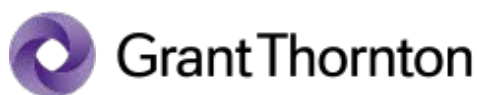




# comScore, Inc.

Online Market Research Service

System and Organization Controls (SOC) for Service Organizations Report for the period of June 1, 2017 to May 31, 2018



Report of Independent Service Auditors issued by  
Grant Thornton LLP



# Contents

<b>I.</b>	<b>Report of Independent Service Auditors.....</b>	<b>1</b>
<b>II.</b>	<b>comScore, Inc.’s Assertion.....</b>	<b>4</b>
<b>III.</b>	<b>comScore, Inc.’s Description of its System.....</b>	<b>6</b>
	A. Scope and Purpose of the Report.....	6
	B. Overview of Services Provided.....	6
	C. Service Commitments and System Requirements.....	7

# I. Report of Independent Service Auditors

Board of Directors and Stakeholders  
comScore, Inc.:

## Scope

We have examined comScore, Inc.'s (the "Company" or "comScore") accompanying assertion titled *comScore, Inc.'s Assertion* (the "assertion") that the controls within comScore's Online Market Research Service, which includes the following brands: MobileXpression, Digital Reflection, OpinionSquare, RelevantKnowledge, PermissionResearch, ScorecardResearch, VoiceFive, and PremierOpinion (the "System") were effective throughout the period June 1, 2017 to May 31, 2018 (the "Specified Period"), to provide reasonable assurance that the criteria for the security and privacy principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* ("applicable trust services criteria") were met, if complementary subservice organizations and user entity controls assumed in the design of comScore's controls operated effectively throughout the period June 1, 2017 to May 31, 2018, and comScore complied with the commitments in its privacy statements throughout the period June 1, 2017 to May 31, 2018. Our examination does not provide a legal determination on the Company's compliance with laws and regulations related to privacy practices or its compliance with the commitments in its privacy statements throughout the Specified Period.

The Company uses four third-party subservice organizations, QTS Realty Trust, Inc., Cyxtera Technologies, Inc., CenturyLink, Inc., and Anexia, Inc. as its third-party hosting providers for servers and equipment related to the Online Market Research Service and one third-party subservice organization, LightSpeed Research, for managing the registration process, including logical access to the system and managing the change management and installation process specific to the Digital Reflection brand of its Online Market Research Service. Management's assertion indicates that certain applicable trust services criteria specified by the Company in Section III, *comScore, Inc.'s Description of its System*, under the section *Subservice Organizations*, can be met only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. Our examination did not extend to the controls of these subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organizations controls.

Management's assertion indicates that certain applicable trust services criteria specified in Section III, *comScore, Inc.'s Description of its System*, under the section *User Entity Controls*, can be met only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

#### **Service Organization's Responsibilities**

comScore is responsible for the System and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the applicable trust service criteria were met. comScore is also responsible for preparing its privacy statements and complying with the commitments in its privacy statements. comScore has also provided the accompanying assertion about the effectiveness of controls within the system and compliance with its the commitments in its privacy statements. When preparing its assertion, comScore is responsible for selecting, and identifying in its assertion, the Applicable Trust service Criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

#### **Service Auditor's Responsibilities**

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the applicable trust services criteria were met, if complementary subservice organizations and user entity controls assumed in the design of comScore's controls operated effectively throughout the period June 1, 2017 to May 31, 2018, and comScore complied with the commitments in its privacy statements throughout the period June 1, 2017 to May 31, 2018. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the System;
- Assessing the risks that controls were not effective to meet the applicable trust services criteria, and the Company did not comply with the commitments in its privacy statements; and
- Performing procedures to obtain evidence about whether controls within the system were effective to meet the applicable trust services criteria, and the Company complied with the commitments in its privacy statements.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

**comScore, Inc.**  
**SOC 3® Report – SOC for Service Organizations: Trust Services Criteria for General Use**  
**Online Market Research Service**

---

**Inherent Limitations**

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the applicable trust services criteria were met or the Company complied with the commitments in its privacy statements. Also, the projection to the future of any conclusions about the effectiveness of controls or conclusions about compliance with the commitments in the privacy statements is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

**Opinion**

In our opinion, management's assertion that the controls within comScore's System were effective throughout the period June 1, 2017 to May 31, 2018, to provide reasonable assurance that the applicable trust services criteria were met, if complementary subservice organizations and user entity controls assumed in the design of comScore's controls operated effectively throughout the period June 1, 2017 to May 31, 2018, and comScore complied with the commitments in its privacy statements throughout the period June 1, 2017 to May 31, 2018, is fairly stated, in all material respects.

