



# >> Certification ISO 27001 : passer à l'offensive pour protéger ses informations



La certification ISO 27001 couvre la conception des logiciels, l'utilisation d'internet mais aussi la sécurité physique comme l'accès aux locaux.

*ISO 27001 certification acts on physical security (access to the premises) and logical security (software conception, use of internet).*

## En fin d'année 2010,

Wikileaks dévoilait des milliers de documents confidentiels. Mars 2011, 150 ordinateurs de Bercy ont subi une attaque informatique. Dernier événement en date, le service de jeu vidéo en ligne de Sony défraie la chronique : les données sécurisées de 77 millions de clients ont été dérobées. Le préjudice se chiffre en milliards de dollars, sans compter l'impact d'image. L'information rime aujourd'hui avec pouvoir et enjeux financiers considérables. Depuis vingt ans, les systèmes d'information se sont multipliés, au point que « la dépendance des entreprises et de l'administration est majeure », estime Philippe Bourdalé, chef de produit chez AFNOR Certification. Se prémunir suppose de réagir contre une multiplicité de menaces, du bug au piratage en passant par l'usurpation d'identité numérique ou la traditionnelle vente d'informations à la concurrence. Le besoin de sécurité concerne

toutes les organisations. Mais pour faire face, des outils existent.

## Délimiter les champs de la sécurité

« La normalisation anglaise a été la première à s'emparer du sujet, avec le standard BS-7799 publié en 1995. L'ISO l'a ensuite repris et révisé pour élaborer la norme 27001 en 2005, qui propose un système de management pour gérer la sécurité des systèmes d'information (SSI) », retrace Jean-Pierre Quémard, directeur réseaux et télécoms chez Cassidian (EADS) et président de la commission de normalisation. « Il consiste à charger des personnes de la sécurité de l'information, à traduire une politique de sécurité en actions, puis à mesurer sa réalisation », explique Philippe Bourdalé. Il vise aussi à agir sur la sécurité physique (accès aux locaux, protection des postes de travail et des serveurs...) et sur la sécurité logique (conception des logiciels, utilisation d'internet...). » La famille des normes ISO 27000 comprend une quinzaine de textes balayant vocabulaire, bonnes pratiques, gestion des risques ou exigences sectorielles. Un arsenal d'outils, qui invite les organisations à considérer leurs systèmes d'information au sens large.

## ISO 27001 certification: Take the offensive to protect your information

*At the end of 2010, Wikileaks disclosed thousands of confidential documents. March 2011, 150 computers from the French Ministry of Economy and Finances were hacked. Last but not least, Sony's online videogame service makes the headlines: the secure data of 77 million clients have been stolen. The financial loss runs in billions, notwithstanding the image impact. Information today rhymes with power and considerable financial issues. For over twenty years, information systems have been on the increase, so much so that "the companies and civil services' dependency is now massive", considers Philippe Bourdalé, head of product at AFNOR Certification. To protect oneself means reacting to numerous threats, from bugs to hacking, numeric identity theft or more traditionally, sale of strategic information to the competition. Every organisation needs security and tools exist to provide it.*





La certification ISO 27001 permet de mieux gérer le risque de rupture d'activité en cas de sinistre.

*ISO 27001 certification also allows companies to manage the operational breakdown risk in case of a disaster.*

« Pensez à la quantité de données obtenue en regardant au-dessus d'une épaule dans un train ! L'ISO 27001 couvre tous les supports d'information, de l'ordinateur portable à la sécurité incendie en passant par les comportements individuels », souligne Philippe Bourdalé.

### Une assurance pour le client

Dans ce contexte, la certification permet de consolider la confiance entre une entreprise et ses clients en démontrant les moyens mis en œuvre au service de la sécurité des informations. Atos Origin, groupe international d'infogérance certifié ISO 27001 depuis septembre 2010 le confirme : « nos clients nous confient la gestion de leurs infrastructures informatiques : nous nous devons de leur offrir un niveau de sécurité maximum », insiste Paul Bayle, directeur de la sécurité. À ses yeux, le référentiel a permis « d'enrichir les processus d'analyse de risques par le biais d'une méthodologie rigoureuse, d'améliorer la sensibilisation à la sécurité et de tenir le système à jour plus régulièrement ». Même témoignage chez Michel Quinton – responsable de la triple certification ISO 9001/20000-1/27001 d'Orange Business Services : « la certification ISO 27001 nous permet de prouver la solidité de la SSI de nos centres situés à l'étranger, qui traitent les données stratégiques de nos clients ».

