INTOSAI
DEVELOPMENT INITIATIVE

INTOSAI
Working Group on IT Audit

MANUEL SUR L'AUDIT INFORMATIQUE PRÉPARÉ PAR LE

WGITA ET L'IDI À L'INTENTION DES INSTITUTIONS SUPÉRIEURES DE CONTRÔLE DES FINANCES PUBLIQUES

(RÉVISION 2022)

MANUEL SUR L'AUDIT INFORMATIQUE PRÉPARÉ PAR LE WGITA ET L'IDI

À L'INTENTION DES INSTITUTIONS SUPÉRIEURES DE CONTRÔLE DES FINANCES PUBLIQUES

(RÉVISION 2022)

DECLARATION SUR L'ASSURANCE QUALITE CONCERNANT LE MANUEL SUR L'AUDIT INFORMATIQUE PRÉPARÉ PAR LE WGITA ET L'IDI À L'INTENTION DES INSTITUTIONS SUPÉRIEURES DE CONTRÔLE DES FINANCES PUBLIQUES (RÉVISION DE 2022), VERSION 1 (19 DECEMBRE 2022)

Le document réalisé conjointement par les présidents d'objectifs de l'INTOSAI et l'IDI intitulé « *Quality assuring INTOSAI public goods that are developed and published outside due process* » (Assurance qualité des biens publics mondiaux de l'INTOSAI développés et publiés en dehors des procédures régulières, non traduit) distingue trois niveaux d'assurance qualité :

Assurance qualité des biens publics mondiaux de l'INTOSAI développés et publiés en dehors des procédures régulières - Niveaux d'assurance qualité

Niveau 1 : Produits ayant été soumis à des processus d'assurance qualité équivalents aux procédures régulières de l'INTOSAI, comportant notamment une période étendue de présentation au public (90 jours)

Niveau 2 : Produits ayant été soumis à des processus d'assurance qualité plus limités, impliquant des parties prenantes extérieures à l'organisation ou au groupe de travail responsable du développement initial des produits. Ces processus d'assurance qualité peuvent comporter, par exemple, une phase pilote, une phase de test et une phase d'invitation des parties prenantes clés à faire part de leurs remarques, sans pour autant aller jusqu'à une présentation au public pendant une période étendue de 90 jours

Niveau 3 : Produits ayant été soumis à des mesures de contrôle qualité rigoureuses au sein de l'organisation ou du groupe de travail responsable de son développement.

Tous les biens publics mondiaux (BPM) ne nécessitent pas forcément le même niveau d'assurance qualité. Ce BPM a été développé conformément au niveau 2 d'assurance qualité

Protocole d'assurance qualité : Version 2.0

Le Protocole d'assurance qualité (AQ) des Biens publics mondiaux (BPM) de l'IDI définit les mesures visant à garantir la qualité, en fonction des trois niveaux d'assurance qualité présentés ci-dessus. Ces mesures comprennent, pour le niveau 2 : l'approbation du Conseil de l'IDI concernant la création du BPM ; la formation d'une équipe compétente de développement de produits ; un examen par des experts externes à l'équipe de développement ; la modification du document basée sur cet examen ; la relecture, l'édition et la traduction du document par des personnes compétentes ; sa présentation aux parties prenantes ; les approbations requises concernant la Version 1 du BPM.

Mises à jour du BPM

Pour s'assurer que ce BPM reste pertinent, l'IDI et le groupe de travail de l'INTOSAI sur l'audit informatique (WGITA) entreprendront tous les deux ans une légère révision du manuel. Si des modifications substantielles doivent être apportés, l'IDI et le WGITA pourront décider de travailler sur une version révisée du manuel. Cette décision sera prise à l'occasion de la revue bisannuelle. Les révisions majeures suivront le Protocole d'assurance qualité de l'IDI. Les révisions légères ne seront normalement pas soumises à ce Protocole.

Ce BPM relève du groupe chargé de l'axe de travail « Des ISC pertinentes » de l'IDI et du groupe de travail WGITA, qui sont conjointement responsable de la maintenance de ce BPM.

Processus d'examen d'assurance qualité

Shourjo Chatterjee (Unité de soutien stratégique, IDI) a entrepris un examen AQ du processus suivi pour l'élaboration du présent BPM, en appliquant la Version 2.0 du protocole AQ. L'examinateur AQ connaît le protocole d'AQ de l'IDI concernant l'AQ des BPM et n'a pas participé à l'élaboration du BPM. Ce processus d'examen AQ est conçu pour fournir à toutes les parties prenantes l'assurance que l'IDI a appliqué les mesures de contrôle de qualité énoncées ci-dessus, conçues pour répondre au niveau 2 d'assurance qualité.

Résultats de l'examen d'assurance qualité

L'examen de l'assurance qualité du processus suivi lors de l'élaboration du présent BPM a permis de conclure que le Protocole a été suivi à tous les égards nécessaires pour le niveau 2 d'assurance qualité.

Conclusion

À l'issue de l'examen d'assurance qualité, l'IDI et le WGITA assurent aux utilisateurs de ce Bien public mondial (BPM) que ce document a été soumis à un processus d'assurance qualité correspondant à la Procédure régulière du Cadre des déclarations professionnelles de l'INTOSAI (IFPP).

E.J Gørrissen
Einar Gørrissen (Feb 22, 2023 10:45 GMT+1)

Einar Gørrissen
Directeur général
Initiative de développement de l'INTOSAI

Girish Chandra Murmu
Chair,
Groupe de travail de l'INTOSAI sur l'audit informatique

19 décembre 2022

TABLE DES MATIÈRES

FIGURES

PRÉAMBULE

L'audit des systèmes, contrôles et processus associés aux technologies de l'information, ou « Audit Informatique », représente désormais dans le monde entier une part importante de l'activité d'audit des Institutions supérieures de contrôle des finances publiques (ISC). Cette situation reflète naturellement la forte dépendance à l'informatique des pouvoirs publics et des organisations du secteur public. Les systèmes informatiques qu'une organisation déploie sont censés protéger ses données, ses actifs, et contribuer à la réalisation de sa mission et de ses objectifs spécifiques, notamment financiers.

Si la généralisation du recours à l'informatique a permis de renforcer la performance des organisations et l'efficacité du service rendu, elle s'accompagne toutefois de risques et de vulnérabilités associés par exemple à la dématérialisation des services et à l'interconnexion accrue avec d'autres systèmes et réseaux, à l'interne autant qu'à l'externe. L'audit informatique vise à apporter l'assurance que des procédures appropriées ont été mises en place pour gérer les risques et vulnérabilités touchant les systèmes d'information. Cette fonction est essentielle, si l'on attend de l'ISC qu'elle présente un compte rendu pertinent de l'efficacité de l'action des pouvoirs publics et des organisations du secteur public.

En 2014, le groupe de travail sur l'audit informatique (WGITA) de l'Organisation internationale des Institutions supérieures de contrôle des finances publiques (INTOSAI) et l'Initiative de développement de l'INTOSAI (IDI) ont réalisé ensemble un premier Manuel sur l'audit informatique, qui visait à fournir aux auditeurs des ISC un recueil de normes et de bonnes pratiques bénéficiant d'une reconnaissance universelle en la matière. L'édition 2022 du manuel propose une présentation actualisée des principaux domaines auxquels les auditeurs des systèmes informatiques pourront être amenés à s'intéresser dans leur activité d'audit.

Le manuel du WGITA et de l'IDI reprend les principes d'audit généraux définis dans les normes internationales des Institutions supérieures de contrôle des finances publiques (ISSAI)[1]. Il s'appuie également sur les référentiels mondialement reconnus dans le domaine des technologies de l'information, dont le référentiel COBIT de l'ISACA, les normes de l'ISO (organisation internationale de normalisation), mais aussi sur les guides et manuels informatiques de certaines ISC. L'objectif est d'apporter aux utilisateurs un socle d'informations et de les accompagner dans la formulation des questions clés qui leur permettront de réussir la planification et l'exécution des audits informatiques.

Le projet de mise à jour du manuel a été piloté par la présidence du WGITA, à savoir l'ISC d'Inde, l'ISC des États-Unis d'Amérique et l'IDI. Le WGITA et l'IDI souhaitent remercier les différents membres de l'équipe, qui ont travaillé sans relâche à l'élaboration de ces lignes directrices. Les auditeurs des SI des ISC d'Australie, du Brésil, de Fidji, d'Inde, du Koweït, des Philippines, de Tanzanie et des États-Unis d'Amérique ont apporté une contribution significative à ce travail en fournissant des exemples de rapports d'audit informatique. Le WGITA et l'IDI adressent également leurs remerciements aux ISC qui leur ont apporté un précieux retour d'expérience et leurs remarques sur les ébauches du manuel.

[1] www.issai.org.

LISTE DES ABRÉVIATIONS

CMMI	Intégration du modèle d'évolution des capacités (modèle CMM, *Capability Maturity Model*®)
CVDS	Cycle de vie du développement de système
FISCAM	*Federal Information Systems Controls Audit Manual*, manuel fédéral d'audit des contrôles et systèmes d'information
GAO	*Government Accountability Office*, ISC des États-Unis d'Amérique
GUID	Guide publié par l'INTOSAI
ICP	Indicateurs clés de performance
IDI	Initiative de développement de l'INTOSAI
IEC	*International Electrotechnical Commission*, commission électrotechnique internationale
INTOSAI	*International Organization of Supreme Audit Institutions*, organisation internationale des Institutions supérieures de contrôle des finances publiques
ISC	Institution supérieure de contrôle des finances publiques
ISO	*International Organization for Standardization*, organisation internationale de normalisation
ISSAI	*International Standards for Supreme Audit Institutions*, normes internationales des institutions supérieures de contrôle des finances publiques (parfois appelées « normes INTOSAI » dans les anciens documents)
ITIL	*Information Technology Infrastructure Library*, bibliothèque pour l'infrastructure des technologies de l'information
NIST	*National Institute of Standards and Technology*, institut national de normalisation et de technologie, rattaché au département du commerce des États-Unis
OLA	*Operational level agreement*, accord sur les niveaux opérationnels
PCA	Plan de continuité de l'activité
PRA	Plan de reprise d'activité
PUSI	Plan d'urgence pour les systèmes d'information
SLA	*Service level agreement*, accord sur les niveaux de service
WGITA	*Working Group on IT Audit*, groupe de travail sur l'audit informatique

INTRODUCTION

La dimension universelle de l'informatique et des technologies de l'information a modifié nos façons de travailler par bien des aspects, et la profession d'auditeur ne fait pas exception. À mesure que les technologies ont progressé, les pouvoirs publics et autres organisations du secteur public ont peu à peu intégré les innovations à leurs systèmes d'information, pour gagner en efficacité dans leurs missions de service public[2]. Les services publics ont connu eux-aussi une transition rapide du mode physique au mode numérique. Cette transition a eu pour conséquence d'amener les organismes publics à fonctionner sur le modèle d'une plate-forme numérique afin de mettre leurs services à la disposition de la population, mais aussi d'assumer le rôle de prestataire d'infrastructures pour les systèmes informatiques nécessaires à ces missions. Le processus constant de dématérialisation de l'information, qui consiste à convertir des archives et des données analogiques dans un format numérique, a lui aussi contribué à renforcer la dépendance globale envers les systèmes informatiques.

Jamais les technologies n'ont évolué si rapidement ; ce rythme a naturellement des répercussions sur l'activité d'audit informatique. Les systèmes informatiques sont de plus en plus complexes, font appel à des technologies variées, et leur implantation géographique est de plus en plus large. Ces systèmes sont interconnectés avec d'autres systèmes et réseaux internes et externes, dont Internet, ce qui les rend plus complexes encore. En parallèle, les organismes du secteur public stockent de plus en plus de données sur des systèmes utilisant l'informatique en nuage[3], pour accélérer les procédures d'achat de services et en réduire le coût. La tendance est à l'informatique omniprésente, l'accès facilité à l'information se généralise, et il ne fait aucun doute que cette tendance se poursuivra.

Cependant, ces avancées technologiques se sont accompagnées d'une multiplication des risques et des vulnérabilités. Ainsi, le développement des systèmes informatiques en ligne et des réseaux a augmenté les risques de sécurité auxquels les organisations du secteur public sont confrontées. Ces organisations recueillent et traitent d'importants volumes d'informations à caractère personnel identifiables[4], dont la confidentialité peut s'avérer complexe à garantir. De même, dans le contexte de pandémie de COVID-19, elles ont fait face à des difficultés inédites, contraintes d'assurer leurs missions tout en garantissant à leur personnel la possibilité de travailler dans de bonnes conditions de sécurité et d'efficacité.

Ces tendances, combinées à la sophistication croissante des attaques des pirates informatiques et autres personnes mal intentionnées, ont augmenté le risque de compromission de données à caractère sensible. Si les systèmes et réseaux d'un organisme ne bénéficient pas d'une protection adéquate, des services essentiels pourraient s'en trouver dégradés. Il est donc impératif d'identifier toute vulnérabilité nouvelle, d'évaluer le risque (probabilité) que cette vulnérabilité soit exploitée et avec quelles conséquences, de l'atténuer en tenant compte de l'appétence de l'organisation pour le risque, pour en définitive le maîtriser de façon appropriée.

---

[2] On peut définir les systèmes d'information (SI) comme un ensemble d'activités stratégiques, managériales et opérationnelles intervenant dans la collecte, le traitement, le stockage, la diffusion et l'utilisation d'informations, en y incluant les technologies associées. Les technologies de l'information (TI), quant à elles, regroupent les éléments matériels et logiciels, les équipements de communication et autres installations qui sont utilisés pour saisir, stocker, traiter, transmettre et générer des données.

[3] L'informatique en nuage (le « Cloud ») facilite la mise en place d'un accès à la demande pour un ensemble de ressources informatiques configurables (par exemple, réseaux, serveurs, applications de stockage, services) susceptibles d'être constituées et diffusées rapidement.

[4] On entend par « information personnelle identifiable » toute information susceptible d'être utilisée pour repérer ou retracer l'identité d'une personne physique (nom, date et lieu de naissance, par exemple), ainsi que d'autres types d'informations à caractère personnel susceptibles d'être associées à une personne physique (données relatives à la santé, à la formation, à la situation financière et professionnelle de la personne physique).

Face à l'augmentation tant des investissements consentis que de la dépendance des entités contrôlées aux systèmes informatiques, l'auditeur doit nécessairement adapter sa méthodologie et son approche. Cette démarche contribue à assurer que l'audit permettra d'identifier avec certitude les risques pour l'intégrité, la disponibilité, la validité, l'utilisation légitime et la confidentialité des données, et apportera l'assurance que des contrôles sont en place pour atténuer les risques identifiés. Dans le contexte d'un audit informatique, on entend par « contrôles » les processus, outils et autres mécanismes de supervision en place pour gérer les fonctions informatiques et éviter les risques et vulnérabilités.

Généralement, le système informatique, surtout s'il est déployé dans un environnement où les contrôles sont inappropriés, expose l'organisation à de nombreux risques que l'auditeur des SI devra identifier. Même si l'organisation auditée a mis en œuvre certaine mesures pour réduire les risques, un audit indépendant fournira l'assurance que des contrôles adéquats sont en place pour protéger les systèmes d'information. Cet audit déterminera si l'organisation a prévu des contrôles informatiques généraux[5] et des contrôles d'application[6] afin de réduire autant que possible l'exposition aux différents risques, et si ces contrôles sont efficaces et performants.

En résumé, la transition des organisations auditées du secteur public vers les systèmes d'information et le traitement numérique des données a rendu nécessaire l'acquisition par les institutions d'audit de capacités appropriées, leur permettant de mener à bien un examen approfondi des contrôles associés aux systèmes informatiques et ainsi de s'acquitter des objectifs généraux de leur mandat d'audit. Plus particulièrement, elles doivent s'assurer que les organisations des pouvoirs publics ont mis en place des contrôles informatiques internes garantissant la confidentialité, l'intégrité, la validité et la disponibilité des données.

Contenu et organisation du manuel

Le présent manuel vise à fournir aux auditeurs des SI des recommandations descriptives sur les différents aspects de l'audit informatique. Il a été conçu en application des exigences du Protocole d'assurance qualité des biens publics mondiaux de l'IDI, version 2.0[7].

Le lecteur y trouvera une présentation générale de la définition de l'audit informatique, des missions des ISC dans ce domaine, ainsi que du périmètre et des objectifs des audits informatiques. Ce chapitre propose une explication des contrôles informatiques généraux et des contrôles d'application, et présente les liens entre ces deux notions. Les chapitres suivants reviendront plus en détail sur ces dimensions du contrôle. Le chapitre 1 décrit également la procédure d'audit informatique et la méthodologie d'évaluation fondée sur le risque appliquée à la sélection des audits informatiques. La description du processus d'audit informatique est générique ; elle s'appuie sur les méthodologies d'audit standard[8] appliquées pour l'audit des systèmes informatiques. Les tableaux et graphiques qui accompagnent la description du processus d'audit sont fournis à titre d'illustration et devront nécessairement être adaptés à la mission d'audit envisagée. Les utilisateurs de ce manuel sont invités à considérer le processus d'audit à la

[5] Les « contrôles informatiques généraux » ne concernent pas spécifiquement un flux opérations ou une application donnée ; ils portent sur les processus encadrant un déploiement informatique à l'appui du développement, de l'implémentation et de l'exploitation d'un système informatique. Ces contrôles englobent habituellement la gouvernance, l'organisation et la structure des technologies de l'information, les contrôles physiques et les contrôles de l'environnement, l'exploitation informatique, la sécurité des systèmes d'information, la continuité opérationnelle, les accès et la gestion du changement.

[6] Les « contrôles d'application » concernent spécifiquement un système informatique et comprennent l'établissement d'une cartographie des règles opérationnelles en usage dans l'application, ce qui permet de définir des contrôles pour la saisie, le traitement, la génération des données, mais aussi des contrôles sur les données de base.

[7] Le protocole est accessible à l'adresse suivante (en anglais) : http://www.idi.no/en/idi-library/global-public-goods.

[8] Cf., par exemple, l'ISSAI 100 de l'Organisation internationale des institutions supérieures de contrôle des finances publiques *: Principes fondamentaux du contrôle des finances publiques* (2019) et l'ISSAI 5100 *Guide d'audit des systèmes d'information* (2019).

lumière des informations connexes présentées dans les ISSAI et les autres référentiels et normes internationaux. Ils se réfèreront également aux manuels et recommandations relatifs à la procédure d'audit appliqués dans leur ISC pour planifier et réaliser chacun de leurs audits.

Les chapitres 2 à 8 apportent une description détaillée des différents domaines des technologies de l'information, afin d'aider les auditeurs à identifier les aspects sur lesquels l'audit pourra porter. À la fin de chaque chapitre, une liste des risques organisationnels associés à chaque domaine a été établie. Grâce à elle, les auditeurs pourront identifier parmi les domaines susceptibles d'être audités, ceux qui présentent un risque élevé. Les recommandations formulées pour chacun des domaines aideront les auditeurs dans leur travail de planification, pour un domaine en particulier ou pour un ensemble de domaines, selon le périmètre et l'objectif de l'audit informatique (par exemple, audit de performance ou audit financier portant sur les systèmes informatiques). Par exemple, les recommandations relatives à l'audit de la gouvernance des technologies de l'information peuvent être utilisées pour planifier un audit des mécanismes de gouvernance des systèmes informatiques mis en place par l'organisation, ou pour planifier l'audit de l'environnement des contrôles généraux, dont la gouvernance des technologies de l'information constitue un élément important.

L'annexe I de ce manuel présente un aperçu des domaines émergents en matière d'audit informatique, et des références permettant au lecteur intéressé d'approfondir le sujet. L'annexe II comprend des liens vers des rapports d'audit soumis par des ISC du monde entier, qui peuvent constituer des exemples pertinents du large spectre de domaines que l'audit informatique peut aborder, tels qu'ils sont présentés au chapitre 2 à 8 du manuel.

L'édition 2014 du Manuel sur l'audit informatique comportait d'autres annexes, qui proposaient des recommandations pas à pas sur l'élaboration d'une matrice d'audit. Ces annexes consacrées à la matrice d'audit recensaient différentes questions clés pour l'audit, les critères applicables, les informations requises, mais également des méthodes d'analyse. L'édition 2014 du Manuel d'audit informatique et les annexes consacrées à la matrice d'audit restent accessibles (en anglais) à partir du lien suivant : https://www.intosaicommunity.net/wgita/wp-content/uploads/2018/04/it-audit-handbook-english-version.pdf

Le périmètre défini pour ce manuel ne comprend pas non plus de recommandations d'ordre technique sur l'utilisation des technologies d'audit assisté par ordinateur. Les ISC sont encouragées à organiser séparément pour leur personnel une formation aux techniques d'audit assisté par ordinateur. Les ISC peuvent également envisager d'inscrire leur personnel au programme de l'IDI sur le renforcement des capacités en matière d'audit informatique.

Rendez-vous sur les sites Web du WGITA et de l'IDI pour plus d'informations sur les ressources disponibles et les programmes de formation à venir :

WGITA : https://www.intosaicommunity.net/wgita/ IDI : http://www.idi.no

Nous espérons que les ISC et leur personnel affecté à l'audit informatique trouveront dans ce manuel un outil utile qui leur permettra d'améliorer leur connaissance et leur compréhension des questions relatives à l'audit informatique, et qui les aidera à planifier et réaliser des audits informatiques. Les lecteurs du guide pourront se référer à d'autres produits documents publiés par l'IDI au niveau mondial, qui sont complémentaires de ce guide. On citera notamment le *Guide de mise en œuvre des ISSAI relatives à l'audit de performance*[9], le *Guide de mise en œuvre des ISSAI relatives à l'audit financier*[10] et le *Guide de mise en œuvre des ISSAI relatives à l'audit de conformité*[11], tous trois publiés par l'IDI.

[9] Initiative de développement de l'Organisation internationale des Institutions supérieures de contrôle des finances publiques : *Guide de mise en œuvre des ISSAI relatives à l'audit de performance*, version 1 (août 2021), https://www.idi.no/elibrary/professional-sais/issai-implementation-handbooks/handbooks-french/1036-performance-audit-issai-implementation-handbook-version-0-french/file.

CHAPITRE 1 L'AUDIT INFORMATIQUE

Comme indiqué plus haut, la transition des organisations du secteur public vers les systèmes informatiques et le traitement numérique des données a rendu nécessaire l'acquisition par les institutions d'audit de capacités propres à leur permettre de mener à bien un examen approfondi des contrôles associés aux systèmes d'information, et ainsi d'atteindre les objectifs généraux fixés dans le cadre de leur mandat d'audit. Plus particulièrement, les ISC doivent s'assurer que les organisations du secteur public ont mis en place des contrôles informatiques internes qui garantissent la confidentialité, l'intégrité, la validité et la disponibilité des données.

Ce chapitre propose un aperçu du processus d'audit des systèmes d'information, également appelé « audit informatique ». Il constitue à la fois une introduction au manuel et un résumé des chapitres 2 à 8. Il diffère donc des autres chapitres, tant dans sa conception que dans son contenu.

La description du processus d'audit informatique qui figure dans ce chapitre est générique, fondée sur des méthodes d'audit normalisées ; elle reflète la méthodologie d'audit appliquée au sein des ISC. Les utilisateurs de ce manuel sont donc invités à considérer ce processus d'audit à la lumière des informations connexes présentées dans les ISSAI et d'autres normes internationales.

I. Qu'est-ce qu'un audit informatique ?

a. Obligation d'audit informatique

Le mandat donné à l'Institution supérieure de contrôle des finances publiques (ISC) aux fins de la réalisation d'un audit des systèmes d'information est contenu dans l'ISSAI 1, la Déclaration de Lima[12]. Par extension, le mandat dont dispose l'ISC pour vérifier les systèmes informatiques d'une entité découle de son mandat général, qui l'habilite à réaliser des audits de la performance, des audits financiers et de conformité ou des audits combinés[13].

- L'**audit de performance** vise à déterminer si les engagements, les programmes et les organisations publiques sont en conformité avec les principes d'économie, d'efficience et d'efficacité et s'il existe des possibilités d'amélioration.
    - L'**audit du principe d'économie** concentre l'audit sur la manière dont les organisations auditées ont réussi à minimiser le coût des ressources, en prenant en compte la qualité de ces ressources.
    - L'**audit de l'efficience** consiste à se demander si les ressources ont été utilisées de manière optimale ou satisfaisante, ou si des résultats semblables ou similaires auraient pu être atteints avec moins de ressources.
    - L'**audit de l'efficacité** évalue les résultats. Pour apprécier l'efficacité, l'ISC examine si et dans quelle mesure la politique publique, le thème d'audit ou l'activité répond aux objectifs fixés.

---

[10] Initiative de développement de l'Organisation internationale des Institutions supérieures de contrôle des finances publiques : *Guide de mise en œuvre des ISSAI relatives à l'audit financier*, version 1 (8 décembre 2020), https://www.idi.no/elibrary/professional-sais/issai-implementation-handbooks/handbooks-french/1167-issai-en-audit-financier-manuel-de-mise-en-oeuvre-version-1-francais-examen-de-toucher-leger-2020/file.

[11] Initiative de développement de l'Organisation internationale des Institutions supérieures de contrôle des finances publiques : *Guide de mise en œuvre des ISSAI relatives à l'audit de conformité*, version provisoire 0 (8 janvier 2018), https://www.idi.no/elibrary/professional-sais/issai-implementation-handbooks/handbooks-french/826-compliance-audit-issai-implementation-handbook-version-0-french/file.

[12] Organisation internationale des Institutions supérieures de contrôle des finances publiques, *Déclaration de Lima*, Partie VII Section 22.

[13] Organisation internationale des Institutions supérieures de contrôle des finances publiques, *ISSAI 100 : Principes fondamentaux du contrôle des finances publiques*.

L'audit de la performance vise à évaluer la performance de l'organisation à l'aune de critères pertinents, qui correspondent à la situation qui doit être constatée ou que l'on souhaite constater dans le cadre de l'examen d'un thème d'audit en particulier, et qui représentent un niveau de performance raisonnable et réaliste. L'audit comprend également une analyse de la cause des écarts par rapport à ces critères, et d'autres problèmes constatés. L'audit de la performance a généralement pour but de déterminer si les pouvoirs publics utilisent efficacement leurs ressources pour mener à bien leurs objectifs politiques. Ce type d'audit examine souvent la mise en œuvre d'une ou de plusieurs politiques.

- L'**audit financier** vise essentiellement à déterminer si les informations financières d'une entité sont présentées conformément au référentiel d'information financière et au cadre réglementaire applicables. L'audit financier est destiné à accroître le degré de confiance des utilisateurs présumés envers les états financiers. Pour y parvenir, l'auditeur formule une opinion dans laquelle il indique si les états financiers sont établis, dans tous leurs aspects significatifs, conformément au référentiel comptable applicable. L'audit financier peut comporter un contrôle détaillé et exhaustif des informations financières.
- L'**audit de conformité** consiste à évaluer de façon indépendante si un sujet donné est conforme aux textes législatifs et réglementaires applicables qui servent de critères. L'auditeur vérifie si les activités, les transactions financières et les informations sont, dans tous leurs aspects significatifs, conformes aux textes législatifs et réglementaires qui régissent l'entité auditée Les audits de conformité créent de la valeur, en apportant une assurance indépendante de la conformité de l'entité auditée, qui s'appuie sur le jugement professionnel indépendant des auditeurs et sur un travail d'analyse bien fondé et solide.
- Un **audit intégré** combine différents types d'audit afin d'évaluer les interactions entre les processus financiers, opérationnels et technologiques et leur apport à la réalisation des objectifs de contrôle[14]. Par exemple, l'audit intégré des états financiers d'une entité peut comporter une analyse des lacunes présentées par les contrôles des systèmes d'information[15].

L'audit informatique fait souvent partie d'une mission d'audit plus large, qui peut être un audit de la performance, un audit financier ou un audit de conformité. Il est possible de réaliser un audit informatique hors du cadre d'un audit de la performance, d'un audit financier ou d'un audit de conformité ; en revanche, les principes généraux, les procédures, les normes et les attentes applicables à ces types d'audit restent valables pour un audit informatique.

b. Définition de l'audit informatique

L'audit informatique examine certains aspects de l'utilisation des technologies de l'information au sein d'une organisation, dont les infrastructures informatiques, les politiques et procédures, les applications, l'utilisation des données. L'audit informatique comprend habituellement une analyse des systèmes et des contrôles, afin de s'assurer qu'ils répondent aux besoins de l'activité de l'entité, sans compromettre la sécurité, la confidentialité, la maîtrise des coûts et d'autres éléments critiques de l'activité. Souvent, l'audit informatique implique également de donner l'assurance que le développement, le déploiement et la maintenance des systèmes informatiques répondent aux objectifs de l'activité, préservent l'information qui constitue un actif, tout en maintenant l'intégrité des données. L'audit informatique nécessite souvent d'identifier les écarts par rapport aux critères, définis en fonction de la nature de la mission d'audit (par exemple, audit de la performance, financier ou de conformité).

Les audits informatiques varient selon qu'ils s'inscrivent dans le cadre plus large de tel ou tel type d'audit. Par exemple :

---

[14] Harvard University, « What Is an Integrated Audit? », https://rmas.fad.harvard.edu/faq/what-integrated-audit.

[15] Voir à titre d'exemple : U.S. Government Accountability Office, *Management Report: Improvements Are Needed in the Bureau of the Fiscal Service's Information Systems Controls,* GAO-14-693R, (18 juillet 2014), https://www.gao.gov/products/GAO-14-693R.

- Dans le contexte d'un audit financier, l'audit informatique pourrait consister en l'examen des contrôles généraux garantissant le fonctionnement des systèmes d'information sur lesquels s'appuient les processus financiers de l'entité, conformément à la situation présentée par ses états financiers[16].
- Dans le contexte d'un audit de performance, l'audit informatique pourrait consister à déterminer dans quelle mesure l'adoption des nouvelles technologies par l'agence gouvernementale a produit des avantages et des économies de coûts mesurables à l'échelle de l'ensemble du secteur public[17].
- Dans le contexte d'un audit de conformité, l'audit informatique pourrait consister en l'examen de l'efficacité des systèmes d'information qui génèrent des rapports de conformité, permettant au personnel d'effectuer et de contrôler les opérations de l'entité.[18]

Les audits informatiques traitent de différents domaines, comme la gouvernance des technologies de l'information, les investissements informatiques (notamment dans les télécommunications), l'existence de contrôles suffisants pour protéger les données d'entités relevant par exemple des collectivités locales, l'analyse de l'application des nouvelles technologies (comme l'intelligence artificielle), ou le développement, l'acquisition et l'exploitation de systèmes informatiques. Les audits informatiques abordent également les questions de sécurité de l'information et de cybersécurité, des thématiques étroitement liées.

- On peut définir la **sécurité de l'information** comme la capacité d'un environnement informatique[19] à protéger l'information et les ressources des systèmes, analogiques ou numériques, pour ce qui concerne la confidentialité, la disponibilité et l'intégrité[20]. La sécurité de l'information englobe les mesures nécessaires pour gérer, prévenir, détecter, documenter et contrer ce type de menace. La sécurité de l'information permet à l'entité de protéger l'infrastructure de son système d'information contre les utilisateurs non autorisés.
- La **cybersécurité** désigne la démarche de protection des informations numériques par la prévention et la détection des cyberattaques et la réponse à ces attaques[21]. Elle englobe la stratégie, la politique et les normes traitant de la sécurité du cyberespace et des opérations qui y sont exécutées. Elle concerne notamment la réduction des menaces et des vulnérabilités, la réponse aux incidents, les processus de résilience et de reprise, ainsi que l'assurance de l'information[22].

L'une des principales différences entre la sécurité de l'information et la cybersécurité est que la cybersécurité se concentre plus précisément sur la protection de l'information numérique, tandis que la sécurité de l'information englobe plus largement la protection de toutes les ressources du système d'information. Si le présent manuel porte avant tout sur la sécurité de l'information, de nombreux

---

[16] Voir à titre d'exemple : U.S. Government Accountability Office, *Management Report: Improvements Needed in the Bureau of the Fiscal Service's Information System Controls Related to the Schedule of Federal Debt,* GAO-22-105569, (17 mars 2022), https://www.gao.gov/products/GAO-22-105569.

[17] Voir à titre d'exemple : U.S. Government Accountability Office, *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked*, GAO-19-58, (4 avril 2019), https://www.gao.gov/products/gao-19-58.

[18] Voir à titre d'exemple : U.S. Government Accountability Office, *Improper Payments: Additional Guidance Needed to Improve Oversight of Agencies with Noncompliant Programs*, GAO-19-14, (7 décembre 2018), https://www.gao.gov/products/gao-19-14.

[19] L'environnement informatique désigne les applications informatiques, les infrastructures sous-jacentes, mais aussi les processus qu'une entité utilise dans le cadre de ses activités, pour réaliser sa stratégie.

[20] National Institute of Standards and Technology, *Glossary,* (2021), https://csrc.nist.gov/glossary.

[21] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1* (2018).

[22] National Initiative for Cybersecurity Careers and Studies, *Cybersecurity Glossary,* (Gaithersburg, MD: 10 mars 2022), https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.

éléments importants de la sécurité de l'information sont également applicables à la cybersécurité. Le WGITA de l'INTOSAI travaille actuellement, dans le cadre d'un autre projet, à l'élaboration d'un guide sur l'audit spécifiquement consacré à la cybersécurité et à la protection des données.

c. Les différentes phases d'un audit informatique

L'audit informatique comporte différentes phases : définition du périmètre, planification, conception, réalisation, puis présentation des résultats de l'audit. Les paragraphes suivants reviennent plus en détail sur chacune d'elles. La section II concerne la planification de l'audit ; la section III, la conception de l'audit ; la section IV, la réalisation de l'audit ; la section V, la présentation des résultats de l'audit.

Figure 1 : Les phases d'un audit informatique

Source : Unknown.

Remarque : cette figure propose un exemple qu'il convient d'adapter à la mission d'audit abordée.

II. Étape 1 : Planifier un audit informatique

Comme pour n'importe quel audit, la planification est une étape essentielle de l'audit informatique. Dans la plupart des ISC, les audits sont planifiés à trois niveaux : planification stratégique ; planification globale ou annuelle ; planification de détail, organisationnelle. La planification n'est pas figée, elle est réévaluée en continu tout au long de l'audit, à mesure que sont découvertes de nouvelles informations susceptibles d'entraîner une réorientation du plan initial. L'exigence de planification est la même si l'audit résulte des conclusions d'un précédent audit, au titre d'une approche d'audit continu. Toutefois, certaines étapes comme la familiarisation avec le fonctionnement de l'organisation, peuvent être allégées dans le cadre d'une approche d'audit continu, des informations ayant déjà été recueillies à l'occasion d'un précédent audit.

a. Planification stratégique

Le plan stratégique de l'ISC correspond à une planification à long terme (3 à 5 ans) des objectifs et des finalités de l'activité d'audit, concernant notamment les systèmes informatiques et les organisations associées relevant de la compétence de l'ISC. Certaines ISC choisissent de n'inclure dans leur plan stratégique que les domaines nouveaux et émergents des systèmes d'information qu'il convient d'auditer. Dans cette optique, l'ISC pourra examiner de nouvelles méthodes de développement de systèmes (par exemple, la programmation agile), les processus d'acquisition ou d'informatique dans le nuage appliqués

au secteur public, ou encore l'adoption de nouvelles technologies comme l'intelligence artificielle ou les blockchains. La démarche de planification stratégique de l'ISC et le plan stratégique établi définissent le ton et l'orientation des objectifs d'audit informatique de l'ISC pour l'avenir. Par exemple, comme on le verra au chapitre 3 consacré au développement et à l'acquisition de systèmes d'information, une organisation qui envisage d'ajuster sa méthodologie de cycle de vie de développement de système pourra prévoir un audit ayant pour objectif de vérifier la situation et le niveau d'avancement de la transition vers le nouveau modèle.

b. Planification globale et approche fondée sur le risque

Généralement, la planification globale de l'activité d'audit s'inscrit dans un cycle annuel, par lequel l'ISC sélectionne certains domaines d'audit. Elle détermine ensuite un processus adapté pour identifier quels domaines feront l'objet d'un audit dans l'année[23]. Face à la diffusion rapide des systèmes d'information modernes parmi les entités du secteur public et compte tenu des ressources limitées dont les ISC disposent, une approche fondée sur le risque permet de hiérarchiser les thèmes d'audit et de sélectionner les aspects prioritaires. En complément des considérations permettant de sélectionner les systèmes d'information devant faire l'objet d'un audit, le choix des thèmes d'audit par l'ISC doit également tenir compte de différentes informations comme la dépense informatique globale, la connectivité avec d'autres entités externes, ainsi que la maturité des processus informatiques et des mécanismes de gouvernance des technologies de l'information. L'ISC devra aussi intégrer à sa planification certains audits imposés par la loi ou une requête du Parlement, du congrès ou d'autres organismes de surveillance

Les ISC auditent régulièrement un grand nombre d'organisations, appliquant différents systèmes d'information. Il peut exister différentes applications pour différentes fonctions et différentes activités, et les systèmes informatiques peuvent être installés sur différents sites géographiques.

Pour déterminer quels systèmes d'information auditer et par quels moyens, il faut notamment disposer au préalable d'une bonne compréhension du risque inhérent à l'organisation. Le **risque inhérent** représente la probabilité que certaines caractéristiques des systèmes d'information de l'organisation contrôlée, par leur nature même, puissent avoir des conséquences défavorables sur l'exécution de la mission pour laquelle l'organisation a été mandatée. Par exemple, un système informatique conçu pour mettre des informations à disposition du public comporte un risque inhérent de performance, en ce sens qu'au-delà d'un nombre prédéfini d'utilisateurs, le système d'information peut échouer à répondre, auquel cas l'information n'est alors plus accessible à aucun utilisateur. Si l'organisation peut mettre en place des contrôles visant à atténuer les risques inhérents, elle n'a souvent d'autre choix que de tolérer l'existence de ces risques, dans des limites acceptables.

Si les systèmes d'information comportent des risques inhérents, ces risques n'impactent pas les mêmes systèmes, et pas de la même manière. Par exemple, le risque d'indisponibilité, ne serait-ce que pour une heure, peut être considéré comme étant un risque grave s'il concerne le système de facturation d'un point de vente très fréquenté. De même, pour un système bancaire en ligne, le risque d'une modification non autorisée peut représenter une source de fraude, avec de possibles pertes. Les environnements techniques dans lesquels les systèmes sont exploités peuvent également avoir une incidence sur le risque associé aux systèmes[24]. Pour déterminer les systèmes informatiques prioritaires pour l'audit, l'auditeur pourra s'appuyer sur une approche fondée sur le risque.

[23] D'un pays à l'autre, les ISC adoptent des structures différentes pour leur organisation. Ici, le premier niveau correspond à une structure d'ISC type, conçue selon le modèle articulant un centre de décision et des opérations de terrain, dans lequel la planification globale est effectuée ou validée par le centre de décision, avant réalisation des missions d'audit au niveau du terrain.

[24] S. Anantha Sayana, ISACA.

Pour appliquer un référentiel d'évaluation du risque, l'ISC doit disposer d'un socle minimum d'informations transversales sur les organismes auditables, qu'elle recueille habituellement au moyen de questionnaires ou d'exercices d'autoévaluation des contrôles. L'encadré ci-contre, « Les étapes d'une approche fondée sur le risque », propose une méthodologie d'évaluation des risques afin d'identifier les systèmes informatiques susceptibles d'être audités[25]. Pour les entités exerçant un mandat plus large, il pourra s'avérer nécessaire de resserrer le périmètre d'audit potentiel, en ciblant par exemple certaines entités ou certains aspects des systèmes d'information, avant d'appliquer la méthodologie.

Exemple : les étapes d'une approche fondée sur le risque

1. Identifier l'univers d'audit qui réunirait l'ensemble des entités auditables relevant de la juridiction de l'ISC.
2. Dresser la liste des systèmes d'information utilisés dans ces entités auditables.
3. Identifier les facteurs qui déterminent la criticité du système pour l'entité, en ce qu'il lui permet de fonctionner et d'assurer le service pour lequel elle a été mandatée.
4. Pondérer les facteurs de criticité. Cette étape peut être effectuée en consultation avec l'entité contrôlée.
5. Compiler des informations pour tous les systèmes, sur l'ensemble des entités, et établir un ordre de priorité pour l'audit des systèmes/entités, selon la note cumulée attribuée à chacun.
6. Préparer un plan d'audit annuel définissant pour chaque audit informatique des priorités, une approche et un calendrier. Cet exercice pourrait être répété chaque année, pour constituer un plan récurrent.

Pour procéder à l'évaluation, fondée sur le risque, de systèmes fonctionnant grâce aux technologies de l'information, l'ISC peut définir une méthodologie appropriée, selon la finalité identifiée. Cette méthodologie peut simplement consister à attribuer à l'environnement informatique un profil de risque élevé, moyen ou faible. Elle peut également impliquer une analyse plus complexe et chiffrée, quantifiant la note de risque à partir de données objectives recueillies auprès de l'entité contrôlée. Pour apprécier le risque, l'ISC s'appuie sur sa connaissance de l'entité et de son environnement, mais également sur le jugement professionnel de l'équipe d'audit informatique. Par exemple, et nous y reviendrons au chapitre 4, l'ISC peut déterminer quels systèmes informatiques auditer en retenant les systèmes qui ont mis en œuvre les changements les plus significatifs, et donc ajouter un critère de gestion des changements à la liste des domaines potentiellement à risque.

