Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1054

(09/2012)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité de l'information et des réseaux – Gestion de la sécurité

Technologie de l'information – Techniques de sécurité – Gouvernance de la sécurité de l'information

Recommandation UIT-T X.1054

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	**X.1050–X.1069**
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

NORME INTERNATIONALE ISO/CEI 27014
RECOMMANDATION UIT-T X.1054

Technologie de l'information – Techniques de sécurité – Gouvernance de la sécurité de l'information

Résumé

La Recommandation UIT-T X.1054 | Norme internationale ISO/CEI 27014 donne des orientations concernant la gouvernance de la sécurité de l'information.

La sécurité de l'information est devenue une question fondamentale pour les organisations. Outre que les prescriptions réglementaires sont de plus en plus nombreuses, l'échec des mesures prises par une organisation en matière de sécurité de l'information peut avoir une incidence directe sur la réputation de cette dernière.

Il est par conséquent de plus en plus demandé à l'organe directeur, dans le cadre de ses responsabilités en matière de gouvernance, de superviser la sécurité de l'information afin de faire en sorte que les objectifs de l'organisation soient atteints.

Par ailleurs, la gouvernance de la sécurité de l'information permet de créer des liens étroits au sein d'une organisation entre l'organe directeur, les cadres supérieurs et ceux qui sont chargés de la mise en place et de l'utilisation d'un système de gestion de la sécurité de l'information.

Elle confère le mandat essentiel à la mise en place d'initiatives de sécurité de l'information dans toute l'organisation.

Par ailleurs, dans le cadre d'une gouvernance efficace de la sécurité de l'information, l'organe directeur reçoit des rapports pertinents – rédigés dans un contexte opérationnel – sur les activités liées à la sécurité de l'information, ce qui permet de prendre en temps opportun des décisions adaptées au sujet des questions relatives à la sécurité de l'information, qui vont dans le sens des objectifs stratégiques de l'organisation.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1054	2012-09-07	17

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas des renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

NORME INTERNATIONALE
RECOMMANDATION UIT-T

Technologie de l'information – Techniques de sécurité – Gouvernance de la sécurité de l'information

1 Domaine d'application

La présente Recommandation | Norme internationale présente des concepts et fournit des orientations concernant les principes et processus régissant la gouvernance de la sécurité de l'information, grâce auxquels les organisations peuvent évaluer, orienter et suivre la gestion de la sécurité de l'information.

La présente Recommandation | Norme internationale est applicable à toutes les organisations, quels que soient leur type et leur taille.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations UIT-T en vigueur.

– ISO/CEI 27000:2009, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

3 Définitions

Pour les besoins de la présente Recommandation | Norme internationale, les termes et définitions figurant dans la norme ISO/CEI 27000 et les définitions suivantes s'appliquent:

3.1 direction générale: personne ou groupe de personnes auxquels l'organe directeur a délégué la responsabilité de mettre en œuvre les stratégies et politiques propres à réaliser le but de l'organisation.

NOTE 1 – La direction générale fait partie de la haute direction. Afin que les rôles soient clairs, la présente norme distingue deux groupes composant la direction: l'organe directeur et les cadres dirigeants.

NOTE 2 – La direction générale peut comprendre le directeur général (CEO), le directeur financier (CFO), le directeur des opérations (COO), le directeur des systèmes d'information (CIO), le directeur de la sécurité des systèmes d'information (CISO) et d'autres fonctions analogues.

3.2 organe directeur: personne ou groupe de personnes responsable des résultats et de la conformité de l'organisation.

NOTE – L'organe directeur fait partie de la haute direction. Afin que les rôles soient clairs, la présente norme distingue deux groupes composant la haute direction: l'organe directeur et les cadres dirigeants.

3.3 gouvernance de la sécurité de l'information: système selon lequel une organisation conduite et contrôle les activités liées à la sécurité de l'information.