### Éviter les ruptures d'activité

Dans une optique d'intelligence économique, la construction d'un système de management

de la SSI garantit la préservation des informations stratégiques comme des dernières innovations. « L'ISO 27001 permet en outre de mieux gérer le risque de rupture d'activité en cas de sinistre – catastrophe naturelle, virus informatique –, en poussant les entreprises à prévoir un site de secours, relais du système défaillant », note Philippe Bourdalé.

La certification n'est cependant pas gage de risque zéro, met en garde Marcel Schipman, auditeur AFNOR. « Les mesures liées à une démarche ISO 27001 rendent le niveau de risque acceptable et gérable, mais ne le suppriment pas. » Instaurer une revue régulière des points clés de vigilance multiplie néanmoins les chances de succès : « la revue des actifs et l'analyse des risques sont fondamentales. Pour être efficaces, elles doivent être exhaustives, hiérarchisées et renouvelées régulièrement. » La mutation continue des techniques, de technologies et des réglementations impose en effet une veille permanente. L'auditeur insiste enfin sur la sensibilisation des collaborateurs à la sécurité. « La fraude est d'origine interne à 70 %. Communiquer sur les mesures de sécurité et sur les succès du système de management de la SSI est à terme dissuasif. »

### Defining security's scope

*“British standardisation was the first to take on the subject with the BS-7799 standard, published in 1995. ISO then picked it up and revised it to draw up the ISO 27001 standard in 2005, which proposes a management system designed for information security”, recounts Jean-Pierre Quémard, Research & Technology Director at Cassidian (EADS) and head of the standardisation commission. “This standard aims at putting somebody in charge of information security, at translating a security policy into actions, and then at measuring their implementation, explains Philippe Bourdalé. It also acts on physical security (access to the premises, workstation and server protection...) and logical security (software conception, use of internet...)”. The ISO 27000 standard family comprises fifteen documents addressing vocabulary, best practices, risk management and sectorial expectations. This whole battery of practical tools encourages organisations to consider their information systems in the widest sense possible. “Just think about the mass of information one can learn just by glancing over a shoulder in a train! ISO 27001 covers every information means, from the laptop to fire safety including individual behaviours”, insists Philippe Bourdalé.*

### A guaranty for the client

*In this context, certification strengthens the trust between a company and its clients by*

### Une accréditation preuve d'engagement

AFNOR Certification est depuis le mois de juin 2010 l'un des deux seuls organismes accrédité par le COFRAC\* pour son activité de certification selon la norme ISO/IEC 27001. « Cette accréditation volontariste assoit notre légitimité et notre compétence sur ce référentiel, et garantit à nos clients transparence et confidentialité », estime Philippe Bourdalé. Cette reconnaissance souligne également les moyens mis en œuvre autour de la norme et de son audit de certification : conseil stratégique, comité de surveillance et d'amélioration, qualification des auditeurs... Déjà leader sur le marché de la certification ISO 27001, AFNOR Certification démontre ainsi son engagement derrière ce référentiel et la volonté de soutenir l'essor de la sécurité de l'information, considérée comme un capital toujours plus stratégique.

\* AFNOR certification est accréditée par le COFRAC sur la certification de systèmes de management ISO 27001. La portée de cette accréditation n° 4-0001 est disponible sur [www.cofrac.fr](http://www.cofrac.fr)

### Proving commitment through accreditation

*Since June 2010, AFNOR Certification is one of the two organizations whose certification activities according to the ISO 27001 standard have been accredited by the COFRAC\* (French Accreditation Association). “This voluntary accreditation establishes our legitimacy and our competency on this framework. It guarantees transparency and confidentiality to our clients”, considers Philippe Bourdalé. This acknowledgement also underlines the means developed in order to support the standard and its certification audit: strategic consulting, supervisory and improvement committee, auditors' qualification process... Already leader on the ISO 27001 certification market, AFNOR Certification demonstrates its commitment for the development of this framework but also its support of information security, an evermore-strategic asset.*