Pour sélectionner l'entité qui fera l'objet d'un audit informatique, l'ISC peut donc procéder à une évaluation des risques. Elle peut également mettre en place un cycle de sélection des organisations auditables, en s'appuyant sur les missions d'audit pour lesquelles elle a été mandatée, ou sur des demandes spécifiques émanant des organismes de surveillance (par exemple, le congrès, le Parlement ou plus largement, le pouvoir législatif).

c. Planification de détail

La planification de détail consiste à élaborer un plan d'audit détaillé pour l'entité sélectionnée, en partant de la définition des objectifs d'audit. Les auditeurs s'appuieront sur ce plan pour préparer le programme d'audit informatique. Avant de pouvoir préparer le programme d'audit, il est nécessaire d'acquérir une bonne compréhension de l'entité auditée et de ses systèmes informatiques. Le présent manuel vise à accompagner les auditeurs, après qu'un plan aura été défini, pour les aider à remplir la matrice d'audit avec des objectifs spécifiques pour chaque domaine (par exemple, gouvernance et sécurité de l'information) qu'il est prévu d'examiner. La planification de détail exige une bonne connaissance de l'entité et une évaluation préalable des contrôles en place pour faciliter la planification détaillée de l'audit. Elle impose également d'envisager l'affectation des ressources et du personnel pour faire en sorte que l'équipe d'audit soit composée de membres possédant collectivement les compétences nécessaires aux

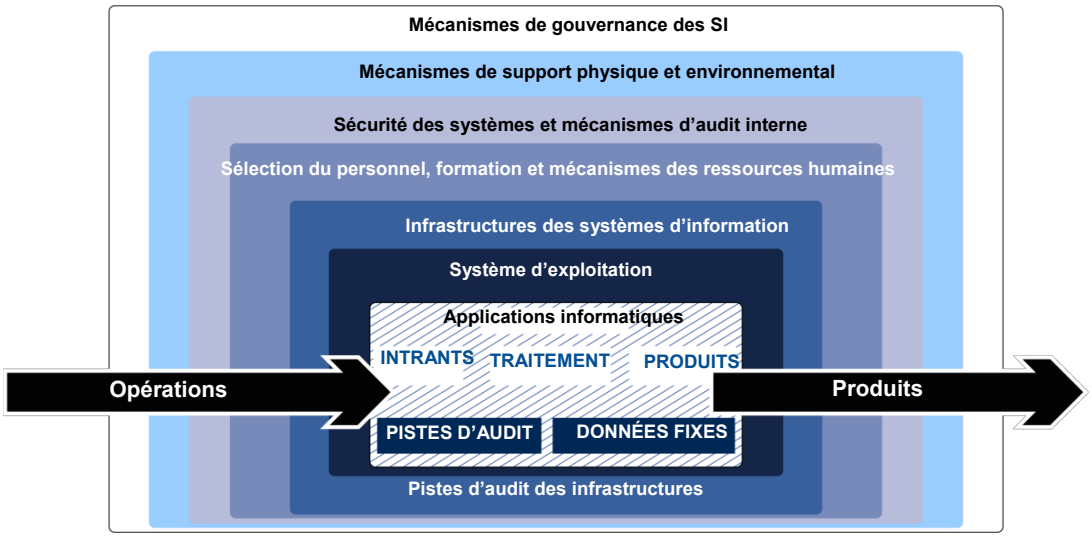
[25] Les auditeurs trouveront un autre exemple de méthodologie d'évaluation des risques associés aux systèmes d'information, ainsi qu'un guide pour l'évaluation des risques dans la planification du travail d'audit, dans la publication suivante : Internal Audit Community of Practice (Communauté des praticiens de l'audit interne), *Risk Assessment in Audit Planning* (avril 2014), https://www.pempal.org/sites/pempal/files/event/attachments/cross_day-2_4_pempal-iacop-risk-assessment-in-audit-planning_eng.pdf.

missions d'audit informatique, afin d'atteindre les objectifs visés. Par exemple, ainsi qu'on le verra au chapitre 6 consacré à la gestion de la continuité de l'activité, l'ISC peut prévoir d'intégrer à l'audit des critères supplémentaires afin d'évaluer la planification de la reprise après sinistre pour les systèmes considérés comme essentiels aux opérations transversales à l'entité auditée.

i. Compréhension de l'entité

Le degré de connaissance de l'entité et de ses processus que l'auditeur des SI doit acquérir dépend pour une large part de la nature de l'entité et du niveau de détail du travail d'audit réalisé. Par exemple, le périmètre de ce qui est contrôlé varie d'un audit informatique à l'autre : un simple système informatique, une entité définie, une branche du secteur public, voire les systèmes nationaux dans leur globalité. Comprendre l'entité implique de connaître les risques opérationnels, financiers et inhérents auxquels l'entité et ses systèmes informatiques sont exposés. Cela implique également d'identifier dans quelle mesure l'entité a recours à l'externalisation de services pour atteindre ses objectifs, et dans quelle mesure les processus opérationnels de l'entité ont été cartographiés dans un environnement informatique[26]. L'auditeur doit utiliser ces informations pour identifier les problèmes potentiels, définir les objectifs et le périmètre de la mission, réaliser le travail, et prendre en considération les actions de gestion sur lesquelles l'auditeur des SI doit être vigilant. La figure 2 présente l'organisation typique du système informatique d'une entité.

Figure 2 : Organisation typique du système informatique d'une entité



Source : Unknown.

Au sein d'une organisation, à toute application formant le cœur d'un système informatique correspondra une pile technologique : un ensemble de langages de programmation, de référentiels et d'outils sur lesquels les développeurs s'appuient pour créer l'application. La pile technologique peut inclure un système de gestion de bases de données associé à des bases de données spécifiques, des logiciels de cartographie des règles opérationnelles dans le système au moyen de modules dédiés, ainsi qu'une ou plusieurs interfaces utilisateurs frontales fonctionnant au moyen de logiciels applicatifs réseau, en

[26] Habituellement, les entités qui passent d'un environnement manuel à un environnement électronique réalisent un exercice de réingénierie des processus opérationnels. Il est possible que certains des processus opérationnels soient réalisés manuellement en parallèle de l'exécution informatisée, ou que l'entité ait développé des processus automatisés efficients ou efficaces, en reproduisant simplement ses processus manuels. Ces scénarios présenteraient un intérêt particulier pour les auditeurs des SI.

présence d'un environnement réseau. Les bases de données et les logiciels d'application sont abrités sur des serveurs, qui sont pour l'essentiel des équipements matériels de grande capacité ou des logiciels capables d'héberger de multiples bases de données et applications de volume important. Les serveurs peuvent être conçus pour répondre aux contraintes spécifiques des utilisateurs : serveurs de données, serveurs d'applications, serveurs Internet, serveurs proxy.

Avant le lancement d'une évaluation des contrôles d'un système d'information, il est important que les auditeurs acquièrent une bonne connaissance de l'architecture du système, des données sous-jacentes et de leurs sources. Ils pourront ainsi identifier les outils et les techniques d'audit nécessaires. En s'appuyant sur leur connaissance du système d'information et de l'entité contrôlée, ils pourront définir leur approche de l'audit informatique.

D'autres activités d'audit peuvent s'avérer utiles pour comprendre l'entité contrôlée :

- cartographie des activités de l'entité contrôlée,
- cartographie des interactions de l'entité avec ses pairs ou avec l'environnement extérieur,
- identification des activités opérationnelles critiques pour les objectifs de l'entité contrôlée,
- identification de toutes les solutions informatiques que l'entité utilise actuellement.

ii. Matérialité

Il convient de déterminer la matérialité, ou la pertinence et le caractère significatif, des enjeux de l'audit informatique en s'appuyant sur le référentiel général que l'ISC utilise pour apprécier le caractère significatif dans la préparation d'un rapport d'audit. Les critères d'appréciation de la matérialité peuvent varier selon la nature de la mission d'audit informatique[27]. L'auditeur pourrait considérer la matérialité du sujet à la lumière, par exemple, des états financiers ou de la nature de l'entité ou de son activité. Dans le contexte des systèmes d'information, la matérialité peut également être définie en termes non financiers.

Il appartient à l'auditeur des SI de déterminer dans quelle mesure une lacune des systèmes d'information peut devenir significative. Il convient d'apprécier le caractère significatif des lacunes des contrôles informatiques généraux en considérant leur effet sur les contrôles d'application (c'est-à-dire, dans quelle mesure ces lacunes rendront également défaillants les contrôles d'application associés). Si l'insuffisance des contrôles d'application est liée aux lacunes des contrôles informatiques généraux, alors leur matérialité est établie. Par exemple, si des calculs fiscaux générés par une application présentent des erreurs majeures, résultant d'un manque de rigueur dans la modification des tableaux de fiscalité, toute décision de la direction de l'entité de ne pas rectifier une défaillance d'un contrôle informatique général et ses conséquences sur l'environnement de contrôle peut devenir significative dès lors qu'elle s'ajoute à d'autres lacunes des contrôles impactant l'environnement de contrôle[28].

iii. Affectation des ressources et constitution de l'équipe d'audit

Il est important d'allouer à l'audit informatique des ressources adaptées. En particulier, l'équipe doit posséder de bonnes connaissances générales sur les systèmes d'information, les processus et les mécanismes dont dépend la réussite d'un déploiement informatique. Si les ressources humaines sont importantes[29], certains aspects ne doivent pas être négligés, comme le budget, les infrastructures, et

---

[27] Le paragraphe 41 de l'*ISSAI 100* indique que « le caractère significatif est souvent exprimé en valeur, mais il comporte aussi d'autres aspects quantitatifs et qualitatifs. Les caractéristiques inhérentes d'un élément ou d'un groupe d'éléments peuvent rendre un sujet significatif par sa nature même. Un sujet peut également être significatif en raison du contexte dans lequel il s'inscrit. »

[28] *Materiality Concepts for Auditing Information,* Lignes directrices de l'ISACA (G6).

[29] L'affectation des ressources humaines est appropriée si les collaborateurs retenus sont familiarisés avec les systèmes d'information et sont capables de procéder le cas échéant à une extraction de données et à leur analyse, la réalisation d'un audit informatique nécessitant invariablement l'application de compétences informatiques. L'ISC se

d'autres paramètres qui pourront être identifiés. Si possible, le calendrier de l'audit est défini en consultation avec l'entité auditée.

Ainsi, l'ISC fait en sorte que les membres de l'équipe d'audit possèdent collectivement les compétences nécessaires pour mener à bien la mission d'audit informatique et atteindre les objectifs visés. L'acquisition des connaissances, qualifications et compétences nécessaires peut prendre la forme a) d'actions de renforcement des capacités, notamment par la formation ou l'expérimentation sur le terrain, b) d'un recrutement, c) d'un recours à des ressources externes, conformément au plan stratégique de l'ISC.

L'ISC a le choix entre plusieurs options en ce qui concerne l'affectation des ressources humaines aux missions d'audit informatique. Elle peut :

- mettre en place un groupe central composé de spécialistes des systèmes d'information, qui auraient pour mission d'aider d'autres équipes d'audit de l'ISC à réaliser ces audits ou à déployer des spécialistes des systèmes d'information ;
- mettre en place un groupe ou un service dédié à l'audit informatique, responsable de la réalisation de toutes les missions d'audit informatique pour l'ISC, qui travaillerait en lien avec d'autres équipes connaissant déjà l'entité auditée ;
- associer des auditeurs généralistes possédant des compétences générales en informatique à des auditeurs spécialisés, détenant une expertise plus précise sur un ou plusieurs aspects des systèmes et technologies de l'information;
- affecter à l'équipe d'audit informatique d'autres collaborateurs internes, à titre provisoire.

L'ISC peut confier la réalisation des audits informatiques à des ressources externes, comme des consultants SI, des prestataires, des spécialistes et des experts si les ressources dont elle dispose à l'interne sont limitées, ou si elle juge cette externalisation plus pratique ou plus économique. L'ISC doit s'assurer que les ressources externes auxquelles elle fait appel disposent d'une formation adaptée et connaissent ses exigences en matière de conduite professionnelle, les processus applicables et les livrables attendus d'un audit informatique. Cette mission doit faire l'objet d'un suivi conforme, au moyen d'un contrat documenté, d'un accord sur les niveaux de service ou d'un engagement de non-divulgation. Le respect de la confidentialité par les ressources externes pourra nécessiter une attention particulière, notamment pour ce qui concerne les informations de l'entité auditée.

Dans le cadre de l'audit des systèmes d'information, l'ISC doit veiller à ce que les membres de l'équipe d'audit soient collectivement en capacité de répondre aux impératifs suivants :

- comprendre les éléments techniques du système informatique, ce qui inclut toutes les instances pertinentes de l'application utilisée, afin d'être en mesure d'accéder à l'infrastructure informatique et de l'utiliser pour les besoins du processus d'audit ;
- comprendre la cartographie des processus d'activité dans la logique de programmation du système informatique ;
- comprendre la méthodologie d'audit, ce qui inclut les normes d'audit et les lignes directrices applicables à l'ISC ;
- comprendre le fonctionnement du système d'information, afin d'être en mesure d'obtenir les éléments probants de l'audit par extraction de systèmes automatisés ;
- comprendre les outils de l'audit informatique pour recueillir, analyser et reproduire les résultats de cette analyse, ou pour être en mesure d'exécuter à nouveau les fonctions auditées ;
- comprendre les méthodes d'évaluation et de comparaison des coûts, notamment en ce qui concerne le travail et les ressources nécessaires, ainsi que les avantages attendus du déploiement d'un système informatique ;

---

référera au paragraphe 39 de l'ISSAI 100 pour veiller à ce que ses auditeurs disposent des compétences nécessaires avant d'entreprendre un audit informatique.

- déterminer les avantages, les inconvénients et le risque opérationnel de l'acquisition d'un système d'information et des pratiques et stratégies d'externalisation ;
- déterminer si les objectifs du projet informatique ont été atteints, en examinant plus particulièrement les aspects qualité et périmètre, dans le respect des contraintes de temps et de budget qui avaient été définies ;
- comprendre les services, exigences et cahiers des charges afin de veiller ce que le prestataire sélectionné soit fiable et compétitif, et que les contrats signés avec le prestataire contiennent les éléments essentiels.

En outre, l'ISC peut s'assurer pour les audits financiers que l'équipe d'audit dispose de manière générale d'une expérience suffisante de la réalisation d'un audit des états financiers et possède une bonne compréhension de ces états financiers.

III. Étape 2 : Concevoir un audit informatique

a. Objectifs d'un audit informatique

Les objectifs d'un audit informatique dépendent de nombreux facteurs, comme le type d'audit dans lequel il s'inscrit (audit de la performance, financier ou de conformité), l'entité ou les entités auditée(s), le type d'opérations informatiques auditées, les principaux risques auxquels l'entité est exposée, entre autres facteurs.

L'audit peut par exemple poursuivre les objectifs suivants :

- pour un audit de la performance, contrôler que les ressources informatiques permettent d'atteindre les objectifs opérationnels de façon efficiente et efficace, et que les contrôles pertinents permettent effectivement de prévenir, détecter et corriger les abus, les dépenses excessives et l'inefficacité dans l'utilisation et la gestion des systèmes d'information ;
- pour un audit financier, évaluer les contrôles pertinents qui ont un impact sur la fiabilité des données générées par les systèmes d'information, lesquels ont à leur tour un impact sur les états financiers de l'entité auditée ; ou évaluer les processus nécessaires aux opérations réalisées dans un domaine ciblé, par exemple un système de paye ou un système de comptabilité financière ;
- pour un audit de conformité, vérifier la conformité des processus des systèmes d'information avec la législation, les politiques et les normes applicables à l'entité auditée.

Le périmètre de l'audit informatique peut couvrir des domaines précis du déploiement d'un système d'information, notamment :

- acquisition, développement et déploiement des systèmes d'information,
- exploitation et maintenance,
- gestion des changements,
- gestion des accès,
- sécurité de l'information et continuité de l'activité,
- rapport coût/efficacité des systèmes d'information,
- progiciels de gestion intégrés ou autres systèmes d'information complexes/spécialisés.

Si l'audit informatique est intégré à une mission d'audit plus large, l'ISC doit veiller à ce que l'équipe d'audit, en tant qu'unité cohérente, travaille de façon intégrée pour atteindre l'objectif global de l'audit. Par exemple, pour que l'intégration soit efficace, l'ISC peut envisager :

- de dresser la liste exhaustive des travaux attendus des auditeurs des SI,
- d'établir un protocole de partage d'informations entre les auditeurs des SI et les autres auditeurs,
- d'identifier les systèmes d'information et les objectifs de contrôle qui entrent dans le périmètre de l'audit.

Quand ils ont défini les objectifs de l'audit et l'approche qui sera suivie, les auditeurs des SI formulent habituellement des questions d'audit précises qui guideront le travail d'audit. Ces questions d'audit doivent découler des objectifs généraux de l'audit ; elles sont généralement formulées avec une plus grande précision, et abordent les thèmes que vous entendez décrire ou évaluer au cours de l'audit. Le but est que les questions d'audit couvrent tous les aspects des objectifs d'audit. Les questions d'audit sont soit **descriptives** (elles décrivent un état), soit **évaluatives** (elles évaluent un état par rapport à des critères, normatifs ou analytiques).

b. Périmètre et méthodologie d'un audit informatique

Plusieurs possibilités s'offrent aux auditeurs des SI lorsque leur revient la tâche de déterminer le périmètre d'un audit. La figure 3 recense les questions qui sont généralement examinées à ce stade.

Figure 3 : Éléments à considérer pour délimiter le périmètre d'un audit informatique

Quoi ?	▪ Quelles sont précisément les questions ou les hypothèses examinées ? ▪ Quels sont les principaux processus pertinents pour l'audit ? ▪ Quel sujet considéré fera l'objet d'une évaluation et d'un rapport ? ▪ Quelles sont les ressources disponibles pour réaliser l'audit ?
Qui ?	▪ Quelles agences et organisations peuvent avoir des responsabilités ou des points de vue pertinents pour l'audit ? ▪ Au sein des agences et organisations concernées, qui est le mieux placé pour fournir des éléments probants suffisants et appropriés pour répondre aux questions d'audit ?
Où ?	▪ Quels sites faut-il couvrir ? ▪ Quels documents et enregistrements faut-il examiner ?
Quand ?	▪ Quelle période faut-il couvrir ?

Source : Équipe de développement IDI/Sous-commission à l'audit de performance

Remarque : cette figure propose un exemple qu'il convient d'adapter à la mission d'audit abordée.

Très souvent, l'auditeur des SI est amené à évaluer les politiques et procédures qui servent à orienter l'environnement informatique global de l'entité auditée, en vérifiant que les contrôles et mécanismes de mise en œuvre correspondants sont bien en place. Définir le périmètre de l'audit informatique implique de déterminer quel sera le niveau de détail des vérifications réalisées pendant l'audit, quels seront les systèmes d'information couverts et quelles fonctionnalités de ces systèmes, quels processus informatiques seront audités, quels sites d'implantation des systèmes d'information seront couverts, y compris les sites hébergés par des tiers, par exemple les prestataires de services Cloud ou autres services externalisés, dont les environnements de contrôle font partie de l'environnement de contrôle de l'entité auditée, et sur quelle période portera l'audit[30].

Lors de la définition du périmètre de la mission d'audit informatique, l'ISC peut choisir la période sur laquelle l'audit portera (par exemple 1 an ou 3 ans). Certains audits peuvent également avoir pour contrainte une date d'achèvement précise. La période retenue doit être pertinente au vu des objectifs définis pour la mission d'audit.

Une fois le périmètre de l'audit délimité, l'équipe d'audit informatique précise la méthodologie ou les étapes qu'elle compte suivre pour atteindre les objectifs de l'audit, dans le respect du périmètre. En

[30] Les sites d'implantation sont notamment les serveurs dorsaux (serveurs d'applications ou de données), les sites d'utilisation, ainsi que les réseaux de manière générale. Lorsque le réseau est distribué entre différents bâtiments, différentes villes, voire différents pays, il conviendra aussi, le cas échéant, de déterminer les sites physiques qui seront couverts.

précisant les détails de la méthodologie, elle s'assure que les étapes qu'elle prévoit de suivre sont cohérentes au vu des données qu'elle prévoit de recueillir, qu'aucune étape n'est superflue, et que les résultats des différentes étapes permettront à l'équipe de formuler une opinion quant aux objectifs d'audit.

L'entité auditée doit être tenue informée du périmètre et des objectifs de l'audit ; elle pourra participer si nécessaire au choix des critères d'évaluation retenus pour l'audit. Le cas échéant, l'ISC peut préciser dans la lettre de mission à l'entité auditée les conditions de réalisation de la mission.

c. Contrôles informatiques généraux et contrôles d'application

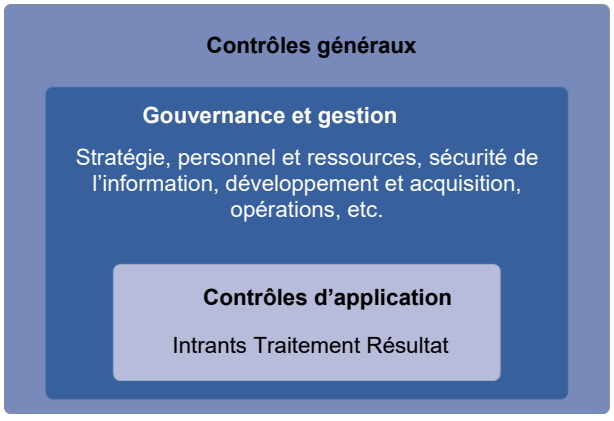
Comme indiqué précédemment, on entend par audit informatique l'examen des contrôles associés aux systèmes d'information, dans l'objectif d'identifier les écarts éventuels par rapport aux critères définis. On entend par **contrôles** les processus, outils et autres mécanismes de supervision en place pour gérer les fonctions informatiques et éviter les risques et vulnérabilités. Les contrôles évalués dans le cadre d'un audit informatique dépendent de l'objectif et du périmètre de l'audit.

Les contrôles sont mis en place pour atténuer les risques auxquels l'entité est exposée. On distingue plus particulièrement différents types de risques ciblés par les contrôles d'un audit informatique :

- Le **risque de contrôle** désigne la probabilité que les contrôles informatiques que l'entité auditée a mis en place échouent à atténuer les conséquences négatives qu'ils étaient censés traiter. Par exemple, un système d'information tenu d'assurer que l'accès à des données confidentielles est réservé aux seules personnes autorisées peut comporter un contrôle exigeant de toute personne tentant d'accéder aux données la saisie d'un nom d'utilisateur et d'un mot de passe. En pareil cas, le risque de contrôle est que le nom d'utilisateur et le mot de passe ne soient pas suffisamment sécurisés, et qu'une personne non autorisée puisse les deviner en multipliant les essais. Il peut en résulter une perte de confidentialité avec des conséquences potentiellement défavorables pour l'entité. Pour une organisation recommandant fortement l'utilisation de mots de passe complexes et sécurisés comportant une combinaison de caractères alphabétiques, numériques et spéciaux, dont le système d'information empêche l'accès à l'identifiant (nom d'utilisateur) au-delà d'un nombre défini de tentatives d'accès, le risque de contrôle est plus faible que pour une organisation n'ayant pas mis en place de telles exigences. Le recours à l'authentification multi-facteurs peut également contribuer à réduire le risque de contrôle dans cette configuration.
- Le **risque de non détection** désigne la probabilité que l'auditeur ne détecte pas l'absence, la défaillance ou le caractère inadapté des contrôles informatiques mis en place par une organisation, cette situation pouvant avoir des conséquences défavorables pour l'organisation.
- Le **risque résiduel** désigne le niveau de risque restant une fois les contrôles appliqués, risque qu'il est possible de réduire encore grâce à une identification des domaines dans lesquels davantage de contrôles sont nécessaires. La direction de l'organisation peut déterminer le niveau de risque cible qu'elle considère comme acceptable (son « appétence pour le risque »).

Dans le contexte d'un système d'information, les contrôles sont répartis en deux catégories, illustrées à la figure 4 : les contrôles généraux et les contrôles d'application. L'affectation d'un contrôle à l'une ou l'autre des catégories dépend de sa portée et de son lien éventuel avec une application en particulier.

Figure 4 : Contrôles généraux et contrôles d'application



Source : Unknown.

Les **contrôles informatiques généraux** sont la base de la structure de contrôle du système d'information. Ces contrôles concernent l'environnement général de développement, d'exploitation, de gestion et de maintenance des systèmes informatiques. Les contrôles généraux sont des procédures manuelles ou

automatisées, qui visent à assurer la confidentialité, l'intégrité et la disponibilité des informations dans l'environnement physique du développement, de la maintenance et de l'exploitation des systèmes d'information. Les contrôles généraux établissent un cadre global pour le contrôle des activités du SI, et fournissent l'assurance que les objectifs d'ensemble du contrôle sont atteints.

Les contrôles généraux sont déployés au moyen de différents outils, dont les politiques, lignes directrices et procédures. Leur déploiement est associé à la mise en œuvre d'une structure de gestion appropriée, notamment pour la gestion des systèmes d'information de l'organisation. Relèvent notamment des contrôles informatiques généraux l'élaboration et la mise en œuvre d'une stratégie et d'une politique de sécurité relatives aux technologies de l'information, la mise en place d'un comité de pilotage des systèmes d'information, l'organisation du personnel informatique dans le but d'éviter les conflits de responsabilité, la mise en place de rôles et privilèges associés au système correspondant aux fonctions de la personne, ou encore l'établissement de plans de prévention des sinistres et de récupération après sinistre.

Les contrôles informatiques généraux ne sont pas associés spécifiquement à un flux d'opérations, à un progiciel de comptabilité ou à des applications financières en particulier. L'objectif des contrôles informatiques généraux consiste à assurer le développement et le déploiement conformes des applications, des programmes et des fichiers de données, ainsi que des activités informatiques.

Les **contrôles d'application** en revanche sont des contrôles spécifiques, associés aux systèmes d'information de chaque application. Au sein d'un système d'information, les contrôles d'application sont des procédures manuelles ou automatisées, selon les technologies de l'information en place, qui affectent le traitement des opérations et peuvent concerner la validation des données saisies, la précision du traitement des données, la livraison des données générées en sortie, mais aussi l'intégrité des données permanentes. Ces contrôles concernent les segments applicatifs, et sont liés aux opérations et aux données existantes. Par exemple, pour une application de paiement en ligne, un contrôle de saisie pourrait consister à vérifier que la date d'expiration de la carte de crédit est ultérieure à la date de l'opération, et que les informations saisies sont chiffrées.

La conception et le déploiement des contrôles informatiques généraux peuvent avoir un impact significatif sur l'efficacité des contrôles d'application. Les contrôles généraux apportent aux applications les ressources dont elles ont besoin pour fonctionner et veillent à ce qu'aucune requête ni aucune modification non autorisée ne puisse être effectuée relativement aux applications (autrement dit, les applications sont protégées contre la reprogrammation) ou aux données sous-jacentes (par exemple, les importants volumes de données des transactions).

Les éléments critiques des contrôles généraux au niveau des applications sont[31] :

- la gestion de la sécurité,
- le contrôle d'accès/la séparation des accès utilisateurs,
- la gestion des configurations/des modifications,
- la gestion des opérations,
- le plan de secours ou d'urgence.

Les contrôles d'application s'exercent sur des opérations ou groupes d'opérations, et sont utilisés pour veiller à la conformité de leur saisie, de leur traitement, et de leur résultat. L'efficacité de la conception et du fonctionnement des contrôles informatiques généraux détermine dans une large mesure la confiance que la direction de l'organisation peut placer dans les contrôles d'application pour gérer les risques.

[31] U.S. Government Accountability Office, *Federal Information System Controls Audit Manual (FISCAM),* GAO-09-232G, (2 février 2009), https://www.gao.gov/products/gao-09-232g.

d. Pourquoi les contrôles informatiques sont-ils importants pour l'auditeur des SI ?

On fait généralement appel à un auditeur des SI pour qu'il teste les contrôles associés aux outils technologiques de l'organisation. À mesure que les organisations sont plus nombreuses à s'appuyer sur les technologies de l'information pour automatiser leurs activités, les différences de rôle entre un auditeur spécialisé dans les SI et un auditeur généraliste sont de moins en moins marquées. Tous les auditeurs doivent au minimum être capables de comprendre l'environnement de contrôle de l'entité auditée, afin de pouvoir fournir une assurance concernant le bon fonctionnement des contrôles internes de l'organisation. Les Principes fondamentaux du contrôle des finances publiques définis dans les ISSAI indiquent que « les auditeurs doivent acquérir une connaissance de la nature de l'entité/du programme à contrôler »[32]. Cette connaissance implique de comprendre les contrôles internes, mais également les objectifs, les opérations, le cadre réglementaire, les systèmes et les processus d'activité en jeu.

Chaque aspect du contrôle s'appuie sur un ensemble d'objectifs de contrôle, qu'une organisation définit pour atténuer un risque de contrôle, et prend en considération les contraintes techniques des systèmes de l'organisation. Le rôle de l'auditeur consiste à comprendre les risques opérationnels et informatiques auxquels l'entité auditée est susceptible d'être exposée, puis d'évaluer si les contrôles déployés permettent effectivement d'atteindre l'objectif de contrôle. En ce qui concerne les contrôles informatiques généraux, il est important que l'auditeur ait identifié les grandes catégories et l'ampleur des contrôles généraux en place, qu'il évalue le degré de surveillance par la direction et la sensibilisation du personnel de l'organisation aux problématiques considérées, et enfin qu'il détermine dans quelle mesure les contrôles sont efficaces afin de pouvoir fournir une assurance. Une insuffisance des contrôles généraux peut dégrader de façon significative la fiabilité des contrôles associés à chacune des applications informatiques.

Dans les chapitres suivants, notamment le chapitre 8 sur les contrôles d'application, nous verrons plus en détail certains des aspects clés des contrôles informatiques généraux et des contrôles d'application.

IV. Étape 3 : Réaliser un audit informatique

La réalisation d'un audit informatique est jalonnée par des étapes clés : la collecte d'éléments probants qui soient suffisants, appropriés, pertinents et fiables, la réalisation d'une première évaluation des contrôles, portant notamment sur les politiques et les procédures dans le but d'en évaluer la fiabilité, et des tests de validation des aspects prioritaires, permettant d'apprécier le degré d'efficacité du fonctionnement d'un contrôle.

a. Collecte d'éléments probants

i. Éléments probants

Les constatations d'audit doivent être étayées par des éléments probants, aussi est-il important de recueillir des preuves suffisantes, autant sur le plan quantitatif que sur le plan qualitatif. L'auditeur des SI doit donc considérer et évaluer en continu le caractère suffisant et approprié des éléments probants qu'il prévoit d'obtenir ou qu'il a déjà obtenus. Le caractère suffisant renvoie à la quantité des éléments probants recueillis. Le caractère approprié renvoie à la qualité des éléments probants, et qualifie leur fiabilité et leur pertinence. Les auditeurs peuvent déterminer si un élément probant est pertinent et fiable en examinant, entre autres choses, la nature et la réputation de la source de l'élément recueilli, les contrôles mis en place par l'entité auditée, la présence d'éléments contradictoires ou confirmatoires, ainsi que les méthodes, les modèles et les hypothèses retenus pour établir les informations consignées dans l'élément probant.

[32] Organisation internationale des Institutions supérieures de contrôle des finances publiques, *ISSAI 100,* paragraphe 45.

Il existe un outil pratique pour évaluer les éléments probants de l'audit, formuler des conclusions et les recommandations : la matrice des constatations d'audit. Grâce à cet outil, l'auditeur peut déterminer si ses constatations et ses recommandations s'appuient, le cas échéant, sur des preuves suffisantes et appropriées. La figure 5 propose un modèle type de matrice des constatations d'audit[33].

Figure 5 : Modèle de matrice des constatations d'audit

Objectif d'audit : indiquez en quoi l'audit consiste, de façon précise et objective.
Question d'audit (celle que vous avez formulée dans la matrice de conception) : pour chaque question d'audit (ou sous-question), reprenez chacun des éléments du tableau suivant.

Constatation	**Énoncé de la constatation (situation observée)**	Occurrences les plus pertinentes relevées à l'occasion du travail de terrain.
	Critères	Informations utilisées pour déterminer si la performance attendue de l'objet audité est satisfaisante, dépasse les attentes ou s'avère insuffisante.
	Éléments probants et analyse	Résultat de l'application des méthodes d'analyse des données ou de l'évaluation de vos éléments probants. Vous pouvez préciser quelles techniques ont été utilisées pour traiter les informations collectées pendant le travail de terrain et quels résultats ont été obtenus.
	Causes	Raisons de la situation observée. Peut être relié au fonctionnement ou à la conception de l'objet audité. Le dirigeant peut n'avoir aucun contrôle sur ces causes. Les recommandations éventuelles doivent être reliées aux causes.
	Effets	Conséquences liées aux causes et aux éléments probants correspondants. Peut constituer une mesure de la pertinence de la constatation.
Les éléments probants sont-ils suffisants (O/N) et sinon, quel travail supplémentaire faudrait-il fournir pour traiter les lacunes éventuelles ?		Étudiez chaque élément probant dont vous disposez pour les différents aspects de la constatation, et déterminez s'il est suffisant et approprié. Si vos éléments probants ne sont pas suffisants, quel travail supplémentaire faudrait-il fournir pour traiter les lacunes éventuelles ?
Bonnes pratiques		Actions identifiées comme contribuant à des performances satisfaisantes. Peuvent être utilisées pour étayer vos recommandations.
Recommandations		Propositions pour traiter les causes (ou les lacunes) identifiées.

Source : adapté du GAO (États-Unis) et de l'ISC du Brésil.

Remarque : ce tableau propose un processus type qu'il convient d'adapter à la mission d'audit abordée.

ii. Phase 1 - évaluation initiale des contrôles informatiques

L'auditeur doit procéder à une première analyse des contrôles informatiques (contrôles généraux et contrôles d'application) du système, pour s'assurer qu'ils sont fiables et suffisants pour atteindre l'objectif d'audit.

[33] Le Guide de mise en œuvre des ISSAI relatives à l'audit de la performance, publié par l'Organisation internationale des Institutions supérieures de contrôle des finances publiques, version 1 (août 2021), propose à la page 180 un exemple de matrice des constatations d'audit complétée : https://www.idi.no/work-streams/professional-sais/work-stream-library/performance-audit-issai-implementation-handbook.

Le périmètre de cette analyse des contrôles informatiques peut couvrir les questions suivantes :

- A-t-on défini, adopté et communiqué une politique des SI ?
- Existe-t-il une structure de gouvernance des technologies de l'information, et est-elle opérationnelle ?
- Les contrôles reflètent-ils avec exactitude les contraintes techniques des systèmes d'information sous-jacents ?
- A-t-on réalisé périodiquement un inventaire des actifs du système d'information, et a-t-on identifié sur ce plan des besoins d'accroissement, de remplacement ou de retrait ?
- A-t-on mis en place des procédures fonctionnelles pour partager les infrastructures et les services communs des systèmes d'information avec d'autres organismes du secteur public ?
- A-t-on défini, adopté et communiqué des procédures encadrant le développement, l'acquisition et la maintenance des outils informatiques (notamment en ce qui concerne la gestion des changements ?
- A-t-on défini, adopté et communiqué des procédures encadrant les activités informatiques (internalisation, externalisation et accords sur les niveaux de service) ?
- A-t-on pris des mesures pour garantir la sécurité physique et le maintien des conditions de travail physiques souhaitées ?
- A-t-on pris des mesures de formation et de sensibilisation des équipes au maintien de la confidentialité, de l'intégrité et de la disponibilité de l'information, mais aussi à la conformité avec les exigences de la politique relative au système d'information et de la structure de gouvernance ?
- A-t-on pris des mesures pour assurer la confidentialité, l'intégrité et la disponibilité des différents modes et canaux de communication ?
- A-t-on pris des mesures pour gérer la conformité avec la réglementation ?
- A-t-on pris des mesures pour gérer la continuité de l'activité et la reprise après sinistre ?
- A-t-on pris des mesures pour assurer le caractère complet, précis, valide et confidentiel des données et des transactions réalisées dans le cadre des processus d'activité ?
- A-t-on pris des mesures pour assurer le traitement ponctuel, précis et complet des informations par les différents éléments du système, notamment entre applications ?

En fonction de l'objectif d'audit, les auditeurs pourront être amenés à examiner la conception, le déploiement et l'efficacité opérationnelle des contrôles. Pour étudier la conception d'un contrôle, l'auditeur pourra réaliser un entretien, ou un examen documentaire des règles opérationnelles. Si l'auditeur étudie le déploiement des contrôles, poser des questions pourra ne pas suffire, et il pourra s'avérer nécessaire de réaliser une visite guidée sur site (technique d'audit servant à valider la bonne compréhension des contrôles) ou une analyse de données, afin de s'assurer que les contrôles ont effectivement été déployés. Enfin, si l'auditeur étudie l'efficacité opérationnelle des contrôles, il pourra avoir à prévoir un test aléatoire sur des transactions, afin d'apporter la preuve que le contrôle a effectivement fonctionné sur l'ensemble de la période considérée.

Les auditeurs peuvent également examiner dans quelle mesure les éléments probants associés aux contrôles généraux ont un impact sur la nature, la séquence et l'étendue des procédures et sur les preuves qu'il est nécessaire de recueillir pour obtenir une assurance concernant le bon fonctionnement des contrôles d'application. Par exemple, les auditeurs devraient examiner également des éléments probants démontrant les conditions d'accès logique du personnel aux systèmes informatiques et la gestion des modifications dans l'environnement de production Si les auditeurs ont obtenu des éléments probants suffisants et appropriés concernant l'efficacité des contrôles généraux, ils pourront être en mesure de formuler une opinion quant à l'efficacité opérationnelle des procédures automatisées de contrôle d'application. Dans ce cas, les auditeurs doivent tester un échantillon de transactions plus réduit, l'efficacité de l'environnement informatique général apportant la preuve de l'efficacité du contrôle d'application sur la période considérée. Si les procédures de contrôle d'application sont manuelles, les auditeurs devront sélectionner une taille d'échantillon adaptée au niveau de confiance retenu.

iii. Phase 2 - tests de validation

À partir de l'évaluation des contrôles informatiques, les auditeurs peuvent identifier des domaines prioritaires pour l'exécution de tests de validation. Cette étape consiste à soumettre les contrôles informatiques à des tests détaillés, au moyen de différentes techniques d'interrogation, d'extraction et d'analyse des données. En phase de validation, les tests sont conçus pour corroborer les hypothèses formulées au vu des objectifs d'audit.

Les auditeurs des SI utilisent différentes techniques pour analyser les données : les rapports par exception, qui documentent les écarts par rapport aux performances attendues ; la comparaison de fichiers ; la stratification ; le tri d'éléments de données en catégories distinctes ; l'échantillonnage ; la double vérification. Une autre possibilité pour tester une solution système consiste à examiner un processus opérationnel à la fois, afin d'identifier les principaux points d'activité et de s'assurer que des contrôles informatiques pertinents et adéquats ont été mis en place pour chacun de ces points. Les auditeurs des SI doivent avoir connaissance de ces différentes possibilités et utiliser l'outil adapté à l'analyse qu'ils souhaitent effectuer. Ils peuvent analyser les informations à l'aide d'un logiciel d'audit généraliste ou spécialisé.

Pour procéder aux tests de validation, les auditeurs des SI doivent s'assurer qu'ils ont recueilli et documenté des preuves électroniques suffisantes, fiables et précises, qui leur permettront d'étayer les observations de l'audit. Ces preuves électroniques peuvent être des fichiers de données, des fichiers de journalisation des utilisateurs, des modèles d'analyse, ou encore des rapports générés à partir des systèmes d'information à l'attention de la direction. Il est important de rassembler et de conserver ces éléments selon une méthode appropriée, garantissant leur disponibilité en vue de la formulation d'une assurance quant à la précision et à la validité du processus d'audit.

L'auditeur des SI doit également sélectionner une méthodologie d'évaluation du risque et appliquer des techniques d'échantillonnage lui permettant de tirer des conclusions pertinentes, sur le fondement d'éléments statistiques suffisants issus de données limitées. Une bonne pratique consiste généralement à faire appel à un expert ou statisticien travaillant dans l'organisation, qui pourra contribuer à choisir et définir une méthode d'échantillonnage adaptée.

Lorsque le volume de données, les capacités de transfert, de stockage et de traitement le permettent, l'auditeur pourra réaliser une évaluation du risque de grande qualité sur l'intégralité de la population, afin d'identifier des tendances corroborant la compréhension que l'auditeur a acquis de l'activité. L'auditeur pourrait par exemple obtenir une liste de tous les utilisateurs, précisant la date de leur dernière connexion au système, et la comparer à une liste des dates de départ officiel pour assurer une analyse à 100 %. Cette méthode lui permettrait d'identifier les anomalies éventuelles concernant les transactions ou les points de données, afin de constituer une partie de l'échantillon en ciblant davantage le risque.

b. Communication avec l'entité auditée

Les ISSAI recommandent aux auditeurs d'établir avec l'entité auditée une communication efficace tout au long du processus d'audit et de la tenir informée de toute question concernant l'audit[34]. Pour un audit informatique, les auditeurs peuvent solliciter la coopération et le soutien actif de l'entité auditée aux fins de la réalisation de l'audit, notamment en facilitant l'accès aux dossiers et aux informations. Les auditeurs peuvent déterminer en consultation avec l'entité auditée le mode d'accès aux données électroniques sous un format permettant leur analyse. Ce mode d'accès aux données serait spécifique à l'ISC.

c. Documenter un audit informatique

La documentation d'un audit des systèmes d'information comprend l'enregistrement du travail d'audit

[34]Organisation internationale des Institutions supérieures de contrôle des finances publiques, *ISSAI 100*.

réalisé et les éléments probants qui étayent les constatations et les conclusions de l'audit. Il est important que les auditeurs des SI assurent la préservation des résultats et des éléments probants, qui doivent être fiables, complets, suffisants et exacts. Les auditeurs doivent également assurer la traçabilité du processus d'audit, afin de permettre la vérification ultérieure des procédures d'analyse. Cette exigence met en jeu l'application de différentes techniques de documentation.

