CUPSA | ASPC

COMMUNIQUÉ

15-COM-001 Le 24 septembre 2015

Publication des lignes directrices sur l'audit des technologies de l'information

L'Association des superviseurs prudentiels des caisses (ASPC) a publié des lignes directrices sur l'audit des technologies de l'information (TI), qui décrivent les principes sains et les pratiques exemplaires d'un audit des TI d'une coopérative de crédit ou d'une caisse populaire au Canada.

Ces lignes directrices sont conformes aux normes internationales et peuvent être adaptées en fonction de la taille, de la portée, de la complexité et du profil de risques d'une institution.

L'ASPC encourage les coopératives de crédit et les caisses populaires canadiennes à envisager d'intégrer les principes, les pratiques, ainsi que les rôles et responsabilités présentés dans ces lignes directrices dans leurs cadres de gestion des risques informatiques.

Chaque membre de l'ASPC peut choisir d'appliquer les lignes directrices dans la forme actuelle ou modifiée à sa propre discrétion.

L'ASPC continuera de suivre les travaux de recherches et les lignes directrices nationaux et internationaux en lien avec le risque informatique afin d'améliorer continuellement les pratiques de gestion du risque des coopératives de crédit et des caisses populaires canadiennes.

À propos de l'ASPC

L'Association des superviseurs prudentiels des caisses (ASPC) est un regroupement interprovincial composé d'organismes d'assurance-dépôts et de superviseurs prudentiels de l'ensemble du Canada. L'ASPC œuvre à maintenir le caractère sain et durable du secteur des caisses canadiennes, au moyen d'actions concertées. Pour en savoir plus, visitez le site Web de l'ASPC à www.cupsa-aspc.ca.

Lignes directrices sur l'audit des technologies de l'information

Un audit des technologies de l'information (TI) est une analyse des pratiques, des politiques et des mesures de contrôle à l'intérieur de l'environnement informatique d'une organisation qui recueille et évalue les données relatives aux systèmes, aux pratiques et aux opérations informatiques d'une organisation. L'évaluation de ces données détermine si les systèmes d'information assurent la protection des actifs en matière d'information, le maintien de l'intégrité des données, la protection contre les risques pour la cybersécurité et l'exploitation efficace et efficiente pour atteindre les buts ou les objectifs d'affaires de l'organisation.

La notion d'*audit des TI* est souvent utilisée à tort comme synonyme de celle d'*audit de la sécurité des TI*. Alors que la sécurité des TI forme une des composantes d'un audit des TI, d'autres aspects de la gouvernance, de la gestion des risques et des opérations des TI sont nécessaires à un audit exhaustif des TI. Les audits des TI portent également sur l'efficacité, l'efficience, le rapport qualité-prix, le retour sur investissement et les questions liées à la culture et aux personnes qui pourraient affecter la capacité de l'environnement des TI à soutenir les objectifs organisationnels.

Ce document d'orientation a été élaboré à l'intention des coopératives de crédit et des caisses populaires afin de mieux faire connaître les notions d'audit des TI et d'aider les cadres supérieurs qui envisagent le recours à un audit des TI dans leur organisation[1]. Les domaines d'audit des TI décrits dans ces lignes directrices peuvent être adaptés en fonction de la taille, de la portée, de la complexité et du profil de risques d'une institution.

Pratiques courantes d'audit des TI

Il est indispensable de définir l'objectif et la portée de l'audit des TI pour recevoir l'assurance requise par le conseil d'administration et la direction. Cette section décrit les divers domaines sur lesquels porte un audit des TI traditionnel. Chaque audit peut comprendre les éléments ci-dessous, à divers degrés; certains audits peuvent examiner avec soin certains de ces éléments. Chaque coopérative de crédit ou caisse populaire doit évaluer la pertinence de ces domaines lors de l'examen de la portée d'un audit des TI.

