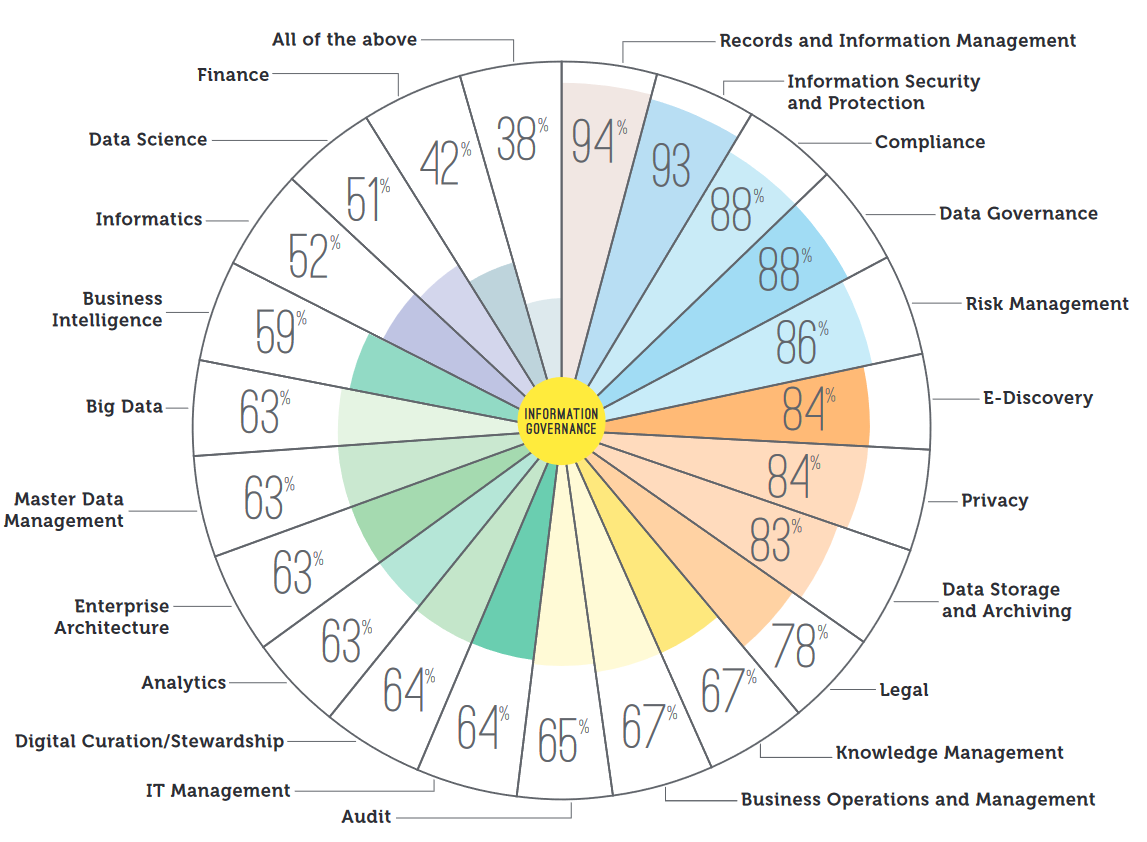
## En résumé

Smallwood résume les différences entre les gouvernances (informationnelle, des données, et IT), ainsi :

« IG consists of the overarching polices and processes to optimize and leverage information while keeping it secure and meeting legal and privacy obligations in alignment with stated organizational business objectives. IT governance consists of following established frameworks and best practices to gain the most leverage and benefit out of IT investments and support accomplishment of business objectives.

Data governance consists of the processes, methods, tools, and techniques to ensure that data is of high quality, reliable, and unique (not duplicated), so that downstream uses in reports and databases are more trusted and accurate. Master data management (MDM) tools can assist in this effort. » (Smallwood 2014a)

# Périmètre de la gouvernance



(Information Governance Initiative 2018)

# Normes et standards

## Normes et standards : quelles différences ?

Une **norme** est un « document, établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné » (Organisation internationale de normalisation 2004, p. 12)

**Exemples d’organisme reconnu :** en Europe, le Comité européen de normalisation (CEN) ; en France, l’Association française de normalisation (AFNOR) ; en Suisse, la Schweizerische Normen-Vereinigung (SNV) ; ou encore en Tunisie, l’Institut national de la normalisation et de la propriété industrielle (INNORPI).

Un **standard** est « l’ensemble de recommandations développées et préconisées par un groupe représentatif d’utilisateurs » (Ministère de l’Éducation nationale et de la jeunesse 2012)

Exemples de groupe représentatif d’utilisateurs : au niveau international, le World Wide Web Consortium (W3C), l’Institute of Electrical and Electronics Engineers (IEEE) ou encore l’Internet Engineering Task Force (IETF) élaborent des standards.

La principale disparité résulte dans le fait qu’un standard est issu d’un processus réactif mené par un groupe d’utilisateurs, alors qu’une norme définit un référentiel créé par un organisme reconnu et officiel (Bergery, 2011).

## Spécifique à la gouvernance de l’information

* **ISO/DIS 24143 Information and documentation — Information Governance — Concept and principles :** La norme vise à définir les concepts et principes relatifs à la gouvernance de l'information.

## En lien avec la gouvernance de l’information

* **ISO 15489-1:2016 Information et documentation — Gestion des documents d’activité — Partie 1: Concepts et principes :** La norme détermine les concepts et les principes liés à la création, la capture et la gestion des documents d'activité.
* **ISO 30300:2011 Information et documentation — Systèmes de gestion des documents d'activité — Principes essentiels et vocabulaire :** La norme « définit les termes et définitions qui s'appliquent aux normes relatives aux systèmes de gestion des documents d'activité (SGDA) et établit également les objectifs associés à l'utilisation d'un SGDA, fournit les principes, décrit une approche par processus et spécifie les rôles de la direction »".
* **ISO 30301:2019 Information et documentation — Systèmes de gestion des documents d'activité — Exigences :** La norme « spécifie les exigences relatives à un système de gestion des documents d'activité (SGDA) visant à soutenir un organisme dans la réalisation de son mandat, de sa mission, de sa stratégie et de ses objectifs par le développement et la mise en œuvre d'une politique et d'objectifs relatifs aux documents des activités et donne des informations sur le mesurage et la surveillance des performances ».
* **ISO 30302:2015 Information et documentation — Système de gestion des documents d'activité — Lignes directrices de mise en œuvre :** La norme « fournit des lignes directrices pour la mise en œuvre d'un Système de Gestion des Documents d'Activité (SGDA) conforme à l'ISO 30301 ».
* **ISO 38500 Technologies de l'information — Gouvernance des technologies de l'information pour l'entreprise :** La nome vise à fournir des principes directeurs sur l'utilisation efficace, efficiente et acceptable des technologies de l'information (TI) dans une organisation de tout type et de toute taille.

## En lien avec la gestion des risques informationnels

* **ISO 18128:2014 Information et documentation — Evaluation du risque pour les processus et systèmes d'enregistrement :** La norme « a pour objet d'aider les organismes à apprécier les risques liés aux processus et aux systèmes documentaires de manière qu'ils puissent s'assurer que les documents d'activité répondent aux besoins de gestion identifiés aussi longtemps que nécessaire ».
* **ISO 27005:2011 Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information :** La norme s’intéresse à la gestion des risques liés à la sécurité de l'information dans une optique des technologies de l'information. Elle se base également sur la norme ISO 31000 :2018.
* **ISO 31000:2018 Management du risque - Principes et lignes directrices :** Norme de référence pour tout ce qui concerne le management du risque, elle en expose les principes et les lignes directrices.
* **ISO 31010:2009 Gestion des risques -Techniques d'évaluation des risques :** Basée sur la norme précédente, elle développe les techniques d'évaluation des risques, toujours dans une optique générique.

