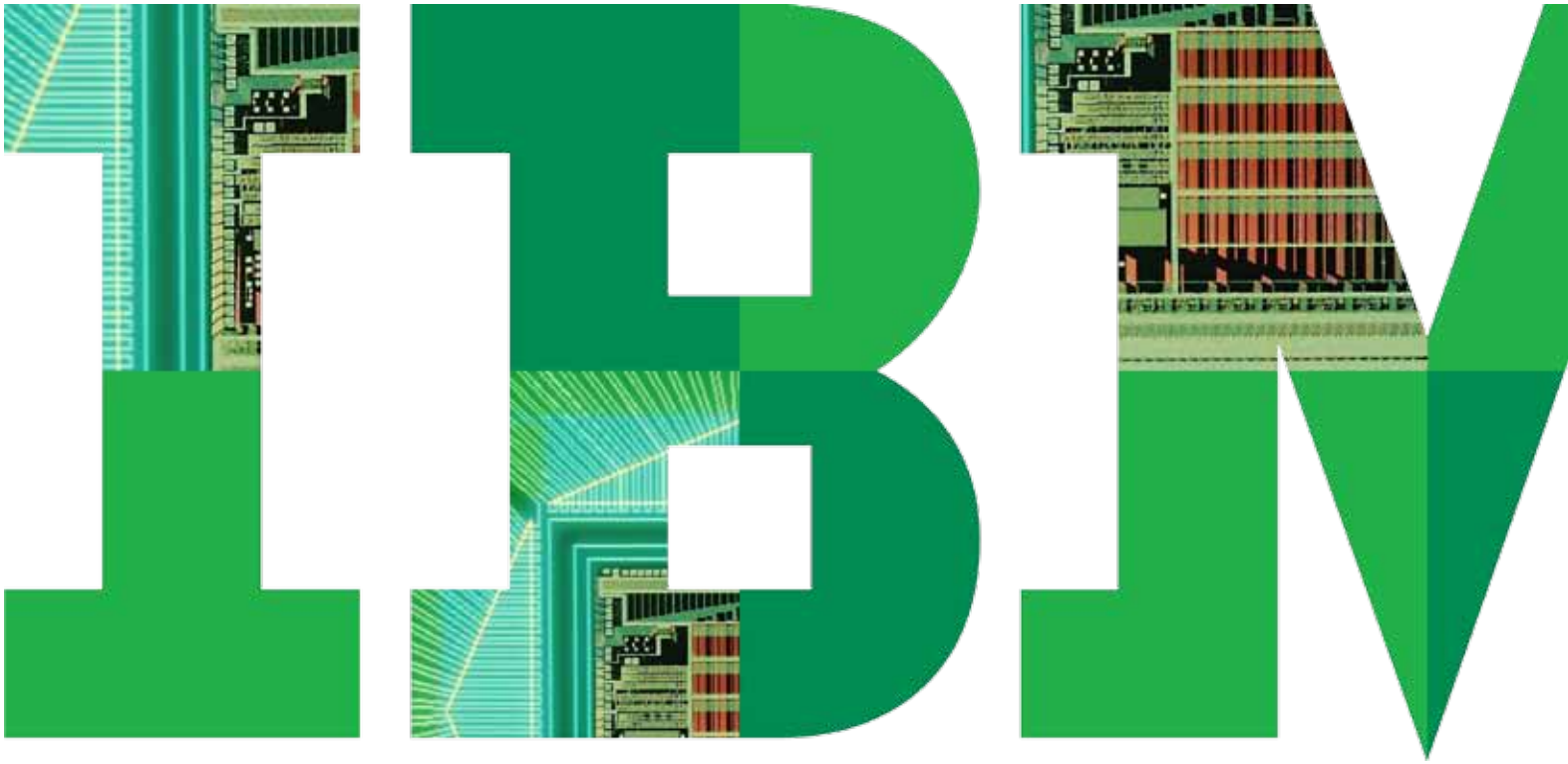
IBM Software

Gérer la conformité et protéger les données de l'entreprise

Respecter la conformité en contrôlant et en protégeant les données de l'entreprise



IBM

1

Le défi de la conformité

Les entreprises s'efforcent d'interpréter leurs obligations légales de conformité et de créer des règles de sécurité des données répondant à ces obligations et protégeant ces données.

