RAPPORT TECHNIQUE

ISO/TR 13569

Deuxième édition
1997-10-01

Banques et services financiers liés aux opérations bancaires — Lignes directrices pour la sécurité de l'information

Banking and related financial services — Information security guidelines

Numéro de référence
ISO/TR 13569:1997(F)

Sommaire

Organisation internationale de normalisation
Case postale 56 • CH-1211 Genève 20 • Suisse
Internet iso@iso.ch

Version française parue en 1999

Imprimé en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Exceptionnellement, un comité technique peut proposer la publication d'un rapport technique de l'un des types suivants:

— type 1, lorsque, en dépit de maints efforts, l'accord requis ne peut être réalisé en faveur de la publication d'une Norme internationale;

— type 2, lorsque le sujet en question est encore en cours de développement technique ou lorsque, pour toute autre raison, la possibilité d'un accord pour la publication d'une Norme internationale peut être envisagée pour l'avenir mais pas dans l'immédiat;

— type 3, lorsqu'un comité technique a réuni des données de nature différentes de celles qui sont normalement publiées comme Normes internationales (ceci pouvant comprendre des informations sur l'état de la technique, par exemple).

Les rapports techniques des types 1 et 2 font l'objet d'un nouvel examen trois ans au plus tard après leur publication afin de décider éventuellement de leur transformation en Normes internationales. Les rapports techniques de type 3 ne doivent pas nécessairement être révisés avant que les données fournies ne soient plus jugées valables ou utiles.

L'ISO/TR 13569, rapport technique du type 3, a été élaboré par le comité technique ISO/TC 68, *Banque, valeurs mobilières et autres services financiers*, sous-comité SC 2, *Gestion de la sécurité et opérations bancaires générales*.

Cette deuxième édition annule et remplace la première édition (ISO/TR 13569:1996), dont elle constitue une révision technique.

Banque et services financiers liés aux opérations bancaires — Lignes directrices pour la sécurité de l'information

1 Introduction

Pour une conduite efficace de leur activité, les établissements financiers s'appuient de plus en plus sur la technologie de l'information (IT).

La gestion du risque est cruciale pour le secteur des services financiers. Les établissements financiers gèrent le risque par l'intermédiaire de pratiques commerciales prudentes, par la prudence dans la passation des contrats, par l'assurance et par l'utilisation de dispositifs de sécurité appropriés.

Il est nécessaire de gérer d'une manière complète la sécurité de l'information au sein des établissements financiers.

Le présent rapport technique ne vise pas à fournir une solution générique pour toutes les situations. Chaque cas doit être examiné pour son propre mérite et les actions appropriées sélectionnées. Le présent rapport technique doit servir de directive et non de solution.

Les objectifs du présent rapport technique sont les suivants:

— présenter une structure de programme de sécurité de l'information;

— présenter un guide de sélection aux contrôles de sécurité qui représentent une pratique commerciale prudente acceptée;

— être cohérent avec les normes existantes et avec les nouveaux travaux portant sur les critères de sécurité objectifs et sur lesquels on peut se reposer.

Le présent rapport technique est destiné à être utilisé par les établissements financiers de toutes tailles et de tous types qui désirent employer un programme de sécurité de l'information raisonnable commercialement et prudent. Il est également utile aux prestataires de services des établissements financiers. Le présent rapport technique peut également servir de document source pour les éducateurs et éditeurs qui sont au service de l'industrie financière.

2 Références

NOTE L'annexe C contient des références à des réglementations, normes et codes nationaux. La liste ci-dessous ne contient que les documents cités dans le corps principal du présent rapport technique.

Normes internationales:

ISO 8730, *Opérations bancaires - Spécifications liées à l'authentification des messages (service aux entreprises).*

ISO 8732, *Banque - Gestion de clés*.

ISO 9564 (toutes parties), *Banque - Gestion et sécurité du numéro personnel d'identification*.

ISO 10126 (toutes parties), *Banque - Procédures de chiffrement de messages (service aux entreprises).*

ISO 10202 (toutes parties), *Cartes de transactions financières - Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré*.

Normes nationales:

ANSI X9/TG-2, *Compréhension et conception des chèques (États-Unis).*

ANSI X9/TG-8, *Guide pour la sécurité des chèques (États-Unis).*

Réglementations:

Bureau fédéral du Contrôleur des Monnaies, Circulaire bancaire BC-226 Définition des règles.

Autres documents:

Institut des normes d'audit interne pour l'exercice professionnel de l'audit interne.

