RESOURCE CENTER

Comment la gestion des mots de passe aide les entreprises à obtenir la certification ISO 27001

Get the full interactive view at https://bitwarden.com/fr-fr/resources/how-password-management-helps-companies-achieve-iso-27001-certification/

bitwarden

Qu'est-ce que la norme ISO 27001 ?

Mise à jour : Depuis mars 27001, Bitwarden est certifié ISO 27001 en conformité avec les ensembles de contrôles ISO 27001 relatifs à la sécurité des données.

La norme internationale ISO 27001 jette les bases de la création, du maintien et du développement de systèmes de gestion de la sécurité de l'information (SGSI), y compris la gestion des données. Les entreprises qui souhaitent obtenir la conformité ou la certification ISO 27001 devraient envisager d'ajouter la gestion des mots de passe ISO 27001 à leur panoplie d'outils.

Le groupe mondial de l'Organisation internationale de normalisation (ISO) élabore et publie des normes techniques, industrielles et commerciales à l'échelle mondiale. Mise à jour en octobre 2022, la norme ISO 27001 pour les SMSI fournit un cadre pour la sécurité des données, composé de 93 ensembles de contrôle. Pour obtenir la certification ISO 27001, les entreprises doivent démontrer qu'elles respectent tous ces critères.

> Pour obtenir la certification ISO 27001, vous devez vous conformer à 93 ensembles de contrôle.

Le processus de certification ISO 27001 consiste en un audit mené par des organismes de certification indépendants qui examinent les politiques et procédures de sécurité des données de l'entreprise, ainsi que la manière dont elles sont appliquées. Le processus peut être long, mais la réussite d'un audit de certification ISO 27001 montre que votre entreprise a procédé à une évaluation des risques de sécurité afin d'identifier les menaces potentielles et qu'elle a mis en place des contrôles de sécurité pour se protéger contre les violations de données.

Table des matières

Les avantages de la certification et de la conformité à la norme ISO 27001

La certification ISO 27001 donne aux organisations un avantage concurrentiel pour attirer et retenir les clients, car elle démontre l'existence de contrôles solides de la sécurité de l'information. La certification peut également attirer et retenir des fournisseurs et d'autres parties prenantes soucieuses de la manière dont leurs informations sont gérées et protégées.

Le simple fait de se préparer au processus d'audit permet de renforcer les politiques ISO 27001 existantes et d'améliorer les systèmes internes, les structures et les processus opérationnels quotidiens. Le processus de gestion des risques peut également aider les organisations à mieux se conformer aux lois sur la protection des données telles que la CCPA et le GDPR, et à éviter les amendes pour non-conformité ou la perte de réputation due à une violation de données qui aurait pu être évitée.

Découvrez comment votre entreprise peut renforcer ses pratiques de cybersécurité pour réussir les audits de sécurité.

L'ensemble des contrôles ISO 27001

Les 93 ensembles de contrôle figurent à l'annexe A et se répartissent en quatre grands thèmes. Pour obtenir la certification ISO 27001, les entreprises doivent démontrer qu'elles respectent ces contrôles. Les catégories sont les suivantes

- Contrôles organisationnels (37 contrôles)
- Contrôles de personnes (8 contrôles)
- Contrôles physiques (14 contrôles)
- Contrôles technologiques (34 contrôles)

La version précédente de l'ISO comprenait 114 contrôles répartis en 14 catégories. Cette version comprenait également des dispositions relatives à la sécurité des systèmes de connexion et de gestion des mots de passe.

Le contrôle de l'ouverture de session sécurisée précise que "l'accès aux systèmes et aux applications doit être contrôlé par une procédure d'ouverture de session sécurisée lorsque la politique de contrôle d'accès l'exige". Avec un gestionnaire de mots de passe, les utilisateurs ont l'avantage d'ajouter une couche de sécurité supplémentaire à leurs identifiants et de disposer d'un endroit unique pour gérer et intégrer l'authentification à deux facteurs pour tous les sites web qui la prennent en charge.