3.4 partie prenante: toute personne ou organisation susceptible d'influer sur une activité de l'organisation, ou d'en subir les effets ou d'estimer qu'elle en subit des effets.

NOTE – Un décideur peut être une partie prenante.

4 Concepts

4.1 Généralités

La gouvernance de la sécurité de l'information doit aligner les objectifs et stratégies en matière de sécurité de l'information soient alignés sur les objectifs et stratégies de l'organisation et elle impose de respecter la législation, la réglementation et les contrats. Elle devrait être évaluée, analysée et mise en œuvre selon une approche de gestion des risques appuyée par un système de contrôle interne.

L'organe directeur est responsable en dernier ressort des décisions et des résultats d'une organisation. S'agissant de la sécurité de l'information, le principal objectif de l'organe directeur est de veiller à ce que l'approche retenue par l'organisation en matière de sécurité de l'information soit efficiente, efficace, acceptable et conforme aux objectifs et stratégies de l'organisation compte dûment tenu des attentes des parties prenantes. Diverses parties prenantes peuvent avoir des valeurs différentes et des besoins différents.

4.2 Objectifs

Les objectifs de la gouvernance de la sécurité de l'information sont les suivants:

- Faire correspondre les objectifs et la stratégie en matière de sécurité de l'information avec les objectifs et stratégies de l'organisation (alignement stratégique).
- Apporter de la valeur à l'organe directeur et aux parties prenantes (création de valeur).
- Faire en sorte que le risque lié à l'information soit traité comme il se doit (responsabilité).

4.3 Résultats escomptés

On attend de la mise en œuvre efficace de la gouvernance de la sécurité de l'information qu'elle produise les résultats suivants:

- Connaissance de la situation en matière de sécurité de l'information pour l'organe directeur.
- Approche souple de la prise de décisions concernant les risques liés à l'information.
- Investissements efficients et efficaces dans la sécurité de l'information.
- Respect des obligations externes (légales, réglementaires ou contractuelles).

4.4 Relations

Une organisation applique des modèles de gouvernance dans d'autres domaines, comme la gouvernance des technologies de l'information et la gouvernance organisationnelle. Chaque modèle de gouvernance fait partie intégrante de la gouvernance d'une organisation, d'où l'importance d'une harmonisation avec les objectifs de l'organisation. En règle générale, l'organe directeur a intérêt à définir une vision globale et intégrée de son modèle de gouvernance, dont la gouvernance de la sécurité de l'information devrait faire partie. Il arrive que les champs d'application des différents modèles de gouvernance se chevauchent. La Figure 1 illustre par exemple la relation entre la gouvernance de la sécurité de l'information et la gouvernance des technologies de l'information.

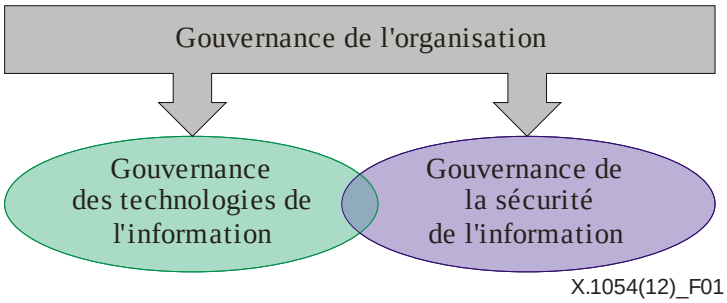

Figure 1 – Relation entre la gouvernance de la sécurité de l'information et la gouvernance des technologies de l'information

La gouvernance des technologies de l'information concerne avant tout les ressources nécessaires pour obtenir, traiter, stocker et diffuser des informations, tandis que la gouvernance de la sécurité de l'information porte sur la confidentialité, l'intégrité et la disponibilité de l'information. Ces deux systèmes de gouvernance doivent être gérés

selon les processus de gouvernance suivants: évaluer, diriger, surveiller (EDM). La gouvernance de la sécurité de l'information nécessite toutefois en plus le processus interne de "communication".

