ANNEXE I : AUTRES THÈMES PRÉSENTANT UN INTÉRÊT POUR L'AUDIT INFORMATIQUE

Dans cette annexe, vous découvrirez d'autres thématiques que les auditeurs des SI pourront rencontrer dans leur travail d'audit. Parmi les sujets abordés, on retrouve :

- l'informatique et l'audit judiciaires,
- les appareils intelligents,
- la technologie sans fil 5G,
- l'exploration de données,
- le Big Data,
- l'intelligence artificielle (IA),
- l'apprentissage automatique et les algorithmes,
- l'automatisation robotisée de processus (ARP),
- la chaîne de blocs.

De nombreux sujets émergents dans le domaine des technologies de l'information peuvent devenir des thématiques susceptibles d'être auditées. Les auditeurs doivent donc se tenir au courant de l'actualité des TI afin d'être en mesure, le cas échéant, de réaliser des audits couvrant ces sujets émergents.

Même si ces domaines peuvent présenter des différences techniques ou des aspects spécifiques, il est possible de les auditer en appliquant les approches et les techniques qui sont présentées tout au long du présent manuel. Leur examen pourra nécessiter des questions d'audit complémentaires, que les auditeurs pourront formuler eux-mêmes au moment d'aborder les thématiques concernées, en fonction des objectifs de leur audit.

I. Informatique et audit judiciaires

L'informatique judiciaire englobe l'approche, les outils et les techniques permettant d'examiner des informations numériques en vue d'identifier, de préserver, de récupérer, d'analyser et de présenter des faits et des opinions concernant les informations stockées. On considère généralement qu'elle fait partie du programme de réponse aux incidents mis en place par l'organisation, dès lors qu'il est nécessaire de réaliser un travail d'analyse et d'enquête supplémentaire pour les éléments probants et les données qui permettront de comprendre un incident. L'informatique judiciaire est également appliquée dans différents domaines d'investigation, dont les cas de fraude, d'espionnage, de meurtre, de chantage, d'activité informatique frauduleuse, de détournement de technologie, de diffamation, de courrier malveillant, de fuite d'informations, de vol de propriété intellectuelle, de pornographie, d'envoi de pourriel, de piratage et de transfert illégal de fonds[1].

L'audit judiciaire est un type d'audit spécifique réalisé pour examiner des supports numériques à la recherche d'éléments probants, dans le cadre d'une enquête ou concernant un litige. Ce type d'audit fait appel à des techniques et principes similaires à ceux qui sont employés pour la récupération de données, mais obéit à des lignes directrices et pratiques complémentaires, visant à créer une piste d'audit judiciaire :

- conservation de preuves (données, accès, journaux, par exemple) pour analyse,
- capture et conservation de données au plus près possible de l'infraction,

[1] ISACA, *IT Audit and Assurance Guideline G38 Computer Forensics*.

- collecte de données répondant aux normes en vigueur, en vue de leur utilisation éventuelle par les organismes d'application de la loi,
- application de méthodes de capture de données peu invasives, sans perturbation des activités commerciales,
- identification des attaquants, si possible.

Références et lectures complémentaires

Electronic Crime Scene Investigation: A Good Practice Guide for Computer-Based Electronic Evidence.

Organisation internationale de normalisation/commission électrotechnique internationale. *ISO/IEC 27035-2:2016, Technologies de l'information — Techniques de sécurité — Gestion des incidents de sécurité de l'information.* Genève, Suisse. Organisation internationale de normalisation, 11 novembre 2016.

National Institute of Justice. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* http://www.ncjrs.gov/pdffiles1/nij/199408.pdf. Avril 2004.

Wikipedia. « Computer Forensics. » http://en.wikipedia.org/wiki/Computer_forensics.

II. Appareils intelligents

Les appareils intelligents, comme les smartphones, tablettes et autres objets connectés relevant de l'Internet des objets[2], tendent à modifier la façon dont les systèmes d'information sont utilisés. Ces appareils fournissent une puissance de calcul mobile et la possibilité de se connecter à l'Internet dans toute zone couverte par un réseau Wi-Fi ou de téléphonie mobile. Il existe de nombreux types d'appareils intelligents différents, mais tous présentent certaines caractéristiques communes : système d'exploitation, connexion à un réseau vocal et de données, stockage de données, système de localisation GPS, entre autres[3].