# Méthodologie

## Audit informationnel

“‘*a systematic evaluation of information use, resources and flows, with verification by reference to both people and existing documents, in order to establish the extent to which they are contributing to an organisation's objectives'. (ASLIB IRM Network, London)*” (Henczel et Robertson 2015)

### Composants de l’audit informationnel

Henczel et Robertson (2015) identifient trois composants de l’audit informationnel :

1. Examen du processus :
   * Analyse des tâches - actions d'information (création, accès, utilisation, transfert, stockage), processus cognitifs, relations avec d'autres tâches.
   * Déconstruction de la tâche - identifier les priorités, les flux et les processus de décision en matière d'information ; identifier les interactions et les dépendances entre personnes et entre personnes et systèmes.
2. Contenu de l'information :
   * Identification de ce qui est détenu, de ce qui est nécessaire mais non disponible, de ce qui est disponible mais non accessible là où c'est nécessaire.
   * Évaluation de l'adéquation aux besoins
3. Capacité et comportement :
   * Identification des lacunes en matière de compétences liées à la création, la découverte, la fourniture, l'accès, le transfert, l'utilisation et le stockage de l'information.
   * Identification des comportements qui influencent la création, la découverte, la fourniture, l'accès, le transfert, l'utilisation et le stockage efficaces de l'information.

### Approches

Griffiths (2012) note un ensemble minimal d'activités liées à l'audit informationnel :

* Vérifier
  + l'authenticité et l'exactitude des informations ajoutées au système d'information de l'organisme ;
  + la provenance des informations au sein d'un système ;
  + le bon fonctionnement du système de stockage et de récupération des informations ;
* Évaluer
  + **la valeur économique des ressources d'information dans les systèmes de l’organisme** et en déduire une valeur financière qui peut (ou non) apparaître dans les comptes de l'organisation - ce qui implique que l'application d'une valeur financière réelle ou théorique crée un actif qui implique certaines normes de gestion de l'information, et aussi que cette valeur est au moins partiellement créée par le contexte fourni par le propriétaire de l'entreprise ou le titulaire de la licence ;
  + **la valeur informationnelle du contenu des systèmes de l’organisme** - c'est-à-dire vérifier non seulement l'intégrité physique de l'information, mais aussi évaluer son exactitude, son actualité, sa fiabilité, sa pertinence, son degré de duplication ou d'unicité, et d'autres éléments qui pourraient être utilisés pour établir un score pour la valeur de la connaissance réelle ou du contenu de l'information pour l'organisation.

Frost et Choo (2017) évoquent sept étapes :

1. **Planifier l'audit** en fixant des objectifs, en identifiant les parties prenantes, en délimitant la portée du projet et en allouant les ressources, en choisissant une méthodologie et en élaborant des stratégies de communication et d'entreprise.
2. **Collecter des données** dans une base de données de ressources d'information, concevoir et distribuer des questionnaires, organiser des groupes de discussion et mener des entretiens personnels.
3. **Analyser les données** recueillies et la recherche.
4. **Évaluer les lacunes et les doublons** dans l'information, cartographier et interpréter les flux d'information, formuler des recommandations et élaborer un plan de gestion du changement.
5. **Communiquer les recommandations** aux parties prenantes par le biais de rapports écrits, de présentations et de séminaires, de pages Web et de retours personnels.
6. **Mettre en œuvre les recommandations** par le biais de programmes de mise en œuvre, de plans de changement formels, de stratégies post-mise en œuvre et de politiques d'information.
7. **Gestion continue des services d'information** pour mesurer et évaluer les changements par le biais d'un audit régulier de l'information et d'un cycle d'évaluation des services.

## Gestion des risques informationnels

### ISO 18128:2014

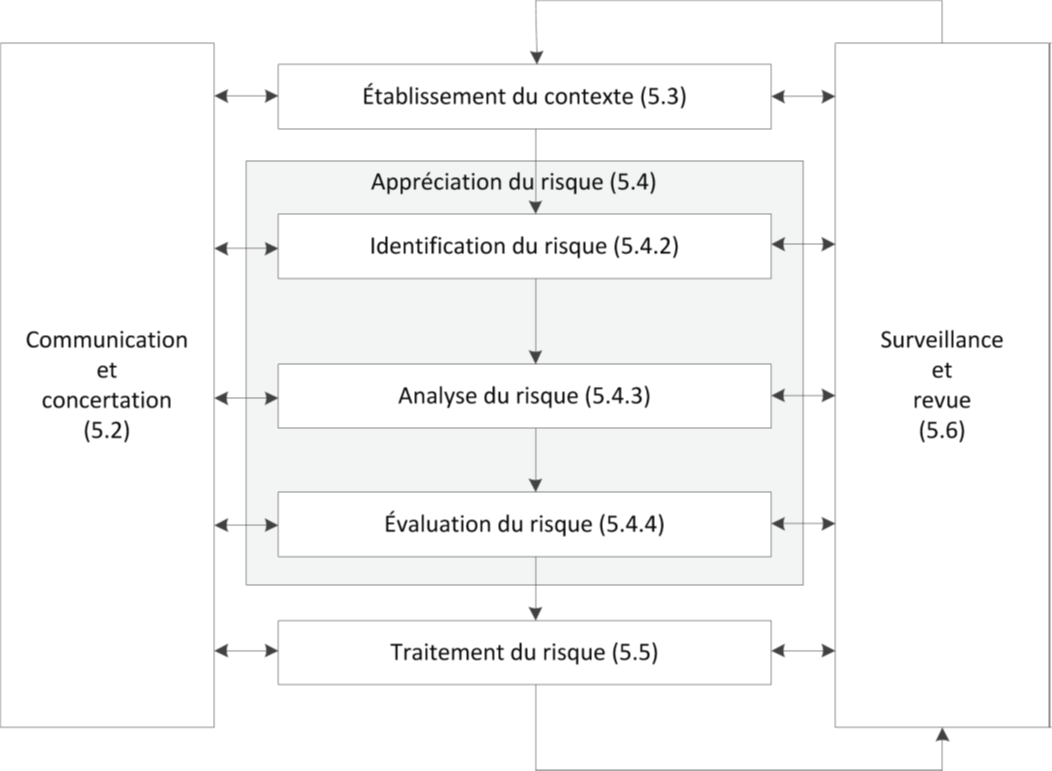
#### Champ d’application

Information et documentation - Évaluation du risque pour les processus et systèmes d'enregistrement

La norme s’intéresse :

* aux documents d’activité, c'est-à-dire les « informations créées, reçues et préservées comme preuve et actif par une personne physique ou morale dans l’exercice de ses obligations légales ou la conduite des opérations liées à son activité » (ISO 15489-1:2016, p. 3) ;
* à l’appréciation des risques appliqués aux documents d’activité (identification, analyse et évaluation)
* à la communication des risques identifiés, analysés et évalués

 Elle ne couvre pas le traitement des risques informationnels.



