Archives

ARCHIVES

TOELLE, E. (2021). *Microsoft 365 Compliance: A Practical Guide to Managing Risk*. Californie : Apress, 524 pages

Jean-Samuel Bisson

Volume 51, numéro 1, 2023

URI : https://id.erudit.org/iderudit/1108734ar
DOI : https://doi.org/10.7202/1108734ar

Aller au sommaire du numéro

Éditeur(s)

Association des archivistes du Québec (AAQ)

ISSN

0044-9423 (imprimé)
2369-9256 (numérique)

Découvrir la revue

Citer ce compte rendu

Bisson, J.-S. (2023). Compte rendu de [TOELLE, E. (2021). *Microsoft 365 Compliance: A Practical Guide to Managing Risk*. Californie : Apress, 524 pages]. *Archives*, *51*(1), 53–58. https://doi.org/10.7202/1108734ar

Microsoft 365 Compliance: A Practical Guide to Managing Risk. E. Toelle.

JEAN-SAMUEL BISSON > Étudiant à la maîtrise en archivistique, Université Laval
Gestionnaire de documents, Ministère de la Famille

TOELLE, E. (2021). *Microsoft 365 Compliance: A Practical Guide to Managing Risk*. Californie : Apress, 524 pages.

L'ouvrage *Microsoft 365 Compliance: A Practical Guide to Managing Risk* a été rédigé par Erica Toelle, qui occupe actuellement le poste de *Senior Product Marketing Manager* (responsable du marketing produit) chez Microsoft. Elle accompagne des entreprises dans leur déploiement d'applications Microsoft à des fins de gestion du cycle de vie de leurs données et de leurs documents. Son livre se veut un guide expliquant les différentes fonctionnalités du « Centre de conformité », la plateforme centrale de Microsoft 365 (M365) permettant à l'administrateur de configurer tous les modules ayant une incidence sur la gestion de l'information. Chaque chapitre de l'ouvrage aborde un module au sein du Centre de conformité, soit chacun des onglets de son interface.

La formule employée par l'autrice consiste à présenter globalement chaque module, puis à lister les licences Microsoft requises pour y avoir accès (les différentes licences modifient de façon très granulaire les fonctionnalités pouvant être utilisées dans M365). Toelle énumère ensuite les permissions qu'un utilisateur doit posséder à l'intérieur de M365 pour configurer le module. Elle explique enfin le fonctionnement et l'utilité du module en incluant des procédures détaillées et illustrées.

Si le premier chapitre constitue une introduction générale à la notion de conformité dans M365, les quinze chapitres suivants sont consacrés aux « solutions de conformité », c'est-à-dire les modules. Ces derniers peuvent être listés comme suit :

- le gestionnaire de conformité ;
- la classification des données ;

- les connecteurs de données ;
- la protection des données ;
- la protection contre la perte de données ;
- les obstacles aux informations ;
- la gouvernance de l'information ;
- la gestion des enregistrements ;
- la gestion du risque interne ;
- la conformité des communications ;
- la recherche de contenu ;
- l'*eDiscovery* (standard et premium) ;
- les enquêtes de données ;
- et le journal de l'audit.

Notons que comme la plateforme M365 est en constante évolution, certaines solutions présentées dans l'ouvrage, et certaines fonctionnalités qui en découlent, peuvent avoir été modifiées depuis sa parution. La documentation disponible sur le site Web officiel de Microsoft peut en revanche fournir les informations les plus à jour. À titre d'exemple, le Centre de conformité semble maintenant s'appeler *Microsoft Purview* dans la version actuelle (Microsoft, 2023). Également, les modules M365 ont tendance à se recouper entre eux. Ainsi, ils ne sont pas mutuellement exclusifs ; par exemple, comme l'explique Toelle dans son ouvrage, la classification des données peut être utilisée en combinaison avec la gestion des enregistrements, pour en retirer un maximum de valeur ajoutée en matière de gestion de l'information. On pourrait en effet configurer le module de classification des données de manière à détecter un type de renseignement (comme un numéro d'assurance sociale) ou un type de document spécifique (comme un curriculum vitæ), et ensuite aller dans le module de gestion des enregistrements pour créer une étiquette de rétention qui s'appliquerait automatiquement à ces documents, de manière à automatiser leur classification et leur destruction au moment opportun.