Les appareils intelligents peuvent également fournir des solutions pratiques pour le travail à distance. Longtemps, le travail à distance a consisté pour les collaborateurs à se connecter au réseau de l'organisation, au moyen d'un ordinateur portable fourni par leur employeur. Les appareils intelligents ont toutefois permis d'élargir l'étendue des applications et fonctionnalités disponibles pour télétravailler.

La connexion d'appareils intelligents au réseau de l'organisation s'accompagne cependant de nouveaux risques également. Le recours aux appareils intelligents doit être pris en compte au moment d'évaluer le positionnement de l'organisation en matière de sécurité. Les risques liés aux appareils intelligents concernent notamment la conformité, la confidentialité, la sécurité physique et la sécurité de l'information. Dans ces différents domaines, les risques concernent plus précisément les différences de versions matérielles ou logicielles qui sont utilisées, la consultation ou la suppression sans autorisation d'informations identifiables à caractère personnel, ainsi que le risque de perte ou de vol de l'appareil, entre autres. Afin d'atténuer l'impact de ces risques, les organisations peuvent déployer des contrôles de sécurité

[2] Technologies et appareils qui recueillent des informations et sont capables de les communiquer sur l'Internet ou d'autres réseaux.

[3] Global Technology Audit Guide, *Auditing Smart Devices*, https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Auditing-Smart-Devices-An-Internal-Auditors-Guide-to-Understanding-and-Auditing-Smart-Devices.aspx.

et des politiques de sécurité : contrôles d'authentification, gestion des possibilités d'effacement à distance, chiffrement matériel, chiffrement logiciel, sauvegarde de données, gestion du parc d'appareils de l'organisation, par exemple.

Pour évaluer les risques et apprécier les contrôles associés aux appareils intelligents, l'auditeur doit notamment :

- comprendre la stratégie de l'organisation en matière d'appareils intelligents,
- évaluer l'effet des appareils intelligents sur l'architecture technologique globale de l'organisation,
- identifier et évaluer les risques introduits par les appareils intelligents,
- déterminer dans quelle mesure la gouvernance et les contrôles de gestion du risque sont adaptés aux appareils intelligents utilisés.

Références et lectures complémentaires

Global Technology Audit Guide. *Auditing Smart Devices*. https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Auditing-Smart-Devices-An-Internal-Auditors-Guide-to-Understanding-and-Auditing-Smart-Devices.aspx.

ISACA. *Mobile Computing Security Audit Program.* https://www.isaca.org/bookstore/audit-control-and-security-essentials/wapmcs. 2010.

Salman, Seyed. « Auditing the Internet of Things. » *Internal Auditor Magazine*. 29 octobre 2015.

U.S. Government Accountability Office. *Internet of Things: Status and Implications of an Increasingly Connected World.* GAO-17-75. https://www.gao.gov/products/gao-17-75. 15 mai 2017.

III. Technologie sans fil 5G

La 5G (pour cinquième génération) correspond à un ensemble de technologies sans fil capables d'assurer des connexions plus fiables et plus efficaces sur les réseaux sans fil. La technologie sans fil 5G promet d'améliorer considérablement la performance et les capacités des réseaux, comme la vitesse et le débit, pour permettre la connexion d'un plus grand nombre d'appareils. D'après les études réalisées sur les avantages socio-économiques de la 5G, la technologie devrait faciliter l'accessibilité et la disponibilité de solutions de pointe en matière de santé et d'éducation, réduire la pollution, renforcer l'efficacité des transports et la réactivité des services publics de sécurité. On s'attend à ce que la performance des réseaux 5G soit nettement supérieure à celle de la précédente génération, à mesure que la technologie progressera sur les dix prochaines années. Ce gain de performance devrait faciliter le développement des applications mobiles large bande actuelles, et l'apparition de nouvelles applications disruptives en milieu professionnel comme dans la société.

La 5G apporte notamment les avancées technologiques suivantes :

- **Amélioration des applications à large bande.** Des connexions plus rapides et un débit plus élevé pourraient améliorer des applications telles que les services en nuage, la diffusion de vidéos en continu, les jeux en ligne et la réalité augmentée.
- **Internet des objets**. La 5G devrait permettre la connexion d'une multitude d'appareils, tels que des capteurs intégrés aux systèmes de transport et de logistique intelligents, aux usines intelligentes et même aux villes intelligentes. Par exemple, les capteurs intégrés aux feux de circulation et aux routes pourraient contribuer à réduire le nombre d'accidents.
- **Communications critiques pour la mission.** Des communications exceptionnellement fiables, à faible latence, pourraient sécuriser la circulation des véhicules à conduite autonome, fiabiliser les équipements industriels, la robotique et les drones.