#### Communication et concertation

Échanger avec les parties prenantes internes et externes afin de prendre en compte les différents points de vue et expertises

#### Établissement du contexte

Énoncé des objectifs, définition des paramètres internes et externes à prendre en compte, détermination du domaine d'application et des critères de risque

#### Appréciation du risque

##### Considérations

Plusieurs éléments sont à prendre en compte :

* **Rôles et responsabilité :** c’est-à-dire « spécifier le rôle des professionnels de la gestion documentaire dans l’appréciation du risque lié aux processus et aux systèmes documentaires » (ISO:18128:2014, p. 2)
* **Étendue et portée des activités d'évaluation des risques :** pour éviter des redondances et d'éventuels conflits avec d'autres domaines d'appréciation des risques, il convient d'en préciser les relations et de leurs limites.
* **Critères de risque en conformité avec les lois, règlements de la juridiction de l’organisme** incluant :
  + Nature et type de conséquences
  + Mode d’expression des probabilités
  + Méthode de détermination des niveaux des risques
  + Critères déterminant le moment ou un traitement du risque devient nécessaire
  + Critères déterminant si un risque est acceptable
  + Conditions et méthodes de combinaison de risques

 L’identification des risques repose sur leur potentiel à compromettre les caractéristiques d’**authenticité**, de **fiabilité**, d’**intégrité** et **exploitabilité** des documents d’activité, les rendant inaptes à remplir les objectifs ayant présidé à leur création. (ISO:18128:2014, p. 3)

##### Identification des risques

Elle est structurée en fonction du contexte, des systèmes et des processus documentaires et prend en compte les éléments suivants :

* Contexte externe
  + Changements dans le contexte politique et social
  + Environnement macro-économique et technologique
  + Environnement physique et infrastructure
  + Menaces extérieures contre la sécurité
* Contexte interne
  + Changements organisationnels
  + Changements technologiques
  + Ressources - Personnel et compétences
  + Ressources - Finances et matériels
* Systèmes documentaire
  + Conception des systèmes
  + Maintenance
  + Durabilité et continuité
  + Interopérabilité
  + Sécurité
* Processus documentaire
  + Conception des documents d’activité
  + Création de documents d’activité et mise en œuvre de systèmes documentaires
  + Métadonnées
  + Utilisation des documents d’activité et des systèmes documentaires
  + Maintenance de l’utilisabilité
  + Sort final des documents d’activité

Analyse des risques

Le niveau de risque se base sur la combinaison de la probabilité et des conséquences .

Probabilité : fréquence à laquelle un risque peut survenir (rare, faible, moyenne, élevée), voir le tableau 1 pour des exemples

Conséquences : impacts subis si le risque survient effectivement (mineur, modéré, majeur, grave), voir le tableau 2 pour des exemples

Méthodes et sources :

* Observation, statistiques, analyse de la documentation concernant :
  + définition des accès, règles de conservation, journal des éliminations, schéma des métadonnées, journaux des utilisations, surveillance des non-conformités, …

##### Évaluation des risques

Comparaison entre le niveau de risque calculé lors de l'analyse et les critères de risque établis auparavant, voir le tableau 3 pour des exemples

#### Surveillance et revue

Il s’agit de contrôles périodiques ou ponctuels des processus et informations de management des risques

**Risques Informationnels dans les Organisations (RIO)**

Il s’agit d’un projet de recherche mené de 2019 à 2021 qui avait comme principaux objectifs de :

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



Paramètres du risque

Les paramètres du risque sont les éléments qui caractérisent un risque :

* **Probabilité (*probability*) :** « possibilité que quelque chose se produise » (Organisation internationale de normalisation 2018) ;
* **Vulnérabilités (*vulnerabilities*) :** faiblesses qui permettent à des menaces spécifiques de provoquer des effets néfastes sur les systèmes et les informations (Organisation internationale de normalisation 2018 ; Saffady 2020) ;
* **Menaces (*threats*) :** événements d'origine humaine ou naturelle qui peuvent provoquer des effets néfastes sur les systèmes et les informations lorsqu'ils sont combinés à des vulnérabilités spécifiques ;
* **Impact / conséquences / perte de valeur (*loss in values*) :** Saffady (2020) définit la conséquence comme un résultat négatif résultant de l’exploitation d’une vulnérabilité par une menace. L'impact d'un risque se reflète dans sa gravité, c'est-à-dire l'intensité de la menace / des dommages potentiels (Merna & Al-Thani 2008), qui peut être interprétée comme le produit de la fraction de la collection susceptible d'être menacée et de la perte de valeur potentielle de la collection (Waller 2013). La perte de valeur peut être définie comme la réduction de la valeur de l'actif informationnel s'il était compromis (Waller 1994 ; Mattord & Wiant 2008) ;
* **Niveaux de risque (*risk magnitude*) :** Cela correspond à l’« importance d'un risque exprimée en termes de combinaison des conséquences et de leur vraisemblance (Organisation internationale de normalisation 2018). Elle peut être calculée comme suit (Waller 1994, 2013 ; Bülow 2010) : Probabilité x Étendue x Fraction susceptible x Perte de valeur.

Traitement du risque

Les traitements du risque correspondent aux moyens d'atténuation :

* Les options de traitement du risque (*risk treatment options*) : correspondent aux différentes possibilités de traitement du risque, comme la réduction, le maintien, le refus ou le transfert du risque.
* Les contrôles existants (*existing controls*) : éléments de sauvegarde du risque déjà en place avant le processus de gestion du risque (ISO 27005).
* Risques résiduels (*residual risks*) : risque restant après le traitement du risque (Organisation internationale de normalisation 2018) ; généralement faible, il est toléré car un traitement supplémentaire n'aurait aucun effet ou à un coût trop élevé (Sutton 2014).

Paramètres des actifs informationnels

Les actifs informationnels peuvent être caractérisés par leur

* format ;
* traitement des données ;
* emplacement ;
* propriétaire ;
* les informations qu'ils contiennent.

Information

*Attributs*

Ces attributs correspondent aux cinq grandes familles d'informations listées par Perrein (2014) :

* **Information engageante**, destinée à être utilisée comme preuve dans un litige ;
* **Information patrimoine**, qui détient une valeur historique pour l'organisation ;
* **Information structurante**, utilisée pour classer d'autres informations ;
* **Information personnelle**, qui permet d'identifier une personne physique et est protégée par des lois et règlements visant à protéger les données personnelles (par exemple, la LPD en Suisse et le RGPD dans l'UE) ;
* **Informations sensible**, qui comprend des données clés pour les organisations, comme les brevets, et qui doit rester confidentielle.

*Propriétés*

Chai (2021) présente la triade CIA comme « un modèle conçu pour guider les politiques de sécurité de l'information au sein d'une organisation. [...] Les éléments de la triade sont considérés comme les trois composantes les plus cruciales de la sécurité ». Les initiales CIA représentent les mots Confidentialité (*Confidentiality*), Intégrité (*Integrity*) et Disponibilité (*Availability*). Raggad (2010) rajoute trois éléments supplémentaires pour compléter la triade :

* **authentification**, c’est-à-dire un mécanisme conçu pour vérifier l'identité d'un agent, humain ou système, avant de lui accorder l'accès ou non
* **non-répudiation**, il s'agit de s'assurer que les deux parties ne peuvent nier avoir bien participé à la transmission, l'expéditeur en envoyant le message et le destinataire en le recevant
* **le concept de risque**.

*Objectifs*

Il s'agit de s'intéresser aux objectifs des actifs informationnels, car la « plupart des auteurs soulignent que l'information a la caractéristique d'"être utile" (Machlup, 1983), "pertinente" (Introna, 1997) ou "d'avoir un effet sur l'action et les décisions" (Kuhlen, 1991, 2004 ; Meadow & Yuan, 1997) » (Boell et Cecez-Kecmanovic 2010).