À travers l'ouvrage, l'autrice reconnaît la complexité de tous ces outils ; c'est pourquoi elle s'efforce de les vulgariser et de référer à des exemples de ce que les organisations qu'elle a aidées ont tendance à appliquer dans la réalité. Il s'agit surtout de grandes entreprises privées américaines.

Nous concevons souvent la gestion documentaire en tant que partie d'une archivistique intégrée (dont les objectifs en sont d'abord d'efficacité organisationnelle, mais aussi de mémoire institutionnelle). Les explications de Toelle situent toutefois la préoccupation de gestion documentaire

au sein d'une notion plus englobante, la conformité, sans trop d'égards par ailleurs aux archives définitives. Que le contenu informationnel soit conforme aux politiques internes d'une organisation, ainsi qu'au contexte réglementaire, semble la finalité des fonctionnalités de la plateforme.

D'abord, Toelle nous dévoile certains « secrets » de M365, soit la structure derrière l'interface. Elle nous informe par exemple qu'une copie de chaque message Teams (conversations privées et canaux) est stockée dans la boîte de courrier Outlook correspondante (celle de l'utilisateur, ou la boîte partagée dans le cas d'une équipe Teams). Quant aux fichiers partagés dans des conversations privées, ils sont stockés dans un dossier spécifique du OneDrive de l'utilisateur. Ceux partagés dans une équipe sont stockés dans la bibliothèque du site SharePoint relié à cette équipe. Enfin, chaque canal dans une équipe Teams possède son propre dossier au sein de la bibliothèque SharePoint de l'équipe.

Ces informations sont utiles pour cartographier le contenu circulant dans notre organisation, contenu pouvant échapper aux gestionnaires de documents confrontés à la grande autonomie documentaire accordée aux utilisateurs par M365. De plus, cela donne une piste de solution dans l'éventualité où l'on devrait archiver des éléments non traditionnels, tels que des conversations (*chats*), à des fins de preuve par exemple. Ces éléments peuvent notamment apparaître dans les résultats d'une « recherche de contenu », le module de recherche de M365 permettant à l'administrateur de consulter l'ensemble des fichiers, messages et courriels indexés dans la plateforme, quel que soit leur emplacement racine.

Dès lors, comment exploiter tout ce contenu, même si on en connaît les emplacements ? Avec le module Classification des données, M365 propose un outil de classification automatisée qui exploite l'intelligence artificielle pour détecter le contenu correspondant à des critères prescrits. On pourra ainsi créer un « classifieur » pour l'objet « contrat », et fournir au système un certain nombre d'exemples positifs (des documents qui sont effectivement des contrats) et d'exemples négatifs (des documents qui n'en sont pas) pour l'entraîner à détecter ce type de documents. Une fois le contrat détecté, le système lui appose la métadonnée appropriée (« étiquette » étant le terme privilégié). Pour cette fonctionnalité, comme pour plusieurs autres, M365 met à la disposition de l'administrateur certains modèles de classifieurs, mais permet aussi d'en créer pour ses besoins spécifiques.

De la même manière, mais à un niveau plus granulaire, ce module de classification propose aussi la fonctionnalité des « types d'informations

sensibles ». Ici, le but est de détecter des informations confidentielles contenues dans les fichiers de notre organisation. On pourra ainsi fournir un exemple de donnée confidentielle, comme un numéro de carte de crédit, pour que le système identifie lui-même ces contenus confidentiels. L'attribution d'une étiquette aide non seulement à classifier ces documents, mais aussi à en restreindre l'accès, et même à en déterminer la durée de conservation.