Si la 5G apporte de nouvelles possibilités dans de nombreux secteurs, cette évolution soulève toutefois des préoccupations concernant les risques pour la cybersécurité et d'autres défis à relever. Par exemple :

- **Déploiement des infrastructures**. Les applications nécessitant une faible latence et une largeur de bande importante exigent des infrastructures considérables, notamment câbles de fibre optique et petites cellules. Le déploiement de cette infrastructure pourrait se révéler coûteux et nécessiter une main-d'œuvre qualifiée. Le temps nécessaire à l'obtention des permis locaux, à la planification et aux approvisionnements pourrait également être une contrainte.
- **Cybersécurité**. Constitué de nombreux composants, le réseau 5G présente un risque plus élevé que certains composants ne soient pas correctement configurés et sécurisés.
- **Confidentialité**. Les réseaux 5G pourraient permettre d'obtenir des données de localisation beaucoup plus précises. En effet, les appareils 5G devraient se connecter à des cellules situées beaucoup plus près les unes des autres. Ces données de localisation plus précises pourraient augmenter le risque d'atteinte à la vie privée des utilisateurs.

Références et lectures complémentaires

Fraunhofer Institute for Production Technology IPT. *5G-Audit.* https://www.ipt.fraunhofer.de/en/Competencies/Productionqualityandmetrology/Productionmetrology/5g-audit.html.

ISACA. *ISACA Outlines Risks and Benefits of 5G Technology.* https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2021/isaca-outlines-risks-and-benefits-of-5g-technology. 9 février 2021.

U.S. Government Accountability Office. *Science & Tech Spotlight : 5G Wireless.* GAO-20-412SP. https://www.gao.gov/products/gao-20-412sp. 27 mars 2020.

U.S. Government Accountability Office. *5G Wireless: Capabilities and Challenges for an Evolving Network.* GAO-21-26SP. https://www.gao.gov/products/gao-21-26sp. 24 novembre 2020.

IV. Exploration de données

L'exploration de données désigne un processus de recherche et d'analyse permettant de trouver des corrélations cachées ou des informations nouvelles à partir d'un large ensemble de données. Les techniques d'exploration de données ont connu un développement rapide, bénéficiant des avancées réalisées dans d'autres domaines connexes, notamment le stockage de données et le Big Data. Grâce à l'exploration de données, les organisations peuvent transformer des données brutes en connaissances utiles, et identifier des tendances ou des anomalies. L'exploration de données peut améliorer la prise de décision dans l'organisation, en apportant des éclairages pertinents pour l'analyse, comme la description de l'ensemble de données cibles ou la prédiction des résultats grâce à l'utilisation d'algorithmes d'apprentissage automatique.

Le processus comprend généralement quatre grandes étapes : définition des objectifs, collecte et préparation des données, application des algorithmes d'exploration de données, évaluation des résultats.

- **Définition des objectifs.** Les parties prenantes doivent travailler ensemble pour identifier le problème à régler, ce qui permet de déterminer les questions auxquelles il faut répondre en ce qui concerne les données.
- **Préparation des données.** Quand on a défini le périmètre, on peut commencer à recueillir des données et à les nettoyer afin d'obtenir les meilleurs résultats possible.
- **Algorithmes d'exploration.** L'analyse des données permet d'identifier des relations, des modèles et des corrélations. On peut également appliquer des algorithmes pour classer les données selon qu'elles ont été préalablement étiquetées ou non.

- **Évaluation.** Une fois les données analysées, on peut évaluer et interpréter les résultats. Les organisations peuvent ainsi utiliser les connaissances acquises pour atteindre les objectifs prévus.

Les progrès réalisés dernièrement dans le domaine de l'apprentissage automatique ont permis d'étendre l'exploration de données à l'analyse textuelle. Cette évolution est importante, si l'on considère que près de 90 % des informations ne sont pas structurées dans des formats du type document, e-mail, réseaux sociaux et autres fichiers. L'analyse de ces données à l'aide de techniques d'exploration de données n'est pas possible, cette technique exigeant des données structurées. L'exploration de texte fait ainsi appel à des techniques statistiques, linguistiques et à l'apprentissage automatique, qui permettent d'analyser des informations non structurées. Comme en matière d'exploration de données, de nouvelles méthodes d'exploration de texte sont actuellement en développement, et aideront les auditeurs à traiter le langage naturel. Ils auront grand besoin de ces outils pour évaluer des quantités toujours plus importantes d'informations électroniques.

