GUID 5100

Lignes directrices sur la vérification des systèmes d'information.

Juin 2019

Les Normes internationales des institutions supérieures de contrôle des finances publiques (ISSAI) sont publiées par l'Organisation internationale des institutions supérieures de contrôle des finances publiques (INTOSAI). Pour plus de renseignements visitez le site www.issai.org

INTOSAI

TABLE DES MATIÈRES

1

INTRODUCTION

1.1 Le GUID 5100 fournit le cadre général pour la vérification des systèmes d'information du IFPP.Le GUID est destiné à servir de base à l'élaboration des futurs GUID des séries 5100-5109 sur le thème de l'audit des systèmes d'information, au sein du IFPP.

1.2 Le cadre défini dans le présent GUID est conforme aux principes fondamentaux de l'audit du secteur public (ISSAI 100), aux principes fondamentaux de l'audit financier (ISSAI 200), aux principes de l'audit de la performance (ISSAI 300) et aux principes de vérification de la conformité (ISSAI 400).

1.3 Les institutions supérieures de contrôle (ISC) sont chargées de contrôler les gouvernements et leurs entités conformément à leurs mandats de contrôle respectifs.[1] Dans le cadre de leurs activités, les ISC visent à promouvoir l'efficience, la responsabilité, l'efficacité et la transparence de l'administration publique[2].

1.4 Les gouvernements et d'autres entités du secteur public n'ont cessé d'innover dans le domaine des technologies de l'information (TI) dans leurs systèmes d'information afin d'améliorer l'efficience et l'efficacité de leur fonctionnement et la prestation des divers services publics. En effet, les technologies de l'information ont permis la saisie, le stockage, le traitement, la récupération et la fourniture d'informations par voie électronique, ce qui, à son tour crée une marge importante pour améliorer l'exactitude, la confidentialité et l'actualité des données des systèmes d'information. En outre, le mode de prestation des services publics passe rapidement du mode physique au mode électronique, ce qui oblige les gouvernements à fonctionner comme des plateformes numériques fournissant des

1 INTOSAI-P 1 La Déclaration de Lima
2 Résolution de l'Assemblée générale des Nations unies A/66/209

services ainsi que des infrastructures pour d'autres systèmes d'information axés sur les TI.

1.5 Ce passage aux systèmes d'information informatisés et au traitement électronique par les entités contrôlées du secteur public a entraîné un changement significatif de l'environnement dans lequel les ISC travaillent. Les dépenses informatiques du secteur public augmentent. Il est également nécessaire de veiller à ce que les entités du secteur public aient adopté des contrôles informatiques internes pour préserver la confidentialité, l'intégrité et la disponibilité des données. Il est donc impératif que les ISC se dotent des capacités nécessaires pour procéder à un examen approfondi des contrôles liés aux systèmes d'information.

2 OBJECTIF DU PRÉSENT GUID

2.1 Les ISSAI 100, 200, 300 et 400 définissent les préceptes de base de l'audit en matière d'audit financier, d'audit de performance et d'audit de conformité. Ces ISSAI portent sur les principes généraux, les procédures, les normes et les attentes d'un auditeur. Elles sont également applicables aux audits des systèmes d'information.

2.2 L'objectif de ce GUID est de fournir des conseils aux auditeurs sur la manière d'effectuer des audits de performance et/ou de conformité liés à l'objet spécifique des systèmes d'information ou lorsque l'audit des systèmes d'information peut faire partie d'une mission d'audit plus large qui peut être l'audit financier, de conformité ou de performance.

2.3 Le contenu du présent GUID peut être appliqué par les auditeurs aux étapes de planification, d'exécution, de rapport et de suivi[3] du processus d'audit.