2

Une réponse globale

Les études de marché montrent que les entreprises sont sous pression pour mettre en place des contrôles plus agressifs sur la sécurité des données.

3

Les clés de l'efficacité

Les entreprises ont besoin d'une approche complète pour protéger leurs données structurées, non structurées, « online » et « offline », issues de sources hétérogènes, et ce, qu'elles appartiennent à des environnements de production ou non.

4

Solutions

La gamme IBM® InfoSphere Guardium apporte des solutions performantes pour assurer la sécurité et la conformité des données. Grâce à ces solutions, les entreprises disposent des moyens de protéger leurs données, tout en restant focalisées sur leurs objectifs métier et en automatisant la conformité.

5

Ressources

Consultez nos études de cas et découvrez comment des entreprises ont bénéficié de la gamme de solutions InfoSphere Guardium pour respecter leurs obligations légales de conformité.

Le défi : comprendre les obligations légales relatives à la protection des données

Les hauts responsables informatiques, les directeurs chargés de la gouvernance de l'entreprise et les responsables métier sont tous focalisés sur la mise en œuvre d'une stratégie de sécurité des données, fondée sur les règles et les contrôles nécessaires pour protéger efficacement leurs données. Les obligations dans ce domaine ont différentes origines. Parmi quelques-unes d'entre elles, figurent : les obligations légales, les lois locales sur la protection des données, les exigences de gouvernance au sein des entreprises, mais aussi la nécessité de protéger avec rigueur les éléments de propriété intellectuelle, comme les codes source ainsi que des documents et feuilles de calcul.

La capacité à comprendre les obligations applicables est particulièrement importante, car la sécurité des données ne s'appuie pas sur un processus ou une technologie isolés. Elle se fonde plutôt sur une approche globale de la protection, adossée à un éventail de technologies et de contrôles conçus pour répondre à des situations spécifiques et à un environnement complexe concernant aussi bien les obligations légales que les menaces. Il n'existe pas de bonnes pratiques universelles.

Les entreprises doivent connaître leurs particularités pour mettre en place un processus décisionnel plus performant, investir de manière plus économique et être plus efficaces dans la mise en œuvre de leurs technologies. Cet aspect pose des difficultés du fait de la persistance des incertitudes économiques et des contraintes pesant sur les ressources. Les entreprises ont du mal à répondre à leurs obligations en manière de sécurité des données, à cause de l'intégration et de l'exploitation de ces données au sein d'une chaîne logistique dynamique de l'information. Ce qui implique des opérations de création, d'accès, d'utilisation et de retrait de ces données. Au fur et à mesure de l'évolution des données au travers de chaque phase, leur valeur et les risques associés évoluent, ce qui impose d'adapter leur protection et leur sécurité.

Les investissements dans des processus de contrôle de la sécurité des données doivent être évalués en les replaçant dans la perspective des objectifs métier, des obligations légales de conformité et des niveaux de risque. Ce qui veut dire connaître parfaitement la manière dont ces données sont exploitées, et les obligations légales de conformité essentielles pour ce système particulier, puisqu'elles peuvent être différentes selon la finalité du système, l'utilisateur concerné, les données, le lieu de stockage et leurs utilisations. Ces connaissances constituent un cadre de référence destiné à accompagner les investissements et la mise en œuvre des technologies et des processus de la manière la plus efficace possible.

La réponse globale aux obligations légales de conformité

Selon l'étude « Best Practices in Data Protection » (Meilleures pratiques pour la protection des données), menée par le Ponemon Institute auprès de 550 entreprises et organisations, la plupart des dirigeants d'entreprise disent considérer l'application substantielle des obligations de conformité résultant de la réglementation, des lois, des normes, des règles et procédures internes comme le principal moteur de leur stratégie en matière de sécurité des données. Ils sont seulement 28 % à dire que cette stratégie est motivée par leur sens des responsabilités en matière de protection des données et 26 % à se dire motivés par le souhait de protéger la réputation de l'entreprise et de renforcer la fidélité des clients.