Les tâches que l'organe directeur doit mener à bien pour instaurer la gouvernance de la sécurité de l'information sont présentées au paragraphe 5. Ces tâches sont également liées aux exigences de gestion définies dans la norme ISO/CEI 27001 et dans d'autres normes de la famille des normes SGSI – systèmes de gestion de la sécurité de l'information (voir la bibliographie).

5 Principes et processus

5.1 Présentation générale

La présente partie décrit les principes et processus qui, pris ensemble, constituent la gouvernance de la sécurité de l'information. Les principes de gouvernance de la sécurité de l'information sont des règles acceptées qui régissent l'action ou la conduite en matière de gouvernance et servent à orienter sa mise en œuvre. Un processus de gouvernance pour la sécurité de l'information décrit une série de tâches qui permettent la gouvernance de la sécurité de l'information, et les relations entre ces tâches. Il fait également apparaître une relation entre la gouvernance et la gestion de la sécurité de l'information. Ces deux éléments sont présentés dans les paragraphes suivants.

5.2 Principes

Pour assurer la sécurité de l'information à long terme, il faut répondre aux besoins des parties prenantes et créer de la valeur pour chacune d'entre elles. On trouvera ci-après six principes orientés vers l'action à appliquer pour atteindre l'objectif de gouvernance consistant à faire correspondre la sécurité de l'information avec les objectifs de l'organisation et créer de la valeur.

Ces principes constituent une base solide pour exécuter les activités de gouvernance de la sécurité de l'information. Pour chaque principe, on décrit les résultats attendus sans toutefois préciser les modalités, les délais et les responsables de la mise en œuvre, car ces points dépendent de la nature de l'organisation appliquant les principes. L'organe directeur devrait exiger l'application de ces principes et nommer une personne qui serait responsable de leur mise en œuvre, qui serait mandatée pour le faire et qui devrait en rendre compte.

Principe 1: Instaurer la sécurité à l'échelle de l'organisation

La gouvernance de la sécurité de l'information devrait veiller à ce que les activités en matière de sécurité de l'information soient globales et intégrées. La sécurité de l'information devrait être administrée au niveau de l'organisation et les décisions devraient tenir compte des aspects liés aux activités, à la sécurité de l'information et à tout autre élément pertinent. Il convient de coordonner étroitement les activités se rapportant à la sécurité physique et logique.

Pour instaurer la sécurité à l'échelle de l'organisation, l'ensemble des activités d'une organisation devrait être soumis à l'obligation de responsabilité et à l'obligation de rendre des comptes en matière de sécurité de l'information. Cet aspect dépasse souvent les "frontières" de l'organisation telles qu'on les perçoit traditionnellement, par exemple lorsque l'information est stockée ou transférée par des parties extérieures.

Principe 2: Adopter une approche en fonction des risques

La gouvernance de la sécurité de l'information devrait reposer sur des décisions prises en fonction des risques. Le niveau de sécurité acceptable devrait être déterminé selon les risques qu'une organisation est prête à prendre (perte d'un avantage concurrentiel, risques sur le plan de la conformité et de la responsabilité, perturbations opérationnelles, réputation ternie et pertes financières, par exemple).

Si l'on veut qu'il soit adapté à l'organisation, le choix en matière de gestion des risques devrait cadrer avec l'approche globale de l'organisation en matière de gestion des risques et y être intégré. Des niveaux de sécurité de l'organisation acceptables devraient être définis selon les risques qu'une organisation est prête à prendre (perte d'un avantage concurrentiel, risques sur le plan de la conformité et de la responsabilité, perturbations opérationnelles, réputation ternie et pertes financières, par exemple). L'organe directeur devrait affecter des ressources suffisantes pour mettre en œuvre une gestion des risques liés à la sécurité de l'information.

