

MSAP

MICROSOFT SECURITY ASSURANCE PROGRAMME

Rest assured of secure, resilient cloud-based infrastructure for your organisations critical online services.

SEQA's MSAP is designed to improve the overall security of Microsoft infrastructure and provide risk assurance for organisations wanting to implement secure cloud architecture. Our MSAP supports the creation of an environment that is hardened to security vulnerabilities by ensuring that the security controls that Microsoft offer have been implemented effectively and to best practice standards.



Is an MSAP right for my organisation?

Is the security of your online Microsoft solutions critical to your business?

As cloud services are increasingly adopted to support business productivity, efficiency and cost savings, it is imperative that cloud apps be built securely, so that you are not inadvertently compromising your cloud environment or opening the door to a data leak.

The objective behind an MSAP is to build secure Microsoft cloud services by identifying misconfigurations and enhancing current configurations. Since, every cloud infrastructure is unique this requires meticulous planning while also performing all the necessary checks. Therefore, SEQA takes a bespoke and pragmatic approach towards defining a tailored programme to ensure your Microsoft cloud infrastructure is secure.



What does an MSAP entail?

An MSAP roadmap developed by SEQA aligns to Microsoft and industry best practices and security standards such as CIS Benchmark. It also involves a combination of security strategy, planning, auditing, consulting and training to ensure a pragmatic approach to help build secure solutions for your organisation.

The MSAP consists of a set of security reviews to identify misconfigurations in your Microsoft cloud service or to provide security enhancements that helps you achieve your cloud security goals. SEQA can provide this service for all your key cloud architecture, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

On the following page is a list of service offerings within SEQA's MSAP programme, so you can select the service that best suits the needs of your organisation.



Why an MSAP is important and it's benefits?

- ✓ Assurance regarding the security of your Microsoft ecosystem and business applications
- ✓ Tailored reviews based on your environment, to help you achieve your cloud security goals
- ✓ Minimise potential risks to your organisation, including cyber-attacks, or privacy and data breaches
- ✓ A Cloud environment that complies with NZ or Global Cloud Security Standards

SEQA's MSAP Services

Microsoft Dynamics 365 Review

REVIEW SCOPE	<ul style="list-style-type: none"> - User Access Security - Change Management Process <ul style="list-style-type: none"> - Log Monitoring - Incident Management - Business Application Management <ul style="list-style-type: none"> - Web Server Review - Database Security Review
OUTCOMES	<ul style="list-style-type: none"> ✓ Security issues and risk pertaining to each identified risk ✓ Practical recommendations and detailed technical hardening steps

Azure AD Review

REVIEW SCOPE	<ul style="list-style-type: none"> - Identity and Access Management (IAM) <ul style="list-style-type: none"> - Threat Protection - Password Policy - Logging and Monitoring <ul style="list-style-type: none"> - Authentication policy - MDM Management - Microsoft Defender Advanced Threat Protection
OUTCOMES	<ul style="list-style-type: none"> ✓ Overview of the existing Azure AD configuration ✓ Provide recommendations based on industry best practices and security configuration improvements

Microsoft Cloud Compliance Audit

REVIEW SCOPE	<ul style="list-style-type: none"> - Identity and Access Management (IAM) <ul style="list-style-type: none"> - Data Management - Password Policy - Logging and Monitoring <ul style="list-style-type: none"> - Authentication policy - Disaster Recovery
OUTCOMES	<ul style="list-style-type: none"> ✓ Overview of existing environment's compliance policies. ✓ Security risk around the non-compliant unit ✓ Practical recommendation to help achieve compliance requirements

Microsoft Azure Security Review

REVIEW SCOPE	<ul style="list-style-type: none"> - Identity Management - Threat Protection - Storage Account - Database Security - Logging and Monitoring <ul style="list-style-type: none"> - Networking - Virtual Machines - Key Management - Application Security <ul style="list-style-type: none"> - App Services
OUTCOMES	<ul style="list-style-type: none"> ✓ Overview of existing configuration ✓ Configuration issues and risk pertaining to each identified risk ✓ Practical recommendation, including support for implementation

Microsoft 365 Configuration Review

REVIEW SCOPE	<ul style="list-style-type: none"> - Access Control - Change Management - Application Permissions <ul style="list-style-type: none"> - Data Protection - Email Security - Auditing and Log Monitoring <ul style="list-style-type: none"> - Data Storage - Device Management
OUTCOMES	<ul style="list-style-type: none"> ✓ Microsoft 365 configuration issues and risk pertaining to each identified risk ✓ Practical recommendations, including detailed technical hardening steps to mitigate the risk

To learn more about SEQA's MSAP service offering, please contact us.

 seqa.co.nz

 0800 SEQA IT

 contact@seqa.co.nz