RESOURCE CENTER

Hoe wachtwoordbeheer bedrijven helpt ISO 27001-certificering te behalen

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

bitwarden

Wat is ISO 27001?

Update: Vanaf maart 27001 is Bitwarden ISO 27001-gecertificeerd in overeenstemming met de ISO 27001-controlesets rondom gegevensbeveiliging.

ISO 27001, een internationale norm, legt de basis voor het creëren, onderhouden en ontwikkelen van beheersystemen voor informatiebeveiliging (ISMS), inclusief gegevensbeheer. Bedrijven die ISO 27001-naleving of -certificering nastreven, moeten overwegen ISO 27001-wachtwoordbeheer toe te voegen aan hun toolset.

De internationale ISO-groep (International Organization for Standardization) ontwikkelt en publiceert wereldwijd technische, industriële en commerciële normen. De ISO 27001-norm voor ISMS, die voor het laatst is bijgewerkt in oktober 2022, biedt een kader voor gegevensbeveiliging dat bestaat uit 93 controlesets. Om ISO 27001 gecertificeerd te worden, moeten bedrijven aantonen dat ze aan al deze criteria voldoen.

> Om gecertificeerd te worden als ISO 27001-bedrijf, moet u voldoen aan 93 controlesets.

Het ISO 27001-certificeringsproces bestaat uit een audit die wordt uitgevoerd door onafhankelijke certificeringsinstanties die het beleid en de procedures voor gegevensbeveiliging van bedrijven beoordelen, evenals de manier waarop deze worden toegepast. Het kan een lang proces zijn, maar het slagen voor een ISO 27001 certificeringsaudit toont aan dat uw bedrijf een beveiligingsrisicobeoordeling heeft uitgevoerd om potentiële bedreigingen te identificeren en beveiligingscontroles heeft geïntroduceerd om te beschermen tegen datalekken.

Inhoudsopgave

De voordelen van ISO 27001 certificering en naleving

ISO 27001-certificering geeft organisaties een concurrentievoordeel bij het aantrekken en behouden van klanten, omdat certificering aantoont dat de informatiebeveiliging goed is geregeld. Certificering kan ook leveranciers en andere belanghebbenden aantrekken en behouden die zich zorgen maken over de manier waarop hun informatie wordt beheerd en beschermd.

Zelfs de voorbereiding op het auditproces kan het bestaande ISO 27001-beleid versterken en de interne systemen, structuren en dagelijkse bedrijfsprocessen verbeteren. Het risicobeheerproces kan organisaties ook helpen om beter te voldoen aan wetten op het gebied van gegevensbescherming, zoals CCPA en GDPR, en boetes voor niet-naleving of reputatieschade als gevolg van een vermijdbare gegevensinbreuk te voorkomen.

Lees meer over hoe uw bedrijf zijn cyberbeveiligingspraktijken kan versterken om te slagen voor beveiligingsaudits.

De ISO 27001 controlesets

De 93 controlesets staan in Bijlage A en vallen onder 4 grotere thema's. Om ISO 27001 gecertificeerd te worden, moeten bedrijven aantonen dat ze aan deze controles voldoen. De categorieën zijn:

- Organisatorische controles (37 controles)
- Mensen controles (8 controles)
- Fysieke controles (14 controles)
- Technologische controles (34 controles)

De vorige versie van ISO bevatte 114 controles verdeeld over 14 categorieën. Die versie bevatte ook bepalingen over veilig inloggen en wachtwoordbeheersystemen.

De controle op veilig aanmelden specificeerde "toegang tot systemen en applicaties moet worden gecontroleerd door een veilige aanmeldprocedure wanneer dit wordt vereist door het toegangscontrolebeleid". Met een wachtwoordmanager profiteren gebruikers van het toevoegen van een extra beveiligingslaag aan aanmeldingen en hebben ze één plek om tweefactorauthenticatie te helpen beheren en integreren voor alle websites die dit ondersteunen.