3 ISSAI 100

3 DÉFINITIONS

3.1 Systèmes d'information : Les systèmes d'information peuvent être définis comme une combinaison d'activités stratégiques, managériales et opérationnelles impliquées dans la collecte, le traitement, le stockage, la distribution et exploitant l'information et ses technologies connexes. La complexité d'un tel système d'information peut aller d'un simple livre dans lequel les entrées pour la réception et le paiement de l'argent sont effectuées manuellement, à un système informatique plus complexe tel qu'un système d'évaluation fiscale, dans lequel tous les processus - collecte des données (par exemple, les déclarations fiscales produites via un portail Web en ligne), stockage sur serveurs, traitement des évaluations (basé sur une programmation observant des règles fiscales) et communication de la déclaration, du remboursement et de l'attestation d'impôts (en temps réel ou selon des intervalles déterminés)- sont automatisés. La technologie de l'information comprend le matériel, les logiciels, les moyens de communication et les autres installations utilisées pour saisir, stocker, traiter, transmettre et générer des données sous quelque forme que ce soit.

3.2 La vérification des systèmes d'information peut être définie comme l'examen des contrôles liés aux systèmes d'information axés sur les TI, afin de déceler les cas d'écart par rapport aux critères, lesquels ont été identifiés en fonction du type de mission d'audit - c-à-d. audit financier, audit de conformité ou audit de performance.

4

DÉLIMITATION DE LA VÉRIFICATION

4.1 Ce GUID peut être utilisé par les auditeurs pour effectuer des audits de performance et/ou de conformité sur l'objet spécifique des systèmes d'information, ainsi que lorsque l'audit des systèmes d'information fait partie d'une mission d'audit plus large qui peut être un audit financier, de conformité et/ou de performance.

4.2 Cette ligne directrice fournit d'autres conseils sur la façon dont une vérification des systèmes d'information pourrait être effectuée au moyen d'une vérification financière, d'une vérification de la performance et d'une vérification de la conformité et ne contient pas d'autres exigences pour la réalisation de la vérification.

5 PLANIFICATION DE L'AUDIT DES SYSTÈMES D'INFORMATION

5.1 Les ISC peuvent adopter une planification d'audit axée sur les risques pour les audits des systèmes d'information, conformément au processus décrit dans les ISSAI 100, ISSAI 200 (Audit financier), ISSAI 300 (Audit de performance) et ISSAI 400 (Audit de conformité), en fonction des objectifs de la mission d'audit.

5.2 L'audit des systèmes d'information sera déterminé par l'objectif et la délimitation de la vérification. Entre autres exemples, on pourrait citer :

1) Évaluer les contrôles généraux[4] et les contrôles d'application[5] pertinents qui ont une incidence sur la fiabilité des données provenant des systèmes d'information et qui, à leur tour, ont une incidence sur les états financiers de l'entité contrôlée.

2) Obtenir une assurance sur la conformité des processus des systèmes d'information avec les lois, politiques et normes applicables à l'entité auditée.

3) S'assurer que les ressources informatiques permettent d'atteindre les objectifs de l'organisation de manière efficace et efficiente et que les contrôles généraux et les contrôles d'application pertinents soient efficaces dans la prévention, la détection et la correction des excès, des extravagances et de l'inefficacité dans l'utilisation et la gestion des systèmes informatiques.

4 Les contrôles généraux sont des procédures manuelles ou automatisées qui visent à assurer la confidentialité, l'intégrité et la disponibilité de l'information dans l'environnement physique où les systèmes d'information sont développés, gérés et exploités.

5 Les contrôles d'application sont des procédures manuelles ou automatisées tributaires de la TI au sein d'un système d'information qui a une incidence sur le traitement des transactions. Ils peuvent concerner la validation des données d'entrée, le traitement précis des données, la diffusion des données de sortie et les contrôles liés à l'intégrité des données de base.

5.3 Sur la base de l'évaluation des risques, la délimitation de la vérification d'un audit des systèmes d'information peut être défini à partir de l'un ou l'ensemble des domaines[6] suivants de l'entité auditée :

1) Politique de l'organisation en matière de TI[7]
2) Structures de gouvernance de l'organisation en matière de TI
3) Contrôles généraux effectués dans le domaine d'activité en cours d'automatisation
4) Gestion d'actifs
5) Développement, acquisition et maintenance des systèmes d'information, y compris la modélisation des processus d'affaires et la logique de programmation associée
6) Gestion des opérations informatiques
7) Gestion de l'environnement physique
8) Gestion des ressources humaines
9) Gestion des communications
10) Gestion de la sécurité de l'information[8]
11) Gestion de la conformité réglementaire
12) Gestion de la continuité des opérations et de la reprise après sinistre
13) Gestion des contrôles d'applications

5.4 Les ISC peuvent choisir la période d'analyse de l'audit (par exemple un an, trois ans, etc.) pour définir le cadre de la mission d'audit des systèmes de l'information. Une période appropriée peut être choisie en fonction des objectifs définis pour la mission d'audit.

