

Technologies de l'information

PERFORMANCE DES SERVICES INFORMATIQUES ET SÉCURITÉ DE L'INFORMATION

Parmi les référentiels relatifs aux systèmes d'information, deux normes publiées par le BSI (British Standards Institute) ont été acceptées au niveau de la normalisation internationale pour devenir les normes ISO/CEI 20000:2005 (Technologies de l'information - Gestion des services) et ISO/CEI 27001:2005 (Technologies de l'information - Systèmes de management de la sécurité de l'information - Exigences).

La norme ISO/CEI 20000:2005

La norme ISO/CEI 20000, publiée en 2005, est la première norme internationale traitant de la gestion des services informatiques. Elle annule et remplace la norme BS 15000 publiée par le BSI en 2000, dont elle est issue. La norme ISO/CEI 20000 s'appuie sur les recommandations d'ITIL (Information Technology Infrastructure Library), ensemble de bonnes pratiques en matière de gestion des services liés aux technologies de l'information.

La norme ISO/CEI 20000 est composée de deux parties présentant la même structure :

- l'ISO/CEI 20000-1:2005 (disponible en français) définit les exigences minimales d'une gestion des services informatiques maîtrisés à l'intention des fournisseurs de services informatiques ; ceux-ci peuvent demander, à un organisme indépendant, une certification de leur système de management des services informatiques ;
- l'ISO/CEI/20000-2:2005 est un guide de bonnes pratiques dont l'objet est de décrire

concrètement les réponses possibles aux exigences de la partie 1.

La norme ISO/CEI 20000-1 est un référentiel de management de la qualité spécifique au métier de fournisseur de services informatiques. Elle reprend, bien entendu, les principes du management de la qualité, notamment :

- l'orientation client ;
- le management par les processus et l'approche systémique ;
- l'amélioration continue par la mise en application de la boucle PDCA (Plan, Do, Check et Act du cycle de Deming).

La norme ISO/CEI 20000-1 s'adresse aux directions des systèmes d'information (DSI) des entreprises et aux fournisseurs externes, par exemple les infogérants ou hébergeurs. Elle facilite le dialogue et la compréhension entre les différents acteurs par un vocabulaire commun : entre le fournisseur de services et la direction générale de l'entreprise, entre le fournisseur de services et les utilisateurs des services, entre le fournisseur de services et ses équipes, entre la DSI et les prestataires externes.

La norme ISO/CEI 20000-1 ne porte pas sur la qualité des produits (intranet, application de gestion commerciale, application de gestion de la production, etc.) mais sur la qualité du service rendu. La qualité de service se caractérise par : la continuité de service en cas d'incident, la capacité (en termes de volumétrie), la disponibilité des services, la



fiabilité des services et la sécurité (intégrité, confidentialité, disponibilité).

La qualité de service est définie au moyen d'objectifs mesurables sur lesquels la performance de l'organisation des fournisseurs de services peut être évaluée. Ces objectifs sont traduits dans des accords de niveaux de services. Le but est d'aligner les services rendus sur les besoins "métier" de l'entreprise.

Cette norme est constituée de quatre groupes de processus :

1. les processus de pilotage tels qu'ils sont définis dans la norme ISO 9001:2000 (engagement de la direction, gestion documentaire, gestion des ressources, planification et amélioration continue) ;
2. les processus de fourniture des services où l'accent est mis sur la planification et l'amélioration à moyen/long terme des services (gestion des niveaux de services, rapport de service, gestion de la continuité et de la disponibilité, comptabilisation et budgétisation, gestion de la capacité, gestion de la sécurité) ;
3. les processus de support des services où l'accent est mis sur les opérations quotidiennes et le support (gestion des incidents, gestion des problèmes, gestion des configurations, gestion des changements, mise en production) ;
4. les processus de gestion des relations (gestion des relations commerciales, gestion des fournisseurs).

Pour le fournisseur de services informatiques qui souhaite mettre en place la norme ISO/CEI 20000-1, trois approches sont possibles :

- compléter le système de management de la qualité ISO 9001 existant en y intégrant les exigences spécifiques de la norme ISO/CEI 20000-1 ;
- implémenter les processus ITIL, puis développer les exigences spécifiques d'un système de management selon la norme ISO/CEI 20000-1 ;
- implémenter la norme ISO/CEI 20000-1 de manière isolée.

