

ISO 17799 : 2005/ISO 27002

Bonnes pratiques pour la gestion de la sécurité de l'information

Éric Lachapelle, CEO Veridion
René St-Germain, Président Veridion

Sommaire

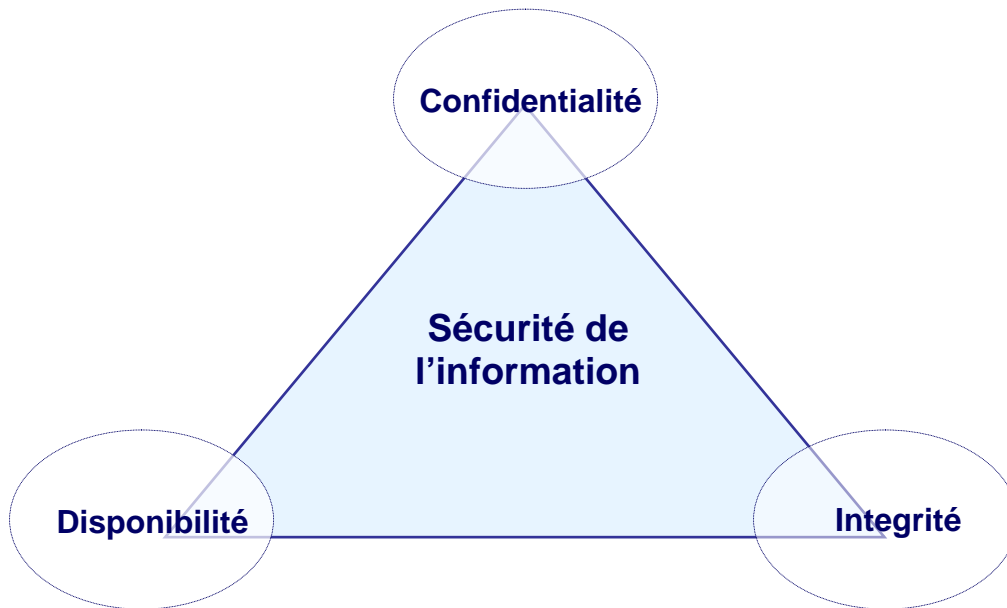
Qu'est-ce que la sécurité de l'information?	3
Présentation d'ISO 17799 : 2005.....	5
Qu'est-ce qu'ISO 17799 : 2005?.....	5
Architecture.....	7
Schéma d'architecture.....	7
Couverture thématique	8
Présentation des 11 thèmes	9
Politique de sécurité.....	9
Organisation de la sécurité de l'information	10
Gestion des actifs	11
Sécurité des ressources humaines	12
Sécurité physique ou environnementale	13
Gestion de la communication et de l'exploitation	14
Contrôles d'accès	16
Acquisition, développement et maintenance des SI	18
Gestion des incidents de sécurité de l'information	19
Gestion de la continuité d'affaires	20
Conformité	21
Utilisation de la norme	22
Utilisation générale	22
Optique de certification et d'audit.....	23
Profil de l'entreprise	24

Qu'est-ce que la sécurité de l'information ?

L'information est un actif qui, comme tout autre actif pour l'entreprise, a une valeur et qui doit donc être convenablement protégé. L'approche de la sécurité de l'information permet de protéger l'information des menaces qui pourraient corrompre sa qualité tout en garantissant la continuité des activités de l'entreprise, en minimisant les pertes et en maximisant le retour sur l'investissement et les opportunités.

L'information peut prendre différentes formes. Elle peut être imprimée ou écrite sur papier, stockée électroniquement, acheminée par voie postale ou par des moyens électroniques, transmise par des films, ou enfin verbale divulguée lors de conversations. Quelle que soit la forme qu'elle revêt, quels que soient les moyens par lesquels elle est partagée, transmise ou stockée, elle doit toujours être correctement protégée.

Lorsque l'on parle de sécurité de l'information, il faut avoir à l'esprit les trois notions suivantes :



- I. **Confidentialité**: il s'agit de s'assurer que l'information est seulement accessible à ceux qui ont l'autorisation d'y accéder.
- II. **Intégrité**: l'information doit être précise, complète et ne doit ni être altérée, ni altérable.
- III. **Disponibilité**: l'information doit être disponible à tout moment aux seules personnes qui ont accès à cette information précise.