\* Accreditation N°. 4-0001. Scope available at [www.cofrac.fr](http://www.cofrac.fr)

/ SUITE / FOLLOWING /

## Certification ISO 27001 : passer à l'offensive pour protéger ses informations

ISO 27001 certification: Take the offensive to protect your information

### La SSI se démocratise

Bien plus qu'une précaution technique, le management de la sécurité des systèmes d'information s'impose aujourd'hui comme un outil de pilotage stratégique. Pour le Cirtill, l'un des centres informatiques qui héberge et exploite les systèmes d'information de l'Urssaf, la certification ISO 27001 s'inscrit dans une « vision globale » : « nous avons intégré

la norme ISO 27001 pour faire face au renforcement de notre activité, précise Thierry Faivre, son directeur adjoint. Être le seul centre informatique de l'Urssaf certifié 9001/14001/27001 nous permet d'envisager plus sereinement les évolutions de notre secteur dans les 5 ou 10 ans à venir. De plus, l'ajout de la certification ISO 27001 à notre système de management entérine notre haut niveau

de professionnalisme. »  
« Cette certification représente un avantage compétitif croissant, ajoute Jean-Pierre Quémard. De plus en plus d'appels d'offres exigent de démontrer son niveau de sécurité et l'ISO 27001 pourrait progressivement devenir une condition d'entrée sur certains marchés. En six ans, cette norme est devenue une vraie référence ». Selon le dernier ISO Survey, près de 13 000 certificats ISO/CEI 27001 ont été délivrés en 2009. Soit 40 % de plus que l'année précédente. Parmi eux, trois hôpitaux taiwanais certifiés par AFNOR Certification en octobre 2010, ont par ce biais démontré leur engagement pour protéger les dossiers médicaux informatisés et rassurer leurs patients sur la confidentialité de leurs données personnelles. Et si la France ne compte aujourd'hui qu'une vingtaine de certifiés, « il existe depuis 2010 un vrai frémissement, observe Philippe Bourdalé. Le management de la SSI sort du périmètre des directeurs de la sécurité et entre dans le radar stratégique des dirigeants. » ■

awareness and keep the system up to date on a more regular basis". The same goes for Michel Quinton – in charge of Orange Business Services triple ISO 9001/20000-1/27001 certification: "the ISO 27001 certification enables us to prove the strength of the overseas centres that treat our client's strategic data".

### Avoiding operational breakdowns

From an economic intelligence perspective, building an information security management system guarantees the protection of strategic information as well as latest innovations. "ISO 27001 also allows companies to manage the operational breakdown risk in case of a disaster – catastrophe, virus – by prompting them to plan for a backup site, serving as a relay for the failing system", notes Philippe Bourdalé.

However, certification doesn't mean zero risk warns Marcel Schipman, an AFNOR auditor. "Security precautions implemented in the scope of an ISO 27001 approach make the risk level acceptable and manageable, but they don't suppress it." Scheduling regular reviews of key aspects nevertheless increases success rates. "The assets review and risk analysis are basics. In order to be efficient, they must be thorough, prioritized and periodically renewed." Indeed, the unceasing mutation of technologies and regulations require a constant watch. The auditor also emphasizes the importance of security awareness campaigns inside companies. "70% of all fraud comes from inside. Informing staff about security measures and about the information security management system's successes proves dissuasive."

### Information security becomes accessible

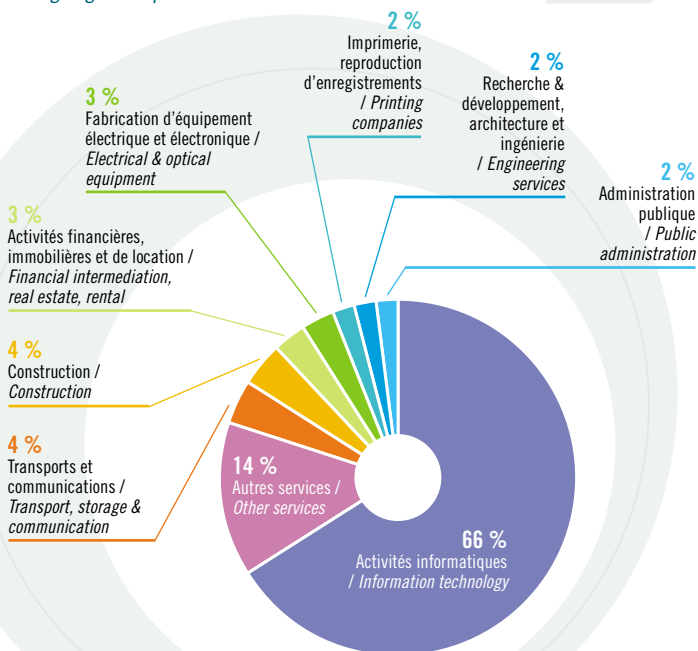
Far more than a technical security precaution, information security

