RESOURCE CENTER

Wie Passwortmanagement Unternehmen hilft, die ISO 27001-Zertifizierung zu erreichen

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

bitwarden

Was ist ISO 27001?

Update: Seit März 27001 ist Bitwarden ISO 27001-zertifiziert in Übereinstimmung mit ISO 27001-Kontrollsätzen rund um die Datensicherheit.

ISO 27001, eine internationale Norm, legt die Grundlage für die Erstellung, Wartung und Entwicklung von Informationssicherheitsmanagementsystemen (ISMS), einschließlich Datenmanagement. Unternehmen, die die ISO 27001-Konformität oder Zertifizierung erreichen möchten, sollten erwägen, ihr Toolset um die ISO 27001-Passwortverwaltung zu erweitern.

Die globale Gruppe der Internationalen Organisation für Normung (ISO) entwickelt und veröffentlicht weltweite technische, industrielle und kommerzielle Standards. Die zuletzt im Oktober 2022 aktualisierte Norm ISO 27001 für ISMS bietet einen Rahmen für die Datensicherheit, der aus 93 Kontrollsätzen besteht. Um die ISO 27001-Zertifizierung zu erhalten, müssen Unternehmen die Einhaltung aller Normen nachweisen.

> Um sich als ISO 27001-Unternehmen zu zertifizieren, müssen Sie 93 Kontrollsätze einhalten.

Der ISO 27001-Zertifizierungsprozess besteht aus einem Audit, das von unabhängigen Zertifizierungsstellen durchgeführt wird, die die Datensicherheitsrichtlinien und -verfahren des Unternehmens und deren Anwendung überprüfen. Der Prozess kann langwierig sein, aber das Bestehen eines ISO 27001-Zertifizierungsaudits zeigt, dass Ihr Unternehmen eine Sicherheitsrisikobewertung durchgeführt hat, um potenzielle Bedrohungen zu identifizieren, und Sicherheitskontrollen zum Schutz vor Datenschutzverletzungen eingeführt hat.

Inhaltsverzeichnis

Die Vorteile der ISO 27001-Zertifizierung und -Compliance

Die ISO 27001-Zertifizierung verschafft Unternehmen einen Wettbewerbsvorteil bei der Gewinnung und Bindung von Kunden, da die Zertifizierung robuste Kontrollen der Informationssicherheit demonstriert. Die Zertifizierung kann auch Lieferanten und andere Stakeholder anziehen und binden, die darüber besorgt sind, wie ihre Informationen verwaltet und geschützt werden.

Selbst die Vorbereitung auf den Auditprozess kann bestehende ISO 27001-Richtlinien stärken und interne Systeme, Strukturen und tägliche Geschäftsprozesse verbessern. Der Risikomanagementprozess kann Unternehmen auch dabei helfen, Datenschutzgesetze wie CCPA und DSGVO besser einzuhalten und Bußgelder für Nichteinhaltung oder Reputationsverlust aufgrund einer vermeidbaren Datenschutzverletzung zu vermeiden.

Erfahren Sie mehr darüber, wie Ihr Unternehmen seine Cybersicherheitspraktiken stärken kann, um Sicherheitsaudits zu bestehen.

Die ISO 27001 Steuersätze

Die 93 Steuersätze sind in Anhang A enthalten und fallen unter 4 größere Themen. Um die ISO 27001-Zertifizierung zu erhalten, müssen Unternehmen die Einhaltung dieser Kontrollen nachweisen. Die Kategorien sind:

- Organisatorische Kontrollen (37 Kontrollen)
- Personenkontrollen (8 Kontrollen)
- Physische Kontrollen (14 Kontrollen)
- Technologische Kontrollen (34 Kontrollen)

Die vorherige Version der ISO enthielt 114 Steuerelemente, die in 14 Kategorien unterteilt waren. Diese Version enthielt auch eine Sprache für sichere Anmelde- und Passwortverwaltungssysteme.

Die sichere Anmeldesteuerung spezifiziert "Der Zugriff auf Systeme und Anwendungen sollte durch ein sicheres Anmeldeverfahren kontrolliert werden, wenn dies von der Zugriffskontrollrichtlinie gefordert wird." Mit einem Passwort-Manager profitieren Benutzer davon, Logins eine weitere Sicherheitsebene hinzuzufügen und einen Ort zu haben, an dem sie die Zwei-Faktor-Authentifizierung für alle Websites, die sie unterstützen, verwalten und integrieren können.

