Multi-Tier Cloud Security (MTCS) Standard for Singapore

Microsoft received certification for the Multi-Tier Cloud Security Standard for Singapore.

Microsoft and MTCS

After rigorous assessments conducted by the MTCS Certification Body, Microsoft cloud services received MTCS 584:2013 certification across all three service classifications—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Microsoft was the first global cloud service provider (CSP) to receive this certification across all three classifications.

Certifications were granted at Level 3 for Microsoft Azure services (IaaS and PaaS), Microsoft Dynamics 365 services (SaaS), and Microsoft Office 365 services (SaaS). A Level 3 certification means that in-scope Microsoft cloud services can host high-impact data for regulated organizations with the strictest security requirements. It's required for certain cloud solution implementations by the Singapore government.

Microsoft in-scope cloud services

- Azure
  Learn more

- Dynamics 365
  Learn more

- Intune

- Office 365
  Learn more

Audits, reports, and certificates

Certification is valid for three years, with a yearly surveillance audit to be conducted.

Microsoft MTCS certification

- Azure
  Learn more

- Intune
  Learn more

- Dynamics 365
  Learn more

- Office 365
  Learn more

Microsoft MTCS cloud service provider disclosure

- Azure
  Learn more

- Intune
  Learn more

- Dynamics 365
  Learn more

- Office 365
  Learn more

How to implement

- **MTCS Implementation Guide**
  Cloud service providers certified to the MTCS standard can get assistance in adopting CSA STAR.
  Learn more

- **Azure compliance: Malaysia**
  Find out how Azure can help address Malaysian compliance, security, and privacy requirements.
  Learn more

Microsoft

About MTCS

The Multi-Tier Cloud Security (MTCS) Standard for Singapore was prepared under the direction of the Information Technology Standards Committee (ITSC) of the Infocomm Development Authority of Singapore (IDA). The ITSC promotes and facilitates national programs to standardize IT and communications, and Singapore's participation in international standardization activities.

The purpose of the MTCS is to provide:

- A common standard that CSPs can apply to address customer concerns about the security and confidentiality of data in the cloud, and the impact on businesses of using cloud services.
- Verifiable operational transparency and visibility into risks to the customer when they use cloud services.

The MTCS builds upon recognized international standards such as ISO/IEC 27001, and covers such areas as data retention, data sovereignty, data portability, liability, availability, business continuity, disaster recovery, and incident management. It also includes a mechanism for customers to benchmark and rank the capabilities of CSPs against a set of minimum baseline security requirements.

MTCS is the first cloud security standard with different levels of security, so certified CSPs can specify which levels they offer. MTCS includes a total of 535 controls, covering basic security in Level 1, more stringent governance and tenancy controls in Level 2, and reliability and resiliency for high-impact information systems in Level 3.

Frequently asked questions

To whom does the standard apply?

It applies to businesses in Singapore that purchase cloud services requiring compliance with the MTCS standard.

What are the differences between MTCS security levels?

MTCS has a total of 535 controls that cover three levels of security:

- Level 1 is designed to be low-cost, with a minimum number of required baseline security controls. It is suitable for web site hosting, test and development work, simulation, and noncritical business applications.
- Level 2 addresses the needs of most organizations that are concerned about data security, with a set of more stringent controls targeted at security risks and threats to data. Level 2 is applicable for most cloud usage, including mission-critical business applications.
- Level 3 is designed for regulated organizations with specific requirements and those willing to pay for stricter security requirements. Level 3 adds a set of security controls to supplement those in Levels 1 and 2. They address security risks and threats in high-impact information systems using cloud services, such as hosting applications with sensitive information and in regulated systems.

Can I use Microsoft compliance in my organization's certification process?

Yes. If you have a requirement to certify your services built on these Microsoft cloud services, you can use the MTCS certification to reduce the impact of auditing your IT infrastructure, to the extent that it relies on them. However, you are responsible for engaging an assessor to evaluate your implementation for compliance, and for the controls and processes within your own organization.

Additional resources

- Microsoft Online Services Terms

Microsoft