Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1208

(01/2014)

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

Sécurité du cyberespace – Cybersécurité

Indicateur de risque de cybersécurité en vue de renforcer la confiance et la sécurité dans l'utilisation des télécommunications/ technologies de l'information et de la communication

Recommandation UIT-T X.1208

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
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

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

Recommandation UIT-T X.1208

Indicateur de risque de cybersécurité en vue de renforcer la confiance et la sécurité dans l'utilisation des télécommunications/technologies de l'information et de la communication

Résumé

La Recommandation UIT-T X.1208 décrit une méthode destinée à être utilisée par les organisations pour calculer une mesure de risque à partir d'indicateurs de cybersécurité et elle dresse une liste d'indicateurs potentiels de cybersécurité.

La Recommandation UIT-T X.1208 vise à aider les organisations qui mettent en oeuvre ou exploitent une partie de l'infrastructure mondiale des technologies de l'information et de la communication à évaluer leur propre capacité en matière de cybersécurité ainsi que le risque auquel elles sont exposées. L'objet de ces lignes directrices est d'aider les organisations à déterminer comment réduire leurs risques et comment identifier les investissements de ressources qu'elles pourraient/devraient faire pour améliorer leurs capacités en matière de cybersécurité.

La Recommandation UIT-T X.1208 ne propose pas l'utilisation d'un indice ou d'un seul indicateur pour exprimer les capacités d'une organisation en matière de cybersécurité.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1208	2014-01-24	17	11.1002/1000/11950

Mots clés

Indicateur de cybersécurité, indicateur de risque de cybersécurité.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

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 de 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

Recommandation UIT-T X.1208

Indicateur de risque de cybersécurité en vue de renforcer la confiance et la sécurité dans l'utilisation des télécommunications/technologies de l'information et de la communication

1 Domaine d'application

La présente Recommandation fournit des lignes directrices en vue d'aider les organisations à définir, choisir et identifier les données à collecter (sur la base des indicateurs choisis) et indique comment utiliser ces informations pour calculer un indicateur de risque de cybersécurité (CSIR, *cybersecurity indicator of risk*). Il est à noter qu'une organisation peut créer un indicateur de risque de cybersécurité à partir d'un ensemble particulier d'indicateurs de cybersécurité (CSI, *cybersecurity indicator*) et que les départements de l'organisation peuvent quant à eux créer un indicateur de risque de cybersécurité à partir d'un ensemble particulier d'indicateurs de cybersécurité (CSI) qui leur est propre. L'indicateur de cybersécurité vise à permettre d'évaluer le niveau de compétence d'une organisation en matière de cybersécurité à un instant donné et, lorsque ce processus est répété à plusieurs reprises, il permet de déterminer les progrès réalisés par l'organisation dans la mise en oeuvre de son programme de cybersécurité au fil du temps.

Par ailleurs, la présente Recommandation dresse une liste d'indicateurs potentiels de cybersécurité et décrit une méthode à utiliser pour calculer, à partir de ces indicateurs, un indicateur de risque de cybersécurité.

La présente Recommandation vise à aider les organisations qui mettent en oeuvre ou exploitent une partie de l'infrastructure mondiale des technologies de l'information et de la communication à évaluer leurs propres capacités en matière de cybersécurité et à calculer leur indicateur de risque de cybersécurité. L'objet de ces lignes directrices est d'aider les organisations à déterminer comment améliorer la cybersécurité et comment réduire leurs risques de cybersécurité. En outre, ces lignes directrices donnent des indications concernant les investissements de ressources que les organisations pourraient/devraient faire pour améliorer leur cybersécurité.

La présente Recommandation n'est pas destinée à être utilisée pour créer un indicateur de risque de cybersécurité au niveau national. En outre, elle ne propose pas l'utilisation d'un indice ou d'un seul indicateur pour exprimer les capacités d'une organisation en matière de cybersécurité (voir le § 6.1).

NOTE 1 – Il convient de ne pas faire de comparaisons entre les organisations en ce qui concerne l'indicateur de risque de cybersécurité calculé. En effet, chaque organisation ou communauté est supposée choisir ce qu'elle juge être un ensemble approprié d'indicateurs de cybersécurité pour elle-même et est censée élaborer une méthode de mesure et des critères qui lui sont propres pour faire face aux risques et préoccupations la concernant. Dans certains cas, elle peut utiliser des informations subjectives, au lieu de données objectives. Par conséquent, il est recommandé de ne jamais comparer l'indicateur de risque de cybersécurité d'une organisation avec celui d'une autre organisation, car ce type d'indicateur dépend fortement du contexte.

NOTE 2 – Il se peut que les indicateurs décrits dans la présente Recommandation ne soient pas compatibles avec ceux qui sont définis dans d'autres secteurs d'activité, car les finalités sont différentes d'un secteur à l'autre.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 audit [b-UIT-T X.800]: analyse et examen indépendants des enregistrements et activités du système afin de s'assurer de l'adéquation des commandes du système, pour garantir le respect de la politique et des procédures opérationnelles établies, détecter les failles dans la sécurité et recommander des modifications appropriées concernant le contrôle, la politique et les procédures.

3.1.2 bot [b-UIT-T X-Sup.8]: programme logiciel automatique utilisé pour effectuer des tâches particulières conçues à des fins malveillantes. Le terme "bot" est interchangeable avec le terme "robot".

3.1.3 cybersécurité [b-UIT-T X.1205]: ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants:

– disponibilité;

– intégrité, qui peut englober l'authenticité et la non-répudiation;

– confidentialité.

3.1.4 mesure [b-ENISA]: fait de mesurer, consistant à déterminer la valeur d'une variable quantitative dans une unité de mesure (standard).

3.1.5 métrique [b-ENISA]: système de mesures connexes permettant de quantifier une certaine caractéristique d'un système, d'un élément ou d'un processus. Une métrique est composée de deux ou trois mesures.

3.1.6 correctif [b-UIT-T X.1206]: correction largement diffusée d'une vulnérabilité propre à un produit et relative à la sécurité. Méthode de mise à jour d'un fichier qui ne remplace que les parties modifiées et non la totalité du fichier.

3.1.7 information d'identification personnelle (PII, *personally identifiable information*) [b-UIT-T X.1252]: toute information: a) identifiant ou permettant d'identifier la personne à laquelle elle se rapporte, de se mettre en rapport avec elle ou de la localiser; b) permettant d'obtenir des informations d'identification ou les coordonnées d'une personne; ou c) étant ou pouvant être directement ou indirectement liée à une personne physique.

3.1.8 risque [b-ISO/CEI 27000]: effet d'incertitude concernant des objectifs.

3.1.9 gestion des risques [b-ISO/CEI 27000]: activités coordonnées visant à diriger et piloter une organisation vis-à-vis du risque.

3.1.10 certificat de sécurité [b-UIT-T X.810]: ensemble de données relatives à la sécurité délivré par une autorité de sécurité ou un tiers de confiance, qui, conjointement avec les informations de sécurité, sont utilisés pour fournir des services d'intégrité et d'authentification de l'origine des données.

3.1.11 contrôles de sécurité [b-NIST FIPS 199]: contrôles de gestion, opérationnels et techniques (mesures de protection) prescrits pour un système informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du système et de ses informations.

3.1.12 incident de sécurité [b-UIT-T E.409]: tout événement préjudiciable pouvant menacer certains aspects de la sécurité.

3.1.13 spam [b-UIT-T X.1242]: information électronique transmise d'un expéditeur à un destinataire au moyen de terminaux, tels que des ordinateurs, des téléphones mobiles, des téléphones fixes, etc., et qui est généralement non sollicitée, indésirable et nuisible pour le destinataire.

3.1.14 menace [b-ISO/CEI 27000]: cause potentielle d'un incident indésirable, susceptible de nuire à un système ou à une organisation.

3.1.15 vulnérabilité [b-UIT-T X.1500]: toute faille qui pourrait être exploitée pour violer un système ou les informations qu'il contient. (Aligné sur l'Annexe A de [b-UIT-T X.800].)

3.1.16 faille [b-UIT-T X.1500]: insuffisance ou imperfection qui, bien qu'elle ne soit pas reconnue comme étant une vulnérabilité en soi, pourrait à un certain moment devenir une vulnérabilité ou contribuer à l'apparition d'autres vulnérabilités.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 indicateur de cybersécurité: élément quelconque d'un ensemble d'indicateurs utilisés pour calculer ou mesurer le niveau de risque affectant la capacité ou la compétence d'une organisation ou d'une communauté sur le plan de la cybersécurité.

NOTE – Les indicateurs de cybersécurité sont choisis en fonction de leur pertinence, c'est-à-dire en fonction de leur lien avec les préoccupations suscitées par les risques.

3.2.2 indicateur de risque de cybersécurité: résultat de la mise en oeuvre d'une méthode de calcul d'un indicateur de risque de cybersécurité.