La sécurité de l'information requiert l'implémentation d'une série de contrôles, de procédures, de politiques de sécurité, etc., devant être mis en place dans un but de garantie des objectifs de l'entreprise, afin de préserver la confidentialité, l'intégrité et la disponibilité de l'information.



Qu'est-ce qu'ISO 17799 : 2005 ?

Révisée en 2005, ISO 17799 est un guide de bonnes pratiques pour la gestion de la sécurité de l'information qui peut représenter un intérêt pour tout type d'organisation (entreprise, corps gouvernementaux...) quelque soit sa taille ou son secteur d'activité.

Cette norme définit des objectifs et des recommandations en termes de sécurité de l'information et a pour ambition de répondre aux préoccupations globales de sécurisation de l'information des organisations et ce pour l'ensemble de leurs activités.

Selon ISO, cette norme a pour objectif de :

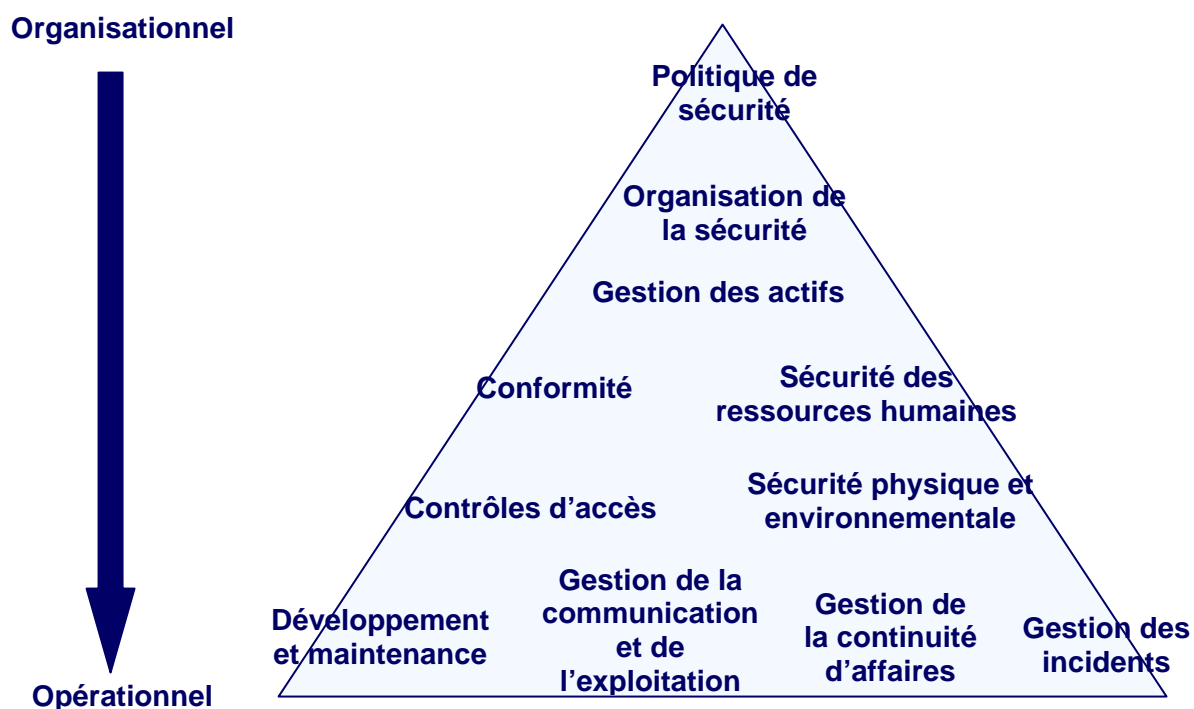
« Donner des recommandations pour gérer la sécurité de l'information à l'intention de ceux qui sont responsables de définir, d'implémenter ou de maintenir la sécurité dans leur organisation. Elle est conçue pour constituer une base commune de développement de normes de sécurité organisationnelle et de pratiques efficaces de gestion de la sécurité, et pour introduire un niveau de confiance dans les relations interentreprises. »



Schéma d'architecture

La norme ISO 17799 comporte 11 chapitres. Chaque chapitre présente un thème de sécurité dans lequel sont exposés des objectifs de contrôles et des recommandations sur les mesures de sécurité à mettre en œuvre et les contrôles à implémenter.