Principe 3: Définir des orientations pour les décisions relatives aux investissements

Dans le cadre de la gouvernance de la sécurité de l'information il conviendrait de mettre en place une stratégie d'investissement dans la sécurité de l'information fondée sur les résultats opérationnels obtenus, de façon à harmoniser les besoins de l'entreprise et les exigences de sécurité, à la fois à court et à long terme, et à répondre ainsi aux besoins actuels et changeants des parties prenantes.

Pour optimiser les investissements dans la sécurité de l'information destinés à appuyer la réalisation des objectifs de l'organisation, l'organe directeur devrait veiller à ce que la sécurité de l'information soit intégrée aux processus en vigueur dans l'organisation en ce qui concerne les dépenses de fonctionnement et d'équipement, la conformité aux cadres légaux et réglementaires et l'établissement de rapports sur les risques.

Principe 4: Veiller au respect des obligations internes et externes

Dans le cadre de la gouvernance de la sécurité de l'information, les politiques et pratiques en matière de sécurité de l'information devraient être conformes aux législations et réglementations obligatoires pertinentes, ainsi qu'aux obligations commerciales ou contractuelles prises et aux autres obligations externes ou internes.

Pour résoudre les problèmes liés à la conformité et au respect des dispositions, l'organe directeur devrait obtenir l'assurance que les activités liées à la sécurité de l'information satisfont aux obligations internes et externes en demandant des audits de sécurité indépendants.

Principe 5: Favoriser un environnement propice à la sécurité

La gouvernance de la sécurité de l'information devrait reposer sur le comportement humain, y compris les besoins en évolution de toutes les parties prenantes, dans la mesure où le comportement humain est l'un des éléments essentiels pour assurer le niveau approprié de sécurité de l'information. Faute d'une coordination adéquate, il risque d'y avoir contradiction entre les objectifs, les rôles, les responsabilités et les ressources, ce qui nuira à la réalisation des objectifs de l'organisation. Par conséquent, il est très important d'assurer une harmonisation et de définir des orientations concertées entre toutes les parties prenantes.

Pour créer une véritable culture de la sécurité de l'information, l'organe directeur devrait exiger, favoriser et appuyer la coordination des activités des parties prenantes pour définir une orientation cohérente en matière de sécurité de l'information, ce qui facilitera la mise en œuvre de programmes d'enseignement, de formation et de sensibilisation dans le domaine de la sécurité.

Principe 6: Evaluer l'efficacité par rapport aux résultats de l'organisation

Dans le cadre de la gouvernance de la sécurité de l'information, il convient de veiller à ce que l'approche retenue pour protéger l'information soit adaptée aux besoins de l'organisation, en assurant les niveaux convenus de sécurité de l'information. Il faudrait maintenir l'efficacité de la sécurité aux niveaux requis pour répondre aux besoins actuels et futurs de l'organisation.

Pour évaluer l'efficacité de la sécurité de l'information du point de vue de la gouvernance, l'organe directeur devrait évaluer cette efficacité sous l'angle de ses incidences sur l'entreprise, et pas uniquement du point de vue de l'efficacité et de l'efficience des contrôles de sécurité. Pour ce faire, il est possible de procéder, sur demande, à des examens d'un programme d'évaluation de l'efficacité à des fins de suivi, d'audit et d'amélioration, de façon à rattacher l'efficacité de la sécurité de l'information et les résultats obtenus par l'entreprise.

5.3 Processus

5.3.1 Présentation générale

L'organe directeur mène à bien les processus "évaluer", "diriger", "surveiller" et "communiquer" pour administrer la sécurité de l'information. En outre, le processus "assurer" permet d'avoir un avis indépendant et objectif sur la gouvernance de la sécurité de l'information et le niveau atteint. La Figure 2 montre les liens entre ces processus.