3.2.3 série d'indicateurs de cybersécurité: ensemble d'indicateurs de cybersécurité choisis pour calculer un indicateur de risque de cybersécurité.

NOTE – Il n'existe pas une seule et unique série d'indicateurs de cybersécurité.

3.2.4 indicateur: ce terme est interchangeable avec le terme "métrique" défini au § 3.1.5.

3.2.5 système de gestion de la sécurité de l'information: partie du système global de gestion, fondée sur une approche risque relatif à l'activité, destinée à mettre en place, implémenter, exploiter, surveiller, analyser, maintenir et améliorer la sécurité de l'information; voir le § 3.2.1 de [b-ISO/CEI 27000].

NOTE – Le système de gestion comporte une structure organisationnelle, des politiques, des activités de planification, des responsabilités, des pratiques, des procédures, des processus et des ressources.

3.2.6 programme (d'activités): série d'activités coordonnées visant à atteindre un objectif précis.

3.2.7 programme (informatique): ensemble d'instructions codées qui permettent à une machine, en particulier un ordinateur, d'exécuter une séquence voulue d'opérations.

3.2.8 source de menace: intention et méthode visant à recourir à l'exploitation délibérée d'une vulnérabilité, ou situation et méthode susceptibles de déclencher accidentellement une vulnérabilité.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ACP analyse en composantes principales

AS système autonome (*autonomous system*)

BSA Business Software Alliance

C&A certifié et homologué (*certified and accredited*)

CIS Center for Internet Security

CSI indicateur de cybersécurité (*cybersecurity indicator*)

CSIR indicateur de risque de cybersécurité (*cybersecurity indicator of risk*)

CVE vulnérabilités et expositions courantes (*common vulnerabilities and exposures*)

CYBEX échange d'informations de cybersécurité (*cybersecurity information exchange*)

DB base de données (*database*)

DDoS déni de service réparti (*distributed denial-of-service*)

DHCP protocole de configuration d'hôte dynamique (*dynamic host configuration protocol*)

DoS déni de service (*denial-of-service*)

DNS système de noms de domaine (*domain name system*)

ID identifiant

IDS système de détection des intrusions (*intrusion detection system*)

IP protocole Internet (*internet protocol*)

IPS système de prévention des intrusions (*intrusion prevention system*)

ISMS système de gestion de la sécurité de l'information (*information security management system*)

IT technologies de l'information (*information technology*)

PIB produit intérieur brut

PII information d'identification personnelle (*personally identifiable information*)

SSL couche de connecteurs sécurisés (*secure socket layer*)

TIC technologies de l'information et de la communication

TLS sécurité de la couche transport (*transport layer security*)

TTP tiers de confiance (*trusted third party*)

5 Conventions

Dans la présente Recommandation, le terme organisation doit être interprété dans un sens large. Il est entendu qu'une communauté devrait être considérée comme étant incluse dans le terme organisation. En revanche, une organisation ne devrait jamais être considérée comme étant équivalente à un pays.

6 Indicateur de cybersécurité

6.1 Introduction

De nombreux efforts ont été déployés pour mesurer la performance des technologies de l'information et de la communication (TIC), suivre les progrès réalisés et évaluer l'impact de l'utilisation des TIC pour les pouvoirs publics, les opérateurs, les chercheurs et les différents secteurs d'activité. Parmi les indicateurs propres au secteur des TIC, on peut citer par exemple le Global Cloud Computing Scorecard [b-BSA] et les métriques de sécurité publiées par le Center for Internet Security [b-CIS]. Les indicateurs décrits dans la présente Recommandation concernent certains aspects particuliers de la cybersécurité.

L'indicateur de risque de cybersécurité décrit dans la présente Recommandation associe plusieurs indicateurs de cybersécurité pour mesurer le niveau de risque affectant, à un moment donné, les capacités de cybersécurité d'une organisation ou d'une communauté et leur efficacité ainsi que l'efficience de la mise en oeuvre de contrôles de sécurité.

On peut calculer une mesure de l'indicateur de risque de cybersécurité soit à partir d'une auto-évaluation de ses capacités de cybersécurité, soit à partir d'un ensemble d'indicateurs calculés par un organisme tiers externe. La présente Recommandation est destinée à être utilisée dans le cas de l'auto-évaluation par les organisations.

Les indicateurs décrits dans la présente Recommandation peuvent être choisis sur la base des normes internationales sur le système de gestion de la sécurité de l'information [b-ISO/CEI 27001], [b-ISO/CEI 27002], [b-ISO/CEI 27003], la sécurité de réseau [b-ISO/CEI 27033-1], [b-ISO/CEI 27033-2], [b-ISO/CEI 27033-4], et d'autres spécifications [b-NIST SP 800-27], [b--NIST SP 800-30], [b-NIST SP 800-53]. Les normes internationales relatives à la gestion permettent aux organisations de concevoir, de mettre en oeuvre et de tenir à jour un ensemble cohérent de politiques, de processus et de systèmes pour gérer les risques affectant leurs ressources en informations, ce qui permet de garantir des niveaux acceptables de risque en matière de sécurité des informations. Les normes internationales relatives à la sécurité de réseau définissent et décrivent les concepts associés à la sécurité de réseau et donnent des indications sur la gestion de la sécurité de réseau. Les autres spécifications définissent le concept de base des contrôles utilisés pour réduire les risques affectant les ressources en informations et indiquent comment gérer les risques dans l'environnement TIC des organisations.

Les indicateurs peuvent être regroupés par activités: gestion des incidents, gestion des vulnérabilités, gestion des correctifs, sécurité des applications, gestion de la configuration et aspects financiers.

La présente Recommandation ne propose pas l'utilisation d'un indice ou d'un seul indicateur pour exprimer les capacités de cybersécurité d'une organisation. En effet, la sécurité d'une organisation dépend de son maillon le plus faible et l'utilisation d'un indice pour exprimer les capacités de cybersécurité d'une organisation ne rend pas compte correctement des incidences potentielles résultant du maillon le plus faible. La présentation d'un indicateur de risque de cybersécurité sous la forme d'un nombre unique peut induire en erreur ceux qui sont censés utiliser ce nombre, et pourrait aussi créer de fausses attentes parmi ceux qui sont censés utiliser ce nombre dans les processus décisionnels. En effet, lorsque plusieurs indicateurs sont regroupés et normalisés pour former un seul nombre (c'est-à-dire un indice), l'existence et l'importance des failles de cybersécurité d'une organisation ne sont plus évidentes. Il serait donc inapproprié d'utiliser cet indice pour indiquer que les capacités de cybersécurité d'une organisation sont satisfaisantes ou d'envisager d'utiliser cet indice de cybersécurité pour comparer les capacités de cybersécurité de différentes organisations.

6.2 Principes généraux applicables aux indicateurs de cybersécurité

Le présent paragraphe décrit les principes généraux à prendre en considération lors de l'établissement d'indicateurs de cybersécurité.

- Pour calculer un indicateur de risque de cybersécurité, il est préférable d'utiliser un ensemble d'indicateurs adoptés à l'échelle mondiale.
- Il convient de choisir des indicateurs de cybersécurité qui puissent être utilisés pour mesurer le niveau de compétence, à un moment donné, d'une organisation ou d'une communauté en matière de cybersécurité face aux menaces ou pour mesurer les progrès réalisés dans la mise en oeuvre d'un programme de sécurité de l'information.
- Il convient de choisir des indicateurs de cybersécurité qui permettent de garantir l'exactitude et la confidentialité des données brutes à collecter et à utiliser pour calculer l'indicateur de risque de cybersécurité.
- Les processus de collecte doivent conserver l'intégrité des données brutes à utiliser pour calculer l'indicateur de risque de cybersécurité.
- Il est également préférable d'utiliser des indicateurs qui puissent aider les décideurs à mesurer la performance de la mise en oeuvre de la politique de sécurité de l'information et à suivre les progrès réalisés dans la mise en oeuvre d'un programme de cybersécurité.
- Il convient d'établir de nouveaux indicateurs ou de mettre à jour les indicateurs existants dans les meilleurs délais compte tenu de l'évolution rapide des services et technologies TIC.

6.3 Lignes directrices relatives au choix des indicateurs de cybersécurité

Lors du choix des indicateurs à utiliser pour calculer un indicateur de risque de cybersécurité, il peut être nécessaire pour une organisation de choisir des indicateurs qui l'aideront à atteindre ses buts et objectifs. A titre d'exemple, les organisations peuvent choisir des indicateurs en fonction des activités les plus importantes.

