コンプライアンスの条件と要件を確認する

100 XP

5 分

このユニットでは、Azure で使用できるコンプライアンス認証の種類について説明します。

Tailwind Traders では、クラウドでのアプリケーションの実行に移行する際に、適用される規制コンプライアンス フレームワークに Azure がどのように準拠しているかを知りたいと考えています。 会社は次のことを質問します。

- 個人データの処理に関して、Azure はどのように準拠しているか。
- Azure の個々のサービスはどのように準拠しているか。

Microsoft のオンライン サービスは、一般的な一連の規制およびコンプライアンスのコントロールに基づいて構築されています。 "コントロール" とは、セキュリティを確保するためにソリューションを比較できる既知の適切な標準と考えてください。 このようなコントロールは、現在の規制に対応し、規制の進化に合わせて調整されます。

Azure 上で使用できるコンプライアンス カテゴリ

他にもたくさんありますが、次の画像は、Azure で使用できる人気のあるコンプライアンス認証の一部を示しています。 このようなオファリングは、次の 4 つのカテゴリに分類されます。グローバル、米国政府機関、業種、地域。

Azure で使用できるさまざまなコンプライアンス認証を理解するために、その一部を詳しく見ていきましょう。

これらのコンプライアンス認証のすべてがご自分やチームに関連するわけではありませんが、コンプライアンスに対する Microsoft の取り組みは包括的で継続的であり、独自にテストおよび検証されていることがわかります。

Criminal Justice Information Service

FBI の Criminal Justice Information Services (CJIS) データベースにアクセスする米国連邦機関または地方機関は、CJIS セキュリティ ポリシーに準拠することが求められます。

Azure は CJIS セキュリティ ポリシーへの準拠を契約上保証する唯一のメジャー クラウド プロバイダーです。 Microsoft は、法執行機関および公安機関が満たす必要があるのと同じ要件に準拠しています。

クラウド セキュリティ アライアンスの STAR 認定資格

Azure、Intune、および Microsoft Power BI については、クラウド セキュリティ アライアンス (CSA) の STAR 認定資格を取得しています。この認定資格には、クラウド プロバイダーのセキュリティ体制について、独立した第三者機関による厳密な評価が含まれます。

STAR 認定資格では、国際標準化機構/国際電気標準会議 (ISO/IEC) 27001 認定資格を取得し、Cloud Controls Matrix (CCM) で指定された条件に適合する必要があります。 この証明書は、以下のクラウド サービス プロバイダーであることを示しています。

- ISO/IEC 27001 の適用される要件に準拠している。
- CCM に記載されているクラウド セキュリティに重要な問題に対処済みである。
- CCM 制御領域でのアクティビティの管理のための STAR 機能成熟度モデルに対して評価済みである。

欧州連合モデル条項

Microsoft は、EU 外での個人データの転送について契約上保証する欧州連合 (EU) 標準契約条項を顧客に提供しています。

Microsoft は EU の第 29 条作業部会 (Article 29 Working Party) から共同承認を受けた最初の会社です。Azure からそのエンタープライズ クラウド顧客に提供される契約上のプライバシー保護は、データの国際転送に関する現行の EU 標準を満たしていることが承認されています。 この標準を満たしているため、Azure の顧客は Microsoft のサービスを使用して、ヨーロッパから世界のその他の地域に Microsoft のクラウドを通して自由かつ確実にデータを移動することができます。

医療保険の携行性と責任に関する法律

医療保険の相互運用性と説明責任に関する法律 (HIPAA) は、患者の保護医療情報 (PHI) を規定する米国の連邦法です。

Azure では、HIPAA および HITECH Act 内の特定のセキュリティおよびプライバシーに関する条項への準拠を明記した HIPAA Business Associate Agreement (BAA) が顧客に示されます。各顧客のコンプライアンスを支援するために、Microsoft は Azure の顧客に契約の補遺として BAA を提供します。

国際標準化機構/国際電気標準会議 27018

Microsoft は、クラウド サービス プロバイダーによる個人情報の処理について規定した ISO/IEC 27018 実務基準を採用した最初のクラウド プロバイダーです。

Multi-Tier Cloud Security シンガポール

Multi-Tier Cloud Security (MTCS) 証明機関による厳密な評価後に、Microsoft のクラウド サービスは、次の 3 つのサービス分類すべてにわたり MTCS 584:2013 認定を受けました。

- サービスとしてのインフラストラクチャ (IaaS)
- サービスとしてのプラットフォーム (PaaS)
- サービスとしてのソフトウェア (SaaS)

Microsoft は、3 つのサービス分類すべてにわたりこの認定資格を取得した最初のグローバル クラウド ソリューション プロバイダーです。

Service Organization Controls 1、2、3

Microsoft でカバーされているクラウド サービスは、Service Organization Controls (SOC) レポート フレームワークに対して、少なくとも年 1 回、独立した第三者機関の監査担当者によって監査されます。

Microsoft クラウド サービスに対する監査は、各サービスに適用される信頼の原則に基づくデータのセキュリティ、可用性、整合性の処理、および機密性管理を対象としています。

National Institute of Standards and Technology Cybersecurity Framework

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) は、サイバーセキュリティに関連するリスクの管理を目的とした、標準、ガイドライン、およびベスト プラクティスから成る自主的なフレームワークです。

Microsoft クラウド サービスは、独立した第三者機関による Federal Risk and Authorization Management Program (FedRAMP) の中程度および高い基準に対する監査を受けています。Microsoft クラウド サービスは FedRAMP 標準に従って認定されました。

さらに、セキュリティおよびプライバシーに関する標準開発で先頭に立つ Health Information Trust Alliance (HITRUST) によって検証済みの評価が実施され、Office 365 は NIST CSF によって指定された目標を満たしていることが認定されました。

イギリス政府の G-Cloud

イギリス (UK) 政府の G-Cloud は、イギリス国内の政府機関によって使用されるサービスを対象にしたクラウド コンピューティング認定資格です。 Azure は、イギリス政府から公式の認定を受けています。