



**Above**  
**SECURITE**

1919, boul. Lionel-Bertrand,  
Bureau 203  
Boisbriand, Qc. J7H 1N8  
Canada  
Téléphone :  
450-430-8166  
Sans frais :  
866-430-8166  
Télécopieur :  
450-430-1858  
info@abovesecurite.com

**La tranquillité d'esprit**

## Livre blanc

**Références sur les standards utilisés dans le  
processus de gestion des risques et de la mise en place  
d'un Système de Management de la Sécurité de l'Information (SMSI)**

### Préparé par :

Martin Dion

CISSP, CISM, ISO:27001 Lead Auditor & Trainer

Chef de la Direction Technologique

Above Sécurité

### Date de publication

Mars 2008



**'Above Security is the only pure-play MSS provider that merits  
consideration as a potential leader.'**

IDC Canadian Managed Security Services 2006 Vendor Analysis

**Table des matières**

**SOMMAIRE À L'ATTENTION DE LA DIRECTION .....3**  
**INTRODUCTION.....4**  
**BS7799-3:2006 GUIDELINES FOR INFORMATION SECURITY RISK MANAGEMENT .....5**  
**AS/NZ 4360:2004 RISK MANAGEMENT GUIDELINES .....6**  
**AS/NZ HB 231:2004 INFORMATION SECURITY RISK MANAGEMENT GUIDELINES.....7**  
**ISO/IEC 27001:2007 INFORMATION SECURITY MANAGEMENT SYSTEMS -  
REQUIREMENTS .....8**  
**ISO/IEC 27002:2005 CODE OF PRACTICE FOR INFORMATION SECURITY  
MANAGEMENT .....9**  
**CONTACTEZ-NOUS .....10**  
**COPYRIGHT .....10**

## Sommaire à l'attention de la direction

Lors de la mise en place d'un processus de gestion des risques au sein d'une entreprise, il incombe à la direction de sélectionner une méthodologie compatible avec les besoins de l'entreprise.

Non seulement la méthode devra permettre d'identifier et de traiter les risques, mais elle devra aussi prévoir la mise en place d'un cadre de référence pour la gestion de ceux-ci.

On entend par gestion des risques la mise en place d'un processus reproductible qui permet d'assurer :

1. L'identification des menaces et vulnérabilités auxquelles l'entreprise fait face;
2. L'identification des seuils de tolérance de l'entreprise face à ces risques;
3. L'établissement d'une approche de mesure qui permettra l'évaluation et la priorisation des risques lors de leur traitement;
4. L'établissement d'une méthodologie claire de traitement des risques; et,
5. Le suivi sur les risques résiduels et les méthodes opératoires qui permettront d'identifier les nouveaux risques et de réévaluer les risques existants auxquels l'entreprise fait face.

Le présent livre blanc vise donc à vous fournir un éclairage sur les standards et méthodes que nous préconisons pour la mise en place d'un système de gestion des risques en entreprise.

Il décrit les diverses normes ISO qui soutiennent la mise en place de ce système de gestion ainsi que les normes ISO:27001 et ISO:27002 qui sont quant à elles, spécifiques à la mise en place d'un SMSI.

Les méthodes ISO qui ont été sélectionnées et qui sont décrites dans ce livre blanc ont été choisies parce qu'elles répondent aux besoins de la norme ISO:27001 en matière de certification du SMSI (Système de Management de la Sécurité de l'Information) en égard au processus de gestion des risques qui doit être mis en place afin qu'une entreprise obtienne sa certification.

Il est important de noter que d'autres normes et méthodes de gestion des risques existent (NIST, Octave, EBIOS, Mehari pour n'en citer que quelques-unes) . Elles ne seront pas traitées dans ce livre blanc qui ne couvre que celles reconnues par l'International Standards Organisation (ISO).

Bonne lecture,



Martin Dion, CISSP/CISM  
ISO:27001 Lead Auditor & Trainer  
CTO, Above Security

## **Introduction**

Ce livre blanc couvre les cinq normes suivantes :

- BS 7799-3:2006 Guidelines for Information Security Risk Management
- AS/NZ 4360:2004 Risk Management Guidelines
- AS/NZ HB 231:2004 Information Security Risk Management Guidelines
- ISO/IEC 27001:2007 Information Security Management Systems - Requirements
- ISO/IEC 27002:2005 Code of practice for information security management

Ces cinq normes se complètent comme vous le verrez dans la page suivante

Chacune de ces normes sera présentée sommairement dans ce livre blanc.