La documentation consiste à enregistrer :

- la planification et la réparation du périmètre et des objectifs de l'audit ;
- les programmes d'audit ;
- les éléments probants recueillis, sur lesquels s'appuient les conclusions formulées ;
- tous les documents de travail, y compris les fichiers d'ordre général relatifs à l'organisation et au système ;
- les points abordés à l'occasion des entretiens, en indiquant clairement le thème de la discussion, la personne interrogée, son titre et ses fonctions, le lieu et l'heure de l'entretien ;
- les remarques de l'auditeur observant l'exécution d'un travail :
  - les remarques doivent préciser au minimum le lieu et l'heure de l'observation, le motif et les personnes concernées ;
- les rapports et les données que l'auditeur a directement extraits du système ou qui lui ont été fournis par le personnel de l'entité auditée :
  - l'auditeur des SI doit veiller à ce que ces rapports indiquent la source du rapport, la date et l'heure, mais également les conditions couvertes par le rapport ;
  - la capture d'écran est une possibilité pour consigner ces détails ;
- les commentaires ou précisions insérés par les auditeurs à différents moments dans la documentation, concernant une question, un doute, un besoin d'informations complémentaires :
  - l'auditeur reviendra plus tard sur ses commentaires et pourra y adjoindre des remarques ou des références indiquant comment et en quelles circonstances les problèmes soulevés ont été résolus.

Les preuves recueillies à l'occasion d'un audit informatique peuvent être horodatées et accompagnées d'informations détaillées concernant les étapes de l'analyse des données effectuée, pour assurer la traçabilité de la création, du stockage et de la dernière modification de l'élément probant, afin d'atténuer le risque d'une modification ultérieure. La figure 6 propose différents exemples de ce qu'un auditeur des SI peut attendre de la documentation d'audit.

Figure 6 : Comprendre la documentation d'un audit informatique

Quelles informations l'auditeur expérimenté peut-il espérer tirer de la documentation d'audit ?	
✓ La nature, la date et l'étendue du travail réalisé. ✓ Les constatations du travail d'audit et les éléments probants obtenus. ✓ Les questions significatives soulevées par l'audit (par exemple, modifications du périmètre de l'approche de l'audit, décisions concernant un nouveau facteur de risque identifié pendant l'audit, mesures prises à la suite d'un désaccord entre l'entité auditée et l'équipe d'audit, etc.). ✓	✓ Les conclusions formulées en réponse à ces questions significatives. ✓ Les décisions importantes ou essentielles prises pour parvenir à ces conclusions.

Source : Équipe de développement IDI/Sous-commission à l'audit de performance

Remarque : Cette figure propose un exemple qu'il convient d'adapter à la mission d'audit abordée.

Comme toute documentation d'audit, la documentation d'un audit informatique doit être conservée et

protégée contre toute modification ou suppression non autorisée. L'ISC peut définir de nouvelles pratiques de référence pour la conservation de la documentation de l'audit informatique ou adapter les normes existantes pour satisfaire aux exigences de conservation de la documentation liée à l'audit informatique. La durée de conservation dépend du mandat de l'ISC et du cadre réglementaire et législatif de ses activités. On accordera une attention particulière au support, au format, à la durée de vie attendue et aux exigences de stockage des données pour garantir que les données pourront être lues sur l'ensemble de la période définie dans la politique de conservation et d'archivage des données de l'ISC. Peut-être faudra-t-il convertir les données d'un format vers un autre, pour tenir compte des avancées technologiques et de l'obsolescence.

En ce qui concerne l'examen de rapports techniques établis par des auditeurs tiers portant sur des sujets technologiques spécifiques, les auditeurs peuvent mettre en place des procédures adaptées pour assurer la fiabilité de certains aspects relatifs à la performance, à la gestion financière ou à la conformité. Si ces procédures permettent d'établir la fiabilité du contenu des rapports techniques, il convient d'indiquer clairement que ces rapports ont été utilisés.

En ce qui concerne la préservation des données électroniques, l'ISC doit assurer la sauvegarde des données transmises par l'entité auditée, mais également du résultat des requêtes et du travail d'analyse. La documentation d'audit doit rester confidentielle et être conservée pendant la durée définie par l'ISC ou imposée par la loi. L'ébauche et la version finale du rapport d'audit font partie intégrante de la documentation d'audit. Si le travail d'audit fait l'objet d'une revue par un pair ou un supérieur hiérarchique, les remarques résultant de ce travail de revue doivent également être consignées dans la documentation.

d. Examen par un superviseur

Il est important d'organiser la supervision du travail de l'équipe d'audit, pendant l'audit, et de soumettre les travaux documentés à l'examen d'un membre assurant une fonction d'encadrement de l'équipe d'audit[35]. Ce membre responsable du personnel d'audit doit également fournir au cours de l'audit les orientations et la formation nécessaires, et assurer un rôle de mentor.

V. Étape 4 : Présenter les résultats d'un audit informatique

Le rapport d'audit informatique adopte la présentation générale habituellement suivie par l'ISC. Le niveau de détail des éléments présentés dans le rapport d'audit informatique correspond aux attentes des destinataires du rapport.

L'auditeur des SI fait en temps utile un compte rendu constructif de ses constatations, afin que celles-ci puissent être utiles à l'entité auditée et présentent un intérêt pour les autres parties prenantes. Il est possible que le rapport soit soumis aux autorités compétentes, en fonction du mandat de l'ISC et de la nature de la mission d'audit informatique.

Les auditeurs doivent s'efforcer de limiter le recours au jargon technique et garder à l'esprit le caractère sensible des informations présentées dans le rapport (notamment, les mots de passe, noms d'utilisateurs et informations personnelles). Si l'audit informatique est un travail technique par nature, les auditeurs doivent faire en sorte que leur rapport puisse être compris sans difficulté par la direction de l'entité auditée, les parties prenantes et le grand public. Il est donc important que les auditeurs des SI aient conscience que leurs rapports s'adressent autant à d'autres experts des technologies de l'information qu'au grand public, et qu'il leur faut expliciter les aspects techniques pour cette dernière catégorie de lecteurs.

[35] Organisation internationale des Institutions supérieures de contrôle des finances publiques, *ISSAI 100,* paragraphes 38, 39 et 50.

Les auditeurs doivent prendre en considération les conséquences potentiellement négatives de la publication du rapport. Par exemple, si le rapport d'audit informatique pointe des failles de sécurité dans le système d'information de l'entité auditée et si ces failles sont révélées avant que l'entité ait pu mettre en place les contrôles nécessaires pour atténuer le risque, la vulnérabilité du système d'information pourrait être exposée au public. En pareilles circonstances, les auditeurs peuvent envisager différentes possibilités : ne publier les résultats qu'après que les contrôles nécessaires ont été mis en place, ne pas révéler précisément tous les aspects de la faille de sécurité afin d'éviter un impact potentiellement négatif pour l'entité auditée, ou encore rédiger un rapport confidentiel distinct/annexé n'ayant pas vocation à être largement diffusé.

L'annexe II propose différents rapports d'audit identifiés par des ISC du monde entier, en lien avec les chapitres de ce manuel. Ces rapports d'audit illustrent avec pertinence le large spectre des domaines de l'audit informatique abordés dans le présent manuel.

a. Les étapes de la présentation des résultats

Les modalités de présentation des résultats de l'audit informatique dépendent des habitudes de l'ISC et de son environnement juridique. Le travail de présentation des résultats accompagne le processus d'audit et comprend différentes étapes :

i. Ébauche de rapport

La présentation des résultats commence avec les échanges concernant la rédaction d'une première ébauche de rapport. Cette ébauche, une fois validée en interne au sein de l'ISC, est transmise à la direction de l'entité auditée avant la réunion de clôture. L'ébauche fait généralement partie des sujets abordés à l'occasion de la réunion de clôture. Cette étape permet d'identifier, de corriger ou d'éliminer en amont les formulations maladroites potentiellement source de conflits, des erreurs factuelles ou des incohérences. Après que l'entité auditée et l'auditeur se sont mis d'accord sur le contenu de l'ébauche, l'auditeur procède aux modifications nécessaires et transmet à l'entité auditée un projet de rapport officiel.

ii. Courrier à la direction

Le courrier à la direction officialise la remise à l'entité auditée du projet officiel de rapport, qui vise à offrir à l'intéressée la possibilité de réagir aux observations formulées. La direction de l'entité peut ainsi examiner les constatations, les conclusions et les recommandations de l'ébauche de rapport qui lui a été communiquée. À ce stade, il revient à la direction de répondre officiellement par écrit aux remarques de l'auditeur et de traiter toutes les constatations du rapport.

iii. Version finale du rapport d'audit

Quand il reçoit les commentaires de l'entité auditée, l'auditeur prépare une réponse faisant état de sa position relative à l'audit. Pour y parvenir, il confronte les remarques de l'auditeur et la réponse de l'entité auditée. Il obtient alors la version finale du rapport d'audit.

En rendant compte des irrégularités ou des non-conformités avec la législation ou la réglementation, les auditeurs doivent faire en sorte de remettre leurs constatations en contexte. Le constat d'une irrégularité peut être établi, sans considération de la qualification de l'opinion de l'auditeur.

Par nature, le rapport d'audit tend à présenter des critiques qui peuvent être significatives. Toutefois, pour que le travail soit constructif, le rapport doit également mentionner les actions qui permettront d'y remédier, en intégrant des déclarations de l'entité auditée ou de l'auditeur, notamment dans les conclusions ou les recommandations[36]. Selon l'ISC, les principaux destinataires du rapport à la direction

[36] Organisation internationale des Institutions supérieures de contrôle des finances publiques, *ISSAI 100,* paragraphe 51.

peuvent être les personnes responsables de la gestion des opérations de l'entité ou les personnes responsables de la supervision des orientations stratégiques de l'entité et de ses obligations de transparence.

Si l'audit comporte un volet relatif aux technologies de l'information, le résultat de l'audit informatique peut dans certains cas être communiqué à l'organisation dans un courrier séparé. Dans ce cas, il peut être important d'expliquer le lien entre le résultat du travail d'audit informatique et les autres communications transmises dans le cadre plus large de l'audit de la performance, financier ou de conformité réalisé, et dans quelle mesure les résultats de l'audit informatique peuvent être pertinents pour le rapport d'audit correspondant de l'ISC.

iv. Formulation des conclusions et recommandations

Les constatations, les conclusions et les recommandations de l'audit doivent s'appuyer sur des éléments probants. Pour formuler ses conclusions, l'auditeur des SI se doit de considérer le caractère significatif de l'élément examiné et de le replacer dans le contexte de la nature de l'audit ou de l'entité contrôlée[37]. Pour que le rapport soit équilibré, il est important d'y consigner également les réussites notables de l'entité et qui relèvent du mandat de l'ISC.

Les auditeurs des SI doivent tirer leurs conclusions des constatations, en gardant à l'esprit les objectifs de l'audit. Ces conclusions doivent être pertinentes, logiques et impartiales. L'auditeur doit s'efforcer d'éviter les conclusions à l'emporte-pièce concernant l'absence de contrôle et les risques, dès lors qu'elles ne sont pas étayées par des tests de validation, notamment par des tests des contrôles.

Les auditeurs des SI ajoutent des recommandations à leur rapport si les constatations montrent qu'il existe un potentiel d'amélioration significative des opérations et de la performance. Les auditeurs doivent également rendre compte des constatations et recommandations significatives de précédents audits pour lesquelles aucune action correctrice n'a encore été prise, et qui ont un impact sur les objectifs de l'audit actuel. Les recommandations constructives peuvent favoriser les améliorations. Les recommandations les plus constructives sont axées sur le traitement de la cause des problèmes identifiés, elles préconisent une action et sont spécifiques, adressées aux parties qui ont autorité pour agir, elles sont réalisables et rentables.

v. Limitations et contraintes de l'audit informatique

Il est important que le rapport pointe également les limites auxquelles le travail d'audit informatique a été soumis. Ces limites sont habituellement un accès inadéquat aux données et aux informations, un manque de documentation pertinente sur les processus informatiques, et le fait que l'auditeur des SI soit amené à concevoir ses propres méthodes d'enquête et d'analyse pour parvenir à des conclusions. Le rapport doit également mentionner toute autre limitation ou contrainte que l'auditeur des SI a rencontrée, et qui a influencé le périmètre ou l'exécution du travail d'audit.

vi. Réponse de la direction de l'entité

Il est extrêmement important que l'entité contrôlée réponde aux observations formulées dans le rapport d'audit informatique. Il convient d'organiser des réunions entre les auditeurs des SI et la haute direction de l'entité contrôlée, et de documenter les réponses qui sont apportées. Si cette concertation n'aboutit pas, les auditeurs doivent consigner à titre de preuve les démarches réalisées et en faire état dans leur rapport.

---

[37] Organisation internationale des Institutions supérieures de contrôle des finances publiques, *ISSAI 100,* paragraphe 50.

VI. Références et lectures complémentaires

Communauté des praticiens de l'audit interne. *Risk Assessment in Audit Planning*. https://www.pempal.org/sites/pempal/files/event/attachments/cross_day-2_4_pempal-iacop-risk-assessment-in-audit-planning_eng.pdf. Avril 2014.

Initiative de développement de l'Organisation internationale des Institutions supérieures de contrôle des finances publiques. *Initiative de développement de l'INTOSAI (IDI). AFROSAI/E- Matériel pédagogique pour l'audit informatique.*

Initiative de développement de l'Organisation internationale des Institutions supérieures de contrôle des finances publiques. *Guide de mise en œuvre des ISSAI relatives à l'Audit de la performance,* version 1. *https://www.idi.no/elibrary/professional-sais/issai-implementation-handbooks/handbooks-french/1036-performance-audit-issai-implementation-handbook-version-0-french/file.* Août 2021.

Organisation internationale des Institutions supérieures de contrôle des finances publiques. *Normes internationales des Institutions supérieures de contrôle des finances publiques, ISSAI) 100 : Principes fondamentaux du contrôle des finances publiques.* 2019.

Organisation internationale des Institutions supérieures de contrôle des finances publiques. *Normes internationales des Institutions supérieures de contrôle des finances publiques, ISSAI) 200 : Principes fondamentaux de l'audit financier.* 2019.

Organisation internationale des Institutions supérieures de contrôle des finances publiques. *Normes internationales des Institutions supérieures de contrôle des finances publiques, ISSAI) 300 : Principes fondamentaux de l'audit de la performance.* 2019.

Organisation internationale des Institutions supérieures de contrôle des finances publiques. *Normes internationales des Institutions supérieures de contrôle des finances publiques, ISSAI) 400 : Principes fondamentaux de l'audit de conformité.* 2019.

Organisation internationale des Institutions supérieures de contrôle des finances publiques. *GUID 5100 : Lignes directrices sur la vérification des systèmes d'information.* 2019.

ISACA. *CISA Review Manual,* 27ème édition.

ISACA. *COBIT 2019 Framework : Governance and Management Objectives. https://www.isaca.org/resources/cobit.* novembre 2018.

ISACA. *IT Audit Framework (ITAF): A Professional Practices Framework for IT Audit,* 4ème édition. 22 octobre 2020.

U.S. Government Accountability Office (ISC des États-Unis) *Federal Information System Controls Audit Manual* (FISCAM). https://www.gao.gov/products/gao-09-232g. 2 février 2009.

CHAPITRE 2 GOUVERNANCE ET GESTION DES TI

I. Qu'entend-on par « gouvernance et gestion des technologies de l'information » ?

On peut voir la gouvernance des TI comme le cadre général dans lequel les opérations informatiques de l'organisation sont exécutées et dont le but est de faire en sorte que les moyens répondent aux besoins actuels des métiers en tenant compte des besoins futurs identifiés et de la croissance prévue de l'organisation. La gouvernance des TI fait partie intégrante de la gouvernance d'entreprise ; elle englobe le leadership organisationnel, les structures et processus institutionnels, ainsi que d'autres mécanismes (présentation des résultats et retour d'expérience, mise en œuvre des politiques, ressources, etc.) dont le but est de veiller à ce que les systèmes d'information viennent en soutien des objectifs et de la stratégie de l'organisation, tout en équilibrant les risques et en assurant une gestion efficace des ressources.

Il est important de comprendre que, comme il est indiqué dans le référentiel COBIT de l'ISACA, gouvernance et gestion sont deux dimensions distinctes[38] :

- La **gouvernance** concerne l'évaluation des besoins, de la situation et des possibilités des parties prenantes en vue de fixer pour l'organisation des objectifs équilibrés et emportant l'adhésion, mais aussi la définition d'orientations en fonction des priorités et des décisions. Les orientations et les objectifs ainsi négociés servent ensuite de référence pour le suivi de la performance et de la conformité.
- La **gestion** planifie, développe, exécute et contrôle des activités en conformité avec les orientations définies par l'organe de gouvernance en vue d'atteindre les objectifs de l'organisation.

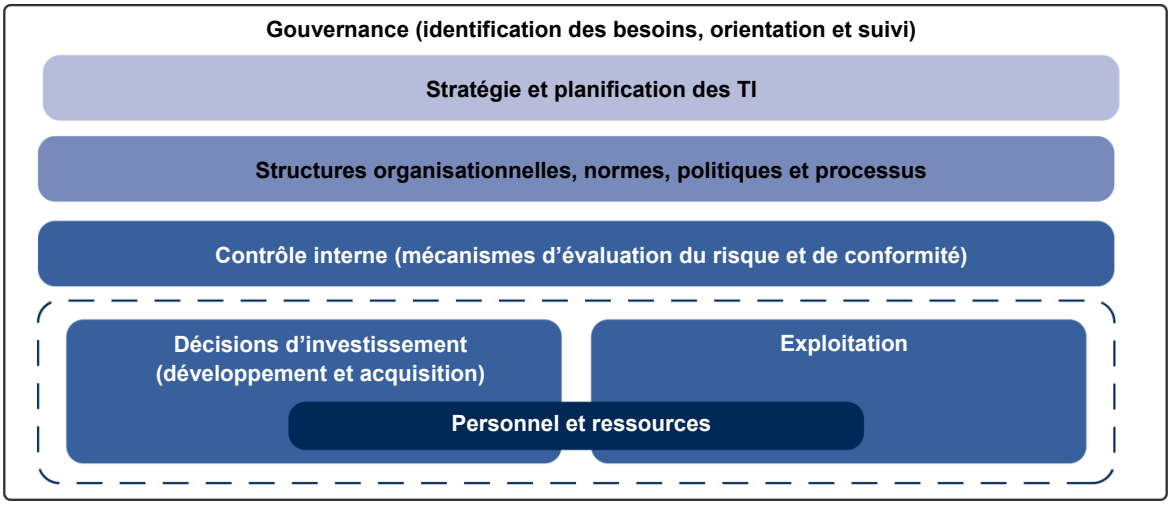
La gouvernance des TI joue un rôle essentiel dans la construction de l'environnement de contrôle. Elle pose les bases d'un contrôle interne solide et d'un compte rendu performant aux différents niveaux hiérarchiques, et elle rend possible le travail de supervision et de revue par la direction. Son rôle est essentiel pour garantir que

- les besoins, la situation et les possibilités des parties prenantes sont évalués dans le but de fixer pour l'organisation des objectifs équilibrés et emportant l'adhésion ;
- les orientations sont définies en fonction des priorités et des décisions ;
- les orientations et les objectifs ainsi négociés servent ensuite de référence pour le suivi de la performance et de la conformité.

Bien souvent, la gouvernance relève de la responsabilité d'un conseil d'administration, dirigé par un président. Certaines responsabilités de gouvernance peuvent être déléguées à des structures organisationnelles dédiées, en particulier dans les grandes organisations complexes.

La figure 7 présente un cadre générique de gouvernance des TI.

[38] Voir la *Section IV : Références et lectures complémentaires* de ce chapitre pour découvrir d'autres références et d'autres ressources concernant la gouvernance et la gestion des TI, les bonnes pratiques et les référentiels applicables en la matière.



Source : Unknown.

Figure 7 : Cadre générique de gouvernance des TI

a. Identification des besoins, orientation et suivi

La gouvernance des TI occupe une place centrale dans la gouvernance générale de l'organisation. Elle permet de garantir que les technologies de l'information apportent une valeur ajoutée qui correspond à la stratégie globale de gouvernance de l'organisation et ne constitue pas une discipline en soi. Une telle approche suppose que toutes les parties prenantes participent au processus décisionnel en matière de gouvernance des TI. De cette manière, la responsabilité des systèmes critiques est partagée par tous et les décisions sur les technologies de l'information sont prises et dictées par les besoins opérationnels.

Pour que la gouvernance des TI permette de faire en sorte que les investissements consentis dans ce domaine génèrent de la valeur pour l'activité et que les risques associés aux TI soient effectivement maîtrisés, il est essentiel de mettre en place une structure organisationnelle intégrant des rôles bien définis en matière de responsabilité de l'information, de processus métiers, d'applications et d'infrastructures.

L'organe directeur évalue les options stratégiques, donne aux cadres dirigeants de l'organisation des directives aux fins de l'application des options stratégiques retenues et surveille les résultats obtenus. La gestion concerne

- l'organisation globale, la stratégie et les activités support des TI ;
- l'identification, l'acquisition et la mise en œuvre de solutions informatiques, et leur intégration aux processus métiers ;
- l'exécution et le support des services informatiques, y compris en matière de sécurité ;
- le suivi de l'efficacité et la conformité des systèmes d'information avec les objectifs de performance, le contrôle interne et les contraintes externes.

La gouvernance des TI doit aussi jouer un rôle dans l'identification des nouveaux besoins des métiers ou dans l'actualisation des besoins, afin que des solutions informatiques (entre autres) adaptées aux utilisateurs puissent être définies. En phase de développement ou d'acquisition de solutions adaptées aux besoins métiers, elle garantit que les solutions sélectionnées répondent effectivement aux besoins métiers, que le personnel possède une formation adéquate et que l'on dispose des ressources nécessaires (équipements, outils, capacité réseau) pour déployer la solution. La fonction d'audit interne ou d'assurance qualité du groupe peut réaliser un suivi et rendre compte périodiquement du résultat de son travail à la direction.

II. Principaux éléments de la gouvernance et de la gestion des TI[39]

a. Stratégie informatique et planification

On entend par « stratégie informatique » le processus de mise en correspondance des objectifs stratégiques informatiques et opérationnels de l'organisation. Les objectifs stratégiques informatiques tiennent compte des besoins actuels et futurs de l'organisation, des capacités informatiques disponibles pour assurer l'exécution des services, et des contraintes liées aux ressources[40]. La stratégie tient compte de l'infrastructure et de l'architecture actuelles des systèmes d'information, des investissements, du modèle d'exécution, de l'approvisionnement en ressources (humaines notamment). Il s'agit de définir un plan intégrant ces différents éléments à l'intérieur d'une approche commune appuyant les objectifs opérationnels.

Il est important que l'auditeur des SI examine la stratégie informatique de l'organisation, non seulement pour acquérir une bonne compréhension du fonctionnement de l'organisation, mais aussi pour pouvoir apprécier dans quelle mesure la gouvernance des technologies de l'information a compté dans les décisions qui ont été prises.

Les organisations qui n'ont défini aucune stratégie informatique seront plus susceptibles de ne pas avoir déterminé comment les technologies de l'information pouvaient répondre à leurs besoins actuels et futurs. En outre, en l'absence de plan stratégique informatique actualisé, corrélé au plan stratégique global de l'organisation qui précise les objectifs, les indicateurs de performance, les stratégies et les liens d'interdépendance entre projets, l'organisation risque de ne pas vraiment savoir ce qu'elle souhaite réaliser au moyen des TI et de ne pas avoir identifié les stratégies qui lui permettront d'atteindre ces résultats.

b. Structures organisationnelles, normes, politiques et processus

Les structures organisationnelles sont essentielles pour la gouvernance des TI, car elles permettent l'articulation des rôles des différents organes de gestion et de gouvernance de l'entité, mais aussi des processus décisionnels. Ces structures doivent prévoir des délégations de pouvoir clairement définies pour la prise de décisions et le suivi des performances. Elles doivent s'appuyer sur des normes, des politiques et des procédures adaptées, afin d'améliorer l'efficacité du processus décisionnel.

Les **parties prenantes** (c'est-à-dire, l'ensemble des groupes, organisations, membres ou systèmes susceptibles d'affecter ou d'être affectées par les opérations de l'organisation) influencent les structures organisationnelles des organisations du secteur public. Les principales parties prenantes externes sont par exemple le pouvoir législatif et d'autres organes des pouvoirs publics, ainsi que les citoyens. Les structures organisationnelles dépendent aussi des **utilisateurs**, internes et externes.

Les utilisateurs internes sont les managers et les services fonctionnels responsables des processus métiers, ainsi que les personnes qui interagissent avec les processus métiers au sein de l'organisation. Les utilisateurs externes sont les organismes et les personnes qui utilisent les produits ou services fournis par l'organisation (par exemple, les citoyens, ou d'autres entités du secteur public). Les structures organisationnelles dépendent également des **prestataires** : société ou unité opérationnelle, personne fournissant un service, à l'externe comme à l'interne.

Ce sont les utilisateurs et les parties prenantes qui sont à l'origine de l'identification d'un besoin de fonctionnalités informatiques. Dans tous les cas, il est important que l'organe directeur définisse le mandat des structures organisationnelles, les rôles et les responsabilités en matière de gouvernance, en

[39] Les principaux éléments présentés dans ce chapitre consacré à la gouvernance des TI sont mis en avant dans les référentiels *COBIT 5* et *COBIT 2019*, et dans la norme *ISO 38500*. Définitions et exemples sont issus pour une large part de ces ouvrages de référence.

[40] Organisation internationale de normalisation, *ISO 38500*.

précisant clairement qui est responsable des différentes décisions et tâches importantes. Ce principe devrait s'étendre aux relations avec les principaux prestataires de services informatiques tiers[41].

Le **comité de direction informatique** constitue généralement l'élément central de la structure organisationnelle des technologies de l'information. Composé de cadres dirigeants et supérieurs, il est chargé d'examiner, de valider et de financer les investissements dans les TI, et de faire en sorte que l'organisation atteigne les principaux objectifs qui ont été définis. Il joue un rôle important dans le choix des technologies à déployer pour appuyer les investissements opérationnels et dans la validation des modes d'acquisition de ces technologies. Typiquement, c'est lui qui décide de lancer la conception ou l'achat d'une solution, en suivant généralement les recommandations de spécialistes ou de comités compétents.

L'action du comité de direction est déterminante pour obtenir l'adhésion autour des solutions retenues. Il apporte l'appui de la direction aux programmes qui impliquent des changements dans l'organisation. Dans de nombreuses organisations du secteur public, ses fonctions relèvent des fonctions de direction. Il est important d'avoir conscience du caractère complexe et polymorphe de la gouvernance des TI. Les structures managériales telles que le comité de direction répondent à différentes finalités et assument des rôles et des responsabilités divers en fonction de différents facteurs, dont les besoins de l'organisation, son secteur d'activité et son environnement. Si les fonctions de gestion sont confiées à différents acteurs en fonction des pays et des secteurs (notamment, entre organisations des secteurs public et privé), on peut citer par exemple :

- Le **Président-directeur général** : ce cadre dirigeant est chargé de la gestion globale de l'organisation.
- Le **Directeur financier :** ce cadre dirigeant est chargé de tous les aspects de la gestion financière, y compris du risque et des contrôles financiers.
- Le **Directeur des opérations** : ce cadre dirigeant est responsable du fonctionnement de l'organisation.
- Le **Directeur des risques :** ce cadre dirigeant est chargé de la gestion des risques au sein de l'organisation. Il peut avoir des fonctions liées au risque informatique et avoir dans ce cadre la mission de superviser le risque lié aux systèmes d'information.
- Le **Responsable de la confidentialité** : ce cadre est responsable du suivi des risques et de l'impact sur l'activité de la législation en matière de respect de la vie privée. Il a également pour mission d'orienter et coordonner la mise en œuvre des politiques et des mesures visant à garantir la conformité avec les directives relatives à la confidentialité.
- Le **Directeur des systèmes d'information** : ce cadre est responsable de la gestion et de l'exploitation des systèmes informatiques de l'organisation. Dans les organisations du secteur public, ses fonctions peuvent être confiées à un groupe ou un service doté du mandat, de l'autorité et des ressources nécessaires.
- Le **Directeur informatique** : ce cadre est notamment chargé de veiller à ce que l'organisation utilise les technologies de l'information de manière efficiente et efficace, en intégrant au déploiement des technologies de l'information les bonnes pratiques et les procédures recommandées. Il apporte également l'expertise nécessaire à l'adoption des technologies émergentes dans l'organisation.
- Le **Responsable de la sécurité des systèmes d'information :** ce cadre dirigeant est responsable de la sécurité de l'information, sous toutes ses formes.
- Le **Directeur des ressources humaines** : ce cadre dirigeant a pour mission d'aligner les politiques et procédures relatives aux ressources humaines sur la mission et les objectifs stratégiques de l'organisation.
- Le **Directeur des connaissances** : ce cadre dirigeant est chargé de la gestion des connaissances au sein de l'organisation.

[41] ISACA, *COBIT 2019*.

En l'absence de structure organisationnelle bien établie, comportant notamment un comité de direction informatique, il arrive que l'organisation ne dispose d'aucune entité responsable, d'une part, des décisions opérationnelles nécessitant un apport technologique à l'appui des investissements d'exploitation, et, d'autre part, de la validation des modes d'acquisition de cette technologie. De même, les organisations ne bénéficient pas toujours de l'appui nécessaire de la direction pour l'application des programmes. Les activités correspondantes risquent alors d'être mises en œuvre de façon incohérente et désorganisée, au détriment de la rentabilité des investissements ou de la réalisation des objectifs du programme.

c. Normes, politiques et procédures

L'organisation adopte les normes et politiques approuvées par la haute direction. Les politiques définissent le cadre général des opérations courantes afin que les objectifs définis par l'organe directeur soient atteints. Les normes prescrivent des mesures quantifiables visant la conformité avec les politiques. Les normes et politiques sont appuyées par des procédures qui définissent la manière dont le travail ou les mesures doivent être exécutés et contrôlés. La haute direction définit des objectifs en vue d'accomplir la mission de l'organisation, tout en assurant la conformité avec les exigences réglementaires et légales.

Les normes, politiques et procédures correspondantes doivent être régulièrement revues et actualisées. Elles doivent être communiquées périodiquement à tous les utilisateurs concernés de l'organisation. Le personnel du service informatique doit être formé à l'application et à l'utilisation de ces politiques, normes et procédures dans ses activités courantes. Les normes, politiques, et procédures en question doivent refléter l'évolution des technologies et des menaces, les modifications importantes des processus, ainsi que les nouvelles contraintes environnementales et réglementaires. L'audit informatique porte habituellement sur les normes des organisations, ces dernières pouvant servir de référence aux fins de l'audit.

Les politiques et procédures correspondantes doivent être régulièrement revues, et ajustées, le cas échéant. Elles doivent être communiquées périodiquement à tous les utilisateurs concernés de l'organisation. Les politiques reflètent l'évolution des technologies et des menaces, les modifications importantes des processus, ainsi que les nouvelles contraintes environnementales et réglementaires. La gouvernance des technologies de l'information est encadrée notamment par les politiques suivantes :

- **Politique relative aux ressources humaines :** la politique relative aux ressources humaines traite du recrutement et de la formation du personnel, de la résiliation des contrats de travail, ainsi que d'autres fonctions au sein de l'organisation. Elle définit le rôle et les responsabilités des différents collaborateurs de l'organisation, ainsi que le niveau de compétence et de formation qu'ils sont tenus de posséder pour s'acquitter de leurs obligations. La politique relative aux ressources humaines peut également encadrer l'attribution des rôles et responsabilités, ainsi que la répartition des tâches. Dans les grandes organisations complexes, cette fonction peut toutefois être déléguée à un service dédié.
- **Politiques relatives à la documentation et à la conservation des documents :** la documentation des systèmes d'information, des applications, des fiches de poste, des systèmes de reporting et de leur périodicité constitue un point de référence important pour aligner les activités informatiques sur les objectifs métiers. Définir des politiques appropriées pour la conservation de la documentation permet d'assurer le suivi et la gestion des modifications régulières apportées à l'architecture du système d'information de l'organisation.
- **Politique d'externalisation :** généralement, l'externalisation des services informatiques permet à la direction de l'organisation de se concentrer sur son cœur de métier. Elle peut également être motivée par la nécessité de réduire les coûts. La politique d'externalisation veille à ce que les propositions d'externalisation de fonctions et d'opérations soient élaborées et mises en œuvre selon des modalités avantageuses pour l'organisation. Les services cloud (informatique dans le nuage), qui offrent un accès à la demande à un ensemble de ressources informatiques configurables (réseaux, serveurs, stockage, etc.), font partie des services informatiques les plus souvent externalisés de nos jours. Le Chapitre 5 contient des informations complémentaires concernant l'externalisation et l'informatique dans le nuage.
- **Politique relative au télétravail :** les organisations devraient établir des politiques et des lignes directrices afin de faire en sorte que leurs effectifs soient préparés à travailler à distance. La

rédaction d'accords de télétravail entre salariés et managers permet généralement de faciliter la mise en place du télétravail. Ces accords doivent en définir les modalités pratiques avant que le salarié ne commence à travailler à distance, préciser les tâches à accomplir et les résultats attendus, les critères d'évaluation de la performance, les résultats mesurables et les livrables de l'activité.

- **Politique relative à la sécurité et à la confidentialité des systèmes d'information :** cette politique établit des exigences pour la protection des actifs informationnels et peut faire référence à d'autres procédures ou outils précisant les modalités de cette protection. Elle doit être accessible à tous les salariés responsables de la sécurité de l'information, ainsi qu'aux utilisateurs des systèmes métiers concernés par la sauvegarde de l'information (notamment, des dossiers du personnel et des données financières entrantes). Le Chapitre 7 contient des informations complémentaires concernant la politique de sécurité et de confidentialité des systèmes d'information.
- **Politique relative à la gestion des données :** les organisations recueillent des données auprès de différentes sources, dont les systèmes transactionnels, scanners, capteurs, réseaux sociaux et appareils connectés. Il leur faut donc définir des politiques et procédures pour gérer le cycle de vie de ces données, qui comprend notamment des étapes de collecte, stockage, sécurité et destruction des données. Le Chapitre 4 contient des informations complémentaires concernant la gestion des données.

Si l'organisation n'a mis en place aucune politique ou norme pour encadrer ses opérations quotidiennes, elle s'expose à un risque accru de non-conformité aux objectifs associés aux systèmes d'information. Par exemple, la politique relative aux ressources humaines est un élément important de la gestion du recrutement et de la formation, comme la politique relative à la sécurité des SI est importante pour garantir la protection des actifs informationnels.

d. Contrôle interne

Comme indiqué précédemment, on entend par « contrôle interne » l'introduction et le déploiement d'un ensemble de mesures et de procédures visant à déterminer si les activités de l'organisation sont conformes aux politiques, normes et plans approuvés. Le cas échéant, des mesures correctrices sont mises en œuvre pour permettre la réalisation des objectifs de la politique.

Le contrôle interne contribue à maintenir le système informatique sur la bonne voie. Les contrôles internes correspondent notamment à la gestion du risque, au respect des procédures et instructions internes et de la législation et réglementation externe, à l'établissement de rapports de gestion périodiques et ponctuels, aux contrôles de progression, à la révision des plans et aux audits, évaluations et actions de suivi[42].

Faute de contrôle interne, le risque que les systèmes d'information de l'organisation ne soient pas conformes aux politiques internes, aux normes, à la législation et à la réglementation augmente.

vii. Gestion du risque

Les risques informatiques doivent être intégrés à la stratégie et aux politiques de gestion du risque de l'organisation. La gestion du risque englobe des activités telles que l'identification des risques auxquels les applications et l'infrastructure actuelle des systèmes d'information sont exposées, mais aussi des activités permanentes, comme la revue périodique et l'actualisation des risques par la direction, ainsi que le suivi des stratégies de maîtrise des risques. La gestion du risque informatique doit être intégrée à la gestion globale du risque au sein de l'organisation.

La gestion des risques est facilitée quand elle s'inscrit dans un plan. Celui-ci permet de documenter le travail d'identification et d'évaluation des risques. Il consigne également par écrit les processus, outils et

[42] « IT Governance in Public Sector: A top priority, » (gouvernance des technologies de l'information, une priorité essentielle. Publié dans *WGITA IntoIT,* nº25, (août 2007).

modes opératoires appliqués pour gérer et maîtriser le risque tout au long d'un projet. Le chapitre 3, consacré au développement et à l'acquisition de systèmes d'information, précise en complément certains aspects de la gestion du risque.

viii. Fonction de contrôle de conformité

Les organisations doivent disposer d'une fonction de contrôle de conformité, qui garantisse l'application effective des politiques, normes et procédures associées. Il convient d'établir dans l'organisation une culture qui amène le personnel à comprendre les conséquences d'un non-respect des politiques, normes et procédures mises en place. La fonction de contrôle de conformité peut être étendue aux fonctions d'assurance qualité et de sécurité, ainsi qu'aux outils automatisés. Chaque rapport d'incident de conformité doit être examiné au niveau hiérarchique compétent, et des mesures doivent être prises en cas de non-conformités graves ou répétées. La direction peut choisir de traiter une non-conformité par des actions de formation de rappel, par la modification des procédures, voire par la mise en place de sanctions progressives selon la nature de la non-conformité (par exemple, violation de sécurité ou absence à une formation obligatoire).

Une assurance indépendante, fournie sous la forme d'un audit (ou d'une revue) interne ou externe, permet d'apporter en temps utile un retour d'information sur la conformité des systèmes d'information avec les politiques, normes et procédures de l'organisation, ainsi qu'avec ses objectifs généraux. Impartiaux et objectifs, ces audits apporteront aux managers une juste évaluation du projet informatique audité.

En l'absence de contrôle de conformité, l'organisation pourrait n'avoir aucune assurance crédible que ses processus et produits ont été déployés conformément à ce qui avait été planifié et qu'ils sont conformes à la description des modes opératoires, normes et procédures.

e. Décisions d'investissement

La gouvernance des TI doit apporter aux utilisateurs métiers des solutions à l'évolution de leurs contraintes. Ces solutions peuvent être déployées par le service informatique, qui appliquera à cette fin des décisions d'investissement consistant soit à développer (concevoir) de nouveaux logiciels et systèmes soit à les acquérir auprès de fournisseurs, si cette solution est plus économique. Pour prendre des décisions d'investissement pertinentes, les bonnes pratiques exigent généralement l'application d'une approche rigoureuse : identifier, analyser, hiérarchiser et valider les contraintes, réaliser une analyse comparative des coûts et avantages respectifs de différentes solutions, pour enfin retenir la meilleure solution (c'est-à-dire, celle qui garantit le meilleur équilibre entre les coûts et les risques, tout en répondant à une part importante des objectifs de l'organisation).

L'étude d'opportunité, qui permet d'identifier les besoins des utilisateurs et de faire apparaître les possibilités et les avantages d'une solution, est un outil efficace pour informer les décisions d'investissement. Elle peut s'intéresser tout d'abord à l'objectif stratégique global, pour détailler ensuite la description des principales activités, des jalons, des responsabilités et des rôles des intervenants. Cet outil dynamique doit être mis à jour en continu pour refléter la situation actuelle et pour anticiper l'évolution de l'initiative. Le Chapitre 3 contient des informations complémentaires sur le développement et l'acquisition de systèmes d'information.

f. Activités informatiques

De manière générale, on entend par « activités informatiques » le fonctionnement quotidien des infrastructures des systèmes d'information pour répondre aux besoins métiers. Bien gérées, ces activités permettent d'identifier les goulots d'étranglement et d'anticiper une évolution des capacités (par exemple, de nouvelles ressources matérielles ou réseau), de mesurer la performance pour s'assurer qu'elle est conforme aux attentes exprimées par la direction, mais également de fournir aux utilisateurs des ressources informatiques une plate-forme d'assistance et d'aide au traitement des incidents. Le Chapitre 4 contient des informations complémentaires sur les activités informatiques.

g. Personnel et ressources

La direction doit procéder à des évaluations régulières pour faire en sorte d'allouer aux systèmes d'information des ressources suffisantes pour répondre aux besoins de l'organisation, en conformité avec les priorités définies et dans le respect des contraintes budgétaires. En parallèle, la dimension humaine doit également être prise en compte dans les politiques, pratiques et décisions relatives aux systèmes d'information, et les besoins actuels et futurs des différents intervenants doivent y être intégrés. Les responsables de la gouvernance doivent régulièrement s'assurer que les ressources sont effectivement utilisées et affectées aux objectifs métiers conformément aux priorités identifiées.

Les organisations ont intérêt à gérer et planifier les ressources humaines des services informatiques en tenant compte de la planification stratégique, en veillant à réunir les compétences informatiques et les effectifs nécessaires, et en intégrant les pratiques de recrutement, de formation, l'évolution des carrières et la gestion des performances. Citons parmi les éléments clés d'une planification efficace des effectifs :

- établir et actualiser un processus de planification des ressources humaines,
- définir les exigences en matière de compétences et de dotation en personnel,
- évaluer régulièrement les besoins de compétences et d'effectifs,
- évaluer les lacunes de compétences et d'effectifs,
- élaborer des stratégies et un plan pour combler les lacunes de compétences et d'effectifs,
- mettre en œuvre des activités pour combler les lacunes, suivre les progrès réalisés par l'organisation pour combler ces lacunes, et
- rendre compte à la direction des progrès réalisés dans le traitement des lacunes.

III. Risques pour l'entité auditée

Les auditeurs doivent se familiariser avec les différentes composantes de la structure de gouvernance des technologies de l'information, afin de pouvoir les évaluer et déterminer si les décisions, les orientations, les ressources, la gestion et le suivi des systèmes d'information soutiennent les stratégies et les objectifs de l'organisation. Pour procéder à cette évaluation, les auditeurs doivent identifier les éléments clés de la gouvernance et de la gestion des TI, ainsi que les risques que tout élément non conforme peut présenter au sein de l'entité.