*Valeur*

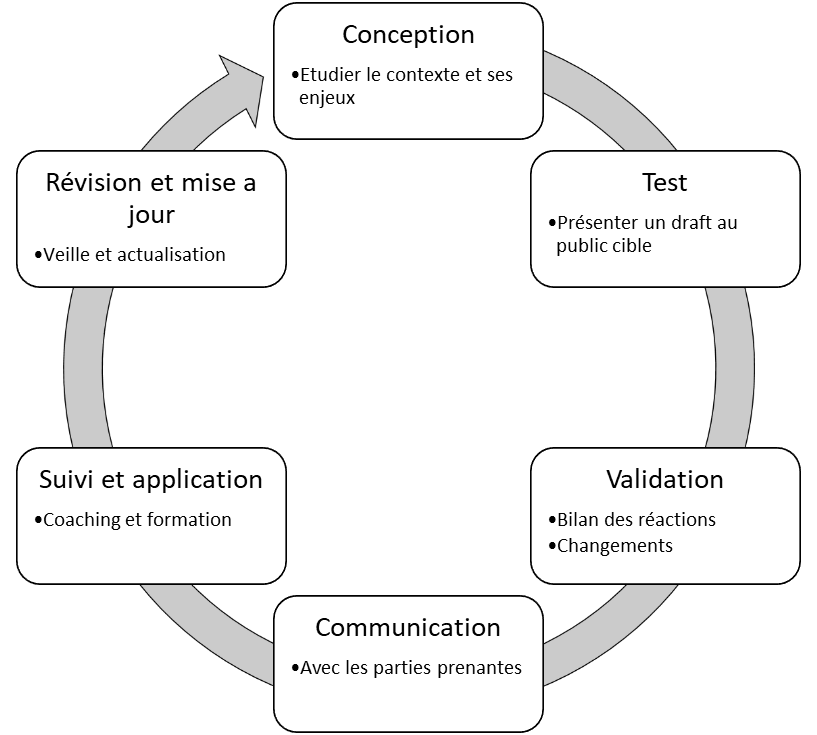
Il s'agit de la valeur attribuée à l'information produite ou acquise par les organisations et fournie sous la forme d'un produit ou d'un service. L'information n'a pas de valeur propre. Elle dépend du contexte, de l'utilisation et de l'objectif de l'information et de la manière dont elle a été obtenue (Maravilhas 2015).

# Outils

## Politique de gouvernance informationnelle

Document directeur élaboré à partir d’une concertation collective impliquant plusieurs acteurs, dans lequel sont formalisés les objectifs, les règles, les processus, les dispositifs nécessaires à l’optimisation de la gestion performante de l’ensemble des ressources informationnelles de l'organisation (ARMA International, 2012; Perrein, 2013; Makhlouf Sabou, 2018)

### Conception d’une politique de gouvernance informationnelle



(Makhlouf Shabou 2018)

#### Conception

* **identifier les buts de la politique** afin d'établir une vision commune de la gouvernance en accord avec les politiques de l'institution qui servira de cadre de référence tout au long du processus de mise en place de la politique
* **recenser les politiques internes de l'institution et les PGI d'autres institutions similaires** afin d'harmoniser la politique avec son contexte d'application
* adapter le contenu de la politique à l'organisation :
  + déterminer le public cible (utilisateurs internes et externes de l'information institutionnelle)
  + identifier les collaborateurs clés de l'organisation et leur attribuer des responsabilités
  + repérer les ressources (humaines, financières, matérielles, logistiques et informatiques) nécessaires
* écriture de la politique selon un processus délibératif afin que le contenu reflète les buts et les attentes de l'ensemble des acteurs de la gouvernance

#### Test et validation

La validation de la politique s’effectue en deux volets :

* test et retours des utilisateurs
* validation de la version finale par la hiérarchie :
  + l’instance responsable du mandat de réalisation
  + la direction

#### Communication

Une campagne de communication et de formation doit être mise en place afin d'aider à la **gestion du changement** en créant une **culture de la gouvernance informationnelle** adoptée par les employés et intégrée dans leurs tâches de tous les jours.

Deux outils principaux :

* Plan de communication
  + segmentation du public afin d'adapter le discours
  + multicanal (bulletins internes, l’intranet, l’internet, les réseaux sociaux, les blogues internes, les courriels, les affiches promotionnelles, les réunions)
* Formation
  + individuellement et/ou en groupe
  + en personne et/ou en ligne

#### Suivi et application

Pour le suivi et l’application de la politique, il est nécessaire d’établir un **plan d’action** qui exposera les objectifs et les tâches de chaque acteur.

* Les tâches doivent être :
  + assignées selon l'expertise
  + intégrées aux activités quotidiennes
  + avalisées par la hiérarchie

#### Révisions et mise à jour

Afin d'évaluer l'implantation de la politique, il convient de faire des **contrôles de qualité** qui nécessite de :

* déterminer le niveau de suivi des principes de GD
* évaluer l'impact des actions
* mesurer le taux de satisfaction du personnel
* disposer de métriques claires et précises

La politique de gouvernance informationnelle est un outil dynamique qui nécessite **une mise à jour régulière** pour s'adapter à un contexte en perpétuelle évolution.

### Structure d’une politique

Il n’existe pas de modèle standardisé de politique. La structure proposée se base sur l’analyse d’une dizaine de politiques.

* Intitulé du document
* Présentation du contexte organisationnel
* Objectifs de la politique
* Champs d’application / public cible
* Environnement normatif
* Environnement légal et règlementaire
* Responsabilités
* Outils opérationnels
* Principes
* Processus et mise en œuvre
  + Administration des documents
  + Accessibilité des informations
  + Sécurité et protection des données
* Glossaire
* Date d’adoption de la politique
* Historique des versions de la politique
* Références

### Format d’une politique

* Officiel
* Structuré en sections thématiques
* Style directif
* Termes clairement définis
* Format permettant une diffusion

## Registre d’actifs informationnels

“a catalogue of the information an organization holds and processes, where it is stored, how it moves and who has access” (Zafrin 2018)

« Registre de catégorisation : Répertoire dans lequel sont consignés les niveaux d’impact, sur le plan de la DIC [disponibilité, intégrité, confidentialité], des actifs informationnels. » (Québec - Secrétariat du Conseil du trésor 2016, p. 27)

### Principaux champs (National Archives of Australia [s. d.] ; The National Archives 2017)

**Description :** rassemble les métadonnées permettant d'identifier les actifs informationnels, comme le nom, l'identifiant, la description et les sujets clés.

**Rôles et responsabilités :** rassemble les métadonnées permettant d'identifier les propriétaires des actifs informationnels et les domaines ou postes ayant une certaine autorité sur leur gestion.

**Sécurité et restrictions associées :** comprend les autorisations qui sont soumises à la position ou à la fonction métier.

**Dispositions relatives à l'utilisation, à l'accès et à la diffusion :** comprend les métadonnées permettant de faciliter les demandes de liberté d'information, le respect des droits d'auteur, le partage général des actifs informationnels et des données ouvertes dans l'ensemble du gouvernement.