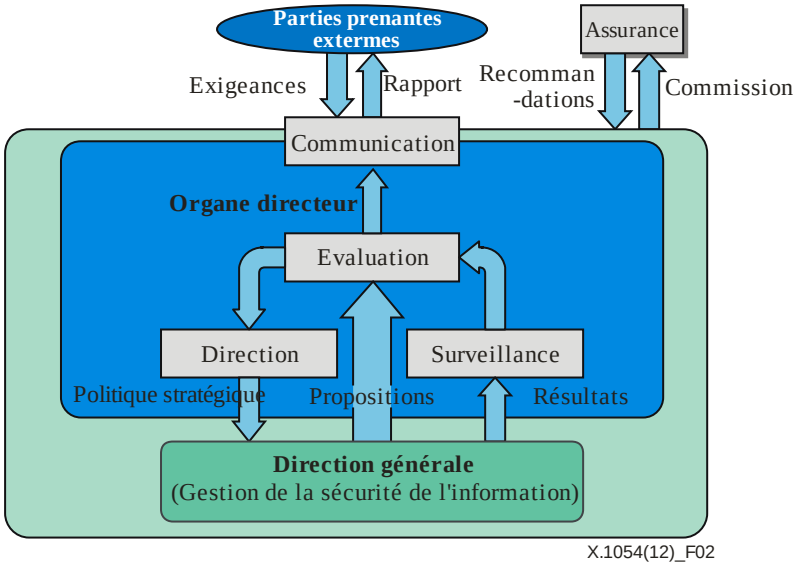

Figure 2 – Mise en œuvre du modèle de gouvernance de la sécurité de l'information

5.3.2 Evaluer

"L'évaluation" est le processus de gouvernance qui consiste à examiner le niveau effectif et prévu de réalisation des objectifs de sécurité à partir des processus actuels et des changements prévus, puis à déterminer les éventuels ajustements nécessaires pour optimiser la réalisation des objectifs stratégiques dans l'avenir.

Pour mener à bien le processus d'"évaluation", l'organe directeur devrait:

- faire en sorte que les initiatives prises par l'organisation tiennent compte des questions liées à la sécurité de l'information;
- tirer les enseignements des résultats obtenus en matière de sécurité de l'information, établir des priorités et prendre les mesures nécessaires.

Pour mener à bien le processus d'"évaluation", la direction générale devrait:

- faire en sorte que la sécurité de l'information favorise et soutienne la réalisation des objectifs de l'organisation;
- soumettre à l'organe directeur de nouveaux projets sur la sécurité de l'information ayant une grande incidence.

5.3.3 Direction

La "direction" est le processus de gouvernance dans le cadre duquel l'organe directeur donne des orientations sur les objectifs de sécurité de l'information et la stratégie à mettre en œuvre. Il peut s'agir de modifier le niveau et l'affectation des ressources ou l'ordre de priorité des activités, ou d'approuver des politiques ainsi que des plans d'acceptation des risques matériels et de gestion des risques.

Pour mener à bien le processus de "direction", l'organe directeur devrait:

- déterminer le niveau de risque accepté par l'organisation;
- approuver la stratégie et la politique en matière de sécurité de l'information;
- engager les investissements et les ressources nécessaires.

Pour mener à bien le processus de "direction", la direction générale devrait:

- élaborer et appliquer une stratégie et une politique en matière de sécurité de l'information;
- faire concorder les objectifs de la sécurité de l'information avec ceux de l'organisation;
- promouvoir une véritable culture de la sécurité de l'information.

5.3.4 Surveiller

La "surveillance" est le processus de gouvernance qui permet à l'organe directeur d'évaluer dans quelle mesure les objectifs stratégiques sont atteints.

Pour mener à bien le processus de "surveillance", l'organe directeur devrait:

- évaluer l'efficacité des activités de gestion de la sécurité de l'information;
- veiller au respect des obligations internes et externes;
- examiner l'évolution du contexte économique, juridique et réglementaire et l'incidence que les changements pourraient avoir sur les risques liés à l'information.

Pour mener à bien le processus de "surveillance", la direction générale devrait:

- choisir des critères de performance appropriés du point de vue de l'entreprise;
- communiquer à l'organe directeur les résultats obtenus en matière de sécurité de l'information, y compris le niveau d'efficacité des mesures déjà identifiées par l'organe directeur et leurs incidences sur l'organisation;
- alerter l'organe directeur sur les faits nouveaux ayant une incidence sur les risques liés à l'information et sur la sécurité de l'information.

