Nova Quantum

Securing your business data with Microsoft 365

Date: 14 Sept 2020

Author: *Michael Deacon, Cloud Security Architect at NovaQuantum*

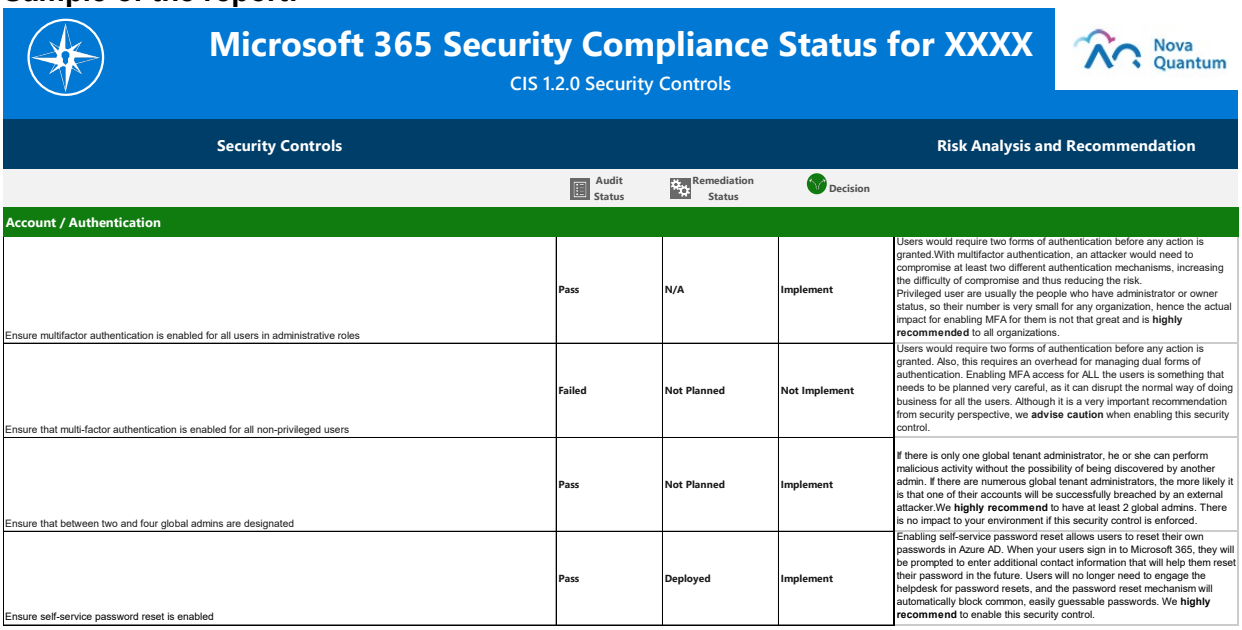
Nova Quantum

Our Microsoft 365 security services:

1. Initial security assessment of your Microsoft 365 services: a comprehensive security assessment against CIS Benchmark Security framework(over 50 security checks that have zero or very limited impact to be implemented). The report includes recommendations for Exchange Online, SharePoint Online, OneDrive for Business, Skype/Teams, Azure Active Directory, and Mobile Devices.

   As part of this phase, we will need an account with enough privileges to M365 so we can audit all the security settings currently configured. Estimated commitment time from the client: 1-2h.

   Sample of the report:



Microsoft 365 Security Compliance Status for XXXX

CIS 1.2.0 Security Controls

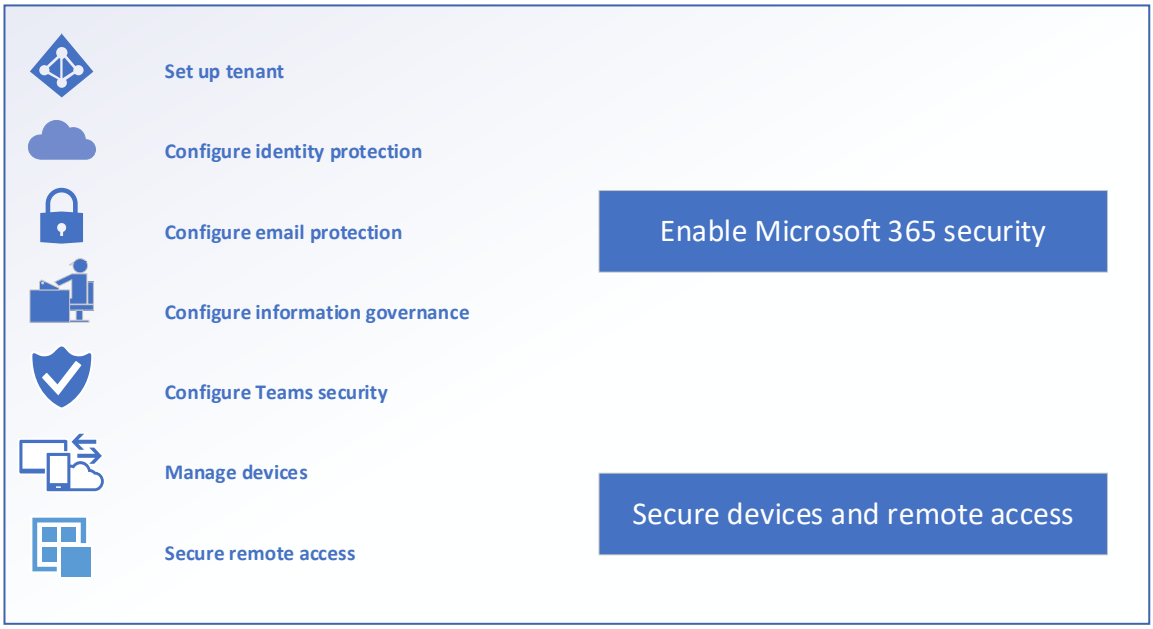
Nova Quantum

Security Controls	Audit Status	Remediation Status	Decision	Risk Analysis and Recommendation
Account / Authentication				
Ensure multifactor authentication is enabled for all users in administrative roles	Pass	N/A	Implement	Users would require two forms of authentication before any action is granted.With multifactor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk. Privileged user are usually the people who have administrator or owner status, so their number is very small for any organization, hence the actual impact for enabling MFA for them is not that great and is **highly recommended** to all organizations.
Ensure that multi-factor authentication is enabled for all non-privileged users	Failed	Not Planned	Not Implement	Users would require two forms of authentication before any action is granted. Also, this requires an overhead for managing dual forms of authentication. Enabling MFA access for ALL the users is something that needs to be planned very careful, as it can disrupt the normal way of doing business for all the users. Although it is a very important recommendation from security perspective, we **advise caution** when enabling this security control.
Ensure that between two and four global admins are designated	Pass	Not Planned	Implement	If there is only one global tenant administrator, he or she can perform malicious activity without the possibility of being discovered by another admin. If there are numerous global tenant administrators, the more likely it is that one of their accounts will be successfully breached by an external attacker.We **highly recommend** to have at least 2 global admins. There is no impact to your environment if this security control is enforced.
Ensure self-service password reset is enabled	Pass	Deployed	Implement	Enabling self-service password reset allows users to reset their own passwords in Azure AD. When your users sign in to Microsoft 365, they will be prompted to enter additional contact information that will help them reset their password in the future. Users will no longer need to engage the helpdesk for password resets, and the password reset mechanism will automatically block common, easily guessable passwords. We **highly recommend** to enable this security control.

2. Planning session to identify all the Microsoft 365 security features that make sense for your business. **(estimated *commitment* time: 2x2h sessions)**
3. Configuration of all security features identified above. **(estimated *commitment* time: 2h)**
4. Security training/education session for the whole team. Explaining in non-technical terms security best practices(Phishing, Privacy and Protection of your own computer topics) that should be followed by everyone. **(estimated duration time: 1-2h)**

More info about why and how we can secure your business data can be found in this short presentation.

An overview of the key steps in enabling the security controls of Microsoft 365 is shown in the following illustration:



For each of these phases, we will review the key steps and any security-related issues to consider. Because each NGO have different security needs and attitudes, the checklist we run through includes suggested recommendations for two common scenarios.

- The **normal scenario** is designed for a typical business that wants to enable secure remote work and balance ease of use with security.
- The **high risk scenario** is more appropriate for a business that wants to maximize security protections and has higher concern for risk (for example, to adhere to regulatory requirements such as HIPAA,PCI or GLBA). This business is also willing to put more effort into maintaining security and control of the work from home environment.

Nova Quantum