## État des lieux de la certification ISO 27001

(étude ISO Survey - décembre 2009)

### ISO 27001 certification report (ISO Survey - 2009/12)

- > Forte expansion dans le monde, surtout en Asie et en Europe / Strong growth in the world, especially Asia and Europe
- > Près de 13 000 certificats / Nearly 13,000 certificates
- > Forte représentation des activités de services / Strong performance of service activities
- > Développement en cours dans les secteurs industriels / Ongoing development in industrial sectors



demonstrating the means implemented to ensure information security. Atos Origin, an international IT management group, has been certificated ISO 27001 since September 2010 and confirms: "our clients trust us with the management of their information technology infrastructures: it is our duty to provide them with the highest level of security", states Paul Bayle, head of Security. In his opinion, the framework helped "enhance the risk analysis process through a meticulous methodology, improve security



## La sécurité, tous concernés

Depuis 30 ans, les membres de la Commission nationale de l'informatique et des libertés (CNIL) scrutent les pratiques des entreprises, et aujourd'hui les réseaux sociaux, les moteurs de recherche, etc. pour protéger les libertés individuelles. Matthieu Grall compte parmi ces experts. Il est aussi vice-président du groupe de coordination de la sécurité des systèmes d'information du groupe AFNOR et éditeur de la norme 27001. Il livre son point de vue.

### Quelles formes peuvent prendre les atteintes à la sécurité des systèmes d'information (SSI) ?

**Matthieu Grall (MG) :** D'après les centres d'alerte et de réaction aux attaques informatiques (CERT), les principales attaques concernent les infections virales, l'envoi de *spams*, la compromission de serveurs web, l'ajout de codes malveillants sur les pages de sites web, les tentatives de *phishing* (usurpation d'identité)... Du côté des entreprises, les incidents sont plutôt des erreurs d'utilisation, la perte de services essentiels, des pannes d'origine interne, le vol ou la disparition de matériel. Pour les particuliers, l'escroquerie à la carte bancaire, les virus et logiciels espions restent préoccupants. Les internautes sont d'ailleurs de plus en plus sensibles à la protection de la vie privée et leurs exigences de sécurité se sont accrues.

### Renforcer la sécurité des systèmes d'information reste encore un objectif essentiel ?

**MG :** Oui. Elle vise à éviter les conséquences des menaces sur les organisations, qui peuvent se traduire par des pertes financières ou d'avantages concurrentiels, ou des impacts négatifs d'image. Mais aussi à protéger l'information, par nature volatile et reproductible, pour laquelle les organisations ont des besoins en termes de disponibilité, d'intégrité et de confidentialité. Une démarche de SSI permet de se prémunir contre différentes sources de risques émanant des collaborateurs, visiteurs, prestataires, concurrents, pirates informatiques, virus, sinistres physiques... Elle contribue enfin à réduire les vulnérabilités des supports de l'information. Dans le domaine de la protection de la vie privée, la SSI est également fondamentale. Dès qu'une donnée à caractère personnel est créée, tout responsable de traitement a entre ses mains un instrument susceptible de nuire, ce qui peut aller du désagrément (refaire des démarches administratives) au drame (suicide du fait d'une réputation anéantie). Chacun est donc concerné. L'étendue des vulnérabilités impose de gérer les risques, seul moyen ne pas se disperser devant la multitude des enjeux.