## **BS7799-3:2006 Guidelines for Information Security Risk Management**

L'identification, l'évaluation, le traitement et la gestion des risques en matière de sécurité de l'information sont des processus clés pour l'entreprise qui veut préserver la sûreté et la sécurité de ses informations. Bien que ces processus soient identifiés à même la norme ISO 27001:2005, des instructions et lignes directrices supplémentaires doivent être établies sur la façon dont la gestion des risques (et leur alignement sur les autres risques de l'entreprise) doit être menée.

BS 7799-3:2006 fournit ces instructions et lignes directrices et couvre les éléments suivants :

- Analyse des risques
- Traitement des risques
- Processus de décision par la direction face au risque
- Réévaluation des risques
- Surveillance et revue des profils de risque
- Les risques liés à la sécurité de l'information dans le contexte de la gouvernance d'entreprise
- La conformité avec les autres normes, standards et réglementation en matière de gestion des risques.

BS 7799-3:2006 fournit des instructions claires soutenant les divers pré-requis établis par la norme ISO/IEC 27001:2005 en égard à tous les aspects du cycle de gestion des risques tel qu'exigé lors de la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI).

Ces requis incluent l'analyse et l'évaluation des risques, l'implantation de contrôles afin de traiter les risques, la surveillance et la revue des risques ainsi que la maintenance et l'amélioration du système de gestion des risques.

Le focus de cette norme est l'atteinte de l'efficacité en matière de sécurité de l'information par la mise en place d'un programme d'encadrement continu des activités liées à la gestion des risques.

Les instructions et lignes directrices contenues dans la norme BS 7799-3 sont applicables et s'adressent à tout type d'organisation nonobstant leur type, taille ou nature de leurs activités.

Elle s'adresse aux divers acteurs, les membres de direction et leurs équipes, impliqués dans les activités de gestion des risques liés au SMSI.

Cette norme étant déjà sous révision par l'ISO, elle sera à terme intégrée sous le nom ISO:27005 - *Security techniques - Information security risk management*.

## **AS/NZ 4360:2004 *Risk Management Guidelines***

Cette norme fournit des instructions et lignes directrices génériques à la gestion des risques. Elle s'applique, tout comme BS7799-3, à un large éventail d'activités, de décisions ou d'opérations dans des contextes privés, publics et gouvernementaux ou même au du point de vue départemental d'une entreprise.

Bien que ce standard semble s'adresser à un large éventail de clientèle, il est important de comprendre que le processus de gestion des risques est commun à presque tous les types d'entités, raison pour laquelle, nous utiliserons le terme 'organisation ' pour tout les définir.

Cette norme spécifie dans le détail tous les éléments qui composent le processus de gestion des risques. La norme met en perspective l'indépendance de ce processus par rapport à l'industrie ou au cadre économique de l'entreprise.

Elle tient compte que l'adoption et l'implantation d'un processus de gestion des risques est influencé par les divers besoins propres à chaque organisation, ses objectifs particuliers, ses produits et services, ses processus et ses obligations réglementaires.

Bien que le standard s'applique à différents stades dans le cycle de vie des activités, fonctions, projets, produits ou actifs de l'entreprise, il est sous-entendu que le bénéfice maximum ne pourra être atteint que si le processus est respecté dès le début du cycle de vie des éléments précédemment mentionnés.

Les diverses étapes suggérées lors de la mise en place du processus et l'opération de celui-ci tiennent compte tant des aspects stratégiques que des aspects opérationnels des organisations.

Il est important de noter que la norme tient compte non seulement des gains potentiels, mais aussi des pertes potentielles, le tout, dans un esprit systémique afin de traiter les divers aspects du risque dans l'organisation lors de leur cycle de vie.

La norme est complétée par les manuels HB:436 – *Risk Management Guidelines Companion Guide* qui quant à lui offre la méthode d'identification, d'analyse, d'appréciation et de traitement du risque en entreprise.

Un deuxième manuel, le HB:231 – *Information Security Risk Management Handbook* qui adresse plus spécifiquement, comme BS7799-3, les risques liés à la sécurité de l'information en entreprise est disponible. (Voir la section suivante pour notre revue du manuel HB : 231.)

## **AS/NZ HB 231:2004 Information Security Risk Management Guidelines**

La gestion des risques est reconnue comme faisant partie intégrante des bonnes pratiques en matière de gestion d'entreprise. La gestion des risques est un processus interactif constitué d'étapes, qui, lorsque suivit en séquence, permettent une amélioration du cycle de prise de décision.

