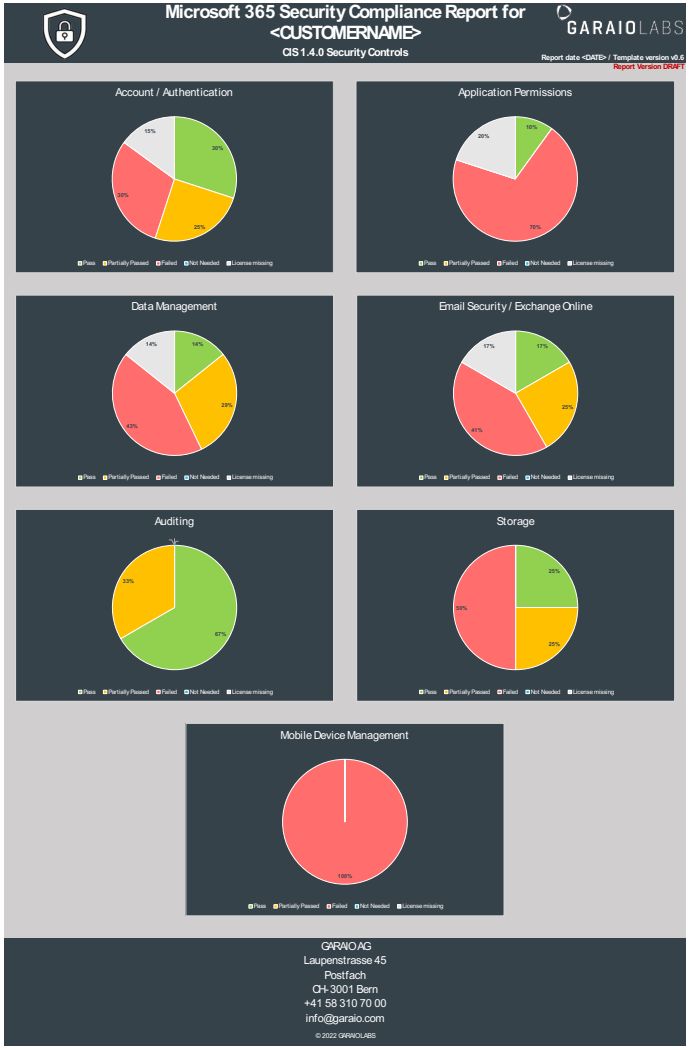
Overview Report



Details Report

Microsoft 365 Security Compliance Report for <CUSTOMERNAME>

CIS 1.4.0 Security Controls

GARAIOLABS

Report date <DATE> / Template version v0.6

Security Controls | Risk Analysis and Impact — Report Version DRAFT

	Profile Definitions	Security Function	Audit Status	Remediation Status	Decision	Notes
Account / Authentication						
Ensure multifactor authentication is enabled for all users in administrative roles	E3 Level 1	Protect	Partially Passed	OK	DONE	No Conditional Access policies, but all users in administrative roles are enabled for MFA by Security Defaults.
Ensure multifactor authentication is enabled for all users in all roles	E3 Level 2	Protect	Partially Passed	OK	DONE	No Conditional Access policies, but all users are enabled for MFA by Security Defaults.
Ensure that between two and four global admins are designated	E3 Level 1	Protect, Detect	Failed	Not Planned	N/A	8 Global Administrators present, based also because of the employees in the IT-Department.
Ensure self-service password reset is enabled	E3 Level 1	Protect	Pass	OK	DONE	Self-Service Password Reset is enabled for everyone.
Ensure that password protection is enabled for Active Directory	E3 Level 1	Protect	Partially Passed	Not Planned	N/A	Password protection is enabled, but will not be enforced.
Enable Conditional Access policies to block legacy authentication	E3 Level 1	Protect	Partially Passed	OK	DONE	No Conditional Access policies, but secured by the Security Defaults.
Ensure that password hash sync is enabled for resiliency and leaked credential detection	E3 Level 1	Identify, Protect				
Enable Azure AD Identity Protection sign-in risk policies	E5 Level 2	Protect, Detect	N/A	OK	N/A	No license available (need Azure AD Premium P2 license which is not included in Microsoft 365 E3).
Enable Azure AD Identity Protection user risk policies	E5 Level 2	Detect	N/A	OK	N/A	No license available (need Azure AD Premium P2 license which is not included in Microsoft 365 E3).
Use Just In Time privileged access to Office 365 roles	E5 Level 2	Protect, Detect	N/A	OK	N/A	No license available (need Azure AD Premium P2 license which is not included in Microsoft 365 E3).
Ensure Security Defaults is disabled on Azure Active Directory	E3 Level 1	Protect	Partially Passed	Not Planned	N/A	Because of the missing Conditional Access policies, it is recommended to enable Security Defaults. We recommend to enable Conditional Access and disable the Security Defaults for better protection.
Ensure that only organizationally managed/approved public groups exist	E3 Level 2	Identify, Protect	Pass	OK	DONE	There are multiple groups with the privacy level "Public". This is deliberately chosen by company regulations - therefore passed.
Ensure that collaboration invitations are sent to allowed domains only	E3 Level 2	Identify, Protect	Pass	OK	DONE	Invitaions can be send to any domain. This is deliberately chosen by company regulations to work with lot of companies - therefore passed.
Ensure that LinkedIn contact synchronization is disabled	E3 Level 2	Identify, Detect	Failed	Not Planned	N/A	Connection is set to yes and therefore connect account with LinkedIn is allowed.
Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users	E3 Level 1	Protect	Failed	Not Planned	N/A	No Conditional Access policies are configured.
Ensure the option to stay signed in is disabled	E3 Level 2	Protect	Failed	Not Planned	N/A	The option to remain signed in is enabled. This allows users to stay signed in and get a persistent refresh token from up to 90 days.
Ensure modern authentication for Exchange Online is enabled	E3 Level 1	Identify, Protect	Pass	OK	DONE	
Ensure modern authentication for Skype for Business Online is enabled	E3 Level 1	Protect	Pass	OK	DONE	
Ensure modern authentication for SharePoint applications is required	E3 Level 1	Protect	Failed	Not Planned	N/A	It is allowed to get access for applications without modern authentication.
Ensure that Office 365 Passwords Are Not Set to Expire	E3 Level 1	Protect	Pass	OK	DONE	Password expiration policy is set to never expire.
Ensure Administrative accounts are separate, unassigned, and cloud-only	E3 Level 1	Protect, Detect	Failed	Not Planned	N/A	Administrative Accounts are synced from On-Premise and have license assigned.
Application Permissions						