Pour mettre en œuvre cette norme, la première question que le fournisseur de services informatiques doit se poser est la suivante : quels sont les objectifs "métier" de l'entreprise cliente ?

Il réalise, ensuite, un état des lieux de ses

services informatiques par rapport aux objectifs de l'entreprise cliente et définit ses propres objectifs en tenant compte de ses ressources et contraintes. Les résultats de ces activités sont un catalogue des services offerts et des contrats de services établis avec ses clients. Puis le fournisseur de services détermine le programme d'amélioration de la gestion des services et le met en œuvre. Enfin, il mesure l'atteinte des objectifs et met en place les plans d'amélioration.

Au même titre que pour la mise en place de la norme ISO 9001:2000, le fournisseur de services informatiques doit :

- adopter le regard du client sur les services fournis ;
- définir le service sous forme de résultat attendu par le client ;
- mesurer les services offerts aux clients et non pas les performances techniques.

Il ne doit pas appliquer les exigences de la norme dans le seul but de... répondre à la norme. Les exigences dans leur ensemble ont une finalité et donnent un sens à la démarche : elles permettent au fournisseur de services informatiques de privi-

léger la voix du client, de se focaliser sur la création de valeur et de favoriser l'amélioration de ses performances.

La norme ISO/CEI 20000-1 est un support méthodologique efficace et la certification une garantie que le fournisseur de services informatiques pourra mettre en avant pour démontrer qu'il a pris les meilleures dispositions possibles. Il gagnera en termes :

- de perception par le client utilisateur de la qualité de bout en bout des services informatiques ;
- de maîtrise des services informatiques et à qualité constante ;
- d'amélioration de sa productivité ;
- de maîtrise des coûts.

En matière de sécurité, la norme ISO/CEI 20000-1 recommande l'utilisation du référentiel ISO/CEI 17799 (renuméroté ISO/CEI 27002 en 2007) "Technologie de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information", norme à laquelle l'ISO/CEI 27001 "Technologie de l'information - Techniques de sécurité - Exigences" fait appel pour la mise en place des mesures

de sécurité. Le management de la sécurité s'appuie donc sur un référentiel spécifique qui reprend lui aussi les concepts classiques des systèmes de management.

La norme ISO/CEI 27001

Au même titre que la norme ISO 9001 est un référentiel relatif aux systèmes de management de la qualité, la norme ISO/CEI 27001 est un référentiel relatif aux systèmes de management de la sécurité de l'information (SMSI). L'objectif est, pour une entreprise, d'améliorer la manière dont elle gère la confidentialité, l'intégrité et la disponibilité des informations qui constituent son patrimoine informationnel.

La norme ISO/CEI 27001, publiée en 2005 et disponible en français depuis juillet 2007, est issue de la norme BS 7799-2 publiée par le BSI en 1998. Elle est un pilier qui est complété par une série de guides associés :
 - l'ISO/CEI 27002⁽¹⁾ détaille les mesures de sécurité contenues dans l'annexe normative de l'ISO 27001 ;
 - l'ISO/CEI 27003 est un guide de mise en œuvre d'un SMSI dont la publication est prévue en 2009 ;
 - l'ISO/CEI 27004 est un guide de mesurage du SMSI qui explique comment mettre en œuvre des indicateurs pour un SMSI et dont la publication est prévue en 2008 ;
 - l'ISO/CEI 27005 est un guide de gestion de risques pour un SMSI dont la publication est également prévue pour 2008 ;
 - l'ISO/CEI 27006, publiée en janvier 2007, s'adresse aux organismes de certification d'un système de management de la sécurité de l'information.

La norme ISO/CEI 27001 a adopté, comme toutes les normes de systèmes de management, les principes de la qualité tels que l'approche processus et l'amélioration continue par la mise en application de la boucle PDCA. La mise en place d'un système de management de la sécurité de l'information permet d'entrer dans un processus d'amélioration de la gestion de la sécurité de l'information. Cette gestion porte, principalement, sur ►►

(1) Par souci de cohérence, la norme ISO 17799 (ancienne norme BS 7799-1) a été renumérotée ISO 27002 en juillet 2007. Cependant, cette norme est très populaire dans le monde de la sécurité des systèmes d'information sous son ancien numéro ISO 17799. Le contenu des normes ISO 17799:2005 et ISO 27002:2005 est identique.

ce qui touche à la sécurité du système d'information, c'est-à-dire ce qui concerne les outils informatiques. Même si certaines mesures de sécurité s'attachent à ce que des documents de valeur ne traînent pas dans les bureaux, c'est bien la sécurité informatique qui est au cœur de la norme. C'est pourquoi cette norme s'adresse en grande partie aux équipes informatiques.