Parmi d'autres enseignements intéressants, l'étude Ponemon « Best Practices in Data Protection » indique que les entreprises s'appuient sur des processus manuels de surveillance de la conformité et que les observations informelles sont des approches courantes. 62 % des répondants mettent en œuvre un processus de surveillance manuelle de la conformité. Par ailleurs, 59 % des répondants utilisent une méthode d'identification des risques basée sur des observations informelles effectuées par les superviseurs et les managers.

Certains défis critiques auxquels les entreprises ont à faire face concernent la conformité et sont décrits dans la suite de ce document.

Quels sont, selon vous, aujourd'hui, les freins les plus significatifs à la mise en œuvre d'activités de protection des données efficaces au sein de votre entreprise ?

Source : Étude du Ponemon Institute, « Best Practices in Data Protection »

Quelles sont les obligations de vérification les plus courantes concernant la protection et la confidentialité des données ?

Exigences d'audit	COBIT (SOX)	PCI-DSS	ISO 27002	Lois sur la protection et la confidentialité des données	NIST SP 800-53 (FISMA)
1. Accès à des données sensibles (réussite/échec dans la sélection)		X	X	X	X
2. Changements de schémas (DDL) (Create/Drop/Alter Tables, etc.)	X	X	X	X	X
3. Changements de données (DML) (Insert, Update, Delete)	X		X		
4. Exceptions de sécurité (échecs de connexion, erreurs SQL, etc.)	X	X	X	X	X
5. Comptes, rôles et autorisations (DCL) (Grant, Revoke)	X	X	X	X	X

DDL - Data Definition Language (pour les changements de schémas)
DML - Data Manipulation Language (changements de valeurs des données)
DCL - Data Control Language

Les clés de l'efficacité

Comment les entreprises peuvent-elles gérer la conformité pour répondre aux réglementations essentielles (SOX/COBIT, PCI DSS, lois sur la confidentialité des données, SCAP, FISMA et HIPAA/HITECH), mais aussi mieux connaître leur contexte propre de protection des données ? Il est possible d'utiliser les six étapes suivantes :

1. Connaître les données de l'entreprise,
2. Établir les politiques et les contrôles appropriés pour protéger les différents types de données (structurées, non structurées, online, offline) en se basant sur la connaissance de ces données par l'entreprise,
3. Évaluer les technologies de protection des données,
4. Penser au-delà des environnements de production,
5. Automatiser et centraliser la surveillance des sources de données,
6. Créer des journaux d'audit et des rapports détaillés.

« Les chargés d'audit examinent de plus près les modalités de contrôle des accès aux gigantesques magasins de données de ces systèmes, et les entreprises sont incitées à adopter des processus de contrôle des données plus agressifs et étendus. »

– Gartner : « Database Activity Monitoring Is Evolving Into Database Audit and Protection », Février 2012

Connaître les données de l'entreprise

À travers le monde, la majorité des données est stockée dans des bases ou des entrepôts de données du commerce tels qu'Oracle DB, Microsoft® SQL Server, IBM DB2, IBM Informix, Sybase, MySQL, IBM Netezza et Teradata. Cependant, la plupart des entreprises ne connaissent pas de manière complète la façon dont fonctionnent leurs magasins de données. Nombre d'entre elles accordent une confiance excessive aux informations données par des experts des systèmes et des applications. Pour protéger les données appartenant à l'entreprise, il est nécessaire de mieux comprendre les relations qui s'opèrent entre elles.

Toutes les données ne nécessitent pas le même type de protection, et en protéger certaines, apparemment peu exposées aux risques, pourra être considéré comme une perte de temps et d'énergie. Gardez également à l'esprit que les données de grande valeur comme les spécifications de conception ou les secrets d'entreprise ne nécessitent pas forcément une protection au sens des obligations légales, mais que, compte tenu de leur valeur, les entreprises souhaiteront les protéger au moyen de contrôles de sécurité stricts.

Pour veiller à l'intégrité de leurs données, les entreprises se doivent d'envisager un processus automatique d'identification des relations entre données et de définir des objets métier, pour éviter une analyse manuelle de plusieurs mois qui n'offrirait aucune garantie d'exhaustivité ou d'exactitude.