Le suivi, l'analyse et l'évaluation continus des indicateurs associés aux initiatives de gouvernance des TI nécessitent d'adopter un point de vue indépendant et équilibré, pour contribuer à l'amélioration des processus informatiques. L'audit apporte une contribution significative à la réussite de la mise en œuvre des actions de gouvernance des TI, en formulant des recommandations qui permettent d'atténuer les risques associés aux aspects suivants de la gouvernance et de la gestion des TI :

- orientation des services informatiques sur la mission, la vision, les valeurs, les objectifs et les stratégies de l'organisation ;
- réalisation des objectifs de performance définis par l'organisation et les services informatiques ;
- cadre légal et environnement, qualité de l'information, contraintes liées aux aspects fiduciaires, à la sécurité et à la confidentialité ;
- environnement de contrôle au sein de l'organisation ;
- risque inhérent à l'environnement de sécurité de l'information ;
- investissements/dépenses informatiques.

Chaque organisation fait face à des défis spécifiques, qui reflètent son environnement et son contexte politique, géographique, économique et social particuliers. La liste suivante, non exhaustive, présente les conséquences les plus fréquentes des risques d'une gouvernance inefficace des TI.

a. Des systèmes d'information ni efficaces ni efficients

Les systèmes d'administration publics, dont l'objectif consiste à servir la société ou les entreprises, ou à améliorer le fonctionnement des organismes du secteur public, sont souvent particulièrement complexes et couvrent un très large périmètre. Il est donc essentiel de bien les concevoir, de les adapter aux besoins réels de l'organisation, de les soumettre à une coordination compétente et de les exploiter avec efficacité. Si la responsabilité des processus, des applications et des données n'est pas clairement définie, la gouvernance des technologies de l'information ne produira pas ses effets. À l'échelle du secteur public comme à l'échelle de l'organisation, une mauvaise gouvernance des technologies de l'information est souvent le premier obstacle à la mise en place de systèmes informatiques de qualité.

b. Sentiment que l'informatique contribue peu à la valeur ajoutée de l'organisation

Les investissements informatiques importants qui ne sont pas stratégiquement alignés sur les objectifs et les ressources de l'organisation peuvent ne créer que peu de valeur (voire aucune valeur) pour les métiers. Ce manque d'alignement stratégique implique que les systèmes d'information, même s'ils sont de bonne qualité, n'apportent pas de contribution efficace et effective à la réalisation des objectifs d'ensemble de l'organisation. Pour réussir cet alignement, un moyen consiste à impliquer dans les décisions sur les SI les utilisateurs et les autres parties prenantes familiarisées avec les problématiques de l'activité. Ces parties prenantes peuvent contribuer à la préparation de l'étude d'opportunité, qui permettra d'aligner l'investissement sur les objectifs et les ressources de l'organisation.

c. Manque d'implication du service informatique de l'organisation

Des études ont montré que les grandes organisations adoptent et mettent en pratique une approche globale de la gestion des systèmes d'information, précisant notamment :

- qui est responsable des « produits informatiques », qui sont par exemple les services de courrier électronique, les services d'assistance et l'acquisition de matériel et de logiciels ;
- qui supervise les systèmes spécifiques à une mission donnée ;
- quelles sont les responsabilités respectives du service informatique et des unités métiers ou composantes de l'organisation.

Si l'autorité et les compétences de supervision ne sont pas centralisées, l'organisation n'a aucune garantie que ses investissements dans les technologies de l'information seront coordonnés à l'échelle de l'organisation et qu'ils permettront de constituer les capacités nécessaires pour appuyer les besoins de la mission, tout en évitant les doublons inutiles.

d. Exposition aux risques pour la sécurité de l'information et la confidentialité

Si l'organisation n'a pas mis en place des contrôles, des structures, des processus et des politiques appropriés en matière de sécurité de l'information, elle s'expose à un risque plus élevé dans ce domaine, ainsi qu'à des incidents et atteintes à la confidentialité des données. Ces risques portent notamment sur le détournement d'actifs, la divulgation d'informations sans autorisation, l'accès sans autorisation, la vulnérabilité aux attaques logiques et physiques, aux cyberattaques, les interruptions de service et l'indisponibilité d'informations, l'utilisation frauduleuse d'informations, le non-respect de la législation et de la réglementation relatives aux données à caractère personnel, l'échec de la reprise après sinistre. La politique de sécurité des systèmes d'information doit définir ce que sont les actifs organisationnels (c'est-à-dire, les données, les équipements, et les processus métiers) qui doivent être protégés, et établir le lien avec les procédures, les outils et les contrôles d'accès physique qui protègent les actifs en question.

Les structures de gouvernance, au niveau de la direction de l'organisation, doivent comporter des politiques, procédures et modes opératoires encadrant la gestion et le suivi des protections mises en place par l'organisation pour assurer la sécurité de l'information et le respect de la confidentialité. Ces documents servent à communiquer les priorités de la mission, les ressources disponibles, ainsi que le niveau général de tolérance aux risques pour la sécurité de l'information. L'organisation doit également avoir adopté une procédure contribuant à la mise en conformité des activités relatives à la sécurité de l'information avec la législation, la réglementation et les lignes directrices applicables en matière de

sécurité de l'information et de respect de la confidentialité. Les personnes responsables de la protection des systèmes et des données doivent notamment rendre compte au niveau hiérarchique compétent, et disposer d'une formation adéquate.

Le présent manuel ne se prétend pas exhaustif. D'autres documents de référence définissent les structures de gouvernance de la sécurité de l'information plus en détail, parmi lesquels :

- ISACA. *COBIT 2019 Framework : Governance and Management Objectives*. 2019.
- Organisation internationale de normalisation/commission électrotechnique internationale. *ISO/IEC 27001: Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences.*
- National Institute of Standards and Technology. *NIST Special Publication* 800-53, *Security and Privacy Controls for Information Systems and Organizations*, rév. 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. Septembre 2020.
- National Institute of Standards and Technology. *NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final. Décembre 2018.

e. Contraintes pour la croissance de l'activité

Si la planification des systèmes d'information est inadéquate ou absente, la croissance de l'activité pourra être limitée par des ressources informatiques insuffisantes ou une utilisation inefficace des ressources disponibles. Pour atténuer ce risque, une solution consiste à élaborer et mettre à jour périodiquement une stratégie informatique, permettant d'identifier les ressources et d'anticiper les besoins futurs de l'activité.

f. Gestion inefficace des ressources

Pour optimiser les résultats en maîtrisant les coûts, l'organisation doit gérer ses ressources informatiques avec efficacité. Elle exploitera tout le potentiel de valeur de ses investissements dans les technologies de l'information en s'assurant que les ressources disponibles sont suffisantes sur le plan technique, matériel, logiciel et humain, et que son personnel possède l'expérience et les connaissances nécessaires à la bonne exécution des services informatiques. Elle peut par exemple définir et contrôler l'utilisation des ressources informatiques en établissant un accord sur les niveaux de service[43], ce qui lui permettra de disposer d'une base objective pour déterminer si les ressources envisagées suffisent à répondre aux besoins des métiers.

Bien appliquée, la gestion prévisionnelle des ressources humaines permet de faire en sorte que le personnel dispose des qualifications requises. L'organisation aura intérêt à appliquer les stratégies de planification des effectifs abordées précédemment, en mettant en place des procédures qui lui permettront d'identifier les principaux besoins en personnel et en compétences, et de concevoir des stratégies pour y répondre.

g. Processus décisionnel inefficace

Le processus décisionnel peut perdre en efficacité si les structures de présentation des résultats ne sont pas bien définies. Cela peut avoir des conséquences sur la capacité de l'organisation à fournir ses services, et l'empêcher d'atteindre ses objectifs. Mettre en place des comités de pilotage et autres instances représentatives contribue à l'efficacité des décisions prises au sein de l'organisation.

[43] Un accord sur les niveaux de service (*Service Level Agreement*, SLA) permet de définir les contraintes et les responsabilités spécifiques du prestataire de services, ainsi que les attentes du client.

h. Échec des projets

Souvent, les organisations négligent l'importance de la gouvernance en matière de technologies de l'information. Elles entreprennent des projets informatiques sans avoir clairement identifié les contraintes associées au projet et la manière dont ce projet contribue aux objectifs de l'organisation. Si ce travail préparatoire n'est pas effectué, les projets informatiques ont plus de risques de ne pas aboutir. Une autre erreur fréquente consiste à acquérir ou développer des applications qui ne répondent pas aux standards minimums en matière de sécurité et d'architecture. En pareil cas, l'organisation pourra être contrainte d'engager des dépenses supplémentaires pour la maintenance et l'administration des systèmes et applications non conformes. Pour réduire le risque d'échec des projets, on pourra définir un **cycle de vie du développement de système** (*system development life cycle*, SDLC) et l'appliquer aux phases de développement et d'acquisition. Le chapitre 3, consacré au développement et à l'acquisition de systèmes d'information, précise certains aspects méthodologiques du SDLC.

i. Problèmes de dépendance envers un tiers ou de fourniture de services par le sous-traitant informatique

En l'absence de procédure de contrôle des processus d'acquisition et d'externalisation, l'organisation peut se retrouver en situation de dépendance totale envers un prestataire ou sous-traitant. Cette situation constitue un environnement à haut risque : en effet, si le prestataire cesse son activité ou fait défaut dans l'exécution des services contractuels, l'organisation connaîtra des difficultés. Un tel environnement entraîne d'autres risques, tels qu'un litige en propriété intellectuelle, un risque de violation de systèmes, des données à caractère personnel ou des bases de données. Les organisations qui font régulièrement appel à l'externalisation de solutions auront intérêt à mettre en place une politique d'externalisation ou d'acquisition, précisant ce qui peut ou ne peut pas être externalisé. Il est tout aussi important pour ces organisations d'identifier et de maîtriser les risques associés à la chaîne d'approvisionnement en phase de développement ou d'acquisition de produits et services informatiques. Le Chapitre 7 contient des informations complémentaires sur la gestion de la chaîne logistique.

En assurant une supervision et un suivi effectifs des contrats, l'organisation crée des conditions favorables à la maîtrise du risque de dépendance envers un prestataire tiers. Les contrats doivent comporter des accords sur les niveaux de service et préciser les droits d'accès du tiers. Pour veiller à ce que le prestataire s'acquitte de ses obligations, l'organisation peut mettre en place un suivi rigoureux de la performance de ses prestataires, comportant des rapports réguliers sur l'avancement du projet et une revue des livrables. Si les mesures de supervision et de suivi détectent un manquement de la part du prestataire, l'organisation peut déployer des actions correctrices.

Les organisations et les auditeurs doivent considérer les prestataires tiers (y compris les fournisseurs de services « cloud » et « back office » sous-traités) comme faisant partie intégrante de l'environnement de contrôle de l'organisation. Par conséquent, les contrôles d'application et les contrôles généraux relevant de la responsabilité du tiers peuvent aussi être intégrés au périmètre de l'audit informatique, en complément d'autres contrôles comme le suivi et la supervision des activités du fournisseur.

j. Manque de transparence et de responsabilité

La responsabilité et la transparence constituent deux volets incontournables d'une bonne gouvernance. La transparence est une véritable force qui, dès lors qu'elle est appliquée de façon systématique, peut contribuer à lutter contre la corruption, améliorer la gouvernance et promouvoir la responsabilité[44]. Faute de structures organisationnelles, de stratégies, de procédures et de contrôles de suivi adaptés, l'institution pourrait n'être pas totalement responsable et transparente.

[44] Organisation internationale des Institutions supérieures de contrôle des finances publiques*, INTOSAI-P 20, Principes de transparence et de responsabilité,* p.5.

k. Non-conformité avec les dispositions légales et réglementaires

Les parties prenantes exigent l'assurance que les organisations se conforment à leurs obligations légales et réglementaires et qu'elles appliquent les pratiques de bonne gouvernance dans leur environnement opérationnel. En outre, les technologies de l'information ayant permis la mise en place de processus métiers très fluides entre organisations, il est de plus en plus nécessaire de veiller à ce que les contrats précisent les principales exigences liées aux technologies de l'information, notamment pour ce qui concerne le respect de la vie privée, la confidentialité, la propriété intellectuelle et la sécurité[45]. Les différentes politiques de l'organisation, notamment en matière de sécurité informatique, d'externalisation et de gestion des ressources humaines, doivent préciser le cadre légal et réglementaire applicable.

l. Dépenses informatiques non chiffrées, excessivement élevées ou insuffisantes

Les organisations constatent souvent qu'elles ne connaissent pas le montant total de leurs dépenses informatiques, ou que ce montant est supérieur à leurs prévisions. Ce manque d'information peut s'expliquer par l'absence de gestion centralisée ou par le fait qu'aucune personne n'ait été désignée responsable de la dépense globale liée aux technologies de l'information, ou encore par un manque de précision dans l'imputation des dépenses informatiques par les divisions opérationnelles de l'organisation. Les bonnes pratiques invitent à mettre en place des mécanismes de validation des décisions relatives aux dépenses d'investissement dans les TI (par exemple, la création d'un comité de gouvernance des systèmes d'information). Les décisions d'investissement informatiques seraient ainsi prises sur le fondement des besoins recensés dans l'organisation. En l'absence d'un tel mécanisme de supervision, l'organisation pourrait ne pas être en mesure de garantir que les aspects prioritaires de ses besoins informatiques ont été traités.

Outre le risque que l'organisation ne connaisse pas le montant global de ses dépenses informatiques ou que ce montant soit excessivement élevé, l'organisation peut constater que son budget informatique ne permet pas de répondre aux nouveaux besoins des métiers ou de faire face aux menaces émergentes. Les organisations réalisent souvent que la majeure partie de leur budget informatique est consacrée à la maintenance des systèmes et des infrastructures, qu'elles dépensent par exemple une part importante de ce budget à l'achat de licences de logiciels et de prestations d'assistance et de maintenance. Il faut disposer d'outils et de connaissances spécialisés pour identifier quelles les licences logicielles sont nécessaires et pour les utiliser, aussi existe-t-il un risque significatif que des sommes soient dépensées pour des logiciels qui ne sont en fait pas utilisés.

Pour mieux contrôler la dépense informatique, l'organisation doit définir ses besoins et ses objectifs opérationnels concernant les systèmes d'information, identifier les projets qui ne contribuent pas à la réalisation de ces objectifs, et prendre des décisions fondées sur l'analyse globale de ses systèmes d'information. Par exemple, on entend souvent que l'informatique dans le nuage contribue à réduire les dépenses opérationnelles. Toutefois, en fonction du service, de sa configuration et de son utilisation, l'informatique dans le nuage peut en réalité s'avérer plus coûteuse. Les principes de bonne gouvernance des technologies de l'information demandent une évaluation rigoureuse de ces nouveaux modes de fonctionnement avant de les adopter.

m. Absence de procédure de gestion des logiciels

En l'absence de procédure déployée pour la gestion des logiciels, il est possible que l'organisation acquière ou développe des logiciels qui ne répondent pas aux besoins des métiers ou aux normes applicables. Les situations suivantes peuvent se présenter :

- acquisition/développement d'un logiciel ne répondant pas aux besoins des métiers de l'organisation,
- acquisition/développement d'un logiciel sans contrôle qualité,
- développement d'un logiciel qui ne sera pas déployé, ne répondant pas aux standards de qualité,

[45] *Référentiel COBIT 5, Annexe E—Principe 5—Conformité.*

- développement d'un logiciel incomplet ou qui ne répond pas au cahier des charges,
- interruption ou abandon d'un projet de développement de logiciel.

IV. Références et lectures complémentaires

Cour des comptes fédérale du Brésil. *Get.it : Governance Evaluation Techniques for Information Technology: A WGITA Guide for Supreme Audit Institutions*. 2016.

ISACA. Whitepaper—*Privacy in Practice 2021: Data Privacy Trends, Forecasts and Challenges*. https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whppip. 2021.

ISACA. *COBIT 2019 Framework : Governance and Management Objectives.* 2019.

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

ISACA. *CISA Review Manual,* 27ème édition.

ISACA. *Vendor Management Using COBIT 5*. 2016.

Organisation internationale de normalisation/commission électrotechnique internationale. *ISO/IEC 38500:2015 Technologies de l'information — Gouvernance des technologies de l'information pour l'entreprise.* https://www.iso.org/standard/62816.html. Février 2015.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity,* version 1.1. https://www.nist.gov/cyberframework/framework. Avril 2018.

Organisation de coopération et de développement économiques. *Principes de gouvernement d'entreprise du G20 et de l'OCDE*. http://www.oecd.org/corporate/principles-corporate-governance. 30 novembre 2015.

U.S. Government Accountability Office. *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*. GAO-20-129. https://www.gao.gov/products/gao-20-129. 30 octobre 2019

U.S. Government Accountability Office. *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses*. GAO-15-315. https://www.gao.gov/products/gao-15-315. 31 mars 2015.

U.S. Government Accountability Office. *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity (remplace AIMD-10.1.23)*. GAO-04-394G. https://www.gao.gov/products/gao-04-394g. 1 mars 2004.

CHAPITRE 3 : DÉVELOPPEMENT ET ACQUISITION DE SYSTÈMES D'INFORMATION

I. Qu'entend-on par « développement et acquisition de systèmes d'information » ?

Les systèmes d'information jouent aujourd'hui un rôle critique dans la réalisation des objectifs des organisations, en élargissant les capacités dont les utilisateurs peuvent disposer. Les organisations cherchent donc de plus en plus à moderniser leurs solutions existantes et à développer et acquérir de nouvelles solutions informatiques. Celles-ci peuvent être développées en interne ou acquises auprès d'un prestataire externe (le chapitre 5 contient des informations complémentaires sur l'externalisation). Les organisations combinent souvent différentes approches. Pour choisir entre développement ou acquisition de solutions informatiques, les organisations devraient retenir l'approche qui répond le mieux à leurs besoins. Parfois, l'organisation achète des solutions informatiques pour les intégrer à ses solutions existantes. Dans d'autres cas, elle choisit de développer en interne de nouvelles solutions parce que les produits disponibles sur le marché ne proposent pas toutes les fonctionnalités dont elle a besoin.

Que l'organisation choisisse l'approche interne ou externe pour développer, acquérir et déployer des solutions informatiques, elle doit planifier le processus de façon à pouvoir gérer les risques et optimiser les chances de réussite du projet. Elle doit également identifier, analyser, documenter et hiérarchiser les contraintes liées à ces solutions. L'organisation peut mandater des spécialistes de l'assurance qualité et des contrôles pour garantir la qualité des solutions retenues.

Habituellement, le développement ou l'acquisition de solutions est confié à une équipe projet. Si les organisations ne formalisent pas systématiquement leur projet, certaines activités clés sont incontournables en phase de planification et d'exécution du processus de développement ou d'acquisition (par exemple, identifier les contraintes et gérer les risques).

D'après le modèle CMMI (*Capability Maturity Model® Integration)* appliqué à l'acquisition, version 1.3, publié par le Software Engineering Institute, les organisations optent de plus en plus pour l'acquisition parce que les produits et services sont facilement disponibles et que cette option revient généralement moins cher qu'un développement en interne. Cependant, le risque est réel d'acquérir des produits qui ne répondent pas aux objectifs métiers ou qui n'apportent pas satisfaction aux utilisateurs. Ce risque doit être traité pour que l'acquisition contribue efficacement aux objectifs et à la mission de l'organisation. Si elle s'inscrit dans un processus rigoureux, l'acquisition de systèmes d'information peut améliorer l'efficacité opérationnelle de l'organisation en s'appuyant sur la capacité des prestataires à fournir des solutions dans des délais courts, pour un tarif contenu, utilisant les technologies les plus appropriées.

Pour acquérir un produit ou une solution, l'organisation doit connaître ses besoins et contraintes métiers, identifiés par la bonne application de ses procédures de gouvernance des TI (le chapitre 2 contient des informations complémentaires sur la gouvernance et la gestion des technologies de l'information). Le travail d'identification des besoins doit inclure toutes les parties prenantes (les propriétaires de processus) concernées par le processus opérationnel, comme les utilisateurs finaux et les techniciens qui assureront en définitive la maintenance et le support du système. Pour l'acquisition de services (par exemple, une plate-forme d'assistance ou une prestation d'automatisation des postes de travail), l'identification des besoins doit inclure le service informatique interne de l'organisation qui assurera l'interface avec le prestataire de services. Il est important de hiérarchiser les besoins. Si le projet fait face à une réduction de budget ou à d'autres contraintes sur les coûts, on pourra alors reporter certains besoins, le cas échéant, à un projet ultérieur de développement ou d'acquisition.

Le processus de développement et d'acquisition de systèmes d'information s'accompagne d'un certain nombre de responsabilités managériales. Les organisations appliquent souvent une méthodologie du type « cycle de vie de développement de système » (SDLC) pour créer une structure de gestion du projet et veiller à ce que les responsabilités soient attribuées. La méthodologie SDLC comprend généralement cinq phases : (1) décision, (2) développement et acquisition, (3) déploiement, (4) exploitation et

maintenance, puis (5) suppression. Nous allons à présent étudier plus en détail les méthodologies SDLC.

a. Méthodologies de projet

Différentes méthodologies SDLC conviennent au développement de solutions informatiques : le classique modèle en cascade (*Waterfall*), le modèle en spirale, et les modèles itératifs du type Agile.

- Le **modèle en cascade** commence avec l'identification des besoins, pour passer ensuite par différentes étapes successives (conception, développement, validation), chacune utilisant comme intrant le résultat de l'étape précédente, jusqu'à obtenir un produit fini. Ce modèle facilite le suivi de l'avancement du projet développement, constitué d'une succession de phases.
- Le **modèle en spirale** utilise une approche fondée sur le risque pour développer progressivement un système par répétition des quatre phases de développement. Selon ce modèle, chaque spirale ou cycle débute habituellement par la détermination des objectifs du développement et du périmètre de la phase de déroulement. Ensuite, on évalue des alternatives, en appliquant des techniques de gestion du risque pour identifier et réduire les risques. L'étape suivante consiste à développer un produit pour la phase en cours (par exemple, un prototype). Enfin, on évalue le produit pour déterminer s'il répond aux objectifs de départ de la phase du cycle.
- Le **modèle Agile** met l'accent sur des phases de développement de courte durée dont le périmètre est clairement délimité, produisant des parties d'un produit fonctionnel. Il utilise des étapes similaires au modèle traditionnel en cascade (définition des besoins, conception, développement et validation) mais applique un cycle de développement plus court, pour réaliser plusieurs itérations dans des délais comparables. On a constaté qu'il était possible d'améliorer le développement et le déploiement des technologies de l'information en appliquant des approches plus progressives et de plus courte durée[46].

  D'autres référentiels s'appuient sur le modèle Agile et en reprennent l'essentiel des principes et pratiques. Par exemple :

  - le **modèle DevOps** met l'accent sur la collaboration entre les développeurs de logiciels (Dev), les administrateurs de systèmes et d'architectures (Ops) et l'assurance qualité, dans l'objectif d'accélérer l'évolution des applications logicielles. De manière générale, les principes de la méthode DevOps sont conformes à la méthode Agile. On considère ce modèle comme une extension des pratiques de déploiement agiles à tous les secteurs du cycle de vie du produit ;
  - le **développement itératif** scinde le processus en différentes étapes appelées itérations, afin de réaliser le travail de conception, de développement et de validation par cycles.

D'après le modèle CMMI (*Capability Maturity Model® Integration*) appliqué au développement, version 1.3, publié par le Software Engineering Institute, l'organisation qui choisit une méthodologie organisationnelle pour le développement et l'acquisition de solutions doit définir et maintenir des exigences et des lignes directrices qui peuvent être spécifiques à un projet particulier. Ces exigences et lignes directrices dépendent du modèle de développement retenu et d'autres problématiques, comme les besoins du client, le coût, le calendrier, et la complexité technique.

Bien que les organisations aient le choix de différentes méthodologies de projet, il existe des bonnes pratiques clés, dont l'application augmente les chances de succès du développement et de l'acquisition de produits et services. Ces pratiques sont par exemple l'identification et la gestion des besoins, la gestion du risque, la gestion de projet, la validation, la supervision du prestataire (en phase d'acquisition, puis en phase d'exploitation ou de maintenance du système), et la formation interne. Nous allons à présent étudier plus en détail ces différentes pratiques.

Quelle que soit la méthodologie de projet retenue, il est toujours important de bien documenter le travail. De même, il convient de veiller à ce que cette documentation reste disponible après que le

[46] Pour en savoir plus sur le modèle Agile, voir le document publié par l'ISC des États-Unis : U.S. Government Accountability Office, *Agile Assessment Guide : Best Practices for Agile Adoption and Implementation,* GAO-20-590g, (28 septembre 2020), https://www.gao.gov/products/gao-20-590g.

développement a été achevé. Si l'organisation s'appuie sur une solution du développeur pour communiquer les besoins, harmoniser les fichiers des utilisateurs et suivre le développement, la documentation ne pourra souvent plus être consultée à l'issue du développement. En conséquence, l'organisation aura des difficultés à retracer le périmètre et la conformité de ce qui a été produit.

II. Principaux éléments de l'acquisition et du développement de SI

a. Réalisation d'une étude de faisabilité

Si l'interprétation de la méthodologie par le chef de projet peut impliquer l'utilisation de différentes phases, dont le nom varie selon les cas, l'organisation peut envisager au départ de réaliser une étude de faisabilité, avant même de définir un cahier des charges. L'étude de faisabilité peut faciliter l'analyse des solutions possibles aux problèmes identifiés, et de leurs avantages. Les objectifs de l'étude de faisabilité sont notamment :

- identifier clairement le besoin ;
- déterminer la meilleure solution de rechange possible, fondée sur le risque (par exemple, faut-il développer en interne ou acquérir la solution) ;
- définir le calendrier du déploiement de la solution ;
- calculer le coût approximatif du développement/de l'acquisition ;
- déterminer si la solution s'inscrit dans la stratégie métier.

L'étude doit s'achever par la rédaction d'un rapport comparatif présentant les résultats des critères analysés (par exemple, coûts, avantages, risques, ressources nécessaires et impact pour l'organisation), formulant une recommandation de solution et un mode d'action (par exemple, développement ou acquisition d'un système).

b. Définition et gestion du cahier des charges

Pour acquérir ou développer un nouveau logiciel ou modifier des systèmes d'information existants, les équipes projet et les développeurs doivent impérativement définir un cahier des charges et gérer les changements qui peuvent y être apportés. Le cahier des charges précise ce que le système est censé réaliser, avec quel niveau d'efficacité, mais également ses interactions avec d'autres systèmes. Un cahier des charges bien conçu et suivi avec rigueur est la base de tout projet réussi de développement ou d'acquisition d'un système. La version 1.3 du modèle *CMMI* appliqué au développement publié par le Software Engineering Institute contient des bonnes pratiques dans quatre domaines liés à la rédaction et au suivi du cahier des charges :

- **établissement du cahier des charges client.** Recensement des besoins, des attentes, des contraintes et des interfaces des parties prenantes, ainsi que toutes les contraintes d'automatisation (dématérialisation) centralisées par le service informatique ou avec la participation significative du service informatique, afin de les traduire dans un cahier des charges client ;
- **établissement du cahier des charges produit.** Affiner et préciser les contraintes du client, afin de rédiger un cahier des charges du produit et des composantes du produit ;
- **analyse et validation du cahier des charges.** Vérifier dans quelle mesure les actifs informatiques existants peuvent être utilisés (y compris les logiciels d'application), le cas échéant ; analyser et valider le cahier des charges au vu de l'environnement présumé de l'utilisateur final ;
- **gestion du cahier des charges.** Gérer le cahier des charges et identifier les incohérences par rapport aux plans du projet et aux produits du travail.

Selon le Software Engineering Institute, les organisations devraient également établir et entretenir des plans précisant les étapes de mise en œuvre de ces bonnes pratiques liées à la rédaction du cahier des charges, en posant les attentes des parties prenantes concernées. Il recommande ainsi d'établir par écrit une procédure de rédaction et de gestion du cahier des charges, permettant de réduire le risque de développer un système qui ne réponde pas aux besoins des utilisateurs, que l'on ne puisse pas

soumettre à des tests adaptés, ou dont les résultats ou le fonctionnement ne soient pas conformes aux prévisions.

c. Gestion du risque

Pour réussir un projet de développement et d'acquisition, l'organisation doit identifier, hiérarchiser et gérer les risques à chaque étape du cycle de vie du développement du système (SDLC). Chaque fois qu'un problème est identifié, il est alors possible de planifier et de déclencher des actions de maîtrise du risque, en cas de besoin, tout au long de la vie du projet, afin d'atténuer l'impact de ces risques sur les objectifs. Une gestion efficace du risque implique d'identifier les risques de façon précoce et active, en organisant la collaboration et l'implication des parties prenantes concernées. Le modèle CMMI du Software Engineering Institute propose de répartir les activités de gestion du risque en quatre domaines :

- **préparation de la gestion du risque.** La préparation concerne l'élaboration et le suivi d'une stratégie d'identification, d'analyse et d'atténuation des risques. La stratégie de gestion des risques définit précisément les actions et l'approche retenues pour appliquer et contrôler le programme de gestion des risques. Elle suppose également d'identifier les parties prenantes concernées et de les impliquer dans le processus de gestion des risques. Les activités associées à la préparation de la gestion du risque sont par exemple l'établissement d'un cahier des charges de gestion du risque et l'élaboration d'une stratégie de gestion du risque ;
- **identification et analyse des risques.** Il s'agit ici d'identifier les risques liés aux sources internes et externes, puis d'évaluer la probabilité et les conséquences de chacun de ces risques. L'analyse des risques comprend l'évaluation, la classification et la hiérarchisation des risques ; on l'utilise pour déterminer les cas qui nécessitent une attention particulière de la direction. Les activités associées à l'identification et à l'analyse des risques sont par exemple l'établissement d'une liste des risques identifiés, en indiquant pour chacun d'eux une catégorie, un degré de priorité et une source ;
- **atténuation des risques.** Atténuer les risques implique de développer des techniques et des méthodes pour éviter, réduire et contrôler la probabilité de concrétisation des risques identifiés. Un plan d'atténuation des risques doit être établi pour les principaux risques auxquels le projet est exposé. Il convient de réévaluer périodiquement le statut de chacun des risques, afin de déterminer si les seuils établis ont été dépassés et s'il faut donc déclencher les plans d'atténuation du risque. Les activités associées à l'atténuation du risque sont par exemple l'élaboration de plans d'atténuation du risque et de plans de secours ou d'urgence ;
- **supervision par la direction.** Les activités associées à la supervision par la direction sont principalement la revue de situation des risques du projet, périodique ou déclenchée par un événement, avec la participation des niveaux hiérarchiques appropriés. Cette revue apporte de la visibilité sur l'exposition potentielle du projet aux risques et sur les actions correctrices appropriées. Le chapitre 2 contient davantage d'informations sur le rôle que la supervision par la direction joue dans l'orientation des activités liées aux SI au sein des organisations.

d. Gestion et maîtrise du projet

La gestion du projet nécessite de définir le plan du projet et les activités de contrôle, mais également de définir des coûts et un calendrier de référence, les jalons de ce calendrier, et d'impliquer les parties prenantes dans les activités clés. La maîtrise du projet correspond aux activités de supervision et de présentation périodique des résultats, et de mise en place de mesures correctrices si le projet ne se déroule pas conformément au plan. Par exemple, si le coût du projet augmente fortement, l'organisation peut choisir de supprimer certaines fonctions du système après consultation des parties prenantes, afin de maîtriser les coûts.

L'approche SDLC ou la stratégie d'acquisition de l'organisation doit préciser la structure de gestion du projet. Généralement, la structure de gestion du projet comprend un chef de projet, un responsable du risque, des gestionnaires d'assurance qualité et d'assistance à la configuration, ainsi que des collaborateurs testeurs, si cette fonction n'est pas intégrée à l'assurance qualité. Le plan de projet sert de référence au pilotage de ces différentes activités. La direction de l'organisation est régulièrement tenue informée de l'avancement du projet et de la façon dont les risques sont gérés. Elle peut ainsi arbitrer les

compromis concernant les coûts, les délais et la performance, car il est rare qu'un projet ne connaisse aucun écart par rapport aux objectifs fixés dans ces domaines.

e. Conception/Développement

En s'appuyant sur le cahier des charges, la conception établit les valeurs de référence du système et des sous-systèmes : description des éléments du système, des interfaces, du déploiement du système au moyen des équipements matériels, des solutions logicielles et réseau retenues. Généralement, la conception comprend également les spécifications du programme et des bases de données, ainsi que les considérations relatives à la sécurité. Ensuite, au cours du développement, on utilisera les spécifications de conception pour commencer à programmer et formaliser les processus opérationnels du système.

D'année en année, les processus de développement des applications métiers ont de plus en plus eu recours aux phases types de la méthode SDLC. Avec la généralisation de l'acquisition de solutions, les phases de conception/développement du cycle de vie classique ont été remplacées par une phase de **sollicitation**[47].

Par conséquent, pour acquérir une solution informatique, les organisations utilisent souvent un dossier de sollicitation (appel d'offres). La sollicitation correspond au travail de documentation du cahier des charges métier et de rassemblement des différents éléments de référence dont le fournisseur aura besoin pour proposer une solution informatique. L'organisation crée un dossier d'appel d'offres et le diffuse, reçoit des propositions et sélectionne un prestataire. Le processus de sélection doit être transparent et objectif, et reposer sur des critères adaptés au système ou aux services achetés. Il est essentiel que l'équipe projet implique le service juridique de l'organisation dans ce processus. L'équipe juridique connaît la législation et la réglementation, et pourra veiller à ce que les critères de sélection des fournisseurs soient équitables et qu'ils puissent être confirmés en justice si les prestataires écartés contestent l'attribution du marché.

f. Assurance qualité et tests

L'assurance qualité apporte aux collaborateurs du projet et à la direction des éléments d'information sur la qualité et les fonctionnalités des produits des étapes intermédiaires et du travail final. Les personnes chargées de l'assurance qualité doivent ainsi établir un référentiel, un manuel de l'utilisateur du système bien documenté, et évaluer périodiquement les produits du travail pour vérifier s'ils sont conformes aux normes de qualité documentées de l'organisation et si les équipes du projet ont suivi les procédures requises pour le développement des produits. Les organisations doivent s'assurer que le produit développé ou acquis est conforme au cahier des charges, aux critères d'acceptation (par exemple, le nombre d'erreurs non critiques reste inférieur au seuil défini) et que des tests ont été réalisés (fonctionnels, d'intégration du système et d'acceptation par l'utilisateur) avec la participation des utilisateurs et des parties prenantes.

L'assurance qualité permet également de vérifier si la méthodologie décidée et validée pour le développement a bien été respectée, de même que les étapes de supervision requises. Par exemple, elle contrôle que les revues (formelles ou informelles) ont bien lieu et que les parties prenantes et les membres concernés de la direction reçoivent effectivement les rapports d'avancement nécessaires. Dans le déroulement du processus d'assurance qualité, les responsables de l'assurance qualité et la haute direction évaluent si l'équipe projet se conforme aux politiques et procédures définies en interne pour les programmes d'acquisition ou de développement. La traçabilité de la supervision par des hauts responsables doit être assurée aux étapes clés du cycle d'acquisition ou de développement.

g. Gestion de la configuration

Le travail de gestion de la configuration permet de s'assurer du respect de l'intégrité des documents, des logiciels, et des autres éléments descriptifs ou complémentaires faisant partie du système en cours de

[47] Également appelée « sélection et acquisition ».

développement ou d'acquisition. La traçabilité des modifications apportées à ces éléments (que l'on appelle également « produits ») est assurée, et des références (ou « versions ») sont conservées, pour permettre à l'organisation de revenir si nécessaire à une version antérieure connue et validée.

L'organisation peut mettre en place un comité de contrôle des configurations pour faciliter ce travail de suivi, constitué de personnes compétentes en gestion des configurations, que l'on consulte pour valider ou autoriser l'installation d'une version du logiciel dans l'environnement de production. Un tel comité est généralement mis en place après les tests par les utilisateurs et les autres tests nécessaires pour s'assurer que les autres systèmes continueront de fonctionner comme avant après installation du nouveau système ou logiciel (par exemple, test d'intégration[48] ou test de régression[49]). Il est important de faire figurer l'intégration aux systèmes existants et les tests de régression associés dans l'accord d'externalisation conclu avec le développeur. Il est tout aussi important de veiller au suivi des configurations non seulement dans l'environnement de production, mais également dans l'environnement de test pendant le développement.

III. Risques pour l'entité auditée

Lorsqu'une organisation développe un logiciel en interne, elle s'expose à un certain nombre de risques ou de difficultés pouvant compromettre la réussite du projet. Ces risques peuvent concerner le niveau de compétence dans le domaine du logiciel, l'expérience dans le domaine des tests et de la gestion de projet, la fiabilité des estimations de coûts et avantages, ou encore la capacité à suivre l'avancement du projet. Des problèmes peuvent par exemple découler d'une mauvaise application des procédures et méthodes de développement agile. Omettre de définir les principaux rôles, de hiérarchiser les contraintes système ou de déployer des capacités automatisées sont certains des problèmes que l'on peut rencontrer ici.

De même, le travail de collecte, de test et de validation des contraintes du logiciel du système doit inclure tous les utilisateurs finaux (internes et externes). Les auditeurs doivent donc vérifier si les utilisateurs ont été consultés en phase de définition du cahier des charges. Les auditeurs doivent également vérifier si les collaborateurs participant au travail d'assurance qualité réalisent une évaluation indépendante et objective de la qualité du système en cours de développement. Comme dans le cas d'une acquisition, il est important d'informer périodiquement la direction de l'état d'avancement du projet, afin qu'elle puisse décider des actions correctrices, le cas échéant.

Le principal aspect sur lequel les auditeurs doivent se concentrer dans l'examen de l'acquisition d'un système (d'un produit) par une organisation consiste à déterminer si l'organisation assure un suivi du travail du prestataire et si elle obtient des rapports périodiques sur l'avancement du projet et les actions correctrices décidées. Pour cela, il faut que le contrat prévoie des jalons, des étapes clés du développement et du déploiement, correspondant à une revue formelle et à l'établissement d'un rapport d'avancement dressant pour l'organisation un état des coûts, des délais, et de la performance. L'auditeur doit s'assurer que la direction de l'organisation ou ses collaborateurs désignés reçoivent et examinent effectivement des rapports d'avancement et un suivi des activités contractuelles, et décident le cas échéant des actions correctrices nécessaires.

---

[48] Les tests d'intégration correspondent à la phase de test du logiciel pendant laquelle les différents modules sont combinés pour les tester ensemble. Ces tests interviennent généralement après les tests isolés et avant les tests de validation ou d'acceptation.

[49] Les tests de régression servent à vérifier que le logiciel précédemment développé et testé continue de fonctionner correctement après une modification ou après son interfaçage avec d'autres logiciels. Ces modifications peuvent concerner des améliorations du logiciel, des correctifs ou des changements de configuration. De nouveaux bogues ou des régressions peuvent être identifiés à l'occasion des tests de régression.

L'auditeur des SI doit également vérifier :

- si un travail de planification du projet a bien été mené, comprenant une estimation des ressources, du budget et du temps alloué ;
- si la décision de développement/acquisition était appropriée ;
- si les objectifs ont été atteints et les contraintes respectées ;
- si les coûts et avantages identifiés dans l'étude de faisabilité sont mesurés, analysés, et dûment communiqués à la direction ;
- si la dérive des objectifs a été maîtrisée ;
- si une revue périodique et une analyse des risques ont été réalisées pour chaque phase du projet.

IV. Références et lectures complémentaires

Chief Information Officers Council. *Resource Library: Publications, Playbooks, Guidance, and More*. https://www.cio.gov/resources/.

Defense Contract Audit Agency. *DCAA Contract Audit Manual*. https://www.dcaa.mil/Guidance/CAM-Contract-Audit-Manual/.

ISACA. *BAI01-BAI10 Manage—Audit Assurance Program*. 2014.

ISACA. *CISA Review Manual,* 27ème édition. 2019.

ISACA. *COBIT 2019 Framework* : *Governance and Management Objectives*. 2019.

ISACA. *System Development and Project Management Audit Program*. 2009.

National Institute of Standards and Technology. *Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View.* https://csrc.nist.gov/publications/detail/sp/800-39/final. Mars 2011.

Software Engineering Institute. *CMMI for Acquisition,* version 1.3. http://www.sei.cmu.edu/library/abstracts/reports/10tr032.cfm. 2010.

Software Engineering Institute. *CMMI for Development*, version 1.3. http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm. 2010.

Tsui, Frank et Orlando Karam. *Essentials of Software Engineering,* 2ème édition. 2011.

U.S. Government Accountability Office. *Agile Assessment Guide : Best Practices for Agile Adoption and Implementation.* GAO-20-590G. https://www.gao.gov/products/gao-20-590g. 28 septembre 2020.

U.S. Government Accountability Office. *Census Bureau Needs to Implement Key Management Practices.* GAO-12-915. https://www.gao.gov/products/gao-12-915. 18 septembre 2012.