Cependant, à la différence de la norme ISO/CEI 20000-1, ce n'est pas la direction des systèmes d'information qui sera propriétaire de ce système de management, mais le responsable sécurité, couramment appelé RSSI pour responsable de la sécurité du système d'information.

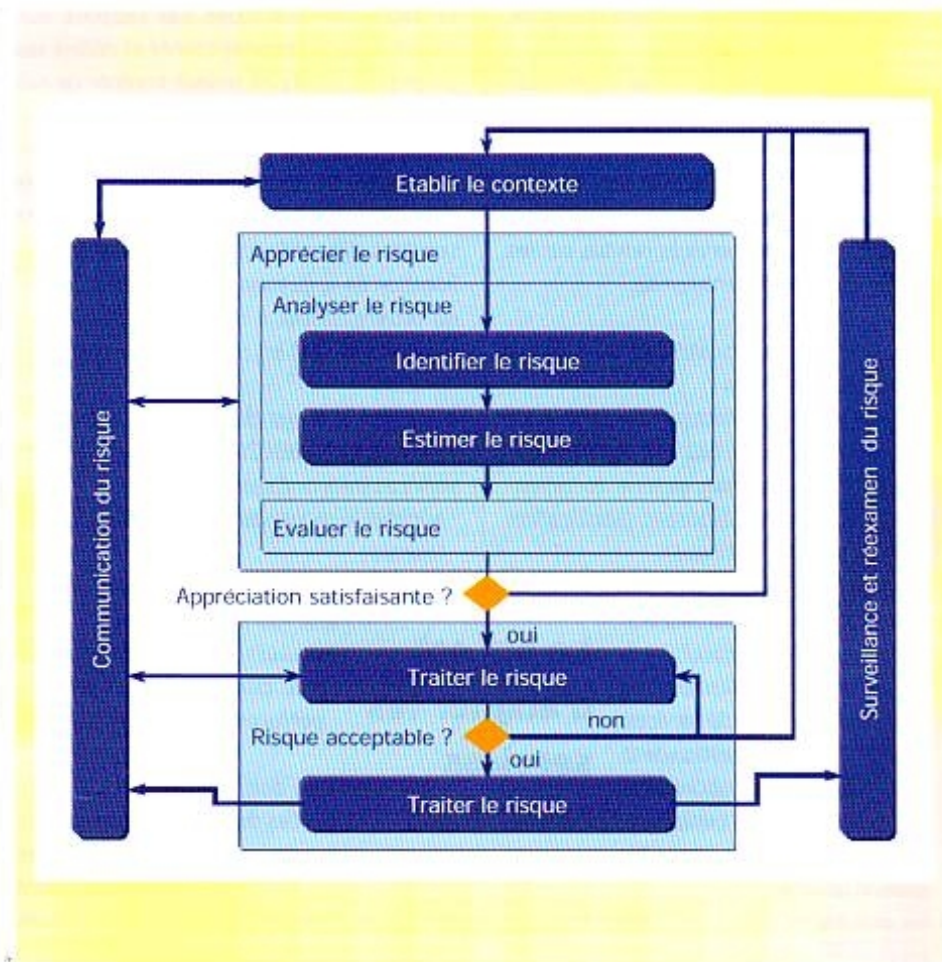
Le processus de sécurité de l'information est un processus transversal qui touche à l'ensemble des métiers et qui bouleverse généralement les habitudes de travail, même quand la norme ISO 9001 est en place.

La mise en œuvre d'un système de management de la sécurité de l'information basé sur la norme ISO/CEI 27001 est une décision stratégique : l'engagement de la direction générale, sans laquelle rien n'est possible, est incontournable. Une fois la décision prise, la démarche de mise en œuvre est la suivante :

- choisir un périmètre et déterminer une politique de sécurité de l'information ;
- établir la liste des actifs de l'entreprise ;
- appliquer une appréciation des risques sur ces actifs sachant qu'elle doit donner des résultats reproductibles et comparables ;
- en déduire des mesures de sécurité (en s'appuyant sur celles proposées par la norme ISO/CEI 27002) qui vont permettre de réduire les risques à un niveau acceptable pour la direction générale ;
- mettre en œuvre les mesures de sécurité choisies ;
- vérifier la mise en œuvre et l'efficacité des mesures ;
- et, bien sûr, reboucler pour s'améliorer.