*Grant Thornton LLP*

Atlanta, Georgia  
July 13, 2018



## II. comScore, Inc.’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within comScore, Inc.’s (the “Company” or “comScore”) Online Market Research Service, which includes the following brands: MobileXpression, Digital Reflection, OpinionSquare, RelevantKnowledge, PermissionResearch, ScorecardResearch, VoiceFive, and PremierOpinion (the “System”) throughout the period June 1, 2017 to May 31, 2018, to provide reasonable assurance that the criteria for the security and privacy principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (“applicable trust services criteria”) were met. We are also responsible for preparing comScore’s privacy statements and complying with the commitments in our privacy statements. Our description of the boundaries of the system is presented in Section III, *comScore, Inc.’s Description of its System*, and identifies the aspects of the System covered by our assertion.

The Company uses four third-party subservice organizations, QTS Realty Trust, Inc., Cyxtera Technologies, Inc., CenturyLink, Inc., and Anexia, Inc. as its third-party hosting providers for servers and equipment related to the Online Market Research Service and one third-party subservice organization, LightSpeed Research, for managing the registration process, including logical access to the system and managing the change management and installation process specific to the Digital Reflection brand of its Online Market Research Service. Certain applicable trust services criteria, specified in Section III, *comScore, Inc.’s Description of its System*, under the section *Subservice Organizations* can be met only if complementary subservice organization controls contemplated in the design of the Company’s controls are suitably designed and operating effectively, along with related controls at the Company.

Certain applicable trust services criteria, specified in Section III, *comScore, Inc.’s Description of its System*, under the section *User Entity Controls* can be met only if complementary user entity controls contemplated in the design of the Company’s controls are suitably designed and operating effectively, along with related controls at the Company.

**comScore, Inc.**

**SOC 3® Report – SOC for Service Organizations: Trust Services Criteria for General Use  
Online Market Research Service**

---

We have performed an evaluation of the effectiveness of the controls within the System throughout the period June 1, 2017 to May 31, 2018, to provide reasonable assurance that the criteria for the security and privacy principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* were met and the Company complied with the commitments in its privacy statements throughout the period June 1, 2017 to May 31, 2018. Our description of the boundaries of the system is presented in Section III, *comScore, Inc.'s Description of its System*, and identifies the aspects of the system covered by our assertion. comScore's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are also presented in Section III *comScore, Inc.'s Description of its System*.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that the applicable trust services criteria are met and compliance with the commitments in the privacy statements.

We assert that the controls within the System were effective throughout the period June 1, 2017 to May 31, 2018, to provide reasonable assurance that the applicable trust services criteria were met, if complementary subservice organizations and user entity controls assumed in the design of comScore's controls operated effectively throughout the period June 1, 2017 to May 31, 2018, and the Company complied with the commitments in its privacy statements throughout the period June 1, 2017 to May 31, 2018.

### III. comScore, Inc.’s Description of its System

#### A. Scope and Purpose of the Report

This report describes the control structure of comScore, Inc. (the “Company” or “comScore”) as it relates to its Online Market Research Service, which includes the following brands: MobileXpression, Digital Reflection, OpinionSquare, RelevantKnowledge, PermissionResearch, ScorecardResearch, VoiceFive, and PremierOpinion (the “System”) and only includes those control activities and related criteria surrounding those operations for the period of June 1, 2017 through May 31, 2018 (the “Specified Period”) for the Security and Privacy principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Principles and Criteria*) (“Applicable Trust Services Criteria”).