CHAPITRE 4 : LES ACTIVITÉS INFORMATIQUES

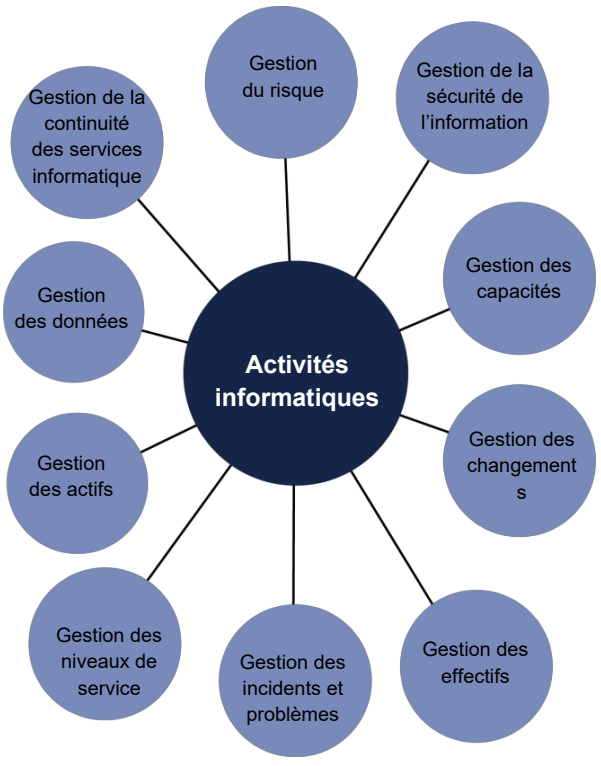
I. Qu'entend-on par « Activités informatiques » ?

Si l'on distingue de nombreuses interprétations ou définitions des activités informatiques, ce terme désigne habituellement les opérations courantes associées à l'exploitation et à l'entretien de l'infrastructure des systèmes d'information d'une organisation (exploitation des serveurs, maintenance, sécurité, gestion des espaces de stockage, plate-forme d'assistance, par exemple). Pour mesurer et gérer ces activités, on utilise des **indicateurs clés de performance** (ICP), qui fournissent une référence pour évaluer l'efficacité opérationnelle des activités. Il convient d'assurer le suivi continu et la revue périodique de ces indicateurs ou de critères équivalents. La plupart des organisations choisissent de les documenter dans un accord, conclu entre les utilisateurs métiers et le département ou prestataire informatique. Cet accord sur les niveaux de service (*service level agreement*, SLA) est un accord formel, dans lequel sont consignés les paramètres en question, ainsi que d'autres dispositions. Le présent chapitre aborde ces aspects plus en détail.

II. Les principales composantes des activités informatiques

Les activités informatiques que l'auditeur doit examiner pour déterminer si l'organisation est efficace en la matière sont, par exemple, la gestion de la continuité des services informatiques, de la sécurité de l'information, des capacités, des effectifs, des incidents et des problèmes, les procédures de maintien de la continuité opérationnelle, la gestion des changements, mais aussi la gestion du risque (voir fig. 8). Ces différents domaines, parmi d'autres, sont définis dans le référentiel ITIL (*Information Technology Infrastructure Library*, bibliothèque pour l'infrastructure des technologies de l'information)[50], l'un des référentiels bénéficiant de la plus large reconnaissance en matière d'identification, de planification, d'exécution et d'accompagnement des services informatiques d'une organisation.

Figure 8 : Les domaines des activités informatiques



Source : Unknown.

Pour établir si l'organisation auditée réalise les services documentés avec efficacité, l'auditeur vérifie si le SLA contient des paramètres spécifiques adaptés à ces services. Dans certains cas, lorsque l'organisation est de taille modeste, l'accord conclu entre l'organisation et le prestataire informatique peut être formalisé par un organigramme ou sous une autre forme, plutôt que dans un SLA. Quel que soit le nom qui lui est donné, ce document doit consigner les modalités de réalisation des services informatiques et être accepté par les groupes d'utilisateurs et le prestataire informatique.

[50] Axelos, « What is ITIL? » https://www.axelos.com/best-practice-solutions/itil/what-is-itil.

a. Gestion de la continuité des services informatiques

La gestion de la continuité vise à maintenir le respect des exigences de continuité de l'activité à un niveau approprié et à réduire les coûts engendrés par les temps d'arrêt et les conséquences des sinistres sur l'activité. Pour y parvenir, le prestataire informatique fixe des objectifs de durée maximale d'interruption (le temps nécessaire à la restauration des services) et des points de récupération (un moment antérieur au sinistre) pour les différents éléments des SI qui soutiennent les processus métiers. Le but est de préserver un niveau optimal de disponibilité et de performance des services. La gestion de la continuité comprend également la revue périodique et l'actualisation des durées maximales d'interruption et des points de récupération, pour s'assurer que ces critères restent conformes aux plans de continuité de l'activité et aux priorités des métiers. Cet aspect est traité plus en détail au chapitre 6.

b. Gestion du risque

La gestion du risque désigne les pratiques permettant de garantir que l'organisation comprend et traite les risques auxquels elle est exposée, ce qui inclut les risques relatifs aux activités informatiques. On entend par « risque » tout problème qui doit être minimisé ou atténué afin d'éviter des conséquences sur la capacité de l'organisation à créer de la valeur pour ses parties prenantes. Les risques pour les activités informatiques sont par exemple un comportement ou une activité sans autorisation sur le système, la divulgation sans autorisation d'informations à caractère personnel identifiables, une modification sans autorisation, etc. Les décisions de l'organisation en matière de risque s'appuient sur les pratiques et procédures de gestion du risque qu'elle a mises en place. Comme indiqué précédemment, les pratiques et procédures de gestion du risque relèvent principalement de quatre domaines : (1) préparation de la gestion du risque, (2) identification et analyse des risques, (3) atténuation des risques et (4) supervision par la direction. Le chapitre 3 apporte des informations complémentaires sur chacun de ces quatre domaines.

c. Gestion de la sécurité de l'information

Gérer la sécurité de l'information consiste à traiter les risques relatifs à la sécurité, à veiller au bon déploiement des contrôles de sécurité de l'information, à prendre des mesures le cas échéant, et à garantir que l'information soit disponible, utilisable, complète et non compromise au moment où on en a besoin. Cela consiste également à faire en sorte que seuls les utilisateurs autorisés puissent accéder à l'information, que l'information soit protégée pendant tout transfert et que son destinataire puisse avoir confiance dans l'intégrité de l'information. Cet aspect est traité plus en détail au chapitre 7.

d. Gestion des capacités

Gérer les capacités implique d'assurer le suivi des différents services sur lesquels l'organisation repose, de façon à pouvoir toujours répondre aux besoins de l'organisation ou des utilisateurs. Optimiser la capacité de débit du réseau, la disponibilité des ressources, les capacités de stockage et anticiper les besoins sont autant d'activités qui relèvent de la gestion des capacités. Le prestataire informatique doit dresser l'état des lieux des conditions existantes et prendre toutes mesures permettant d'assurer la mise à disposition de capacités complémentaires pour les utilisateurs. Il peut, par exemple, augmenter la puissance de traitement lorsque certains seuils sont franchis (si le taux d'utilisation des ordinateurs atteint ou dépasse 75 % pendant 60 % de la journée de travail, par exemple).

e. Gestion des changements

Habituellement, la gestion des changements pour un prestataire informatique concerne le suivi et la maîtrise des modifications apportées aux systèmes d'information et à leurs composants, dont les logiciels, le matériel et la documentation associée. Il est nécessaire de mettre en place des contrôles, pour s'assurer que tous les changements apportés à une configuration système sont autorisés, testés,

documentés et contrôlés, de sorte que le système continue à appuyer les activités opérationnelles dans les conditions prévues, et que la traçabilité des modifications soit garantie[51].

Dans la mise en œuvre des changements, il est important d'assurer une séparation des tâches de développement, de test et de production. Les développeurs de la modification ne doivent pas avoir accès à l'environnement de production. On réduit ainsi le risque de lancer directement en production des modifications qui n'ont pas été testées ou validées.

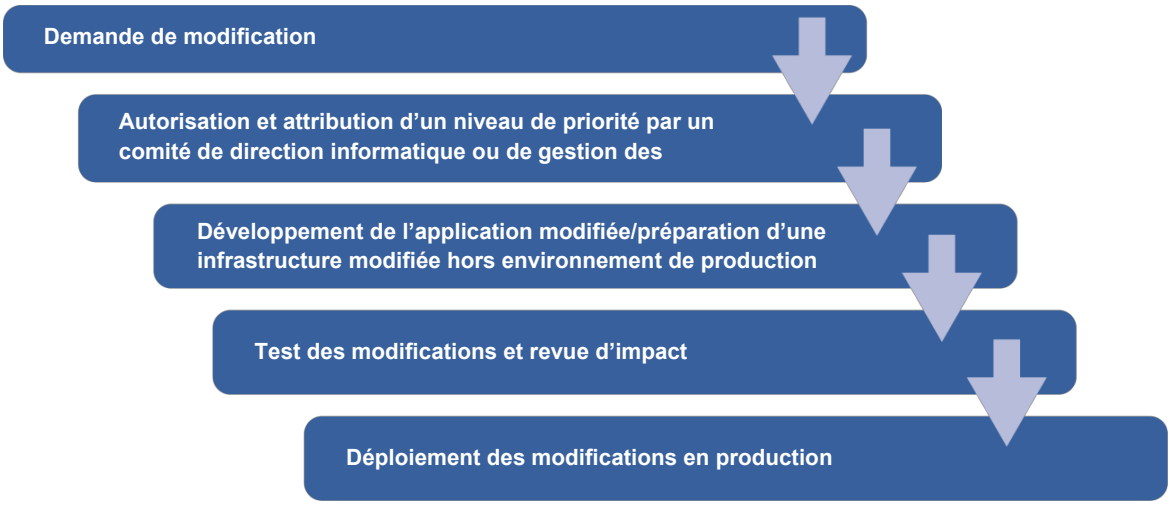
Une modification involontaire ou non validée pourrait compromettre la continuité de l'activité, avec des conséquences financières pour l'organisation. Il est important que l'organisation suive une procédure formalisée de gestion des changements, qui exige la validation de toute modification par un comité avant son déploiement dans l'environnement opérationnel. Cette procédure de gestion des changements doit permettre de s'assurer que les modifications sont enregistrées, évaluées, autorisées, hiérarchisées, planifiées, testées, mises en œuvre, documentées et examinées conformément aux procédures mises en place en matière de gestion des changements.

Un changement correspond à une modification de l'environnement opérationnel, du modèle d'affaires ou des besoins d'interfaçage des métiers, et peut être déclenché par l'analyse d'un incident ou d'un problème. La procédure de gestion des changements doit prévoir les activités suivantes :

- autorisation de la modification (par exemple, formalisation de la demande de modification),
- tests approfondis et autorisation par la direction opérationnelle avant déploiement en production,
- revue par la direction des effets de toute modification,
- conservation d'enregistrements adéquats,
- établissement de plans de secours (si quoi que ce soit se passe mal),
- établissement de procédures encadrant les modifications d'urgence.

La figure 9 présente les différentes étapes d'une procédure de gestion des changements.

Figure 9 Les étapes de la gestion des changements



Source : Unknown.

[51] Toutes les procédures visées dans cette section ne s'appliquent pas systématiquement à chaque changement apporté au SI. Par exemple, les **changements standards** sont généralement mineurs et présentent un faible niveau de risque pour les systèmes d'information. Ils requièrent par conséquent une supervision moins poussée (par exemple, abandon de la validation par un comité des changements, mais maintien des tests et de la validation opérationnelle).

La décision d'autorisation et de hiérarchisation du changement tient compte du coût, de l'impact sur le système d'information et les objectifs des métiers, des conséquences qu'il y aurait à ne pas déployer le changement, ainsi que de l'évolution anticipée des ressources.

Certaines **modifications d'urgence** doivent être déployées dans les meilleurs délais et ne peuvent suivre le déroulement de la procédure normale de contrôle des changements. Le temps disponible pour réaliser et tester ces modifications est réduit, ce qui augmente le risque d'erreur, notamment en programmation.

S'il existe une procédure de modification d'urgence, l'auditeur doit s'assurer qu'elle est raisonnable et comporte une certaine forme de contrôle. Par exemple, la validation de la modification d'urgence par un responsable habilité, le nommage des versions avec un suivi tout au long de la piste d'audit (au moyen d'applications de suivi automatisé des modifications), validation rétroactive par le comité de gestion des changements ou le propriétaire du système, tests *a posteriori*, mise à jour de la documentation.

f. Gestion des effectifs

La gestion des effectifs vise à garantir que les collaborateurs de l'organisation possèdent les compétences et connaissances requises pour leur rôle dans l'organisation. Pour un prestataire informatique travaillant au service des métiers, on considère que la gestion des effectifs est efficace si le personnel informatique déployé possède les qualifications et la formation requises, si les ressources sont suffisantes et les outils appropriés pour assurer le suivi du réseau et le fonctionnement des plates-formes d'assistance, et si des collaborateurs sont affectés de façon proactive au traitement de goulots d'étranglement sans compromettre la réactivité aux besoins des métiers. Comme indiqué au chapitre 2, les organisations devraient régulièrement évaluer leurs besoins en matière de ressources humaines (par exemple, compétences ou effectifs), analyser les manques, élaborer des stratégies et des plans pour y remédier, parmi d'autres activités essentielles.

g. Gestion des incidents et problèmes

La gestion des incidents correspond aux systèmes et pratiques mis en œuvre pour déterminer si les incidents ou erreurs sont consignés, analysés et résolus en temps utile. La gestion des problèmes vise à résoudre les difficultés rencontrées au moyen de l'analyse approfondie de tout incident majeur ou récurrent, afin d'en identifier les causes d'origine. Quand un problème a été identifié et que l'analyse des causes d'origine a été effectuée, ce problème devient une erreur ou déficience connue, et une solution peut être développée pour y remédier et empêcher que des incidents connexes ne se produisent à l'avenir.

Une procédure doit être formalisée pour documenter les conditions pouvant entraîner la détection et l'identification d'un incident. La partie du SLA consacrée aux activités informatiques doit comporter des procédures documentées de détection et d'enregistrement des conditions anormales. Pour faciliter l'analyse de ces conditions anormales, les organisations tiennent souvent un journal des différents incidents. Le journal, manuel ou automatisé, d'un logiciel dédié du SI permet d'enregistrer ces conditions. Les incidents sont par exemple un accès utilisateur sans autorisation ou une intrusion (sécurité), une défaillance réseau (exploitation), le mauvais fonctionnement d'un logiciel (niveau de service), ou le manque de qualification d'un utilisateur final (formation).

Dans le cadre de l'audit de la gestion des incidents et problèmes, l'auditeur doit examiner les rapports et journaux d'incidents/de problèmes, pour s'assurer que les différents points ont été résolus en temps utile et qu'ils ont été affectés aux personnes ou aux équipes les plus capables de les résoudre. Dans certains cas, il conviendra de déclencher un plan de reprise d'activité pour résoudre un incident. Les chapitres 6 et 7 contiennent davantage d'informations sur les plans de reprise d'activité et la gestion des incidents relatifs à la sécurité de l'information, respectivement.

h. Gestion des niveaux de service

Comme indiqué précédemment, le SLA recense les différents paramètres que le prestataire informatique applique pour fournir des services aux métiers. Les paramètres consignés dans le SLA sont généralement validés par les responsables métiers et par le prestataire informatique. L'auditeur utilise les paramètres du SLA pour déterminer si le prestataire informatique respecte les niveaux de service et si les responsables métiers sont satisfaits et prennent les mesures qui s'imposent en cas d'écart par rapport aux paramètres validés de niveau de service. Ces paramètres comportent des métriques permettant de quantifier la disponibilité, le degré d'utilisation ou le nombre d'erreurs. Généralement, un SLA ou une autre forme d'accord officiel est également conclu entre le prestataire informatique et ses sous-traitants. Par exemple, un prestataire informatique peut conclure plusieurs SLA avec ses différents fournisseurs de services d'externalisation (infogérance) ou d'informatique en nuage.

Dans certaines organisations, un accord peut également être conclu entre le prestataire informatique et les clients métiers au sein de l'organisation. On parle alors d'un accord sur les niveaux opérationnels (*Operational Level Agreement* - OLA). Les OLA sont similaires aux SLA par leur contenu, mais il s'agit d'accords internes par lesquels un prestataire de services définit les moyens qu'il met en œuvre pour respecter un SLA. Un OLA peut préciser par exemple un délai de réaction pour le traitement d'un incident, ou un niveau de disponibilité des serveurs. En général, les OLA servent à représenter les rapports internes entre le prestataire informatiques et un autre département de l'organisation.

Le SLA et l'OLA précisent notamment les ICP associés aux services informatiques. L'auditeur s'appuie sur l'examen des ICP pour poser des questions concernant les aspects suivants :

- les systèmes fonctionnent-ils conformément aux accords documentés ?
- a-t-on mis en place des mécanismes permettant d'identifier les lacunes de performance ou de sécurité, de traiter les lacunes identifiées et de suivre la mise en œuvre des actions correctrices décidées en conséquence de l'évaluation de la performance de l'organisation ?
- a-t-on identifié des problèmes liés au contrôle au sein de l'organisation auditée, ce qui aide à déterminer la nature, la séquence et le périmètre des tests ?

Le tableau suivant propose un exemple d'ICP, la définition correspondante et l'objectif de gestion du changement qui lui est associé :

Processus	Objectif (facteur clé de succès)	Indicateur clé de performance	Architecture de mesure
Gestion des changements	Réduire les incidents provoqués par des modifications accidentelles	Réduction du pourcentage d'incident résultant d'un accès non autorisé	Suivi de la gestion de l'incident et de la modification, compte rendu mensuel

L'auditeur pourra souhaiter analyser ces indicateurs plus en détail si les ICP ne permettent pas à l'organisation d'évaluer avec efficacité la progression et la réalisation des objectifs. Dans ce travail d'analyse, l'auditeur doit déterminer si les indicateurs contiennent des attributs importants qui en font un instrument efficace pour apprécier une progression et pour déterminer dans quelle mesure une organisation ou un prestataire atteint ses objectifs. Voici quelques exemples d'attributs possibles :

- **Clarté.** La mesure est énoncée clairement, sa désignation et sa définition sont cohérentes par rapport à la méthodologie appliquée pour la calculer.
- **Objectif mesurable.** La mesure vise une finalité numérique : elle est quantifiable ou contient des objectifs quantifiables ou d'autres mesures permettant de comparer la performance attendue aux résultats constatés.
- **Objectivité.** La mesure est raisonnablement exempte de biais significatif ou de toute manipulation susceptible de fausser l'évaluation de la performance.
- **Fiabilité.** La mesure produit les mêmes résultats dans des conditions identiques.

- **Données de référence et tendances.** La mesure est associée à des données de référence et à des tendances qui permettent d'identifier, de suivre et de rendre compte d'un changement de performance, et qui contribuent à ce que la performance soit considérée en contexte.
- **Lien.** La mesure est alignée sur les objectifs et les missions définis à l'échelle de la division et de l'organisation ; elle est communiquée clairement dans l'ensemble de l'organisation[52].

Dans certains cas, le prestataire informatique choisit de confier à un fournisseur la majeure partie de ses attributions. En pareilles circonstances, le prestataire informatique assure l'interface entre le fournisseur et les utilisateurs. Il assure le suivi du travail du fournisseur, pour veiller à ce que les besoins des métiers soient satisfaits. Le Chapitre 5 contient des informations complémentaires concernant l'externalisation.

i. Gestion des actifs

Gérer les actifs consiste à identifier et inventorier les actifs matériels ou immatériels qui méritent d'être protégés. Ces actifs englobent les collaborateurs, l'information, l'infrastructure, les finances et la réputation. Il est impossible de protéger ou gérer de manière efficace un actif qui n'aurait pas été préalablement identifié. La gestion des actifs permet également aux organisations de s'assurer que leurs actifs sont entretenus, mis à niveau, puis cédés de façon conforme. Auparavant, les actifs étaient plus faciles à contrôler, parce qu'ils étaient souvent gérés à l'intérieur du périmètre de l'organisation. Aujourd'hui en revanche, les organisations externalisent des services et des actifs. La gestion des actifs présente différents avantages : elle permet notamment d'améliorer l'utilisation, limiter les déperditions, optimiser la productivité et contribuer au maintien de la continuité opérationnelle.

j. Gestion des données

La gestion des données consiste à traiter et sécuriser les données qui constituent une ressource de valeur pour l'organisation. Dans ce cadre, l'organisation recueille, stocke et sécurise des données, gère leur accessibilité et leur intégration, et nettoie les données pour analyse. Les organisations recueillent des données auprès de différentes sources, dont les systèmes transactionnels, scanners, capteurs, réseaux sociaux et appareils connectés. Les données collectées peuvent ensuite être utilisées pour prendre des décisions et créer de la valeur. La gestion des données recouvre différentes activités :

- générer, consulter et actualiser des données
- stocker des données sur plusieurs sites et en nuage
- garantir une disponibilité élevée des données, et la reprise après sinistre
- utiliser des données à l'appui des applications, de l'analyse, des algorithmes
- garantir la confidentialité et la sécurité des données
- supprimer les données conformément à la législation et à la réglementation applicables

Les organisations s'appuient sur des systèmes de gestion des données pour traiter les données nécessaires aux travaux d'analyse et aux algorithmes qu'elles utilisent. Bien que les organisations mettent en place des outils automatisés pour gérer ces systèmes, elles doivent conserver dans leurs effectifs des administrateurs de bases de données capables d'intervenir manuellement.

Pour mieux gérer ses données, l'organisation peut mettre en place des pratiques de gouvernance des données. La gouvernance des données fournit un cadre à la gestion des données dans l'organisation. Les organisations définissent des politiques et procédures qui guident leur gestion des données tout au long du cycle de vie de ces données. La gouvernance aide les organisations à protéger leurs données en documentant les actifs et les contrôles d'accès, en identifiant les responsables et les propriétaires des données, en élaborant des politiques de diffusion interne et externe des données. La gestion des données comprend d'autres fonctions :

---

[52] Pour plus d'informations sur les principaux attributs des ICP, voir la publication du GAO, l'ISC des États-Unis : U.S. Government Accountability Office, *Defense Logistics: Improved Performance Measures and Information Needed for Assessing Asset Visibility Initiatives*, GAO-17-183, (16 mars 2017), https://www.gao.gov/products/gao-17-183.

- la **gestion de l'architecture des données**, qui définit les données dont l'organisation a besoin ;
- le **développement de données**, qui désigne le développement, le déploiement et la maintenance de solutions permettant de répondre aux besoins de l'organisation en matière de données ;
- la **gestion des opérations sur données**, qui désigne la planification, le contrôle et l'aménagement d'un support pour les données structurées tout au long du cycle de vie des données ;
- la **gestion de la sécurité des données**, qui consiste à exécuter les politiques et procédures de sécurité pour garantir la confidentialité, l'intégrité et la disponibilité des données ;
- la **gestion des entrepôts de données et l'informatique décisionnelle**, qui met en place des processus permettant de prendre des décisions concernant les rapports de données, les requêtes et l'analyse de données.

III. Risques pour l'entité auditée

Comme indiqué précédemment, les principaux outils de l'auditeur sont les accords SLA et OLA. Ces accords définissent les paramètres, les indicateurs de performance et les exigences qui serviront de référence pour mesurer l'efficacité du prestataire informatique. Si ces documents n'ont pas été établis ou n'ont pas été formellement revus et validés par les propriétaires des (processus) métiers, l'organisation court le risque que ses ressources informatiques ne soient pas utilisées de manière efficace et optimale. Après avoir obtenu communication du SLA et de l'OLA, l'auditeur doit obtenir les rapports périodiques du prestataire informatique dans lesquels sont consignés le suivi et les résultats des indicateurs. Il doit également consulter le compte rendu d'examen de ces rapports par la direction ainsi que les actions requises ou les directives au prestataire informatique dès lors que des écarts significatifs ont été constatés par rapport aux paramètres convenus dans l'accord.

Pour ce qui concerne la gestion des changements, l'auditeur doit vérifier si l'organisation a mis en place des procédures de contrôle des changements qui garantissent que l'intégrité du système est préservée et que seules sont introduites dans l'environnement opérationnel des applications validées et testées.

L'auditeur doit également apprécier dans quelle mesure l'organisation gère les capacités (par exemple, en matière de stockage, d'utilisation des processeurs et des ressources réseau) par anticipation, de manière à assurer la réactivité aux besoins des utilisateurs et à pouvoir traiter les incidents et autres problèmes de sécurité sans compromettre le fonctionnement opérationnel.

IV. Références et lectures complémentaires

Atlassian. *What Is IT Asset Management (ITAM)?* https://www.atlassian.com/itsm/it-asset-management. 2022.

Axelos. *What is ITIL?* https://www.axelos.com/best-practice-solutions/itil/what-is-itil.

Axelos. *ITIL Foundation: ITIL 4 Edition (ITIL 4 Foundation)*. Norwich : TSO, 2019.

Cichonski, Paul, Thomas Millar, Tim Grance, and Karen Scarone. *NIST Special Publication 800-61, rev. 2: Computer Security Incident Handling Guide*. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final. 2012.

CISA. *Item Development Guide.* https://www.isaca.org/-/media/files/isacadp/project/isaca/certification/cisa/cisa-item-development-guide_bro_eng_0219.pdf. Octobre 2018.

Cisco. *Gestion de niveau de service : Livre blanc sur les pratiques recommandées.* https://www.cisco.com/c/fr_ca/support/docs/availability/high-availability/15117-sla.html. 4 octobre 2005.

DAMA International. *Data Management Body of Knowledge,* 1st ed. https://www.dama.org/cpages/body-of-knowledge. 2010.

ISACA. *Change Management Audit Programme.*

ISACA. *CISA Review Manual*. 27ème éd. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KokCEAS. ISACA, 2011.

ISACA. *COBIT 2019 Framework* : *Governance and Management Objectives*. 2019.

Knight, Michelle. *What is Data Governance?* https://www.dataversity.net/what-is-data-governance/. 18 décembre 2017.

Oracle. *What Is Data Management?* https://www.oracle.com/database/what-is-data-management/.

Profisee. *Data Governance—What, Why, How, Who & 15 Best Practices.* https://profisee.com/data-governance-what-why-how-who/.

SAS. *Data Management : What It Is and Why It Matters.* https://www.sas.com/en_us/insights/data-management/data-management.html.

U.S. Government Accountability Office. *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities.* GAO-20-129. https://www.gao.gov/products/gao-20-129. 30 octobre 2019.

U.S. Government Accountability Office. *Defense Logistics: Improved Performance Measures and Information Needed for Assessing Asset Visibility Initiatives*. GAO-17-183. https://www.gao.gov/products/gao-17-183. 16 mars 2017.

CHAPITRE 5 EXTERNALISATION

I. Qu'est-ce que l'externalisation ?

L'externalisation consiste à confier à une entité externe une fonction ou un service opérationnel que l'organisation assurait jusqu'alors en interne, ou une nouvelle fonction ou un nouveau service opérationnel. L'entité sous-traitante est responsable de l'exécution des services contractuels, en contrepartie d'une rémunération négociée. L'organisation peut choisir d'externaliser certaines parties (ou la totalité) de ses infrastructures, de ses services ou de ses processus informatiques. L'organisation doit avoir rédigé une politique ou une déclaration d'intention précisant quelles fonctions opérationnelles sont externalisées (généralement, les technologies de l'information) et quelles fonctions sont conservées en interne.

a. Les avantages de l'externalisation

L'externalisation présente certains avantages, dont voici une liste non exhaustive :

ix. Souplesse dans la gestion du personnel

Si un projet exige des compétences qui ne sont pas présentes dans l'organisation à la date considérée, l'organisation peut décider d'externaliser le projet plutôt que de former des collaborateurs. Elle économise ainsi du temps et le coût de la formation. En outre, pour les opérations pour lesquelles il existe une demande saisonnière ou cyclique, l'externalisation permet d'ajouter des ressources aux équipes quand l'organisation en a besoin, puis de s'en séparer quand les opérations saisonnières sont terminées. Cette possibilité peut être particulièrement avantageuse sur les marchés volatils, la flexibilité et l'évolutivité des effectifs permettant de réduire le risque.

x. Réduction des coûts

L'externalisation permet habituellement de réduire les coûts en transférant le coût de la main-d'œuvre et d'autres dépenses connexes à un fournisseur dont le coût de main-d'œuvre est inférieur. Les prestataires informatiques s'efforcent d'externaliser les activités qu'il serait plus coûteux de réaliser en interne. Par exemple, un travail relatif à un logiciel, exigeant des compétences spécialisées. Les organisations qui ne comptent pas dans leurs effectifs des collaborateurs qualifiés pour effectuer ce travail auront financièrement intérêt à externaliser ce travail. L'externalisation d'opérations non essentielles aide également l'organisation à se concentrer sur son cœur de métier, pour délivrer de meilleurs résultats.

xi. Experts sur demande

L'externalisation permet à l'organisation de contacter des experts en cas de besoin pour l'aider à traiter des problèmes connus ou émergents. L'organisation peut ainsi réagir rapidement à l'évolution des besoins des métiers (par exemple, de nouvelles missions ou la prise en charge de fonctions supplémentaires) avec l'aide des experts. Les experts peuvent aussi aider les collaborateurs internes de l'organisation qui travaillent avec le fournisseur, en assurant une formation sur le terrain et un transfert direct de connaissances.

xii. Atténuation du risque

Sur les marchés volatils en particulier, les organisations cherchent à atténuer le risque en renforçant le recours à l'externalisation. Elles peuvent par exemple diminuer les ressources et le personnel informatiques dont elles disposent en interne, et les externaliser pour gagner en flexibilité et en évolutivité dans un environnement changeant. Les prestataires informatiques peuvent décider d'externaliser tout ou partie de leurs opérations, et en fonction du niveau de risque associé au service externalisé, décider d'y appliquer des contrôles plus ou moins formels. Il faut absolument garder à l'esprit que l'organisation reste responsable en dernier recours de la réalisation des fonctions ou services. En effet, elle a transféré une fonction, pas la responsabilité qui lui est associée.

b. Exemples d'externalisation

D'après l'ISACA[53], les organisations peuvent externaliser différents aspects de leurs activités et infrastructures informatiques. Par exemple :

- l'infrastructure opérationnelle, qui peut comprendre un centre de données et les processus associés
- le traitement d'applications internes par un prestataire de services
- le développement de systèmes ou la maintenance d'applications
- l'installation, la maintenance et la gestion des équipements de bureautique et des réseaux associés

L**'informatique en nuage** est aujourd'hui l'un des services parmi les plus externalisés. Le modèle de l'informatique en nuage permet d'accéder à la demande, sur le réseau, à un ensemble de ressources informatiques configurables (applications, réseaux, serveurs, stockage et autres services). Entre autres avantages, l'informatique en nuage peut aider les organisations à accéder à des ressources informatiques sur le principe du paiement à l'utilisation, et leur apporter la flexibilité nécessaire pour faire évoluer rapidement une solution informatique.

Par exemple, l'organisation peut externaliser le traitement de données ou un autre service, que le sous-traitant assurera à l'aide de ses propres ressources informatiques. Dans ce cas, c'est généralement le sous-traitant qui héberge l'équipement, tandis que l'organisation conserve la maîtrise des applications et des données. L'informatique en nuage peut aussi impliquer l'utilisation des ordinateurs du sous-traitant pour stocker et sauvegarder les données de l'organisation, en conservant la possibilité d'un accès en ligne. L'organisation doit posséder une connexion Internet performante si elle souhaite que son personnel ou ses utilisateurs bénéficient d'un accès rapide aux données ou à l'application de traitement des données. Dans l'environnement actuel, les données ou les applications sont également accessibles à partir de plates-formes mobiles (un ordinateur portable connecté à Internet par le Wi-Fi ou au moyen d'une carte de données mobiles, un Smartphone, une tablette).

L'informatique en nuage désigne habituellement trois modèles de services distincts :

- **Logiciel à la demande** (***Software as a service*, SaaS)**. L'organisation utilise l'application et l'infrastructure fournies par le sous-traitant.
- **Plate-forme à la demande (*Platform as a service*, PaaS**). L'organisation utilise l'infrastructure en nuage fournie par le sous-traitant pour exécuter des applications dont le sous-traitant est propriétaire.
- **Infrastructure à la demande (*Infrastructure as a service***). L'organisation externalise différentes ressources informatiques auprès d'un sous-traitant, notamment, capacité de traitement et de stockage, réseaux. L'organisation ne gère pas l'infrastructure, mais maîtrise l'application et le système d'exploitation utilisés.

En complément des différents modèles de services, on distingue quatre modèles de déploiement :

- **Nuage privé**. L'infrastructure est fournie pour utilisation exclusive par une seule organisation.
- **Nuage communautaire**. L'infrastructure en nuage est fournie à une communauté de consommateurs partageant souvent des intérêts communs (concernant par exemple, la mission, la sécurité ou la conformité).
- **Nuage public**. L'infrastructure est mise à la disposition du grand public. Elle est habituellement gérée par une entreprise, une organisation universitaire ou publique.
- **Nuage hybride**. L'infrastructure combine au moins deux des modèles d'infrastructures précédemment cités, qui sont interopérables pour faciliter la portabilité des données et des applications.

[53] *Outsourced IT Environments Audit /Assurance Programme (*2009) (Programme d'audit/d'assurance des Environnements informatiques externalisés)

Bien configurer le nuage informatique contribue à réduire le risque de failles de sécurité. L'application de contrôles de sécurité supplémentaires permet de créer un environnement en nuage dont la défense peut être assurée. Les contrats d'informatique en nuage doivent également contenir des dispositions concernant la non-divulgation de données sensibles, définir ce qui constitue une violation de sécurité, et décrire comment le sous-traitant informera l'organisation en cas de violation.

En résumé, l'informatique en nuage peut être avantageuse à plus d'un titre pour l'organisation : maîtrise des coûts, disponibilité immédiate, flexibilité et évolutivité dynamiques, solution de sauvegarde limitant les temps d'arrêt. En revanche, comme toute solution d'externalisation, le déploiement de l'informatique en nuage présente également des risques et des difficultés. L'informatique en nuage peut ainsi introduire de nouveaux risques, comme une erreur de configuration, une mauvaise interprétation des responsabilités communes, des contrôles d'accès insuffisants, des ressources en nuage partagées avec d'autres utilisateurs du fournisseur de services d'informatique en nuage, des vulnérabilités dans la chaîne logistique. Le modèle de facturation à l'utilisation de l'informatique en nuage peut aussi s'avérer très coûteux, si l'organisation ne met pas en place une surveillance et un contrôle de l'utilisation de ces services.

II. Les principales composantes de l'externalisation

a. Politique d'externalisation

Les organisations doivent avoir rédigé une politique précisant quelles fonctions peuvent être externalisées et quelles fonctions doivent être conservées en interne[54]. Elles externalisent habituellement les activités informatiques de routine, les opérations de maintenance et les plates-formes de matériel bureautique. Les dossiers des ressources humaines du personnel sont généralement tenus en interne, sous surveillance étroite, et font l'objet de nombreuses contraintes de confidentialité et de sécurité. En raison d'un coût élevé, externaliser cette fonction ne serait pas rentable.

L'auditeur doit commencer son travail par l'examen de la politique et des procédures de l'organisation concernant l'externalisation. Les grandes organisations, qui externalisent souvent une grande partie de leurs activités opérationnelles, doivent impérativement avoir mis en place une politique d'externalisation validée, définissant clairement les processus de sous-traitance. Si les petites organisations ne disposent pas forcément d'une politique formalisée, il est important qu'elles appliquent des procédures d'appel d'offres efficaces et transparentes. Quelle que soit leur taille, les organisations doivent appliquer une réelle stratégie de gouvernance fixant les orientations et les objectifs de l'externalisation.

b. Sollicitation

La sollicitation correspond au travail de documentation du cahier des charges du système et au collationnement des différents éléments de référence dont le fournisseur aura besoin pour construire ce système. L'organisation crée un dossier d'appel d'offres et le diffuse, reçoit des propositions et sélectionne un prestataire parmi les soumissionnaires. Le processus de sélection doit être transparent, objectif, et reposer sur des critères adaptés au système ou aux services achetés. Pour prendre sa décision, l'organisation doit examiner attentivement les candidatures, afin de détecter toute difficulté susceptible de faire obstacle à la bonne exécution du service.

c. Gestion des fournisseurs

La gestion des fournisseurs est un aspect important du processus d'externalisation. Elle permet d'assurer que les services sont exécutés conformément aux attentes de l'organisation. L'organisation doit donc

[54] Organisation internationale de normalisation/commission électrotechnique internationale. *Information Technology—Cloud Computing—Guidance for Policy Development* (Genève, Suisse : Organisation internationale de normalisation, janvier 2019).

avoir mis en place des processus encadrant le suivi périodique de l'avancement du projet, de la qualité du service, et les tests sur les produits réalisés avant leur déploiement en environnement opérationnel. Ce suivi des fournisseurs peut comporter un audit des processus d'assurance qualité internes des fournisseurs, pour vérifier si les collaborateurs du fournisseur appliquent à l'ensemble de leur travail les procédures et les plans validés contractuellement.

Le SLA est un élément important de la gestion des fournisseurs. Comme indiqué précédemment, le SLA est un accord conclu entre l'organisation et le fournisseur, qui joue un rôle clé dans le suivi des relations. Le SLA doit préciser les services que l'on attend du fournisseur ainsi que les paramètres techniques de ces services ; cet accord conclu entre le fournisseur et l'organisation est légalement contraignant.

Le SLA couvre généralement les aspects suivants de la gestion des fournisseurs :

- la nature des prestations qui seront assurées par le fournisseur ;
- la répartition des responsabilités entre l'organisation et le fournisseur ;
- les services qui seront mesurés, la période et la durée des mesures, les sites et les périodes visés par le compte rendu (par exemple, taux de défaillance, délai de réaction, horaires de disponibilité de la plate-forme d'assistance) ;
- le temps nécessaire au déploiement d'une nouvelle fonctionnalité, l'ampleur des remaniements ;
- le niveau des droits d'accès octroyés au fournisseur pour l'exécution des prestations ;
- le type de documentation requise pour les applications développées par le fournisseur ;
- le lieu d'exécution des prestations ;
- la fréquence des sauvegardes et les paramètres de récupération des données ;
- les modalités de résiliation et les méthodes et formats de remise des données ;
- la procédure de remise de rapports réguliers, la communication d'informations concernant les incidents et problèmes ;
- les clauses d'incitation et de pénalité.

Si le SLA concerne l'informatique en nuage, l'organisation peut y contractualiser différentes pratiques pour contribuer à garantir que les services seront réalisés de manière efficace, efficiente et sécurisée[55]. Voici quelques exemples de ces pratiques :

- définir des critères de mesure de la performance, comme le niveau de service (par exemple, une durée), le niveau de capacité (par exemple, un nombre maximum d'utilisateurs) et le délai de réaction (par exemple, la rapidité de traitement d'une transaction) ;
- préciser quand et comment l'organisation accède à ses données et réseaux hébergés chez le fournisseur, en particulier à la résiliation du contrat ;
- préciser les modalités de surveillance de la performance par le fournisseur d'informatique en nuage et à quel moment l'organisation effectuera une revue de performance ;
- définir des métriques de sécurité, comme l'identité des personnes pouvant accéder aux données et les protections entourant les données ;
- définir les conditions de notification en cas de violation de l'accord.

En résumé, le SLA doit consigner l'essentiel des aspects critiques pour l'organisation. L'auditeur doit demander à consulter le SLA ou tout autre document (contrat ou accord formalisé) où ces paramètres sont consignés. Il doit déterminer si l'organisation a établi un cahier des charges pour la fonction

[55] Organisation internationale de normalisation/commission électrotechnique internationale, *ISO/IEC 19086-1, Technologies de l'information — Informatique en nuage — Cadre de travail de l'accord du niveau de service — Partie 1 : Aperçu général et concepts* (15 septembre 2016), https://www.iso.org/standard/67545.html et U.S. Government Accountability Office, *Cloud Computing : Agencies Need to Incorporate Key Practices to Ensure Effective Performance,* GAO-16-325, (7 avril 2016), https://www.gao.gov/products/GAO-16-325.

externalisée avant de sélectionner un fournisseur (les contraintes spécifiques et les paramètres opérationnels sont-ils consignés dans le contrat et le SLA ?), si l'organisation contrôle le respect par le fournisseur des exigences énoncées dans le SLA (au moyen de rapports d'avancement périodiques) et le cas échéant, si l'organisation a pris des mesures lorsque le fournisseur n'a pas respecté les paramètres énoncés dans le SLA (sous la forme d'actions correctrices ou de pénalités financières).

d. Analyse de rentabilité

Les organisations peuvent recourir à l'externalisation dans un objectif de réduction des coûts. L'externalisation est rentable si le coût d'achat des services auprès d'un fournisseur est inférieur au coût d'utilisation de la main-d'œuvre et des infrastructures internes de l'organisation. D'autres avantages ne sont pas directement mesurables, comme la possibilité de tirer profit des infrastructures du fournisseur pour faire évoluer rapidement le niveau du service, ou de s'appuyer sur son expertise dans certaines circonstances. Dans la mesure du possible, l'organisation doit s'efforcer de déterminer si le gain financier escompté est réalisé sur une période donnée. Le résultat de cet examen est l'un des critères sur lesquels fonder la décision de poursuivre l'externalisation des capacités, ou d'y mettre fin.

e. Sécurité

L'externalisation n'exonère pas le prestataire informatique de l'organisation de l'obligation d'évaluer si ses fournisseurs ont mis en place des pratiques de sécurité suffisamment rigoureuses et s'ils sont à même de se conformer aux exigences internes de sécurité. Si les prestataires informatiques jugent généralement que les pratiques de sécurité des fournisseurs sont impressionnantes (souvent supérieures à leurs pratiques internes), le fait même que les données aient été externalisées augmente le risque de violation de sécurité et la nécessité de protéger la propriété intellectuelle. Les questions de confidentialité doivent elles aussi être réglées. Parmi les autres préoccupations de sécurité, citons l'utilisation frauduleuse ou la divulgation de données sensibles, l'accès non autorisé aux données, aux applications, au plan de reprise d'activité après sinistre. Si ces problématiques constituent rarement un obstacle majeur à l'externalisation, il est important de consigner par écrit les exigences en la matière.