### Où en sont les entreprises françaises en matière de SSI ?

**MG :** Elles possèdent souvent un socle de fondamentaux ou ont formalisé une politique de SSI. Mais cette politique est souvent mise en œuvre de manière insuffisante. Une nouvelle étape doit être franchie : l'écriture des règles ne suffit plus, il faut les appliquer et prouver sa démarche. En cela, la certification ISO 27001 se révèle un outil précieux.

## Security, Everyone is Affected

*For the last 30 years, members of the French Information and Liberty Commission (CNIL) have been scrutinizing company practices, social networks, search engines, etc. in order to protect individual liberties. Matthieu Grall is one of these experts. He is also vice-president of the AFNOR Group information security systems coordination group and publisher of the ISO 27001 standard. He shares his thoughts.*

### How do breaches of information security systems manifest themselves?

**Matthieu Grall (MG) :** According to the Computer Emergency Response Teams (CERT), the main attacks nowadays consist of viral infections, spamming, compromising servers, adding malevolent codes on web sites, phishing attempts... On the business side, incidents are often related to misuse, loss of essential services, theft or equipment disappearance. As for private individuals, credit card fraud, virus and spywares remain worrying. For that matter, Internet users are increasingly sensitive to private life protection issues and their expectations in terms of security have risen.

### Strengthening information systems security thus remains a primary goal?

**MG :** Yes it does. It aims at avoiding the consequences of various threats on businesses. Those can manifest themselves through financial or competitive advantage loss, or through negative image impact. Security protects the information, volatile and repeatable by nature, and for which organisations need availability, integrity and confidentiality. An information security management approach aims to protect oneself against various sources of risk, coming from employees, visitors, providers, competitors, hackers, virus, and catastrophes... It contributes to reduce the vulnerabilities of the information supports. In the area of private life protection, information security is also of the essence. As soon as a personal data is generated, anyone processing it detains a potentially harmful tool, rating from inconvenience (if one has to redo administrative formalities) to tragedy (committing suicide following the destruction of one's reputation). Each and everyone can be affected. The scope of vulnerabilities calls for risk management, which is the only way to avoid dispersion faced with the mass of issues to address.

### Where do French companies stand in terms of information security?

**MG :** Most of them have the basics under control and even have a written information security policy. However, this policy is very often insufficiently implemented. They need to take a new step: writing rules is no longer enough; businesses must apply them and demonstrate their approach. In this aspect, the ISO 27001 proves to be a precious ally.

management is becoming a strategic instrument. The Cirtil is one of the centres which hosts and operates information systems for the French administration in charge of collecting professional social security contributions (Urssaf). For them, an ISO 27001 certification contributes to a "global vision: we integrated the ISO 27001 standard in order to cope with the increase of our activities, explains Thierry Faivre, deputy director. Being the sole computer centre of the Urssaf to have an ISO 9001/ISO 14001/ISO 27001 certification helps us consider our sector's evolutions in the ten years to come with more equanimity. Furthermore, the adjunction of the ISO 27001 standard to our management system confirms our high level of professionalism."

"Without a doubt, this certification represents a growing competitive advantage, adds Jean-Pierre Quémard. An increasing number of tenders contain demands regarding security level. ISO 27001 could very well become progressively a condition to penetrate certain markets. In a little over six years, this standard has become a reference." According to the last ISO Survey, around 13,000 certificates were delivered in 2009. A 40% increase compared to the previous year. Amongst them, AFNOR Certification certificated three Taiwan Hospitals in October 2010, thus proving their commitment to protect computerized medical files and reassuring their patients on their personal information's confidentiality. And even though France only counts 20 certificated companies, "one can feel a real change since 2010, observes Philippe Bourdalé. Information security management leaves the sole perimeter of security managers to enter the strategic radar of company leaders." ■

/ SUITE / FOLLOWING /

## Certification ISO 27001 : passer à l'offensive pour protéger ses informations

*ISO 27001 certification: Take the offensive to protect your information*



Défendre la confidentialité des informations, un enjeu pour Pôle Emploi.

*Information systems have to be up to scratch.*

## Pôle Emploi assure sa sécurité

Chaque jour, Pôle Emploi traite des milliers de données confidentielles. Pour garantir leur fiabilité, la Direction générale adjointe des systèmes d'information (DGASI) vient d'obtenir la certification ISO 27001. Retour d'expérience avec Lionel Duplaix, responsable qualité et maîtrise des activités.