En effet, ces étiquettes peuvent être exploitées ensuite par le module Gestion des enregistrements. Celui-ci permet d'appliquer, de manière automatisée ou non (car on peut déléguer cette responsabilité aux utilisateurs), des étiquettes de rétention pour déterminer la durée de conservation des contenus correspondant aux critères souhaités, et possiblement à partir d'un événement précis (comme la fermeture d'un dossier). Il est aussi possible d'appliquer une politique de rétention à l'échelle d'un contenant, comme une équipe Teams ou une boîte courrier, fonctionnalité potentiellement utile puisqu'il n'est pas possible, ni souhaitable, selon l'autrice, de classifier chaque message Teams ou même chaque courriel.

L'ouvrage présente ainsi des fonctionnalités innovantes pour les réalités de la gestion de l'information moderne. À travers les chapitres, on constate à quel point Microsoft cherche à tirer profit de l'intelligence artificielle et de l'automatisation, des technologies incontournables pour les organisations actuelles devant composer avec une quantité astronomique de contenu. Le livre aborde même des fonctionnalités permettant de surveiller les communications au sein de l'organisation, pour prévenir la fuite de données par exemple, ainsi que des façons d'intégrer le contenu provenant d'applications tierces à M365.

Si l'ouvrage présente des solutions inédites, on ne peut s'empêcher de remarquer que la notion de gestion documentaire telle que nous la connaissons au Québec se traduit difficilement dans M365. Ce qui s'en rapproche le plus est probablement le module Gestion des enregistrements (appelé *Records Management* dans l'interface anglaise), introduisant entre autres la possibilité de distinguer les documents d'archives (*records*) parmi le reste de la masse informationnelle. Et bien sûr, les étiquettes de rétention peuvent s'apparenter aux délais de nos calendriers de conservation québécois.

Malgré ces éléments plus « traditionnels », l'ouvrage de Toelle montre bien que M365 préfère la notion de conformité. Plutôt que sur le document,

l'accent est mis sur les différents objets documentaires numériques plus granulaires (les données, les fichiers, les métadonnées, les messages, etc.) et sur la façon de les exploiter de manière automatisée. La notion de classification, quant à elle, semble délaisser les arborescences traditionnelles au profit d'un étiquetage pouvant être effectué de façon transversale sur des ensembles de contenus plus ou moins structurés.

Le tout est présenté sous l'angle de considérations comme la sécurité informationnelle, la catégorisation de l'information, la gestion des risques, la protection des renseignements ainsi que le respect du cadre légal. Toutes ces notions semblent s'insérer dans ce que Microsoft qualifie de « gestion de la conformité » au sein d'une organisation. Plusieurs facteurs peuvent justifier cette approche, notamment la transformation des processus organisationnels avec le numérique, mais aussi les idiosyncrasies propres aux applications de travail collaboratif, les controverses dans l'actualité concernant les fuites de données, les nouvelles lois mettant l'accent sur la protection des informations confidentielles. Sur ce dernier point, on peut imaginer le potentiel de M365 dans le contexte de la Loi 25 sur la modernisation des dispositions législatives en matière de protection des renseignements personnels (RLRQ, chapitre 25), où il devient nécessaire de catégoriser les actifs informationnels. Le module de classification des données pourrait ainsi être exploité afin d'identifier des types d'informations sensibles contenues dans les documents d'une organisation, et déterminer les mesures de protection nécessaires selon le niveau de confidentialité de ces informations.

En ce sens, s'il est sûrement possible de concevoir un système de gestion électronique des documents dans M365, le Centre de conformité propose plusieurs angles devant être exploités en complémentarité afin d'en tirer les meilleurs résultats. En d'autres termes, ils exigent de prendre un certain recul par rapport à nos préoccupations archivistiques traditionnelles. M365 étant notamment une solution populaire au sein des ministères et organismes québécois, il apparaît inévitable pour ceux-ci de concevoir, par le biais de comités multidisciplinaires, une gouvernance de l'information qui exploitera ce que Microsoft 365 peut offrir.

Jean-Samuel Bisson

BIBLIOGRAPHIE

MICROSOFT. (2023). Documentation sur la conformité Microsoft Purview. Repéré à https://learn.microsoft.com/fr-ca/microsoft-365/compliance/

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (RLRQ, chapitre 25). Repéré à https://www.canlii.org/fr/qc/legis/loisa/lq-2021-c-25/derniere/lq-2021-c-25.html