Pour résumer, les premières étapes d'une protection et d'une conformité globales de vos données consistent à :

- Localiser et inventorier les bases de données présentes dans l'entreprise ;
- Identifier les données à caractère sensible ;
- Connaître les relations entre les données ;
- Décrire et gérer les données en continu.

Établir des politiques et des contrôles adéquats

Grâce à ce processus d'inventaire complet, les entreprises vont mettre en évidence un mix de données (structurées, non structurées, online, offline).

Pour mettre en place le type de politique de sécurité approprié, les entreprises doivent se poser quelques questions simples concernant leurs exigences en matière de protection des données. Quelques exemples :

- Quelles données considérez-vous comme sensibles ?
- Lesquelles constituent un secret d'entreprise ?
- De quoi sont constituées les données personnelles ?
- Quelle est la définition des données à haut risque ?
- Quelles sont les données soumises à des obligations légales, et celles qui ne le sont pas ?

Le processus de découverte des données doit être suivi par une équipe d'experts transdisciplinaires issus des fonctions métier et informatique (responsables informatiques, responsables des directions fonctionnelles, directeurs chargés de la gestion du risque).

Ces points de vue différents se doivent de converger pour établir un vocabulaire commun et conduire à une connaissance approfondie des données sensibles de l'entreprise. Par ailleurs, il est nécessaire de mettre en place des politiques standardisées.

Évaluer les technologies de protection des données

Il s'agit de technologies destinées à maximiser le niveau de protection et de conformité des données :

- **Évaluation des vulnérabilités**
  Une fois les données sensibles identifiées, leur vulnérabilité doit être évaluée. Cette évaluation peut comporter différentes opérations, qu'il s'agisse de la vérification des accès privilégiés au niveau des administrateurs ou de l'absence de vulnérabilités connues dans les configurations des bases de données.

- **Édition des données sensibles**
  Elle permet de protéger des données non structurées. L'édition des données sert à supprimer des informations sensibles des documents et formulaires, selon les fonctions professionnelles ou les objectifs métier de l'intervenant. À titre d'exemple, les médecins ont besoin d'accéder à des données sensibles, telles que les symptômes ou les pronostics, alors qu'un employé chargé de la facturation y cherchera le numéro de mutuelle du patient et son adresse de facturation.
- **Masquage de données statiques**
  L'anonymisation des données dans des environnements hors production revient simplement à procéder systématiquement à une suppression, à un masquage ou à une transformation d'éléments qui pourraient servir à une identification. Ce procédé permet aux développeurs, aux testeurs et aux formateurs d'utiliser des données réelles et de produire des résultats pertinents tout en protégeant les données sensibles.
  Ce point intéressera tout particulièrement les entreprises qui sous-traitent les activités de développement ou de test.
- **Masquage de données dynamiques**
  Cette action empêche les utilisateurs indésirables d'accéder, en temps réel, à des données structurées. Les entreprises peuvent programmer des règles sophistiquées et flexibles de masquage en se basant sur des règles et des exigences métier. Les politiques de masquage des données dynamiques permettent de cacher des informations sensibles à la volée, dès leur extraction de la base de données. Les résultats masqués sont ensuite renvoyés à l'application web ayant émis la requête. Les entreprises faisant appel à des centres d'appels utilisent le masquage de données dynamiques pour dissimuler les informations clients aux employés.
- **Vérification et surveillance de bases de données**
  Ces opérations servent à surveiller de manière proactive les activités des bases de données et à analyser les accès. Ces solutions permettent l'identification et l'émission d'alertes en temps réel en cas de comportements inappropriés, indésirables ou illégaux dans des bases de données, et génèrent des rapports d'activité comme la plupart des réglementations citées l'exigent.
- **Cryptage des données**
  Il existe différents types de cryptage. Les entreprises se doivent d'envisager un cryptage des fichiers, car il s'agit d'une solution unifiée, conviviale et évolutive pour crypter les données, structurées ou non, et ce, sans sacrifier les performances des applications ou créer de la complexité pour la gestion des clés. Le cryptage constitue une solution idéale pour protéger les données « online » et « offline ».