It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

#### B. Overview of Services Provided

comScore, Inc. (NASDAQ: SCOR) is a cross-platform measurement company that measures audiences, brands, and consumer behavior in the digital world. comScore’s Online Market Research Service measures what people do as they navigate the digital world – and turns that information into insights and actions for clients to maximize the value of their digital investments. comScore maintains a group of panelists who have monitoring software and/or cookies (brands including MobileXpression, Digital Reflection, OpinionSquare, RelevantKnowledge, PermissionResearch, ScorecardResearch, VoiceFive and PremierOpinion) on their computers or mobile devices. In exchange for joining the comScore research panels, users are presented with various benefits, including computer security software, Internet data storage, virus scanning, and chances to win cash or prizes. comScore was founded in 1999 by Magid Abraham and CEO Gian Fulgoni and became a public company in June, 2007. Headquartered in Reston, Virginia and armed with more than 80 locations in 30 countries, comScore serves over 3,200 clients worldwide.



Client Web Sites
<input type="checkbox"/> <a href="#">PermissionResearch Privacy Statement</a>
<input type="checkbox"/> <a href="#">RelevantKnowledge Privacy Statement</a>
<input type="checkbox"/> <a href="#">OpinionSquare Privacy Statement</a>
<input type="checkbox"/> <a href="#">ScorecardResearch Privacy Statement</a>
<input type="checkbox"/> <a href="#">PremierOpinion Privacy Statement</a>
<input type="checkbox"/> <a href="#">VoiceFive Privacy Statement</a>
<input type="checkbox"/> <a href="#">MobileXpression Privacy Statement</a>
<input type="checkbox"/> <a href="#">Digital Reflection Privacy Statement</a>

### C. Service Commitments and System Requirements

#### Overview

comScore designs its processes and procedures related to the Online Market Research Service to meet its objectives for its business. Those objectives are based on the service commitments that comScore makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that comScore has established for the services. The Online Market Research Service is subject to the security and privacy requirements of EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Frameworks, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which comScore operates.

Security commitments and privacy to user entities are documented and communicated in our privacy policies and other customer agreements, as well as in the description of the service offering provided online. Security and privacy commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Online Market Research Service are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role;
- Use of reasonable precautions to protect the security of the information that we collect;
- Make commercially reasonable efforts to automatically filter certain personal information collected from our Panelists such as password and account numbers; however, we may inadvertently collect information about our panelists; and
- Make commercially reasonable efforts to destroy or encrypt any information that is not filtered automatically.

**comScore, Inc.**

**SOC 3® Report – SOC for Service Organizations: Trust Services Criteria for General Use  
Online Market Research Service**

---

comScore establishes operational requirements that support the achievement of security and privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in comScore’s system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected.

These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Online Market Research Service.

Subservice Organizations

The Company utilizes subservice organizations to perform certain functions to improve operating and administrative effectiveness. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party service organizations described below. The examination by the independent Service Auditor did not extend to the policies and procedures at these subservice organizations. The most significant subservicing organizations used by the Company are noted below.

<b>Subservice Organization</b>	<b>Services provided</b>	<b>Associated Criteria</b>
Lightspeed Research	The Company uses Lightspeed Research for the management and hosting of the registration/new panelist recruitment process for Digital Reflection. The following control areas are critical to achieving the Applicable Trust Services Criteria: <ul style="list-style-type: none"><li>• Controls around the logical access of internal and external users to the Digital Reflection system.</li><li>• Controls around change management regarding registration for Digital Reflection.</li></ul>	CC5.1*, CC5.2*, CC5.3*, CC5.4*, CC5.5*, CC5.6*, CC5.7*, CC5.8*

Subservice Organization	Services provided	Associated Criteria
	<p>In addition, the Company has identified the following controls to help monitor the subservice organization:</p> <ul style="list-style-type: none"> <li>On an annual basis, management evaluates the third parties who have access to confidential data or perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on the risk rating, management either performs a vendor security assessment of the third party, reviews the third party’s System and Organization Control reports such as SOC 2 Type II reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary.</li> </ul>	
Anexia, Inc.	<p>The Company uses Anexia for the hosting of servers and equipment related to the Online Market Research Service, including the restriction of physical access to the defined system including, but not limited to, facilities and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Applicable Trust Services Criteria:</p> <ul style="list-style-type: none"> <li>Controls around the physical security of the Data Centers hosting the in-scope applications.</li> </ul> <p>In addition, the Company has identified the following controls to help monitor the subservice organization:</p> <ul style="list-style-type: none"> <li>On an annual basis, management reviews employee access to the third-party Data Center.</li> <li>On an annual basis, management evaluates the SOC report related to the third-party organization to help ensure compliance with commitments and agreed-upon service level agreements.</li> </ul>	CC5.5*