Le schéma ci-dessous représente les 11 thèmes d'ISO 17799 et permet de voir si ces thèmes traitent de la sécurité de l'information au niveau organisationnel ou opérationnel:



Pour chaque thème abordé, les préconisations cherchent à garantir la confidentialité, l'intégrité et la disponibilité de l'information.

Couverture thématique

ISO 17799 couvre 11 thèmes de sécurité de l'information :

- La politique de sécurité
- L'organisation de la sécurité de l'information
- La gestion des actifs
- La sécurité des ressources humaines
- La sécurité physique et environnementale
- La gestion de la communication et de l'exploitation
- Les contrôles d'accès
- L'acquisition, le développement et la maintenance des systèmes d'information
- La gestion des incidents de sécurité de l'information
- La gestion de la continuité des affaires
- La conformité

Pour ces 11 thèmes de sécurité, ISO 17799 présente 39 objectifs de sécurité au total. Chacun des objectifs de sécurité comporte un objectif de contrôle et un ou plusieurs contrôles pouvant s'appliquer pour atteindre l'objectif de contrôle.

Présentation des 11 thèmes

Politique de sécurité

Le premier thème abordé dans ISO 17799 est la **politique de sécurité de l'information**. Le seul objectif de contrôle cherche à démontrer l'appui de la direction en ce qui concerne la gestion de la sécurité de l'information.



Pour cela ISO 17799 préconise deux contrôles. Le premier concerne la création d'un document de politique de sécurité de l'information. Celui-ci représente un moyen privilégié pour la direction d'établir son appui et de présenter l'approche de l'organisation en termes de sécurité de l'information. Afin d'être parfaitement efficace, ce document sera publié et communiqué aux employés et tiers qui y trouveraient un intérêt.

Le second contrôle concerne la révision de la politique de sécurité. Ceci devra être fait régulièrement, que ce soit à des intervalles planifiés ou tout simplement en cas de changements significatifs des exigences en sécurité de l'information. La révision régulière de la politique de sécurité assurera sa continuité et son efficacité.

Organisation de la sécurité de l'information

En ce qui concerne l'organisation de la sécurité de l'information, ISO 17799 propose deux objectifs de contrôle de sécurité.

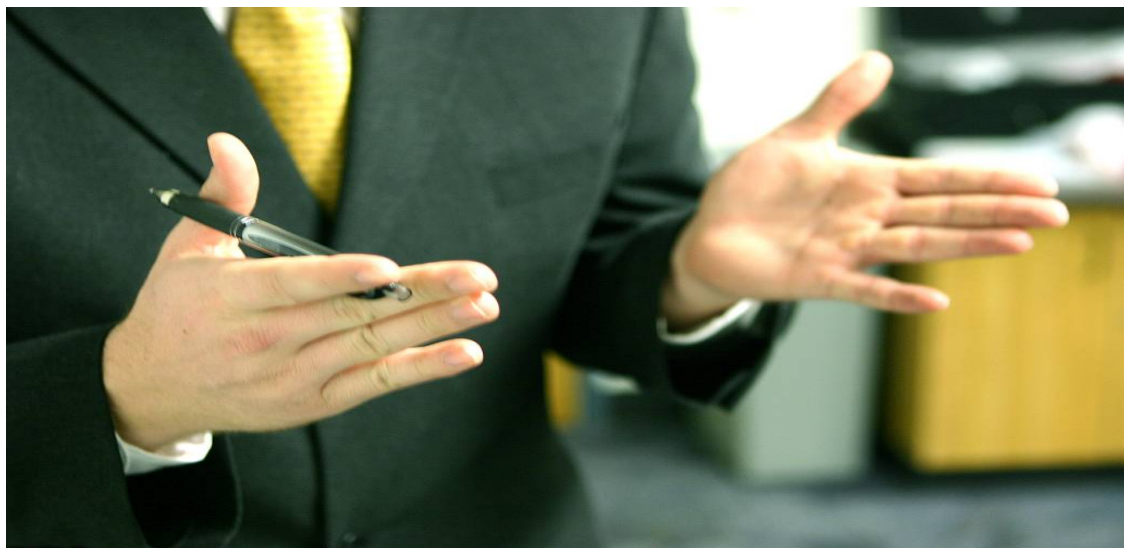
Le premier objectif de contrôle de sécurité concerne l'**organisation interne**. Il s'agit de gérer la sécurité de l'information dans l'organisation par le biais d'un cadre de gestion. Celui-ci permettra d'initialiser et de contrôler l'implémentation de la sécurité de l'information au sein de l'organisation.