En particulier, un indicateur de cybersécurité devrait:

- permettre de mesurer le principal impact sur les résultats en termes de performance;
- pouvoir être utilisé pour résoudre des problèmes au niveau des systèmes, au niveau du programme ou aux deux niveaux, selon le cas;
- permettre de mesurer les progrès réalisés dans la mise en oeuvre d'un programme de cybersécurité, de contrôles de sécurité spécifiques et des politiques et procédures associées en matière de cybersécurité;
- permettre de mesurer des aspects utiles pour déterminer l'efficacité et l'efficience d'un programme de cybersécurité;
- permettre de mesurer l'impact positif ou négatif d'un programme de cybersécurité sur la mission d'une organisation;
- permettre de mesurer la performance des politiques de cybersécurité, et d'obtenir des résultats au niveau des systèmes, au niveau du programme ou aux deux niveaux;
- permettre de mesurer les impacts positifs et négatifs sur la vie quotidienne des utilisateurs.

En outre, lors du choix d'un indicateur de cybersécurité, il convient de veiller à pouvoir collecter les données brutes de manière précise et fiable. Pendant tout le processus de mesure, il est nécessaire de garantir la disponibilité des données brutes, l'intégrité des données utilisées et la protection de la confidentialité des données.

6.4 Classement des indicateurs

On distingue trois types d'indicateurs suivant leur nature: mise en oeuvre, efficacité/efficience et impact. Les indicateurs de mise en oeuvre sont utilisés pour montrer les progrès réalisés dans la mise en oeuvre d'un programme de sécurité de l'information, de mesures de protection de la sécurité spécifiques et des politiques et procédures de sécurité associées. Ils se subdivisent en deux sous-types: les indicateurs de mise en oeuvre au niveau du programme et les indicateurs de mise en oeuvre au niveau des systèmes. Comme exemple d'indicateur de mise en oeuvre au niveau des systèmes, on peut citer le pourcentage de membres du personnel de sécurité des systèmes informatiques qui ont reçu une formation à la sécurité.

Les indicateurs d'efficacité/efficience peuvent être utilisés pour vérifier si les processus au niveau du programme et les contrôles de sécurité au niveau des systèmes sont mis en oeuvre correctement, s'ils fonctionnent comme prévu, et s'ils satisfont aux buts et objectifs voulus. Ils portent sur deux aspects des résultats de mise en oeuvre des contrôles de sécurité: l'efficacité (robustesse) et l'efficience (rapidité) du résultat. Comme exemple d'indicateur d'efficacité, on peut citer le pourcentage d'incidents de sécurité de l'information dus à un contrôle d'accès mal configuré; comme exemple d'indicateur d'efficience, on peut citer le pourcentage d'éléments des systèmes dont la maintenance est réalisée au moment prévu.

Les indicateurs d'impact peuvent être utilisés pour spécifier l'impact de la sécurité de l'information sur la mission d'une organisation. Ils peuvent être utilisés pour quantifier les réductions de coûts engendrées par le programme de sécurité de l'information, les coûts encourus pour faire face aux incidents de sécurité de l'information, le degré de confiance accordé par le public au programme de sécurité de l'information, ou d'autres impacts de la sécurité de l'information sur la mission. Comme exemple d'indicateur d'impact, on peut citer le pourcentage de dépenses consacrées par l'organisation à la sécurité de l'information par rapport aux dépenses totales consacrées aux systèmes informatiques.

En outre, les indicateurs peuvent être classés suivant les activités: gestion des incidents, gestion des vulnérabilités, gestion des correctifs, sécurité des applications, sécurité de la configuration, aspects financiers, sécurité des données et du réseau, etc.

7 Processus d'établissement d'indicateurs de cybersécurité

7.1 Introduction

La série d'indicateurs de cybersécurité devrait être considérée comme un outil important qui peut être utilisé pour évaluer si la politique de sécurité de l'information est appliquée de manière judicieuse et pour déterminer la situation à un moment donné en matière de sécurité de l'information dans une organisation.

7.2 Méthode d'élaboration d'une série d'indicateurs de cybersécurité

L'élaboration d'une série d'indicateurs de cybersécurité est une tâche complexe qui doit être entreprise par des professionnels très compétents ayant des connaissances en économie, cybersécurité et statistiques. Pour élaborer la liste d'indicateurs de cybersécurité, il faut tenir compte du contexte de l'organisation et des différents aspects du ou des risques à mesurer.

Pour l'établissement des indicateurs de cybersécurité, il convient de tenir compte du fait qu'un indicateur donné peut présenter une très grande variabilité – contrairement aux indicateurs avec un grand nombre d'échantillons – en raison du petit nombre d'échantillons mesurés, par exemple des incidents, sur une durée d'observation qui peut être limitée. Par conséquent, l'analyse macroscopique devrait être effectuée avec la plus grande attention.

Les étapes à suivre pour élaborer une série d'indicateurs de cybersécurité et pour rendre les informations immédiatement utilisables peuvent être les suivantes:

- identifier les indicateurs fondamentaux à choisir et à utiliser pour calculer l'indicateur de risque de cybersécurité;
- identifier les sources de données;
- adopter une marche à suivre pour les observations manquantes;
- rendre les indicateurs comparables entre eux;
- convertir les indicateurs en valeurs de mesure de risque;
- exploiter les valeurs de mesure de risque.

7.2.1 Choix des indicateurs pour calculer une mesure de risque

Le choix des indicateurs pour calculer une mesure de risque dépend de ce qui est à mesurer ainsi que de la question de savoir s'il est possible de collecter les données brutes.

NOTE – Même s'il est actuellement impossible de réaliser une mesure, on peut malgré tout envisager sérieusement de choisir un indicateur. A partir de là, il est possible que de nouveaux travaux soient engagés afin de pouvoir collecter les données nécessaires qui permettront d'évaluer correctement le risque.

Le nombre d'indicateurs peut dépendre de la mission et des objectifs de l'organisation, ou du type de technologies utilisées par l'organisation. Il est recommandé d'utiliser un large éventail d'indicateurs (par exemple, de 10 à 30 indicateurs) pour calculer la mesure de risque pour un indicateur de risque de cybersécurité. Le mélange d'indicateurs subjectifs et de mesures objectives peut influer sur la validité du calcul résultant. Il est donc recommandé d'éviter d'utiliser des indicateurs subjectifs lors de l'élaboration d'un indicateur de risque de cybersécurité. Toutefois, pour certaines activités de gestion des risques, un indicateur subjectif peut être nécessaire, de sorte qu'il est essentiel de définir avec rigueur la manière dont un indicateur subjectif doit être défini. Une fois les indicateurs choisis, il peut être souhaitable de les regrouper en différentes catégories en fonction des activités concernées (gestion des incidents, gestion des vulnérabilités, gestion des correctifs, etc.). Ainsi, les indicateurs sont plus faciles à gérer et les comparaisons plus pertinentes.

La procédure de définition des indicateurs est décrite en détail au § 7.3.

7.2.2 Sources de données

La plus ou moins grande disponibilité des données pour les indicateurs de cybersécurité peut influer sur le nombre et la qualité des indicateurs utilisés pour calculer un indicateur de risque de cybersécurité. Le fait de trop se fier à une seule source de données peut entraîner des erreurs et des omissions. Il est donc essentiel que les données soient vérifiées par rapport à différentes sources avant de les utiliser pour calculer un indicateur de risque de cybersécurité.

7.2.3 Adoption d'une marche à suivre pour les données manquantes

Lors de la collecte des mesures de risque pour un indicateur de cybersécurité, il se peut, dans certains cas, que des données manquent ou ne soient pas disponibles. En pareils cas, on peut soit laisser les données en blanc – auquel cas l'organisation n'affectera aucune valeur à l'indicateur correspondant – soit recourir à une extrapolation pour estimer les données manquantes. Le fait de laisser les données en blanc risque d'exclure certains aspects d'un indicateur de cybersécurité. Quant à l'extrapolation, elle peut amplifier la valeur des données et gonfler les résultats de calcul. Il faut trouver un compromis entre extrapolation et omission, compte tenu de la valeur des données ou de l'importance des indicateurs. Il convient éventuellement de réaliser un test de sensibilité afin de déterminer dans quelle mesure les fluctuations de la valeur extrapolée ou le remplacement des données laissées en blanc par une valeur estimée influent sur les résultats calculés.

7.2.4 Transformation des données

La phase de transformation comporte deux étapes: la conversion des valeurs absolues en valeurs relatives et la conversion des valeurs relatives des indicateurs en un indicateur de risque de cybersécurité. Les valeurs absolues sont généralement rendues comparables en les divisant par le nombre total d'éléments. Il est possible que de nombreux indicateurs soient fournis après avoir été transformés, ce qui permet de se passer de cette étape.

7.3 Processus de définition des indicateurs de cybersécurité

Le processus de définition des indicateurs de cybersécurité consiste à choisir les indicateurs qui sont appropriés pour la mission et les objectifs de l'organisation ou de la communauté. Il comporte cinq étapes: identification des intérêts des parties prenantes, définition des buts et des objectifs, examen des politiques, lignes directrices et procédures relatives à la sécurité de l'information, examen de la mise en oeuvre de la sécurité de l'information et choix des indicateurs.

