GUID 5101

Orientations sur l'audit de la sécurité de l'information

INTOSAI

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.orgnal

1) Approuvé en 2025

GUID 5101 est disponible dans toutes les langues officielles de l´INTOSAI: arabe, anglais, français, allemand et espagnol.

TABLE DE MATIÈRES

1

INTRODUCTION

1) Le GUID 5101 complète le GUID 5100 par des orientations sur l'audit de la sécurité de l'information. Les orientations énoncées dans le présent GUID sont conformes aux principes fondamentaux du contrôle des finances publiques (ISSAI 100) et aux principes de l'audit de conformité (ISSAI 400).

2) Étant donné que les entités auditées du secteur public connaissent une transition vers des systèmes d'information informatisés et vers le traitement électronique de l'information, il est impératif que les ISC se dotent des capacités appropriées pour auditer les contrôles liés aux systèmes d'information. Dans le cadre des audits relatifs à ceux-ci, il faut veiller à ce que les entités auditées conçoivent et appliquent des contrôles pour préserver la confidentialité, l'intégrité et la disponibilité de ces systèmes et des données (c'est-à-dire la sécurité de l'information).

3) Les violations de la sécurité de l'information peuvent entraîner des préjudices considérables sur les plans juridique et financier, donner lieu à des atteintes graves à la réputation/crédibilité ainsi qu'à la productivité, et exposer à des intrusions ultérieures. Ces violations de la sécurité peuvent résulter de faiblesses et de vulnérabilités à l'origine d'une exposition accidentelle, de la divulgation d'informations à des parties non autorisées, d'une perte de disponibilité ou de modifications non autorisées des systèmes et des données.

2 OBJECTIFS DU PRÉSENT GUID

4) Les orientations applicables à l'audit des systèmes d'information sont énoncées dans le GUID 5100. L'objectif du présent GUID est de fournir des orientations spécifiques et supplémentaires en vue de la réalisation d'un audit de conformité portant sur la sécurité de l'information.

5) L'audit de la sécurité de l'information peut prendre la forme d'un audit de conformité ou, dans certaines circonstances, d'un audit combinant des aspects de l'audit financier, de l'audit de conformité et/ou de l'audit de la performance. Le présent GUID porte sur les audits de la sécurité de l'information réalisés sous la forme d'un audit de conformité distinct ou dans le cadre d'une mission d'audit combinée, dans le but d'examiner si la gestion des technologies de l'information est conforme aux normes et exigences nécessaires en matière de sécurité de l'information.

6) Les auditeurs peuvent mettre en application le contenu du présent GUID lors des étapes du processus d'audit que sont la planification, la réalisation, l'établissement du rapport et le suivi. Le GUID énumère des sujets potentiels de travaux d'audit, des facteurs de risque auxquels la sécurité de l'information est exposée, des sources de critères d'audit et des questions d'audit de haut niveau. Ces listes sont indicatives et non exhaustives.

3

DÉFINITIONS

a) **Sécurité de l'information:** protection de l'information et des systèmes d'information contre l'accès, l'utilisation, la divulgation, la perturbation, la modification ou la destruction non autorisés, afin d'assurer leur confidentialité, leur intégrité et leur disponibilité.

b) **Cybersécurité :** prévention de tout dommage aux ordinateurs, aux systèmes de communication électronique, aux services de communication électronique, aux communications par fil, aux communications électroniques, y compris les données qui y sont incluses, ainsi que la protection et la restauration de ces éléments afin d'assurer leur disponibilité, leur intégrité et leur confidentialité.

c) **Confidentialité :** préservation des restrictions autorisées en matière d'accès à l'information et de divulgation de celle-ci, y compris les moyens de protéger la vie privée et les informations exclusives. Ce terme peut aussi désigner la protection des informations sensibles contre la divulgation non autorisée. Une perte de confidentialité désigne la divulgation non autorisée d'une information.

d) **Intégrité :** protection contre la modification ou la destruction inappropriée de l'information. Elle consiste entre autres à assurer la non-répudiation[1] et l'authenticité[2] de l'information. Ce terme peut aussi désigner l'exactitude et l'exhaustivité de l'information, ainsi que sa validité en fonction des valeurs et attentes de l'entité. Une perte d'intégrité désigne la modification ou la destruction inappropriée de l'information.