Le second objectif de contrôle concerne les **tiers** : il s'agit de maintenir la sécurité des informations qui sont accessibles, diffusées, communiquées ou gérées par des tiers et des équipements qui la délivrent. En effet, l'introduction de produits ou services en provenance de tiers ne doit pas avoir d'impact sur la sécurité de l'information. Une évaluation des risques permettra de mettre en lumière les contrôles à mettre en place pour limiter les incidents de sécurité.



Le troisième thème, qui évoque la gestion des actifs, comporte deux parties : les responsabilités pour les actifs et la classification de l'information.

Définir les **responsabilités pour les actifs** permet d'atteindre et de maintenir une protection adéquate des actifs de l'organisation. En effet, tous les actifs de l'organisation doivent être comptabilisés et avoir un propriétaire : celui-ci aura le devoir de maintenir les contrôles adéquats pour l'actif dont il est responsable. Bien entendu, il pourra déléguer une partie de ses tâches (notamment l'implémentation de contrôles spécifiques) s'il le juge nécessaire, mais demeurera le seul responsable de la protection des actifs.



En ce qui concerne la **classification de l'information**, celle-ci permet de s'assurer que l'information reçoit un niveau de protection approprié à ses caractéristiques : certaines peuvent exiger un niveau de protection supplémentaire en raison de leur degré de criticité ou de sensibilité. Pour cela, l'information doit être classée afin de mettre en relief les besoins, priorités et degrés de protection attendus. Le développement d'un schéma de classification pourrait alors s'avérer judicieux, notamment en ce qui concerne les informations nécessitant des traitements spéciaux.

Ce thème distingue trois objectifs de contrôle de sécurité, un par étape du cycle de vie d'un individu dans une organisation.

Avant l'embauche, l'objectif est de s'assurer que les parties signataires au contrat (futur employé, organisation, tiers) comprennent leurs responsabilités et qu'ils acceptent les rôles qui leurs sont assignés, afin de réduire le risque de vol, fraude ou de mauvaise utilisation des équipements. A cet effet, deux documents seront produits : la description d'emploi, qui exposera les responsabilités de chacun, et un accord d'acceptation des rôles et des responsabilités. Ce dernier devra être signé pour être valide.

Lors du mandat de l'individu, l'objectif est de vérifier et garantir que les signataires du contrat sont non seulement conscients des menaces en termes de sécurité de l'information (et donc de leurs responsabilités en la matière), mais aussi qu'ils appuient la politique de sécurité organisationnelle pendant leur mandat pour réduire le risque d'erreur humaine. La formation permettra de minimiser le risque d'un niveau inadéquat de compréhension des procédures de sécurité ou de mauvaise utilisation des équipements. A cet effet, un processus disciplinaire formel de gestion des failles de sécurité pourra être établi.

