L'auditeur face au chantier du GDPR

(*General Data Protection Regulation* ou Règlement sur la protection des données)

© robu_s - Fotolia.com

Un besoin d'adapter le programme d'audit interne aux besoins de la nouvelle règlementation

Georges Ataya, Professeur à **Solvay Brussels School of Economics and Management** et Associé gérant du cabinet de conseil **ICT Control SA**

Le nouveau règlement européen approuvé fin 2015 sera en vigueur à partir de mai 2018. Il est à craindre que les entreprises ne soient pas prêtes à temps même si elles commencent à se préparer dès à présent.
Le GDPR est une évolution logique suite à la première initiative européenne de 1995 appelée « Directive sur la protection des données ». Elle a été suivie en 2012 par l'obligation de notification des violations des données et en 2014 par le droit à l'oubli. Présentant des enjeux et des amendes faramineuses pour les acteurs économiques publics et privés, il impactera les activités d'audit et les processus de contrôle interne.

Obligations du GDPR

Les données à protéger sont celles du personnel, des clients, des fournisseurs, des prospects ou autres qui se trouvent sur tout ordinateur, serveur ou dispositif – nomade ou fixe – appartenant à l'entreprise. Il peut s'agir au-delà des fiches signalétiques, de simples échanges d'e-mails, de journaux d'activité, de logs techniques ou bien encore de données de traçage géographique ou technique des visiteurs de sites web. Ces données devraient être sécurisées de manière à les protéger contre le vol ou tous risques de divulgation à des tiers mettant en danger la vie privée des individus concernés.

L'entreprise qui détient les données possède la charge de la gestion de leur intégrité ainsi que celle de la détection de toute menace de leur intégrité et confidentialité. En cas d'incident de compromission des données, l'entreprise devra notifier l'autorité compétente dans les soixante-douze heures qui suivront la découverte. Et dans des cas spécifiques graves, elle devra aussi informer les individus concernés.
Le règlement impose l'obtention de l'autorisation des individus lorsque leurs données privées seraient rassemblées ou traitées. La conservation des données ne devra pas dépasser les besoins raisonnables liés à leur utilisation. De même, l'entreprise devra permettre aux individus l'accès aux informations les concernant ainsi que la possibilité de répondre à leurs demandes de modifier ou d'effacer ces données. Celles-ci ne pourront être transférées en dehors de l'Union Européenne que dans des cadres bien définis. De même, le traitement par des tiers, sous-traitants ou filiales, devra offrir les mêmes garanties de confidentialité.
Les autorités de contrôle vont pouvoir infliger des amendes administratives à concurrence de 20 millions d'euros ou de 4 % du chiffre d'affaires annuel si ce montant est plus élevé.

L'entreprise devra maîtriser à tout moment l'inventaire des données dont elle dispose, leur localisation, l'objet de leur collecte, le modèle de sécurisation, de stockage et de leur effacement. Pour prouver sa conformité à la directive, la société devra conserver les documentations pertinentes de manière à rassurer les autorités de contrôle lorsque nécessaire.

Certaines entreprises devront désigner un délégué à la protection des données, ou *Data Protection Officer* (DPO). Le responsable du traitement et le sous-traitant désigneront respectivement un délégué à la protection des données dans des cas spécifiques. Ce sera le cas lorsque le traitement est effectué par une autorité publique ou un organisme public ; lorsque les activités exigent un suivi régulier et systématique à grande échelle des personnes concernées et lorsque les activités consistent en un traitement à grande échelle de catégories particulières de données sensibles ou à caractère personnel relatives à des condamnations pénales ou à des infractions.
La règlementation concerne tous les acteurs, même ceux situés en dehors de l'union européenne dès qu'ils seraient amenés à traiter des données appartenant à des individus européens. Elle distingue les rôles de responsable du traitement et exécutant du traitement, ou sous-traitant ayant chacun leurs entières responsabilités. Les données nouvelles tels l'adresse IP, les données de géolocalisation et les identifiants techniques sont formellement identifiées et font partie des données considérées comme privées.

Modifications du contrôle interne

La mise en place de la règlementation nécessite une révision des contrôles internes et une mise en place des modifications nécessaires. Il s'agit d'actions à quatre niveaux : le niveau de la gouvernance et de l'organisation globale de la conformité ; le niveau des processus fonctionnels et de leurs adaptations ; le niveau des opérations et de la journalisation des traitements et l'inventaire des données et des activités et finalement le niveau des solutions technologiques nécessaires.