Références et lectures complémentaires

IBM. *Data Mining*, https://www.ibm.com/cloud/learn/data-mining. 15 janvier 2021.

Scholtes, Jan. *Text Mining and eDiscovery for Big Data Audits*. https://medium.com/ecajournal/text-mining-and-ediscovery-for-big-data-audits-82a1592cac91. 6 mars 2020.

V. Big Data

Le Big Data désigne de grands ensembles de données complexes, traités en grand volume et qui sont souvent gérés sous forme de données non structurées ou semi-structurées. Ces énormes volumes de données peuvent être utilisés pour résoudre des problèmes impossibles à résoudre auparavant. Voici certaines des activités que le Big Data peut contribuer à optimiser :

- **Développement de produit.** Les modèles prédictifs peuvent aider les organisations à anticiper la demande du client, et à formuler des suggestions de produits.
- **Maintenance prédictive.** Le Big Data peut faciliter la prédiction des défaillances mécaniques, grâce à l'analyse des entrées des journaux et des données des capteurs, et ainsi contribuer à l'optimisation de la maintenance au sein des organisations.
- **Fraude et conformité**. Le Big Data peut aider les organisations à identifier dans les données des tendances pouvant indiquer des cas de fraude ou d'autres activités malveillantes.
- **Expérience client**. Le big data permet aux organisations de recueillir des données issues des réseaux sociaux, des visites d'un site Web, des journaux d'appel, et d'autres sources afin de personnaliser l'expérience client.
- **Apprentissage automatique.** Le Big Data a créé les conditions permettant l'entraînement et l'apprentissage des machines, plutôt que leur programmation.

Le volume important du Big Data nécessite une solution de stockage garantissant à la fois accessibilité et sécurité. Le Big Data implique de pouvoir traiter des données non structurées, issues notamment des flux des réseaux sociaux, des capteurs intégrés aux machines, ou de l'optimisation des équipements mécaniques. Les organisations ont souvent recours à des prestataires de services externalisés pour se doter de la puissance de calcul et de l'espace de stockage nécessaires à l'analyse du Big Data.

Parmi les risques associés au Big Data, citons la faible qualité des données, l'incompatibilité des technologies, une sécurité insuffisante, un manque de maturité des pratiques de gouvernance des données. L'auditeur doit mobiliser le directeur des systèmes d'information et d'autres responsables de l'organisation, pour les amener à mieux comprendre les risques du Big Data en matière de collecte de données, de stockage, d'analyse, de sécurité et de confidentialité.

Pour évaluer les outils et les techniques associés au Big Data, l'auditeur doit envisager les aspects suivants :

- **Stockage**. Comment l'organisation gère-t-elle le stockage d'un volume toujours plus important de données, et comment les solutions de stockage actuelles permettent-elles d'intégrer de nouvelles sources de données ?
- **Sur site ou en nuage**. L'organisation gère-t-elle l'environnement du Big Data sur site ou en l'externalisant à des prestataires d'informatique en nuage ?
- **Outils de découverte de données.** Quel est le niveau de maturité de l'organisation en ce qui concerne la compréhension des données, l'acquisition des données et l'apprentissage exploitant ces données ?
- **Outils de surveillance**. Quels sont les indicateurs clés de performance mis en place par l'organisation pour suivre l'efficacité et la performance des systèmes du Big Data ?
- **Acquisition de logiciels**. Il faudra nécessairement comprendre les différences entre les systèmes du Big Data et les systèmes traditionnels pour être en mesure de sélectionner les logiciels qui conviennent.

Références et lectures complémentaires

Colombo, Pierro, and Elena Ferrari. « Access Control Technologies for Big Data Management Systems: Literature Review and Future Trends. » *Cybersecurity*, Vol. 2, n° 3 https://doi.org/10.1186/s42400-018-0020-9. 2019.

Global Technology Audit Guide. *Understanding and Auditing Big Data.* https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Understanding-and-Auditing-Big-Data.aspx.

Murphy, Maria L. and Journal of Accountancy, « How to Prepare for Auditing in a Digital World of Big Data. » *Journal of Accountancy*. https://www.journalofaccountancy.com/news/2014/oct/201411104.html. 16 octobre 2014.

Oracle. *Qu'est-ce que le Big Data ?* https://www.oracle.com/fr/big-data/what-is-big-data/.