Penser au-delà des environnements de production

Si la priorité, en termes de temps et d'objectifs, est donnée aux systèmes de production critiques, les entreprises devraient garder à l'esprit que les données sensibles sont stockées dans de nombreux autres endroits. À combien de reprises votre base de données de production a-t-elle été clonée ? Existe-t-il des copies pour effectuer des tests, ou pour le développement, l'assurance qualité ou les reprises après incident ? Ces environnements situés hors production sont-ils traités de la même manière que les systèmes de production ? S'ils contiennent des données identiques, ils doivent être considérés comme faisant partie intégrante d'une approche globale de la sécurité des données.

Les développeurs, les testeurs et les professionnels de l'assurance qualité apprécient de travailler avec des données actives, car elles produisent des résultats que toutes les personnes concernées peuvent comprendre. Cependant, les environnements ne relevant pas de la production ne nécessitent pas forcément de données actives. Si l'utilisation de données réalistes est essentielle pour les tests, les données actives ne sont pas obligatoirement nécessaires. Les fonctionnalités d'anonymisation ou de masquage de données de production constituent une bonne pratique pour protéger les données sensibles, tout en menant à bien les processus de test. Le masquage permet aux développeurs, aux testeurs et aux professionnels de l'assurance qualité d'utiliser des données proches de celles nécessaires à la production et d'obtenir des résultats de test valides, et ce, tout en restant conforme aux politiques de sécurité.

Automatiser et centraliser la surveillance des sources de données

Malheureusement, il ne suffit pas de connaître les données sensibles et d'établir les types appropriés de politiques, pour assurer la protection des données. Il est nécessaire de surveiller en permanence les sources de données pour détecter d'éventuels comportements suspects. Il est préférable que les entreprises ne se fient pas à des procédures manuelles d'audit pour détecter ces comportements. En effet, cette approche prolonge la durée des audits et consomme des ressources.

Dans la plupart des environnements informatiques, les utilisateurs privilégiés que sont les administrateurs de bases de données, les développeurs et les personnels externalisés bénéficient d'un accès totalement libre aux données sensibles, avec peu ou pas de contrôle sur leurs activités. Ces super-utilisateurs peuvent facilement contourner les points de contrôle assurant la sécurité des applications ou des réseaux.

En outre, la détection des changements dans les bases de données est essentielle du point de vue de la mise en place de contrôles concernant les utilisateurs privilégiés. Cependant, la détection de ces changements est également essentielle du point de vue de la sécurité. De tels changements peuvent constituer des indicateurs d'une altération de la base de données.

Les types de changements concernés sont les suivants :

- Structures de bases de données, notamment les tables, les déclencheurs et les procédures stockées ;
- Valeurs de données critiques, notamment les données relatives à l'intégrité des transactions financières ;
- Objets de contrôle de la sécurité et des accès, notamment les utilisateurs, les rôles et les autorisations ;
- Fichiers de configuration de bases de données et autres objets externes pouvant influer sur votre sécurité, notamment les variables d'environnement/de registre, les fichiers de configuration (par exemple, NAMES.ORA), les scripts de shell, les fichiers de systèmes d'exploitation et les fichiers exécutables tels que les programmes Java™.

Créer des journaux d'audit et des rapports détaillés

Pour démontrer et valider la conformité des données, les entreprises doivent disposer d'un processus défini pour surveiller, enregistrer et décrire, de manière périodique, les accès aux bases de données et les changements opérés. Un journal d'audit détaillé permet d'identifier les informations fondamentales de chaque transaction (identité, nature de la transaction, horodatage, localisation, modalités). Grâce à un processus continu de surveillance et de reporting, la détection des violations concernant les accès aux données apporte aux responsables informatiques et aux chargés d'audit les informations nécessaires pour démontrer que les contrôles mis en place sont adaptés et fonctionnent. Les journaux d'audit contiennent les détails et les analyses des comportements et des modèles considérés comme suspects, par rapport à des transactions légitimes ou courantes. Tout comportement ne relevant pas des activités courantes et d'un accès valide à une base de données doit être examiné et analysé de manière détaillée.