5.5 Lorsqu'un audit des systèmes de l'information fait partie d'une mission d'audit, l'ISC peut s'assurer que l'équipe d'audit dans son ensemble travaille de manière intégrée pour atteindre l'objectif global d'audit. Pour parvenir à une intégration efficace, les ISC peuvent envisager :

1) Documentation complète du travail à effectuer par les auditeurs des systèmes d'information.
2) Élaborer un protocole d'échange d'informations entre les auditeurs des

6 Une majorité des domaines décrits ont été adaptés d'ISO/IEC 27001.
7 Y compris les aspects de la gestion stratégique
8 Y compris la cybersécurité

systèmes d'information et les autres auditeurs ;

3) Déterminer les systèmes d'information et les objectifs de contrôle qui entrent dans le cadre de la vérification ;

5.6 Les ISC peuvent s'assurer que l'équipe d'audit est composée de membres qui, collectivement, ont la compétence nécessaire pour mener à bien des missions d'audit des systèmes d'information en vue d'atteindre les objectifs d'audit prévus.

5.7 Les connaissances, aptitudes et compétences nécessaires peuvent être acquises par une combinaison de formation, de recrutement et d'engagement de ressources externes, conformément au plan stratégique de l'ISC.

5.8 Les ISC peuvent s'assurer que les équipes d'audit du systèmes d'information aient collectivement la capacité de

1) comprendre les éléments techniques d'un système d'information axé sur les TI, y compris toutes les instances pertinentes de l'application utilisée, afin de pouvoir accéder à l'infrastructure des TI et l'utiliser pour le processus d'audit.
2) Comprendre les règles, les réglementations et l'environnement existants dans lesquels les systèmes d'information de l'entité auditée axés sur les TI, fonctionnement.
3) Comprendre la modélisation des processus d'affaires dans la logique de programmation du système d'information de l'entité auditée
4) Appliquer à la fois les connaissances opérationnelles et informatiques pour évaluer le risque d'annulation manuelle d'un programme ou d'une configuration de système qui permettrait un traitement exceptionnel des transactions.
5) Évaluer la conception et tester l'efficacité opérationnelle des contrôles d'application dans les systèmes d'information pertinents.
6) Comprendre la méthodologie de contrôle, notamment les normes et lignes directrices de contrôle pertinentes applicables à l'ISC.
7) Comprendre les critères de performance/conformité informatique auxquels les résultats de l'audit doivent être comparés, notamment les

cadres de gestion des systèmes d'information, tels que COBIT, ITIL, TOGAF.

8) Comprendre les techniques des systèmes d'information pour pour recueillir des preuves d'audit à partir de systèmes automatisés

9) Comprendre les outils d'audit des systèmes d'information pour collecter, analyser et reproduire les résultats d'une telle analyse ou réexécuter les fonctions auditées.

10) Accéder à l'infrastructure des systèmes d'information et l'utiliser pour receuillir et conserver les éléments probants de la vérification

11) Accéder aux outils d'audit des systèmes d'information et les utiliser pour analyser les éléments probants recueillis.

5.9 Les ISC peuvent envisager différentes options pour affecter des ressources humaines dans le cadre des missions d'audit des systèmes d'information. Il pourrait s'agir de créer un groupe central composé de spécialistes en TI qui aideraient d'autres équipes d'audit de l'ISC à réaliser ces audits ou à déployer des spécialistes en TI selon les besoins. Au fur et à mesure que le nombre de missions d'audit des systèmes d'information menées augmente, les ISC peuvent envisager de créer un groupe ou une fonction spécifique d'audit des systèmes d'information. Ce groupe peut se voir confier la responsabilité de mener toutes les missions d'audit des systèmes d'information (SI) pour le compte de l'ISC et interagir avec d'autres équipes de l'ISC qui ont une connaissance historique de l'entité contrôlée, afin de comprendre rapidement les fonctions de l'entité et les processus opérationnels connexes. Au fur et à mesure que la technologie s'intègre dans les systèmes d'information, les ISC peuvent s'assurer que tous les auditeurs acquièrent des compétences appropriées en matière d'audit informatique.