De façon générale, le processus de gestion des risques appliqué à la sécurité de l'information vise l'ensemble du système d'information et des facilités de traitement, mais les méthodes préconisées dans ce manuel permettent aussi l'évaluation d'un sous-ensemble de composantes ou de services, lorsque praticables, réalistes et utiles.

C'est un manuel de référence auprès de trois auditoires bien précis :

1. Les membres de la direction imputables de la gestion de la sécurité de l'information;
2. Le personnel responsable d'initier, implanter et/ou surveiller le programme de gestion des risques d'entreprises; et,
3. Le personnel responsable d'initier, implanter et/ou maintenir le Système de Management de la Sécurité de l'Information de l'entreprise.

Étant donné que ce manuel est basé sur la norme AS/NZ 4360:2004, il respecte les principes directeurs suivants :

- l'adoption et l'implantation d'un processus de gestion des risques est influencé par les divers besoins propres à chaque organisation, ses objectifs particuliers, ses produits et services, ses processus et ses obligations réglementaires;
- Bien que le standard s'applique à différents stades dans le cycle de vie des activités, fonctions, projets, produits ou actifs de l'entreprise, il est sous-entendu que le bénéfice maximum ne pourra être atteint que si le processus est respecté dès le début du cycle de vie des éléments précédemment mentionnés; et,
- Que les diverses étapes suggérées lors de la mise en place du processus et l'opération de celui-ci tiennent compte tant des aspects stratégiques que des aspects opérationnels des organisations.

Il est important de noter que ce manuel est spécifique aux systèmes d'information et aux composants d'un SMSI (ISO:27001) et qu'il n'a pas été créé afin de couvrir la gestion des risques dans le cadre d'un processus 'santé et sûreté' ou 'sûreté dans l'utilisation de matériel électrique/électronique/à programmation embarquée'.

Ce manuel a été conçu afin de supporter les besoins de la norme ISO:27001 et la sélection des contrôles adéquats au traitement des risques tels que détaillés dans la norme ISO:27002.

## **ISO/IEC 27001:2007 Information Security Management Systems – Requirements**

Les origines de la norme ISO/IEC 27001:2007 remontent au milieu des années 90 lorsque le British Standard Institute a mis en place divers groupes de travail et comités afin d'élaborer des normes spécifiques à la gestion de la sécurité de l'information et à la certification d'un Système de Management de la Sécurité de l'Information.

Au fil des années et en réponse à l'adoption massive de cette norme à travers le Commonwealth Britannique (norme connue originalement sous le nom BS:7799), l'ISO a décidé d'adopter et d'intégrer la BS7799 dans son corpus de standard. Un sous-comité ISO a été formé, aujourd'hui connus sous l'appellation SC27000, il a adopté et uniformisé la numérotation du standard.

Les normes du BSI étaient en deux parties, soit la BS7799-1 et la BS7799-2, cette dernière étant la norme établissant les requis pour la certification d'un SMSI. Cette norme de certification est maintenant connue sous l'appellation en titre et porte le numéro ISO:27001.

La norme est adaptée à tous les types d'organisation et spécifie les conditions à respecter lors de l'établissement, l'implantation, l'opération, la surveillance, la révision, la maintenance, la documentation et l'amélioration d'un SMSI dans le contexte spécifique des risques auxquels une entreprise en particulier fait face. Elle spécifie aussi la nécessité pour une organisation d'implanter les contrôles adéquats et personnalisés à ses propres besoins.

La certification d'un SMSI a pour but de démontrer qu'une démarche structurée a été respectée. Cette démarche permet à l'organisation d'établir et d'assurer de façon indépendante, à travers un registraire, un niveau de confiance à des parties intéressées sur l'adoption des contrôles appropriés au sein de l'organisation.

La norme établit les obligations de l'entreprise dans le processus d'implantation et d'opération d'un SMSI en matière de :

- Politique et directive en matière de sécurité de l'information;
- Identification, traitement et gestion des risques propres à l'organisation;
- Gestion de la sécurité de l'information à l'aide des contrôles applicables;
- Responsabilité de l'équipe de direction;
- Documentation des divers processus liés à l'opération du SMSI;
- Revue et Audit du SMSI; et,
- Amélioration continue du SMSI.

Toute entreprise devrait évaluer la mise en place de la norme ISO/IEC 27001:2007. La certification d'un SMSI d'entreprises assure aux clients et fournisseurs de celle-ci que la sécurité de l'information est une affaire sérieuse aux yeux de l'équipe de direction et que l'entreprise a mis en place un processus qui permettra de traiter adéquatement les menaces et risques auxquels l'entreprise fait face.