Un système de management de la sécurité de l'information comprend, au minimum :

- des éléments documentaires (politique, objectifs, cartographie des processus impactés, activités de sécurité, mesures) et les enregistrements issus des activités relatives à la sécurité de l'information ;
- une méthode d'analyse des risques ;
- les processus impliqués dans la sécurité de l'information ;



- les responsabilités relatives à la sécurité de l'information ;
- les ressources nécessaires à la mise en œuvre du SMSI ;
- les mesures et les actions d'amélioration du SMSI.

L'objectif de la norme ISO 27001 est d'améliorer la manière dont une entreprise gère son patrimoine informationnel.

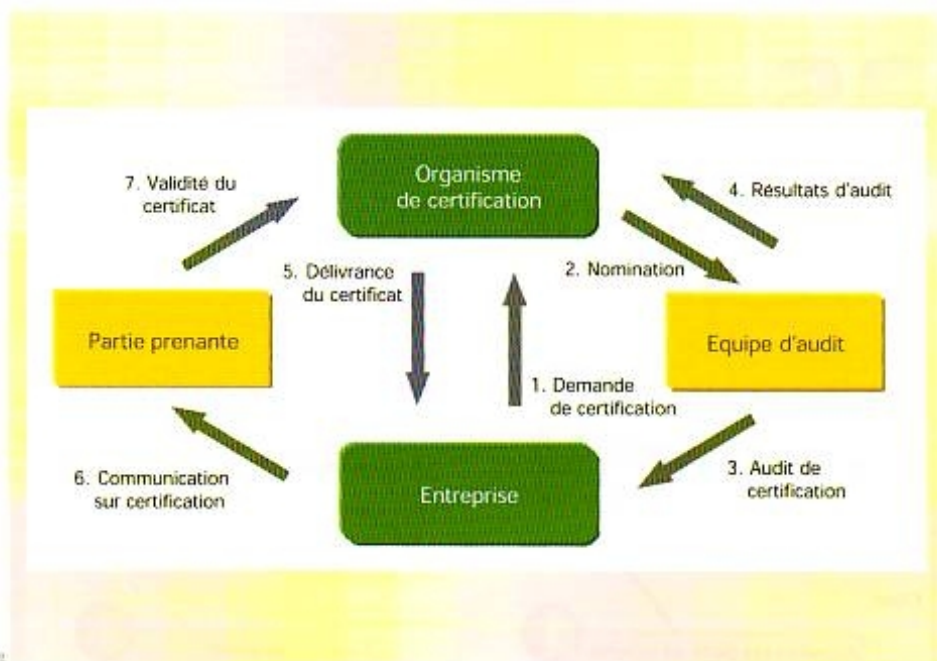
Lorsque la norme ISO 9001 est en place, des principes tels que l'approche processus, l'amélioration continue ou la gestion des documents sont acquis par l'entreprise. Cependant, l'expérience montre que la mise en œuvre de la norme ISO/CEI 27001 impose au responsable de la sécurité du système d'information (RSSI) un travail auquel il n'est

pas habitué, par exemple :

- la mise en place d'une sensibilisation à la sécurité de l'information auprès de tout le personnel, c'est-à-dire allant au-delà du périmètre du SMSI ;
- la mise en place d'un processus d'audit interne du SMSI ;
- la conservation des enregistrements de ce qui a été fait.

Le responsable sécurité doit construire une gestion de risques s'inscrivant, elle aussi, dans un cycle d'amélioration continue. Il doit redévelopper une appréciation des risques périodiquement, en revalidant avec les propriétaires des processus métiers, afin de bien concentrer la mise en œuvre des mesures de sécurité sur ce qui compte réellement le plus pour l'entreprise et donc réduire les risques les plus importants. Même si cette appréciation des risques ("analyse de risque") était déjà l'une des bases de la sécurité des systèmes informatiques, le fait de l'intégrer dans un processus cyclique est nouveau.