Code de bonne pratique pour la gestion de la sécurité.

Norme fédérale pour la protection des informations (FIPS), PUB 140-1, Exigences de sécurité relatives aux modules cryptographiques, Institut national de normalisation et de technologie (États-Unis).

Sécurité de l'argent électronique, publié par la Banque internationale d'investissement, Bâle, août 1996.

3 Résumé cadre

Les établissements financiers et leur direction supérieure ont toujours été responsables de la mise en œuvre de contrôles efficaces pour assurer la protection des biens informatiques. La confidentialité, l'intégrité, l'authenticité et la disponibilité de ces informations sont d'une importance capitale pour les affaires. À ce titre, il est impératif que ces actifs soient disponibles et protégés contre toute divulgation, modification, fabrication, duplication et destruction, accidentelle ou intentionnelle. Il est impératif pour un établissement financier de protéger le transfert de ses actifs, qui sont codés sous forme d'informations fiables.

Les entreprises dépendent de plus en plus de systèmes d'informations informatisés. La technologie devient indissociable des affaires financières. L'utilisation des ordinateurs et des réseaux ne cesse de progresser et il est nécessaire qu'ils puissent fonctionner ensemble. Dans de nombreux établissements, la quantité de travail accomplie sur des ordinateurs personnels et des réseaux locaux est plus importante que celle réalisée sur de gros ordinateurs. Les contrôles de sécurité de ces ordinateurs ne sont pas aussi développés que sur les gros systèmes. La sécurité nécessaire pour tous les systèmes d'information est d'une importance sans cesse plus grande. Les établissements financiers utilisent de plus en plus les systèmes d'images, les systèmes de données/voix numériques, les systèmes de traitement distribué et d'autres technologies nouvelles. Ceci rend la sécurité des informations encore plus importante pour le succès commercial ou même pour la survie d'un établissement.

Les contrôles de sécurité sont nécessaires pour limiter la vulnérabilité des informations et des systèmes de traitement des informations. Le niveau de contrôle de protection doit être rentable, c'est-à-dire en cohérence avec le degré d'exposition et les répercussions des pertes subies par l'établissement. Les expositions comprennent les pertes financières, les inconvénients vis-à-vis de la concurrence, une réputation entachée, une divulgation erronée, des poursuites judiciaires ou des sanctions réglementaires. Des normes, des règles et des lignes directrices de sécurité bien pensées sont le fondement d'une bonne sécurité de l'information.

Aux États-Unis, au Canada et dans la Communauté Européenne, des travaux cherchent à établir des Critères Communs pour l'évaluation de la technologie de l'information. Ces critères, associés à des classes de fonctionnalités prédéfinies par le secteur financier, permettront aux établissements financiers d'obtenir des installations de sécurité uniformes et fiables. Il convient que le présent Rapport Technique soit utilisé en tant que contribution à ce processus.

Avec la poursuite de l'expansion de l'information distribuée, l'intérêt et la pression sont de plus en plus grands s'assurer de manière raisonnable que les établissements financiers disposent de contrôles appropriés. Cet intérêt s'exprime dans les lois et les réglementations. Un extrait de la déclaration de politique BC-226, Circulaire bancaire du Bureau américain du Contrôleur des devises, illustre cette préoccupation.

"Il est de la responsabilité du Conseil d'Administration de s'assurer que les politiques d'entreprises appropriées, qui identifient les responsabilités de gestion et les pratiques de contrôle pour tous les domaines et activités de traitement des informations, ont été établies. L'existence d'une telle " politique de sécurité de l'information d'entreprise ", l'adéquation de ces normes et la supervision de gestion de ces activités seront évaluées par les examinateurs lors de revues de supervision régulières de l'établissement."

Le présent rapport technique inclut un guide pour élaborer un programme complet de sécurité de l'information.

Note relative à la seconde édition

Depuis la publication de la première édition du présent rapport technique, de nombreux points ont changé. Ces changements n'ont pas simplifié le sujet. Pratiquement aucune des menaces, ni aucun des contrôles énumérés dans la première édition, ne sont devenus obsolètes. De nouvelles menaces ont fait leur apparition, ainsi que de nouvelles opportunités d'amélioration des services offerts à la clientèle. Les activités bancaires sur Internet, l'argent électronique, les découvertes et les redécouvertes révolutionnaires dans les technologies de l'information sont le reflet d'une époque passionnante. Le présent rapport technique concerne autant que possible l'environnement tel qu'il est connu. Notre expérience des quatre années écoulées impose une vigilance permanente comme l'exigence minimale d'une sécurité viable.