Ces exigences de conformité nécessiteront des chantiers importants. Les méthodes de travail de toutes les fonctions concernées de l'entreprise devront être adaptées. Les exigences fonctionnelles des applications informatiques actuelles et celles des applications en construction devront être actualisées. Les exigences non fonctionnelles seront renforcées pour confirmer les protections, les garanties de service et la documentation des opérations (*logs* des activités et journaux des incidents).

Des modifications importantes du contrôle interne seront nécessaires pour d'une part réaliser la conformité et d'autre part pour que cette conformité soit atteinte de manière optimale en coût, en effort et en risque.

> ***« Les sept leviers risquent d'être mis en place de manière séquentielle plutôt que simultanée, retardant du coup la date finale de la conformité effective »***

Les nouvelles règles actuelles de contrôle interne devront être revues rapidement, déjà en 2016, pour que les chantiers puissent débuter et pour que l'entreprise puisse être conforme au courant de l'année 2018.

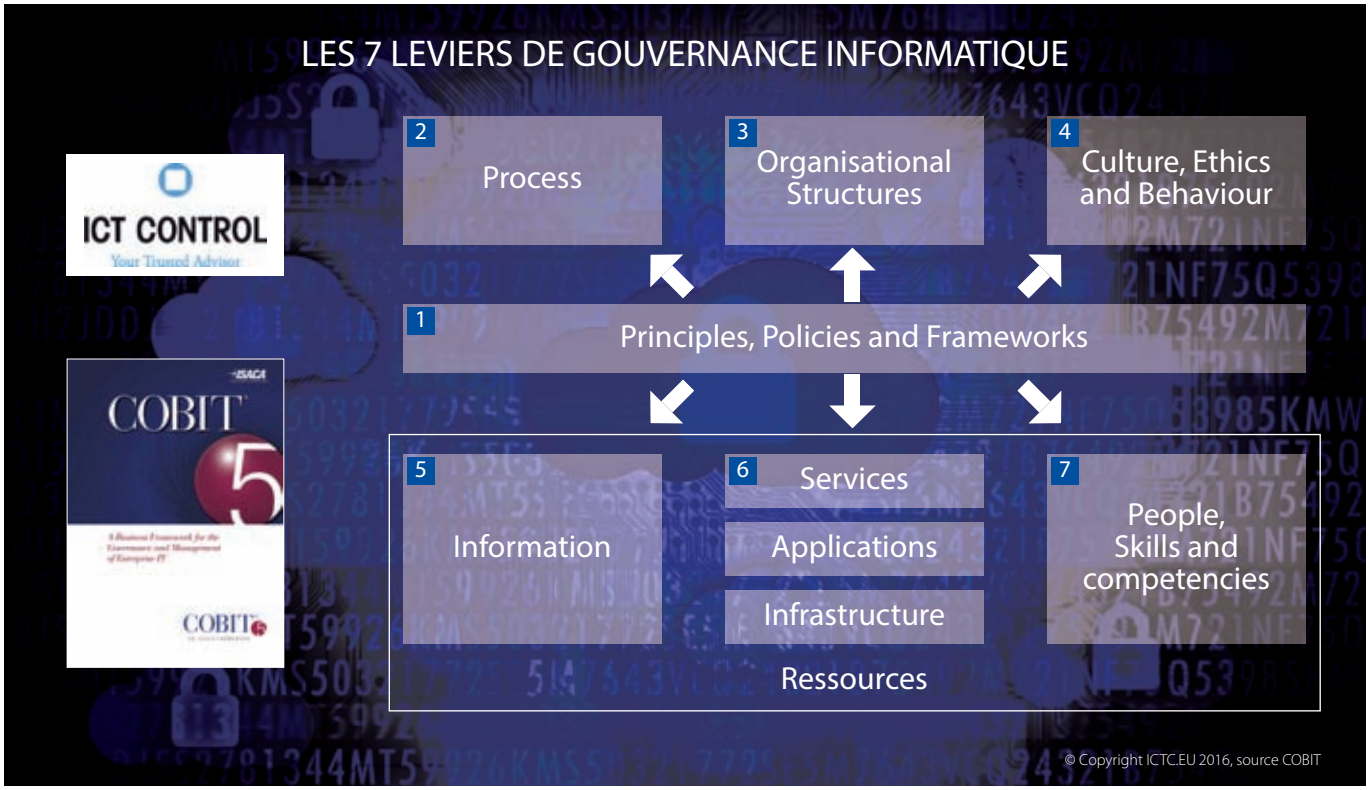
Le contrôle interne et sa maturité dépendent de leviers critiques. Si on se réfère à la définition du cadre COBIT, on cite alors sept leviers : le premier levier concerne la disponibilité des systèmes, des applications et des services. Le deuxième levier concerne le personnel qui devrait pouvoir consentir à un effort important face à ce changement en acquérant de nouvelles compétences. Le troisième levier est relatif à l'organisation qui devra être modifiée pour intégrer ces adaptations.
D'autres leviers tels que la disponibilité de l'information de gestion (quatrième levier), le développement de nouvelles politiques et règles de travail (cinquième levier) et finalement celui du comportement des employés, des fournisseurs et même des clients, sont à installer pour renforcer les contrôles utiles (sixième levier). Le septième levier consiste en une définition des processus et des activités de confidentialité commune à l'entreprise.
Il ne sera certes pas aisé de réaliser cette mise en place pourtant essentielle. Il est même à parier que pour des entreprises d'une certaine taille et d'une certaine inertie, les sept leviers risquent d'être mis en place de manière séquentielle plutôt que simultanée, retardant du coup la date finale de la conformité effective.