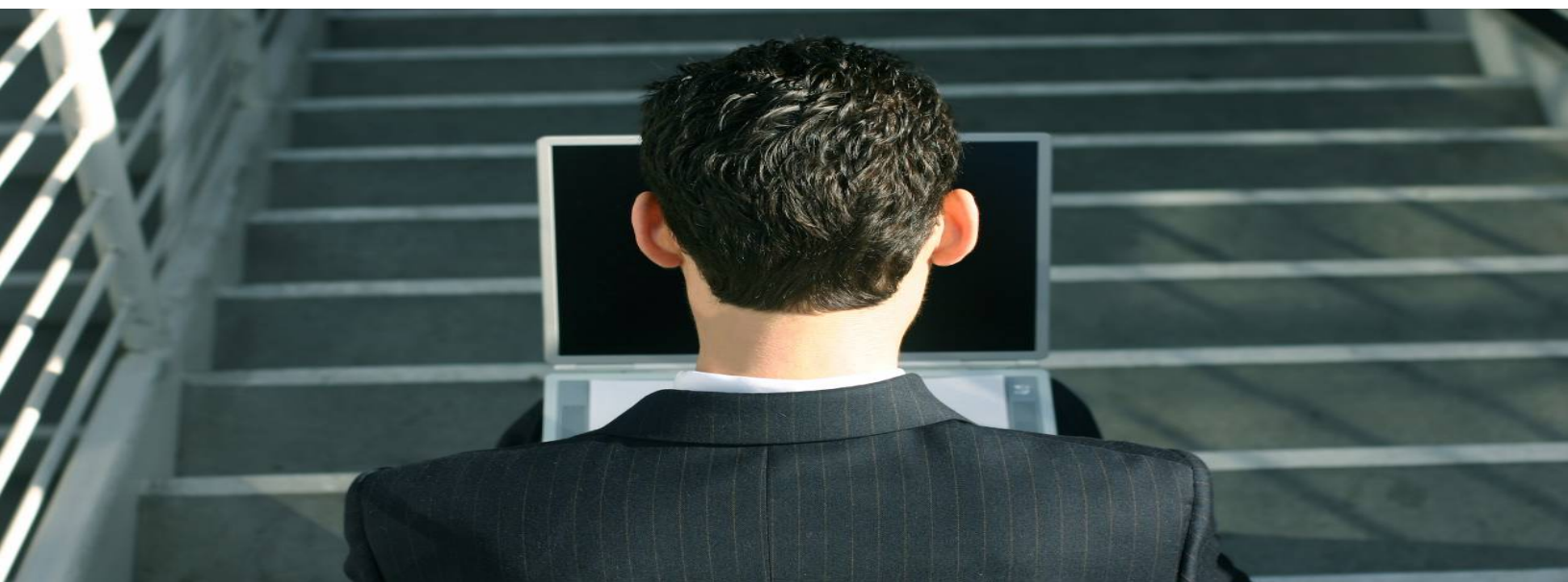
A la fin du contrat ou en cas de changement d'emploi, le but est de s'assurer que les signataires concernés quittent l'organisation ou changent d'emploi de manière organisée. En cas de départ de l'organisation, on vérifie que tout l'équipement est retourné et que les droits d'accès ont été effacés. Le changement d'emploi sera quant à lui découpé en deux étapes : la fin d'un mandat et le début d'un nouvel emploi (nouvelles fonctions).

Sécurité physique ou environnementale

Deux points sont à prendre en compte lorsque l'on parle de sécurité physique et environnementale : les zones sécurisées et la sécurité des équipements.

Les **zones sécurisées** ont pour but de prévenir les accès physiques non autorisés, les dommages et les intrusions dans les bâtiments et informations de l'organisation. Elles hébergeront les équipements qui délivrent ou stockent des données sensibles ou critiques et seront renforcées par des périmètres de sécurité, barrières de sécurité et codes d'accès. Ici on cherche à protéger physiquement les équipements selon les risques identifiés.

L'objectif de contrôle relatif à la **sécurité des équipements** cherche à prévenir les pertes, les dommages, les vols ou les compromissions d'actifs, et les interruptions des activités de l'organisation. La protection de l'équipement face aux menaces physiques et environnementales peut nécessiter des contrôles spéciaux (équipements de fourniture d'électricité...) et devra prendre en compte leur disposition et leur localisation pour être efficace.



Ce chapitre, dense, comporte 10 objectifs de contrôles de sécurité.

Le premier évoque l'implémentation de **procédures d'exploitation** et de définition des **responsabilités** pour assurer le fonctionnement correct et sécurisé des équipements délivrant et stockant l'information. Il conseille le développement de procédures de fonctionnement appropriées aux caractéristiques des équipements.

Le deuxième objectif de contrôle, relatif aux **prestations de services en provenance de tiers**, vise à implémenter et maintenir un niveau de sécurité de l'information et de prestation de service conforme aux accords de prestation passés avec les tiers.

Le troisième objectif, la **planification du système**, a pour but de minimiser les risques de pannes du système d'information. A cet effet, ISO 17799 préconise de réaliser des projections afin d'assurer la disponibilité des ressources et des capacités mais aussi d'éviter une surcharge du système.

Le quatrième objectif de contrôle est de protéger l'intégrité des logiciels et des informations contre les **codes mobiles et malveillants** (virus informatiques, chevaux de Troie, bombes logiques...). Pour cela l'organisation pourra établir un programme d'information des dangers de ces codes sur la sécurité et introduire des contrôles.