Par la nature même des fonctionnalités de cette technologie, l'utilisation de l'informatique en nuage renforce également la nécessité de mettre en place des pratiques de sécurité rigoureuses. La dépendance envers des tiers, la complexité croissante de la mise en conformité avec la législation et la réglementation (sur un territoire couvrant parfois plusieurs pays), la dépendance à l'Internet en tant que principal canal de données, et le caractère dynamique de l'informatique en nuage (par exemple, la multiplicité des sites de traitement), comptent parmi les problématiques de sécurité à prendre en considération. La suite du chapitre apporte davantage d'informations à ce sujet et sur les risques connexes.

Certains fournisseurs ou organismes prestataires font l'objet d'audits indépendants, en raison de leur taille et du nombre d'organisations sous contrat. Pour ces fournisseurs, un rapport de contrôle est établi, dressant la liste des contrôles de sécurité de l'information, avec une évaluation de leur efficacité. Ces rapports comprennent une évaluation indépendante des contrôles mis en place par le fournisseur ou l'organisme prestataire, dont les contrôles internes et les contrôles relatifs à la sécurité, à la disponibilité, à l'intégrité et à la confidentialité. L'auditeur peut demander à consulter ces rapports via l'organisation auditée.

III. Risques pour l'entité auditée

a. Perte de la connaissance métier et de la propriété des processus métiers

L'externalisation présente un risque inhérent de perte de la connaissance métier, détenue par les développeurs des applications. Si le fournisseur n'est pas capable d'assurer ce service, le prestataire informatique doit se préparer à assumer à nouveau cette responsabilité. De même, si l'application est développée en externe, l'organisation risque d'abandonner ou de perdre la propriété du processus métier, dont le fournisseur pourra alors revendiquer la propriété intellectuelle. Les organisations doivent

régler cette question à l'étape de contractualisation, et veiller à disposer d'une documentation complète du processus de développement du système et de la conception du système. Il est essentiel que le dossier d'appel d'offres envoyé aux fournisseurs soit en cohérence avec la planification stratégique de l'organisation, qu'il soit suffisamment précis et détaillé pour écarter toute ambiguïté ou imprécision concernant les exigences. Cette rigueur permettra également à l'organisation de changer plus facilement de fournisseur, le cas échéant.

b. Incapacité du fournisseur à assurer la prestation

Il est possible qu'un fournisseur ne respecte pas les délais de livraison d'un produit ou que le produit doive être abandonné parce qu'il n'assure pas les fonctionnalités requises. Si la procédure d'externalisation n'est pas appliquée correctement, il est très probable que le système ou les services fournis ne répondront pas aux besoins des utilisateurs ou aux standards de qualité, qu'ils seront plus coûteux et que leur maintenance et leur exploitation exigeront l'engagement de ressources significatives, voire même, que l'organisation sera contrainte de les remplacer à brève échéance. La défaillance d'un fournisseur s'explique généralement par la mauvaise rédaction du contrat, certaines lacunes de la procédure de sélection des fournisseurs, un manque de précision des jalons du projet, ou encore une conjoncture défavorable.

Pour faire face à cette éventualité, les prestataires informatiques ont besoin de plans de secours. Au moment d'envisager l'externalisation d'un service, le prestataire informatique doit évaluer les conséquences d'une possible défaillance du fournisseur (une défaillance aura-t-elle des conséquences significatives sur la performance de l'organisation ?). Disposer d'une documentation détaillée sur la conception et le développement du système aidera l'organisation à assurer la continuité de l'activité en ayant recours à un autre fournisseur ou en s'appuyant sur ses ressources internes.

c. Manque de personnel qualifié au sein de l'organisation pour gérer les contrats d'externalisation

L'organisation doit former et conserver dans ses effectifs des collaborateurs qualifiés, capables d'assurer la gestion conforme des contrats d'externalisation. Si elle manque de personnel qualifié au cours de l'exécution du contrat, l'organisation auditée pourrait payer au fournisseur des sommes qui ne sont pas dues ou ne pas obtenir les résultats attendus. L'externalisation pourrait même s'avérer un échec complet. De même, les organisations ont intérêt à mettre en concurrence plusieurs fournisseurs, à évaluer en continu les prestations afin de les optimiser. En l'absence de supervision efficace, les organisations n'obtiendront pas la flexibilité attendue et perdront la maîtrise des prestations informatiques externalisées.

d. Caractère imprécis des prévisions de coûts et de délais

Tous les contrats externalisés s'appuient sur des données de référence et des hypothèses. Si en fin de compte le travail ne correspond pas au devis, le client doit payer la différence de coût qui en résulte. Bien des services informatiques ont découvert avec surprise que le prix n'était pas « fixe » (par exemple, le prix des ressources nécessaires à l'informatique en nuage) ou que le fournisseur s'attendait à être payé proportionnellement aux changements graduels apportés au périmètre du projet. De même, les organisations préparent souvent des études de cas excessivement optimistes, voire irréalistes. Il faut alors augmenter considérablement l'étendue des travaux au fur et à mesure de l'intégration des prestations externalisées.

e. Renouvellement fréquent des interlocuteurs

Sous l'effet de la croissance rapide des fournisseurs, le marché du travail connaît un grand dynamisme dans ce secteur d'activité. Certains collaborateurs sont fréquemment sollicités pour de nouveaux projets complexes, et le risque existe qu'ils soient débauchés par des fournisseurs délocalisés. Si les chiffres dont on dispose sur ces fournisseurs indiquent généralement un taux de renouvellement global des effectifs plutôt faible, le renouvellement des collaborateurs chargés spécifiquement de la gestion d'un

compte reste la principale statistique à surveiller. Le taux de renouvellement est alors de l'ordre de 15 à 20 %. Il est donc raisonnable d'établir les modalités contractuelles sur cette base.

f. Risques externes

Dans le domaine de l'informatique en nuage en particulier, les fournisseurs de prestations d'externalisation sont souvent implantés à l'étranger. Dans un tel environnement, l'externalisation expose l'organisation à des risques spécifiques : la réglementation étrangère sur le stockage et le transfert d'informations peut encadrer ce qu'il est permis de stocker et les conditions de traitement des informations, les données sont susceptibles d'être utilisées par les organismes d'application de la loi du pays sans que l'organisation en soit informée, les normes de confidentialité et de sécurité ne sont pas toujours adaptées et il est impossible d'écarter totalement la possibilité d'un litige de compétence judiciaire.

g. Sécurité de l'information

L'externalisation comporte de nombreux risques pour la sécurité de l'information, tels que l'utilisation frauduleuse ou la divulgation de données sensibles, ou encore l'accès non autorisé aux données, comme évoqué précédemment. L'utilisation de services d'informatique en nuage présente également des conséquences et des risques opérationnels dans les domaines suivants :

- Dépendance accrue envers des tiers, pouvant induire une augmentation des risques liés :
  - à la vulnérabilité des interfaces externes,
  - à l'agrégation des centres de données,
  - à l'application de processus d'assurance indépendants,
  - au fait que les organisations ne sont plus propriétaires des données et ne supervisent pas les contrôles appliqués par les tiers ;
- Complexité accrue de la mise en conformité avec la législation et la réglementation, ce qui entraîne :
  - un risque accru pour la confidentialité,
  - le transfert transfrontalier d'informations à caractère personnel identifiables,
  - des conséquences pour la conformité contractuelle ;
- Dépendance à l'Internet en tant que principal canal de données, ce qui entraîne :
  - des problèmes de sécurité inhérents à l'utilisation d'un environnement public,
  - des problèmes de connexion et de disponibilité du réseau Internet ;
- Caractère dynamique de l'informatique en nuage, induisant la possibilité :
  - d'un changement de localisation des installations de traitement par souci d'équilibrage des charges,
  - d'une implantation des installations de traitement dans différents pays,
  - d'un partage des équipements opérationnels avec des concurrents,
  - de problèmes juridiques (responsabilité, propriété, etc.), résultant des différences de législation dans les pays d'hébergement, ce qui peut exposer les données à un risque ;
- Risques en matière de gouvernance des technologies de l'information :
  - perte de gouvernance et de maîtrise des TI par l'organisation en lien avec l'utilisation de prestations d'informatique en nuage,
  - perte de réactivité aux besoins des clients par rapport à une exécution en interne des prestations,
  - un manque d'appui en interne, s'expliquant par la culture organisationnelle et par le fait que le client considère que les services en nuage sont associés à un niveau de risque plus élevé ;
- Risques liés à l'audit :
  - impossibilité d'accéder aux systèmes et aux journaux de sécurité des tiers ;
  - perte ou dégradation de l'information transmise aux clients par le prestataire en ce qui concerne les incidents de sécurité et la traçabilité de la piste d'audit,

- absence de ségrégation des données de journalisation entre différents clients, ainsi que d'autres risques de fuite de données de journalisation.

h. Enfermement propriétaire

L'enfermement propriétaire est un problème que l'organisation rencontre lorsqu'elle souhaite changer de fournisseur ou réinternaliser des activités externalisées, et qu'elle constate que ce changement s'avère trop coûteux. Cette situation peut se présenter quand l'organisation réalise des investissements significatifs dans un produit ou un service unique d'un fournisseur, mais qu'elle ne peut pas utiliser le produit ou le service sans passer par le fournisseur actuel. Dans le contexte de l'informatique en nuage, cette situation peut poser de graves difficultés, notamment parce que le transfert de données vers un autre environnement exige alors de reformater les données. D'autre part, l'organisation peut devenir dépendante du logiciel qu'elle utilise dans sa relation avec un fournisseur en particulier, et n'a pas la possibilité de changer facilement de fournisseur. Pour limiter le risque d'enfermement propriétaire, l'organisation doit examiner attentivement les services qui lui sont proposés, veiller à ce que les données puissent être facilement transférées, effectuer des sauvegardes fonctionnelles des données, et faire appel dans ce domaine aux services de plusieurs fournisseurs.

IV. Références et lectures complémentaires

Cour des comptes fédérale du Brésil (TCU). *Report Highlights: Cloud Computing*. https://portal.tcu.gov.br/en_us/biblioteca-digital/report-highlights-cloud-computing.htm. 15 juillet 2015.

Organisation internationale de normalisation/commission électrotechnique internationale. *ISO/IEC, 19086-1:2016, Technologies de l'information — Informatique en nuage — Cadre de travail de l'accord du niveau de service — Partie 1 : Aperçu général et concepts.* https://www.iso.org/fr/standard/67545.html. 15 septembre 2016.

Organisation internationale de normalisation/commission électrotechnique internationale. ISO/IEC, *19086-2:2018, Technologies de l'information — Informatique en nuage — Cadre de travail de l'accord du niveau de service — Partie 2 : Modèle métrique.* Genève, Suisse. Organisation internationale de normalisation, décembre 2018.

Organisation internationale de normalisation/commission électrotechnique internationale. ISO/IEC, *TR 22678:2019, Information technology – Cloud computing – Guidance for policy development.* Genève, Suisse. Organisation internationale de normalisation, janvier 2019.

Organisation internationale de normalisation/commission électrotechnique internationale. ISO/IEC, *27036-1:2014, Technologies de l'information — Techniques de sécurité — Sécurité d'information pour la relation avec le fournisseur — Partie 1 : Aperçu général et concepts.* Genève, Suisse. Organisation internationale de normalisation, 1er avril 2014.

International Organization for Standardization, organisation internationale de normalisation. *ISO 37500:2014, Lignes directrices relatives à l'externalisation*. Genève, Suisse. Organisation internationale de normalisation, 11 novembre 2014.

National Institute of Standards and Technology. *Special Publication 500-292: Cloud Computing Reference Architecture.* http://www.nist.gov/customcf/get_pdf.cfm?pub%5Fid=909505. Septembre 2011.

National Institute of Standards and Technology. *Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf. Décembre 2011.

National Institute of Standards and Technology. *Special Publication 800-145: The NIST Definition of Cloud Computing.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Septembre 2011.

National Security Agency. *Mitigating Cloud Vulnerabilities.* https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/csi-mitigating-cloud-vulnerabilities_20200121.pdf. 22 janvier 2020.

Secrétariat du Conseil du Trésor du Canada. *Ligne directrice sur les ententes de services – Synthèse* https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=25748. 4 juillet 2012.

U.S. Government Accountability Office. *Cloud Computing : Agencies Need to Incorporate Key Practices to Ensure Effective Performance.* GAO-16-325. https://www.gao.gov/products/GAO-16-325. 7 avril 2016.

CHAPITRE 6 : GESTION DE LA CONTINUITÉ DES ACTIVITÉS

I. Qu'entend-on par « gestion de la continuité des activités » ?

Les organisations du secteur public doivent pouvoir compter sur des systèmes d'information disponibles et opérationnels pour s'acquitter des obligations prévues par leur mandat. Ces systèmes jouent un rôle important dans différents aspects de l'activité des organisations, parmi lesquels l'évaluation et la collecte des revenus fiscaux et douaniers, le versement des retraites des fonctionnaires et des prestations de sécurité sociale, le traitement des statistiques nationales (par exemple, les données relatives aux naissances, aux décès, à la criminalité ou aux maladies). Dans les faits, de nombreuses activités seraient irréalisables ou ne pourraient pas être réalisées correctement sans l'apport des systèmes d'information. Pour limiter les interruptions et les temps d'arrêt de ces systèmes, les organisations doivent élaborer une stratégie de continuité des activités et des procédures pour la mettre en œuvre.

Les sinistres et autres situations de crise sont par nature imprévisibles. Si ces événements ne peuvent pas tous être évités, un plan de continuité permet souvent d'en atténuer l'impact. Les conséquences d'une rupture d'alimentation, d'un mouvement social, d'un incendie ou d'actes de malveillance sur les systèmes d'information peuvent être désastreuses. Faute d'avoir mis en place un plan de continuité exploitable, l'organisation pourrait devoir attendre des semaines avant de reprendre ses activités. En outre, les organisations confient souvent une part importante de leurs activités informatiques à des fournisseurs externes. Si un fournisseur de prestations externalisées venait à subir une interruption d'activité à cause d'un sinistre, les conséquences de cette situation pourraient également être graves pour l'organisation.

Les organisations doivent mettre en place des activités de gestion de la continuité opérationnelle pour éviter que des risques connus n'entraînent des interruptions de service. Pour cela, elles peuvent notamment planifier la **continuité de l'activité** et la **reprise d'activité**, et établir un **plan d'urgence pour le système d'information**. On utilise parfois l'un pour l'autre les termes « plan de continuité d'activité » et « plan de reprise d'activité », mais ils correspondent en fait à des réalités distinctes, bien que complémentaires. Ces deux types de plans sont importants pour l'auditeur des SI, parce qu'ensemble, ils garantissent que l'organisation sera capable de fonctionner à un niveau de capacité défini après une interruption, qu'elle soit d'origine naturelle ou humaine. Le plan d'urgence pour le système d'information est comparable au plan de reprise d'activité, mais il cible la restauration du système, quelle qu'en soit la localisation. Nous allons à présent examiner chaque type de plan :

- L'organisation utilise le **plan de continuité d'activité** pour planifier et tester la reprise de ses processus opérationnels après un sinistre. Ce plan décrit également la manière dont l'organisation continuera de fonctionner face à des circonstances défavorables (par exemple, des catastrophes d'origine naturelle ou autre, ou même l'absence de membres incontournables du personnel). Il a pour finalité de faire en sorte que l'organisation soit la plus résiliente possible. Une organisation résiliente est capable de maintenir les fonctions critiques à sa mission en cas de sinistre ou d'interruption de service.
- L'organisation utilise le **plan de reprise d'activité** pour planifier et tester la reprise de ses infrastructures informatiques après une catastrophe d'origine naturelle ou autre. Il est complémentaire du plan de continuité d'activité. Le plan de continuité d'activité s'applique aux fonctions opérationnelles de l'organisation, tandis que le plan de reprise d'activité concerne les infrastructures informatiques qui permettent les fonctions opérationnelles.
- L'organisation utilise le **plan d'urgence pour le système d'information** pour planifier et tester la remise en marche des différents systèmes d'information. Également complémentaire du plan de continuité d'activité, chaque plan d'urgence concerne un système en particulier. Le plan d'urgence sert à guider la reprise d'un système d'information, et peut être activé quelle que soit la localisation de ce système.

Par essence, le **plan de continuité d'activité (PCA)** prépare la capacité de l'organisation à maintenir son fonctionnement en cas de perturbation des conditions normales. Il englobe les politiques, les procédures et les pratiques qui permettent à l'organisation de restaurer et relancer après un sinistre ou

autre événement de crise les processus manuels et automatisés qui sont essentiels pour sa mission. En plus de définir les pratiques à appliquer en cas d'interruption, le PCA comprend parfois d'autres éléments comme les mesures à prendre pour la reprise après sinistre, les mesures d'urgence, la restauration des utilisateurs et les mesures de secours pour les systèmes d'information, certaines activités de gestion de crise. Les organisations qui appliquent ce type de PCA considèrent la planification de la continuité de l'activité comme un processus global, qui couvre autant la récupération après sinistre que la reprise des activités opérationnelles.

Toutefois, qu'il fasse partie intégrante du PCA ou qu'il soit consigné dans un document séparé, le **plan de reprise d'activité (PRA)** doit définir les ressources, les actions, les tâches et les données requises pour gérer la procédure de récupération de l'organisation en cas d'interruption de l'activité. Ce plan aide également l'organisation à restaurer les processus métiers affectés. Il énonce ainsi pas-à-pas les différentes mesures que l'organisation doit prendre pour préparer la reprise. Plus précisément, le PRA facilite la préparation et la planification avancées nécessaires pour limiter les dommages consécutifs aux sinistres et garantir la disponibilité des systèmes d'information essentiels de l'organisation. En ce qui concerne les technologies de l'information, le PRA recense les actifs technologiques critiques, dont les systèmes, applications, bases de données, matériels de stockage et autres ressources réseau[56].

En complément du PRA, les **plans d'urgence pour le système d'information (PUSI)** sont un élément critique de tout programme complet de planification de la continuité des activités. Les organisations peuvent élaborer un PUSI pour chaque système, en fonction du niveau de risque associé au système. En général, les étapes et les procédures décrites dans le PUSI sont équivalentes aux éléments du PCA, mais les PUSI sont conçus indépendamment du site ou de l'emplacement du système. Entre autres choses, le PUSI précise des informations importantes et spécifiques au système, telles que les rôles et responsabilités, informations d'inventaire, procédures d'évaluation et procédures détaillées de restauration du système concerné.

II. Les principaux éléments de la gestion de la continuité des activités

L'auditeur des SI est tenu d'évaluer les dispositifs de gestion de la continuité d'activité mis en place par l'organisation, ce qui implique notamment d'examiner les PCA, PRA et PUSI de l'organisation. Pour cela, l'auditeur doit comprendre les enjeux de l'élaboration d'un tel dispositif, et identifier les mesures qui lui permettront d'en évaluer l'efficacité.

Un travail efficace de planification de la continuité comporte différentes phases, communes à tous les systèmes d'information. Voici les phases génériques du processus[57] :

- définition d'une politique, d'un plan et de l'organisation de la continuité de l'activité ;
- constitution d'une équipe de gestion de la continuité de l'activité ;
- bilan d'impact sur l'activité et évaluation du risque ;
- contrôles préventifs et contrôles de l'environnement ;
- documentation du plan ;
- test du plan et formation ;
- déploiement de la sécurité ;
- définition des sauvegardes et de la reprise après sinistre pour les services externalisés.

---

[56] Iia.org, *The IT Auditor's Role in Business Continuity Management*, IIA Publication. http://www.theiia.org/intAuditor/itaudit/archives/2008/january/the-it-auditors-role-in-business-continuity-management

[57] Le National Institute of Standards and Technology a publié un document d'orientation sur la planification des situations d'urgence (non traduit) : *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*.

Ces différentes phases sont les éléments clés d'une solution globale de gestion de la continuité d'activité. Nous allons à présent les examiner successivement plus en détail.

a. Définition d'une politique, d'un plan et d'une organisation pour la continuité de l'activité

Pour gérer avec efficacité la continuité de l'activité, il faut tout d'abord définir une politique en la matière. Dans cette déclaration de politique, l'organisation précise les objectifs généraux de la continuité et pose le cadre organisationnel précisant les responsabilités associées à la planification de la continuité. L'équipe de gestionnaires de la continuité des activités (nous y reviendrons) est constituée de personnes représentatives des différentes fonctions métiers, et joue un rôle important dans la réussite du PCA de l'organisation. Le renouvellement de personnes clés au sein de l'organisation peut poser problème pour assurer la continuité de l'activité, et des mesures doivent être prises pour garantir que les ressources nécessaires seront disponibles.

i. Prévention et minimisation des dommages et des interruptions potentiels

L'organisation doit prendre différentes mesures visant à éviter ou minimiser les dommages qui peuvent affecter les opérations automatisées en conséquence d'un événement imprévu. Ces mesures relèvent de plusieurs catégories :

- routine de copie ou de sauvegarde de tous les fichiers de données, programmes informatiques et documents essentiels avec stockage hors site, mise en place d'une sauvegarde à distance/d'installations de reprise d'activité sur lesquelles l'organisation peut basculer si des dommages rendent ses installations courantes inutilisables ;
- constitution de capacités de reprise et reconstitution du système d'information à son état initial, en cas de perturbation ou de défaillance ;
- déploiement de contrôles de l'environnement, tels que systèmes d'extinction d'incendie ou dispositifs d'alimentation électrique de secours ;
- sensibilisation du personnel et des autres utilisateurs du système aux responsabilités qui leur incombent en cas d'urgence ;
- maintenance conforme du matériel, traitement des problèmes et gestion des changements.

De même, dans le cadre des procédures d'externalisation, l'organisation doit s'assurer que ses fournisseurs ont mis en place des mécanismes similaires, et que ces mécanismes sont fonctionnels.

ii. Déploiement de procédures de sauvegarde des données et programmes

De manière générale, sauvegarder régulièrement les fichiers de données et de logiciels et entreposer ses fichiers sur un site sécurisé et distant constituent les mesures les plus efficaces et économiques qu'une organisation puisse prendre pour atténuer les conséquences d'une interruption de service. Si les équipements peuvent souvent être facilement remplacés, le coût de ce remplacement peut être significatif, et la reconstruction des fichiers de données et le remplacement des logiciels peuvent s'avérer très coûteux et demander beaucoup de temps. En outre, il n'est pas toujours possible de reconstruire certains fichiers de données. En plus du coût direct de la reconstruction des fichiers et du rachat des logiciels, les interruptions de service peuvent entraîner des pertes financières conséquentes.

iii. Formation

Le personnel doit être formé et sensibilisé à ses responsabilités en matière de prévention, d'atténuation et de gestion des situations d'urgence. Par exemple, le personnel support de la sécurité de l'information doit suivre une formation périodique aux procédures d'urgence en cas d'incendie, de dégât des eaux ou de déclenchement d'une alarme, et connaître ses responsabilités liées au démarrage et à l'exploitation d'un site de traitement des données de repli. De même, si certains utilisateurs externes ont un rôle

critique pour les opérations de l'organisation, ils doivent être informés des mesures à prendre en cas d'urgence.

iv. Organiser la maintenance du matériel, le traitement des problèmes et la gestion des changements

Une interruption de service non planifiée peut survenir en cas de défaillance matérielle ou du remplacement d'un équipement sans information préalable des utilisateurs du système. Pour éviter ce type d'incident, il faut mettre en place un programme effectif de maintenance, de traitement des problèmes et de gestion du remplacement d'équipements matériels.

b. Constitution d'une équipe de gestion de la continuité de l'activité

Pour être efficace, l'équipe de gestionnaires de la continuité de l'activité doit représenter toutes les fonctions métiers concernées. Les cadres dirigeants et autres mandataires de l'organisation doivent apporter leur appui au programme de continuité de l'activité et être associés au processus d'élaboration de la politique en la matière. Il est important d'identifier et de définir clairement les rôles et les responsabilités de chaque membre de l'équipe.

c. Bilan d'impact sur l'activité et évaluation du risque

xiii. Évaluation du caractère critique et sensible des opérations du système et identification des ressources connexes

Dans toute organisation, la continuité de certaines opérations est prioritaire sur d'autres. Il n'est donc pas rentable d'assurer le même niveau de continuité pour toutes les opérations. Pour cette raison, l'organisation doit identifier les opérations les plus critiques et les ressources nécessaires à la restauration et au support de ces opérations. Pour y parvenir, elle réalise un bilan d'impact sur l'activité et une évaluation du risque[58]. Ce travail vise à identifier les menaces probables et leur impact sur les systèmes d'information et les ressources connexes de l'organisation, ce qui inclut les données et applications, ainsi que les opérations. Le bilan d'impact permet d'identifier et de hiérarchiser les composants du système en leur associant les différents processus opérationnels de l'organisation dont le système permet le fonctionnement. L'évaluation du risque et le bilan d'impact doivent couvrir tous les domaines fonctionnels. Lorsque l'impact d'une menace identifiée est minime ou si les systèmes de contrôle permettent d'en atténuer les conséquences en temps utile, l'organisation peut décider que le risque résiduel est admissible.

xiv. Identification et hiérarchisation des données et opérations critiques

Le caractère critique et sensible des différentes données et opérations doit être déterminé et hiérarchisé en fonction des catégories de sécurité, des contraintes de disponibilité et de l'évaluation globale du risque associé aux opérations de l'organisation[59]. Cette évaluation du risque sert de référence pour l'établissement du plan de sécurité de l'organisation. Les facteurs à prendre en compte sont notamment le caractère significatif et sensible des données et autres actifs de l'organisation, et le coût de l'incapacité à restaurer rapidement les données ou les opérations. Par exemple, une interruption d'une journée d'un important système de collecte d'impôts ou de redevances ou la perte de données associées à ce système pourraient entraîner le ralentissement significatif ou l'arrêt du recouvrement des créances, diminuer le contrôle exercé sur des millions de dollars de revenus, et dégrader la confiance de l'opinion

[58] Le NIST américain publie un modèle de bilan d'impact sur l'activité : https://csrc.nist.gov/CSRC/media/Publications/sp/800-34/rev-1/final/documents/sp800-34-rev1_bia_template.docx.

[59] Pour en savoir plus sur les catégories de sécurité, voir le document publié par le NIST américain : https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

publique. À l'inverse, un système encadrant la formation du personnel pourrait subir une interruption de plusieurs mois sans graves conséquences.

De manière générale, c'est le personnel impliqué dans les opérations des métiers et programmes de l'organisation qui effectue l'identification et le classement des données et opérations critiques. Il est important que cette appréciation soit également validée par la direction de l'organisation et qu'elle reçoive l'assentiment des autres catégories concernées du personnel.

La liste des ressources et informations critiques, établie par ordre de priorité, doit être revue périodiquement pour veiller à ce qu'elle reflète les conditions réelles. Cette revue doit intervenir à chaque changement significatif apporté à la mission et aux opérations de l'organisation, ou à l'emplacement ou à la conception des systèmes sur lesquels ces opérations s'appuient.

xv. Identification des ressources support des opérations critiques

Après les données et les opérations critiques, il faut identifier les ressources minimum nécessaires à leur exploitation, et analyser leur rôle. Citons, parmi les ressources à prendre en compte :

- les ressources informatiques, dont le matériel, les logiciels, les fichiers de données ;
- les réseaux et leurs composants tels que routeurs et pare-feux ;
- les fournitures, dont le papier et les formulaires pré-imprimés ;
- les services de télécommunications ;
- toutes autres ressources nécessaires à l'opération, dont le personnel, les installations et fournitures de bureau, les archives papier.

Comme les ressources essentielles seront vraisemblablement détenues ou gérées par différents groupes de personnes au sein de l'organisation, il est important que les membres du personnel support de la sécurité de l'information et des programmes travaillent ensemble pour identifier les ressources nécessaires aux opérations critiques.

xvi. Identifier les traitements prioritaires en cas d'urgence

En plus d'identifier et de hiérarchiser les fonctions critiques, l'organisation doit élaborer un plan de restauration des opérations critiques. Ce plan doit clairement identifier l'ordre dans lequel les différents aspects du traitement doivent être rétablis, qui en est responsable, et quels seront pour cela les équipements ou autres ressources nécessaires. L'existence d'un plan bien conçu de rétablissement du traitement peut aider les organisations à déclencher immédiatement le processus de rétablissement, et à exploiter de la manière la plus efficace possible les ressources informatiques limitées dont elles disposent en situation d'urgence. Les utilisateurs du système et le personnel support de la sécurité de l'information doivent participer au travail de définition des priorités du traitement.

d. Contrôles préventifs et contrôles de l'environnement

Les contrôles de l'environnement visent à prévenir ou atténuer les dommages causés aux installations et les interruptions de service. Voici quelques exemples de contrôles de l'environnement :

- extincteurs et systèmes de lutte contre les incendies ;
- alarmes incendie ;
- détecteurs de fumée ;
- détecteurs d'eau ;
- éclairage de secours ;
- systèmes redondants de refroidissement de l'air ;
- alimentation électrique de secours ;
- vannes de sectionnement et procédures d'isolement des conduites de plomberie du bâtiment susceptibles de compromettre les installations de traitement ;

- utilisation de matériaux résistant au feu pour les installations de traitement, conception réduisant la propagation de l'incendie ;
- règlement interdisant de consommer de la nourriture et des boissons ou de fumer dans l'enceinte des installations informatiques ;
- stockage de sauvegarde hors site ;
- contrôles techniques de sécurité, tels que l'utilisation de clés cryptographiques.

Les contrôles de l'environnement peuvent diminuer les pertes consécutives à certaines interruptions, comme les incendies, ou éviter des incidents par la détection précoce, en vue d'un traitement rapide, des situations pouvant poser problème (fuite d'eau, émission de fumées, etc.). De même, la présence d'une alimentation électrique de secours ou d'une alimentation non interruptible (UPS) permet de maintenir l'installation en cas de rupture d'alimentation de courte durée, et peut donner le temps nécessaire à la sauvegarde des données ou à l'exécution des procédures d'arrêt conforme en cas de rupture d'alimentation de plus longue durée.

e. Documentation du plan

Les plans de continuité (tels que PCA, PRA et PUSI) doivent être clairement documentés, être communiqués aux personnels concernés et être mis à jour pour refléter les conditions réelles. Ces plans doivent également être actualisés afin qu'ils décrivent l'environnement actuel d'exploitation. Les PRA et PUSI doivent être alignés sur le PCA et donner des instructions pas-à-pas visant à minimiser l'impact d'un sinistre. Les stratégies et plans de reprise d'activité doivent être modifiés pour accompagner l'évolution de la technologie. Toute modification des plans implique de réaliser un nouveau bilan d'impact, afin de consigner sans ambiguïté les nouvelles priorités et contraintes en cas d'urgence.

xvii. PCA

Le PCA vise à maintenir la mission et les processus opérationnels de l'organisation en cas de sinistre ou de perturbation. C'est un élément critique, qui indique la procédure suivie par l'organisation pour maintenir ses activités pendant et après un sinistre ou une perturbation. Il peut être établi pour une unité opérationnelle en particulier ou pour l'ensemble de l'organisation. Son périmètre peut également être défini de manière à traiter les fonctions identifiées comme étant les plus critiques. Il doit être coordonné avec les autres plans de reprise d'activité, pour garantir l'harmonisation des procédures et des comportements attendus.

Le PCA doit comprendre des éléments permettant d'orienter les priorités de rétablissement des systèmes, tels qu'un bilan d'impact sur l'activité. Les stratégies de reprise doivent également être documentées, en précisant notamment les ressources nécessaires à la reprise et les modalités de validation des stratégies de reprise par la direction. Le PCA doit renfermer certaines informations comme la composition des équipes de rétablissement des systèmes et les exigences en matière de collecte de données. Il doit indiquer les exigences en matière d'exercice de sécurité et d'activités de maintenance, pour faire en sorte que les stratégies de reprise soient précises et actualisées. S'il comprend ces différents éléments, il sera complet et permettra de guider la rédaction d'autres plans, dont le PRA.

xviii. PRA

Un PRA doit être développé pour préparer la restauration des applications critiques. Ce travail implique de prendre des dispositions aménageant des installations de traitement de rechange dans l'éventualité où les installations habituelles seraient considérablement endommagées ou deviendraient inaccessibles. À l'échelle de l'organisation, des règlements et des procédures encadrent le travail de planification de la reprise d'activité et les exigences documentaires. Un plan établi pour l'ensemble de l'organisation doit également identifier les systèmes et applications critiques, ainsi que, le cas échéant, les plans subordonnés ou connexes à ce plan global.

Le PRA doit être validé à la fois par les métiers et par le service responsable de la sécurité de l'information, avant communication au personnel concerné. Il doit représenter les risques identifiés et les

priorités opérationnelles définies par l'organisation. Le coût de la préparation à la reprise ne doit pas être supérieur aux coûts associés aux risques que le plan entend atténuer. Le plan doit être suffisamment détaillé et documenté pour que la réussite de son application ne dépende pas des connaissances ou de l'expertise d'une ou deux personnes seulement. Il doit être diffusé en plusieurs exemplaires, dont certains conservés hors site pour garantir qu'ils ne seront pas détruits par les mêmes événements que ceux qui ont provoqué l'indisponibilité des installations de traitement initiales.

Selon le niveau de continuité de service requis, le site ou les installations de repli pourront aller du site de traitement entièrement équipé et immédiatement opérationnel (un « **centre de secours immédiat** ») au site non équipé qui nécessitera un certain temps de préparation avant d'être opérationnel (une « **salle blanche** »). D'autres types de prestations peuvent également être convenues d'avance avec les fournisseurs. Des dispositions peuvent être prises avec les fournisseurs de matériel informatique et de services de télécommunications, les fournisseurs des formulaires nécessaires à l'activité et autres fournitures de bureau.

iii. PUSI

Les organisations doivent concevoir des plans d'urgence pour chaque système d'information susceptible d'être impacté en cas de sinistre[60]. La rédaction du PUSI doit être coordonnée avec celle d'autres plans, comme le PRA. Les systèmes d'information peuvent être très complexes et être utilisés par plusieurs fonctions métiers différentes. Pour concevoir un PUSI, les organisations doivent donc travailler conjointement avec la direction, afin d'attribuer au plan un niveau de risque approprié, et pour prendre toute la mesure de l'impact qu'aurait une panne ou une perturbation du système.

Un PUSI contient généralement cinq volets principaux : contexte, activation et notification, reprise, reconstitution et annexes. Nous allons à présent décrire rapidement chacun de ces cinq éléments :

- **Contexte** : informations essentielles de contexte, pour faciliter la compréhension, la mise en œuvre et le suivi du plan.
- **Activation et notification** : envoi de notifications au personnel responsable de la reprise, réalisation d'une évaluation de la panne, activation du plan.
- **Reprise** : mise en œuvre des stratégies de reprise afin de restaurer les capacités du système, réparer les dommages et reprendre les opérations.
- **Reconstitution** : validation de la réussite des actions de reprise, et désactivation du plan. Cette étape peut comporter des tests de fonctionnement, pour garantir que toutes les fonctionnalités du système sont revenues à la normale.
- **Annexes** : les annexes contiennent des informations utiles, qui ne sont pas mentionnées dans le corps du plan.

En joignant ces éléments d'information au plan, l'organisation sera dans les meilleures conditions pour réagir aux conséquences du sinistre sur le système.

f. Test du plan et formation

xix. Test périodique des plans de continuité

Il convient de tester les plans de continuité régulièrement pour déterminer s'ils fonctionneront conformément aux attentes face à une situation d'urgence. Le cas échéant, les tests doivent révéler les lacunes majeures des plans ; par exemple, le fait que les installations de secours ne soient pas en mesure de reproduire les opérations critiques conformément à ce qui avait été prévu. Cette procédure de test doit permettre une amélioration significative des plans.

[60] Le National Institute of Standards and Technology a publié un document d'orientation sur la planification des situations d'urgence (non traduit) : *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*.

La fréquence des tests dépend du caractère critique des opérations de l'organisation. Généralement, les plans de continuité des systèmes et fonctions particulièrement critiques doivent être testés une fois par an ou tous les deux ans, chaque fois qu'une modification importante a été apportée au plan ou si des membres clés de l'effectif ont été remplacés. La direction de l'organisation doit évaluer les risques des problèmes pouvant survenir dans l'exécution du plan de continuité, et rédiger une politique encadrant la fréquence et l'étendue des tests.

xx. Actualisation du plan de continuité à partir des résultats des tests

Les résultats des tests sont un bon indicateur de la faisabilité des plans de continuité. Ils doivent donc être présentés à la direction de l'organisation, qui s'appuiera sur ces résultats pour apprécier la nécessité d'apporter des modifications ou d'effectuer des tests complémentaires. La direction sera ainsi informée du risque qu'il y aurait à poursuivre les opérations en l'absence d'un plan de continuité adéquat.

xxi. Formation

Les personnes exerçant des responsabilités en lien avec le plan de continuité doivent être formées, pour garantir qu'elles connaissent leur rôle et possèdent les compétences requises pour remplir ce rôle. De cette façon, le personnel sera prêt à participer aux tests et à faire face à une situation de panne réelle. Les collaborateurs doivent également être formés autant que nécessaire pour remplir leur rôle sans avoir besoin de se reporter à la documentation détaillant leurs fonctions. La visite guidée et documentée peut s'avérer être un outil utile pour simuler la situation d'urgence avec les principales personnes impliquées.

g. Déploiement de la sécurité

La sécurité des ressources et des opérations doit être intégrée au PCA. En effet, les données critiques, les applications, les opérations et les ressources ont tendance à être facilement compromises en cas de sinistre et pendant les interventions de gestion de continuité de l'activité. Par exemple, un manque de sécurité pendant la sauvegarde des données rend possible la création d'exemplaires doublons et la fuite de données importantes. Dans le même temps, il est possible que les données sauvegardées soient compromises pendant l'opération de sauvegarde elle-même (les données étant copiées du serveur opérationnel vers un serveur de sauvegarde).

h. Définition des sauvegardes et de la reprise après sinistre pour les services externalisés

Les organisations sont nombreuses à externaliser tout ou partie de leurs activités informatiques à des prestataires de services. Dans ce cas, c'est le prestataire qui assure les opérations et les contrôles courants. Il est donc essentiel que l'organisation fasse en sorte que le PCA et le PRA soient intégrés au contrat d'externalisation. L'organisation doit également s'assurer que le prestataire garantit la préparation au déclenchement des plans de continuité de l'activité et de reprise après sinistre. Cette vérification s'étend à l'état de préparation du prestataire lui-même pour ce qui concerne les questions de sécurité. Il est également possible que l'organisation ait besoin de s'assurer que le prestataire préserve la confidentialité des données. L'organisation doit conserver la propriété des processus métiers et la maîtrise des risques associés. Elle doit également disposer d'un PCA pour garantir la continuité opérationnelle en cas de cessation d'activité d'un prestataire. Comme indiqué précédemment, cette assurance est souvent fournie dans le cadre du contrat conclu avec le prestataire, sous la forme de rapports détaillant les contrôles mis en place.

III. Risques pour l'entité auditée

Les services ou produits critiques sont ceux dont l'organisation a absolument besoin pour assurer sa survie, éviter des pertes ou répondre à ses obligations, notamment légales. Planifier la continuité est un travail d'anticipation, qui vise à faire en sorte que les processus métiers et les infrastructures des systèmes d'information soient en mesure de répondre aux besoins de la mission de l'organisation après

un sinistre ou toute autre perturbation. Les organisations du secteur public répondent à de nombreux besoins critiques (versement de prestations aux citoyens, service de santé, d'éducation, de défense et autres services publics sur lesquels les citoyens s'appuient). Une interruption prolongée de ces services aura pour conséquence des pertes financières, ainsi que d'autres dommages. Les auditeurs doivent vérifier que toutes les organisations du secteur public ont mis en place des processus de planification de la continuité qui leur permettront de continuer à assurer leur mission auprès des citoyens.

Pour évaluer si les plans mis en place sont en mesure d'améliorer la fiabilité et la continuité des infrastructures des SI et des processus métiers, les auditeurs peuvent se concentrer sur certains risques d'audit identifiés : l'organisation a-t-elle rédigé les documents nécessaires (PCA, PRA, PUSI) pour couvrir tous les domaines fonctionnels critiques ? Si les rôles et responsabilités ne sont pas clairement définis et si le personnel concerné ne les comprend pas bien, même le meilleur des PCA restera inefficace.

Réaliser un bilan d'impact, concevoir des contrôles préventifs, des contrôles de l'environnement et la documentation associée, tester le plan de secours et former le personnel sont autant d'actions qui contribuent à la mise en œuvre efficace d'un programme de gestion de la continuité des activités. Si la sécurité entourant l'application du PCA et du PRA n'est pas rigoureuse, l'organisation court le risque de perdre des données et un temps précieux, et s'expose à des pertes financières en conséquence d'une reprise d'activité inefficace après sinistre.

Les services externalisés représentent un domaine de risque distinct, pour lequel l'organisation ne maîtrise pas totalement la planification de la continuité. Les risques liés à la sécurité des données, à la perte de données, à l'utilisation sans autorisation et aux fuites de données doivent être pris en compte. En cas d'externalisation, les organisations s'exposent également à des risques pour la continuité de leurs activités en raison de la perte de connaissance métier ou de maîtrise des processus, mais aussi de l'impossibilité de changer de fournisseur si les performances du fournisseur sont insuffisantes ou s'il met un terme à son activité.

IV. Références et lectures complémentaires

IIa. « The IT Auditor's Role in Business Continuity Management, » *Internal Auditor*. https://elearn.iia.org.au/mod/resource/view.php?id=10550. Janvier 2008.

Organisation internationale de normalisation/commission électrotechnique internationale. *ISO/IEC 22301:2019 – Sécurité et résilience – Systèmes de management de la continuité d'activité – Exigences.* https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en. 2019.