4 Comment utiliser ce rapport technique

Le présent rapport technique a été conçu pour répondre à de nombreux objectifs. Le présent article donne une cartographie pour le reste du présent rapport technique.

Article 5: Exigences: Cet article définit un point de départ pour la création d'un programme de sécurité. Il définit les exigences minimales d'un programme de sécurité d'information adéquat. Il peut également servir d'étalon pour mesurer l'état du programme de sécurité des informations d'un établissement.

Article 6: Composants du programme de sécurité d'information: Cet article contient des informations plus spécifiques sur la manière dont il convient qu'un programme de sécurité de l'information fonctionne. On suggère des responsabilités particulières pour divers responsables et fonctions d'un établissement. On identifie les lignes de communication entre les fonctions qui sont considérées comme contribuant à une pratique de sécurité saine. Cet article peut être utilisé par des cadres supérieurs pour s'assurer que les entraves structurelles à une pratique de sécurité saine sont minimisées. Le personnel chargé de la sécurité des informations peut également utiliser cet article pour évaluer l'efficacité du programme de sécurité des informations.

Article 7: Objectifs de contrôle et solutions suggérées: Cet article est au cœur du présent rapport technique. Il aborde les menaces qui pèsent sur l'information, en termes suffisamment spécifiques pour permettre au personnel financier de déterminer s'il existe un problème au sein de son établissement, sans pour autant former de délinquants. Les quatre premiers alinéas traitent des contrôles communs à de nombreuses plates-formes de livraison: classification, contrôle d'accès logique, contrôle de change et trace d'audit. Les alinéas suivants abordent les problèmes de sécurité concernant les installations de traitement de l'information, les ressources humaines et ceux spécifiques à la plate-forme de livraison utilisée. Cet article se termine par les transferts de fonds électroniques et le traitement électronique des chèques.

Article 8: Mise en œuvre de contrôles cryptographiques: Cet article donne des informations contribuant à garantir que les contrôles cryptographiques sont mis en œuvre de manière efficace.

Article 9: Sources d'aide complémentaires: Cet article répertorie les types d'organisations pouvant aider à informer les professionnels de la sécurité de l'information. Cet article est destiné à être utilisé parallèlement à l'Annexe C.

Annexe A: Exemples de documents: Cette annexe rassemble des exemples de formulaires prêts à l'emploi pour différentes utilisations relatives à la sécurité de l'information.

Annexe B: Principes pour la protection de la vie privée: Cette annexe présente un ensemble d'exemples de principes de protection de la vie privée.

Annexe C: Noms et adresses des organismes nationaux: Cette annexe répertorie les noms et coordonnées d'organismes nationaux susceptibles de venir en aide au personnel chargé de la sécurité de l'information.

Annexe D: Normes de sécurité extérieures à la communauté financière: Il s'agit d'une liste complète des normes de sécurité mises en œuvre par des organismes de normalisation autres que l'ASC X9 (États-Unis) ou l'ISO/TC 68.

Annexe E: L'évaluation des risques et de la vulnérabilité indique une méthode d'identification des risques à l'intérieur d'un établissement.

5 Assurance de la sécurité

Au niveau le plus élevé, il est primordial de faire partager à la direction et au personnel l'acceptation de valeurs éthiques et d'impératifs de contrôle, et de renforcer régulièrement cette approche. Les informations représentent un actif qui exige un système de contrôle, tout comme d'autres actifs plus facilement réductibles à des termes monétaires. Un contrôle prudent de l'actif représenté par les informations d'un établissement constitue une bonne pratique commerciale.

Il convient que la protection des informations soit centrée sur la protection des processus commerciaux déterminants. La notion d'information et de ses attributs change dans le contexte d'un processus commercial et il convient que les exigences de sécurité soient examinées à chaque étape de ce processus.

Le développement, le maintien et la surveillance d'un programme de sécurité de l'information requièrent la participation de plusieurs disciplines au sein de l'organisation. Une coordination étroite est nécessaire entre le directeur commercial et le personnel chargé de la sécurité des informations. Il convient que des disciplines telles que l'audit, les assurances, le respect des réglementations, la sécurité physique, la formation, le personnel ou le droit, soient utilisées pour soutenir le programme de sécurité de l'information. La sécurité de l'information relève à la fois d'un effort collectif et d'une responsabilité individuelle.