Le cinquième point de sécurité concerne les **sauvegardes** : elles ont pour objectif de maintenir la disponibilité et l'intégrité des informations et des équipements délivrant l'information grâce à la création de politiques de routine.

Le sixième objectif, la **gestion de la sécurité du réseau** garantit la protection de l'information contenue dans le réseau et celle de l'infrastructure de support.



Le septième objectif de contrôle, relatif à **l'utilisation d'accessoires informatiques**, vise à prévenir toute modification, destruction ou déplacement d'actif mais aussi les interruptions des activités de l'organisation. Il préconise l'utilisation de protections physiques et incite à l'implémentation de contrôles.

Huitième objectif, le contrôle des **échanges d'informations** garantit le maintien de la sécurité de l'information et des logiciels échangés entre l'organisation et toute entité externe grâce à la création d'une politique d'échange formelle et d'accords d'échange.

Le contrôle des **services de commerce électronique** (transactions en ligne...), objet du neuvième objectif, assure la sécurité des services de commerce en ligne et leur utilisation sécurisée.

Enfin, l'objectif d'**encadrement** est de détecter les activités de livraison d'information qui ne seraient pas autorisées en enregistrant les erreurs d'identification.

Contrôles d'accès

Ce thème présente les sept objectifs de contrôle qui permettent de prévenir tout accès non autorisé.

Le premier objectif sert à prendre en compte les **exigences d'affaires** dans le contrôle d'accès à l'information. En effet, pour prévenir tout risque, les contrôles d'accès à l'information devront non seulement être conformes aux exigences d'affaires, mais aussi aux politiques et autorisations de divulgation de l'information.

Ensuite il faut **gérer les accès aux utilisateurs** grâce à des procédures d'allocation des droits d'accès aux systèmes d'information et aux services. On apportera une attention spéciale à l'allocation d'accès privilégiés dans la mesure où ceux-ci permettent aux utilisateurs d'outrepasser les contrôles du système.



Autre objectif de contrôle, la détermination des **responsabilités des utilisateurs** permet de prévenir les compromissions et les vols d'informations et d'équipements délivrant l'information. Ici la coopération entre utilisateurs est essentielle pour qu'il soient conscients de leurs rôles et ainsi assurer le maintien d'un système de contrôle d'accès efficace.

ISO 17799 accorde une place particulière aux **contrôles d'accès au réseau**, aux **contrôles d'accès aux systèmes d'exploitation** et aux **contrôles d'accès à l'information et aux applications**. En effet, une mauvaise gestion de ces accès serait fortement préjudiciable à la sécurité de l'organisation. Afin d'éviter tout risque, les contrôles et procédures devront être renforcés, les équipements de sécurité contrôleront les accès. Le but est de fournir une protection supplémentaire tout en ne compromettant pas le système de contrôle d'accès déjà en place.

Le dernier objectif de contrôle concerne le **télétravail et les équipements informatiques mobiles**. Ce type de travail spécifique fera l'objet d'une évaluation des risques à part, étant donné que les protections concernent le site de télétravail lui-même.



Dans un premier temps, ISO 17799 définit un objectif de contrôle relatif aux **exigences de sécurité pour les systèmes d'information** pour assurer que la sécurité de l'information fait partie intégrante du système d'information.

Ensuite la norme évoque le **déroulement correct des applications**, qui permet de prévenir les erreurs, pertes, modifications non autorisées ou mauvaises utilisations de l'information contenue dans les applications. Pour cela, il convient de choisir les contrôles appropriés pour valider les données entrantes et sortantes des applications.

Puis, ISO 17799 recommande les **contrôles cryptographiques** afin de protéger l'authenticité, la confidentialité et/ou l'intégrité de l'information de l'organisation. Une politique spécifique d'utilisation de ces contrôles devra être établie et l'aide d'une équipe qualifiée pour gérer les techniques de cryptographie pourra être envisagée.

Enfin, la norme développe des objectifs de contrôle à propos de la **sécurité des fichiers systèmes** et de la **sécurité des processus de développement et de support**. Il s'agit dans les deux cas de maintenir la sécurité de l'information par l'implémentation de contrôles adaptés, la définition de responsabilités et la gestion des changements.