In der Passwortverwaltungssystemsteuerung heißt es: "Passwortverwaltungssysteme müssen kooperativ sein, um die Qualität von Passwörtern zu gewährleisten." ISO empfiehlt die Verwendung eines Passwort-Managers, der es Benutzern ermöglicht, starke und eindeutige Passwörter zu erstellen und sichere Freigabefunktionen für die Zusammenarbeit bietet.

> **Passwort-Manager legen die Passwortstärke fest, erzwingen 2FA und verwenden Ereignisprotokolle, um die Benutzeraktivität zu überwachen - alle Funktionen, die Unternehmen erreichen müssen, um die Anforderungen der ISO-Zugriffskontrolle, des Schutzes personenbezogener Daten und des Endpoint-Schutzes zu erfüllen.**

Die neueste Version der ISO 27001 befasst sich mit der Passwortverwaltung in Anhang A 5.17. Es gibt viele zusätzliche Anhang-A-Anforderungen, die durch die Einführung eines Passwort-Managers erfüllt oder unterstützt werden können. Obwohl nicht erschöpfend, sind Beispiele:

- **Anlage A 5.3, Aufgabentrennung**: Widersprüchliche Aufgaben und widersprüchliche Verantwortungsbereiche sind zu trennen.
- **Anhang A 5.14, Informationsübertragung**: Regeln, Verfahren oder Vereinbarungen zur Informationsübertragung müssen für alle Arten von Übertragungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien vorhanden sein.

- **Anhang A 5.15, Zugriffskontrolle**: Regeln zur Kontrolle des physischen und logischen Zugriffs auf Informationen und andere damit verbundene Vermögenswerte müssen auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen festgelegt und implementiert werden.
- **Anhang A 5.16, Identitätsmanagement**: Der gesamte Lebenszyklus von Identitäten muss verwaltet werden.
- **Anhang A 5.17, Authentifizierungsinformationen**: Die Zuweisung und Verwaltung von Authentifizierungsinformationen muss durch einen Verwaltungsprozess kontrolliert werden, einschließlich der Beratung des Personals beim Umgang mit Best Practices für Authentifizierungsinformationen.
  - Eine detaillierte Einführung zu diesen Kriterien enthält Passwortempfehlungen mit Ratschlägen zur Verwaltung von Passwörtern, einschließlich der Möglichkeit, sichere Passwörter zu erstellen. Darüber hinaus empfiehlt das Ziel Unternehmen, schwache, weit verbreitete oder kompromittierte Anmeldeinformationen zu vermeiden.

> Angesichts dieser Kriterien würden Unternehmen idealerweise ein Passwortverwaltungssystem einsetzen, das es ihnen ermöglicht, über exponierte, wiederverwendete, schwache oder potenziell gefährdete Passwörter zu berichten und verwertbare Erkenntnisse darüber zu erhalten.

- **Anhang A 5.34, Datenschutz und Schutz personenbezogener Daten (PII)**: Die Organisation muss die Anforderungen an die Wahrung der Privatsphäre und den Schutz personenbezogener Daten gemäß den geltenden Gesetzen und Vorschriften sowie den vertraglichen Anforderungen identifizieren und erfüllen.
- **Anhang A 8.1, Endgeräte des Benutzers**: Informationen, die auf Endgeräten des Benutzers gespeichert, von diesen verarbeitet oder über diese zugänglich sind, sind zu schützen.
- **Anhang A 8.4, Zugriff auf Quellcode**: Der Lese- und Schreibzugriff auf Quellcode, Entwicklungstools und Softwarebibliotheken ist angemessen zu verwalten.
- **Anhang A 8.5, Sichere Authentifizierung**: Sichere Authentifizierungstechnologien und -verfahren müssen auf der Grundlage von Informationszugriffsbeschränkungen und der themenspezifischen Richtlinie zur Zugriffskontrolle implementiert werden.
  - Dieses Ziel konzentriert sich auf die Verwendung der Multi-Faktor-Authentifizierung für die sichere Anmeldung bei Systemen. Mit einem Passwort-Manager profitieren Benutzer davon, Logins eine weitere Sicherheitsebene hinzuzufügen und einen Ort zu haben, an dem sie die Zwei-Faktor-Authentifizierung (2FA) für alle Websites, die sie unterstützen, verwalten und integrieren können. Das Ziel hebt auch hervor, dass Passwörter jederzeit vertraulich behandelt werden sollten, was ein starkes Argument für einen vollständig verschlüsselten Passworttresor ist.