[1] De plus, l'ASPC encourage les coopératives de crédit à se pencher sur les principes et les pratiques des organismes de normalisation internationaux en matière d'audit des TI (p. ex., l'ISACA, l'Institut de l'audit interne (IIA), l'Organisation internationale de normalisation (ISO), et autres).

L'annexe « A » énumère des ressources en ligne supplémentaires[2] qui aideront le lecteur à mieux comprendre chacun des domaines de vérification suivants plus en détail.

Analyse de l'alignement stratégique de l'entreprise et des TI

L'analyse de l'alignement stratégique de l'entreprise et des TI consiste à déterminer si les ressources des technologies de l'information correspondent au plan stratégique et aux besoins opérationnels de la coopérative de crédit. Voici un aperçu des pratiques courantes :

- Déterminer s'il existe des mécanismes et des paramètres pour s'assurer que les projets des TI s'harmonisent avec les objectifs de l'entreprise;
- Évaluer si la direction dispose d'informations fiables sur les projets des TI à des fins de prise de décisions;
- Analyser les moyens par lesquels la coopérative de crédit ou la caisse populaire mesure la valeur obtenue à partir de l'investissement dans les TI.

Analyse de l'administration des systèmes

L'analyse de l'administration des systèmes consiste à évaluer la pertinence et l'efficacité des procédures d'administration, des pratiques en matière de sécurité et des processus d'entretien des serveurs et des systèmes internes, y compris les systèmes d'exploitation, les plateformes virtualisées, les systèmes de bases de données, etc. Voici un aperçu des pratiques courantes :

- L'examen de la gestion, de l'entretien et des pratiques en matière de sécurité entourant les serveurs et les postes de travail internes;
- L'examen des politiques et des procédures entourant l'administration du système (p. ex., la gestion des correctifs, l'octroi de licences).

Examen des applications

L'examen des applications (aussi connu comme examen du contrôle des applications), évalue les applications commerciales, les systèmes de traitement de l'information et les systèmes d'information de gestion critiques d'une entreprise. Il est essentiel que l'auditeur soit familiarisé avec les fonctions commerciales de l'organisation pour effectuer ces types d'examen. Voici un aperçu des pratiques courantes en matière d'audit :

- L'examen de la conformité d'une application aux règles commerciales dans le flux et la précision du traitement;
- La confirmation des capacités de validation des entrées de données à l'intérieur de chaque application;
- L'examen du contrôle de l'accès et des autorisations de tous les utilisateurs à l'intérieur d'une application;

[2] Les ressources fournies le sont uniquement à des fins d'information et ne sont pas approuvées par l'ASPC.

- La vérification de la gestion des erreurs et des exceptions, de la consignation et des pistes d'audit des applications.

Évaluation de la sécurité du réseau

L'évaluation de la sécurité du réseau se concentre sur l'architecture de réseau interne et externe qui soutient l'environnement informatique d'une organisation, y compris les pare-feu, les routeurs, les commutateurs, etc. Voici un aperçu des pratiques courantes en matière d'audit :

- L'examen de l'architecture de réseau de l'organisation;
- L'examen des contre-mesures de sécurité du périmètre (p. ex., les pare-feu, les systèmes de détection/prévention des intrusions, etc.);
- L'examen de l'architecture et des politiques de sécurité interne générales;
- L'examen de l'efficacité et de l'exhaustivité des implantations/configurations de l'infrastructure de réseau (p. ex., contrôle des accès);
- L'examen des politiques et des procédures des processus de gestion de la sécurité (p. ex., la gestion des incidents, l'évaluation de la vulnérabilité, la gestion des correctifs).

Examen de la continuité des activités

L'examen de la continuité des activités se concentre sur la pertinence et l'efficacité de la documentation, de l'infrastructure et des capacités de reprise après catastrophe d'une organisation. Voici un aperçu des pratiques courantes :

- L'évaluation de la qualité et de la pertinence de la documentation et des processus de planification de la continuité des activités/plan de reprise après catastrophe (PCA/PRC);
- L'examen des procédures d'entretien et de tests de la documentation et des processus de PCA/PRC;
- L'examen des capacités du site en matière de reprise après catastrophe et de la stratégie de reprise afin de répondre aux exigences organisationnelles.