**Risques**: concernant les activités et les actifs informationnels eux-mêmes.

### Exemples de modèles

* National Archives of Australia : <https://www.naa.gov.au/sites/default/files/2021-06/Information-Asset-Register-template.XLSX>
* Office of the Victorian Information Commissionner (2020) : <https://ovic.vic.gov.au/resource/sample-information-asset-register-iar-template/>
* The National Archives (s.d.) : <http://www.nationalarchives.gov.uk/documents/information-management/iar_template.xls>
* Monash University : <https://adm.monash.edu/records-archives/archives/IAR/information-asset-register.xml>

## ITrust IG Maturity Models (Makhlouf Shabou 2019)

Il s’agit d’un modèle basé sur différentes recherches dans le cadre du projet InterPARES EU 29 et EU 30 : Information Governance Maturity in European Public Administrations: Nature, Assessment tools and Methods (phase I & II, 2016-2018) :

* un travail de master : Information governance: nature and implementation from the European public administrations’ perspective
* un projet de recherche : La maturité de la gouvernance de l’information dans les administrations publiques européennes : la perception de la gouvernance de l’information dans l’administration publique genevoise
* une synthèse des modèles existants avec l'aide du travail de Proença et al. (2017)

Plusieurs tendances ont été identifiées :

* croisement de différents dimensions à travers différents niveaux indiquant le développement et la progression à atteindre;
* utilisation des dimensions et des sous-dimensions pour cibler des aspects progressivement différents à évaluer dans les pratiques informationnelles;
* généralement 5 niveaux de développement
* application d'une collecte de données qualitatives (entretiens, observation, etc.) pour l'évaluation de la pratique informationnelle

### Dix dimensions

1. **Responsabilités et rôles (*responsibilities and roles*) :** il s’agit de la définition explicite des rôles et règles pour les utilisateurs, producteurs et gestionnaires de l'information ;
2. **Engagement des parties prenantes (*stakeholder engagement*) :** il s’agit de la connexion explicite avec tous ceux qui ont un intérêt direct dans l'information de l’institution ;
3. **Cadre et politique, y compris la gestion des risques (*framework and policy including risk management*) :** regroupe les documents stratégiques de l’institution définissant les ressources d'information, leur contexte spécifique et la gestion des risques y relatifs ;
4. **Identification, création et propriété des actifs informationnels (*information asset identification, creation and ownership*) :** prise en compte de la création, de la cocréation et de la propriété citoyenne des informations (Adesemowo, Von Solms, & Botha, 2016) ;
5. **Valeur, qualité et livraison de l'information (*information value, quality and delivery*) :** regroupe les outils, normes et règles permettant de fournir des données fiables ;
6. **Gestion des droits (*rights management*) :** regroupe la gestion des droits d’accès afin d’assurer la confidentialité des données ;
7. **Gestion des documents d’activité (*records management*) :** regroupe les outils, normes et règles pour les calendriers et processus de conservation et d'élimination des données et des documents et plan de classification ;
8. **Sécurité et résilience de l'information (*information security and resilience*) :** assurer la disponibilité et les protections de l'information afin de garantir le maintien de l'information pour les activités de l’institution ;
9. **Préservation à long terme (*long-term preservation*) :** regroupe les infrastructures, outils, normes et directives garantissant l'accès durable aux documents et archives organisationnels ;
10. **Suivi et changement (*monitoring and change*) :** activités et actions soutenant les changements et les évolutions pour garantir que le système reste à jour et pertinent, en répondant aux nouveaux défis et opportunités.

### Trois critères

* **Personnes (*people*) :** critères relatives aux personnes incluant des éléments comme le leadership, l'expertise professionnelle ou encore l'inclusion de citoyens
* **Système (*system*) :** critères comprenant aussi bien le développement des processus que l'infrastucture en passant par les logiciels et les outils
* **Éthique (*Ethics*) :** critères s'intéressant aux conformités aux lois, règlements et normes, tant bien généraux que spécifiques

### Cinq niveaux

1. Non existant (*not existent*)
2. En développement (*developing*)
3. Normes minimales (*minimum standards*)
4. Normes aspirationnelles (*aspirational standards*)
5. Transformationnel (*transformational*)

## Outils de records management

Inventaire typologique

Plan de classement

Calendrier de conservation

# Perspectives

## Grandes tendances (Dawson 2019; Markarian 2019)

### Sécurité

Les malwares deviennent de plus en plus sophistiqués et visent désormais les appareils mobiles et les infrastructures réseaux.

### Conformité et e-discovery

Le règlement général sur la protection des données (RGPD) réaffirme le rôle de la gouvernance informationnelle en demandant la création d’un registre des activités de traitement.

### Automatisation

L’automatisation pour les fonctions de classification ou d’évaluation s’avèrent désormais indispensables pour gérer le volume des informations produites. Dawson (2019) relève que les organisations créent, enregistrent et gèrent beaucoup trop d'informations pour un classement manuel. Dayley et al. (2018) notent dans leur recherche que plus de 80% de l'information d'une organisation est composée de données non structurées, réparties ainsi :

* Données réglementaires ou de conformité = < 1%
* Données sur la mise en suspens légale = < 1%
* Données dignes de mention = < 2%
* Données en cours de fabrication, données de référence ou de valeur analytique = ~15%
* Données redondantes, obsolètes et/ou triviales = ~80%

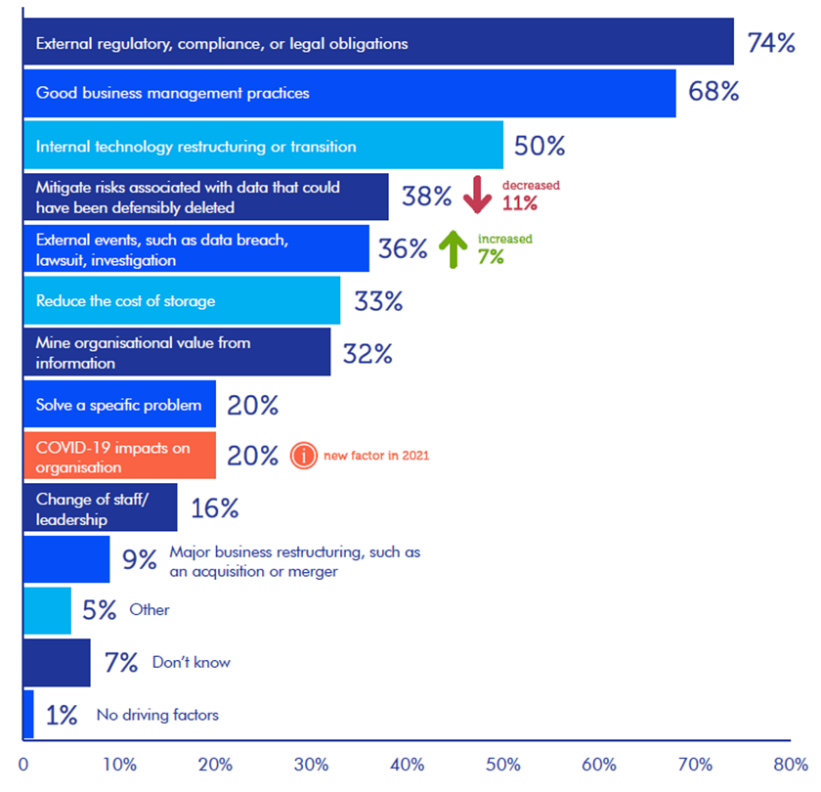
## IG en Australie et Nouvelle-Zélande: enquête 2019

### Profil des participants

L’enquête cible majoritairement l’Australie (85% de répondants) et la Nouvelle-Zélande (8%).

Les participants proviennent pour la plupart d’organisations gouvernementales (61%) et sont impliqués dans la gouvernance informationnelle.