5.10 Les ISC peuvent faire appel à des ressources externes telles que des consultants en TI, des entrepreneurs, des spécialistes et des experts pour effectuer un audit des systèmes d'information, en cas de ressources limitées. Les ISC peuvent veiller à ce que ces ressources externes soient correctement formées et sensibilisées aux directives de déontologie et aux processus et produits de l'audit du des systèmes d'information applicables à l'ISC, et à ce que leurs travaux fassent l'objet d'un suivi adéquat au moyen d'un contrat documenté ou d'un accord de niveau de service et de la participation appropriée du personnel des ISC aux étapes de la planification, de la réalisation, de la production des rapports et du suivi de

l'audit. Conséquemment, les ISC peuvent avoir besoin de membres de l'équipe compétents et bien informés à l'interne pour surveiller les travaux des ressources externes et faire respecter les directives et les accords de niveau de service.

5.11 Pour procéder à l'évaluation des risques dans le cadre des missions d'audit des SI, les auditeurs peuvent appliquer les principes énoncés dans les ISSAI 100, 200, 300 et 400, en plus de ceux utilisés pour la réalisation d'objet spécifique de l'Audit des SI, comme indiqué ci-dessous :

1) La probabilité selon laquelle certaines caractéristiques des systèmes d'information d'une entité auditée axés sur les TI puissent, de par leur nature même, avoir une incidence défavorable sur l'exécution de la fonction que l'entité doit remplir représenterait un risque inhérent. Par exemple, un système d'information d'une entité auditée qui est tenu de mettre des informations à la disposition de tous les membres du public comporte le risque inhérent de performance dû au fait qu'au-delà du nombre maximum d'utilisateurs prévu, le système pourrait ne pas répondre et entrainerait une indisponibilité des informations pour tout utilisateur. Bien que l'entité vérifiée puisse adopter des contrôles pour atténuer les risques inhérents, dans de nombreux cas, elle peut simplement être amenée à tolérer l'existence de tels risques, dans les limites d'un niveau de risque acceptable. Le risque inhérent peut être évalué avant que l'influence du contrôle ou du risque de détection ne soit prise en compte par les auditeurs.

2) La probabilité selon laquelle les contrôles informatiques adoptés par l'entité auditée ne parviennent pas à atténuer l'impact négatif auquel devait répondre leur conception représenterait le risque de contrôle pour un SI. Par exemple, un système d'information d'une entité contrôlée qui est tenu de s'assurer que l'accès aux données confidentielles est réservé au personnel autorisé, peut décider d'exiger la présentation d'un nom d'utilisateur et d'un mot de passe au personnel qui tente d'y avoir accès. Dans cette situation, le risque de contrôle réside dans le fait que le nom d'utilisateur et le mot de passe ne sont pas suffisamment protégés et peuvent être devinés par le personnel non autorisé au moyen de tentatives répétées, ce qui entraîne une perte de confidentialité et des répercussions négatives potentielles sur l'entité. Une entité qui insiste sur l'utilisation

de mots de passe sécurisés et non triviaux comportant une combinaison de lettres, de chiffres et de symboles spéciaux, et qui veille à ce que le système d'information empêche l'accès au nom d'utilisateur au-delà d'un certain nombre de tentatives d'accès ratées aurait un risque de contrôle moindre que celle qui ne comporte pas ces caractéristiques.

3) La probabilité selon laquelle l'auditeur ne détecte pas l'absence, la défaillance ou l'insuffisance des contrôles informatiques adoptés par une entité, qui peuvent avoir un impact potentiellement négatif sur l'entité représenterait le risque de détection.