---

1 La non-répudiation correspond à la protection contre un individu qui nie de façon mensongère avoir effectué une certaine action, ainsi qu'à la capacité de déterminer si un individu a réalisé une certaine action, telle que la création d'une information, l'envoi d'un message, l'approbation d'une information ou la réception d'un message.

2 L'authenticité désigne le fait d'être authentique, vérifiable et fiable, ainsi que la confiance dans la validité d'une transmission ou d'un message ou dans l'expéditeur d'un message.

e) **Disponibilité :** fait, pour des utilisateurs autorisés, de disposer d'un accès rapide et fiable à une information ou à un système d'information, ainsi que de les utiliser. Ce terme désigne aussi le fait qu'une information soit disponible à présent et à l'avenir lorsque le processus l'exige, ainsi que la protection des ressources nécessaires et des capacités connexes. Une perte de disponibilité désigne l'interruption de l'accès à une information ou à un système d'information, ou de leur utilisation.

f) **Évaluation des vulnérabilités/Tests d'intrusion:** une évaluation des vulnérabilités sert à détecter les problèmes de sécurité dans les applications informatiques, les postes de travail ou l'ensemble du réseau de l'organisation, de façon systématique et organisée. Cette évaluation permet aux auditeurs de cataloguer, de hiérarchiser et de classer les vulnérabilités en matière de sécurité en fonction des niveaux de risque en vue d'y remédier en temps opportun. Les tests d'intrusion sont semblables au piratage éthique et consistent en la réalisation d'une simulation autorisée de piratage ou d'attaque contre un système informatique, en vue d'en évaluer la sécurité.

4

LE SUJET CONSIDÉRÉ

7) Lors d'un audit portant sur la sécurité de l'information, l'auditeur évalue la conformité du sujet considéré (à savoir, la sécurité de l'information ou tout aspect/élément spécifique de celle-ci) aux textes législatifs et réglementaires applicables (par exemple des lois, des règlements, une politique, une procédure, des normes ou des pratiques).

8) Les travaux d'audit sur la sécurité de l'information seront déterminés en fonction des objectifs et de l'étendue de l'audit. Cette dernière peut englober différents sujets tels que:

a) la culture en matière de sécurité de l'information, y compris l'impulsion et l'engagement; l'orientation et les politiques concernant la gestion; les objectifs visés par la sécurité de l'information; les rôles, responsabilités et autorités au sein de l'organisation (dont ceux relatifs au travail mobile et au télétravail, par exemple);

b) les processus de gestion des risques pour la sécurité de l'information, qui couvrent:

   i. l'évaluation des risques pour la sécurité de l'information (y compris les seuils et critères d'acceptation de ces risques, leur détection, leur analyse et leur hiérarchisation), ainsi que le traitement de ces risques;

   ii. la communication (interne et externe) et la documentation pertinentes pour le système de gestion de la sécurité de l'information;

   iii. le réexamen et l'amélioration continue de la sécurité de l'information et de la gestion des risques;.

c) la sécurité de l'information dans les relations avec les fournisseurs;

d) la sécurité des ressources humaines à différentes étapes, à savoir avant l'embauche, pendant la durée du contrat de travail et après la cessation des fonctions;

e) la gestion et le contrôle des actifs informationnels, y compris leur inventaire et leur classement; les règles pour une utilisation acceptable; le transport, la restitution et la mise au rebut de ces actifs;

f) les contrôles d'authentification, d'autorisation et d'accès, y compris la détermination des contrôles de gestion et des contrôles cryptographiques;

g) la sécurité physique et environnementale;

h) la sécurité du réseau et des communications, ainsi que la gestion de la cybersécurité;

i) la gestion des incidents liés à la sécurité de l'information ainsi que les tests et le suivi en matière de sécurité;

j) la sécurité dans le cadre de l'acquisition et du développement de systèmes;

k) la sécurité des opérations, y compris les procédures et responsabilités opérationnelles; la protection contre les maliciels; la sauvegarde/récupération des données, ainsi que la journalisation et le suivi;

l) la conformité aux exigences externes et internes;

m) les lois nouvelles ou modifiées.