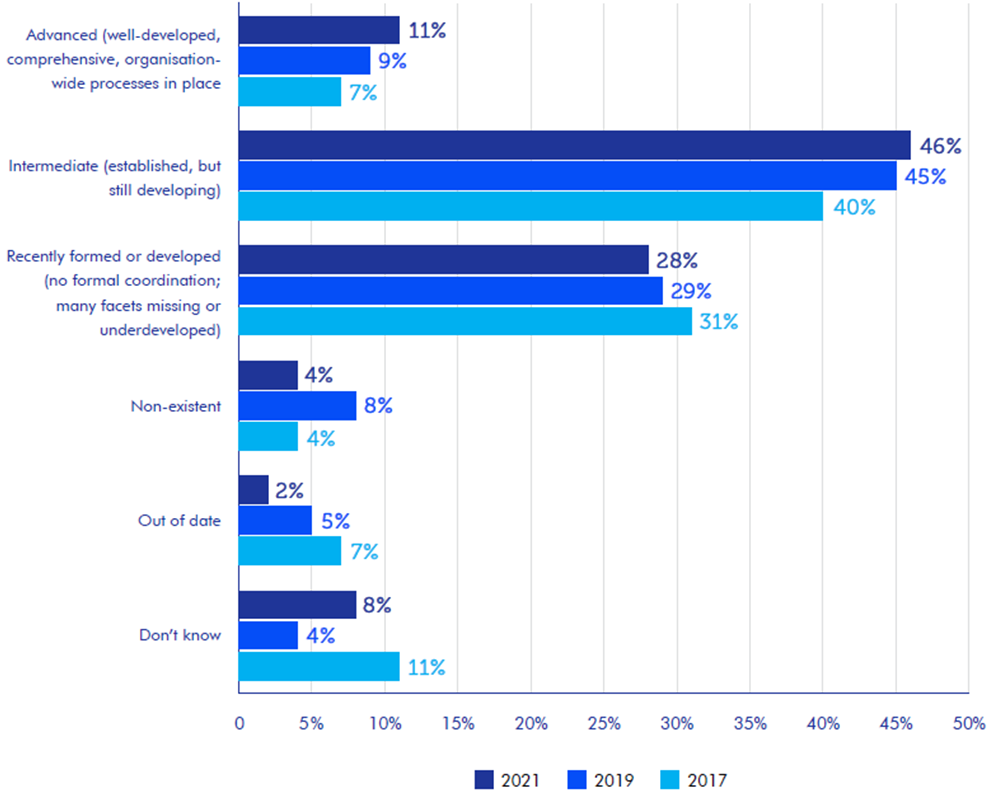
### Les principaux facteurs motivant les projets d'IG

Selon les participants, quatre principaux facteurs motivent les projets de gouvernance informationnelle :

1. Efficience administrative
2. Conformité
3. Transition numérique
4. Risques informationnels

(Information Governance ANZ 2021, p. 8)

### Maturité de la gouvernance informationnelle



(Information Governance ANZ 2021, p. 9)

## 10 éléments à savoir sur l'automatisation de la GI (AIIM 2019)

1. 79% des organisations réalisent qu’ils doivent opérer une véritable transformation numérique pour survivre ;
2. Dans les deux ans qui suivent le volume d'information croitra d'un facteur 4.2 et plus de 60% de ces informations seront non ou semi-structurées ;
3. Près des trois-quarts des organisations estiment la gouvernance informationnelle comme importante ou critique pour leur stratégie ;
4. En cinq ans, le pourcentage d'organisation affirmant avoir des politiques de gouvernance informationnelles robustes et à l'échelle de l'organisation a presque doublé, passant de 14% à 25% ;
5. Les risques perçus comme associés à un échec de gouvernance informationnelle ne se limitent plus au risque légal et concernent également :
   * pour 41% la perte de confiance ou la mauvaise publicité liées à la perte de données
   * pour 38% les mesures prises suite à une perte ou une exposition de données personnelles
   * pour 35% la perte de propriété intellectuelle ou d'informations confidentielles pour l'entreprise
   * pour 34% les coûts liées à des litiges suite à une mauvaise tenue des dossiers
6. 43% des organisations estiment qu'elles ne dépensent pas assez pour la GI vis-à-vis des risques informationnels et 14% estiment qu'elles dépensent trop ;
7. 53% des organisations estiment l'automatisation des processus de gouvernance informationnelle comme très importants ;
8. 70& des organisations voient un lien entre l'intelligence artificielle et leur futur succès, en matière de capture de l'information ;
9. Seuls 38% des organisations s'estiment avancées ou très avancées dans l'adoption d'outils d'intelligence artificielle pour l'automatisation des processus de gouvernance informationnelle ;
10. Seuls 42% des organisations s'estiment avancées ou très avancées dans l'utilisation de *machine learning* afin d'extraire le contenu et alimenter les métadonnées d'un document.

Vous trouverez l’infographie en annexe.

## Télétravail

La situation sanitaire l’a accéléré, mais le phénomène existait déjà avant, celui du travail. Cela entraine différents :

* défis (Craine 2021) :
  + Garantir la sécurité des données
  + Assurer ses obligations de conformité
* et problématiques (Combs 2020) :
  + Utilisation excessive des fichiers stockés localement
  + Partage inapproprié de contenu
  + Raccourcissement des processus de révision et d'approbation importants

Cullen (2021) liste plusieurs recommandations pour opérationnaliser la sécurité au service de la productivité et de la gouvernance :

* Inventorier ses données
* Arrêter le marquage par l'utilisateur final
* Laisser les anciens serveurs derrière vous
* Permettre un partage contrôlé
* Évaluer la gouvernance

# Bibliographie

ADESEMOWO, Adeniji K., VON SOLMS, Rossouw & BOTHA, Reinhard A., 2016. Safeguarding information as an asset: Do we need a redefinition in the knowledge economy and beyond?. *South African Journal of Information Management* [en ligne]. Vol. 18, n° 1. [Consulté le 14 octobre 2021]. Disponible à l’adresse : <http://dx.doi.org/10.4102/sajim.v18i1.706>

ARMA INTERNATIONAL, 2012. *Glossary of records and information management terms*. Overland Park, KS, ARMA International

ASSOCIATION FOR INTELLIGENT INFORMATION MANAGEMENT (AIIM), 2019. *10 Things You Need to Know About Automating Information Governance* [en ligne]. [Consulté le 24 novembre 2021] Disponible à l'adresse : <https://info.aiim.org/10-things-you-need-to-know-about-automating-information-governance>

BERGERY, Line, 2011. *Le management par les valeurs*. Paris: Hermès science publications - Lavoisier.

CLEMENT, J., 2021. Annual number of data breaches and exposed records in the United States from 2005 to 2020 (in millions). *Statista* [en ligne]. 3 mars 2021. [Consulté le 18 octobre 2021]. Disponible à l'adresse : <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

Club informatique des grandes entreprises françaises (CIGREF), 2000. Gérer les connaissances: Défis, enjeux et conduite de projet [en ligne]. Octobre 2000. [Consulté le 28 septembre 2021]. Disponible à l’adresse : <http://www.cigref.fr/cigref_publications/RapportsContainer/Parus2000/2000_-_Gerer_les_connaissances.pdf>

COMBS, Tara, 2020. Remote Working: The Information Governance Challenge of the Decade. *GRC World Forums* [en ligne]. 14 mai 2020. [Consulté le 24 novembre 2021]. Disponible à l'adresse : <https://www.grcworldforums.com/governance/remote-working-the-information-governance-challenge-of-the-decade/416.article>

CRAINE, Kevin, 2021. Remote Work and Information Governance. *Workflow* [en ligne]. 13 septembre 2021. [Consulté le 23 novembre 2021]. Disponible à l'adresse : <https://www.workflowotg.com/remote-work-and-information-governance/>

CULLEN, Ann Marie, 2021. Work Remotely Without Compromising Your Data. *AIIM Blog* [en ligne]. 7 janvier 2021. [Consulté le 23 novembre 2021]. Disponible à l'adresse : <https://info.aiim.org/aiim-blog/tips-for-working-remotely-information-governance>

DAWSON, Pat, 2019. Information Governance Innovations in 2019. *Everteam* [en ligne]. 22 janvier 2019. [Consulté le 24 novembre 2021]. Disponible à l'adresse : <https://www.everteam.com/en/information-governance-innovations-in-2019/>