Le contrôle du système de gestion des mots de passe stipule que "les systèmes de gestion des mots de passe doivent être coopératifs pour garantir la qualité des mots de passe". L'ISO recommande d'utiliser un gestionnaire de mots de passe qui permet aux utilisateurs de créer des mots de passe forts et uniques et qui offre des capacités de partage sécurisées pour la collaboration.

> **Les gestionnaires de mots de passe renforcent les mots de passe, appliquent le 2FA et utilisent les journaux d'événements pour surveiller l'activité des utilisateurs - autant de fonctionnalités que les entreprises doivent mettre en œuvre pour répondre aux exigences de l'ISO en matière de contrôle d'accès, de protection des informations confidentielles et de protection des terminaux.**

La dernière version de la norme ISO 27001 traite de la gestion des mots de passe à l'annexe A 5.17. De nombreuses autres exigences de l'annexe A peuvent être satisfaites ou soutenues par l'adoption d'un gestionnaire de mots de passe. Les exemples suivants ne sont pas exhaustifs :

- **Annexe A 5.3, Séparation des tâches**: Les conflits de tâches et de domaines de responsabilité doivent être séparés.
- **Annexe A 5.14, Transfert d'informations**: Des règles, procédures ou accords de transfert d'informations doivent être mis en place pour tous les types d'installations de transfert au sein de l'organisme et entre l'organisme et d'autres parties.

- **Annexe A 5.15, Contrôle d'accès**: Des règles de contrôle de l'accès physique et logique aux informations et autres biens associés sont établies et mises en œuvre sur la base des exigences de l'entreprise et de la sécurité de l'information.
- **Annexe A 5.16, Gestion des identités**: Le cycle de vie complet des identités doit être géré.
- **Annexe A 5.17, Informations d'authentification**: L'attribution et la gestion des informations d'authentification doivent être contrôlées par un processus de gestion, notamment en conseillant le personnel sur les meilleures pratiques en matière de traitement des informations d'authentification.
  - Un document d'information détaillé sur ce critère présente les recommandations en matière de mots de passe, ainsi que des conseils sur la gestion des mots de passe, y compris la possibilité de créer des mots de passe sécurisés. En outre, l'objectif recommande aux organisations d'éviter les informations d'identification faibles, largement utilisées ou compromises.

> Compte tenu de ces critères, les organisations devraient idéalement déployer un système de gestion des mots de passe qui leur permette de rendre compte et d'avoir des informations exploitables sur les mots de passe exposés, réutilisés, faibles ou potentiellement compromis.

- **Annexe A 5.34, Vie privée et protection des informations personnelles identifiables (IPI)**: L'organisme doit identifier et satisfaire les exigences relatives à la préservation de la vie privée et à la protection des IPI conformément aux lois et réglementations applicables et aux exigences contractuelles.
- **Annexe A 8.1, Dispositifs d'extrémité de l'utilisateur**: Les informations stockées, traitées ou accessibles via des dispositifs d'extrémité de l'utilisateur doivent être protégées.
- **Annexe A 8.4, Accès au code source**: L'accès en lecture et en écriture au code source, aux outils de développement et aux bibliothèques de logiciels doit être géré de manière appropriée.
- **Annexe A 8.5, Authentification sécurisée**: Les technologies et procédures d'authentification sécurisée sont mises en œuvre sur la base des restrictions d'accès à l'information et de la politique de contrôle d'accès propre à chaque thème.
  - Cet objectif porte sur l'utilisation de l'authentification multifactorielle pour se connecter en toute sécurité aux systèmes. Avec un gestionnaire de mots de passe, les utilisateurs ont l'avantage d'ajouter une couche de sécurité supplémentaire à leurs identifiants et de disposer d'un endroit unique pour gérer et intégrer l'authentification à deux facteurs (2FA) pour tous les sites web qui la prennent en charge. L'objectif souligne également que les mots de passe doivent rester confidentiels à tout moment, ce qui plaide en faveur d'un coffre-fort à mot de passe entièrement crypté.

