Microsoft Compliance Manager

Cpa firm Report

2025-12-26 12:19:43 AM UTC

Table of contents

Executive Summary

Introduction

The Compliance Manager report summarizes the current status of those assessments on your environment, as they map to the associated controls. This report does not represent a complete compliance report for the standard, nor does it ensure compliance. However, it can be a valuable tool for organizations that are looking to improve their compliance posture

The Compliance Manager report includes the following information:

* The name of the compliance standard or framework that is being assessed.

* The specific controls that are being assessed.

* The current status of each control (compliant, non-compliant, or not applicable).

* Any recommendations for improving compliance.

The Compliance Manager report can be used to identify areas where your cloud environment is not compliant with a particular standard or regulation. This information can then be used to take steps to improve your compliance posture.

About AICPA Privacy Management Framework Regulation

The Privacy Management Framework (PMF) is a set of data and information privacy policies and procedures that are used as a foundational element in establishing and operating a comprehensive information privacy program that addresses privacy obligations and risks while facilitating current and future business opportunities. The Privacy Management Framework (PMF) can be used as a foundational element in establishing and operating a comprehensive information privacy program that addresses privacy obligations and risks while facilitating current and future business opportunities.

More info on Privacy Management Framework - https://www.incpas.org/docs/default-source/blog-article/privacy-management-framework.pdf

Total Controls Tested

86

Passed Controls

0

Failed Controls

86

Microsoft Compliance Manager Sections Summary

The following is a summary status for each of the sections of the Microsoft cloud security benchmark. For each section, you will find the overall number of passing and failing controls, based on automated assessments run by Microsoft Compliance Manager.

A failing control indicates that at least one Microsoft Compliance Manager assessment associated with this control failed. A passing control indicates that all the Microsoft Compliance Manager assessments associated with this control passed. Note that status is shown only for supported controls, i.e. controls that have relevant Microsoft Compliance Manager assessments associated with them.

Control Category Summary : aicap serv

The control status for each of these areas can be either passed or failed. The Compliance Posture report provides a summary of the control status for your cloud environment, as well as any recommendations for improving compliance.

Control Family	Passed Controls	Failed Controls		
Security for privacy	0	25		0%
Disclosure to third parties	0	11		0%
Collection and creation	0	7		0%
Agreements, notices and communication	0	8		0%
Access	0	7		0%
Use, retention and disposal	0	4		0%
Management	0	18		0%
Monitoring and enforcement	0	5		0%
Data integrity and quality	0	1		0%

Control Summary : aicap serv

The following is a summary status for each supported control of the Cpa firm Assessment. For each control, you will find the overall number of passed and total actions associated with that control.

Note that status is shown only for supported controls, i.e. controls that have relevant Microsoft Compliance Manager assessments associated with them.

Control Name	Test Completed	
Use encryption to protect data	0 / 5	0%
Protect encryption keys	0 / 7	0%
Restrict access to information assets	0 / 4	0%
Validate physical access periodically	0 / 3	0%
Manage physical access	0 / 3	0%
Use antivirus and anti-malware software	0 / 7	0%
Restrict logical and physical access to PI	0 / 3	0%
Protect end point and mobile devices	0 / 1	0%
Use encryption technologies or secure communication channels to protect data	0 / 2	0%
Manage points of access	0 / 7	0%
Implement internal physical access control	0 / 2	0%
Establish, document and manage user and system identification policy and procedure requirements	0 / 7	0%
Manage credentials for granting access	0 / 4	0%
Implement logical access security control	0 / 5	0%
Implement policies for physical protection of information in media	0 / 4	0%
Consider network segmentation	0 / 2	0%