> Passwortverwaltungssysteme ermöglichen es Unternehmen, alle Elemente in ihren Tresoren mit inaktiven 2FA zu identifizieren.

- **Anhang A 8.11, Datenmaskierung**: Die Datenmaskierung muss in Übereinstimmung mit der themenspezifischen Richtlinie der Organisation zur Zugriffskontrolle und anderen damit verbundenen themenspezifischen Richtlinien und Geschäftsanforderungen unter Berücksichtigung der geltenden Gesetzgebung verwendet werden.
- **Anhang A 8.12, Datenleck**: Maßnahmen zur Verhinderung von Datenlecks sind auf Systeme, Netzwerke und alle anderen Geräte anzuwenden, die sensible Informationen verarbeiten, speichern oder übertragen.

Wussten Sie schon?

Bitwarden bietet Vault Health Reports an, die dazu beitragen können, starke Cybersicherheitspraktiken zu fördern und es Mitarbeitern zu ermöglichen, Konten mit schwachem Schutz zu identifizieren.

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

Erreichen Sie die ISO 27001-Zertifizierung mit Hilfe eines Passwort-Managers

Ein Passwortverwaltungssystem unterstützt die zahlreichen Anforderungen des Anhangs A, die oben aufgeführt sind, und viele der Anforderungen, die in den gesamten Kontrollsätzen enthalten sind.

Benutzer können Authentifizierungsinformationen geheim halten, Best Practices für Passwörter anwenden, z. B. das Generieren starker, eindeutiger Passwörter, und Passwörter sicher mit einem Passwort-Manager teilen, der vertrauliche Informationen mit Ende-zu-Ende-Verschlüsselung schützt. Durch die Einschränkung, wer bestimmte sensible oder kritische Informationen sehen kann, tragen Passwort-Manager auch dazu bei, Aufgaben zu trennen und Insider-Bedrohungen zu begrenzen.

Organisationen, die Passwort-Manager verwenden, legen Anforderungen an die Passwortstärke fest, erzwingen die Zwei-Faktor-Authentifizierung (2FA) und verwenden Ereignisprotokolle, um die Benutzeraktivität zu überwachen — alle Funktionen, die Unternehmen erreichen müssen, um die Anforderungen an die ISO-Zugriffskontrolle, den Schutz personenbezogener Daten und den Endpunktschutz zu erfüllen. Die meisten seriösen Passwort-Manager erleichtern auch die SSO-Integration und statten Administratoren mit den Tools aus, die sie benötigen, um den Zugriff und den Authentifizierungsprozess zu verwalten. Diese Funktion trägt dazu bei, die Anforderung der sicheren ISO-Authentifizierung zu erfüllen.

Bei der Bewertung von Passwort-Managern zur Unterstützung der ISO 27001-Zertifizierung sollten Unternehmen prüfen, ob die Software den Sicherheits- und Compliance-Standards der Enterprise-Klasse entspricht, z. B. SOC2-Typ-2-Compliance, DSGVO-Compliance, Data Privacy Framework und HIPAA. Unternehmen sollten eine Lösung wählen, die eine Ende-zu-Ende-Zero-Knowledge-Verschlüsselung bietet.

Erste Schritte mit Bitwarden

Möchten Sie den Bitwarden ISO 27001-konformen Passwort-Manager nutzen, um die ISO 27001-Standards für Informationssicherheitsmanagementsysteme zu erfüllen? Starten Sie noch heute eine kostenlose Testversion für Unternehmen mit Bitwarden!

Fallstudien:

Inventory Hive, eine führende Softwareplattform für Immobilieninspektionen und virtuelle Touren in Großbritannien, hat die

ISO 27001-Zertifizierung mit Bitwarden erhalten.

Sowohl Bitwarden Secrets Manager als auch Bitwarden Password Manager ermöglichen es Titanom Technologies, die Widerstandsfähigkeit der Cybersicherheit zu demonstrieren und für die ISO 27001-Zertifizierung in Betracht zu ziehen.

"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