

IT1 ICT audit Light Geconsolideerd overzicht



VERTROUWELIJKHEIDSLCLAUSULE

Opgesteld voor: KLANTNAAM

Opgesteld door: IT1 bv









Scandatum: 08/03/2023









2021/02/03

Management Plan

The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

RISK SCORE	RECOMMENDATION	ERNST	KANS
90	On Premise Sync has been configured for the organization and is enabled; however, the time since the last sync is greater than 15 days. This may indicate an issue with the onpremise sync. Investigate and remediate issues with On Premise Sync.		
90	Unimplemented Microsoft Control: Block Legacy Authentication. You have 39 of 40 users that don't have legacy authentication blocked. Today, most compromising sign-in attempts come from legacy authentication. Older office clients such as Office 2010 don't support modern authentication and use legacy protocols such as IMAP, SMTP, and POP3. Legacy authentication does not support multi-factor authentication (MFA). Even if an MFA policy is configured in your environment, bad actors can bypass these enforcements through legacy protocols.		
90	Unimplemented Microsoft Control: Customer Lockbox Not Enabled. Turning on the customer lockbox feature requires that approval is obtained for datacenter operations that grants a Microsoft employee direct access to your content. Access may be needed by Microsoft support engineers if an issue arises. There's an expiration time on the request and content access is removed after the support engineer has fixed the issue.		
90	Unimplemented Microsoft Control: Integrated		

RISK SCORE	RECOMMENDATION	ERNST	KANS
	<p>Apps. Tighten the security of your services by regulating the access of third-party integrated apps. Only allow access to necessary apps that support robust security controls. Third-party applications are not created by Microsoft, so there is a possibility they could be used for malicious purposes like exfiltrating data from your tenancy. Attackers can maintain persistent access to your services through these integrated apps, without relying on compromised accounts.</p>		
90	<p>Unimplemented Microsoft Control: Multi-factor Authentication. You have 10 out of 40 users that are not registered and protected with MFA. See Users section in Azure AD Report for details. Multi-factor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised.</p>		
90	<p>Unimplemented Microsoft Control: Self Service Password Reset. You have 40 of 40 users who don't have self-service password reset enabled. With self-service password reset in Azure Active Directory, users no longer need to engage help desk to reset passwords. This feature works well with Azure AD dynamically banned passwords, which prevents easily guessable passwords from being used.</p>		
90	<p>Unimplemented Microsoft Control: Sign in Risk Policy. You have 40 of 40 users that don't have the sign-in risky policy turned on. Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication (MFA).</p>		
90	<p>Unimplemented Microsoft Control: User Risk Policy. You have 40 users out of 40 that do not have user risk policy enabled. With the user risk policy turned on, Azure Active Directory detects the KANS that a user</p>		

RISK SCORE	RECOMMENDATION	ERNST	KANS
	<p>account has been compromised. As an administrator, you can configure a user risk conditional access policy to automatically respond to a specific user risk level. For example, you can block access to your resources or require a password change to get a user account back into a clean state.</p>		

 Low Risk

RISK SCORE	RECOMMENDATION	ERNST	KANS
25	<p>Team settings allows guests to create and remove channels. This could cause loss of data as guests add and remove channels.</p> <p>Verify if guest creation and removal of channels is desired on the specified Teams. When not necessary, disable the ability of Team guests to create and remove channels to avoid potential data loss and channel proliferation.</p> <p><input type="checkbox"/> Administrative</p>	