Examen de l'intégrité des données

L'examen de l'intégrité des données porte sur les données en direct, en transit ou stockées, et permet de vérifier la robustesse et la pertinence des mesures de contrôle, l'impact des lacunes et la fiabilité et la crédibilité des données et des renseignements au sein de l'organisation. Voici un aperçu des pratiques courantes :

- Vérifier l'exactitude et la cohérence des données stockées dans les bases de données, entrepôts de données, dépôts de données, etc.;
- Examiner l'utilisation continue de la vérification des erreurs et des routines de validation;
- Évaluer les mécanismes de protection comme le cryptage, la sauvegarde des données, les contrôles d'accès, la validation de la saisie et des données, etc.

Examen de la sécurité physique

Les examens physiques comprennent les évaluations de la sécurité physique, de l'alimentation électrique, de la climatisation, du contrôle de l'humidité, de la lutte contre les incendies et d'autres facteurs environnementaux et de leurs effets sur les opérations des technologies de l'information. Voici un aperçu des pratiques courantes :

- Activités de collecte de renseignements et de reconnaissance à distance;
- Examen des contrôles de sécurité physique des bâtiments, des centres de données et d'autres installations liées aux ressources des technologies de l'information;
- Tests de pénétration physique et évaluation des contre-mesures;
- Sous l'angle des PCA/PRC, détermination du niveau de protection, de la résilience et de la reprise fournis par les lieux physiques.

Examen de la gestion des projets et de la gestion du changement

L'examen de la gestion des projets et de la gestion du changement porte sur les pratiques et les processus de gestion de projet et de gestion du changement utilisés lors des étapes de la planification, de la conception, de l'élaboration, de la mise en œuvre et de test des initiatives de TI.

Voici un aperçu des pratiques courantes :

- Analyse et examen de l'utilisation des éléments livrables de gestion de projets informatiques au cours des projets de TI (chartes, plans, demandes de changement, etc.);
- Réalisation de bilans des projets achevés pour évaluer l'atteinte des buts et des objectifs, la conformité ou le dépassement des attentes des utilisateurs ou du système, et le respect de la portée, des échéanciers, des budgets, etc.;
- Examen des processus de gestion du changement pour l'intégration des nouveaux systèmes et détermination de la manière dont les systèmes récents ont été présentés aux utilisateurs et introduits aux environnements informatiques.

Rôles et responsabilités en matière d'audit des TI

Une bonne compréhension des rôles et des responsabilités adéquats est essentielle à une fonction efficace de l'audit des TI. L'ASPC a défini les rôles et les responsabilités clés[3] comme suit :

Conseil d'administration/Comité d'audit

- Veiller à ce que l'audit des TI soit inclus et abordé dans le cadre de contrôle interne;

[3] Les rôles et les responsabilités décrits devraient être appliqués en fonction de la taille, de la portée et de la complexité des coopératives de crédit ou des caisses populaires.

- Déterminer la méthode la plus efficace pour obtenir des ressources pour l'audit des TI (à l'interne ou à l'externe);
- Assurer un niveau efficace de connaissance et de compréhension des TI parmi les membres du conseil d'administration;
- Examiner et approuver des plans d'audit des TI adéquats;
- Évaluer les réponses de la direction aux conclusions et aux recommandations de l'audit;
- Évaluer le rendement des initiatives d'audit des TI;
- Préserver l'indépendance des auditeurs des TI, sans égard au choix pour l'audit des TI;
- Recevoir et examiner les rapports de la haute direction sur les risques informatiques importants, y compris les processus de gestion de ces risques.