Besoins de sécurisation de l'information

La sécurité de l'information consistait dans le passé en des activités techniques comme l'installation de dispositifs de protection de l'infrastructure et de logiciel technique. Pour rappel, il s'agissait de pare-feu, de détecteurs d'intrusion ainsi que de programmes de mises-à-jour automatiques de nouvelles versions de systèmes d'exploitations et autres programmes de *middleware* (intergiciel).

Les risques ont bien évolué et les vulnérabilités ne sont plus limitées à la couche technique de l'infrastructure, notamment des serveurs et des réseaux. Elle atteint rapidement les couches les plus élevées puisque qu'elles concernent actuellement les données et les opérations essentielles à la poursuite des activités.

Les trois catégories de risques les plus courants sont la continuité des opérations, l'intégrité des données et de la confidentialité. Ces deux dernières catégories sont les plus concernées par le GDPR.



Plusieurs publications structurent l'entreprise numérique en une couche architecturale avec les composants suivants : infrastructure, applications, services, information et processus métiers.

La couche des applications semble actuellement être la plus négligée en ce qui concerne les risques inhérents et les besoins en efforts de sécurisation. La dette technique, c'est à dire la masse d'efforts nécessaires pour mettre les applications critiques à un niveau acceptable de sécurité, est souvent immense, comme régulièrement rapporté par plusieurs études spécialisées (par exemple : it-cisq.org/standards/technical-debt).
La couche applicative contient souvent des failles non documentées, des imperfections insérées naturellement par l'action humaine qui continue à construire du logiciel en artisanat parfois en oubliant les principes de base de construction de logiciel. Le nouveau standard ISO/IEC 27034 apporte à ce sujet des méthodes formelles de sécurisation des applications critiques.

La sécurité de l'information nécessite des activités sur toutes les couches architecturales. Parmi celles-ci citons-en quatre essentielles :

- **Activité 1 :** La gouvernance de la sécurité et la définition de sa responsabilité et de ses objectifs relatifs au GDPR. Il s'agit d'identifier les informations, services et autres actifs à protéger et définir les niveaux de protection.
- **Activité 2 :** L'analyse des risques (menaces, vulnérabilités attaques possibles...) et le développement de plans d'amélioration pour la mitigation de ces risques.
- **Activité 3 :** La mise en place de projets de protection qui concernent souvent les infrastructures, les applications, les données et leurs gestionnaires fonctionnels dans l'organisation.
- **Activité 4 :** Le développement des méthodes, de la communication et de la gestion potentielle de crise en cas d'incident.

> ***« La couche applicative est la couche architecturale la plus souvent négligée et elle nécessite des efforts de sécurisation immenses »***

Ces quatre activités constituent le corps de connaissance de la certification CISM (*Certified Information Security Manager* que l'auteur a contribué à développer en 2002. Il existe actuellement plus de 25 000 professionnels certifiés dans le monde).
Les menaces liées à la cyber sécurité augmentent d'année en année les exigences et les besoins de sécurisation. Les attaques contre les données privées, la menace de publication de ces données sur Internet avec chantage de rançon et le chiffrage des données sont devenus des cas très fréquents.