De controle van het wachtwoordbeheersysteem stelt dat "wachtwoordbeheersystemen coöperatief moeten zijn om de kwaliteit van wachtwoorden te waarborgen". ISO raadt aan om een wachtwoordmanager te gebruiken waarmee gebruikers sterke en unieke wachtwoorden kunnen aanmaken en waarmee ze veilig kunnen samenwerken.

> Wachtwoordbeheerders bepalen de sterkte van wachtwoorden, dwingen 2FA af en gebruiken eventlogs om gebruikersactiviteiten te monitoren - allemaal mogelijkheden die bedrijven nodig hebben om te voldoen aan de ISO-vereisten voor toegangscontrole, bescherming van PII en endpointbeveiliging.

In de nieuwste versie van ISO 27001 wordt wachtwoordbeheer behandeld in Bijlage A 5.17. Er zijn veel aanvullende Bijlage A-vereisten waaraan kan worden voldaan of die kunnen worden ondersteund door een wachtwoordmanager te gebruiken. Voorbeelden zijn niet uitputtend:

- **Bijlage A 5.3, Scheiding van taken**: Tegenstrijdige taken en tegenstrijdige verantwoordelijkheidsgebieden moeten worden gescheiden.
- **Bijlage A 5.14, Informatieoverdracht**: Regels, procedures of overeenkomsten voor informatieoverdracht moeten aanwezig zijn voor alle soorten overdrachtsfaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.

- **Bijlage A 5.15, Toegangscontrole**: Regels om de fysieke en logische toegang tot informatie en andere bijbehorende bedrijfsmiddelen te controleren, moeten worden opgesteld en geïmplementeerd op basis van bedrijfs- en informatiebeveiligingseisen.
- **Bijlage A 5.16, Identiteitsbeheer**: De volledige levenscyclus van identiteiten moet worden beheerd.
- **Bijlage A 5.17, Authenticatiegegevens**: De toewijzing en het beheer van authenticatie-informatie wordt gecontroleerd door een beheerproces, met inbegrip van het adviseren van personeel over de beste praktijken voor het omgaan met authenticatie-informatie.
  - Een gedetailleerde inleiding over deze criteria geeft aanbevelingen voor wachtwoorden met advies over het beheren van wachtwoorden, inclusief de mogelijkheid om veilige wachtwoorden te maken. Daarnaast raadt de doelstelling organisaties aan om zwakke, veelgebruikte of gecompromitteerde referenties te vermijden.

> Gezien deze criteria zouden organisaties idealiter een wachtwoordbeheersysteem implementeren dat hen in staat stelt om te rapporteren over en bruikbare inzichten te krijgen in blootgestelde, hergebruikte, zwakke of mogelijk gecompromitteerde wachtwoorden.

- **Bijlage A 5.34, Privacy en bescherming van persoonlijke identificeerbare informatie (PII)**: De organisatie moet de vereisten met betrekking tot het behoud van privacy en de bescherming van PII identificeren en naleven volgens de toepasselijke wet- en regelgeving en contractuele vereisten.
- **Bijlage A 8.1, Eindpuntapparatuur van de gebruiker**: Informatie die is opgeslagen op, verwerkt door of toegankelijk is via eindpuntapparatuur van gebruikers moet worden beschermd.
- **Bijlage A 8.4, Toegang tot broncode**: Lees- en schrijftoegang tot broncode, ontwikkeltools en softwarebibliotheken moet op passende wijze worden beheerd.
- **Bijlage A 8.5, Beveiligde authenticatie**: Veilige authenticatietechnologieën en -procedures worden geïmplementeerd op basis van informatiebeperkingen en het themaspecifieke beleid inzake toegangscontrole.
  - Dit doel richt zich op het gebruik van multi-factor authenticatie om veilig in te loggen op systemen. Met een wachtwoordmanager profiteren gebruikers van het toevoegen van een extra beveiligingslaag aan aanmeldingen en hebben ze ook één plek om tweefactorauthenticatie (2FA) te helpen beheren en integreren voor alle websites die dit ondersteunen. De doelstelling benadrukt ook dat wachtwoorden te allen tijde vertrouwelijk moeten worden behandeld, wat een sterk pleidooi is voor een volledig versleutelde wachtwoordkluis.