5.12 Pour effectuer des évaluations fondées sur les risques des systèmes informatiques, les ISC peuvent choisir une méthodologie adaptée à leur objectif. Ces méthodologies peuvent aller de la simple classification du profil de risque de l'environnement informatique de l'entité contrôlée comme élevé, moyen et faible sur la base de la compréhension de l'entité, de son environnement et du jugement professionnel de l'équipe d'audit du SI d'une ISC à des calculs plus complexes et numériques qui quantifient la notation du risque à partir de données objectives recueillies auprès de l'entité contrôlée[9].

5.13 L'importance relative d'une question d'audit de système d'information peut être décidée dans le cadre général permettant de déterminer l'importance relative d'une ISC. La perspective de l'importance relative peut varier en fonction de la nature de la mission d'audit du SI. L'importance relative des audits financiers, des audits de performance et des audits de conformité dans le secteur public, à partir desquels la mission d'audit du SI sera créée, a été décrite dans les ISSAI 100, 200, 300 et 400.[10]

9 Manuel WGITA IDI sur les audits informatiques pour les institutions supérieures de contrôle

10 Principes d'audit financier d'ISSAI 200, Principes d'audit de performance d'ISSAI 300, Principes d'audit de conformité d'ISSAI 400

6 RÉALISATION DE L'AUDIT DES SI

6.1 Les ISC peuvent effectuer des audits des SI conformément au processus décrit pour les missions d'audit financier (ISSAI 200), d'audit de performance (ISSAI 300) et d'audit de conformité (ISSAI 400), selon le cas, en fonction de la nature du mandat.

6.2 Dans le cas particulier d'un audit du SI, les auditeurs peuvent solliciter la coopération et le soutien nécessaires de l'entité auditée pour mener à bien l'audit, notamment en ce qui concerne l'accès aux dossiers et aux informations. Les auditeurs peuvent déterminer le mode d'accès aux données électroniques dans le format nécessaire à l'analyse, en collaboration avec l'entité auditée. Le mode d'accès aux données serait spécifique aux ISC.

6.3 Avant d'entreprendre l'évaluation des contrôles dans un système d'information, les vérificateurs peuvent acquérir une compréhension de l'architecture du système, des données sous-jacentes et de leurs sources afin de déterminer les outils et techniques de vérification requis.

6.4 En cas de réception de vidages[11] de l'entité auditée, les auditeurs peuvent s'assurer que chaque vidage de mémoire est accompagné d'une lettre de l'entité auditée. Cette lettre de transmission peut préciser

1) La source (par référence à l'horodatage de la génération du vidage de mémoire/ du numéro de hachage pour le vidage de mémoire) des

11 Le vidage de mémoire est défini comme une grande quantité de données transférées d'un système ou d'un emplacement à un autre.

données dans le but d'assurer l'intégrité des données, l'authentification[12] et la non-répudiation[13]

2) Les paramètres d'extraction utilisés pour créer le vidage de mémoire, c'est-à-dire les requêtes utilisées/rapports exécutés.

3) Si une telle lettre de transmission de la part de l'entité auditée n'est pas reçue, les auditeurs peuvent produire des documents internes indiquant des informations importantes telles que la date à laquelle les données ont été transmises, à partir de quel fichier le vidage de mémoire a été créé et si les données proviennent de l'environnement de production ou de tout autre environnement, etc.

6.5 Les auditeurs peuvent procéder à une évaluation des contrôles informatiques (contrôles généraux et d'application) adoptés par l'entité auditée, afin d'examiner leur fiabilité et leur adéquation. L'évaluation peut être effectuée grâce à une combinaison appropriée des techniques suivantes : Entretien, questionnaire, observation, révision structurée, organigrammes, saisie et analyse de données, vérification, re-calcul, retraitement et confirmation par une tierce partie. Le cadre de l'évaluation des contrôles informatiques peut comprendre l'examen de ce qui suit :

1) La politique du SI a été définie, adoptée et communiquée

2) La structure de gouvernance du SI est en place et fonctionnelle.