Salijeni, George, Anna Samsonova-Taddie, and Stuart Turley. « Understanding How Big Data Technologies Reconfigure the Nature and Organization of Financial Statement Audits: A Sociomaterial Analysis. » *European Accounting Review, vol. 30, n°3.* https://www.tandfonline.com/doi/full/10.1080/09638180.2021.1882320. 2021.

VI. Intelligence artificielle

L'intelligence artificielle (IA) est une technologie transformatrice dont on retrouve les applications dans le domaine médical, agricole, industriel, les transports, la défense et d'autres domaines encore. L'intelligence industrielle s'est construite sur l'idée que l'on pouvait utiliser les machines pour stimuler l'intelligence humaine. La conceptualisation de l'IA a connu trois grandes vagues de développement. La première vague, correspondant aux débuts de l'IA, comprend les systèmes experts ou fondés sur des règles, dans lesquels on programme un ordinateur sur la base de connaissances expertes ou de critères. La deuxième vague des systèmes d'IA correspond à l'apprentissage statistique ou automatique à partir de données, permettant de déduire des règles ou des procédures décisionnelles prédisant de façon précise des résultats spécifiques. La troisième vague de développement de l'IA reprend les deux premières vagues, en ajoutant des capacités de complexité contextuelle, d'abstraction et d'explication.

L'IA ouvre d'importantes perspectives d'amélioration des conditions de vie et de renforcement de la compétitivité économique, par différents aspects. Voici quelques exemples de domaines dans lesquels l'application de l'IA pourrait avoir des conséquences majeures :

- **Cybersécurité**. Les systèmes automatisés et les algorithmes avancés peuvent contribuer à réduire le temps et le travail nécessaires pour identifier les vulnérabilités, les corriger, détecter les attaques et se défendre contre les attaques en cours.
- **Véhicules automatisés**. Les constructeurs automobiles et les sociétés de technologies intègrent des outils fondés sur l'IA pour évaluer une situation, concevoir un plan et exécuter des décisions permettant le contrôle des véhicules.
- **Justice pénale**. Les algorithmes automatisent certaines parties du travail d'analyse, et apportent des données éclairant les décisions humaines.
- **Services financiers.** Les outils fondés sur l'IA peuvent contribuer à optimiser les activités du service client, la gestion de patrimoine, le profilage des risques grand public, ainsi que les contrôles internes.

Si l'IA peut présenter de nombreux avantages dans bien des secteurs d'activité, elle apporte également de nouveaux risques ; elle pourrait remplacer des emplois humains et creuser les inégalités socio-économiques. L'adoption de l'IA pose notamment des difficultés dans les domaines suivants :

- recueillir et partager les données fiables et de qualité nécessaires à l'entraînement de l'IA ;
- accéder à des ressources informatiques adaptées et disposer d'une main-d'œuvre possédant les connaissances, les compétences et la formation nécessaires pour utiliser ces ressources ;
- s'assurer que la législation et la réglementation encadrant les systèmes rendus possibles par l'IA sont adaptées, et que l'application de l'IA ne porte pas atteinte aux libertés civiles ;
- concevoir un cadre déontologique de l'utilisation de l'IA et s'assurer que les actions et les décisions des systèmes d'IA peuvent être expliquées de manière adéquate et qu'elles sont acceptées par ceux qui interagissent avec ces systèmes.

Lorsqu'ils évaluent l'utilisation de l'IA par les organisations du secteur public et d'autres entités, les auditeurs devraient envisager d'évaluer les pratiques clés dans des domaines tels que la gouvernance, les données, la performance et la surveillance. Voici quelques exemples de procédures auditables dans ces domaines, à l'échelle de l'organisation :

- **Gouvernance.** Les organisations doivent définir clairement les objectifs, les rôles et les responsabilités associés aux activités, faire la preuve de leurs valeurs et principes pour inciter à la confiance, constituer une main-d'œuvre qualifiée, mobiliser des parties prenantes aux points de vue différents pour atténuer les risques, et mettre en œuvre un plan de gestion des risques spécifiques à l'IA.
- **Données.** Les organisations doivent documenter la source et l'origine des données pour assurer la fiabilité des données, et évaluer la pertinence des attributs des données, variables et augmentations/améliorations.
- **Performance**. Les organisations doivent cataloguer les composants modélisés et non modélisés qui constituent le système d'IA, définir des métriques et évaluer performance et résultats pour chaque composant.
- **Surveillance**. Les organisations doivent élaborer des plans de surveillance continue du système d'IA et documenter les résultats et les mesures correctrices prises pour garantir que le système produit les résultats souhaités.