> Met wachtwoordbeheersystemen kunnen organisaties alle items in hun kluizen identificeren met inactieve 2FA.

- **Bijlage A 8.11, Afscherming van gegevens**: Afscherming van gegevens moet worden gebruikt in overeenstemming met het onderwerpspecifieke beleid van de organisatie inzake toegangscontrole en ander gerelateerd onderwerpspecifiek beleid en bedrijfsvereisten, rekening houdend met toepasselijke wetgeving.
- **Bijlage A 8.12, Lekkage van gegevens**: Maatregelen ter voorkoming van datalekken moeten worden toegepast op systemen, netwerken en andere apparaten die gevoelige informatie verwerken, opslaan of verzenden.

Wist je dat?

Bitwarden biedt Vault Health Reports waarmee sterke cyberbeveiligingspraktijken kunnen worden gestimuleerd en waarmee werknemers accounts met een zwakke beveiliging kunnen identificeren.

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

ISO 27001 certificering behalen met behulp van een wachtwoordmanager

Een wachtwoordbeheersysteem ondersteunt de vele vereisten van Bijlage A die hierboven zijn opgesomd, en met veel van de vereisten die zijn opgenomen in de algemene controlesets.

Gebruikers kunnen verificatiegegevens geheim houden, best practices voor wachtwoorden toepassen zoals het genereren van sterke, unieke wachtwoorden en wachtwoorden veilig delen met een wachtwoordmanager die gevoelige informatie beveiligt met end-to-end encryptie. Door te beperken wie bepaalde gevoelige of kritieke informatie kan zien, helpen wachtwoordbeheerders ook bij het scheiden van taken en het beperken van bedreigingen van binnenuit.

Organisaties die wachtwoordmanagers gebruiken, stellen eisen aan de sterkte van wachtwoorden, dwingen tweefactorauthenticatie (2FA) af en gebruiken eventlogs om gebruikersactiviteiten te monitoren - allemaal mogelijkheden die bedrijven moeten realiseren om te voldoen aan de ISO-vereisten voor toegangscontrole, bescherming van PII en endpointbeveiliging. De meeste gerenommeerde wachtwoordmanagers faciliteren ook SSO-integratie, zodat beheerders de tools hebben die ze nodig hebben om de toegang en het verificatieproces te beheren. Deze mogelijkheid helpt om te voldoen aan de ISO-vereiste voor veilige authenticatie.

Bij het evalueren van wachtwoordbeheerders voor het ondersteunen van ISO 27001-certificering, moeten organisaties evalueren of de software voldoet aan enterprise-grade beveiligings- en nalevingsstandaarden, zoals SOC2 type 2-naleving, GDPR-naleving, het Data Privacy Framework en HIPAA. Bedrijven moeten een oplossing kiezen die end-to-end zero-knowledge encryptie biedt.

Aan de slag met Bitwarden

Geïnteresseerd in het gebruik van de Bitwarden ISO 27001-compliant wachtwoordmanager om te voldoen aan de ISO 27001-normen voor beheersystemen voor informatiebeveiliging? Start vandaag nog een gratis proefperiode met Bitwarden!

Casestudies:

Inventory Hive, een toonaangevend softwareplatform voor vastgoedinspectie en virtuele rondleidingen in het Verenigd Koninkrijk, heeft met Bitwarden de ISO 27001-certificering behaald.

Zowel Bitwarden Secrets Manager als Bitwarden Password Manager stellen Titanom Technologies in staat om cybersecurity veerkracht aan te tonen en in aanmerking te komen voor ISO 27001 certificering.

"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