5.3.5 Communiquer

La "communication" est le processus de gouvernance bidirectionnel par lequel l'organe directeur et les parties prenantes échangent des informations sur la sécurité de l'information en fonction de leurs besoins particuliers.

L'une des méthodes de "communication" consiste à établir des rapports sur l'état de la sécurité de l'information qui présentent aux parties prenantes des renseignements sur les activités menées dans ce domaine et les problèmes rencontrés. On trouvera dans les Annexes A et B des exemples de ces rapports.

Pour mener à bien le processus de "communication", l'organe directeur devrait:

- informer les parties prenantes externes que l'organisation applique un niveau de sécurité de l'information adapté à la nature de ses activités;
- communiquer à la direction générale les résultats des évaluations extérieures éventuelles qui ont fait apparaître des problèmes de sécurité de l'information et demander que des mesures correctives soient prises;
- prendre en considération les informations concernant les obligations réglementaires, les attentes des parties prenantes et les besoins de l'entreprise en matière de sécurité de l'information.

Pour mener à bien le processus de "communication", la direction générale devrait:

- informer l'organe directeur de tout problème qui doit retenir son attention et appelle éventuellement une décision;
- donner aux parties prenantes concernées des instructions concernant les mesures détaillées à prendre à l'appui des directives et des décisions de l'organe directeur.

5.3.6 Assurer

"L'assurance" est le processus de gouvernance par lequel l'organe directeur fait procéder à des audits, à des examens ou à des certifications indépendants et objectifs, qui permettront d'identifier et de valider les objectifs et les mesures liés à la mise en œuvre des activités de gouvernance et à l'exécution de tâches visant à atteindre le niveau de sécurité de l'information voulu.

Pour mener à bien le processus d'"assurance", l'organe directeur devrait:

- demander des avis indépendants et objectifs pour déterminer dans quelle mesure il satisfait à son obligation de rendre des comptes pour le niveau de sécurité de l'information voulu.

Pour mener à bien le processus d'"assurance", la direction générale devrait:

- appuyer les audits, les examens ou les certifications demandés par l'organe directeur.

Annexe A

Exemple de rapport sur l'état de la sécurité de l'information

(La présente annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale.)

Une organisation peut élaborer un rapport sur l'état de la sécurité de l'information et s'en servir comme outil de communication sur la sécurité de l'information en le transmettant aux parties prenantes.

L'organisation devrait choisir et arrêter le format et le contenu du rapport sur l'état de la sécurité de l'information. L'Annexe A donne un exemple de rapport d'audit sur la sécurité de l'information indiquant que les conditions sont respectées.

Tableau A – Rapport sur l'état de la sécurité de l'information

La direction a pu constater que, pendant la période allant du **mmm** au **nnn**, les contrôles et les procédures en matière de sécurité de l'information, effectués selon les critères définis dans **xyz** (par exemple, normes de la série 27000, COBIT), concernant les procédures et systèmes opérationnels de l'organisation et complétés par des contrôles de gestion de haut niveau étaient suffisamment efficaces pour avoir une assurance raisonnable que les objectifs définis en matière de contrôle de la sécurité de l'information pour ce qui est de la confidentialité, de l'intégrité et de la disponibilité ont été atteints. La direction a remis à **ABC**, en sa qualité de vérificateur extérieur de la sécurité de l'information, une lettre de déclaration à cet effet. Le Conseil d'administration a chargé ABC d'examiner les déclarations de la direction concernant le contrôle de la sécurité de l'information. Cet examen a été mené conformément aux normes établies et a consisté à évaluer la conception et l'efficacité des contrôles et procédures en matière de sécurité de l'information au moyen d'un test par échantillonnage. A cet égard, **ABC** a communiqué à la direction un avis selon lequel les résultats des tests effectués montrent que, sauf exceptions spécifiques, selon les critères de gestion identifiés dans la norme **xyz** (par exemple, normes de la série 27000, COBIT), les contrôles étaient à tous égards importants efficaces. L'intégralité de la déclaration de la direction et le rapport du vérificateur extérieur avec les éventuelles exceptions identifiées concernant les contrôles de sécurité de l'information, ont été examinés avec le comité d'audit et transmis à tous les membres du Conseil d'administration. Des exemplaires sont à la disposition des parties prenantes sur demande.