Références et lectures complémentaires

Raji, Inioluwa Deborah, and Andrew Smart, Rebecca N. White, Margaret Mitchell, Timnit Gebru, Ben Hutchinson, Jamila Smith-Loud, Daniel Theron, and Parker Barnes. « Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing. » Présenté à l'occasion de la série de *Conférence sur l'équité, la responsabilité et la transparence* à Barcelone, Espagne, en 2020. https://arxiv.org/abs/2001.00973. 28 janvier 2020.

UK Information Commissioner's Office. *Big data, Artificial Intelligence, Machine Learning and Data Protection*. Version : 2.2. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. 4 septembre 2017.

U.S. Government Accountability Office. *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*. GAO-21-519SP. https://www.gao.gov/products/gao-21-519sp. Juin 2021.

U.S. Government Accountability Office. *Artificial Intelligence: Emerging Opportunities, Challenges, and Implications*. GAO-18-142SP. https://www.gao.gov/products/gao-18-142sp. 28 mars 2018.

VII. Apprentissage automatique et algorithmes

En informatique, l'apprentissage automatique désigne des méthodes permettant de développer des modèles à partir d'intrants de données, afin de générer des prédictions concernant des données. L'apprentissage automatique utilise des algorithmes programmés pour prédire les valeurs de sortie dans une fourchette acceptable. Ces algorithmes apprennent et optimisent leurs performances à mesure qu'ils reçoivent de nouvelles données. Un algorithme est un ensemble de règles et d'instructions qu'un ordinateur applique automatiquement lorsqu'il effectue des calculs pour résoudre un problème ou répondre à une question. Les algorithmes peuvent se présenter sous de nombreuses formes, dont les modèles de calcul, arbres de décision et autres modèles de données complexes et applications d'autoapprentissage.

On a généralement l'impression que les algorithmes deviennent de plus en plus intelligents. En effet, avec l'augmentation du volume des données et l'évolution technique des matériels disponibles, les algorithmes sont capables de traiter une plus grande quantité de données, plus rapidement. Les algorithmes deviennent donc plus innovants, et couvrent un plus large spectre d'applications. Ils peuvent appuyer et améliorer la gestion opérationnelle et les prestations de services des organisations. Ils servent aussi à rendre plus performants les processus qui utilisent des données complexes. Les algorithmes font des prédictions ou analysent des données, que les experts utilisent ensuite dans leur travail.

L'utilisation d'algorithmes peut toutefois présenter différents risques pour les organisations. Par exemple :

- il est possible que le public ne perçoive pas clairement l'impact de l'algorithme,
- l'algorithme ou l'ensemble de données utilisé par l'algorithme peut contenir des biais,
- le programmeur ou le scientifique des données peut manquer de connaissances spécifiques ou de contexte précis pour permettre à l'algorithme de prendre des décisions éclairées,
- l'algorithme peut enclencher un processus d'apprentissage non souhaité,
- il est possible que les détails sous-jacents de l'algorithme ne soient connus que du prestataire.

L'audit de l'apprentissage automatique peut inclure les composants de l'infrastructure informatique qui utilisent des algorithmes d'apprentissage automatique. L'audit doit toujours comporter une évaluation des risques des systèmes informatiques connexes ; en effet, on n'utilise habituellement pas les algorithmes comme des logiciels autonomes. Pour procéder à l'évaluation ou à l'analyse des algorithmes, l'auditeur doit considérer les aspects suivants :

- **Gouvernance et responsabilité.** Cet aspect comprend les rôles, les responsabilités, l'expertise, la gestion du cycle de vie de l'algorithme, les facteurs de risque associés à l'utilisation de l'algorithme, ainsi que les accords conclus avec les parties prenantes externes. L'évaluation de la gouvernance et de la responsabilité peut s'appuyer sur les modèles de gouvernance des technologies de l'information décrits dans le référentiel COBIT[4].
- **Modèle et données.** Cet aspect concerne la qualité des données, ainsi que la création, l'utilisation et le suivi du modèle sous-jacent de l'algorithme. Il peut également comprendre des questions concernant les données et les biais éventuels inhérents aux données, la minimisation des données et les tests effectués sur le modèle.

[4] COBIT est un référentiel de contrôle de la gouvernance des technologies de l'information, conçu pour répondre à la nécessité d'évaluer les risques liés à l'information et à l'informatique.