La norme mentionne aussi la **gestion des vulnérabilités techniques**, qui a pour but de réduire les risques résultant de l'exploitation des vulnérabilités techniques publiées. L'implémentation de contrôles et de mesures d'efficacité qui s'inscrivent dans un processus d'amélioration continue permettra de minimiser les vulnérabilités techniques auxquelles l'organisation pourrait faire face.



Pour ce thème, ISO 17799 définit deux objectifs de contrôle.

Le premier est relatif aux **rapports des événements et faiblesses de la sécurité de l'information**. Il assure que ces rapports sont communiqués de manière à permettre des actions correctives rapides. Il préconise des rapports formels d'événements et la création d'échelles de procédures connues de tous. Les échelles de procédures définissent les priorités de traitement entre les incidents.

Le second concerne la **gestion des incidents et des améliorations de la sécurité de l'information** et garantit qu'une approche consistante et efficace est implémentée. Il faut notamment que les responsabilités et les procédures soient définies et mises en place, qu'un processus d'amélioration continue soit développé et que l'organisation prenne garde aux exigences légales dans sa récolte de preuves d'incidents de sécurité de l'information.

Gestion de la continuité d'affaires



Ce chapitre développe les **aspects de sécurité de l'information dans la gestion de continuité d'affaires**. L'objectif de contrôle cherche à contrer les interruptions d'activité et à protéger les processus d'affaires critiques des effets de catastrophes ou de failles majeures dans le système d'information. Il permet en outre d'assurer la reprise rapide des activités de l'organisation grâce à l'implémentation d'un processus d'amélioration continue.

Ce dernier thème développe la conformité avec les exigences légales, la **conformité technique et la conformité avec les normes et politiques de sécurité** et enfin expose des considérations sur les audits des systèmes d'information.

La **conformité avec les exigences légales** a pour but d'éviter d'aller à l'encontre des lois, des obligations contractuelles, statutaires ou de régulation, et des exigences de sécurité. A cet effet, ISO 17799 évoque la possibilité de demander l'avis de conseillers afin de mieux appréhender la loi et ses exigences.

Le deuxième type de conformité explicité dans ce chapitre assure la conformité des systèmes avec les politiques et les normes de sécurité organisationnelles. Elle nécessite un audit et doit être correctement documentée. De plus, pour être efficiente sur le long terme, elle doit être révisée régulièrement.

Enfin, les **considérations sur les audits de systèmes d'information** permettent de maximiser l'efficacité du processus d'audit des systèmes. Elles préconisent une protection spécifique garantissant l'intégrité du processus et prévenant une mauvaise utilisation des outils d'audit.



