



# Microsoft Compliance Manager

## ISO/IEC 27001:2022 Assessment Report

2024-12-11 12:45:43 PM UTC

# Table of contents

- 1. Executive Summary
- 2. Microsoft Compliance Manager Sections Summary
  - \* Control Category Summary : Microsoft 365
  - \* Control Summary : Microsoft 365

## 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 ISO/IEC 27001:2022 Regulation

The International Organization for Standardization (ISO) 27001 standard provides requirements for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS). Internal and external parties can use this international standard to assess an organization's ability to meet the organization's information security requirements.

More info on ISO 27001 - <https://www.iso.org/standard/82875.html>

### Total Controls Tested

108

### Passed Controls

54

### Failed Controls

54

# 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 : Microsoft 365

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	
Organizational controls	9	24	<div><div></div></div> 27%
Technological controls	13	18	<div><div></div></div> 41%
People controls	3	4	<div><div></div></div> 42%
Performance evaluation	1	3	<div><div></div></div> 25%
Physical controls	11	3	<div><div></div></div> 78%
Planning	4	0	<div><div></div></div> 100%
Support	6	0	<div><div></div></div> 100%
Context of the organization	2	0	<div><div></div></div> 100%
Improvement	1	1	<div><div></div></div> 50%
Leadership	2	0	<div><div></div></div> 100%
Operation	2	1	<div><div></div></div> 66%

## Control Summary : Microsoft 365

The following is a summary status for each supported control of the ISO/IEC 27001:2022 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	
Identity management	4 / 6	<div><div></div></div> 66%
Access rights	2 / 5	<div><div></div></div> 40%
Labelling of information	2 / 6	<div><div></div></div> 33%
Protection of records	5 / 6	<div><div></div></div> 83%
Addressing information security within supplier agreements	4 / 4	<div><div></div></div> 100%
Managing information security in the information and communication technology (ICT) supply chain	3 / 4	<div><div></div></div> 75%
Monitoring, review and change management of supplier services	3 / 4	<div><div></div></div> 75%
Information security incident management planning and preparation	2 / 3	<div><div></div></div> 66%
Assessment and decision on information security events	3 / 4	<div><div></div></div> 75%
Response to information security incidents	1 / 2	<div><div></div></div> 50%
Learning from information security incidents	1 / 2	<div><div></div></div> 50%
Collection of evidence	1 / 1	<div><div></div></div> 100%
Segregation of duties	2 / 2	<div><div></div></div> 100%
ICT readiness for business continuity	4 / 5	<div><div></div></div> 80%
Intellectual property rights	1 / 3	<div><div></div></div> 33%

Compliance with policies, rules and standards for information security	2 / 2	<div><div></div></div>	100%
Management responsibilities	1 / 2	<div><div></div><div></div></div>	50%
Inventory of information and other associated assets	2 / 3	<div><div></div><div></div></div>	66%
Acceptable use of information and other associated assets	2 / 2	<div><div></div></div>	100%
Return of assets	3 / 3	<div><div></div></div>	100%
Classification of information	1 / 5	<div><div></div><div></div><div></div><div></div><div></div></div>	20%
Information transfer	2 / 4	<div><div></div><div></div><div></div><div></div></div>	50%
Access control	2 / 5	<div><div></div><div></div><div></div><div></div><div></div></div>	40%
Authentication information	1 / 1	<div><div></div></div>	100%
Information security in supplier relationships	2 / 2	<div><div></div></div>	100%
Information security roles and responsibilities	2 / 2	<div><div></div></div>	100%
Privacy and protection of personal identifiable information (PII)	0 / 1	<div><div></div></div>	0%
Threat intelligence	0 / 4	<div><div></div><div></div><div></div><div></div></div>	0%
Information security for use of cloud services	0 / 1	<div><div></div></div>	0%
Independent review of information security	0 / 2	<div><div></div><div></div></div>	0%
Legal, statutory, regulatory and contractual requirements	0 / 1	<div><div></div></div>	0%
Policies for information security	0 / 1	<div><div></div></div>	0%
Documented operating procedures	0 / 1	<div><div></div></div>	0%
Installation of software on operational systems	2 / 5	<div><div></div><div></div><div></div><div></div><div></div></div>	40%
Information access restriction	1 / 4	<div><div></div><div></div><div></div><div></div></div>	25%
Information deletion	2 / 2	<div><div></div></div>	100%
Data masking	1 / 2	<div><div></div><div></div></div>	50%
Data leakage prevention	0 / 3	<div><div></div><div></div><div></div></div>	0%