- **Confidentialité.** Les algorithmes peuvent utiliser des données à caractère personnel. Ils doivent alors être conformes à la réglementation encadrant le traitement de ce type de données.
- **Contrôles informatiques généraux.** Il s'agit des contrôles informatiques classiques, tels que droits d'accès, gestion de la continuité et gestion des changements.

Références et lectures complémentaires

ISACA. *COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT*. 2012.

Netherlands Court of Audit. *Understanding Algorithms*. https://english.rekenkamer.nl/publications/reports/2021/01/26/understanding-algorithms. 2021.

Institutions supérieures de contrôle des finances publiques de Finlande, des Pays-Bas, de Norvège et du Royaume-Uni. *Auditing Machine Learning Algorithms*. https://www.auditingalgorithms.net/. 24 novembre 2020.

VIII. Automatisation robotisée de processus (ARP)

L'automatisation robotisée de processus (ARP) désigne l'automatisation des opérations de routine de l'organisation, selon une logique commerciale et avec des intrants structurés. L'ARP comprend le traitement de transactions, le déclenchement de réponses et la communication avec d'autres systèmes numériques. Les opérations sont souvent des fonctions telles que copier-coller, moissonnage du Web, réalisation de calculs, ouverture et déplacement de fichiers, analyse d'e-mails et extraction de données.

Mise en œuvre de manière efficace, l'ARP peut aider les organisations à réduire leurs frais de personnel et à limiter les erreurs humaines. Elle peut aussi améliorer certains indicateurs commerciaux, comme la satisfaction des clients, et libérer du temps de travail que le personnel peut consacrer à la résolution de problèmes, à des analyses et autres travaux à valeur ajoutée. L'ARP est généralement peu coûteuse à mettre en œuvre et il est rare qu'elle nécessite l'intégration d'un logiciel sur mesure. Les organisations peuvent parfois recourir à l'apprentissage automatique ou à d'autres technologies de l'intelligence artificielle pour optimiser leur ARP.

L'ARP, comme toute technologie d'automatisation, est susceptible de détruire des emplois, ce qui peut poser des problèmes de gestion des ressources humaines dans les organisations. Par rapport aux applications informatiques types, l'ARP peut aussi augmenter l'exposition aux risques. Certains aspects doivent ainsi être pris en compte à la mise en œuvre de l'ARP, comme la modification des rôles professionnels, la sécurité des accès, la gestion des changements d'application et la gouvernance de l'environnement ARP, par exemple. L'automatisation d'un processus métier peut introduire des changements dans les exigences de contrôle des processus. L'audit des environnements automatisés, qui détermine si les processus permettent effectivement d'obtenir les résultats souhaités, est donc incontournable pour l'auditeur.

Cet audit comprend l'examen de différentes phases du processus d'ARP, et pour chacune d'entre elles, l'évaluation de certaines étapes en particulier :

- **Planification**. À ce stade, afin d'obtenir une vision claire des domaines dans lesquels l'ARP est déployée, l'auditeur définit le niveau d'automatisation, analyse les flux de travail et détermine quels autres systèmes intégrés doivent être inclus.
- **Revue.** Après que l'auditeur a identifié les automatisations présentes dans un environnement, il lui faut tester les risques associés à chaque étape automatisée du processus. La revue de code est particulièrement utile pour identifier les risques, comprendre les contrôles et les systèmes associés à l'automatisation.
- **Conception.** Il faut considérer l'automatisation comme un élément des technologies de l'information. L'auditeur doit donc inclure les automatisations les plus pertinentes dans le périmètre de la conception.

Par exemple, toute automatisation déclenchant la production de rapports ou d'autres résultats exploités aux fins de la gestion. L'auditeur doit aussi évaluer dans quelle mesure les contrôles appliqués permettent d'atténuer et d'éliminer les risques associés à chaque automatisation du processus.

- **Rapports**. Si l'automatisation est utilisée pour créer des rapports, l'auditeur doit évaluer le caractère complet et exact des rapports en évaluant le code, la logique et les paramètres utilisés pour générer ces rapports.

Références et lectures complémentaires

Automation Anywhere. *What is Robotic Process Automation (RPA)?* https://www.automationanywhere.com/rpa/robotic-process-automation.

Boulton, Clint. *What is RPA? A Revolution in Business Process Automation.* https://www.cio.com/article/3236451/what-is-rpa-robotic-process-automation-explained.html.

Deloitte. *Auditing the RPA environment, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-auditing-the-rpa-environment-noexp.pdf*. Mars 2018.