> Les systèmes de gestion des mots de passe permettent aux organisations d'identifier tous les éléments dans leurs coffres-forts avec un 2FA inactif.

- **Annexe A 8.11, Masquage des données**: Le masquage des données est utilisé conformément à la politique thématique de l'organisation en matière de contrôle d'accès et à d'autres politiques thématiques connexes, ainsi qu'aux exigences de l'entreprise, en tenant compte de la législation applicable.
- **Annexe A 8.12, Fuite de données**: Des mesures de prévention des fuites de données sont appliquées aux systèmes, réseaux et autres dispositifs qui traitent, stockent ou transmettent des informations sensibles.

Le saviez-vous ?

Bitwarden propose des rapports sur l'état de santé du coffre-fort qui peuvent contribuer à encourager des pratiques de cybersécurité solides et permettre aux employés d'identifier les comptes dont la protection est insuffisante.

ISO recommends using a that enables users to create strong and unique passwords and offers secure sharing capabilities for collaboration.

Obtenir la certification ISO 27001 à l'aide d'un gestionnaire de mots de passe

Un système de gestion des mots de passe répond aux nombreuses exigences de l'annexe A énumérées ci-dessus, ainsi qu'à un grand nombre d'exigences incluses dans les ensembles de contrôle généraux.

Les utilisateurs peuvent garder secrètes les informations d'authentification, appliquer les meilleures pratiques en matière de mots de passe, telles que la création de mots de passe forts et uniques, et partager les mots de passe en toute sécurité avec un gestionnaire de mots de passe qui sécurise les informations sensibles par un cryptage de bout en bout. En limitant l'accès à certaines informations sensibles ou critiques, les gestionnaires de mots de passe permettent également de séparer les tâches et de limiter les menaces internes.

Les organisations qui utilisent des gestionnaires de mots de passe établissent des exigences en matière de force des mots de passe, appliquent l'authentification à deux facteurs (2FA) et utilisent des journaux d'événements pour surveiller l'activité des utilisateurs - toutes les capacités que les entreprises doivent atteindre pour répondre aux exigences de l'ISO en matière de contrôle d'accès, de protection des IIP et de protection des points d'extrémité. La plupart des gestionnaires de mots de passe réputés facilitent également l'intégration SSO, fournissant aux administrateurs les outils dont ils ont besoin pour gérer l'accès et le processus d'authentification. Cette capacité permet de répondre aux exigences de l'ISO en matière d'authentification sécurisée.

Lors de l'évaluation des gestionnaires de mots de passe pour la prise en charge de la certification ISO 27001, les organisations doivent déterminer si le logiciel respecte les normes de sécurité et de conformité de niveau entreprise, telles que la conformité SOC2 de type 2, la conformité GDPR, le cadre de confidentialité des données et l'HIPAA. Les entreprises devraient choisir une solution qui offre un cryptage de bout en bout sans connaissance.

Commencer avec Bitwarden

Vous souhaitez utiliser le gestionnaire de mots de passe Bitwarden conforme à la norme ISO 27001 pour vous aider à respecter les normes ISO 27001 relatives aux systèmes de gestion de la sécurité de l'information ? Commencez un essai gratuit avec Bitwarden dès aujourd'hui !

Études de cas :

Inventory Hive, l'un des principaux logiciels d'inspection immobilière et de visites virtuelles au Royaume-Uni, a obtenu la certification ISO 27001 avec Bitwarden.

Bitwarden Secrets Manager et Bitwarden Password Manager permettent à Titanom Technologies de démontrer sa résilience en matière de cybersécurité et d'obtenir la certification ISO 27001.

"I want to set guidelines on the password generator about how strong the password must be. That's very important right now for us to achieve the ISO 27001 certification."

Jannis Morgenstern, head of IT at Titanom Technologies