5

PLANIFICATION D'UN AUDIT PORTANT SUR LA SÉCURITÉ DE L'INFORMATION

9) Un audit de la sécurité de l'information peut être lancé à la suite d'une évaluation des risques. Quelques facteurs de risque pertinents sont présentés ci-après:

a) L'entité auditée a développé un nouveau système d'information, ou elle a remplacé ou mis à niveau un système d'information existant (une application et/ou une infrastructure), notamment dans un domaine d'activité essentiel;

b) Un système d'information ancien et historique n'a pas été mis à niveau ou remplacé, alors que l'infrastructure technologique sous-jacente est obsolète et n'est actuellement plus supportée par les correctifs/mises à jour de sécurité;

c) Des tests de sécurité internes/externes périodiques n'ont pas été réalisés, y compris concernant les systèmes d'information opérationnels, notamment ceux pour lesquels d'importantes mises à niveau des applications ou des infrastructures ont eu lieu;

d) Un post mortem a été établi concernant un incident ou une violation majeur(e) en matière de sécurité avec des répercussions négatives sur le système d'information concerné; ou un incident ou une violation en matière de sécurité a eu des répercussions négatives sur des systèmes d'information mis en place de façon analogue dans d'autres entités auditées;

e) Des préoccupations en matière de protection des données et de vie privée sont apparues concernant les systèmes informatiques existants ainsi que la nécessité d'une mise à niveau/à jour pour se conformer aux dernières lois applicables;

f) D'autres audits (internes ou externes/réalisés par une ISC) ont permis de détecter d'importantes menaces pour la sécurité de l'information dans l'environnement ou des risques pour la sécurité de l'information concernant le système d'information de l'entité auditée; ou des faiblesses dans les évaluations, les appréciations ou les contrôles, détectées lors d'audits précédents de la sécurité de l'information, n'ont été traitées que partiellement, voire pas du tout.

g) D'importants changements ont été apportés aux politiques et structures mises en place dans l'organisation pour gérer la mise en œuvre des systèmes d'information, y compris la sécurité de l'information.

10) S'il utilise une approche d'audit fondée sur les risques, l'auditeur peut apprécier le processus de gestion des risques mis en place par l'entité auditée (entre autres pour détecter, évaluer et traiter les risques) et tenir compte d'audits ou d'évaluations internes ou externes précédent(e)s dans le cadre de la détection et de l'évaluation des risques.

11) L'auditeur peut examiner si des politiques et procédures pertinentes sont disponibles et réexaminées à intervalles appropriés, puis actualisées au besoin, tout en évaluant les rôles organisationnels. L'auditeur peut aussi chercher à déterminer si la sensibilisation et la compréhension des utilisateurs, y compris leur culture en matière de sécurité de l'information, sont appropriées.

12) L'importance relative d'une question d'audit sur la sécurité de l'information peut être décidée dans le cadre général mis en place par l'ISC en matière d'importance relative, ainsi qu'à la lumière des orientations spécifiques concernant l'importance relative dans le cas des audits portant sur les systèmes d'information.

5.1 Sources des critères d'audit

13) L'auditeur peut utiliser des cadres reconnus au niveau national ou international en matière de sécurité de l'information comme sources pour les critères d'audit.

14) Les cadres qui servent de sources pour les critères d'audit peuvent comporter des normes telles que la suite ISO/CIE 27000, le cadre COBIT établi/actualisé par l'ISACA, les normes et cadres relatifs à l'information et à la cybersécurité établis par l'Institut national des normes et des technologies des États-Unis, ainsi que les mesures de contrôle prises par les centres pour la sécurité informatique. Parmi les cadres et normes davantage ciblés/spécifiques à un secteur figurent entre autres le règlement général sur la protection des données (RGPD) de l'Union européenne, la norme de sécurité des données de l'industrie des cartes de paiement, ainsi que la loi des États-Unis relative à la portabilité et à la responsabilisation en matière d'assurance-maladie pour le secteur des soins de santé.

15) Le choix des critères d'audit par l'auditeur peut dépendre:
- du contexte spécifique dans lequel évoluent l'ISC et le pays (y compris les exigences légales et réglementaires, le cas échéant);
- de l'entité/des entités auditée(s) concernée(s);
- de l'étendue de l'audit.