IX. Chaîne de blocs

Une chaîne de blocs est un registre partagé, qui autorise des transactions en temps réel sur des actifs numériques. Plus précisément, une chaîne de blocs est un registre d'événements numériques organisés en blocs chronologiques, qui sont chiffrés puis distribués à de nombreuses entités différentes. La mise à jour des blocs est possible uniquement lorsqu'une majorité d'entités valident la transaction. La chaîne de blocs utilise un cadre pair à pair dans lequel chaque nœud de la chaîne possède une copie identique des données, un mécanisme de consensus synchronisant les données entre les nœuds. On obtient ainsi une mise à jour en temps réel des données, sans qu'il soit nécessaire de faire valider les transactions par une autorité centrale ou un tiers. Les transactions peuvent être écrites une fois seulement sur la chaîne de blocs, aucune annulation n'est possible. Les technologies associées à la chaîne de blocs ont notamment pour attributs fondamentaux le fait d'être :

- **Décentralisées**. La chaîne de blocs est opérationnelle indépendamment de tout intermédiaire ou de toute autorité, ce qui lui permet de fonctionner selon le principe du pair-à-pair.
- **Partagées.** Le registre de la chaîne de blocs est partagé et dupliqué sur tous les nœuds du réseau.
- **Traçables.** Chaque entrée sur la chaîne de blocs est liée à la transaction précédente, de sorte qu'il se forme une piste d'audit complète et traçable, un registre des transactions sous-jacentes.
- **Validées.** Les transactions sont validées par les nœuds participants, en référence au mécanisme de consensus, avant d'être ajoutées à la chaîne de blocs.
- **Immuables.** Les transactions de la chaîne de blocs sont immuables, ce qui signifie qu'une fois qu'elles ont été validées, il n'est plus possible de les remplacer, de les annuler ou de les modifier.
- **Vérifiables**. Les transactions de la chaîne de blocs sont transmises à tous les nœuds du réseau, chaque nœud pouvant vérifier l'historique des transactions.

Si la chaîne de blocs ouvre des possibilités, comme celles qui sont mentionnées ci-dessus, la mise en œuvre de ces technologies peut poser différents problèmes :

- **Embranchements divergents.** Au niveau de ces embranchements, deux branches divergentes de la chaîne de blocs ont été créées. Cet événement se produit habituellement lorsqu'il existe un désaccord entre les nœuds concernant les règles régissant la chaîne de blocs.
- **Double dépense.** Ce problème concerne principalement les cryptomonnaies, lorsqu'un actif peut être transféré à des entités multiples.

- **Attaque des 51 %.** Ce problème peut se poser lorsqu'une entité contrôle la majorité du réseau, ce qui lui donne la possibilité d'agir de manière malveillante.
- **Mauvaises performances**. Les mécanismes de consensus opèrent souvent un compromis entre rapidité (performance) et fiabilité des transactions.

La fiabilité des données est un élément important à considérer dans l'audit des technologies de chaîne de blocs. Plus précisément, les auditeurs doivent savoir si la chaîne de blocs peut être manipulée ou modifiée. L'algorithme de consensus utilisé par certaines chaînes de blocs peut être manipulé, si bien qu'il est possible que des transactions soient ajoutées à la chaîne de blocs sans avoir été dûment autorisées. La confidentialité doit également être prise en compte dans l'audit des chaînes de blocs. Par exemple, le stockage des données d'identifiants numériques sur la chaîne de blocs peut entraîner la divulgation ultérieure d'informations à caractère personnel, en cas de défaillance du chiffrement.

Références et lectures complémentaires

Deloitte. *An Internal Auditor's Guide to Blockchain: Blurring the Line between Physical and Digital*. https://www2.deloitte.com/us/en/pages/risk/articles/internal-auditing-guide-to-blockchain.html. 2019.

KPMG. *Auditing Blockchain Solutions.* https://assets.kpmg/content/dam/kpmg/in/pdf/2018/10/Auditing_Blockchain_Solutions.pdf. Octobre 2018.

RSM US. *How Blockchain Technology Will Affect the Audit.* https://rsmus.com/what-we-do/services/assurance/how-blockchain-technology-will-affect-the-audit.html. 13 novembre 2019.

U.S. Government Accountability Office. *Blockchain : Emerging Technology Offers Benefits for Some Applications but Faces Challenges.* GAO-22-104625. *https://www.gao.gov/products/gao-22-104625.* 23 mars 2022.