DAYLEY, Alan, TIRSU, Julian, DE SIMONI, Guido, LANDERS, Garth, MEUNIER, Marc-Antoine, 2018. Market Guide for File Analysis Software. *Gartner Research Publication* [en ligne]. ID: G00317005. 27 mars 2018. [Consulté le 24 novembre 2021]. Disponible à l'adresse : <https://www.gartner.com/en/documents/3869701>

FERREBOEUF, Hugues (dir.), 2018. *Lean ICT - Pour une sobriété numérique* [en ligne]. The Shift Project, octobre 2018. [Consulté le 28 septembre 2021]. Disponible à l'adresse: <https://theshiftproject.org/wp-content/uploads/2018/11/Rapport-final-v8-WEB.pdf>

FOUCAULT-DUMAS, Charles, 2019. Comment Justitia 4.0 compte dématérialiser la justice suisse. *ICT Journal* [en ligne]. 15 février 2019. [Consulté le 28 septembre 2021]. Disponible à l'adresse : <https://www.ictjournal.ch/news/2019-02-15/comment-justitia-40-compte-dematerialiser-la-justice-suisse>

FROST, Robert B. et CHOO, Chun Wei, 2017. Revisiting the information audit: A systematic literature review and synthesis. *International Journal of Information Management* [en ligne]. Février 2017. Vol. 37, n° 1, pp. 1380‑1390. [Consulté le 1er octobre 2021]. Disponible à l’adresse : <https://doi.org/10.1016/j.ijinfomgt.2016.10.001>

GAUDIAUT, Tristan, 2021. Le Bitcoin dévore plus d'électricité que la Suisse. *Statista* [en ligne]. 5 mai 2021. [Consulté le 28 septembre 2021]. Disponible à l'adresse : <https://fr.statista.com/infographie/18624/comparaison-consommation-energetique-electricite-bitcoin-et-pays/>

GOUVERNEMENT FRANÇAIS, 2021. Action Publique 2022 : pour une transformation du service public. *Gouvernement.fr* [en ligne]. 30 octobre 2018. Mis à jour le 21 juin 2021. [Consulté le 28 septembre 2021]. Disponible à l'adresse : <https://www.gouvernement.fr/action/action-publique-2022-pour-une-transformation-du-service-public>

GRIFFITHS, Peter, 2012. Information Audit: Towards common standards and methodology. *Business Information Review* [en ligne]. Mars 2012. Vol. 29, n° 1, pp. 39‑51. [Consulté le 1er octobre 2021]. Disponible à l’adresse : <https://doi.org/10.1177/0266382112436791>

HENCZEL, Sue et ROBERTSON, Graham, 2015. Demystifying the Information Audit. *SLA 2015 Boston* [en ligne]. 16 juin 2015. [Consulté le 5 octobre 2021]. Disponible à l'adresse : <https://www.sla.org/wp-content/uploads/2015/06/1650_Demystifying-the-Information-AuditHenczel.pdf>

INFORMATION GOVERNANCE ANZ, 2021. *IG Industry Survey Report* [en ligne]. Mai 2019. [Consulté le 7 juin 2022] Disponible à l'adresse : <https://www.infogovanz.com/resources/#survey-reports>

INFORMATION GOVERNANCE INITIATIVE, 2018. IGI State of the Industry Report [en ligne]. Vol. 3. [Consulté le 19 octobre 2021]. Disponible à l’adresse : <https://iginitiative.com/wp-content/uploads/The-State-of-IG-Report-Volume-III-highres.pdf>

INTERPARES TRUST, 2018a. Governance (English). *ITrust Terminology* [en ligne]. [Consulté le 28 septembre 2021]. Disponible à l’adresse : <https://interparestrust.org/terminology/term/governance/en>

INTERPARES TRUST, 2018b. Information (English). *ITrust Terminology* [en ligne]. [Consulté le 8 juin 2022]. Disponible à l’adresse : <https://interparestrust.org/terminology/term/information/en>

INTERPARES TRUST, 2018c. Information asset (English). *ITrust Terminology* [en ligne]. [Consulté le 8 juin 2022]. Disponible à l’adresse : <http://interparestrust.org/terminology/term/information%20asset>

JENIK, Claire, 2019. Une minute sur Internet en 2019. *Statista* [en ligne]. 18 juillet 2019. [Consulté le 28 septembre 2021]. Disponible à l'adresse : <https://fr.statista.com/infographie/13160/activite-sur-internet-en-une-minute/>

MAKLOUF SHABOU, Basma, 2018. An Information Governance Policy Is Required for My Institution, What to Do?: Practical Method and Tool Enabling Efficient Management for Corporate Information Assets. In: KATUU, Shadrack (ed.). *Diverse Applications and Transferability of Maturity Models*. IG Global, pp. 61-91. ISBN 9781522570806. [Consulté le 14 octobre 2021]. Disponible à l'adresse : <https://arodes.hes-so.ch/record/3209?ln=fr>

MAKLOUF SHABOU, Basma (ed.), 2019. Strategies, methods and tools enabling records governance in a cloud environment. In: DURANTI, Luciana et ROGERS, Corinne (ed.). *Trusting records and data in the cloud* [en ligne]. London : Facet Publishing, pp. 97-116. [Consulté le 17 octobre 2021]. Disponible à l’adresse : <https://arodes.hes-so.ch/record/7958?ln=fr>

MAKHLOUF SHABOU, Basma, NOBS, Gregory, [s.d.]. Modèle de politique de gouvernance informationnelle pour les organisations : structure et contenu. In: MAUREL, Dominique, DUFOUR, Christine, ZWARICH, Natasha (éd.). *La gouvernance informationnelle dans les organisations*. Québec: Presses universitaires du Québec. En cours de publication.

MAKHLOUF SHABOU, Basma, NOBS, Gregory, NICOLET, Aurèle, 2019. *Analyse de politiques de gouvernance informationnelle : rapport de recherche* [en ligne]. 26 juin 2019. [Consulté le 14 octobre 2021]. Disponible à l'adresse : <https://arodes.hes-so.ch/record/3773?ln=fr>

MANCINI, John, 2019. *Accessible AND Secure – Best Practices for Automating Information Governance* [en ligne]. AIIM Industry Watch. [Consulté le 24 novembre 2021] Disponible à l'adresse : <https://info.aiim.org/accessible-and-secure-best-practices-for-automating-information-governance>

MARKARIAN, Josh, 2019. Information Governance in the Cloud: 9 Trends To Watch. *Teris* [en ligne]. 21 octobre 2019. [Consulté le 24 novembre 2021]. Disponible à l'adresse : <https://teris.com/information-governance-in-the-cloud-9-trends-to-watch-2/>

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE, 2012. Accessibility: indexation de ressources (métadonnées, normes et standards). *Éduscol : l'actualité du numérique* [en ligne]. 15 octobre 2012 [Consulté le 28 septembre 2021]. Disponible à l'adresse : <http://eduscol.education.fr/numerique/dossier/archives/metadata/@@document_whole>

MONASH UNIVERSITY, 2017. *Information Asset Register* [en ligne]. 14 décembre 2017. [Consulté le 6 octobre 2021]. Disponible à l'adresse : <https://adm.monash.edu/records-archives/archives/IAR/information-asset-register.xml>

MOORE, Susan, KEEN, Emma, 2018. Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. *Gartner* [en ligne]. 15 août 2018. [Consulté le 28 septembre 2021]. Disponible à l'adresse : <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>

THE NATIONAL ARCHIVES, 2017. *Identifying Information Assets and Business Requirements* [en ligne]. Février 2017. [Consulté le 14 octobre 2021]. Disponible à l'adresse : <https://www.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf>