5.2 Ressources

16) Les considérations sur l'affectation de ressources humaines aux missions d'audit sur les systèmes d'information (y compris sur la sécurité de l'information) sont énoncées dans le GUID 5100 et s'appliquent globalement aux audits de la sécurité de l'information. Il convient en outre de noter que les autorités compétentes peuvent imposer aux auditeurs un processus de sélection spécial s'ils traitent des informations sensibles et confidentielles.

6

RÉALISATION D'UN AUDIT PORTANT SUR LA SÉCURITÉ DE L'INFORMATION

6.1 Objectif des procédures d'audit [3]

17) Pour un audit de la sécurité de l'information, les procédures d'audit seront conçues pour axer ce dernier sur l'évaluation des éléments suivants: a) la confidentialité, b) l'intégrité, y compris la non-répudiation et c) la disponibilité des données et des systèmes informatiques relevant du champ d'application de la mission d'audit.

6.2 Procédures d'audit destinées à collecter des éléments probants

18) Les procédures d'audit peuvent inclure une combinaison des éléments suivants: a) examen de la documentation; b) observation, inspections, entretiens et questionnaires; c) analyse des données électroniques, par exemple concernant les journaux d'audit de différents types; d) évaluation des vulnérabilités/tests d'intrusion. Si l'auditeur doit réaliser une évaluation des vulnérabilités/des tests d'intrusion, il se peut qu'une entente et un accord, comprenant des garanties juridiques et des indemnisations le cas échéant, doivent être conclus avec l'entité auditée en vue de la réalisation de tels tests d'intrusion. Si un tiers a réalisé une évaluation des vulnérabilités/des tests d'intrusion, les éléments probants peuvent en inclure les résultats. En l'occurrence, l'auditeur doit acquérir une compréhension suffisante de l'étendue de l'évaluation des vulnérabilités/des tests d'intrusion, ainsi que des constatations et de leurs implications.

19) Pour évaluer la sécurité physique et environnementale, l'auditeur peut envisager une visite physique (ou une inspection commune) des centres de données en guise de procédure d'audit qui s'ajouterait au contrôle

[3] L'annexe présente des questions d'audit de haut niveau à titre d'exemples.

documentaire, aux entretiens, etc.

20) L'auditeur peut évaluer le caractère approprié des normes, lignes directrices et procédures conçues pour concrétiser la politique en matière de sécurité de l'information et les politiques relatives au signalement et à la gestion des incidents/problèmes.

21) L'audit relatif au processus de gestion des risques peut comporter l'examen de la fréquence des analyses périodiques des risques ainsi que du caractère approprié des mesures de suivi prises pour atténuer les risques détectés et évalués. La décision sur les seuils d'acceptation des risques (et l'acceptation des risques résiduels qui en résulte) relève(nt) de la compétence de la direction.

22) Les politiques relatives au recensement, au classement et au contrôle des actifs informationnels sont liées au processus de gestion des risques (notamment à leur détection et à leur évaluation). Les procédures d'audit peuvent consister à examiner si les utilisateurs comprennent les politiques et si ces dernières sont mises en œuvre de façon efficace.

23) Les procédures d'audit relatives aux contrôles d'authentification, d'autorisation et d'accès peuvent consister à examiner si une authentification multifactorielle (qui s'ajoute généralement à l'authentification fondée sur un mot de passe) est mise en œuvre et si cela est requis ou préconisé par la politique ou le contrat en vigueur.

24) Lorsqu'il faut examiner les journaux pour déterminer si un contrôle d'accès a été mis en œuvre comme prévu, une telle analyse des journaux peut comporter la réception de données transférées ou extraites. Lorsqu'il reçoit des données transférées en provenance de l'entité auditée en vue d'une analyse électronique, l'auditeur peut envisager de demander une lettre, comme cela est indiqué au paragraphe 6.4 du GUID 5100, en vue d'en assurer l'authenticité, y compris l'intégrité et la non-répudiation.

25) Pour auditer la gestion des incidents en matière de sécurité de l'information, l'auditeur peut envisager de demander à un échantillon d'utilisateurs (qui ont détecté des incidents et leur ont attribué un ticket) si la résolution a été appropriée. Cette démarche s'ajoute à l'examen des processus et de la documentation en matière de détection, de journalisation, d'évaluation et de résolution des incidents.