L'étape 1 – Identification des intérêts des parties prenantes – consiste à identifier les parties prenantes concernées et leurs intérêts. Les principales parties prenantes sont le chef de l'organisation, le directeur de l'informatique, le directeur de la sécurité, le responsable de la sécurité des systèmes informatiques, le gestionnaire du programme, l'administrateur du réseau, les ingénieurs sécurité et le personnel d'appui aux systèmes informatiques. Dans cette étape, on compile tous les intérêts en matière de mesure de la sécurité de l'information. Chaque partie prenante peut demander un ensemble différent d'indicateurs correspondant à son domaine de responsabilité.

L'étape 2 – Définition des buts et des objectifs – consiste à identifier les buts et les objectifs en matière de sécurité de l'information, qui peuvent être exprimés sous forme de politiques, d'exigences, de lignes directrices ou d'orientations. Les buts et objectifs du programme de sécurité de l'information peuvent être déterminés à partir des buts et objectifs de haut niveau de l'organisation pour assurer sa mission.

L'étape 3 – Examen des politiques, lignes directrices et procédures relatives à la sécurité de l'information – consiste à décrire en détail la manière dont les contrôles de sécurité devraient être mis en oeuvre dans les politiques et procédures propres à l'organisation.

L'étape 4 – Examen de la mise en oeuvre de la sécurité de l'information – consiste à examiner les indicateurs existants et les répertoires de données pertinents qui peuvent être utilisés pour définir de nouveaux indicateurs.

L'étape 5 – Choix des indicateurs – consiste à choisir et à définir au besoin des indicateurs des trois types décrits au § 6.4, c'est-à-dire à choisir une série d'indicateurs de mise en oeuvre, d'efficience/efficacité et d'impact, et, si nécessaire, à définir au besoin de nouveaux indicateurs.

8 Indicateurs de cybersécurité potentiels

Le présent paragraphe décrit divers indicateurs de cybersécurité qui ont été identifiés comme étant des indicateurs fondamentaux et qui peuvent être utilisés pour élaborer une série d'indicateurs de cybersécurité pour une organisation. Les indicateurs peuvent être classés en trois catégories: indicateurs de base, indicateurs recommandés et indicateurs facultatifs. Ils peuvent aussi être classés en trois catégories selon leur nature: indicateurs de mise en oeuvre, indicateurs d'efficacité/efficience et indicateurs d'impact. Le niveau d'exigence associé à chaque indicateur n'est pas défini dans la présente Recommandation, mais devrait être précisé par les organisations en fonction de leur politique de sécurité. En outre, les organisations pourront définir d'autres indicateurs adaptés à leur propre situation et sont invitées à le faire.

Les indicateurs décrits dans le présent paragraphe (voir les Tableaux 8-1 à 8-30) sont destinés à être utilisés par une organisation; ils peuvent toutefois s'appliquer à une communauté si l'on agrège les indicateurs des organisations faisant partie de la communauté.

On distingue les indicateurs pour lesquels il est souhaitable d'avoir une valeur élevée, ceux pour lesquels il est souhaitable d'avoir une valeur faible et ceux pour lesquels il n'est pas évident de savoir s'il vaut mieux une valeur élevée ou une valeur faible.

Tableau 8-1 – Indicateur 1: Gestion des vulnérabilités (au niveau du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Pourcentage de vulnérabilités à fort impact qui ont été réduites.
But	L'organisation devrait faire face aux vulnérabilités connues en temps voulu.
Indicateur	Pourcentage de vulnérabilités à fort impact qui ont été réduites dans le délai défini par l'organisation après leur découverte.
Formule	(Nombre total de vulnérabilités à fort impact réduites en temps voulu/nombre total de vulnérabilités à fort impact recensées) × 100.
Données brutes	• Nombre de vulnérabilités recensées pendant la période spécifiée par l'organisation. (Il est à noter que le nombre de vulnérabilités à fort impact recensées pendant la période spécifiée par l'organisation doit être calculé à partir des données brutes.) • Nombre de vulnérabilités à fort impact réduites pendant la période.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	Recommandation UIT-T X.1521, Système d'évaluation des vulnérabilités courantes, [b-UIT-T X.1521] et Recommandation UIT-T X.1520, Vulnérabilités et expositions courantes, [b-UIT-T X.1520].

Tableau 8-2 – Indicateur 2: Tenue à jour des journaux d'audit (au niveau des systèmes, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Pourcentage de dispositifs de point d'extrémité pour lesquels un journal d'audit est tenu à jour.
But	L'organisation devrait tenir à jour un journal d'audit des systèmes afin de rechercher les activités inappropriées des points d'extrémité.
Indicateur	Pourcentage de dispositifs de point d'extrémité pour lesquels un journal d'audit est tenu à jour.
Formule	(Nombre total de dispositifs de point d'extrémité avec un journal d'audit/nombre total de dispositifs de point d'extrémité) × 100.
Données brutes	• Nombre de dispositifs d'utilisateur final pour lesquels un journal d'audit est tenu à jour par un serveur centralisé ou un dispositif de point d'extrémité. • Nombre total de dispositifs de point d'extrémité.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-3 – Indicateur 3: Réaction en cas d'incident (au niveau des systèmes et au niveau du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Réaction en cas d'incident.
But	L'organisation devrait signaler les incidents en temps voulu pour chaque catégorie d'incident.
Indicateur	Pourcentage d'incidents signalés dans le délai requis pour chaque catégorie applicable.
Formule	(Nombre d'incidents signalés en temps voulu/nombre total d'incidents signalés) × 100, pour chaque catégorie.
Données brutes	• Nombre d'incidents signalés dans le délai défini par l'organisation. • Nombre total d'incidents signalés.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	Recommandation UIT-T X.1544, Liste et classification des schémas d'attaque courants, [b-UIT-T X.1544]

Tableau 8-4 – Indicateur 4: Délai moyen pour réduire les vulnérabilités (au niveau des systèmes et au niveau du programme, valeur faible souhaitable)

Champ	Données
ID de l'indicateur	Délai moyen pour réduire les vulnérabilités.
But	L'indicateur est conçu pour indiquer la performance de l'organisation pour faire face aux vulnérabilités recensées. Moins il faut de temps pour réduire les vulnérabilités, plus l'organisation est à même de réagir efficacement afin de réduire le risque d'exploitation des vulnérabilités.
Indicateur	Le délai moyen pour réduire les vulnérabilités quantifie le délai nécessaire en moyenne pour réduire les vulnérabilités recensées dans l'organisation.
Formule	Somme (date_de_réduction – date_de_détection)/nombre (vulnérabilités_réduites)
Données brutes	• Date de détection des vulnérabilités. • Date de réduction des vulnérabilités. • Nombre total de vulnérabilités détectées. • Nombre total de vulnérabilités réduites signalées.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	Recommandation UIT-T X.1521, Système d'évaluation des vulnérabilités courantes, [b-UIT-T X.1521] et Recommandation UIT-T X.1520, Vulnérabilités et expositions courantes, [b-UIT-T X.1520]

Tableau 8-5 – Indicateur 5: Utilisation d'un programme de correctifs de sécurité (au niveau des systèmes, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Programme de correctifs de sécurité.
But	Les dispositifs de point d'extrémité devraient utiliser un programme de correctifs de sécurité afin de réduire les vulnérabilités.
Indicateur	Pourcentage de dispositifs de point d'extrémité qui utilisent le système de gestion de correctifs.
Formule	(Nombre total de dispositifs de point d'extrémité utilisant un programme de correctifs de sécurité/nombre total de dispositifs de point d'extrémité) × 100.
Données brutes	• Nombre total de dispositifs de point d'extrémité utilisant le programme de correctifs de sécurité. • Nombre de dispositifs de point d'extrémité.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-6 – Indicateur 6: Délai moyen pour installer un correctif (au niveau des systèmes et au niveau du programme, valeur faible souhaitable)

Champ	Données
ID de l'indicateur	Délai moyen pour installer un correctif.
But	Le délai moyen pour installer un correctif quantifie le délai nécessaire en moyenne pour installer un correctif pour les systèmes de l'organisation. Plus les correctifs peuvent être installés rapidement, plus le délai moyen pour installer un correctif est court, et moins longtemps l'organisation exploite les systèmes dans un état connu pour être vulnérable.
Indicateur	Délai moyen nécessaire pour installer un correctif pour les systèmes de l'organisation.
Formule	Somme (date_d'installation – date_de_disponibilité)/nombre (correctifs_installés).
Données brutes	• Date d'installation. • Date de disponibilité. • Nombre total de correctifs installés.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-7 – Indicateur 7: Délai moyen pour changer de configuration (au niveau des systèmes et au niveau du programme, valeur faible souhaitable)