## **ISO/IEC 27002:2005 Code of practice for information security management**

Comme pour la norme ISO:27001, la norme ISO/IEC 27002:2005 puise ses origines au British Standard Institute. Anciennement connue sous le nom BS:7799-1 cette norme est maintenant connue sous l'appellation en titre et porte le numéro ISO:27002, elle est aussi encadrée par le sous-comité ISO 27000.

La norme ISO/IEC 27002 :2005 établit les lignes directrices ainsi que les principes généraux nécessaires à l'initiation, l'implantation, la maintenance et l'amélioration de la gestion de la sécurité de l'information en entreprise. Bien noter qu'on ne parle pas ici de l'amélioration du système de gestion mais bien de sa gestion elle-même.

En effet, et contrairement à la norme ISO:27001, les objectifs définis dans cette norme ne couvrent pas le Système de Management de la Sécurité de l'Information, mais bien les contrôles généralement acceptés par l'industrie nécessaires à la maîtrise de la sécurité en entreprise. Ce document est donc un compagnon essentiel et indissociable à la 27001. Les bonnes pratiques et contrôles définis dans la norme sont groupés dans les 11 catégories suivantes :

1. Politique de sécurité
2. Organisation de la sécurité de l'information
3. Gestion des biens
4. Sécurité liée aux ressources humaines
5. Sécurité physique et environnementale
6. Gestion de l'exploitation et des télécommunications
7. Contrôle d'accès
8. Acquisition, développement et maintenance de systèmes d'information
9. Gestion des incidents liés à la sécurité de l'information
10. Gestion du plan de continuité des activités
11. Conformité

Dans les faits, la norme ISO:27001 s'attend, tel que décrite dans son annexe, que les objectifs de contrôles ainsi que les contrôles décrits en détail dans la norme ISO:27002 soient implantés, et ce, afin de traiter les divers risques identifiés par l'organisation.

L'objectif premier de cette norme est, et a toujours été, d'être une base de référence et de communication commune pour les professionnels de l'industrie afin de permettre l'établissement de processus organisationnels en respectant une norme, promouvant ainsi un langage normalisé et jetant les bases de confiance par l'utilisation d'un système commun extra-organisationnel.

## Profil de l'entreprise

Fondée en 1999, Above Sécurité est aujourd'hui l'une des plus grandes compagnies canadiennes spécialisées uniquement en sécurité de l'information. Notre mission consiste à soutenir nos clients dans l'amélioration de leur posture et de leur gouvernance en sécurité de leur système d'information.

Nos solutions ainsi que notre portefeuille de service-conseil aident nos clients du point de vue de la conformité, de l'intégrité, de la disponibilité et de la confidentialité.

Forte de plus de 200 entreprises, notre clientèle s'étend dans une vingtaine de pays distribués dans les trois Amériques, l'Europe, les Caraïbes et l'Afrique. Notre clientèle se compose principalement d'entités gouvernementales et d'entreprises privées du Fortune 500 dans les secteurs financiers, pharmaceutiques et des télécommunications.

## Contactez-nous

### Above Sécurité Canada

1919 Lionel Bertrand, bureau 203

Boisbriand (QC) Canada, J7H1N8

**Téléphone :** (450)430-8166

**Fax :** (450) 430-1858

**Courriel :** [info@abovesecurite.com](mailto:info@abovesecurite.com)

### Président & Chef de la Direction

Marcel Dion, CGA

Téléphone : (450) 434-8055

[Marcel.dion@abovesecurite.com](mailto:Marcel.dion@abovesecurite.com)

### Vice-président, Opération

Daniel Gaudreau

Téléphone : (450) 434-8046

[Daniel.gaudreau@abovesecurite.com](mailto:Daniel.gaudreau@abovesecurite.com)

### Chef de la Direction Technologique

Martin Dion, CISSP/CISM

Téléphone : (450) 430-8166

Mobile : +41.79.516.0447

[Martin.dion@abovesecurite.com](mailto:Martin.dion@abovesecurite.com)

### Vice-président, Conseil Stratégique

Guy Langevin, Ing.

Téléphone : (450) 434-8051

[Guy.Langevin@abovesecurite.com](mailto:Guy.Langevin@abovesecurite.com)

[www.abovesecurite.com](http://www.abovesecurite.com)

## Copyright

Les informations contenues dans ce document sont la propriété exclusive d'Above Sécurité. Toute reproduction complète ou partielle de ce document est interdite. Ce document est exclusivement destiné à l'usage interne d'entreprises n'offrant pas de services-conseils en technologie de l'information et/ou en gouvernance ainsi qu'aux divers gouvernements municipaux, provinciaux ou fédéraux.