À l'image de la qualité, la sécurité de l'information est affaire de bon sens et d'un minimum de rigueur. L'entreprise doit



adopter une démarche pragmatique s'inscrivant dans le temps avec des objectifs successifs réalistes.

La norme ISO/CEI 27001 est rapidement adoptée par les entreprises, car elle représente un "espéranto" en matière de sécurité des systèmes d'information. De très nombreuses entreprises, qui ne voient pas d'intérêt à la certification car elles n'ont pas de parties prenantes qui le leur demandent, en utilisent d'ores et déjà les principes.

Aperçu de la certification selon les normes ISO/CEI 20000-1 et ISO/CEI 27001

Comme nous l'avons vu précédemment :

- la norme ISO/CEI 20000-1:2005 spécifie les exigences relatives aux systèmes de management des services informatiques ;
- la norme ISO/CEI 27001:2005 spécifie les exigences relatives aux systèmes de management de la sécurité de l'information.

Ces deux normes sont des normes d'exigences qui permettent une certification de conformité. Contrairement à la norme ISO 9001 qui accepte des exclusions, aucune exclusion d'exigence n'est admise lorsqu'une entreprise demande une certification ISO/CEI 20000-1 ou ISO/CEI 27001.

La certification selon ces normes se déroule selon le même processus que pour les normes de type ISO 9001, ISO 14001, etc. :

un certificat a une durée de validité de 3 ans, avec un audit annuel (ou semestriel à la demande de l'entreprise) réalisé par l'organisme de certification.

Les intérêts des normes ISO/CEI 20000-1 et ISO/CEI 27001 sont multiples : avantage concurrentiel, amélioration de la maîtrise des services informatiques et des coûts liés aux prestations pour la norme ISO/CEI 20000-1, augmentation du niveau de sécurité pour la norme ISO/CEI 27001, etc.

Le nombre de certificats ISO/CEI 27001 a très nettement progressé.

L'un des avantages majeurs de la norme ISO/CEI 27001 est pour les fournisseurs. En effet, le certificat de conformité tierce partie vaut présomption de fiabilité devant les tribunaux : dans l'affrontement après sinistre ou incident majeur, l'organisation certifiée conforme à la norme aura très certainement le dessus par rapport à celle qui ne l'est pas, ne serait-ce que parce qu'elle aura l'ensemble des preuves et enregistrements de sécurité exigés par la norme.

Sauf cas particuliers, la certification aux normes de ce type est volontaire. Les entreprises françaises attendent un signal fort du marché pour aller à la certification. Pourtant, la mise en place d'un système de management, quelle que soit sa nature (qualité, environnement, sécurité, etc.), demande du temps. Il s'agit davantage d'inculquer une culture et une façon de travailler que de

Depuis sa publication par l'ISO (Organisme international de normalisation) en tant que norme internationale, le nombre de certificats ISO/CEI 27001 a très nettement progressé dans tous les secteurs d'activité. Fin août 2007, il y avait 2 323 certificats, hors Japon, enregistrés sur le site de l'association internationale ISMS User Group, notamment :

- Royaume-Uni : 352 ;
- Allemagne : 73 ;
- États-Unis : 52 ;
- Italie : 44 ;
- Espagne : 12 ;
- France : 5.

→ www.iso27001certificates.com

En matière de certificats ISO/CEI 20000-1, le site de l'itSMF présente les chiffres suivants (fin septembre 2007) :

- Royaume-Uni : 23 ;
- Japon : 16 ;
- Allemagne : 12 ;
- États-Unis : 3.

→ www.isoiec20000certification.com

À fin août 2007, trois entreprises françaises sont certifiées.

rédigier des procédures. Quand un appel d'offres impose une certification, il n'est plus temps si l'entreprise ne s'y est pas déjà préparée. Comme pour leur parente ISO 9001, il y a fort à parier qu'une certification selon les normes ISO/CEI 20000-1 et ISO/CEI 27001 sera de plus en plus exigée par les clients et les donneurs d'ordre ■

Sylvie Durand⁽²⁾,
Hervé Schauer⁽³⁾,
Armelle Troitin⁽⁴⁾

(2) Sylvie Durand Consultant, www.sdconsultant.com.

(3) Hervé Schauer Consultants, www.hsc.fr.

(4) Armelle Troitin - LSTI, www.lsti.fr.