Champ	Données
ID de l'indicateur	Délai moyen pour changer de configuration.
But	Le délai moyen pour changer de configuration quantifie le délai nécessaire en moyenne pour effectuer un changement dans les systèmes de l'organisation. Plus le changement peut être effectué rapidement, moins les systèmes de l'organisation restent longtemps dans un état connu pour être instable.
Indicateur	Délai moyen nécessaire pour changer de configuration dans les systèmes de l'organisation.
Formule	Somme (date_d'achèvement – date_de_soumission)/nombre (changements_effectués)
Données brutes	• Date d'achèvement. • Date de soumission. • Nombre total de changements effectués.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-8 – Indicateur 8: Couverture de l'évaluation des risques (au niveau des systèmes et au niveau du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Couverture de l'évaluation des risques.
But	L'organisation devrait mener une évaluation des risques couvrant le plus grand nombre possible d'applications présentes dans ses systèmes.
Indicateur	Pourcentage d'applications qui ont fait l'objet d'une évaluation des risques à un moment donné.
Formule	Nombre (applications_ayant_fait_l'objet_d'une_évaluation_des_risques)/nombre (applications) × 100.
Données brutes	• Nombre d'applications ayant fait l'objet d'une évaluation des risques. • Nombre d'applications.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-9 – Indicateur 9: Couverture du programme de détection et de traitement des logiciels malveillants (au niveau des systèmes, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Programme de détection et de traitement des logiciels malveillants
But	Les dispositifs d'utilisateur final devraient utiliser un programme antivirus afin d'héberger moins de logiciels malveillants et de virus.
Indicateur	Pourcentage de dispositifs de point d'extrémité utilisant un programme de détection et de traitement des logiciels malveillants.
Formule	(Nombre total de dispositifs de point d'extrémité utilisant un programme de détection et de traitement des logiciels malveillants/nombre total de dispositifs de point d'extrémité) × 100.
Données brutes	• Nombre total de dispositifs de point d'extrémité utilisant un programme antivirus. • Nombre de dispositifs de point d'extrémité.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-10 – Indicateur 10: Couverture de la planification d'urgence (au niveau du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Tests du plan d'urgence.
But	L'organisation devrait mener des tests du plan d'urgence pour les systèmes informatiques.
Indicateur	Pourcentage de systèmes informatiques pour lesquels des tests du plan d'urgence ont été menés.
Formule	(Nombre de systèmes de point d'extrémité pour lesquels des tests du plan d'urgence ont été menés/nombre total de systèmes de point d'extrémité) × 100.
Données brutes	• Nombre de systèmes informatiques pour lesquels des tests du plan d'urgence ont été menés. • Nombre de systèmes de point d'extrémité.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-11 – Indicateur 11: Evaluation de la sécurité (au niveau du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Pourcentage de systèmes informatiques ayant passé avec succès l'évaluation de la sécurité.
But	Les systèmes de point d'extrémité de l'organisation devraient être certifiés et homologués avant leur installation afin de garantir un environnement sûr et fiable pour le personnel, les installations et les produits.
Indicateur	Pourcentage de nouveaux systèmes de point d'extrémité qui ont été certifiés et homologués avant leur installation.
Formule	(Nombre de systèmes informatiques qui ont été certifiés et homologués/nombre total de systèmes informatiques) × 100.
Données brutes	• Nombre de nouveaux systèmes de point d'extrémité qui ont été certifiés et homologués. • Nombre de systèmes de point d'extrémité.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-12 – Indicateur 12: Engagement de sécurité (au niveau du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Engagement de sécurité ou code de conduite.
But	Les employés qui sont autorisés à accéder aux systèmes de point d'extrémité de l'organisation devraient signer un engagement de sécurité avant d'y accéder.
Indicateur	Pourcentage de membres du personnel de sécurité des systèmes informatiques qui ont signé l'engagement de sécurité.
Formule	(Nombre de membres du personnel qui sont autorisés à accéder aux systèmes après avoir signé les règles de comportement/nombre total de membres du personnel qui sont autorisés à accéder aux systèmes de point d'extrémité) × 100.
Données brutes	• Nombre d'employés qui sont autorisés à accéder aux systèmes après avoir signé l'engagement de sécurité. • Nombre d'employés qui sont autorisés à accéder aux systèmes.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Mise en oeuvre.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-13 – Indicateur 13: Contrôle d'accès à distance avec passerelle de sécurité (au niveau des systèmes/du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Points d'accès à distance protégés.
But	L'organisation devrait installer une passerelle de sécurité afin d'assurer un accès à distance protégé et de protéger ses actifs internes.
Indicateur	Pourcentage de points d'accès à distance protégés.
Formule	(Nombre de points d'accès à distance protégés qui utilisent une passerelle de sécurité/nombre total de points d'accès à distance dans l'organisation) × 100.
Données brutes	• Nombre de points d'accès à distance protégés qui utilisent une passerelle de sécurité. • Nombre de points d'accès à distance protégés.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-14 – Indicateur 14: Contrôle d'accès à distance avec fonction de sécurité assurant la prévention ou la détection des intrusions (au niveau des systèmes/du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Points d'accès à distance protégés.
But	L'organisation devrait utiliser une fonction de sécurité assurant la prévention ou la détection des intrusions afin de protéger ses actifs internes.
Indicateur	Pourcentage de points d'accès à distance protégés.
Formule	(Nombre de points d'accès à distance qui utilisent la fonction de sécurité assurant la prévention ou la détection des intrusions/nombre total de points d'accès à distance) × 100.
Données brutes	• Nombre de points d'accès à distance protégés qui utilisent la fonction de sécurité assurant la prévention ou la détection des intrusions. • Nombre de points d'accès à distance.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-15 – Indicateur 15: Contrôle d'accès sans fil (au niveau des systèmes/du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Points d'accès sans fil protégés.
But	L'organisation devrait prévoir des points d'accès sans fil protégés afin de protéger le réseau interne contre tout accès non autorisé.
Indicateur	Pourcentage de points d'accès sans fil protégés.
Formule	(Nombre de points d'accès sans fil protégés/nombre total de points d'accès sans fil) × 100.
Données brutes	• Nombre de points d'accès sans fil protégés. • Nombre de points d'accès sans fil.
Fréquence	Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-16 – Indicateur 16: Sécurité du personnel (au niveau des systèmes/au niveau du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Contrôle de sécurité du personnel.
But	Pour accéder aux systèmes de point d'extrémité, le personnel autorisé devrait avoir la permission de l'organisation.
Indicateur	Pourcentage d'individus contrôlés avant de pouvoir accéder aux systèmes de point d'extrémité de l'organisation.
Formule	(Nombre d'individus contrôlés/nombre total d'individus disposant d'un accès) × 100.
Données brutes	• Nombre d'individus contrôlés. • Nombre d'individus.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Mise en oeuvre.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-17 – Indicateur 17: Protection des informations d'identification personnelle (PII) (au niveau des systèmes/du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Pourcentage d'informations d'identification personnelle sensibles protégées.
But	L'organisation devrait protéger ses informations d'identification personnelle sensibles en les cryptant.
Indicateur	Pourcentage d'informations d'identification personnelle sensibles protégées.
Formule	(Nombre d'informations d'identification personnelle sensibles cryptées/nombre total d'informations d'identification personnelle) × 100.
Données brutes	• Nombre d'informations d'identification personnelle protégées. • Nombre total d'informations d'identification personnelle.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Efficacité/efficience et mise en oeuvre.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-18 – Indicateur 18: Protection des données de secours (au niveau des systèmes/du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Taux d'inspection de l'intégrité des données de secours.
But	L'organisation devrait assurer la protection de l'intégrité des données de secours.
Indicateur	Pourcentage de données de secours dont l'intégrité est protégée.
Formule	(Quantité de données de secours dont l'intégrité est protégée/quantité totale de données de secours) × 100.
Données brutes	• Quantité de données de secours dont l'intégrité est protégée. • Quantité totale de données de secours.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Efficacité/efficience et mise en oeuvre.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-19 – Indicateur 19: Couverture du système certifié de gestion de la sécurité (par exemple ISMS) (au niveau des systèmes/du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Couverture du système de gestion.
But	Les systèmes de point d'extrémité de l'organisation devraient être couverts par le système certifié de gestion de la sécurité (par exemple ISMS).
Indicateur	Pourcentage de systèmes de point d'extrémité couverts par le système certifié de gestion de la sécurité.
Formule	(Nombre de systèmes de point d'extrémité couverts par le système certifié de gestion de la sécurité (par exemple ISMS)/nombre total de systèmes de point d'extrémité) × 100.
Données brutes	• Nombre de systèmes de point d'extrémité couverts par le système certifié de gestion de la sécurité (par exemple ISMS). • Nombre total de systèmes de point d'extrémité.
Fréquence	Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Efficacité/efficience et mise en oeuvre.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-20 – Indicateur 20: Utilisation d'un serveur sécurisé (au niveau des systèmes/au niveau du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Utilisation d'un serveur sécurisé.
But	Les services de réseau de l'organisation devraient échanger des informations au moyen d'un tunnel sécurisé pour l'accès à distance.
Indicateur	Pourcentage de services de réseau qui utilisent un tunnel sécurisé, par exemple TLS, SSL ou secure shell.
Formule	(Nombre de services de réseau qui utilisent un tunnel sécurisé/nombre total de services de réseau) × 100.
Données brutes	• Nombre de services de réseau qui utilisent un canal sécurisé. • Nombre total de services de réseau.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Efficacité/efficience et mise en oeuvre.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	
NOTE – Le serveur sécurisé (mentionné dans l'intitulé de l'indicateur) peut être mis en oeuvre de diverses manières pour disposer d'un tunnel sécurisé entre les points d'extrémité: serveur protégé par SSL/TLS, secure shell, etc.	