26) Un audit de la sécurité de l'information peut comporter une évaluation de la planification et de la mise en œuvre de la continuité des activités et du rétablissement après sinistre, afin d'apprécier le volet «disponibilité» des services d'information ainsi que la sécurité de l'information pendant la période de rétablissement après sinistre. Sinon, ces aspects peuvent être couverts dans le cadre d'un audit portant sur la gestion des opérations des systèmes d'information.

6.3 Considérations relatives aux modalités d'externalisation

27) En ce qui concerne la sécurité de l'information dans les relations avec les fournisseurs/prestataires externes, l'entité auditée reste tenue de rendre compte de la sécurité de l'information, même si la responsabilité pour certaines activités des systèmes d'information est confiée à un fournisseur externe. En outre, des aspects tels que la séparation des fonctions incompatibles (par exemple entre les équipes chargées du développement, des tests et de la production) sont importants, selon que le développement, la mise en œuvre, les opérations et la maintenance du système d'information sont assurés en interne ou par l'intermédiaire d'un fournisseur externe.

7

ÉTABLISSEMENT D'UN RAPPORT SUR UN AUDIT DE LA SÉCURITÉ DE L'INFORMATION

28) Lors d'un audit portant sur la sécurité de l'information, l'auditeur peut suivre les orientations sur l'évaluation des éléments probants et sur l'établissement de rapports présentées dans l'ISSAI 400, ainsi que les orientations supplémentaires sur l'établissement de rapports présentées dans le GUID 5100 (en sa section 7, qui fait aussi référence au caractère sensible des informations communiquées sur les risques en matière de sécurité de l'information avant la mise en œuvre des contrôles nécessaires destinés à les atténuer).

29) Lors de l'établissement d'un rapport sur la sécurité de l'information, l'auditeur peut tenir compte de l'impact que la révélation au public de lacunes techniques et de risques en matière de sécurité pourrait avoir sur les activités de l'entité. En l'occurrence, il peut recourir à des mécanismes appropriés, y compris l'occultation des informations sensibles ou des lettres de recommandations pour communiquer des détails et l'impact potentiel du risque pour l'entité auditée.

30) Lors de l'établissement du rapport, l'auditeur peut tenir compte des points de vue des parties prenantes habituelles des audits du secteur public, mais aussi des éclairages spécifiques d'autres parties prenantes, telles que les fournisseurs de services techniques de soutien externalisés aux entités auditées.

31) L'auditeur peut formuler des recommandations en vue d'améliorer la sécurité de l'information. Lors de leur élaboration, il peut tenir compte de toutes les implications d'ordre pratique pour l'entité auditée, y compris du coût de leur mise en œuvre.

8

SUIVI

32) L’auditeur envisage le suivi conformément aux principes de l’audit de conformité énoncés dans l’ISSAI 400.

33) Les systèmes informatiques ne cessent d’évoluer. À titre d’exemple, ils sont de plus en plus souvent fondés sur l’internet et hébergés en nuage. L’auditeur peut envisager de tenir compte de ces changements importants lorsqu’il arrêtera le calendrier des audits de suivi.

34) Lorsqu’il planifie un suivi, l’auditeur peut prendre en considération des facteurs tels que la technologie disponible, le coût, la compatibilité des systèmes, qui sont susceptibles d’avoir un impact sur la capacité de l’entité auditée à donner suite aux constatations d’audit et à mettre en œuvre les recommandations.

ANNEXE

Suggestions de questions d'audit de haut niveau

L'annexe comporte des questions d'audit de haut niveau en lien avec l'audit de la sécurité de l'information. Cette liste n'est pas exhaustive, doit servir d'orientation et est présentée seulement à titre indicatif. La pertinence des éléments repris dans ce tableau dépendra des éventuelles obligations imposées à l'entité auditée, par la législation ou d'autres voies, de respecter les critères énoncés dans les objectifs. Les questionnaires d'audit détaillés seront fonction, entre autres, du type de système d'information, de l'organisation, du cadre et de l'étendue de l'activité d'audit.