Details Report

Microsoft 365 Security Compliance Report for <CUSTOMERNAME>

CIS 1.4.0 Security Controls

GARAIOLABS

Report date <DATE> / Template version v0.6

	Security Controls						Risk Analysis and Impact
	Profile Definitions	Security Function	Audit Status	Remediation Status	Decision	Notes	Report Version DRAFT
Account / Authentication							
Application Permissions							
Data Management							
Email Security / Exchange Online							
Ensure the Common Attachment Types Filter is enabled	E3 Level 1	Protect	Failed	Not Planned	N/A	Common attachments filter is not enabled.	Blocking known malicious file types can help prevent malware-infested files from infecting a host. Blocking common malicious file types should not cause an impact in modern computing environments.
Ensure Exchange Online Spam Policies are set correctly	E3 Level 1	Protect	Failed	Not Planned	N/A	No notification of the IT-Admin is configured. So it is not possible to find such blocked accounts without intervention of the enduser.	A blocked account is a good indication that the account in question has been breached and an attacker is using it to send spam emails to other people. Notification of users that have been blocked should not cause an impact to the user.
Ensure all forms of mail forwarding are blocked and/or disabled	E3 Level 1	Identify, Protect	Partially Passed	Not Planned	N/A	No forwarding rules configured. But the Parameter AutoForwardEnabled is set to True. No Rule for "Client Rules To External Block" is configured.	Attackers often create these rules to exfiltrate data from your tenancy, this could be accomplished via access to an end-user account or otherwise. Care should be taken before implementation to ensure there is no business need for case-by-case auto-forwarding. Disabling auto-forwarding to remote domains will affect all users and in an organization. Any exclusions should be implemented based on organizational policy.
Ensure mail transport rules do not whitelist specific domains	E3 Level 1	Protect	Pass	OK	DONE	Only a specific email address is whitelisted and not critical.	Whitelisting domains in transport rules bypasses regular malware and phishing scanning, which can enable an attacker to launch attacks against your users from a safe haven domain. Care should be taken before implementation to ensure there is no business need for case-by-case whitelisting. Removing all whitelisted domains could affect incoming mail flow to an organization although modern systems sending legitimate mail should have no issue with this.
Ensure the Safe Links policy is enabled	E5 Level 2	Protect	N/A	Not Planned	N/A	No license available (need Microsoft Defender for Office 365 license which is not included in Microsoft 365 E3).	Safe Links extends phishing protection to include redirecting all email hyperlinks through a forwarding service which will block malicious ones even after the email has been delivered to the end user. When enabling and configuring Safe Links impact to the end-user should be low. Users should be informed of the change as, in the event a link is unsafe and blocked, they will receive a message that it has been blocked.