Tableau 8-21 – Indicateur 21: Taux de réception de spams (programme, valeur faible souhaitable)

Champ	Données
ID de l'indicateur	Taux de réception de spams
But	L'organisation devrait utiliser un filtre antispam pour bloquer les spams par courrier électronique avant qu'ils ne parviennent aux employés.
Indicateur	Pourcentage d'employés qui ont reçu davantage de spams par courrier électronique que le nombre défini par l'organisation pendant la période définie.
Formule	(Nombre d'employés qui ont reçu un certain nombre de spams par courrier électronique/nombre total d'employés) × 100.
Données brutes	• Nombre d'employés qui ont reçu un nombre de spams par courrier électronique dépassant le nombre défini par l'organisation pendant la période définie. • Nombre d'employés.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Efficacité/efficience et mise en oeuvre.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-22 – Indicateur 22: Programme de sensibilisation dans l'organisation (valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Programme de sensibilisation dans l'organisation.
But	Les employés devraient avoir participé à un programme de sensibilisation.
Indicateur	Pourcentage d'employés qui ont participé à un programme de sensibilisation.
Formule	(Nombre d'employés qui ont participé à un programme de sensibilisation/nombre total d'employés) × 100.
Données brutes	• Nombre d'employés qui ont participé à un programme de sensibilisation. • Nombre d'employés.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Efficacité/efficience et mise en oeuvre.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-23 – Indicateur 23: Formation et éducation à la sécurité (au niveau du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Formation et éducation à la sécurité.
But	Les employés de l'organisation devraient suivre la formation et l'éducation à la sécurité afin de réagir de manière appropriée en cas d'incidents de sécurité.
Indicateur	Pourcentage d'employés qui ont suivi la formation et l'éducation à la sécurité pendant la période définie par l'organisation.
Formule	(Nombre d'employés qui ont suivi la formation et l'éducation à la sécurité/nombre total d'employés) × 100.
Données brutes	• Nombre d'employés qui ont suivi la formation et l'éducation à la sécurité. • Nombre d'employés.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Impact/mise en oeuvre.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-24 – Indicateur 24: Rôle et responsabilité en matière de cybersécurité (au niveau du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Rôle et responsabilité.
But	L'organisation devrait recruter et organiser une équipe s'occupant d'activités liées à la cybersécurité.
Indicateur	Pourcentage de membres du personnel s'occupant d'activités liées à la cybersécurité.
Formule	(Nombre de membres du personnel s'occupant d'activités liées à la cybersécurité/nombre total de membres du personnel informatique) × 100.
Données brutes	• Nombre de membres du personnel s'occupant d'activités liées à la cybersécurité. • Nombre total de membres du personnel informatique.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Impact/mise en oeuvre.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-25 – Indicateur 25: Infection par des logiciels malveillants (au niveau du programme et au niveau des systèmes, valeur faible souhaitable)

Champ	Données
ID de l'indicateur	Dispositifs de point d'extrémité infectés par des logiciels malveillants.
But	Les dispositifs de point d'extrémité des employés devraient être protégés contre divers logiciels malveillants.
Indicateur	Pourcentage d'ordinateurs des employés infectés par des virus ou des logiciels malveillants ou compromis par des attaquants au moyen de techniques de piratage.
Formule	(Nombre total de dispositifs de point d'extrémité infectés par des logiciels malveillants/nombre total de dispositifs de point d'extrémité) × 100.
Données brutes	• Nombre de dispositifs de point d'extrémité infectés par des virus ou des logiciels malveillants ou compromis par des attaquants au moyen de techniques de piratage. • Nombre total de dispositifs de point d'extrémité dans l'organisation.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Impact et efficacité.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-26 – Indicateur 26: Fuite d'informations d'identification personnelle (au niveau du programme)

Champ	Données
ID de l'indicateur	Fuite d'informations d'identification personnelle.
But	L'organisation devrait protéger les informations d'identification personnelle contre les fuites vers l'extérieur.
Indicateur	Pourcentage d'unités d'informations d'identification personnelle qui ont fui pendant la période définie, signalées dans un incident PII. NOTE – Ceux qui définissent cet indicateur devraient définir leur propre unité d'informations d'identification personnelle.
Formule	(Nombre d'unités d'informations d'identification personnelle qui ont fui pendant la période spécifiée par l'organisation, signalées dans un incident PII/nombre total d'unités d'informations d'identification personnelle) × 100.
Données brutes	• Nombre d'unités d'informations d'identification personnelle qui ont fui pendant la période spécifiée par l'organisation, signalées dans un incident PII. • Nombre total d'unités d'informations d'identification personnelle.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Impact.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-27 – Indicateur 27: Pourcentage du budget pour les TIC consacré à la sécurité (au niveau du programme)

Champ	Données
ID de l'indicateur	Pourcentage du budget pour les TIC de l'organisation qui est consacré à la cybersécurité.
But	L'organisation devrait prévoir un budget pour la cybersécurité dans des limites définies.
Indicateur	Pourcentage du budget pour les TIC de l'organisation qui est consacré à la cybersécurité; le budget pour la sécurité est supposé faire partie du budget pour l'informatique.
Formule	(Budget pour la cybersécurité/budget total pour les TIC) × 100.
Données brutes	• Montant du budget pour la cybersécurité. • Montant du budget total pour les TIC.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Impact.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-28 – Indicateur 28: Taux de dispositifs autorisés (valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Taux de dispositifs autorisés de l'organisation parmi tous les dispositifs.
But	L'organisation devrait suivre/contrôler/empêcher/corriger l'accès au réseau par les dispositifs (ordinateurs, éléments de réseau, imprimantes, tout objet ayant une adresse IP), sur la base d'un inventaire des dispositifs qui sont autorisés à se connecter au réseau.
Indicateur	Taux de dispositifs autorisés de l'organisation parmi tous les dispositifs.
Formule	(nombre de dispositifs autorisés/nombre de dispositifs) × 100.
Données brutes	• Nombre de dispositifs autorisés. • Nombre de dispositifs.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Impact.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau 8-29 – Indicateur 29: Taux de logiciels autorisés (valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Taux de logiciels autorisés de l'organisation parmi tous les logiciels.
But	L'organisation devrait suivre/contrôler/empêcher/corriger l'installation et l'exécution de logiciels sur les ordinateurs, sur la base d'un inventaire des logiciels approuvés.
Indicateur	Taux de logiciels autorisés de l'organisation parmi tous les logiciels.
Formule	(nombre de logiciels autorisés/nombre total de logiciels) × 100.
Données brutes	• Nombre de logiciels autorisés. • Nombre total de logiciels.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Impact.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	Recommandation UIT-T X.1528, Système commun d'énumération des éléments d'une plate-forme, [b-UIT-T X.1528] et ISO/CEI 19770-2, Technologies de l'information – Gestion des actifs logiciels – Partie 2: Etiquette d'identification du logiciel, [b-ISO/CEI 19770-2].

Tableau 8-30 – Indicateur 30: Sécurité des logiciels applicatifs (valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Taux de logiciels applicatifs de l'organisation qui sont protégés contre les principales attaques logicielles au niveau des applications (par exemple CWE top 25) parmi tous les logiciels applicatifs.
But	L'organisation devrait détecter et bloquer les attaques logicielles au niveau des applications, et générer une alerte ou envoyer un courrier électronique au personnel administratif de l'entreprise dans les 24 heures suivant la détection et le blocage.
Indicateur	Taux de logiciels applicatifs de l'organisation qui sont protégés contre les principales attaques logicielles au niveau des applications parmi tous les logiciels applicatifs.
Formule	(nombre de logiciels applicatifs qui sont protégés contre les principales attaques logicielles au niveau des applications/nombre total de logiciels applicatifs) × 100.
Données brutes	• Nombre de logiciels applicatifs qui sont protégés contre les principales attaques logicielles au niveau des applications. • Nombre total de logiciels applicatifs.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Impact.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	Recommandation UIT-T X.1524, Liste des failles courantes, [b-UIT-T X.1524] et Recommandation UIT-T X.1544, Liste et classification des schémas d'attaque courants, [b-UIT-T X.1544].