Information backup	2 / 2	<div><div></div></div> 100%
Redundancy of information processing facilities	1 / 1	<div><div></div></div> 100%
Logging	2 / 4	<div><div></div></div> 50%
Monitoring activities	1 / 2	<div><div></div></div> 50%
Privileged access rights	2 / 5	<div><div></div></div> 40%
Networks security	1 / 4	<div><div></div></div> 25%
Security of network services	1 / 1	<div><div></div></div> 100%
Segregation of networks	2 / 4	<div><div></div></div> 50%
Web filtering	4 / 4	<div><div></div></div> 100%
Use of cryptography	1 / 3	<div><div></div></div> 33%
Secure development life cycle	2 / 2	<div><div></div></div> 100%
Application security requirements	1 / 2	<div><div></div></div> 50%
Secure system architecture and engineering principles	1 / 1	<div><div></div></div> 100%
Secure coding	1 / 1	<div><div></div></div> 100%
Security testing in development and acceptance	1 / 2	<div><div></div></div> 50%
Outsourced development	1 / 1	<div><div></div></div> 100%
Separation of development, test and production environments	2 / 2	<div><div></div></div> 100%
Test information	2 / 2	<div><div></div></div> 100%
Protection of information systems during audit testing	0 / 1	<div><div></div></div> 0%
Capacity management	1 / 1	<div><div></div></div> 100%
Protection against malware	2 / 4	<div><div></div></div> 50%
Management of technical vulnerabilities	2 / 5	<div><div></div></div> 40%
Configuration management	2 / 2	<div><div></div></div> 100%
User end point devices	0 / 3	<div><div></div></div> 0%
Clock synchronization	0 / 1	<div><div></div></div> 0%
Use of privileged c programs	0 / 1	<div><div></div></div> 0%

Screening	3 / 4	<div><div></div></div>	75%
Terms and conditions of employment	1 / 1	<div><div></div></div>	100%
Information security awareness, education and training	1 / 1	<div><div></div></div>	100%
Disciplinary process	2 / 2	<div><div></div></div>	100%
Responsibilities after termination or change of employment	4 / 5	<div><div></div></div>	80%
Remote working	5 / 7	<div><div></div></div>	71%
Information security event reporting	3 / 7	<div><div></div></div>	42%
Monitoring, measurement, analysis and evaluation	1 / 2	<div><div></div></div>	50%
General - Internal audit	1 / 1	<div><div></div></div>	100%
Management review inputs	1 / 2	<div><div></div></div>	50%
Management review results	0 / 1	<div><div></div></div>	0%
Physical security perimeters	3 / 3	<div><div></div></div>	100%
Storage media	2 / 3	<div><div></div></div>	66%
Supporting utilities	1 / 1	<div><div></div></div>	100%
Cabling security	1 / 1	<div><div></div></div>	100%
Equipment maintenance	3 / 3	<div><div></div></div>	100%
Secure disposal or re-use of equipment	4 / 4	<div><div></div></div>	100%
Physical entry	2 / 2	<div><div></div></div>	100%
Securing offices, rooms and facilities	3 / 3	<div><div></div></div>	100%
Physical security monitoring	3 / 3	<div><div></div></div>	100%
Protecting against physical and environmental threats	1 / 1	<div><div></div></div>	100%
Working in secure areas	2 / 2	<div><div></div></div>	100%
Equipment siting and protection	1 / 1	<div><div></div></div>	100%
Security of assets off-premises	2 / 3	<div><div></div></div>	66%
Clear desk and clear screen	0 / 1	<div><div></div></div>	0%

General - Actions to address risks and opportunities	1 / 1	<div><div></div></div>	100%
Information security risk assessment - Actions to address risks and opportunities	1 / 1	<div><div></div></div>	100%
Information security risk treatment - Actions to address risks and opportunities	1 / 1	<div><div></div></div>	100%
Planning of changes	1 / 1	<div><div></div></div>	100%
Resources	1 / 1	<div><div></div></div>	100%
Competence	1 / 1	<div><div></div></div>	100%
Awareness	1 / 1	<div><div></div></div>	100%
General - Documented information	1 / 1	<div><div></div></div>	100%
Creating and updating - Documented information	1 / 1	<div><div></div></div>	100%
Control of documented information - Documented information	1 / 1	<div><div></div></div>	100%
Determining the scope of the information security management system	1 / 1	<div><div></div></div>	100%
Information security management system	1 / 1	<div><div></div></div>	100%
Nonconformity and corrective action	2 / 2	<div><div></div></div>	100%
Continual improvement	0 / 1	<div><div></div></div>	0%
Leadership and commitment	1 / 1	<div><div></div></div>	100%
Organizational roles, responsibilities and authorities	1 / 1	<div><div></div></div>	100%
Operational planning and control	1 / 1	<div><div></div></div>	100%
Information security risk assessment	1 / 1	<div><div></div></div>	100%
Information security risk treatment	1 / 2	<div><div></div><div></div></div>	50%