1

### À quels enjeux la DGASI de Pôle Emploi doit-elle répondre ?

**Lionel Duplaix (LD) :** Notre politique de sécurité des systèmes d'information vise six objectifs. Assurer la continuité des services ; garantir la protection du matériel informatique et celle du patrimoine immatériel (applications, données de Pôle Emploi). Mais aussi conserver la confiance des usagers, notamment en défendant la confidentialité des informations que nous traitons. Le cinquième enjeu consiste à développer des canaux de communication protégés des intrusions et des pollutions. Enfin, nous nous devons de respecter les réglementations en vigueur et de suivre leurs évolutions.

2

### Qu'est-ce qui a motivé une certification ISO 27001 ?

**LD :** La DGASI est certifiée ISO 9001 depuis 2005, et la démarche a été généralisée à l'ensemble des services Pôle Emploi l'an dernier. Pour aller plus loin, la DGASI a décidé d'ajouter des normes ciblées sur les cœurs de métiers de l'informatique, ce qui a conduit à une certification combinée ISO 27001/ISO 20000-1. Ceci dans l'objectif de construire un système de management aussi intégré que possible. Nous voulions aussi faire reconnaître par un organisme indépendant le savoir-faire et le professionnalisme de nos équipes.

3

### Comment voyez-vous les retombées de cette démarche ?

**LD :** La préparation de la certification a permis de compléter les systèmes en place et de confronter formellement nos processus aux exigences de la norme. Par exemple, avant la certification, nous n'avions pas de déclaration d'applicabilité formalisée (liste de l'ensemble des contrôles de sécurité, NDLR). Elle a depuis été instaurée. La démarche recèle deux bénéfices majeurs. Dans un premier temps, l'audit fournit une mesure claire et impartiale du niveau de sécurité atteint et souligne les points d'amélioration à envisager. Ensuite, au quotidien, la sécurité du système d'information se voit intégrée dans la mise en œuvre des processus métiers. La DGASI a ainsi instauré une méthodologie pour incorporer la sécurité dans la conduite de projets. Elle oblige ainsi tout chef de projet à se poser la bonne question à chaque étape et à y répondre de manière formalisée. Nous avons donc aujourd'hui un historique de la prise en compte de la sécurité sur n'importe quel projet conduit par nos services.

## Pôle emploi Strengthens its Information Security Management System

*Clients' expectations regarding data security and confidentiality keep rising. Pôle emploi (the French equivalent of the Job Center) is no exception to the rule. Given this context, the deputy branch for information system (DGASI) led a successful ISO 27001 approach. Lionel Duplaix, head of quality and activity control shares his field experience.*

### Which strategic issues is Pôle emploi's DGASI confronted with?

**Lionel Duplaix (LD) :** First and foremost we need to address an issue, which is directly linked with our core service. Pôle emploi uses computers daily to ensure its missions (registration, compensation, job offers, statistics...). Therefore information systems have to be up to scratch in order to guarantee the continuity of the services delivered to our users. Besides, the ever-growing development of communication channels such as the Internet and telephony requires their protection, considering the risks these technologies are exposed to. Furthermore, we have to observe the legal obligations relating to information systems (CNIL, HADOPI, property rights...). But ultimately, the major issue is to preserve the trust our clients have in Pôle emploi.

### What drove you to move towards an ISO 27001 certification?

**LD :** This initiative constitutes an extension of previous actions. For several years now we have built an information systems security approach, based on a risk analysis and driven by general management. In addition, DGASI was certified according to ISO 9001, and at the time our management system already included some of the ISO 20000-1 and ISO 27001 expectations. Consequently, we decided to launch a combined ISO 20000-1/ISO 27001 certification. Finally, the governmental expectations towards civil services and administrations, such as conformity with the French General Security Framework – which aligns with the ISO 27001 approach –, consolidated our decision.

### What are the benefits of the approach?

**LD :** This process constitutes a true stepping-stone for information security. It consolidates the whole DGASI staff's awareness on information system security issues. Moreover the certification audit provided us with a clear and unbiased assessment of our security management level, based on basic notions and solid practices. Last but not least, obtaining an ISO 27001 certification also acknowledges our teams' know-how and professionalism.