Organisation internationale de normalisation/commission électrotechnique internationale. *ISO/IEC 22300:2021*— Sécurité et résilience — Terminologie. https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en. 2021.

Organisation internationale de normalisation/commission électrotechnique internationale. *ISO/IEC 22313:2020 – Sécurité et résilience – Systèmes de management de la continuité d'activité - Lignes directrices concernant l'utilisation de l'ISO 22301*. https://www.iso.org/standard/75107.html. 2020.

ISACA. *COBIT 2019 Framework : Governance and Management Objectives.* 2019.

National Institute of Standards and Technology. *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.

National Institute of Standards and Technology. *Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Septembre 2020.

National Institute of Standards and Technology. *Standards for Security Categorization of Federal Information and Information Systems, FIPS 199.* https://csrc.nist.gov/publications/detail/fips/199/final Février 2004.

U.S. Government Accountability Office. *Federal Information Systems Audit Manual (FISCAM).* https://www.gao.gov/products/gao-09-232g. 2 février 2009.

CHAPITRE 7 : LA SÉCURITÉ DE L'INFORMATION

I. Qu'entend-on par « sécurité de l'information » ?

Comme indiqué au chapitre 1, l'expression « sécurité de l'information » désigne la protection de l'information et des systèmes d'information contre tout accès, utilisation, divulgation, interruption, modification ou destruction sans autorisation, afin d'assurer la confidentialité, l'intégrité et la disponibilité des informations et systèmes[61]. La sécurité de l'information englobe les mesures nécessaires pour gérer, prévenir, détecter, documenter et contrer ce type de menace, et permet à l'organisation de protéger l'infrastructure de son système d'information contre les utilisateurs non autorisés.

Étroitement liée à la cybersécurité, qui consiste à protéger l'information en empêchant, en détectant et en répondant aux cyberattaques dont la source est souvent externe, la sécurité de l'information désigne toutefois un processus distinct[62]. Cette notion englobe la stratégie, la politique et les normes traitant de la sécurité du cyberespace et des opérations qui y sont exécutées. Elle comprend notamment le traitement des menaces et vulnérabilités, la réponse aux incidents, les activités de résilience et de restauration, ainsi que l'assurance de l'information[63]. Si de nombreux aspects essentiels de la sécurité de l'information qui sont abordés dans ce chapitre peuvent être appliqués à la cybersécurité, ce chapitre vise principalement les politiques, procédures et pratiques liées à la sécurité de l'information que les organisations devraient mettre en œuvre. Le groupe de travail WGITA de l'INTOSAI travaille actuellement, dans le cadre d'un autre projet, à l'élaboration d'un guide d'audit spécifique consacré à la cybersécurité et à la protection des données.

Une finalité centrale de la sécurité de l'information, qui conditionne tous les autres processus, consiste à assurer la **confidentialité**, l'**intégrité** et la **disponibilité** de la formation.

- La **confidentialité** assure le maintien des restrictions validées concernant la consultation et la divulgation d'informations, et comprend les moyens permettant de protéger les informations revêtant un caractère personnel et confidentiel. La divulgation non autorisée d'informations constitue une perte de confidentialité.
- L'**intégrité** protège les informations contre toute modification ou destruction non conforme, ce qui implique de garantir la non-répudiation[64] des informations, ainsi que leur authenticité[65]. La modification ou la destruction d'informations constitue une perte d'intégrité.
- Par **disponibilité** on entend un état dans lequel les utilisateurs peuvent accéder à tous les systèmes d'information, éléments matériels, réseaux de communication, applications logicielles et données associés, à tout moment utile pour mener à bien leurs activités opérationnelles. La disponibilité garantit également la possibilité de consulter et d'utiliser les informations en temps voulu, dans de bonnes conditions de fiabilité. Une interruption de la consultation ou de l'utilisation d'informations ou

---

[61] National Institute of Standards and Technology, *Glossary* (2021), https://csrc.nist.gov/glossary.

[62] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* version 1.1, 2018.

[63] National Initiative for Cybersecurity Careers and Studies, *Cybersecurity Glossary*, https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.

[64] La **non-répudiation** apporte l'assurance que l'expéditeur de l'information obtient une preuve de remise et que le destinataire obtient une preuve d'identité de l'expéditeur, de sorte que ni l'expéditeur ni le destinataire ne peut ultérieurement nier avoir traité l'information. La non-répudiation n'est pas forcément nécessaire pour apprécier l'intégrité en vue de répondre à un objectif d'audit.

[65] Une information **authentique** est originale, elle peut être vérifiée et est digne de confiance ; l'authenticité démontre la validité d'une transmission, d'un message ou de l'émetteur d'un message. L'authenticité n'est pas forcément nécessaire pour apprécier l'intégrité en vue de répondre à un objectif d'audit.

d'un système d'information constitue une perte de disponibilité.

La sécurité de l'information est importante à plus d'un titre pour l'organisation. Elle n'est pas une finalité en soi, mais doit être un outil au service de l'organisation et de ses objectifs. La sécurité de l'information contribue par exemple aux objectifs opérationnels en protégeant l'accès aux actifs informationnels de l'organisation. Le programme de sécurité de l'information doit ainsi protéger les données de l'organisation tout en permettant de poursuivre ses objectifs opérationnels, ce qui implique de tolérer un niveau de risque acceptable.

L'organisation doit également fournir aux utilisateurs qui en ont besoin les informations nécessaires. Pour appliquer les principes de la sécurité de l'information à l'utilisation du matériel, des réseaux de communication et des applications logicielles et à l'accès aux données, il faut mettre en place une politique en matière de contrôle d'accès. L'objectif du **contrôle d'accès** consiste à garantir que les utilisateurs ont accès uniquement aux ressources et services qu'ils sont en droit d'utiliser, et que les utilisateurs autorisés ne se voient pas refuser l'accès aux services qu'ils sont légitimement en droit d'utiliser. Il est aussi important de fournir l'information à ceux qui en ont besoin que de protéger l'information contre les accès non autorisés.

Fondamentalement, la sécurité de l'information s'appuie sur la gestion du risque pour minimiser l'exposition, dans tous les domaines du modèle de gouvernance des TI. L'absence de processus d'atténuation des risques dans un domaine en particulier et de suivi de ces processus peut avoir des conséquences pour l'organisation toute entière. Même si l'on a généralement conscience de l'importance d'une gestion efficace des risques pour la sécurité de l'information, il est fréquent que ces risques soient sous-estimés ou que les précautions de sécurité ne soient pas actualisées pour refléter l'évolution de l'environnement.

a. La sécurité de l'information : une nécessité

La sécurité de l'information est de plus en plus importante pour les organisations du secteur public. Le déploiement de programmes de sécurité de l'information devient incontournable, à mesure que l'interconnexion des réseaux publics et privés et le partage des ressources d'information rendent plus complexes le contrôle d'accès et le maintien de la confidentialité, de l'intégrité et de la disponibilité des données.

Les systèmes d'information font appel à un assemblage incroyablement complexe de technologies, de processus et de compétences, qui doivent travailler ensemble pour assurer le traitement, le stockage et la transmission de l'information à l'appui de la mission et des fonctions opérationnelles de l'organisation. Il est donc essentiel que chaque organisation établisse un programme pour la sécurité de l'information.

L'objectif d'un tel programme de sécurité des systèmes d'information est de protéger les actifs informationnels de l'organisation en maintenant à un niveau acceptable le risque de perte de confidentialité, d'intégrité et de disponibilité des informations. Si l'organisation n'a pas mis en place ce type de programme, elle s'expose à un risque accru de menaces pour la continuité de ses activités et la réalisation de ses objectifs généraux, ce qui peut au final avoir des conséquences pour sa crédibilité.

Plus le potentiel, la complexité et le périmètre des technologies de l'information se développent, plus la sécurité de l'information devient un sujet central de l'audit informatique. Toute faille dans la sécurité de l'information peut avoir de graves conséquences pour l'organisation et ses activités. Les éléments suivants comptent parmi les conséquences possibles d'une faille de sécurité de l'information :

- violation d'obligations légales et réglementaires ;
- amendes, indemnisations, perte de chiffre d'affaires, dépenses de réparation ou de récupération ;
- dégradation de l'efficacité ou de l'efficience d'un projet, d'un programme ou du service global fourni par l'organisation ;
- perte ou vol de ressources informatiques, d'actifs ou de fonds ;

- consultation, divulgation, modification ou destruction non conformes d'informations sensibles (par exemple, informations relevant de la sécurité nationale, informations à caractère personnel identifiables ou informations commerciales protégées) ;
- actes de piratage, éventuellement assortis de demandes de rançon ;
- perturbation d'opérations essentielles pour certaines infrastructures critiques, pour la défense nationale ou les services d'urgence ;
- affaiblissement des missions de l'organisation, en conséquence d'incidents portant atteinte à sa réputation ou à sa situation financière ;
- utilisation de ressources informatiques dans un but non autorisé ou pour lancer des attaques sur d'autres systèmes ;
- dommages causés aux réseaux et aux équipements.

Ces dommages peuvent être le résultat des événements suivants :

- **violation de sécurité**, détectée ou non ;
- **connexions extérieures non autorisées**, à des sites distants ;
- **exposition d'informations**, divulgation d'actifs et d'informations sensibles de l'organisation à des parties non autorisées ; l'ingénierie sociale est un exemple de malveillance pouvant conduire à ce type de dommages : des criminels appliquent des techniques de manipulation reposant sur la confiance instinctive pour tromper des personnes victimes et les inciter à transmettre des informations confidentielles ;
- **menaces internes**, des utilisateurs exploitent leur position dans l'organisation pour obtenir un accès sans restriction et causer des dommages ;
- **vulnérabilités du système**, les accès sans autorisation à des systèmes et données peuvent donner lieu à un large éventail d'attaques malveillantes, et permettre d'autres intrusions.

Les organisations du secteur public utilisent de plus en plus les réseaux sociaux, et cette activité peut également être ciblée par l'audit informatique. L'utilisation des réseaux sociaux, dont certains services populaires comme Facebook, Twitter et YouTube, permet aux organisations de partager plus facilement l'information avec le public et de solliciter un retour d'expérience. Cependant, elle pose également des difficultés, notamment sur le plan de la protection des informations à caractère personnel et de la sécurité de l'information et des systèmes. Par exemple, l'attaquant peut utiliser les réseaux sociaux pour recueillir des données et lancer des attaques contre les systèmes d'information d'une organisation. La confidentialité pourrait également être compromise en l'absence de limites claires concernant la façon dont l'organisation utilise les informations à caractère personnel auxquelles elle a accès dans le cadre de son activité sur les réseaux sociaux. Pour faire face à ces difficultés, les organisations doivent avoir intégré l'utilisation des réseaux sociaux aux politiques et procédures qu'elles ont mis en place pour gérer le risque pour la sécurité et la protection de la confidentialité[66].

b. Établir une culture de sécurité de l'information

La réussite du déploiement d'un programme de sécurité de l'information dans une organisation repose pour beaucoup sur l'instauration d'une culture organisationnelle en matière de traitement des problèmes de sécurité. Dans les grandes organisations, la mise en place d'un modèle cohérent permettra de traiter de façon homogène les problèmes de sécurité de l'information[67]. Voici une liste non exhaustive des éléments caractéristiques d'une culture efficace en matière de sécurité de l'information :

---

[66] Pour en savoir plus sur l'audit des politiques et procédures de l'organisation concernant l'utilisation des réseaux sociaux, consulter le document publié à ce sujet par l'ISC des États-Unis, le GAO - *Social Media : Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate,* GAO-11-605, (28 juin 2011), https://www.gao.gov/products/GAO-11-605.

[67] ISACA, *Business Model for Information Security,* 2010.

- **Sensibilisation à la thématique de la sécurité.** Il s'agit ici d'actions de sensibilisation générale à la sécurité de l'information, mais aussi de sessions de formation ciblées à destination du personnel de l'organisation. Ces sessions fournissent un cadre propice pour commencer à présenter les responsabilités en matière de sécurité de l'information. Le service des ressources humaines peut prendre en charge une première formation de sensibilisation pour les nouveaux collaborateurs. La formation doit ensuite se poursuivre au cours de l'emploi et jusqu'à ce que la personne quitte les effectifs, afin d'actualiser constamment les connaissances en matière de sécurité.
- **Effort d'engagement de la direction.** L'engagement de la direction joue un rôle central pour l'instauration d'une culture de sécurité de l'information. La direction démontre son engagement non seulement en préparant la documentation formelle associée aux politiques relatives à la sécurité de l'information, mais aussi par son implication active. Faute d'un soutien sincère de la direction, les collaborateurs pourront difficilement développer un sens d'obligation ou de responsabilité envers les programmes de sécurité de l'information. Il est donc essentiel que la direction accepte de piloter la sécurité de l'information, et qu'elle apporte son soutien total aux programmes mis en place.
- **Coordination efficace, grâce à la création d'équipes transversales aux différentes fonctions.** Étant donné que la sécurité de l'information concerne différents aspects de l'organisation, qui doivent être coordonnés, on peut envisager de constituer des équipes transversales (dont les membres sont issus de différents départements de l'organisation, dont le service informatique). La mise en place d'équipes transversales favorise la communication et la collaboration, réduit le cloisonnement des services et contribue à éviter les doublons dans les démarches entreprises.

L'instauration d'une culture de sécurité de l'information fait partie intégrante du déploiement de la gouvernance au sein de l'organisation, et se caractérise notamment par les éléments suivants :

- **Alignement des objectifs de sécurité de l'information et des objectifs métiers.** Il est important d'aligner les objectifs de sécurité de l'information et les objectifs métiers, car les objectifs de sécurité contribuent à la réalisation des objectifs métiers. Le programme de sécurité de l'information doit être aligné sur les processus organisationnels et comporter des contrôles pratiques, qui permettent de réduire le risque de façon concrète et mesurable.
- **Équilibre entre organisation, ressources humaines, procédures et technologie.** Pour être efficace, la sécurité de l'information doit bénéficier d'un appui organisationnel, de collaborateurs compétents, de procédures performantes et de solutions technologiques adaptées. Chaque élément présente des interactions avec d'autres domaines, impactant et soutenant tout à la fois d'autres éléments, de manière souvent complexe, aussi est-il essentiel de parvenir à équilibrer les différents aspects en jeu. La défaillance d'un seul élément aura des conséquences sur la sécurité globale de l'information.
- **Gestion du risque.** Le déploiement de la sécurité de l'information doit être porté par la gestion du risque. Dans sa publication spéciale consacrée à la gestion du risque pour la sécurité de l'information, le National Institute of Standards of Technology américain distingue quatre aspects du processus de gestion du risque[68] :
    - attribution des responsabilités en matière de gestion du risque pour la sécurité aux dirigeants de l'organisation ;
    - recensement constant et compréhension par les dirigeants de l'organisation des risques de sécurité de l'information auxquels sont exposés les activités et les actifs organisationnels, les personnes et les autres organisations, en conséquence de l'exploitation et de l'utilisation des systèmes d'information ;
    - définition de la tolérance au risque de l'organisation et communication de cette tolérance dans l'ensemble de l'organisation, notamment au moyen de lignes directrices présentant l'impact de la tolérance au risque sur les processus décisionnels quotidiens ;
    - responsabilité assumée par les dirigeants de l'organisation pour les décisions qu'ils ont prises en matière de gestion du risque et pour le déploiement de programmes efficaces de gestion du

[68] National Institute of Standards and Technology, *Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View*, 2011.

risque à l'échelle de l'organisation.

II. Les principales composantes de la sécurité de l'information

Au sein d'une organisation, la sécurité de l'information concerne 12 domaines :

- évaluation des risques
- politique de sécurité
- organisation de la sécurité des SI
- gestion des activités et des enregistrements
- gestion des actifs
- sécurité des ressources humaines
- sécurité physique et environnementale
- contrôle d'accès
- développement, acquisition et maintenance de systèmes informatiques
- gestion des incidents de sécurité liés aux TI
- gestion de la continuité de l'activité
- conformité.

a. Évaluation des risques

On entend par « évaluation des risques » le travail d'identification, d'analyse et d'évaluation des risques au sein de l'infrastructure de sécurité des systèmes d'information. Ce terme englobe également l'appréciation des risques pour la sécurité associés aux menaces internes et externes auxquelles sont exposés l'organisation, ses actifs et son personnel. Le processus d'évaluation du risque comprend l'identification et l'analyse des éléments suivants :

- ensemble des actifs et processus liés au système ;
- environnements externalisés liés au système ;
- menaces susceptibles d'affecter la confidentialité, l'intégrité ou la disponibilité du système ;
- vulnérabilités du système et menaces associées ;
- impact potentiel et risques associés à l'activité constituant la menace ;
- impératifs de protection permettant d'atténuer les risques ;
- identification des mesures de sécurité appropriée et analyse des rapports au risque.

Si l'évaluation des risques n'est pas menée correctement, il est possible que l'infrastructure et les informations sensibles ne soient pas suffisamment protégées ou qu'elles bénéficient d'une surprotection inutile. Dans sa publication spéciale *Guide for Conducting Risk Assessments*[69], le National Institute of Standards of Technology américain distingue quatre étapes du processus d'évaluation des risques :

- **Préparation** de l'évaluation, en élaborant un cadre relatif aux risques spécifiques à l'organisation
- **Réalisation** de l'évaluation,
  - en identifiant les sources et les événements constituant des menaces,
  - en identifiant les vulnérabilités et les conditions prédisposant au risque,
  - en déterminant la probabilité du risque,
  - en déterminant l'ampleur de l'impact dans l'éventualité d'une violation de sécurité,

[69] National Institute of Standards and Technology, Joint Task Force Transformation Initiative, Special Publication 800-30*, Guide for Conducting Risk Assessments*, 2012.

- en utilisant les informations précédentes pour déterminer le niveau de risque global.

- **Communication** des résultats de l'évaluation.
- **Actualisation** de l'évaluation.

L'évaluation des risques n'est pas une activité ponctuelle, qui apporterait aux décideurs des informations permanentes et définitives permettant d'orienter et d'éclairer la réaction aux risques concernant la sécurité de l'information. Au contraire, l'organisation doit considérer l'évaluation des risques comme une activité régulière, dont la fréquence de réalisation et l'ampleur des ressources engagées correspondent à la finalité et au périmètre définis.

L'application de l'évaluation des risques aidera la direction à sélectionner les contrôles appropriés pour atténuer les risques de façon efficace. Pour déterminer les contrôles de sécurité appropriés, la norme fédérale 199 des États-Unis relative au traitement de l'information[70] définit trois niveaux d'impact potentiel (faible, modéré et élevé) pour les organisations ou les personnes en cas de violation de sécurité (c'est-à-dire, une perte de confidentialité, d'intégrité ou de disponibilité). La définition des niveaux d'impact doit être appréciée dans le contexte spécifique à chaque organisation, mais aussi en fonction de l'intérêt global à l'échelle nationale.

- L'impact potentiel est jugé **faible** si la perte de confidentialité, d'intégrité ou de disponibilité peut avoir des conséquences défavorables **limitées** sur les activités et les actifs de l'organisation, ou sur les personnes.
- L'impact potentiel est jugé **modéré** si la perte de confidentialité, d'intégrité ou de disponibilité peut avoir des conséquences défavorables **importantes** sur les activités et les actifs de l'organisation, ou sur les personnes.
- L'impact potentiel est jugé **élevé** si la perte de confidentialité, d'intégrité ou de disponibilité peut avoir des conséquences défavorables **graves ou désastreuses** sur les activités et les actifs de l'organisation, ou sur les personnes.

Le classement dans l'une ou l'autre des catégories d'impact détermine la rigueur des tests réalisés dans différents domaines de la sécurité de l'information. Par exemple, les évaluations du risque organisationnel (et de la tolérance au risque) sont des facteurs importants pour élaborer les politiques et procédures de contrôle d'accès. Les politiques et procédures de contrôle d'accès correspondant à une ressource donnée doivent être adaptées au niveau d'impact (c'est-à-dire, à la perte de confidentialité, d'intégrité ou de disponibilité) qu'une violation de sécurité liée à cette ressource aurait sur l'organisation.

b. Politique de sécurité

On entend par « politique de sécurité » de l'organisation l'ensemble des lois, des règles et des pratiques encadrant la façon dont l'organisation gère, protège et répartit ses ressources pour atteindre les objectifs de sécurité définis. Ces lois, règles et pratiques doivent impérativement identifier des critères permettant de déterminer l'autorité attribuée aux individus, et peuvent préciser les conditions d'exercice de cette autorité. Pour être utiles, ces lois, règles et pratiques doivent apporter aux individus la possibilité de déterminer si leurs actions sont en infraction ou sont conformes à la politique.

[70] Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004.

Le tableau ci-dessous présente les éléments qu'il est recommandé d'inclure dans une politique de sécurité des SI.

Éléments d'une politique de sécurité des SI	Définition de la sécurité de l'information, objectifs et périmètre (y compris confidentialité des données)
	Détail des principes de sécurité, normes et exigences de conformité (par exemple, les collaborateurs du service informatique ne doivent pas avoir de responsabilités opérationnelles ou comptables)
	Définition des responsabilités générales et spécifiques concernant tous les aspects de la sécurité de l'information
	Utilisation des actifs informationnels et accès au courrier électronique et à l'Internet
	Mode et méthode d'accès (y compris politiques de contrôle d'accès et d'authentification)
	Procédures de sauvegarde
	Procédures de traitement des logiciels et programmes malveillants (par exemple, suivi continu, détection des intrusions, systèmes de prévention des intrusions)
	Éléments de sensibilisation et de formation à la sécurité
	Procédure de signalement et de réaction aux incidents de sécurité soupçonnés
	Plans de continuité de l'activité
	Gestion des correctifs
	Sécurité physique
	Méthodes de communication de la politique et des procédures adoptées en matière de sécurité de l'information auprès du personnel

c. Organisation de la sécurité des SI

L'organisation de la sécurité des SI nécessite souvent de déployer une politique de sécurité par entité. La responsabilité du déploiement de la politique de sécurité peut être attribuée à une unité ou à une personne, qui travaillera ensuite avec l'organisation à l'acquisition des outils et processus nécessaires à la mise en œuvre efficace de la politique. Une fois la politique déployée, l'organisation doit assurer la formation du personnel et le traitement des incidents de sécurité. L'organisation doit également assurer la protection suffisante des données auxquelles des entités extérieures ont accès ou qui sont transférées à des entités extérieures. L'auditeur doit contrôler que les entités extérieures concernées sont en mesure de respecter les exigences de sécurité.

d. Gestion des activités et des enregistrements

L'organisation doit assurer la traçabilité des procédures appliquées dans le cadre de ses activités opérationnelles. Ce suivi concerne par exemple les procédures qui garantissent le traitement conforme des données et la documentation du traitement des médias et des données, les procédures d'urgence, l'authentification sur le réseau, les procédures de sauvegarde.

e. Gestion des actifs

Au sens large, la gestion des actifs désigne tout système permettant d'assurer le suivi et la maintenance des éléments présentant de la valeur pour l'organisation. La gestion des actifs est un processus systématique d'exploitation, de maintenance, de mise à niveau, et d'élimination des actifs respectant un critère de rentabilité.

Dans le domaine des technologies de l'information, la gestion des actifs comprend la tenue d'un inventaire précis des équipements et des données, l'identification des licences requises pour l'utilisation

des équipements, ainsi que la maintenance et la protection (par exemple, verrouillage et local à accès contrôlé) des équipements. La gestion des actifs informatiques englobe également le suivi de la documentation des logiciels et des processus dont l'organisation a besoin.

La gestion des actifs informatiques est essentielle pour l'organisation, qui doit disposer d'un inventaire précis et complet de ses actifs. En l'absence d'inventaire complet des actifs informatiques, l'organisation ne sera pas en mesure de déterminer si les contrôles de sécurité qu'elle applique sont appropriés pour la totalité des actifs. De même, quand elle dispose d'un inventaire complet des actifs informatiques, l'organisation évite des complications au moment de mettre à niveau des logiciels pour répondre à l'évolution de ses besoins métiers.

f. Sécurité des ressources humaines

Les collaborateurs qui traitent des données à caractère personnel au sein de l'organisation doivent avoir suivi une formation de sensibilisation adaptée, assortie de mises à niveau régulières, pour contribuer à la préservation des données qui leur sont confiées. Les rôles et responsabilités doivent être définis pour chaque poste dans l'organisation, et documentés conformément à la politique de sécurité appliquée. Les données de l'organisation doivent être protégées contre toute interférence et contre l'accès, la divulgation, la modification et la destruction sans autorisation. La gestion des risques de sécurité et de confidentialité dans le domaine des ressources humaines doit être assurée tout au long de la présence des collaborateurs dans les effectifs de l'organisation.

On distingue trois aspects de la sécurité des ressources humaines :

- **Avant le recrutement :** à ce stade, il convient de définir les rôles et responsabilités du poste, les droits d'accès aux informations à caractère sensible associés à la fonction, et le niveau de détail de l'examen des candidats, conformément à la politique de sécurité SI de l'organisation. C'est pendant cette phase que sont établies les modalités contractuelles.
- **Pendant l'emploi :** il convient de rappeler périodiquement leurs responsabilités aux collaborateurs qui bénéficient d'un accès aux informations à caractère sensible dans l'organisation, et de leur apporter une formation continue de sensibilisation à la sécurité, avec des mises à jour régulières. De cette façon, les collaborateurs concernés connaîtront les menaces actuelles et les pratiques de sécurité qui permettent d'en atténuer l'impact.
- **À la résiliation de l'emploi :** pour éviter tout accès non autorisé aux informations à caractère sensible, les droits d'accès des utilisateurs autorisés doivent être immédiatement supprimés dès que ces collaborateurs quittent les effectifs. Les collaborateurs concernés sont également tenus de restituer tout actif en leur possession et appartenant à l'organisation. À ce stade, un document spécifique peut être établi, afin de consigner l'ensemble du travail réalisé par le collaborateur, de contrôler que tous les droits d'accès ont bien été supprimés et que tous les actifs ont été restitués, le cas échéant.

Un programme de sensibilisation à la sécurité doit être en place, afin de rappeler à l'ensemble du personnel les risques et les situations possibles d'exposition aux risques, ainsi que les responsabilités de chacun en tant que gardien des informations de l'organisation.

g. Sécurité physique et environnementale

On entend par « sécurité physique » les mesures conçues pour empêcher les personnes non autorisées (ce qui inclut les attaquants comme les intrus accidentels) d'accéder physiquement à un bâtiment, à des installations, à une ressource ou à des informations stockées. La sécurité physique concerne également l'élaboration de lignes directrices pour la conception de structures capables de résister aux actes d'agression éventuels. La sécurité physique peut désigner une simple porte fermant à clé autant qu'un dispositif complexe comportant plusieurs niveaux de barrières, des gardes de sécurité armés, la mise en place d'un poste de garde.

La sécurité physique sert avant tout à interdire l'accès physique des personnes non autorisées (généralement considérées comme des intrus) aux installations contrôlées, même si les mesures de

sécurité physique présentent également un intérêt dans d'autres circonstances (par exemple, pour restreindre l'accès à une installation ou à des actifs en particulier, pour établir des contrôles de l'environnement permettant de circonscrire un incident matériel, comme un incendie ou une inondation).

La sécurité engendre inévitablement des coûts et ne peut jamais être achevée ; elle permet de réduire les risques mais pas de les éliminer totalement. Étant donné que les contrôles sont imparfaits, une sécurité physique rigoureuse répond au principe de défense en profondeur, en appliquant différentes combinaisons de contrôles redondants et complémentaires. Par exemple, on met généralement en place des contrôles d'accès physique pour les installations protégées pour les raisons suivantes :

- décourager les intrus potentiels (au moyen de panneaux d'avertissement et d'une délimitation d'un périmètre, par exemple) ;
- distinguer les personnes autorisées des personnes non autorisées (au moyen de cartes d'accès et de clés, par exemple) ;
- retarder, gêner, et dans l'idéal, empêcher les tentatives d'intrusion (murs solides, portes verrouillées, coffres, etc.) ;
- détecter les intrusions et surveiller/enregistrer les intrus (au moyen d'alarmes anti-intrusion et de systèmes de vidéosurveillance, par exemple) ;
- déclencher une réaction appropriée à l'incident (intervention des gardes de sécurité ou de la police, par exemple).

Les contrôles d'environnement concernent principalement les installations de l'organisation qui concentrent les ressources système (par exemple, centres de données, locaux de l'ordinateur central, locaux de serveurs, salles de communication). Si les contrôles environnementaux sont insuffisants, en particulier dans des environnements très difficiles, il est possible que la disponibilité des systèmes et des composants nécessaires pour soutenir la mission de l'organisation et les fonctions métiers soit dégradée.

h. Contrôle d'accès

Le contrôle d'accès consiste à exercer un contrôle sur les personnes autorisées à interagir avec une ressource. Souvent, mais pas systématiquement, la procédure implique une autorité chargée d'exercer le contrôle. La ressource contrôlée peut être un bâtiment, un groupe de bâtiments ou des systèmes informatiques. Qu'il soit physique ou logique, le contrôle d'accès est en réalité intégré aux activités quotidiennes. Par exemple, le verrouillage des portières d'un véhicule constitue une forme simple de contrôle d'accès. La saisie d'un code de sécurité sur un distributeur bancaire, ou l'utilisation d'un dispositif d'authentification biométrique sont d'autres formes de contrôle d'accès. La mise en place du contrôle d'accès est essentielle pour toute organisation souhaitant sécuriser des informations importantes, confidentielles ou sensibles, ainsi que des équipements. Le contrôle d'accès permet[71] :

- de créer, gérer, vérifier, révoquer et auditer les identités et les identifiants correspondant aux appareils, aux utilisateurs et aux processus aux autorisés ;
- de gérer et protéger l'accès physique aux actifs ;
- de gérer l'accès distant (si l'organisation l'utilise) ;
- de gérer les permissions et autorisations d'accès, en intégrant les principes du moindre privilège et de séparation des tâches[72] ;

[71] U.S. Government Accountability Office (ISC des États-Unis) *Federal Information System Controls Audit Manual*, 2009.

[72] Le principe du moindre privilège implique que chaque utilisateur reçoive les privilèges du niveau le plus bas requis aux fins de l'exécution des tâches autorisées. L'application de ce principe limite les dommages susceptibles de résulter d'un accident, d'une erreur ou de l'utilisation d'un système d'information sans autorisation. La séparation des tâches constitue un contrôle basique, qui empêche ou détecte les erreurs et les irrégularités en attribuant à différentes personnes la responsabilité du lancement des opérations, de l'enregistrement des opérations et de l'enregistrement de la garde des actifs. Ce principe est généralement appliqué dans les services informatiques de

- de protéger l'intégrité du réseau (par exemple, séparation du réseau, segmentation du réseau) ;
- de contrôler les identités et de les lier à des identifiants de connexion vérifiés au cours des interactions ;
- d'authentifier les utilisateurs, les appareils et autres actifs (par exemple, authentification à un seul ou plusieurs facteurs), en fonction du risque associé à la transaction (par exemple, risque pour la sécurité et la confidentialité des personnes, et autres risques organisationnels).

Les évaluations du risque organisationnel et de la tolérance au risque sont importantes pour élaborer les politiques et procédures du contrôle d'accès. Les politiques et procédures de contrôle d'accès correspondant à une ressource donnée doivent être adaptées au niveau d'impact (c'est-à-dire, à la perte de confidentialité, d'intégrité ou de disponibilité) qu'une violation de sécurité liée à cette ressource aurait sur l'organisation.

Dans le secteur public, le contrôle d'accès est important parce que de nombreux organismes publics traitent des données sensibles et que les impératifs de confidentialité restreignent le périmètre des personnes autorisées à consulter les différentes parties de l'information. Le contrôle d'accès permet que seuls les utilisateurs disposant des identifiants requis aient accès aux données à caractère sensible.

i. Développement, acquisition et maintenance de systèmes informatiques

Il est important que les organisations identifient et maîtrisent les risques associés à la chaîne d'approvisionnement dans les phases de développement et d'acquisition de produits et services informatiques. La chaîne logistique commence avec l'approvisionnement des produits et s'étend à la conception, au développement, à la fabrication, au traitement, à la manutention et à la livraison de produits et services à l'utilisateur final. Les relations au sein de la chaîne logistique étant complexes et interconnectées, la **gestion du risque de la chaîne logistique** constitue une fonction organisationnelle critique. L'un des principaux objectifs de la gestion du risque de la cyber-chaîne logistique est d'identifier, d'évaluer et de traiter les produits et services qui sont susceptibles de contenir des fonctionnalités potentiellement malveillantes, qui constituent des contrefaçons ou qui sont vulnérables en raison d'un manque de rigueur des pratiques de fabrication et de développement au sein de la cyber-chaîne logistique. La gestion du risque de la cyber-chaîne logistique correspond à différentes activités, parmi lesquelles[73] :

- la définition des exigences de cybersécurité pour les fournisseurs ;
- la mise en œuvre des exigences de cybersécurité au moyen d'accords formels (par exemple, des contrats) ;
- la communication aux fournisseurs pour leur indiquer comment les exigences de cybersécurité seront vérifiées et validées ;
- la vérification du respect des exigences de cybersécurité par l'application de différentes méthodes d'évaluation, par exemple, par la soumission de rapports au centre des opérations de sécurité, s'il existe ;
- l'encadrement et la gestion des activités précitées.

Il est nécessaire de mettre en place une maintenance continue après le développement ou l'acquisition d'un produit ou service informatique. La maintenance d'un système informatique tout au long de son cycle de vie inclut les modifications et mises à jour du système (par exemple, l'installation de correctifs) pour répondre à de nouvelles exigences, la réparation des erreurs système ou les améliorations correspondant à de nouvelles interfaces.

---

grande ampleur, afin que personne ne soit en mesure d'introduire un code frauduleux ou malveillant sans que cela soit détecté.

[73] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* version 1.1, 2018.

L'organisation doit concevoir une **procédure de gestion des correctifs**. La gestion des correctifs correspond à l'identification, à l'acquisition, à l'installation et à la vérification des correctifs pour les produits et systèmes. Les correctifs permettent de remédier à des problèmes de sécurité et de fonctionnement touchant les logiciels et microprogrammes. Du point de vue de la sécurité, l'intérêt des correctifs est généralement de permettre d'atténuer les vulnérabilités des failles logicielles ; l'application de correctifs pour éliminer ces vulnérabilités réduit considérablement la possibilité qu'elles soient exploitées[74].

j. Gestion des incidents et événements de sécurité liés aux technologies de l'information

Comme indiqué au chapitre 4 consacré aux Activités informatiques, la gestion des incidents correspond aux systèmes et pratiques mis en œuvre pour déterminer si les incidents ou erreurs sont consignés, analysés et résolus en temps utile. Dans les domaines de la sécurité informatique et des technologies de l'information, la gestion des incidents de sécurité implique de mettre en place une surveillance et de détecter les événements de sécurité sur un ordinateur ou un réseau informatique et d'appliquer des réponses appropriées à ces événements. La gestion des incidents de sécurité liés aux TI est une forme particulière de gestion des incidents.

Les organisations doivent établir un processus, un plan et une politique formels de réponse aux incidents. Le processus typique de réponse aux incidents comporte quatre phases :

- **Préparation.** Cette phase implique la création et la formation d'une équipe de réponse aux incidents, la constitution d'une capacité de réponse aux incidents afin que l'organisation soit prête à y répondre. Elle concerne également la prévention des incidents, en veillant à ce que les systèmes, réseaux et applications soient suffisamment sécurisés, en appliquant aux systèmes d'information des contrôles de sécurité intégrant les risques.
- **Détection et analyse.** Cette phase consiste à détecter les incidents par différents moyens, avec différents niveaux de détail et d'exactitude. Ces moyens de détection sont notamment les systèmes de détection et de prévention des intrusions basés sur le réseau et sur l'hôte, les logiciels antivirus, les analyseurs de journaux et les rapports d'utilisateurs. Une fois l'incident détecté, l'équipe de réponse aux incidents analyse et valide rapidement chaque incident selon un processus prédéfini, en documentant chaque mesure prise.
- **Confinement, éradication, récupération.** Dès qu'un incident a été détecté, les organisations doivent s'efforcer d'en circonscrire le périmètre. Le confinement d'un incident repose avant tout sur la prise de décisions (par exemple, faut-il arrêter un système, le déconnecter du réseau, désactiver certaines fonctions ?). Ces décisions sont plus faciles à prendre si l'on a établi à l'avance des stratégies et procédures de confinement d'un incident. Confiner l'incident donne à l'organisation le temps nécessaire pour concevoir une stratégie de réaction adaptée.

  Une fois l'incident confiné, il peut être nécessaire de l'éradiquer pour éliminer les composants de l'incident. Par exemple, en supprimant des logiciels malveillants et en désactivant les comptes d'utilisateurs qui ont été violés, mais aussi en détectant toutes les vulnérabilités qui ont été exploitées, pour les atténuer.

  Au stade de la récupération, les administrateurs rétablissent le fonctionnement normal des systèmes, confirment que les systèmes fonctionnent normalement et (le cas échéant) corrigent les vulnérabilités afin d'éviter que des incidents similaires ne se produisent. L'étape de récupération peut impliquer de restaurer des systèmes à partir de sauvegardes fonctionnelles, de reconstruire intégralement des systèmes, de remplacer des fichiers compromis par des versions propres, d'installer des correctifs, de modifier des mots de passe et de renforcer la sécurité du périmètre du réseau (par exemple, règles de pare-feu et listes de contrôle d'accès des routeurs de périphérie).
- **Activité post-incident.** Après avoir résolu un incident, les organisations ont intérêt à communiquer le résultat aux collaborateurs informatiques concernés et à faire de cette expérience une opportunité d'apprentissage et d'amélioration. Après un incident, il convient d'organiser des réunions consacrées

[74] National Institute of Standards and Technology, *Special Publication 800-40, rev. 3: Guide to Enterprise Patch Management Technologies*, 2013.

aux enseignements tirés de l'incident, de collecter des données sur l'incident, de conserver des preuves et de revoir les processus de réponse à incident pour y intégrer les enseignements tirés.

k. Gestion de la continuité de l'activité

L'organisation utilise le plan de continuité d'activité pour planifier et tester la reprise de ses processus opérationnels après un sinistre. Ce plan décrit également la manière dont l'organisation continuera de fonctionner face à des circonstances défavorables (par exemple catastrophe d'origine naturelle ou autre). Le Chapitre 4 contient des informations complémentaires sur la gestion de la continuité de l'activité.

l. État de conformité :

L'auditeur des SI doit examiner et évaluer la conformité avec toutes les exigences internes et externes (par exemple, légales et environnementales, et les exigences relatives à la qualité, à la fiabilité et à la sécurité de l'information).

III. Risques pour l'entité auditée

La mise en œuvre des politiques et procédures de sécurité informatique permet à l'organisation de protéger l'infrastructure de ses systèmes d'information contre les utilisateurs non autorisés. La politique de sécurité informatique définit des exigences strictes, que l'organisation et ses collaborateurs appliquent pour protéger les actifs essentiels. Elle régit également la formation du personnel en matière de sécurité et veille au respect des procédures établies pour l'accès aux données et le contrôle. En outre, la politique de sécurité informatique rappelle la législation et la réglementation que l'organisation est tenue d'appliquer. La mise en œuvre d'un système efficace de sécurité de l'information ne se fait pas sans difficulté. Si l'organisation n'a pas mis en place une gouvernance performante pour encadrer la gestion des obstacles qui se présentent, il est probable qu'elle ne parvienne pas à atteindre ses objectifs.

Étant donné que l'environnement, le contexte politique, géographique, économique et social sont différents pour chaque organisation, chacune rencontre également des défis spécifiques. Chacun de ces défis peut constituer un obstacle à l'efficacité de la gouvernance des technologies de l'information. Le rôle de l'auditeur des SI est ici de signaler à la direction les risques pour la sécurité de l'information qui ont été identifiés.

Voici certains des risques significatifs auxquels la plupart des organisations sont exposées :

- divulgation d'informations sans autorisation,
- modification ou destruction d'informations sans autorisation,
- attaque des systèmes d'information,
- destruction de l'infrastructure du système d'information,
- perturbation de la consultation ou de l'utilisation d'informations ou du système d'information,
- perturbation des processus de traitement du système d'information,
- vol d'informations ou de données.

Pour apprécier l'exposition aux risques des organisations auditées, il convient d'examiner plus particulièrement les domaines suivants :

- les stratégies de sécurité de l'information ne sont pas alignées sur les exigences des métiers ou des technologies de l'information ;
- les politiques ne sont pas appliquées uniformément ;
- la conformité avec les exigences internes et externes n'est pas assurée ;
- la sécurité de l'information n'est pas intégrée aux processus de maintenance et de développement des projets ;
- la conception de l'architecture entraîne des solutions de sécurité de l'information qui ne sont ni

efficaces, ni efficientes, ni correctement orientées ;

- les mesures de sécurité physique et la gestion des actifs ne sont pas adaptées ;
- la configuration des applications du système matériel n'est pas adaptée ;
- l'organisation des processus de sécurité de l'information est inefficace et les responsabilités associées à la sécurité de l'information ne sont pas définies ou pas de façon précise ;
- les solutions pour les ressources humaines ne sont pas adaptées ;
- les ressources financières allouées à la sécurité de l'information ne sont pas utilisées efficacement, et la structure de valeur de la sécurité de l'information (rapport coût/avantage) n'est pas alignée sur les besoins ou les objectifs des métiers ;
- la sécurité de l'information ne fait l'objet d'aucune surveillance ou la surveillance n'est pas efficace.

Lorsqu'il audite la sécurité de l'information, l'auditeur doit traiter les problèmes liés aux 12 domaines mentionnés ci-dessus concernant la sécurité de l'information[75]. Pour commencer, il doit apprécier le caractère adéquat des méthodes d'évaluation des risques et considérer les problématiques d'audit liées à la mise en œuvre de la sécurité de l'information. L'auditeur pourra s'aider d'une matrice d'audit pour formuler les questions d'audit, les critères d'évaluation, identifier les documents requis et la méthodologie d'analyse technique à appliquer. Pour terminer, l'auditeur peut concevoir un programme d'audit détaillé adapté aux besoins et à l'évolution du travail de terrain effectué dans le cadre de l'audit.

