



# Independent Service Auditor's Report

Microsoft Corporation Global  
Foundation Services

# Independent Service Auditor's Report

**Deloitte & Touche LLP**  
Suite 3300  
925 Fourth Avenue,  
Seattle, WA 98104-1126  
USA  
Tel: +1 206 716 7000  
www.deloitte.com

## To: Microsoft Corporation Global Foundation Services

We have examined the effectiveness of Microsoft Corporation (Microsoft) Global Foundation Services (GFS) controls over the security and availability of the GFS Information Technology Infrastructure and Services during the period October 1, 2012 through March 31, 2013, based on the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) trust services security and availability criteria. GFS' management is responsible for maintaining the effectiveness of these controls. Our responsibility is to express an opinion based on our examination.

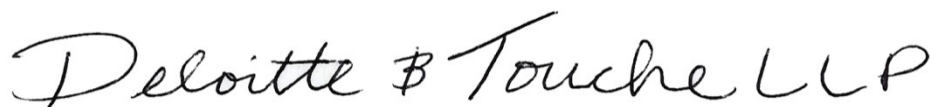
Management's description of the aspects of the GFS Information Technology Infrastructure covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with Attestation Standards established by the AICPA and, accordingly, included (1) obtaining an understanding of the controls related to the security and availability of the GFS Information Technology Infrastructure and Services, (2) testing and evaluating the operating effectiveness of the GFS' controls, and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, GFS' ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, and failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, GFS maintained, in all material respects, effective controls over the security and availability of the GFS Information Technology Infrastructure to provide reasonable assurance that the GFS Information Technology Infrastructure was protected against unauthorized access (both physical and logical) and was available for operation and use as committed or agreed during the period October 1, 2012 through March 31, 2013, based on the AICPA and CICA trust services security and availability criteria.

The SOC 3 SysTrust for Service Organizations Seal on the Microsoft GFS web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide additional assurance.



May 28, 2013  
Seattle, WA

# Management Assertion – GFS

## Assertion by Management of Microsoft GFS

### Management Assertion Regarding the Effectiveness of its Controls

Microsoft GFS maintained effective controls over the security and availability of the GFS Information Technology (“IT”) Infrastructure and Services, as defined by the following Systems/Services Description, to provide reasonable assurance that:

- The systems were protected against unauthorized access (both physical and logical) and were available for operation and use as committed or agreed, during the period October 1, 2012 through March 31, 2013, based on the AICPA and CICA trust services security and availability criteria, which are available at [www.webtrust.org](http://www.webtrust.org).

The AICPA and CICA contain the following definition of security and availability of the systems:

- Security – The System was protected against unauthorized access (both physical and logical).
- Availability – The System is available for operation and use as committed or agreed.

The following Systems/Services Description of the Microsoft GFS environment identifies the aspects of the IT infrastructure and services covered by this assertion.

**Microsoft GFS**

May 28, 2013

# Description of Microsoft GFS System

## Overview of Operations

GFS is an organization within Microsoft that provides hosting and operational support solutions for the Microsoft online and cloud services environment. GFS operates an Information Technology (IT) infrastructure that supports more than 200 Microsoft online and cloud services (e.g., Office 365, Dynamics CRM Online, and Windows Azure, etc.) which are offered around the world. GFS' infrastructure is distributed over multiple data centers on three continents (North America, Europe, and Asia). GFS' operational infrastructure services include:

- Deployment, hosting, and data center services.
- Engineering and operations for core infrastructure, such as networking, directory services, access services, data retention and backup, hardware, and software procurement.
- Service support, monitoring, and escalation.
- Information security management and compliance monitoring.

The components of the GFS environment are categorized as follows:

- People (organizational structure, groups and teams)
- Infrastructure (facilities, equipment, and networks)
- Software (systems, services, applications and tools)
- Procedures (policies, standards and processes)

## People

Various GFS teams provide the delivery and management of the operational infrastructure. These include:

### **Data Center Services**

The Data Center Services team focuses on designing, constructing, and operating the data center assets.

### **Microsoft Operations Center**

The Microsoft Operations Center is a 24x7x365 Tier 1 operations center located across multiple locations. This team is responsible for providing the first line of operational and service support to the Microsoft online and cloud services supporting incident, change, and problem management.

### **Global Networking Services**

The Global Networking Services team is responsible for deployment, operation, and administration of the network devices that reside in the GFS managed data centers.

