

David J. Aubrey, CIA, CFE  
Inspector General  
**Office of the Inspector General**

## OIG Memorandum

**TO:** K. A. LaMarca, Director, Information Services  
**FROM:** D. J. Aubrey, Inspector General  
**SUBJECT:** Review of Service Organization Controls (SOC) Reports for Microsoft Office 365  
(October 2019 – June 2021)  
**DATE:** August 25, 2021

---

The Office of the Inspector General (OIG) has reviewed the most current and available Service Organization Controls reports for the Microsoft Office 365 Service Provider (see attachments; the attached reports are noted for “Restricted Use” and should be treated accordingly). This review was performed by R. McReynolds, IT Auditor, with reports provided by Kevin LaMarca, Director, Information Services. The objective of this review is to provide reasonable assurance that the service provider for the Microsoft Office 365 systems has controls in place to mitigate risk regarding security, availability, processing integrity, confidentiality, privacy, and that the controls have been tested and any material issues remediated. Microsoft is the contracted service provider for email, Office, Sharepoint, OneDrive, MSTeams and Skype applications for the Authority’s cloud-based back office systems. To accomplish this review OIG has reviewed the following audit reports:

- SOC 2 Report (SOC2) Office 365 Central;
- SOC 1 Type 2 Report (SOC1) and Statement on Standards for Attestations Engagements (SSAE) 18 Report for Office 365 Microservices T1;
- SOC 2 Type 1 Report (SOC2) and Statement on Standards for Attestations Engagements (SSAE) 18 Report for Office 365 Microservices T1;
- SOC 2 Type 2 Report (SOC2) and Statement on Standards for Attestations Engagements (SSAE) 18 Report for Office 365 Microservices T2; and,
- Microsoft Bridge Letter.

The scope of the reports provided and reviewed were valid from October 1, 2019 through September 30, 2020, with the bridge letter for October 1, 2020 through June 30, 2021.

These independent audit reports are control attestations supplied by the third-party service provider to provide assurance to their clients (in this case, the Authority) that the contracted services and facilities have an adequate control environment in place to protect our data. The reports also document the testing and results of the controls by the independent attesting organization.

Microsoft's (the cloud application provider) policies and procedures were evaluated for system access and operations controls. Microsoft locations were reviewed for adherence to policy and procedures for logical access to systems, physical security, network security, environmental protection, power backup, fire alert and suppression capabilities, application hosting, disaster recovery and data backup.

For the period October 1, 2019 through September 30, 2020, the independent attesting organization, Deloitte (Seattle, WA), reported no exceptions based on their testing of the controls for Microsoft within their SOC 2 and SOC 1 reports, both dated January 20, 2021.

The bridge letter from Microsoft states that the controls have not changed from October 1, 2020 through June 30, 2021.

Based on review of the reported results from the independent attesting organization, OIG concurs with the conclusion that an appropriate control environment exists at Microsoft. No further actions are required.

OIG has shared the results of this review with IS management and will continue to work with IS management in review of third-party provider IT controls as the annual SOC audits are conducted and reports made available.

Attachments (restricted use)

*(Note: The noted attachments have not been included due to their proprietary and confidential nature.)*

cc: C. Parker  
J. Nash  
T. DeFoor  
H. Rigo  
C. Pike-Nase  
A. Nelson  
J. Hanson  
R. Santarelli  
M. Wing  
R. McReynolds