3) L'inventaire des actifs du SI a été effectué périodiquement et les besoins d'augmentation, de remplacement et d'élimination ont été identifiés.

4) Des processus de partage de l'infrastructure et des services communs pour les systèmes d'information avec d'autres entités publiques sont en place et fonctionnels.

5) Les processus de développement, d'acquisition et de maintenance des systèmes d'information ont été définis, adoptés et communiqués (notamment ceux de la gestion du changement).

6) Les processus pour les opérations de TI (internalisation, externalisation, ententes de services) ont été définis, adoptés et communiqués.

12 L'authentification est définie comme l'acte de vérification de l'identité d'un utilisateur - Glossaire des termes de l'ISACA

13 La non-répudiation est définie comme l'assurance qu'une partie ne peut nier ultérieurement les données d'origine ; la fourniture d'une preuve de l'intégrité et de l'origine des données et pouvant être vérifiée par un tiers - Glossaire des termes de l'ISACA

7) Des mesures visant à assurer la sécurité physique et les conditions de travail physiques prévues ont été adoptées.

8) Des mesures de formation et de sensibilisation des ressources humaines visant à garantir la confidentialité, l'intégrité et la disponibilité de l'information, ainsi que le respect des exigences de la politique en matière de SI et de la structure de gouvernance, ont été adoptées

9) Des mesures visant à garantir la confidentialité, l'intégrité et la disponibilité des divers modes et canaux de communication ont été adoptées.

10) Des mesures de gestion de la sécurité de l'information ont été adoptées

11) Des mesures de gestion de la conformité réglementaire ont été adoptées.

12) Des mesures de continuité des opérations et de gestion de la reprise après sinistre ont été adoptées.

13) Les contrôles d'application adoptés dans chaque système d'information sont adéquats et fiables. Une telle évaluation peut comprendre l'identification des composantes importantes de l'application, l'identification du caractère crucial de l'application pour l'entité, l'examen de la documentation disponible, l'entrevue réalisée auprès du personnel, la compréhension des risques liés au contrôle des applications et de leur impact sur l'entité, et l'élaboration de tests pour examiner la pertinence et la fiabilité de ces contrôles des applications.

6.6 L'évaluation des contrôles généraux et d'application peut donc porter sur les politiques, les processus, les personnes et les systèmes de l'entité auditée, conformément aux objectifs de l'audit du SI.

6.7 Selon l'objectif de la vérification, les vérificateurs peuvent s'intéresser à la conception, à la mise en oeuvre et à l'efficacité opérationnelle des contrôles. Lorsque la conception du contrôle est l'objet de l'attention de l'auditeur, un entretien ou une inspection des règles de gestion documentées peut suffire. Lorsque le vérificateur se penche sur la mise en oeuvre des contrôles, l'enquête peut ne pas être suffisante par conséquent une révision structurée ou une analyse des données peut être nécessaire pour confirmer que le contrôle tel que conçu a été mis en oeuvre. Enfin, si l'auditeur s'intéresse à l'efficacité opérationnelle du contrôle, il/elle peut être amené

à tester un échantillon d'opérations pour démontrer que le contrôle a fonctionné efficacement tout au long de la période considérée.

6.8 Les vérificateurs peuvent également examiner comment les éléments probants concernant les contrôles généraux influent sur la nature, le moment et l'étendue des éléments probants requis pour obtenir l'assurance du fonctionnement des contrôles de l'application. Si l'auditeur a obtenu des éléments probants suffisants et appropriés concernant l'efficacité des contrôles généraux à l'appui de l'accès logique du personnel aux systèmes informatiques et à la gestion du changement dans l'environnement de production, il/elle peut être en mesure de conclure de l'efficacité opérationnelle des procédures de contrôle automatisé des applications. Pour ce faire, il est possible de tester un échantillon plus restreint d'opérations, car l'efficacité de l'environnement informatique général fournit à l'auditeur des éléments probants sur l'efficacité du contrôle de l'application au cours de la période concernée. Dans le cas de procédures manuelles de contrôle de l'application, les auditeurs peuvent être amenés à tester un échantillon d'une taille appropriée au niveau de confiance choisi.