NOTE – Les mentions "nn", "mmm", "xyz" et "ABC" sont des noms fictifs qui devraient être remplacés par des dates et des noms précis dans les déclarations réelles.

Annexe B

Exemple de rapport détaillé sur l'état de la sécurité de l'information

(La présente annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale.)

La présente Annexe donne un exemple de rapport sur l'état de la sécurité de l'information avec un contenu détaillé. Ce type de rapport est particulièrement utile pour les organisations qui pensent améliorer leur réputation en mettant en avant la sécurité qu'elles offrent, par exemple les entreprises spécialisées dans les TIC. La transparence de l'approche adoptée par l'organisation en ce qui concerne le niveau de risque qu'elle accepte en matière de sécurité et la divulgation d'informations à ce sujet contribuent également efficacement à renforcer la confiance. Ces activités permettent aux parties prenantes d'avoir une connaissance commune de la situation.

Tableau B – Rapport détaillé sur l'état de la sécurité de l'information

Introduction

- **Portée** (stratégie, politiques, normes), **périmètre** (unités géographique/organisationnelles), **période couverte** (mois/trimestre/semestre/année)

Situation générale

- Satisfaisante/pas encore satisfaisante/non satisfaisante

Mise à jour (s'il y a lieu)

- Progrès accomplis dans la mise en œuvre de la stratégie de sécurité de l'information

  Eléments menés à bien/en cours/prévus
- Changements apportés au système de gestion de la sécurité de l'information

  Révision de la politique en matière de système de gestion de la sécurité de l'information (ISMS), structure organisationnelle pour mettre en œuvre le système ISMS (y compris l'attribution des responsabilités)
- Progrès accomplis dans la certification

  (Nouvelle) certification du système ISMS, audits certifiés de la sécurité de l'information
- Budget/personnel/formation
  Situation financière, dotation en personnel adaptée, qualifications dans le domaine de la sécurité de l'information
- Autres activités liées à la sécurité de l'information

  Participation de la direction à la continuité des activités, campagnes de sensibilisation, assistance pour les audits internes/externes

Questions importantes (le cas échéant)

- Résultats des évaluations de la sécurité de l'information

  Recommandations, solutions proposées par la direction, plans d'action, échéances
- Progrès réalisés en ce qui concerne la suite donnée aux principaux rapports d'audit interne/externe

  Recommandations, solutions proposées par la direction, plans d'action, échéances
- Incidents relatifs à la sécurité de l'information

  Incidences prévues, plans d'action, échéances
- (Non-)Respect de la législation et des réglementations connexes

  Incidences prévues, plans d'action, échéances

Décision(s) requise(s) (le cas échéant)

- Ressources supplémentaires

  Ressources nécessaires pour faire en sorte que la sécurité de l'information appuie les initiatives de l'entreprise

Bibliographie

[1] Recommandation UIT-T X.1051 (2008) | ISO/CEI 27011:2008, *Technologies de l'information – Techniques de sécurité – Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002*.

[2] ISO/CEI 27001:2005, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*.

[3] ISO/CEI 27002:2005, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information*.

[4] ISO/CEI 27005:2011, *Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information*.

[5] ISO/CEI 38500:2008, *Gouvernance des technologies de l'information par l'entreprise*.

[6] ITGI, *Information Security Governance framework: 2009*.

[7] ISF, *Standard of Good Practice for Information Security: 2011*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2013