L'exigence de base du présent Rapport Technique est d'établir un programme de sécurité de l'information qui

a) inclut une politique et une déclaration de sécurité de l'information communes à l'ensemble de l'établissement et contenant:

   i. une déclaration selon laquelle l'établissement considère les informations, quelle que soit leur forme, comme étant un actif de l'établissement;

   ii. une identification des risques et l'exigence de mise en œuvre de contrôles visant à garantir la protection des capitaux d'informations. L'article 7 du présent rapport fait état des contrôles appropriés;

   iii. une définition des responsabilités attribuées aux postes concernant la sécurité de l'information, pour chaque directeur, employé et sous-traitant. L'article 6 du présent rapport technique énumère les responsabilités suggérées;

   iv. un engagement en faveur de la sensibilisation et de la formation à la sécurité;

b) nomme un ou plusieurs cadres à titre de responsables du programme de sécurité de l'information;

c) prévoit la désignation d'individus chargés de protéger les actifs d'information et de spécifier les niveaux de sécurité appropriés;

d) comprend un programme de sensibilisation ou de formation, afin de veiller à ce que les employés et les sous-traitants soient conscients de leurs responsabilités en matière de sécurité de l'information;

e) résout et fait état des incidents de sécurité de l'information;

f) élabore des plans écrits pour la reprise de l'activité à la suite de sinistres;

g) fournit l'identification et les procédures d'adressage des exceptions ou écarts par rapport à la politique de sécurité de l'information ou des documents connexes;

h) encourage la coordination avec les parties concernées, telles que les cadres responsables de l'audit, des assurances et du respect des règlements;

i) définit la responsabilité pour mesurer le respect et la validité du programme de sécurité;

j) assure l'examen et la mise à jour du programme en fonction des nouveaux dangers et des nouvelles technologies. Il convient par exemple que l'émergence des critères d'évaluation du traitement de l'information aide les professionnels de la sécurité à choisir et mettre en œuvre des contrôles de sécurité normalisés;

k) prévoit si nécessaire la production d'archives d'audit et leur surveillance.

6 Composants du programme de sécurité de l'information

Le paragraphe 6.1 traite des responsabilités en matière de sécurité de l'information au sein de l'établissement. Les paragraphes 6.2 et suivants abordent les fonctions relatives à la sécurité de l'information. Les contrôles suggérés dans le présent rapport technique sont ceux qui appliquent ou prennent en charge la protection de l'information et des ressources de traitement de l'information. Bien que certains de ces contrôles concernent parfois d'autres domaines de la gestion bancaire, il convient de ne pas considérer le présent document comme une liste exhaustive des contrôles de gestion.

6.1 Responsabilités générales

6.1.1 Administrateurs

Les administrateurs ont le devoir, vis-à-vis de l'établissement et de ses actionnaires, de superviser la gestion de l'établissement. La mise en œuvre de pratiques efficaces pour la sécurité de l'information constitue une pratique commerciale prudente et prouve que l'établissement cherche à gagner la confiance du public. Il convient que les administrateurs fassent percevoir l'importance de la sécurité de l'information et apportent leur soutien à un programme de sécurité de l'information.

6.1.2 Président directeur général

Le président directeur général ou le directeur général assume, en tant que cadre le plus haut placé dans la hiérarchie de l'établissement, la responsabilité ultime du fonctionnement de l'établissement. Il convient que le PDG permette la mise en place et assure le soutien d'un programme de sécurité de l'information conforme aux normes reconnues, supervise les grandes décisions d'évaluation des risques et contribue à faire percevoir l'importance de la sécurité de l'information.

6.1.3 Directeurs

Les directeurs ont pour mission de superviser et surveiller l'établissement et les employés. Ils jouent donc un rôle décisif dans les programmes de sécurité de l'information. Il convient que chaque directeur

- comprenne, soutienne et respecte la politique, les normes et les directives de sécurité de l'information de l'établissement;
- s'assure que les employés, les fournisseurs et les sous-traitants comprennent, soutiennent et respectent également la politique, les normes et les directives de sécurité de l'information de l'établissement, par exemple le code pratique pour la gestion de la sécurité de l'information;
- mette en œuvre des contrôles de sécurité de l'information qui répondent aux exigences du commerce et des pratiques commerciales prudentes;
- crée une atmosphère positive qui encourage les employés, fournisseurs et sous-traitants à signaler les problèmes liés à la sécurité de l'information;
- signale immédiatement au responsable concerné tout problème de sécurité de l'information;
- participe au programme de communication et de sensibilisation à la sécurité de l'information;
- applique des principes commerciaux et de sécurité sains lors de l'élaboration des requêtes d'exception;