IV. Références et lectures complémentaires

Cichonski, Paul, Thomas Millar, Tim Grance, and Karen Scarone. NIST Special Publication *800-61, rev 2: Computer Security Incident Handling Guide*. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final. 2012.

ISACA ITAF. *A Professional Practices Framework for IT Assurance.* USA, 2008.

ISACA. *Risk IT Framework.* https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2. 2020.

ISACA. *COBIT 5 Framework*. https://www.isaca.org/bookstore/cobit-5/wcb5. 2012.

ISACA. *Information Security Audit/Assurance Program.* 2010.

ISACA. *IT Risk Management Audit/Assurance Program*. 2012.

Organisation internationale de normalisation/commission électrotechnique internationale. *ISO/IEC 27000 : Systèmes de management de la sécurité de l'information*. https://www.iso.org/standard/54534.html. 2013.

Organisation internationale de normalisation/commission électrotechnique internationale. *ISO/IEC 27005 : Gestion des risques liés à la sécurité de l'information.* https://www.iso.org/standard/75281.html. 2018.

National Institute of Standards and Technology. *Federal Information Processing Standards Publication 199 : Standards for Security Categorization of Federal Information and Information Systems*. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf. Février 2004.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity,* version 1.1. https://www.nist.gov/cyberframework/framework. 2018.

[75] Organisation internationale de normalisation, *Série ISO 27000 consacrée au système de management de la sécurité de l'information.*

National Institute of Standards and Technology. *Special Publication 800-40, rev. 3: Guide to Enterprise Patch Management Technologies*. https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final. 2013.

National Institute of Standards and Technology. *Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View.* https://csrc.nist.gov/publications/detail/sp/800-39/final. 2011.

U.S. Government Accountability Office. *Federal Information System Controls Audit Manual (FISCAM)*. https://www.gao.gov/products/gao-09-232g. 2 février 2009.

U.S. Government Accountability Office. *Information Security : Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies.* https://www.gao.gov/products/gao-15-758t. 8 juillet 2015.

U.S. Government Accountability Office. *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks.* GAO-21-171. https://www.gao.gov/products/gao-21-171. 15 décembre 2020.

CHAPITRE 8 : LES CONTRÔLES D'APPLICATION

I. Qu'entend-on par « Contrôles d'application ? »

Comme indiqué précédemment, le contrôle interne est un processus conçu pour apporter, dans la mesure du raisonnable, l'assurance que :

- les opérations, y compris l'utilisation des ressources de l'organisation, sont conduites de façon efficace et efficiente ;
- la présentation des résultats financiers, ce qui inclut les rapports sur l'exécution budgétaire, les états financiers et d'autres rapports à usage interne et externe, est fiable ;
- la législation et la réglementation applicables sont respectées.

Les contrôles des systèmes d'information sont les contrôles internes qui dépendent des opérations réalisées par les systèmes d'information et comprennent des contrôles généraux (à l'échelle de l'organisation et d'un système), des contrôles d'application des processus métiers, ainsi que des contrôles utilisateurs qui dépendent des systèmes d'information (ces contrôles sont effectués par les personnes qui utilisent les systèmes d'information).

Les processus métiers sont les principales fonctions que l'organisation déploie pour accomplir sa mission. Une application pour processus métier correspond à la combinaison des éléments matériels et logiciels utilisés pour traiter les informations du processus métier afin de répondre aux besoins d'un processus en particulier. Elle peut comporter des procédures manuelles et informatisées pour l'origination d'opérations, le traitement de données, la tenue d'enregistrements et la préparation de rapports. Chaque organisation peut faire fonctionner différentes applications, dont la taille varie du système à l'échelle de l'entreprise, que chaque collaborateur utilise, aux petites applications client qu'un seul collaborateur utilise. Le logiciel d'application peut être un système de gestion de la paie, un système de facturation, un système de gestion des stocks ou un progiciel de gestion intégré.

Les contrôles d'application des processus métiers, que l'on désigne généralement par l'appellation **contrôles d'application**, sont des contrôles spécifiques à une application informatique donnée. Si les processus métiers sont automatisés dans une application informatique, les règles métiers sont également intégrées à l'application sous la forme de contrôles d'application. Ces contrôles concernent les segments applicatifs, et sont liés aux opérations et aux données existantes. Les contrôles d'application portent sur l'intégrité, l'exactitude, la validité, la confidentialité et la disponibilité des opérations et des données au cours du traitement par l'application.

- Les **contrôles d'intégrité** doivent apporter l'assurance raisonnable que toutes les opérations effectuées ont bien été saisies dans le système, que leur traitement a été accepté, que le système les a traitées une fois et une fois seulement, et qu'elles ont été correctement incluses dans le résultat produit.
- Les **contrôles d'exactitude** doivent apporter, entre autres choses, l'assurance raisonnable que les opérations ont été correctement enregistrées, pour le bon montant/avec les bonnes données, et en temps utile.
- Les **contrôles de validité** doivent apporter l'assurance raisonnable (1) que toutes les opérations enregistrées ont effectivement été exécutées, qu'elles concernent l'organisation et qu'elles ont été dûment approuvées conformément aux procédures d'autorisation de la direction et (2) que le résultat produit contient uniquement des données valides.
- Les **contrôles de confidentialité** doivent apporter l'assurance raisonnable que les données, les rapports et les autres résultats produits par l'application sont protégés contre tout accès non autorisé.
- Les **contrôles de disponibilité** doivent apporter l'assurance raisonnable que les utilisateurs peuvent facilement accéder aux données, rapports et autres informations de l'application qui sont pertinents pour les métiers, quand ils en ont besoin.

La revue des contrôles d'application permet à l'auditeur de proposer à la direction une évaluation indépendante de la performance et de l'efficacité de la conception et du fonctionnement des contrôles

internes et des procédures opérationnelles portant sur l'automatisation d'un processus métier, mais aussi d'identifier les problèmes éventuels liés aux applications, qu'il convient de traiter. Si les contrôles informatiques généraux de l'organisation définissent le cadre global du contrôle des systèmes d'information, les contrôles d'application sont intégrés spécifiquement à certaines applications, dans l'objectif de garantir et protéger l'exactitude, l'intégrité, la fiabilité et la confidentialité de l'information. Ils garantissent par exemple que le lancement d'une opération a été dûment autorisé, que le traitement porte sur des données entrantes valides, que ces données sont totalement enregistrées et que les résultats présentés sont exacts. Les contrôles généraux contribuent à garantir que le travail effectué pour mettre en œuvre un contrôle d'application est proportionnel au risque d'une défaillance de cette application. Par exemple, la probabilité qu'une personne non autorisée accède à une configuration clé pour un contrôle d'application, ou que cette configuration soit modifiée sans autorisation ou test approprié.

Comme les contrôles d'application sont étroitement liés aux différentes opérations, un test de ces contrôles permettra à l'auditeur d'obtenir plus directement l'assurance de l'exactitude d'une fonctionnalité en particulier. Par exemple, tester les contrôles d'une application de paie fournit une assurance concernant les chiffres de paie des comptes d'un client. Tester les contrôles informatiques généraux (par exemple, les procédures de contrôle des changements) du client, qui couvrent un périmètre plus large, ne permet pas d'obtenir un niveau d'assurance similaire pour un même solde de compte.

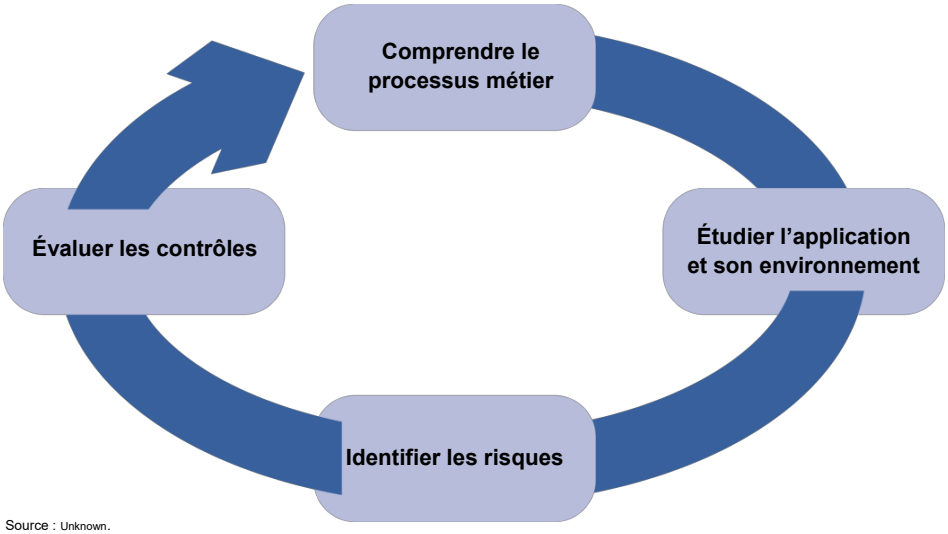
Selon les objectifs spécifiques de l'audit, différentes approches peuvent être adoptées pour examiner et tester les contrôles d'application. On pourra par exemple axer la revue de l'application sur la conformité avec les lois et les normes. Dans ce cas, l'objectif serait de vérifier si les contrôles d'application contribuent effectivement à assurer cette conformité. La revue de l'application peut aussi être effectuée dans le cadre d'un audit de performance, auquel cas il serait important d'étudier comment les principes de gestion se reflètent dans l'application. Dans le contexte d'une analyse de la sécurité de l'information, l'accent pourrait être mis sur les contrôles d'application visant à garantir la confidentialité, l'intégrité et la disponibilité des données.

a. Procédure de revue des contrôles d'application

Les étapes à réaliser pour effectuer la revue des contrôles d'application s'inscrivent souvent dans un cycle d'activités. La figure 10 montre les étapes typiques du cycle de revue des contrôles d'application. Même si, comme le montre la flèche, la logique invite à commencer par acquérir une compréhension globale du processus métier, il est important de noter qu'il n'existe pas de hiérarchie stricte entre les différentes étapes du cycle.

La figure est suivie d'une brève description des quatre phases du cycle.

Figure 10 Le cycle de revue d'une application



Source : Unknown.

xxii. Comprendre le processus métier

Pour étudier les aspects techniques de l'application, il est utile d'acquérir en premier lieu une vue d'ensemble des processus métier que l'application permet d'automatiser : les règles, les flux, les acteurs, les rôles et les exigences de conformité associés. Comprendre le processus métier sous-jacent est une étape importante pour vérifier la cohérence des contrôles d'application et des processus automatisés. Les activités correspondant à cette étape varient selon l'objectif de l'audit. Il s'agit habituellement d'étudier les procédures d'exploitation et les modes opératoires, le schéma des flux de processus de l'organisation, ou d'autres documents de référence. L'équipe d'audit peut également être amenée à rencontrer et à interviewer des managers métiers, des responsables informatiques et des utilisateurs d'applications clés. Elle peut juger intéressant d'établir ses propres organigrammes et d'y reporter les processus, contrôles, systèmes, interfaces et rapports qui constituent le processus. Ce type d'organigramme créé par l'équipe d'audit peut être utile car, souvent, les processus client sont soit trop complexes et détaillés, soit pas assez détaillés pour permettre une bonne compréhension et pour identifier les aspects et les risques pertinents du processus.

xxiii. Comprendre l'application et son environnement

L'auditeur a pris connaissance du processus métier. Il doit maintenant comprendre les réseaux et systèmes spécifiques utilisés à l'appui des applications clés de ce processus. Les informations recueillies au cours de cette étape contribuent à l'identification des points de contrôle critiques et apportent une base de référence pour comprendre où interviennent les contrôles au niveau des applications. Cette étape comprend un travail de revue documentaire (organigrammes, flux de données, manuels d'utilisation), des entretiens avec les collaborateurs clés, l'étude des principales fonctions du logiciel par observation et interaction avec les opérateurs en cours de travail. Complété par des discussions, ce travail permet de suivre concrètement le déroulement de l'ensemble du processus métier et de l'application, de l'entrée source au produit sortant et au rapprochement des données. À ce stade, l'auditeur peut observer toute activité manuelle connexe susceptible de constituer un contrôle complémentaire.

Les auditeurs peuvent également obtenir de la documentation sur l'infrastructure technique (système d'exploitation, environnement réseau, système de gestion des bases de données, interfaces avec d'autres applications, sources internes ou externes, traitement des opérations par lots, en temps réel et en ligne), dont ils peuvent discuter avec les responsables, les opérateurs et les développeurs. Ces discussions et cette documentation peuvent apporter des indications utiles quant aux incidences de

l'infrastructure sur l'application.

xxiv. Identifier les risques

En s'appuyant sur la compréhension du processus qu'il a acquise lors des étapes précédentes, l'auditeur doit tout d'abord évaluer la nature et l'ampleur du risque lié aux applications clés pour les systèmes d'information. Cette étape vise à identifier les risques associés à l'activité/la fonction métier utilisant l'application, pour déterminer les défaillances que l'application est susceptible de présenter, et pour voir comment ces risques sont traités par les contrôles en place dans le logiciel d'application. Il est possible qu'une évaluation du risque du processus métier soit déjà disponible, provenant par exemple d'un précédent audit ou d'une revue de gestion. L'auditeur pourra s'appuyer sur ce travail antérieur, après avoir déterminé dans quelle mesure il peut se fier à la précédente évaluation du risque.

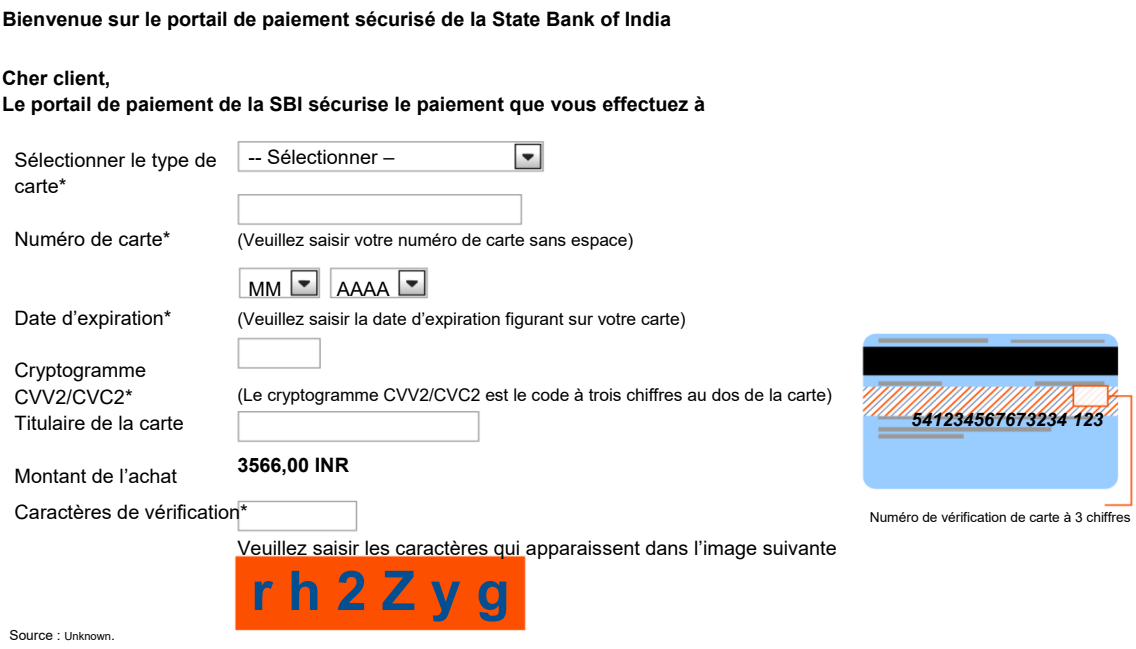
xxv. Comprendre et évaluer les contrôles

Pour chaque application clé des processus métiers, l'auditeur doit identifier les différents types de contrôle au niveau de l'application qui présentent un intérêt pour les objectifs d'audit. Après s'être familiarisé avec l'environnement (métier et technique) de l'application, l'auditeur est mieux à même d'évaluer les contrôles utilisés pour traiter les risques identifiés. Il doit faire appel à son jugement pour évaluer les contrôles d'application et considérer les coûts et les avantages au moment de formuler des recommandations d'amélioration. Par exemple, un excès de détail dans les journaux des opérations peut entraîner une augmentation des coûts généraux, sans fournir la traçabilité souhaitée. Cette évaluation implique d'examiner les contrôles d'application à la lumière des éléments décrits ci-après. L'auditeur pourra également constater que plusieurs contrôles sont parfois en place pour atténuer un même risque. Dans ce cas, il pourra proposer au client une recommandation d'amélioration du processus.

b. Illustration

La figure 11 propose une illustration des éléments des contrôles d'application. Pour une application de paiement en ligne, une condition de saisie pourrait consister à vérifier que la date d'expiration de la carte de crédit est ultérieure à la date de l'opération. Une autre condition pourrait porter sur la validité du numéro de carte, et sa correspondance avec le nom du titulaire de la carte et le cryptogramme (CVV) indiqué au dos, d'après les informations de la base de données de l'émetteur de la carte de paiement. Ou encore, que les données transmises sur le réseau soient cryptées. Les contrôles, tels que ceux qui sont intégrés à l'application, doivent garantir que ces conditions sont incontournables, et ainsi, améliorer la validation des opérations.

Figure 11 : Exemple de contrôles d'application



Source : Unknown.

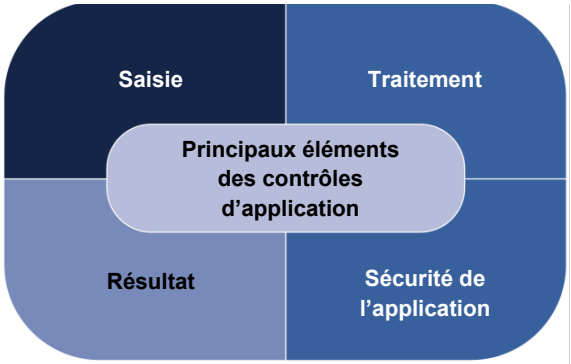
En complément des contrôles automatisés tels que ceux que l'on a décrits, les contrôles d'application comprennent également des procédures manuelles qui s'exécutent à proximité de l'application. Ces contrôles ne sont pas seulement intégrés aux applications en question, mais également aux processus métiers connexes. Par exemple, un opérateur de saisie de données peut exiger qu'un formulaire de saisie de données soit signé (c'est-à-dire, validé) avant la saisie dans l'application. Le choix de la combinaison de contrôles manuels et automatisés retenue dépend souvent de considérations de coûts et de contrôle, examinées au moment de la conception de l'application.

II. Les principaux éléments des contrôles d'application

Un contrôle d'application se compose principalement des segments suivants : saisie des données (origination et saisie de données), traitement de l'opération, sortie de données (distribution des résultats) et sécurité (journalisation, communication, stockage). Les contrôles d'une application sont intégrés à chaque segment de cette application, avec les contrôles qui restreignent l'accès à l'application et aux fichiers maîtres.

Naturellement, il n'est pas réaliste de fournir ici le détail des tests et des listes de contrôle de chaque permutation possible d'une application, mais l'auditeur doit connaître les concepts de contrôle qui sont communs à presque toutes les applications et tous les processus métiers.

Figure 12 : Les principaux éléments des contrôles d'application



Source : Unknown.

La compréhension de ces contrôles communs aux applications nourrira la réflexion de l'auditeur, et lui

donnera des pistes pour concevoir des étapes de test d'audit concernant plus spécifiquement l'application auditée.

La figure 13 présente certains des éléments de contrôle les plus fréquents pour chacun des 4 domaines clés identifiés :

Figure 13 : Exemples de contrôles d'application

Contrôles à l'entrée	▪ Quelles sont précisément les questions ou les hypothèses examinées ? ▪ Vérification de saisie de données/de champs (par ex., validation du numéro de carte de crédit saisi) ▪ Gestion des documents sources (par ex., procédures de préparation et de conservation) ▪ Mécanismes de traitement des erreurs (messages d'erreur, fichiers d'attente)
Contrôles de traitement	▪ Mappage des règles métier ▪ Contrôles d'intégrité, rapport des déséquilibres ▪ Calculs automatisés ▪ Rapprochement des saisies
Contrôles à la sortie	▪ Validation d'intégrité et d'exactitude, rapprochement ▪ Revue et traçabilité des résultats ▪ Examen et suivi des rapports d'exception générés par l'application ▪ Procédures d'étiquetage, traitement, conservation et distribution des résultats
Contrôles de sécurité de l'application	▪ Mécanismes de traçabilité (piste d'audit, revue de journaux, utilisation d'identifiants uniques) ▪ Contrôle d'accès logique aux fonctionnalités et aux données de l'application ▪ Protection des données stockées

Source : Unknown.

a. Contrôles à l'entrée

Les contrôles à l'entrée cherchent à valider et à authentifier les activités de préparation, d'autorisation et de saisie des données sources, de sorte que l'application accepte en temps utile des données précises, fiables et complètes Bien que la saisie de données puisse être manuelle ou déclenchée par l'interface système, il est possible de réduire les erreurs et omissions par une bonne conception de la saisie, par la séparation pertinente des tâches concernant l'origination et la validation des documents intrants, et par la mise en place d'une vérification efficace de l'authenticité, de l'exactitude et de l'intégrité des données (au moyen d'options de menu ou de messages interactifs). Le tableau suivant recense les principaux éléments des contrôles à l'entrée.

Éléments des contrôles à l'entrée	Description
Contrôles de la saisie des données (validité, intégrité, recherche de doublons)	Contrôles automatisés de validité des données saisies (par ex., la date du voyage se situe en dehors de la période d'ouverture des réservations), contrôles d'exhaustivité pour s'assurer que toutes les informations importantes pour l'opération ont été saisies (par ex., date du voyage, nom des passagers, et numéro d'identité sont des champs obligatoires), recherche de doublons par comparaison des nouvelles opérations aux opérations enregistrées précédemment (par ex., contrôle des factures en double), assurance que toute saisie hors paramètres déterminés par la direction déclenche une erreur.
Gestion des documents sources	Documentation des procédures de préparation des documents sources, définition d'une stratégie relative aux données des opérations et de procédures de conservation des documents, les documents sources des saisies de données doivent être enregistrés et traçables, les documents sources doivent fournir des codes d'entrée prédéterminés pour réduire les erreurs et comporter une section permettant de documenter les autorisations.

Procédures de traitement des erreurs	Il existe des procédures pour traiter les entrées rejetées (par ex., utilisation de messages d'erreur appropriés, invites permettant de recommencer la saisie, utilisation de données transitoires), les erreurs sont examinées et des mesures correctrices sont décidées en conséquence.
Autorisation de la saisie	Le formulaire de saisie de données exige des procédures manuelles et la validation de la saisie par le superviseur. (Par ex., validation des détails de la déclaration d'entrée par le superviseur avant saisie par l'opérateur chargé de la saisie de données dans le cadre du traitement des applications douanières), les procédures de validation sont appliquées pour la saisie des données.

b. Contrôles de traitement

Les mesures de contrôle de traitement visent à protéger l'intégrité, la validité et la fiabilité des données, et à les préserver des erreurs de traitement tout au long du cycle de traitement des opérations, de la réception des données transmises par le sous-système d'entrée jusqu'à leur envoi à la base de données, aux sous-systèmes de communication ou de sortie. Elles permettent également d'assurer que les données valides saisies sont traitées une fois seulement, et que la détection d'opérations erronées n'interrompt pas le traitement des opérations valides. Les contrôles renforcent ainsi la fiabilité des programmes d'application qui exécutent des instructions répondant aux besoins spécifiques des utilisateurs.

Dans ce domaine, les procédures de contrôle comportent également la création et la mise en place de mécanismes autorisant le déclenchement du traitement des opérations, la vérification que seuls sont utilisés des applications et des outils appropriés et validés, et la vérification régulière du caractère complet et exact des contrôles automatisés, le cas échéant. Les contrôles peuvent inclure la vérification de la séquence de traitement et la recherche d'erreurs de redondance ou de dépassement de la mémoire tampon, le suivi du nombre d'opérations/d'enregistrements, des contrôles d'intégrité référentielle et des contrôles par fourchette, la comparaison du total de contrôle et du total obtenu par hachage.

Les systèmes en temps réel peuvent utiliser d'autres contrôles compensatoires, comme le contrôle un-pour-un, le groupage rétrospectif, les rapports par exception, et les rapports des comptes d'attente. Le tableau suivant recense les principaux éléments des contrôles de traitement.

Éléments des contrôles de traitement	Description
Mappage des règles métier	Vérifier les configurations pour garantir que les opérations sont exécutées conformément aux paramètres et tolérances prédéterminés, qui sont spécifiques à la gestion du risque de l'organisation. Documenter les paramètres et les tolérances, et faire en sorte que la direction examine régulièrement les restrictions qui en découlent. Veiller à ce que les opérations correspondent aux autorisations de la direction.
Contrôles d'intégrité	Examiner un échantillon de journaux du système pour les opérations. Établir si les applications exécutent les vérifications d'édition et de validation appropriées en fonction des données traitées, si elles génèrent les messages d'erreur ou les rejets appropriés, et si elles communiquent effectivement aux utilisateurs les erreurs traitées.
Calculs automatisés	Déterminer dans quelle mesure le traitement de données par l'application est automatisé et standardisé. Examiner la documentation de conception sur laquelle le traitement s'appuie et vérifier que les applications et les données utilisées correspondent à la bonne version.
Rapprochement de la saisie	Inspecter les procédures de rapprochement périodique pour déterminer si les rapprochements sont bien effectués et documentés, en examinant plus en détail certaines de ces procédures pour recueillir des éléments probants appropriés. Déterminer si le système est configuré pour s'équilibrer automatiquement, lorsque cela est possible.

c. Contrôles à la sortie

Les contrôles à la sortie correspondent à des mesures intégrées à l'application, visant à garantir que le résultat de l'opération est complet, exact et correctement distribué. L'objectif est également de protéger les données traitées par une application de toute modification ou distribution sans autorisation.

Les processus de contrôle comportent une définition précise des résultats, des rapports souhaités aux étapes de conception et de développement du système, une documentation pertinente de la logique d'extraction des rapports, des contrôles limitant l'accès aux données traitées, un examen des résultats, un rapprochement, une revue finale. Le tableau suivant recense les principaux éléments des contrôles à la sortie.

Éléments des contrôles à la sortie	Description
Contrôles d'intégrité, vérifiant le caractère complet et exact	Effectuer des contrôles d'intégrité des données en rapprochant les intrants et les produits du processus, pour en vérifier le caractère complet et exact en référence aux procédures documentées. Vérifier le caractère acceptable et complet des résultats, y compris les totaux de contrôle et les journaux d'erreurs. Vérifier le volume, la valeur et le type des résultats produits par rapport aux attentes.
Examen, suivi et traçabilité des produits, y compris des résultats traités	Contrôler les procédures de gestion pour définir et attribuer le produit du processus ou les rapports en fonction des besoins des utilisateurs finaux. Examiner les rapports de suivi des résultats du traitement, le contenu et le calendrier des revues par la direction des résultats traités, et déterminer dans quelle mesure la direction surveille les contournements appliqués aux opérations. Examen et suivi des rapports d'exception générés par l'application. Examiner les rapports de sortie pour vérifier leur conformité aux lois et règlements applicables.
Étiquetage, manipulation, distribution et conservation des résultats produits	Examiner les procédures en place pour contrôler l'utilisation des données de sortie dans les rapports de gestion ou d'autres communications externes et examiner un échantillon de données issues de ces communications. S'assurer que les utilisateurs ont un accès aux données de sortie qui soit conforme à leur rôle.

d. Contrôles de sécurité de l'application

La sécurité des applications vise à préserver la confidentialité, l'intégrité et la disponibilité des informations au niveau de la couche applicative. Dans le cadre d'un audit de la sécurité des applications, il est important de comprendre les interfaces (c'est-à-dire, les différentes sources des données qui entrent et sortent de l'application) et la manière dont les données sont stockées.

Généralement, l'accès aux applications nécessite des identifiants utilisateurs et des mots de passe personnalisés. D'autres formes de connexion ont toutefois gagné en popularité, compte tenu du large éventail d'applications disponibles en environnement professionnel. Aussi est-il important de déterminer d'emblée comment l'application a été conçue pour le provisionnement et l'accès des utilisateurs. Par exemple, afin de bien comprendre les règles d'accès utilisées dans l'application, l'auditeur peut avoir besoin d'examiner les politiques et procédures de l'organisation encadrant l'obtention et la révocation des accès des utilisateurs. L'accès des utilisateurs peut être réagi localement par l'application, ou à l'échelle de l'organisation, au moyen de plusieurs systèmes connectés appliquant un mécanisme unique d'ouverture de session[76].

Pour comprendre les procédures de contrôle de sécurité de l'application, l'auditeur doit identifier les acteurs, les rôles et les responsabilités associés à l'application, dont les administrateurs, les superutilisateurs/utilisateurs privilégiés et les utilisateurs ordinaires. La méthode de contrôle d'accès d'une application peut varier et faire appel au modèle standard par identifiant utilisateur et mot de passe,

[76] L'ouverture de session unique permet à un utilisateur de conserver les mêmes identifiants pour se connecter à différentes applications.

utiliser des certificats numériques permettant d'identifier un utilisateur de façon certaine[77], utiliser un jeton ou des données biométriques[78], ou encore utiliser plusieurs méthodes d'authentification à deux facteurs ou plus[79]. Le contrôle d'accès peut concerner chaque module, option de menu ou écran d'une application, faire appel à des objets et dépendre du rôle. L'auditeur informatique doit examiner la conception du module de contrôle d'accès, en gardant à l'esprit le caractère critique des fonctions/actions disponibles.

Voici quelques exemples d'aspects des contrôles de sécurité des applications qui sont susceptibles d'être audités :

- **Examen du suivi de l'audit et de la gestion des configurations.** Cet examen porte sur la traçabilité des opérations, comme la journalisation des transactions et la conservation de la piste d'audit, comprend la création et le suivi de journaux, le contrôle des mouvements et l'accès aux programmes, données et bibliothèques de programmes, l'évaluation périodique des changements, et contrôle l'utilisation d'identifiants et de rôles uniques pour effectuer les changements. Dans l'idéal, le journal de piste d'audit consigne les enregistrements ou les champs qui ont été modifiés, la date de ces modifications, la situation antérieure et le résultat de la modification, ainsi que l'auteur de la modification.
- **Examen des contrôles d'accès.** Cet examen comprend une revue des comptes d'utilisateurs, des autorisations et des politiques de gestion des mots de passe, l'utilisation de comptes d'invités, de comptes de test et de comptes génériques, l'utilisation de comptes privilégiés et de comptes d'administrateur, l'examen des contrôles compensatoires, des procédures d'attribution et de révocation des accès, de l'application du principe de moindre privilège, de l'accès de l'équipe informatique/de développement aux bases de données de production, des procédures formelles de validation et d'attribution des accès, de l'utilisation de mots de passe forts, de l'application des changements périodiques, ainsi que du chiffrement des mots de passe.
- **Contrôle du paramétrage et de la maintenance des données permanentes.** Les données permanentes sont des informations clés, partagées par plusieurs fonctions des applications. Les contrôles comprennent l'examen de la configuration des champs de données clés, la vérification que les modifications des données permanentes sont autorisées et effectuées conformément aux règles de modification, que les données permanentes sont à jour, exactes et cohérentes dans toute l'organisation, que l'intégrité et la confidentialité des données permanentes sont préservées. Les données permanentes sont par exemple les coordonnées des fournisseurs et des clients (nom, adresse, téléphone, numéro de compte), un taux d'inflation ou encore des données d'administration du système, comme des fichiers de mots de passe et des permissions de contrôle d'accès.
- **Séparation des accès utilisateurs.** L'accès des utilisateurs doit être séparé pour éviter les conflits entre opérations et activités, et cet accès doit être suivi au moyen de modes opératoires formalisés, d'un processus de supervision et de revue.
- **Établissement d'un plan de secours.** Ce travail de planification comprend l'appréciation du caractère critique et sensible de l'application, la définition d'étapes permettant de prévenir et de minimiser les conséquences dommageables ou l'interruption de l'application, ainsi qu'une évaluation de la planification globale de l'organisation pour les situations d'urgence.

---

[77] Les certificats numériques sont émis par une source de confiance, et fournissent une assurance quant à l'identification d'une personne.

[78] Les dispositifs biométriques sont utilisés pour identifier les personnes à partir de caractéristiques anatomiques, physiologiques et comportementales mesurables.

[79] L'authentification multifacteurs exige au moins deux types d'éléments d'authentification différents pour accorder un accès.

III. Contrôles des systèmes d'interface et de gestion et des données

En complément des contrôles d'application des processus métiers présentés ci-dessus, les contrôles d'interface et de gestion des données contribuent de façon significative à garantir le bon fonctionnement des applications.

a. Contrôles d'interface

Les contrôles d'interface ont une incidence sur les interactions entre les différentes applications du processus métier. Ces contrôles portent d'une part sur le traitement en temps utile, exact et complet des informations entre les applications et d'autres systèmes qui transmettent et reçoivent des données en continu, et d'autre part, sur la migration complète et exacte de données propres pendant la conversion. Les interfaces permettent l'échange structuré de données entre deux applications informatiques. Ces applications peuvent résider sur le même système informatique ou sur des systèmes différents, qui peuvent ou non se trouver dans le même environnement physique. Les interfaces sont périodiques et récurrentes par nature.

L'objectif des contrôles d'interface est de mettre en œuvre une stratégie et une conception efficaces, de déployer des procédures de traitement garantissant que les interfaces sont traitées de façon complète et exacte, que les erreurs sont corrigées, que l'accès aux données d'interface et au processus est restreint conformément aux besoins, que les données sont fiables et qu'elles ont été obtenues uniquement auprès de sources autorisées. Dans la mesure où les intrants de données sont issus d'autres applications, l'auditeur évaluera ces données en tenant compte des contrôles à l'entrée.

b. Contrôles de gestion des données

Les applications qui soutiennent les processus métiers génèrent, accumulent, traitent, stockent, communiquent et affichent des données. Les applications qui traitent d'importants volumes de données emploient souvent des systèmes de gestion de données pour exécuter certaines fonctions de traitement. Ces systèmes font appel à des logiciels spécialisés, qui peuvent nécessiter un matériel spécialisé. Ce sont par exemple les systèmes de gestion de bases de données, les logiciels spécialisés de transport et de communication de données (généralement appelés programmes intermédiaires), les processus de chiffrement utilisés en association avec les contrôles intégrité des données, les logiciels d'entrepôts de données et les logiciels de génération de rapports/d'extraction de données. Ces systèmes de gestion de données permettent de déployer une part importante des contrôles des données d'entrée et de leur traitement, tels que les contrôles de validation, les contrôles d'existence et les seuils décrits précédemment. Ces types de contrôles déployés dans les systèmes de gestion de données sont souvent désignés sous l'appellation de « règles métiers ».

Pour apprécier l'efficacité des contrôles d'application, l'auditeur doit évaluer les fonctions des systèmes de gestion de données qui sont spécifiques au processus métier examiné, en plus des contrôles généraux. Pour la plupart des applications de grande ampleur et/ou à haute performance, les différents composants des systèmes de gestion de données résident sur des serveurs distincts, qui utilisent généralement différents systèmes d'exploitation et différentes technologies matérielles. L'auditeur doit s'efforcer de comprendre les liens entre les différentes technologies de gestion de données en jeu, et de considérer les risques associés de manière appropriée.

Pour être en mesure de bien évaluer le risque, l'auditeur doit comprendre la conception logique et l'architecture physique des composants de gestion de données de l'application. En plus de prendre en charge des fonctions de stockage et d'extraction des données, les applications utilisent habituellement des systèmes de gestion de données pour traiter les aspects opérationnels de l'application, tels que la gestion des données d'état des sessions utilisateur transitoires, les informations de sécurité spécifiques aux sessions, les journaux d'audit transactionnels et d'autres fonctions essentielles au fonctionnement de l'application. Les contrôles associés à ces types de fonctions peuvent être critiques pour la sécurité de l'application.

Les contrôles intégrés à un système de gestion des données doivent tenir compte des chemins d'accès à ce système. En général, cet accès peut être obtenu directement par des chemins d'accès facilités par l'application, ou par le système d'exploitation sous-jacent au système de gestion des bases de données.

Les systèmes de gestion de données ont des comptes privilégiés intégrés, utilisés pour l'administration et la maintenance du système. L'auditeur doit déterminer si des contrôles appropriés sont en place pour sécuriser ces comptes privilégiés. L'auditeur doit identifier ces comptes privilégiés, mais aussi comprendre le rôle du système de gestion de données dans l'authentification et l'autorisation de l'application.

IV. Risques pour l'entité auditée

Les conséquences d'une défaillance des contrôles d'application dépendent généralement de la nature de l'application métier. Le risque encouru va de l'insatisfaction d'un utilisateur à de réelles catastrophes, pouvant entraîner des décès. L'organisation peut par exemple perdre des parts de marché en cas d'indisponibilité d'un service, elle peut perdre du chiffre d'affaires si les systèmes de gestion des ventes en ligne n'enregistrent pas certaines commandes d'achat, les citoyens peuvent perdre confiance dans les services publics, le non-respect des exigences légales peut entraîner des poursuites judiciaires, certains foyers peuvent être privés d'électricité, des comptes bancaires peuvent être liés à des fraudes.

Plus précisément, en l'absence de contrôles efficaces à l'entrée, l'organisation court le risque d'un traitement erroné ou frauduleux des données, et l'application pourrait ne pas répondre aux objectifs métiers qu'elle doit servir. Dans ce cas, les données traitées par l'application pourraient être incohérentes, et les programmes pourraient fournir des résultats inappropriés. Dans certaines situations très spécifiques, il est également possible de contourner les contrôles des systèmes. Pour traiter ces cas, il est impératif de mettre en place des contrôles compensatoires, tels que des journaux et des règles d'autorisation. Sinon, le privilège de contournement pourrait être utilisé à mauvais escient et conduire à l'entrée de données incohérentes dans l'application.

Pour atténuer les risques auxquels l'organisation est exposée, la bonne gestion des documents source et des autorisations de saisie des données sont également des contrôles à l'entrée importants. En l'absence de gestion efficace des documents sources, la traçabilité de la source des informations du système ne pourra être assurée, la conformité légale ne pourra être garantie, et les politiques de conservation pourraient ne pas être respectées, avec pour conséquence l'entrée de données non fiables dans l'application. À l'inverse, l'absence de contrôle d'autorisation peut conduire à des erreurs ou à des fraudes rendues possibles par les données non autorisées.

Une défaillance des contrôles de traitement peut entraîner des erreurs de traitement, et l'application pourra ne pas répondre aux objectifs métiers. Ce type de défaillance peut résulter d'un mauvais mappage des règles métiers, d'un manque de validation du code programme, ou d'un manque de contrôle sur les différentes versions des programmes utilisées pour rétablir l'intégrité du traitement après un problème ou une interruption inattendue. L'absence de contrôle adapté sur le traitement peut entraîner la répétition d'opérations erronées, avec des incidences sur les objectifs métiers et la cote d'estime de l'organisation.

Les systèmes de traitement en temps réel privent l'organisation de certaines mesures de contrôle, comme le rapprochement des totaux d'entrée et de sortie par lots, qui permet d'évaluer le caractère exhaustif des intrants, ou la conservation de certains documents d'origination de données permettant d'alimenter un journal de piste d'audit. Toutefois, les systèmes en temps réel embarquent d'autres contrôles compensatoires dans les applications, avec le contrôle interactif d'exhaustivité des données, des invites de validation ou la journalisation des tentatives d'accès.

L'absence de contrôles adéquats à la sortie entraîne un risque de modification/suppression de données sans autorisation, de génération de rapports de gestion inadaptés, ou de violation de la confidentialité des données. En outre, les conséquences de la génération de résultats erronés dépendront pour beaucoup de la façon dont l'organisation utilise les informations produites.

Sur le plan de la sécurité des applications, l'insuffisance des mécanismes de journalisation peut empêcher d'identifier avec certitude l'auteur d'un comportement inapproprié. De même, on peut atténuer le risque d'utilisation abusive des systèmes d'information en informant les utilisateurs de l'existence de procédures d'examen des journaux et de dispositifs de signalement. Les erreurs portant sur les données permanentes ont des effets considérables sur l'application, car ces données peuvent être utilisées pour une très grande partie des opérations traitées par l'application.

Plus généralement, l'insuffisance des contrôles de sécurité de l'information peut entraîner des risques plus ou moins graves, comme la perte de chiffre d'affaires, l'interruption d'un service, la perte de crédibilité, une interruption des activités, une mauvaise utilisation des informations, des conséquences juridiques ou judiciaires, une violation de propriété intellectuelle. Ces différents risques et les contrôles permettant de les atténuer sont abordés plus en détail au chapitre 7 consacré à la sécurité de l'information.

IV. Références et lectures complémentaires

Davis, Chris, Mike Schiller and Kevin Wheeler. *IT Auditing: Using Controls to Protect Information Assets*, 2ème éd. 31 janvier 2011.

ISACA. *IT Audit and Assurance Guideline G38, Access Controls.* 2007.

National Institute of Standards and Technology. *Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations,* rév. 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. Septembre 2020.

Office of the Comptroller & Auditor General of India. *Manual of Information Technology Audit,* vol. I. https://ag.ap.nic.in/GSSA/PDF_Files/ITAM Vol_I.pdf.

U.S. Government Accountability Office. *Federal Information Systems Audit Manual (FISCAM).* https://www.gao.gov/products/gao-09-232g. 2 février 2009.