6.9 Sur la base de l'évaluation des contrôles informatiques, les auditeurs peuvent identifier des domaines prioritaires pour la réalisation des tests de corroboration, qui comprennent des tests détaillés des contrôles informatiques grâce à diverses techniques d'audit assisté par ordinateur (TAAO) pour la recherche, l'extraction et l'analyse de données. Les vérificateurs peuvent concevoir et exécuter des tests de corroboration afin de corroborer les objectifs de la vérification. Les vérificateurs peuvent choisir les TAAO appropriés en fonction de leurs exigences.

6.10 Les auditeurs peuvent utiliser les TAAO pour mettre en oeuvre des techniques d'audit des SI telles que l'analyse du journal de l'utilisateur, les rapports d'exception, la totalisation par champs, la comparaison de fichiers, la stratification, l'échantillonnage, les contrôles de doublons, la détection des écarts, le vieillissement, les calculs de champs virtuels, etc. Les avantages de l'utilisation des TAAO comprennent l'analyse de grands volumes de données, la répétabilité des tests sur différents ensembles de données et avec différents critères et la documentation automatisée des tests d'audit et des résultats avec horodatage.

6.11 Les auditeurs peuvent ne pas toujours être en mesure d'examiner toutes les cas, transactions, modules ou systèmes informatiques, compte tenu des contraintes

de ressources et des compromis coûts-avantages de l'audit. Dans une telle situation, les ISC peuvent, sur la base de considérations d'importance relative, procéder à un examen détaillé par échantillonnage afin de tirer des conclusions de contrôle raisonnables. Les ISC peuvent utiliser les TAAO appropriées pour effectuer différents types d'échantillonnage et déterminer la taille appropriée de l'échantillon, en fonction des risques de contrôle inhérents et sous-jacents. Des échantillons d'audit[14] sont prélevés afin de fournir à l'auditeur une base raisonnable lui permettant de tirer des conclusions sur l'ensemble de la population de données, sur la base des conclusions tirées de l'application des procédures d'audit et de l'analyse de l'échantillon. Les auditeurs peuvent prendre en considération le but de la procédure d'audit et les caractéristiques de la population dans laquelle l'échantillon sera prélevé, et déterminer une taille d'échantillon suffisante pour réduire le risque d'échantillonnage à un niveau acceptable. L'audit dans un environnement informatique peut faciliter l'analyse de 100% d'une population, en particulier au stade de l'évaluation préliminaire. Toutefois, des échantillons peuvent être nécessaires pour effectuer des tests de corroboration. Lorsqu'ils effectuent un échantillonnage dans le cadre d'un audit financier, les auditeurs des SI peuvent appliquer la norme ISSAI 2530 pour la sélection des échantillons.[15]

6.12 Les vérificateurs peuvent s'assurer que les éléments probants électroniques recueillis et documentés sont suffisants, fiables et exacts pour étayer leurs observations. Ces éléments probants électroniques peuvent être constitués de fichiers de données, des journaux d'utilisateurs, des modèles analytiques, des rapports sur les systèmes d'information de gestion, etc. et peuvent être recueillis et conservés de façon appropriée afin d'être disponibles pour garantir l'exactitude et la validité du processus d'audit. Les éléments probants recueillis au cours d'un audit des SI peuvent nécessiter des horodatages et des détails contenant les étapes de l'analyse des données effectuée, de sorte que l'on sache quand les éléments probants ont été créés, stockés et modifiés pour la dernière fois, afin de réduire le risque de modifications ultérieures.

6.13 La documentation relative à l'audit des SI peut être conservée et protégée contre toute modification ou suppression non autorisée. Les ISC peuvent élaborer de nouvelles normes pour la conservation de la documentation relative à l'audit des SI ou adapter les normes existantes pour répondre aux exigences de conservation de

14 ISSAI 2530, Audit financier, Audit par échantillonnage, sections 6 à 9.

15 ISSAI 2530, Audit financier, échantillonnage aux fins de la vérification, sections 6 à 9.

la documentation relative à l'audit des SI. La durée de conservation ainsi déterminée dépendrait du mandat de chaque ISC et du ou des statuts régissant ses activités. Une attention particulière peut être accordée aux supports, au format, à la durée de vie et aux exigences de stockage de ces données, afin de garantir leur lisibilité dans les délais définis dans la politique de conservation et d'archivage des données de chaque ISC. Cela peut nécessiter la conversion de données d'un format à un autre pour suivre le rythme des avancées technologiques et l'obsolescence.