L'élaboration d'un environnement centralisé d'audit et de reporting apporte les avantages suivants :

- Un référentiel centralisé et sécurisé contenant un journal d'audit détaillé de l'ensemble des activités de la base de données à l'échelle de l'entreprise, ainsi que les activités de partage de fichiers importants ;
- Un processus d'automatisation personnalisable du workflow, permettant de générer de manière périodique des rapports de conformité, de les diffuser vers des équipes de surveillance pour validation et remontée hiérarchique, et stocker les résultats des activités de résolution dans le référentiel ;
- Une surveillance et une analyse permanentes des données pour identifier les activités interdites ou suspectes, et déclencher une réaction, qui peut aller du blocage en temps réel de la transaction jusqu'à la génération d'une alerte.

Solutions IBM InfoSphere Guardium

Une entreprise doit déterminer les obligations légales de conformité les plus pertinentes en fonction de son activité et de son propre contexte. Il est impossible d'assurer la protection contre toutes les menaces et la conformité à toutes les obligations. Une entreprise doit procéder à une analyse des risques et prendre des décisions en toute connaissance de cause concernant un risque résiduel acceptable en termes de conformité. Pour cela, il est nécessaire d'établir un processus formel permettant d'analyser les scénarios de sécurité, les situations d'utilisation, les dommages possibles et l'impact métier des questions de sécurité Il est nécessaire de garder à l'esprit que la plupart des lois sont délibérément vagues pour pouvoir être appliquées, le cas échéant, par les entreprises, quelles que soit leur taille. Ces lois sont également conçues pour être technologiquement neutres, ce qui laisse aux entreprises le contrôle dont elles ont besoin.

La gamme IBM InfoSphere Guardium apporte des solutions performantes pour assurer la sécurité et la conformité des données. Grâce à ces solutions, les entreprises disposent des moyens de se protéger dans un environnement complexe porteur de menaces, notamment concernant les activités frauduleuses ou négligentes du personnel, les changements non autorisés et les attaques venues de l'extérieur, et ce, tout en restant focalisées sur leurs objectifs métier et en automatisant la conformité.

Les solutions IBM InfoSphere Guardium apportent une réponse globale de protection des données pour sécuriser des types de données variés (structurées, non structurées, online, offline) localisées à différents emplacements, notamment les environnements de production et hors production (développement, test, formation). Ces solutions permettent de rationaliser le processus de conformité en mettant en œuvre des contrôles unifiés et une application cohérente des politiques de gouvernance à l'échelle de l'entreprise.

Les solutions IBM InfoSphere Guardium apportent des réponses aux problématiques suivantes :

- **Découverte et classification des données,**
- **Évaluation des vulnérabilités,**
- **Édition des données sensibles,**
- **Cryptage des données,**
- **Masquage des données statiques,**
- **Surveillance des bases de données,**
- **Audit et reporting.**

Pour en savoir plus, visitez le site : **ibm.com**/guardium ou **ibm.com**/security/fr

Ressources

Étude de cas : Mise en œuvre d'un processus de surveillance des activités d'une base de données pour un acteur international majeur des télécommunications.
Un leader international des télécommunications recherchait une solution économique pour protéger la confidentialité de ses données client et respecter ses obligations légales de conformité.

Étude de cas : Mise en œuvre d'un processus de surveillance et d'audit des activités d'une base de données au sein d'une mutuelle de santé parmi les plus performantes.
Identifier une solution économique permettant de mettre en œuvre des contrôles pour la protection des données sensibles et la validation d'un processus de conformité à une multiplicité d'obligations légales.

Étude de cas : Aviva UK Health renforce sa conformité à la norme PCI et à la réglementation en matière de confidentialité des données.
Aviva UK Health rencontrait des difficultés pour répondre à des exigences de conformité PCI-DSS et DPA incompatibles, ce qui menaçait sa capacité à maintenir la possibilité de paiement par carte de crédit pour ses clients.

Pour en savoir plus sur la gestion de la sécurité de vos bases de données au sein de votre entreprise, visitez le site : **ibm.com**/guardium ou **ibm.com**/security/fr

IBM France
17 Avenue de l'Europe
92275 Bois Colombes Cedex

NIB03012-FRFR-00