Utilisation de la norme

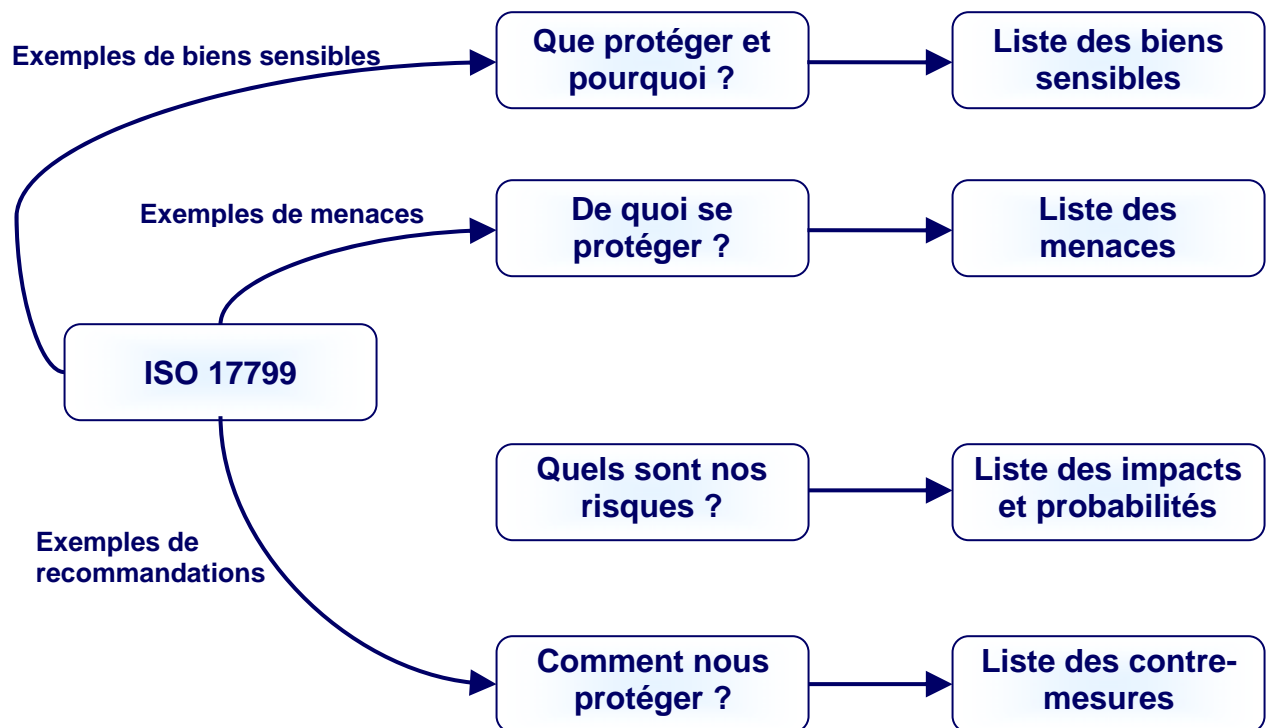
Utilisation générale

Le corps de la norme ISO 17799 indique « **quoi** » faire pour la sécurité de l'information mais ne mentionne pas **comment** le faire.

A ce titre, l'organisation pourra chercher à mettre en œuvre directement une partie plus ou moins étendue des contrôles proposés, mais elle pourra aussi s'en servir comme check list pour un sujet particulier.

La norme ISO 17799 constitue donc un élément de référence pour aider l'organisation à établir ses propres objectifs à atteindre en matière de sécurité et lui permet de construire sa propre démarche de mise en œuvre.

Le schéma ci-dessous résume les étapes de mise en œuvre de la norme.



Une certification est délivrée par un organisme indépendant et permet de garantir la conformité d'un produit, service ou d'un système à des exigences définies. Elle s'appuie sur un audit réalisé par des personnes n'ayant aucun intérêt dans l'organisation auditée.

Or ISO 17799, en tant que guide de bonnes pratiques de gestion de la sécurité de l'information, ne définit aucune exigence relative à un produit, service ou système. Il n'est donc pas possible d'être certifié ISO 17799.

En revanche, cette norme peut être support à comparaison entre la réalité des bonnes pratiques de l'entreprise et celles définies dans ISO 17799. A ce titre, elle permettra de mettre en relief les écarts et de définir des axes d'amélioration pour l'organisation.

Les bonnes pratiques définies par ISO 17799 peuvent donc représenter une aide précieuse pour toute entreprise qui cherche la certification ISO 27001.



Profil de l'entreprise

Créée en 2005, Veridion Inc. est une entreprise spécialisée dans le secteur de la sécurité de l'information.

En fournissant à la fois des produits de qualité et des prestations de services, telles que la formation, le consulting ou l'audit, Veridion Inc. est le partenaire idéal pour toute entreprise soucieuse de la sécurité de l'information.

Nos domaines d'expertise sont les suivants :

- l'analyse de risque ;
- le développement de guides et de pratiques de sécurité ;
- l'élaboration de systèmes de gestion de la sécurité de l'information ;
- les politiques de sécurité basées sur ISO 17799 / ISO 27002 ;
- les audits de sécurité ;
- la formation en gestion du risque

Notre mission est de permettre à toutes les entreprises de gérer et de réduire leurs risques, de bâtir une stratégie de sécurité de l'information adaptée à leurs besoins.

En vous proposant des logiciels, des outils et un accompagnement dans l'analyse complète de vos risques, nous mettons un point d'honneur à rendre vos prises de décisions efficaces et efficientes.

Veridion Inc. Siège social

1750 St-Denis, Bureau 201
Montréal, QC
H2X 3K6
Canada

Téléphone: 1-514-849-2088
Fax: 1-514-371-1500
Sans frais: 1-866-949-2088
Site web: www.veridion.net
Email: info@veridion.net