NATIONAL ARCHIVES OF AUSTRALIA, [s.d.]a. Designing and maintaining an information asset register. *Site des archives nationales d'Australie* [en ligne]. Consulté le 4 octobre 2021]. Disponible à l'adresse : <https://www.naa.gov.au/information-management/information-governance/conducting-information-review/designing-and-maintaining-information-asset-register>

NATIONAL ARCHIVES OF AUSTRALIA, [s.d.]b. Information asset register template. *Site des archives nationales d'Australie* [en ligne]. Consulté le 4 octobre 2021]. Disponible à l'adresse : <https://www.naa.gov.au/sites/default/files/2021-06/Information-Asset-Register-template.XLSX>

OFFICE OF THE VICTORIAN INFORMATION COMMISSIONER, 2020. *Sample Information Asset Register (IAR) Template* [en ligne]. Novembre 2019. Mis à jour novembre 2020. [Consulté le 5 octobre 2021]. Disponible à l'adresse : <https://ovic.vic.gov.au/resource/sample-information-asset-register-iar-template/>

ORGANISATION INTERNATIONALE DE NORMALISATION, 2004. *Guide 2: Normalisation et activités connexes — Vocabulaire général* [en ligne]. 8e éd. Genève : ISO. [Consulté le 19 octobre 2021]. Disponible à l'adresse : <https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/fr/iso_iec_guide_2_2004.pdf>

ORGANISATION INTERNATIONALE DE NORMALISATION, 2011a. *Information et documentation — Systèmes de gestion des documents d’activité — Principes essentiels et vocabulaire*. Genève : ISO, 15 décembre 2011. ISO 30300

ORGANISATION INTERNATIONALE DE NORMALISATION, 2011b. *Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information*. 2e éd. Genève : ISO, 6 janvier 2011. ISO/IEC 27005

ORGANISATION INTERNATIONALE DE NORMALISATION, 2014. *Information et documentation - Évaluation du risque pour les processus et systèmes d'enregistrement*. Genève : ISO, 15 mars 2014. ISO/IEC 18128

ORGANISATION INTERNATIONALE DE NORMALISATION, 2015a. *Information et documentation — Système de gestion des documents d'activité — Lignes directrices de mise en œuvre*. Genève : ISO, 15 septembre 2015. ISO 30302

ORGANISATION INTERNATIONALE DE NORMALISATION, 2015b. *Technologies de l'information — Gouvernance des technologies de l'information pour l'entreprise*. 2e éd. Genève : ISO, 15 février 2015. ISO/IEC 38500

ORGANISATION INTERNATIONALE DE NORMALISATION, 2016. *Information et documentation — Gestion des documents d’activité —* *Partie 1 : Concepts et principes*. 2e éd. Genève : ISO, 15 avril 2016. ISO 15489-1

ORGANISATION INTERNATIONALE DE NORMALISATION, 2018. *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*. 5e éd. Genève : ISO, février 2018. ISO/IEC 27000

ORGANISATION INTERNATIONALE DE NORMALISATION, 2019. *Information et documentation — Systèmes de gestion des documents d'activité — Exigences*. 2e éd. Genève : ISO, février 2019. ISO 30301

ORGANISATION INTERNATIONALE DE NORMALISATION, 2022. *Information et documentation — Gouvernance de l’information — Concept et principes*. Genève : ISO, mai 2022. ISO/DIS 24143

PERREIN, Jean-Pascal, 2010. Gestion de l’information : Comment définir le terme Information ?. *3org – Points de vue sur le flux Information* [en ligne]. 29 octobre 2010. [Consulté le 28 septembre 2021]. Disponible à l’adresse :

<http://www.3org.com/news/gouvernance_de_linformation/gestion-de-linformation-comment-definir-le-terme-information/>

PERREIN, Jean-Pascal, 2011a. Définition de la gouvernance de l’information. *3org – Points de vue sur le flux Information* [en ligne]. 11 janvier 2011. [Consulté le 28 septembre 2021]. Disponible à l’adresse : <http://www.3org.com/news/gouvernance_de_linformation/definition-de-la-gouvernance-de-linformation/>

PERREIN, Jean-Pascal, 2011b. Sexy RSE, attention aux fondamentaux ! *3org – Points de vue sur le flux Information* [en ligne]. 20 juin 2011. [Consulté le 28 septembre 2021]. Disponible à l’adresse : <http://www.3org.com/news/culture_et_usages/rse-rso-nm-sexy-mais-attention-aux-fondamentaux/>

PERREIN, Jean-Pascal, 2013. Définition de la gouvernance de l’information par des mots : Extrait du livre GouvInfo “Océan bleu”. *3org – Points de vue sur le flux Information* [en ligne]. 2 avril 2013. [Consulté le 14 octobre 2021]. Disponible à l’adresse :

<http://www.3org.com/news/gouvernance_de_linformation/definition-de-la-gouvernance-de-linformation-par-des-mots-extrait-du-livre-gouvinfo-ocean-bleu/>

QUÉBEC (PROVINCE), SOUS-SECRÉTARIAT DU DIRIGEANT PRINCIPAL DE L’INFORMATION, Québec (Province), CONSEIL DU TRÉSOR, SECRÉTARIAT et DIRECTION DES COMMUNICATIONS, 2016. Guide de catégorisation de l’information. [en ligne]. [Consulté le 30 septembre 2021]. ISBN 978-2-550-71120-9. Disponible à l’adresse : <http://collections.banq.qc.ca/ark:/52327/2959773>

Révolution numérique*. Wikipédia : l'encyclopédie libre* [en ligne]. Dernière modification de la page : 11 octobre 2021 à 17:48. [Consulté le 14 octobre 2021]. Disponible à l'adresse : <https://fr.wikipedia.org/w/index.php?title=R%C3%A9volution_num%C3%A9rique&oldid=187069229>

SAFFADY, William, 2020. *Managing information risks: threats, vulnerabilities, and responses*. Lanham : Rowman & Littlefield. ISBN 978-1-5381-3548-8.

SMALWOOD, Robert, 2014a. Defining the Differences Between Information Governance, IT Governance, & Data Governance. *aiim community* [en ligne]. 18 août 2014. [Consulté le 28 septembre 2021]. Disponible à l’adresse : <http://community.aiim.org/blogs/robert-smallwood/2014/08/18/defining-the-differences-between-information-governance-it-governance--data-governance>

SMALLWOOD, Robert F., 2014b. *Information governance: concepts, strategies and best practices*. Hoboken : Wiley. Wiley CIO series. ISBN 9781118218303.

SOCIETY OF AMERICAN ARCHIVISTS, [s. d.]. Information management. *Dictionary of Archives Terminology* [en ligne]. Society of American Archivist, 2005-2021. [Consulté le 19 octobre 2021]. Disponible à l’adresse : <https://www2.archivists.org/glossary/terms/i/information-management>

TEXIER, Bruno, 2020. Service public : vers le 100 % dématérialisé. *Archimag* [en ligne]. 6 septembre 2019. Mis à jour le 13 février 2020. [Consulté le 28 septembre 2021]. Disponible à l'adresse: <https://www.archimag.com/demat-cloud/2019/09/06/service-public-dematerialise-action-publique-2022>

VISIATIV INDUSTRY, [s.d.]. La transformation numérique dans l’industrie. *visiativ-industry.ch* [en ligne]. [Consulté le 8 juin 2022]. Disponible à l'adresse: <https://www.visiativ-industry.ch/transformation-numerique-industrie/>

ZAFRIN, Waren, 2018. Why organizations need an information assets register. *Corporate compliance insights* [en ligne]. 11 avril 2018. [Consulté le 5 octobre 2021]*.* Disponible à l’adresse : <https://www.corporatecomplianceinsights.com/organizations-need-information-asset-register/>