### **Online Services Security and Compliance**

The Online Services Security and Compliance (OSSC) team operates a comprehensive security program and control framework that is evaluated regularly by external parties. OSSC is also responsible for developing, maintaining and monitoring compliance with the information security policies and standards in the Microsoft GFS environment. In addition, OSSC manages the physical security of the data centers through established procedures in security and operations.

## **Shared Services**

The Shared Services team provides core infrastructure technologies and services, such as Active Directory, backup, remote access, to Microsoft online and cloud services.

## **Infrastructure**

GFS applications, data, and infrastructure are hosted in data centers located in geographically distributed sites across the world. These purpose-built facilities are part of a network of data centers that provide mission critical services to both Microsoft and the company's global customer base. GFS infrastructure resides in locations that include Amsterdam; Dublin; Hong Kong; Japan; Singapore; Chicago, Illinois; San Antonio, Texas; and Quincy, Washington.

Main access to the data center facilities is restricted to single points of entry that are staffed by security personnel. Entrances have electronic card access control devices on the perimeter door(s), which restrict access to the interior facilities. Rooms within the data centers that contain critical systems (servers, generators, electrical panels, network equipment, etc.) are restricted through various security mechanisms, such as electronic card access control devices, keyed locks on individual doors, interlocking door controllers (i.e., man traps), and biometric devices.

Data center surveillance systems monitor areas such as main entrances, colocation entrances, cages, locked cabinets, aisle ways, shipping and receiving areas, critical environments, perimeter doors, and parking areas.

GFS also operates a tiered global network architecture that provides network segregation and access controls to various Microsoft online and cloud services.

## **Software**

Systems, services, applications and tools utilized by GFS to support the Microsoft online and cloud services environment include:

- Data center automation and tooling
- Imaging servers
- Business continuity applications
- Security monitoring, scanning and support systems
- Core infrastructure monitoring tools and supporting systems
- Work ticketing and management services
- Service operation center systems
- Identity management and directory services
- Data backup services
- Remote access systems and services
- Definitive software libraries
- Replication services
- Storage area network devices
- Simple Mail Transfer Protocol (SMTP) systems
- Networking infrastructure and tools
- Antivirus services
- Vulnerability management services
- Security incident management systems
- Enterprise tooling and support

## **Procedures**

### **Information Security Program**

GFS has established an Information Security Program (ISP) that provides documented management direction and support for consistent implementation of information security for the GFS environment. The ISP has adopted an information security strategy to protect the confidentiality, integrity, and availability of the GFS and Microsoft online and cloud services assets. It provides a framework to assess risks to the environment, to develop mitigating strategies, and to monitor existing policies and effectiveness of safeguards. The ISP consists of the following components:

- Policy and Standards
- Risk Assessment
- Training and Education
- ISP Implementation
- Review and Compliance
- Evaluation and Adjustment
- Management Reporting

### **Microsoft Security Policy**

GFS has implemented the Microsoft Security Policy as a component of the ISP. The Security Policy contains rules and requirements that are met by GFS and online and cloud services staff in the delivery and operations of the Microsoft online and cloud services environment. The Security Policy is derived from the ISO/IEC 27001:2005 standard and is augmented to address relevant regulatory and industry requirements for the Microsoft online and cloud services environment.

In addition, GFS has established the following Standards that serve as adjuncts to the Security Policy:

- Acceptable Use
- Asset Classification and Protection
- Employment and Training
- Physical and Environmental Security
- Change Management
- Network Security
- Host Security
- Identity Management
- Key Management
- Security Incident Management
- Business Continuity Management

### **Data**

This report is limited to the controls in operation to support the operational infrastructure services as defined in the GFS Scope Boundary. The Scope Boundary includes specific production systems residing in the GFS data centers which provide the GFS services mentioned above under the 'Software' section.

Application data that resides within the infrastructure is the responsibility of individual Microsoft online and cloud services. GFS is not responsible for this data other than our obligations of security and availability with respect to data center infrastructure.

### **Applicability of Report**

This report has been prepared to provide information on GFS' internal controls that may be relevant to the requirements of its customers to meet the security and availability trust principles. This report has been prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each customer may consider important. This report is limited to the controls in operation to support the operational infrastructure services as defined in the GFS Scope Boundary. The authorized users of the system providing these infrastructure services are limited to GFS personnel. This report may not address controls over all services or procedures provided to other internal Microsoft online and cloud services. For example, with the exception of controls regarding physical security this report does not address internal controls over Microsoft online and cloud services such as Office 365, CRM, Intune or Azure. Where available, Microsoft online and cloud services should refer to their respective Service Organization Control (SOC) reports of these services for the design and effectiveness of their internal controls.