Appendice I

Exemples d'indicateurs de mesures de risque de sécurité de l'information et de métriques

(Le présent appendice ne fait pas partie intégrante de la Recommandation.)

Le présent appendice donne en exemple deux ensembles d'indicateurs de mesures de risque de sécurité de l'information et de métriques qui pourraient être utilisés pour calculer un indicateur de cybersécurité.

Le document [b-NIST SP 800-55] définit des mesures de risque envisageables au niveau des systèmes et/ou du programme, regroupées comme suit:

- Mesures de risque au niveau des systèmes:
  - contrôle d'accès;
  - audit et respect de l'obligation de rendre des comptes;
  - identification et authentification;
  - maintenance;
  - évaluation des risques.
- Mesures de risque au niveau du programme:
  - dépenses pour la sécurité, gestion des vulnérabilités;
  - sensibilisation et formation;
  - certification, homologation et évaluations de la sécurité;
  - gestion de la configuration;
  - planification d'urgence;
  - environnement physique.
- Mesures de risque au niveau du programme et au niveau des systèmes:
  - réaction en cas d'incident;
  - protection des médias;
  - planification;
  - sécurité du personnel;
  - acquisition de systèmes et communications;
  - intégrité des systèmes et des informations.

Par ailleurs, l'indice de préparation au réseau [b-NRI] du Forum économique mondial (WEF) comporte plusieurs indicateurs tandis que le taux de pénétration des serveurs sécurités [b-WEF] repose sur un certificat de couche de connecteurs sécurisés (SSL) ou un certificat de sécurité de la couche transport (TLS) propre au fournisseur.

Appendice II

Classement des indicateurs selon leur nature

(Le présent appendice ne fait pas partie intégrante de la Recommandation.)

Pour que les organisations adhèrent largement à cette Recommandation, il serait utile de recenser les mesures minimales qu'elles peuvent obtenir et utiliser sans engager de dépenses importantes.

Par exemple, l'indicateur 24 (rôle et responsabilité en matière de cybersécurité) défini au § 8 pourrait être un indicateur facile à mettre en oeuvre pour commencer, étant donné que pour le mesurer, il suffit de compter des nombres de personnes. En ce qui concerne d'autres indicateurs, il faut installer d'autres outils et/ou bases de données pour pouvoir les mesurer. Par exemple, l'indicateur 1 (gestion des vulnérabilités) nécessite que des outils et des bases de données associées de gestion des vulnérabilités soient en place. Par conséquent, les organisations qui souhaitent utiliser cet indicateur doivent examiner les avantages et les coûts qu'entraînerait la réalisation des investissements nécessaires pour disposer des informations en question. De même, l'indicateur 2 nécessite qu'une fonction de gestion des actifs des TIC soit déjà opérationnelle dans l'organisation considérée. En ce qui concerne d'autres indicateurs encore, il faut que l'organisation dispose de certaines capacités pour pouvoir les mesurer. Par exemple, l'indicateur 4 (délai moyen pour réduire les vulnérabilités) nécessite que la date de survenue soit connue, ce qui serait difficile en l'absence de capacités d'audit et d'analyse.

Le présent appendice donne un classement des indicateurs selon leur nature: ceux qui peuvent être mesurés facilement, ceux qui peuvent être mesurés à l'aide des outils et/ou des bases de données qui sont normalement présents dans une organisation, et ceux qui peuvent être mesurés si l'organisation a décidé de mettre en place des capacités de mesure améliorées.

Tableau II.I – Classement des indicateurs selon leur nature

Nature des indicateurs	Numéro de l'indicateur	ID de l'indicateur
Indicateurs qui peuvent être mesurés facilement	Indicateur 12: Engagement de sécurité	Engagement de sécurité ou code de conduite
	Indicateur 16: Sécurité du personnel	Contrôle de sécurité du personnel
	Indicateur 24: Rôle et responsabilité en matière de cybersécurité	Rôle et responsabilité en matière de cybersécurité
	Indicateur 27: Pourcentage du budget pour les TIC consacré à la sécurité	Pourcentage du budget pour les TIC de l'organisation qui est consacré à la sécurité de l'information
Indicateurs qui peuvent être mesurés à l'aide des outils de mesure et/ou des bases de données qui sont normalement présents dans une organisation	Indicateur 1: Gestion des vulnérabilités.	Pourcentage de fortes vulnérabilités qui ont été réduites
	Indicateur 2: Tenue à jour des journaux d'audit	Pourcentage de dispositifs de point d'extrémité pour lesquels un journal d'audit est tenu à jour
	Indicateur 3: Réaction en cas d'incident	Réaction en cas d'incident
	Indicateur 8: Couverture de l'évaluation des risques	Couverture de l'évaluation des risques

Tableau II.I – Classement des indicateurs selon leur nature

Nature des indicateurs	Numéro de l'indicateur	ID de l'indicateur
	Indicateur 9: Couverture du programme de détection et de traitement des logiciels malveillants	Couverture du programme de détection et de traitement des logiciels malveillants
	Indicateur 21: Taux de réception de spams	Taux de réception de spams
	Indicateur 22: Programme de sensibilisation de l'organisation	Programme de sensibilisation de l'organisation
	Indicateur 23: Formation et éducation à la sécurité	Formation et éducation à la sécurité
	Indicateur 28: Taux de dispositifs autorisés	Taux de dispositifs autorisés de l'organisation parmi tous les dispositifs
	Indicateur 29: Taux de logiciels autorisés	Taux de logiciels autorisés de l'organisation parmi tous les logiciels
	Indicateur 30: Sécurité des logiciels applicatifs	Taux de logiciels applicatifs de l'organisation qui sont protégés contre les principales attaques logicielles au niveau des applications (par exemple CWE top 25) parmi tous les logiciels applicatifs.
Indicateurs qui nécessitent probablement la mise en place de capacités de mesure supplémentaires au sein de l'organisation	Indicateur 4: Délai moyen pour réduire les vulnérabilités	Délai moyen pour réduire les vulnérabilités
	Indicateur 5: Utilisation d'un programme de correctifs de sécurité	Programme de correctifs de sécurité
	Indicateur 6: Délai moyen pour installer un correctif	Délai moyen pour installer un correctif
	Indicateur 7: Délai moyen pour changer de configuration	Délai moyen pour changer de configuration
	Indicateur 10: Couverture de la planification d'urgence	Tests du plan d'urgence
	Indicateur 11: Evaluation de la sécurité	Pourcentage de systèmes informatiques ayant passé avec succès l'évaluation de la sécurité
	Indicateur 13: Contrôle d'accès à distance avec passerelle de sécurité	Points d'accès à distance protégés
	Indicateur 14: Contrôle d'accès à distance avec fonction de sécurité assurant la prévention ou la détection des intrusions	Points d'accès à distance protégés

Tableau II.I – Classement des indicateurs selon leur nature

Nature des indicateurs	Numéro de l'indicateur	ID de l'indicateur
	Indicateur 15: Contrôle d'accès sans fil	Points d'accès à distance protégés
	Indicateur 17: Protection des informations d'identification personnelle (PII)	Pourcentage d'informations d'identification personnelle sensibles protégées
	Indicateur 18: Protection des données de secours	Taux d'inspection de l'intégrité des données de secours
	Indicateur 19: Couverture du système certifié de gestion de la sécurité	Couverture du système de gestion
	Indicateur 20: Utilisation de serveurs sécurisés	Utilisation de serveurs sécurisés
	Indicateur 25: Infection par des logiciels malveillants	Dispositifs de point d'extrémité infectés par des logiciels malveillants
	Indicateur 26: Fuite d'informations d'identification personnelle	Fuite d'informations d'identification personnelle

Appendice III

Indicateurs expérimentaux

(Le présent appendice ne fait pas partie intégrante de la Recommandation.)

Le présent appendice décrit plusieurs indicateurs expérimentaux (voir les Tableaux III.1 à III.6) pouvant être utilisés par les organisations.