Haute direction

- Déterminer la méthode la plus efficace pour l'obtention des ressources d'audit des TI (à l'interne ou à l'externe) – cette responsabilité devrait être partagée avec le conseil d'administration;
- Cerner les domaines liés au risque en matière de TI grâce à la fonction de gestion interne des risques;
- Évaluer et approuver le cadre de contrôle informatique de l'organisation;
- Aborder les conclusions et recommandations de l'audit des TI et mettre en œuvre les améliorations aux mesures de contrôle;
- Obtenir des données faisant état des audits des TI sur les produits et services confiés à un fournisseur externe[4].

Audit externe/interne

- Évaluer les mesures de contrôle et les pratiques des TI fondées sur les plans d'audit approuvés;
- Obtenir une expertise externe pour les domaines d'audit des TI qui exigent des connaissances et des compétences supplémentaires;
- Communiquer régulièrement les résultats des conclusions de l'audit des TI au conseil d'administration ou au comité d'audit.

Les fournisseurs externes de services

- Fournir des preuves des audits des TI effectués sur les produits et les services qu'ils offrent aux coopératives de crédit et aux caisses populaires.

[4] Lorsqu'elle se fie aux rapports d'audit de fournisseurs externes, il incombe à la direction de veiller à ce que la portée de la vérification corresponde aux services reçus par la coopérative de crédit ou la caisse populaire.

Organismes de réglementation

- Évaluer si les risques liés aux TI auxquels la coopérative de crédit est exposée sont gérés à l'aide d'un cadre de gouvernance des TI;
- Encourager les coopératives de crédit et les caisses populaires à obtenir la confirmation que tous les produits et services des TI (à la fois à l'interne et à l'externe) sont vérifiés ou examinés par un tiers et que les recommandations de l'audit sont abordées.

CUPSA | ASPC

Annexe A – Ressources supplémentaires en matière d'audit des TI

Analyse de l'harmonisation stratégique de l'entreprise/des TI

- http://info.knowledgeleader.com/bid/179384/Auditing-IT-Management-Aligning-IT-with-Business-Priorities
- https://businessitalignment.wordpress.com/2010/12/22/strategic-alignment-maturity-model-luftman/
- http://www.gvv-web.nl/alignmentMeasure.html

Analyse de l'administration des systèmes

- http://www.sans.org/reading-room/whitepapers/bestprac/system-administrator-security-practices-657
- http://www.sfisaca.org/download/gensecaudpgm.pdf

Examen des applications

- http://www.theiia.org/bookstore/downloads/freetomembers/0_1033.dl_gtag8.pdf
- http://resources.infosecinstitute.com/itac-application-controls/
- http://www.sans.org/reading-room/whitepapers/auditing/application-audit-process-guide-information-security-professionals-1534

Évaluation de la sécurité du réseau

- http://www.sans.org/reading-room/whitepapers/auditing/base-security-assessment-methodology-1587
- http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Examen de la continuité des activités

- http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Business-Continuity-Management-Audit-Assurance-Program.aspx
- http://www.computerweekly.com/feature/Disaster-recovery-audit-maintenance-and-continuous-improvement
- http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/bsnss-cntnt-plnnng/index-eng.aspx

Examen de l'intégrité des données

- http://info.knowledgeleader.com/bid/161188/What-is-Data-Integrity-Risk

- http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/T/Top-10-Reasons-to-Audit-the-Integrity-of-Your-Data.aspx
- http://www.testingexcellence.com/what-is-data-and-database-integrity-testing/

Examen de la sécurité physique

- http://www.sans.org/reading-room/whitepapers/physical/implementing-robust-physical-security-1447
- http://www.securestate.com/Services/Profiling/Pages/Physical-Security-Assessment.aspx
- http://www.sans.edu/research/security-laboratory/article/281

Examen de la gestion des projets et de la gestion du changement

- https://iaonline.theiia.org/auditing-it-project-management
- http://www.brighthubpm.com/monitoring-projects/32883-project-management-audit-process/
- https://www.bia.ca/articles/UndertakingaSuccessfulProjectAudit.htm