Identify environmental threats	0 / 4		0%
Restrict transmission of information	0 / 1		0%
Implement incident management and recovery testing	0 / 1		0%
Evaluate confidentiality, completeness, integrity and availability of systems and back-up data	0 / 2		0%
Restrict physical access	0 / 1		0%
Identify and authenticate users	0 / 4		0%
Consider different types of ongoing and separate evaluations	0 / 1		0%
Protect removable media	0 / 1		0%
Implement business continuity plan testing	0 / 1		0%
Provide notice of breaches and incidents	0 / 4		0%
Communicate privacy policies to third parties	0 / 5		0%
Notify the suspected unauthorized disclosures of PI	0 / 4		0%
Create and retain record of authorized disclosures	0 / 1		0%
Capture, identify and communicate requests for information	0 / 3		0%
Obtain privacy commitments from vendors and other third parties	0 / 4		0%
Disclose PI only to appropriate third parties for new purposes and uses	0 / 3		0%
Report actual or suspected unauthorized disclosures	0 / 3		0%
Identify types of PI and handling processes	0 / 2		0%
Remediate misuse of PI by third parties	0 / 2		0%

Create and retain record of detected or reported unauthorized disclosures	0 / 4		0%
Communicate consequences of denying or withdrawing consent	0 / 2		0%
Obtain explicit and implicit consent	0 / 4		0%
Implement PI collection and creation.	0 / 3		0%
Obtain consent for data transfers	0 / 4		0%
Document and obtain consent for new purposes and uses	0 / 2		0%
Allow ability to opt-out	0 / 3		0%
Ensure data subjects are informed of collection, use and disclosure of PI	0 / 3		0%
Re-execute the updated agreements.	0 / 3		0%
Execute formal agreements	0 / 6		0%
Ensure clear and conspicuous privacy	0 / 2		0%
Approve changes done to privacy agreements/notices	0 / 2		0%
Ensure entities and activities covered	0 / 2		0%
Implement data subject revocations	0 / 4		0%
Perform ongoing notices and communications	0 / 1		0%
Implement agreements, notices and communications	0 / 2		0%
Provide understandable PI within reasonable time	0 / 2		0%
Authenticate data subjects identities	0 / 4		0%
Permit data subjects to update or correct PI	0 / 2		0%

Communicate denial of access requests and correction requests	0 / 2		0%
Allow ability to access the stored PI	0 / 1		0%
Permit data subjects access to their PI	0 / 2		0%
Inform data subjects when access is denied	0 / 1		0%
Ensure PI is used for intended purposes	0 / 3		0%
Dispose of, destroy and redact personal information (PI)	0 / 3		0%
Retain and protect personal information (PI)	0 / 6		0%
Capture, identify and flag requests for deletion	0 / 4		0%
Implement data governance program	0 / 4		0%
Data and Information Classification	0 / 2		0%
Document data and information privacy policies and procedures	0 / 8		0%
Perform privacy (risk) impact assessment	0 / 6		0%
Implement governance of policies and procedures	0 / 4		0%
Establish accountability	0 / 3		0%
Establish an overall governance and legal structure	0 / 2		0%
Identify, classify and prioritize critical PI	0 / 4		0%
Communicate policy to personnel and related parties	0 / 3		0%
Provide privacy awareness and training	0 / 4		0%
Review contracts for consistency with privacy policy	0 / 2		0%

Evaluate and address the impact of any privacy policy changes	0 / 2		0%
Perform ongoing and separate evaluations on privacy controls and deficiencies	0 / 2		0%
Implement privacy incident response plan	0 / 2		0%
Implement a policy governance and accountability process	0 / 2		0%
Establish qualifications of internal personnel	0 / 1		0%
Notify relevant authorities in the event of system and privacy information breaches	0 / 2		0%
Identify data privacy security controls	0 / 1		0%
Document and report instances of noncompliance	0 / 3		0%
Document and report compliance review results	0 / 5		0%
Address inquiries, complaints and disputes	0 / 3		0%
Document and communicate dispute resolution and recourse	0 / 2		0%
Perform ongoing monitoring	0 / 1		0%
Ensure accuracy and completeness of personal information (PI)	0 / 3		0%