Tableau III.1 – Indicateur III-1: Délai moyen pour découvrir un incident (au niveau des systèmes et au niveau du programme, valeur faible souhaitable)

Champ	Données
ID de l'indicateur	Délai moyen pour découvrir un incident.
But	L'organisation devrait détecter les incidents dès qu'ils surviennent et mesurer le délai moyen pour découvrir un incident afin de prouver son efficacité dans la détection des incidents de sécurité. En général, plus l'organisation détecte un incident rapidement, moins l'incident risque d'occasionner des dégâts.
Indicateur	Durée moyenne écoulée, en heures, entre la survenue et la découverte d'un incident pour un ensemble donné d'incidents.
Formule	Somme (heure_de_découverte – heure_de_survenue)/nombre (incidents).
Données brutes	• Heure de découverte des incidents, pour chaque incident. • Nombre total d'incidents signalés.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	• Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau III.2 – Indicateur III-2: Redondance des liaisons (systèmes, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Pourcentage de liaisons de réseau avec redondance.
But	L'organisation devrait mettre en place des liaisons redondantes dans le réseau principal pour garantir la disponibilité et la continuité de ses services.
Indicateur	Pourcentage de liaisons de réseau avec redondance.
Formule	(Nombre de liaisons avec redondance/nombre total de liaisons de réseau) × 100.
Données brutes	• Nombre de liaisons avec redondance pour les routeurs, le système de noms de domaine (DNS), le protocole de configuration d'hôte dynamique (DHCP), les pare-feu, ou les bases de données (DB). • Nombre de liaisons sans redondance.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau III.3 – Indicateur III-3: Infection par des bots (au niveau des systèmes, valeur faible souhaitable)

Champ	Données
ID de l'indicateur	Pourcentage de dispositifs de point d'extrémité infectés par des bots.
But	L'organisation devrait réduire la présence des bots dans son réseau.
Indicateur	Pourcentage de dispositifs de point d'extrémité de l'organisation infectés par des bots connus. L'organisation est supposée utiliser un système de détection des infections par des bots.
Formule	(Nombre total de dispositifs de point d'extrémité infectés par des bots connus/nombre total de dispositifs de point d'extrémité) × 100.
Données brutes	• Nombre de dispositifs de point d'extrémité infectés par des bots.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau III.4 – Indicateur III-4: Mesures face au déni de service réparti (DDoS) (au niveau des systèmes, valeur faible souhaitable)

Champ	Données
ID de l'indicateur	Mesures face au DDoS.
But	L'organisation devrait protéger ses systèmes de point d'extrémité contre les attaques DDoS (ou les attaques par déni de service (DoS)) pendant la période qu'elle a définie.
Indicateur	Pourcentage de systèmes de l'organisation qui sont indisponibles pendant une certaine durée en raison d'attaques DDoS (DoS).
Formule	(Nombre de systèmes de l'organisation qui sont indisponibles pendant une certaine durée en raison d'attaques DDoS pendant la période spécifiée par l'organisation/nombre total de sites web que l'organisation possède) × 100.
Données brutes	• Nombre de sites web qui sont indisponibles pendant une certaine durée en raison d'attaques DDoS pendant la période définie par l'organisation. • Nombre total de sites web.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Tableau III.5 – Indicateur III-5: Performance des journaux d'audit (au niveau des systèmes et au niveau du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Pourcentage d'incidents de sécurité informatique pour lesquels un journal d'audit a enregistré des traces observables.
But	L'organisation devrait évaluer l'efficacité des journaux d'audit.
Indicateur	Pourcentage d'incidents de sécurité informatique pour lesquels un journal d'audit a enregistré des traces observables.
Formule	(Incidents signalés pour lesquels on trouve des traces observables dans les journaux/nombre total d'incidents signalés) × 100.
Données brutes	• Nombre d'incidents signalés pour lesquels on trouve des traces observables dans les journaux d'audit. (Journal centralisé ou journaux agrégés à partir des points d'extrémité) • Nombre total d'incidents signalés.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).

Tableau III.5 – Indicateur III-5: Performance des journaux d'audit (au niveau des systèmes et au niveau du programme, valeur élevée souhaitable)

Champ	Données
Référence pour les techniques CYBEX	

Tableau III.6 – Indicateur III-6: Performance de la réduction des incidents (au niveau des systèmes et au niveau du programme, valeur élevée souhaitable)

Champ	Données
ID de l'indicateur	Pourcentage d'incidents de sécurité informatique situés dans les systèmes certifiés et homologués (points d'extrémité ou groupes de points d'extrémité).
But	L'organisation devrait évaluer l'efficacité des procédures de certification et d'homologation.
Indicateur	Pourcentage d'incidents de sécurité informatique situés dans les systèmes certifiés et homologués.
Formule	(Incidents signalés qui étaient situés dans les systèmes certifiés et homologués/nombre total d'incidents signalés) × 100.
Données brutes	• Nombre d'incidents signalés qui étaient situés dans les systèmes certifiés et homologués • Nombre total d'incidents signalés.
Fréquence	• Hebdomadaire, mensuelle, trimestrielle, annuelle.
Type	Efficacité/efficience.
Niveau d'exigence	
Applicable à	Organisations (une communauté par agrégation).
Référence pour les techniques CYBEX	

Bibliographie

[b-UIT-T E.409] Recommandation UIT-T E.409 (2004), *Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication*.

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991) | ISO/CEI 7498-2 (1989), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

[b-UIT-T X.810] Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général.*

[b-UIT-T X.1205] Recommandation UIT-T X.1205 (2008), *Présentation générale de la cybersécurité.*

[b-UIT-T X.1206] Recommandation UIT-T X.1206 (2008), *Cadre de notification automatique d'informations liées à la sécurité et de diffusion de mises à jour, indépendant du fournisseur.*

[b-UIT-T X.1242] Recommandation UIT-T X.1242 (2009), *Système de filtrage des spams du service de messages courts (SMS) basé sur des règles spécifiées par l'utilisateur.*

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité.*

[b-UIT-T X.1500] Recommandation UIT-T X.1500 (2011), *Techniques d'échange d'informations sur la cybersécurité.*

[b-UIT-T X.1520] Recommandation UIT-T X.1520 (2011), *Vulnérabilités et expositions courantes.*

[b-UIT-T X.1521] Recommandation UIT-T X.1521 (2011), *Système d'évaluation des vulnérabilités courantes.*

[b-UIT-T X.1524] Recommandation UIT-T X.1524 (2012), *Liste des failles courantes.*

[b-UIT-T X.1528] Recommandation UIT-T X.1528 (2012), *Système commun d'énumération des éléments d'une plate-forme.*

[b-UIT-T X.1544] Recommandation UIT-T X.1544 (2013), *Liste et classification des schémas d'attaque courants.*

[b-UIT-T X-Sup.8] Recommandations UIT-T de la série X − Supplément 8 (2010), *UIT-T X.1205 − Supplément sur les bonnes pratiques de lutte contre les menaces liées aux botnets*.

[b-ISO/CEI 19770-2] ISO/CEI 19770-2:2009, *Technologies de l'information – Gestion des actifs logiciels – Partie 2: Etiquette d'identification du logiciel*.

[b-ISO/CEI 27000] ISO/CEI 27000:2012, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire.*

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

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

[b-ISO/CEI 27003] ISO/CEI 27003:2010, *Technologies de l'information – Techniques de sécurité – Lignes directrices pour la mise en oeuvre du système de management de la sécurité de l'information.*

[b-ISO/CEI 27033-1] ISO/CEI 27033-1:2009, *Technologies de l'information – Techniques de sécurité – Sécurité de réseau – Partie 1: Vue d'ensemble et concepts.*

[b-ISO/CEI 27033-2] ISO/CEI 27033-2:2012, *Technologies de l'information – Techniques de sécurité – Sécurité de réseau – Partie 2: Lignes directrices pour la conception et l'implémentation de la sécurité de réseau.*

[b-ISO/CEI 27033-4] ISO/CEI 27033-4:2014, *Technologies de l'information – Techniques de sécurité – Sécurité de réseau – Partie 4: Sécurisation des communications entre réseaux en utilisant des portails de sécurité.*

[b-NIST SP 800-27] NIST SP 800-27 Revision A (2004), *Engineering Principles for IT Security (A Baseline for Achieving Security), Revision A*.

[b-NIST SP 800-30] NIST SP 800-30 Revision 1 (2012), *Guide for Conducting Risk Assessments*.

[b-NIST SP 800-53] NIST SP 800-53 Revision 4 (2013), *Security and Privacy Controls for Federal Information Systems and Organizations*.

[b-NIST SP 800-55] NIST SP 800-55 Revision 1 (2008), *Performance Measurement Guide for Information Security*.

[b-NIST FIPS 199] NIST FIPS PUB 199 (2004), *Standards for Security Categorization of Federal Information and Information Systems*.

[b-ENISA] ENISA (V6_2, 2011), *Measurement Frameworks and Metrics for Resilient Networks and Services: technical report*.

[b-NRI] World Economic Forum (2013), *Networked Readiness Index*.

[b-WEF] World Economic Forum (2013), *Secure Internet servers*. (Sources: The World Bank, World Development Indicators Online; national sources).

[b-CIS] Center for Internet Security (2010), *The CIS security metrics*.

[b-Nelson] Nelson, C. E. (2010), *Security metrics: An overview,* ISSA Journal, Vol.8, No. 8.

[b-BSA] BSA (2013), *BSA Global Cloud Computing Scorecard*. http://cloudscorecard.bsa.org/2013/

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, 2014