Il sera impératif de renforcer la capacité de défense nécessaire et suffisante pour assurer la conformité avec les nouvelles exigences de la règlementation GDPR. Parmi celles-ci citons les trois activités à ajouter aux quatre définies plus haut :

- **Activité 5 :** La détection rapide des incidents est déterminante pour réaliser une défense efficace. Or, il n'est pas rare de découvrir une attaque cyber criminelle plusieurs jours, semaines, voire mois après son premier enclenchement. Les processus et activités de détection nécessitent d'une part un renforcement des protections techniques et d'autre part l'adéquate conscientisation du personnel afin qu'il devienne le premier vecteur de détection. Celui-ci devra se familiariser avec tout indice inquiétant et reconnaitre les détecteurs d'anomalies et de signaux d'attaques.
- **Activité 6 :** La réponse appropriée aux attaques est essentielle. Les premiers

instants sont déterminants pour la gravité de l'envahissement et des conséquences subies. Le personnel devra apprendre à agir de manière adéquate selon le type de l'attaque. La direction devra éviter de communiquer sur l'incident, que ce soit en interne ou en externe, de manière maladroite et irrécupérable. Une notification légale devra parfois être préparée à l'avance et elle dépendra du type d'intrusion.

- **Activité 7 :** La récupération et le retour à une situation normalisée consistent à planifier déjà en avance et selon l'attaque, les dispositifs, les opérations, les modalités et les séquences nécessaires pour une remise à niveau saine. Des erreurs dans ce parcours peuvent susciter plus de dommages que ceux créés par l'attaque elle-même.

Les activités d'audit

Sur la base de ce qui précède, les activités d'audit sont essentielles pour donner une assurance sur les différentes étapes de mise en place de la conformité selon la règlementation GDPR.

Lors de la phase de développement des contrôles internes répondant aux risques, l'audit interne devra maîtriser les éléments suivants :

- La définition d'une stratégie d'attaque et de l'implication de tous les acteurs concernés par la directive. L'auditeur s'assurera que les différentes exigences et modalités de mise en place ont été attribuées à des décideurs au sein de l'entreprise.

> ***« Les activités d'audit sont essentielles pour donner une assurance sur les différentes étapes de mise en place de la conformité »***

Il faudra s'assurer que des activités fonctionnelles seront réalisées tels un cadre légal, des principes de protection de la confidentialité ; des rôles et des responsabilités ; une gestion du cycle de vie des données ; des processus adaptés aux concepts de confidentialité ; une classification des données ; une labellisation de l'information ; une sécurité des bases de données physiques et logiques et finalement une méthodologie de protection contre les fuites des données *(Data Leakage)*.

- L'existence d'une feuille de route détaillée et une gestion de la conformité en tant que programme intégré. Celui-ci devra recevoir la visibilité nécessaire et disposer d'un planning raisonnable vers l'horizon 2018 ainsi que d'un budget adapté.
- La réalisation d'une analyse des contrôles internes nouveaux et nécessaires à la conformité.

Lors de la phase de mise en place, Il devra développer son plan d'audit et ses missions sans faire l'économie d'un plan d'audit adapté à la spécificité de l'entreprise. Ceci est d'autant plus important que la règlementation mentionne la « Protection des données dès la conception » *(Privacy By Design)*. Ceci signifie qu'en cas de conception de nouveaux traitements, l'entreprise doit intégrer la protection des données à caractère personnel dès le début du processus. L'implication de l'auditeur dans les activités de conception des systèmes et de leurs architectures sera indispensable.
La refonte de l'organisation de sécurité devra s'accompagner d'une évaluation des sept activités de sécurité de l'information citées plus haut. Ceci comprend aussi l'analyse de l'adéquation des sept leviers.
Il est nécessaire dès lors d'analyser la description de fonction du DPO et évaluer sa capacité à réaliser ce qu'on attend de cette fonction.
Le processeur des données et ses sous-traitants éventuels doivent déclarer toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. L'audit des activités opérationnelles y compris celles des sous-traitants et de leurs risques devient une activité importante à ajouter aux plans d'audits annuels.

L'auditeur est un acteur important pour la réussite d'une mise en place de la conformité GDPR. ■

P. S. : Source du texte original du règlement GDPR : http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf