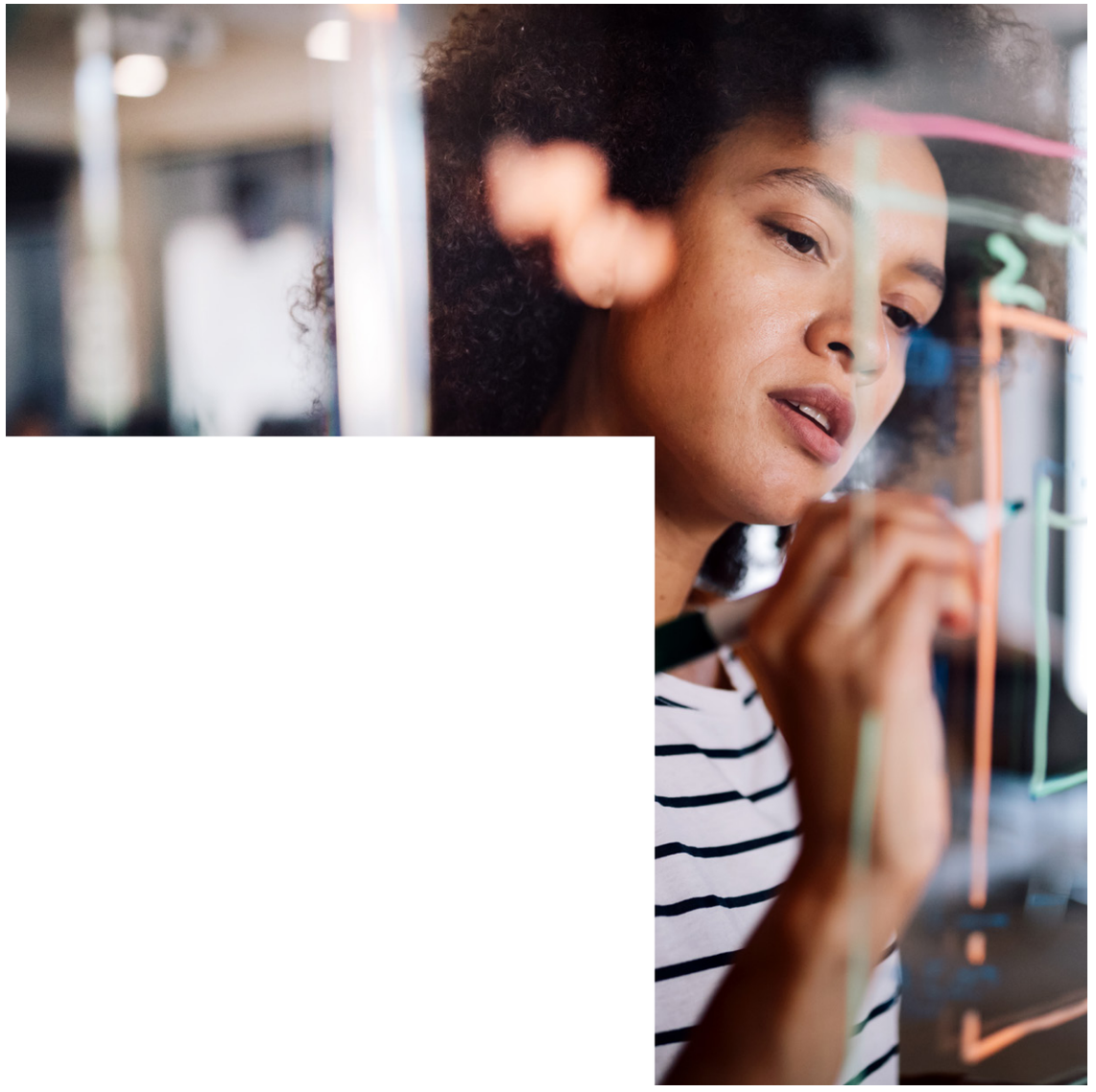
Home

# Microsoft Azure Security Architecture Assessment – 3 Weeks

EXPLORE →



CGI

# Getting your Azure transformation off on the right foot…

CGI is recognized as a Leader in the IDC MarketScape Canadian Security Services 2022 Vendor Assessment .“CGI maintains one of the biggest security teams in Canada, and one out of CGI’s nine SOCs (security operation centres) worldwide is in Canada,” writes Yogesh Shivhare, research manager at IDC Canada. “The company leverages its national and global security capabilities to offer a one-stop shop for end-to-end solutions to support customers’ ecosystems across the value chain. CGI can bring together multidisciplinary teams to deliver complex digital transformation projects for clients with integrated security.”

Backed by over 25 years of quality service delivery, CGI helps companies in the government, healthcare, manufacturing, financial, utilities, and retail sectors transform their IT operations to the Azure Cloud.

Migrating IT functions to Azure makes sense for different reasons. Among other advantages, Azure brings powerful capabilities to the table, including a comprehensive range of powerful Azure-native security tools, such as Defender, to establish a trusted environment with balanced and managed security for your critical assets. At CGI, we can help you ensure that you have implemented those tools correctly and have the capacity to maximize their value and protect your business.

**300+**

Cyber experts Canada-wide

**1,800**

Cyber experts globally

**25 years**

Of experience providing cyber services

**9**

Security operations centers worldwide

# About Azure Security Architecture Assessments

CGI provides Microsoft Azure Security Architecture Assessments leveraging **Microsoft Defender for Cloud** as a **Cloud Security Posture Management (CSPM)** and **Cloud Workload Protection Platform (CWPP)** tools. These posture management features provide hardening guidance to improve security and visibility into your current security situation.

## Defender for Cloud

- **Defender for Cloud** offers security alerts that are powered by **Microsoft Threat Intelligence**. It also includes a range of advanced, intelligent, protections for your workloads. The workload protections are provided through **Microsoft Defender** plans specific to the types of resources in your subscriptions.
- **Defender for Cloud** is used to detect threats across Azure PaaS services including **Azure App Service, Azure SQL, Azure Storage Account**, and data services.
- **Defender for Cloud** includes capabilities that help automatically classify data in Azure SQL, including assessments for potential vulnerabilities across Azure SQL and Storage services, and recommendations for how to mitigate them. The list of recommendations is enabled and supported by the **Azure Security Benchmark**. This Microsoft-authored, Azure-specific, benchmark provides a set of guidelines for security and compliance best practices based on common compliance frameworks.
- **Defender for Cloud** groups the recommendations into security controls and adds a secure score value to each control.

# Azure Security Benchmarks

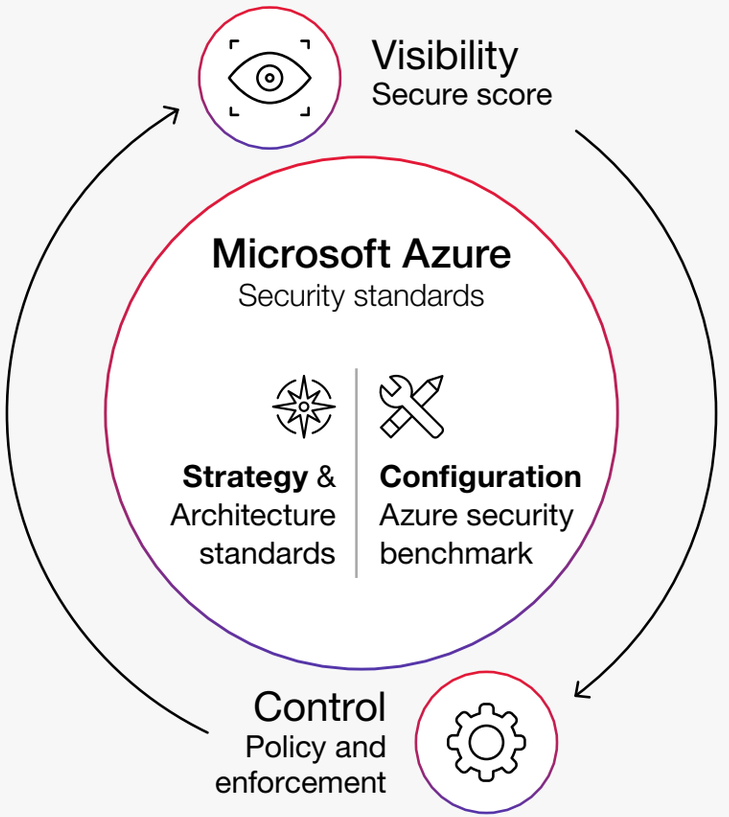
**Azure Security Benchmarks** and service baselines are used to define your configuration baseline for each respective Azure offering or service. The **Azure Security Benchmark** focuses on cloud-centric control areas. These controls are consistent with well-known security benchmarks, such as those described by the Center for Internet Security (CIS) Controls, National Institute of Standards and Technology (NIST), and Payment Card Industry Data Security Standard (PCI-DSS), and other regulatory frameworks as appropriate for the client's business requirements.

**The Azure Security Benchmark (ASB)** provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. This benchmark is part of a set of holistic security guidance that also includes:

- **Azure Cloud Adoption Framework**: Guidance on security, including strategy, roles and responsibilities, Azure Top 10 Security Best Practices, and reference implementation.
- **Azure Well-Architected Framework**: Guidance on securing your workloads on Azure.
- **Microsoft Security Best Practices**: Recommendations with examples on Azure.
- **Microsoft Cybersecurity Reference Architectures (MCRA)**: Visual diagrams and guidance for security components and relationships

**Azure Security Benchmarks provide guidelines for the following Control Domains:**

# Identifying your security gaps
## and actions to achieve compliance




CGI will generate a secure score for your subscriptions based on an assessment of your connected resources compared with the guidance in **Azure Security Benchmark** and use the score to understand your security posture, and the compliance dashboard to review your compliance with the built-in benchmark.

When you've enabled the enhanced security features, you can customize the standards used to assess your compliance, and add other regulations (such as NIST and Azure CIS) or organization-specific security requirements.

CGI leverages the **Azure Reference Architecture** and **Cloud Adoption Framework Landing Zone Architecture** for critical security controls and configurations across Azure resources.

# What can you expect?

CGI will use industry consulting best practices and its quality framework to identify existing gaps and resulting risks, and provide recommendations on:

- Additional measures that should be undertaken to reduce residual risk;
- Implications for security governance and regulatory requirements;
- How you can better leverage and optimize Azure cloud-native tools and services for risk management, security monitoring and incident response.

Due to the broad range of needs, scale and complexity, we work with clients to understand their requirements and provide a firm quote for scope, effort/duration and cost that will ensure their business needs are met.

Contact us for a quote…

canadacybersecurity@cgi.com

# About CGI

## Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.


# About CGI's cybersecurity services

For more than 25 years, CGI has been helping organizations across the globe achieve the most appropriate and effective levels of protection for their changing business. Through our team of 1,800 cybersecurity professionals, nine security operations centers, and two certification and test labs, CGI provides a diversity of services including strategic and technical cybersecurity consulting, engineering and architecture, advanced Managed Security Services and Incident Response. With CGI, public and private sector organizations gain a powerful and dynamic cyber force multiplier.

**cgi.com/canada**