6.14 En cas d'examen de rapports techniques préparés par des auditeurs tiers sur des sujets technologiques spécifiques, les auditeurs peuvent adopter des procédures appropriées pour vérifier la conformité, les aspects financiers ou de performance de ces rapports.[16] Si, à la suite de ces procédures, on se fie au contenu de ces rapports, l'objet de cette confiance peut être divulgué de façon appropriée.

6.15 Les ISSAI prévoient que les auditeurs doivent établir une communication efficace tout au long du processus d'audit et tenir l'entité auditée informée de toutes les questions relatives à l'audit (voir ISSAI 100 paragraphe 43). Dans les audits impliquant des travaux d'audit des SI, le résultat de l'audit des SI peut, dans certains cas, être communiqué à l'entité par le biais d'une lettre distincte. Dans ces cas, il peut être important d'expliquer en quoi le résultat des travaux d'audit est lié à d'autres communications qui font partie du même audit financier, de performance ou de conformité et en quoi les résultats des travaux d'audit des SI peuvent être pertinents pour le rapport d'audit de l'ISC qui en résultera.

16 Lorsque le champ d'application relève de l'audit financier, les auditeurs peuvent utiliser la norme ISSAI 2402, Considérations liées à la vérification relatives à une entité faisant appel à un organisme de service

7 RAPPORT SUR L'AUDIT DES SI

7.1 Étant donné qu'une mission d'audit des SI peut être soit un audit financier (ISSAI 200), soit un audit de performance (ISSAI 300), soit un audit de conformité (ISSAI 400), les auditeurs peuvent considérer les exigences en matière de rapport en conséquence. Cela serait donc propre à chaque ISC. De même, chaque ISC peut avoir ses propres seuils de déclaration en fonction de l'importance relative des résultats des contrôles. En outre, un auditeur, lorsqu'il rend compte d'une mission d'audit des SI, il peut tenir compte des limitations légales et internes à la divulgation d'informations financières et techniques.

7.2 Les vérificateurs peuvent être conscients de la nécessité de limiter l'utilisation du jargon technique et de la sensibilité de l'information présentée dans le rapport (p. ex. mots de passe, noms d'utilisateur, identifiants et renseignements personnels). Nonobstant la nature technique d'un audit des SI, les auditeurs peuvent veiller à ce que le rapport soit parfaitement compréhensible par la haute direction de l'entité auditée, les parties prenantes et le grand public. Les auditeurs peuvent incorporer un glossaire de termes bien détaillé dans les rapports, qui renvoie à la définition d'un acronyme ou d'un terme avec une explication fondée sur un scénario de la façon dont cela fonctionne dans un environnement contrôlé.

7.3 Les auditeurs peuvent considérer l'impact négatif potentiel du rapport dès que le rapport d'audit des SI est publié. Par exemple, si le rapport d'audit des SI détecte certains risques de sécurité dans le système d'information d'une entité auditée et que ces risques sont signalés avant que les contrôles nécessaires pour atténuer les risques n'aient été adoptés, la vulnérabilité

du système d'information peut être exposée au public. Dans un tel scénario, les auditeurs peuvent envisager des options telles que de ne rendre compte qu'après l'adoption des contrôles nécessaires, ou de ne pas communiquer intégralement le risque de sécurité précis, afin d'éviter tout impact négatif potentiel sur l'entité contrôlée.

8 SUIVI

8.1 Dans la mesure où une mission d'audit sur les systèmes d'information provient d'un ou de plusieurs des principaux types d'audits, les auditeurs peuvent considérer que les exigences de suivi relatives à ces missions d'audit sont équivalentes à celles d'audit financier (ISSAI 200), d'audit de performance (ISSAI). 300) et audit de conformité (ISSAI 400).