N°	Domaine de la sécurité de l'information	Objectif	Observations
1	Politique en matière de sécurité de l'information	Déterminer si une telle politique est définie, adoptée et communiquée.	Cette politique doit aussi être réexaminée à intervalles réguliers.
2	Structure organisationnelle en matière de sécurité de l'information	Déterminer si la responsabilité en matière de sécurité de l'information a été clairement attribuée à une telle structure de gouvernance.	Les auditeurs peuvent examiner la clarté des définitions, de la structure organisationnelle, de la composition et du mandat.
		Déterminer si les responsabilités du personnel dans le cadre de cette structure de gouvernance, les rôles individuels et le mécanisme de communication d'informations ont été définis.	Au sein de l'organisation, il faut qu'il existe une séparation des fonctions, avec des rôles et responsabilités distincts pour chaque emploi, avec une hiérarchie pour la transmission d'informations en vue du signalement des problèmes.
		Déterminer si les aspects de sécurité relatifs aux ressources humaines impliquées dans les systèmes d'information ont été traités.	Les contrôles en lien avec les ressources humaines devraient être exercés à toutes les étapes de la gestion de celles-ci.
		Déterminer si l'organisation favorise une culture de la sécurité de l'information auprès du personnel à tous les niveaux.	La culture de l'organisation joue un rôle important dans la détermination du niveau de sécurité de l'information en son sein.
3	Gestion des actifs informationnels	Déterminer si les actifs des systèmes d'information font l'objet d'un inventaire régulier et si les exigences en matière de sécurité sont définies pour chaque type d'actif.	Les actifs informationnels devraient être classés, étiquetés et gérés de façon appropriée.
4	Développement, acquisition et maintenance des systèmes d'information	Déterminer si les aspects liés à la sécurité ont été définis, adoptés et communiqués pour chacun de ces processus.	La sécurité de l'information doit être un élément fondamental pendant toute la durée du cycle de vie des systèmes d'information.
		Déterminer si la sécurité de l'information est assurée par les vendeurs dans toutes les interactions.	En fonction des risques, vérifier si l'entité auditée a fait examiner, par des ressources qualifiées internes ou externes, le code et les modules du système d'information développé/acquis afin de s'assurer qu'il n'existe aucune fonctionnalité cachée susceptible de compromettre la confidentialité, l'intégrité et la

			disponibilité des données.
5	Opérations informatiques	Déterminer si la sécurité des opérations informatiques a été définie, adoptée et communiquée.	Examiner les contrats/accords de niveau de service passés avec les parties auxquelles des opérations informatiques sont externalisées, afin de vérifier l'inscription de clauses de non-divulgation, de non-concurrence, de non-modification sans autorisation et de non-transmission ainsi que d'autres clauses standard destinées à assurer la confidentialité, l'intégrité et la disponibilité des données.
6	Sécurité physique et environnementale	Déterminer si la sécurité de l'environnement physique du système d'information est assurée.	Vérifier la mise en place d'obstacles physiques (grilles extérieures, portes intérieures et agents de sécurité) qui nécessitent l'identification des membres du personnel et limitent aux seules personnes autorisées l'accès au matériel de stockage, tel que les serveurs. La gestion des installations est un aspect important de l'ensemble de l'écosystème de la sécurité.
7	Sécurité des réseaux et des communications	Déterminer si la sécurité de l'information est assurée lors des communications.	Vérifier si les canaux de communication assurent le cryptage de messages, afin d'éviter leur interception par des tiers et la perte de confidentialité; vérifier également les contrôles cryptographiques pour les communications numériques de nature formelle.
		Déterminer si l'architecture de sécurité du réseau est appropriée pour assurer la sécurité de l'information.	Le cas échéant, les auditeurs peuvent vérifier l'existence de contrôles cryptographiques et d'autres contrôles de la cybersécurité.
8	Continuité des activités et rétablissement après sinistre	Déterminer si les aspects liés à la sécurité relatifs à ces processus ont été traités et si la sécurité de l'information est appropriée pour assurer la transition et le fonctionnement en cas de rétablissement après sinistre.	Les auditeurs peuvent contrôler si le dispositif pour la sécurité de l'information est approprié pendant le processus de rétablissement après sinistre.