Subservice Organization	Services provided	Associated Criteria
CenturyLink, Inc.	<p>The Company uses CenturyLink for the hosting of servers and equipment related to the Online Market Research Service, including the restriction of physical access to the defined system including, but not limited to, facilities and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Applicable Trust Services Criteria:</p> <ul style="list-style-type: none"> <li>• Controls around the physical security of the Data Centers hosting the in-scope applications.</li> </ul> <p>In addition, the Company has identified the following controls to help monitor the subservice organization:</p> <ul style="list-style-type: none"> <li>• On an annual basis, management reviews employee access to the third-party Data Center.</li> <li>• On an annual basis, management evaluates the SOC report related to the third-party organization to help ensure compliance with commitments and agreed-upon service level agreements.</li> </ul>	CC5.5*
QTS Realty Trust, Inc.	<p>The Company uses QTS for the hosting of servers and equipment related to the Online Market Research Service, including the restriction of physical access to the defined system including, but not limited to, facilities and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Applicable Trust Services Criteria:</p> <ul style="list-style-type: none"> <li>• Controls around the physical security of the Data Centers hosting the in-scope applications.</li> </ul>	CC5.5*

Subservice Organization	Services provided	Associated Criteria
	<p>In addition, the Company has identified the following controls to help monitor the subservice organization:</p> <ul style="list-style-type: none"> <li>• On an annual basis, management reviews employee access to the third-party Data Center.</li> <li>• On an annual basis, management evaluates the SOC report related to the third-party organization to help ensure compliance with commitments and agreed-upon service level agreements.</li> </ul>	
<p>Cyxtera Technologies, Inc.</p>	<p>The Company uses Cyxtera for the hosting of servers and equipment related to the Online Market Research Service, including the restriction of physical access to the defined system including, but not limited to, facilities and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Applicable Trust Services Criteria:</p> <ul style="list-style-type: none"> <li>• Controls around the physical security of the Data Centers hosting the in-scope applications.</li> </ul> <p>In addition, the Company has identified the following controls to help monitor the subservice organization:</p> <ul style="list-style-type: none"> <li>• On an annual basis, management reviews employee access to the third-party Data Center.</li> <li>• On an annual basis, management evaluates the SOC report related to the third-party organization to help ensure compliance with commitments and agreed-upon service level agreements.</li> </ul>	<p>CC5.5*</p>

\* The achievement of design and operating effectiveness related to this particular Trust Services Criterion assumes that complementary controls at this subservice organization that support this criterion are in place and are operating effectively.

User Entity Controls

The processes of the Company were designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve the Applicable Trust Services Criteria included in this report.

This section highlights those internal control responsibilities that the Company believes should be present for each user organization and has considered in developing its control policies and procedures described in this report. In order for users to rely on the control structure's policies and procedures reported on herein, each user must evaluate its own internal control structure to determine if the following procedures are in place. Furthermore, the following list of control policies and procedures is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user. Accordingly, this list does not allege to be, and is not, a complete listing of the control policies and procedures that provide a basis for management's assertions related to the Applicable Trust Services Criteria.

User Entity Control	Associated Criteria
Individuals are responsible for submitting complaints to the Company and for following up to help ensure that those complaints are addressed appropriately.	CC6.1*, CC6.2*, P6.3*, P6.6*, P6.7*, P8.1*
Individuals are responsible for providing explicit consent when the Company informs them that their personal information is now being used for a new purpose not previously identified.	P1.1*, P2.1*, P3.2*, P6.1*
Individuals are responsible for giving the Company explicit consent at or before the time that personal information is collected.	P2.1*, P3.2*, P6.1*
Individuals are responsible for giving the Company permission to transfer personal information to or from an individual's computer or other similar device.	P2.1*, P3.2*, P6.1*
Individuals are responsible for informing the Company if they wish to access their personal information which is maintained by the Company.	P2.1*, P3.2*, P5.1*, P5.2*, P6.2*, P6.8*
Individuals are responsible for following up with the Company if their requests are not responded to timely.	P5.1*, P5.2*
Individuals are responsible for challenging denials of access to their personal information, as specifically permitted or required by law or regulation.	P5.1*, P5.2*
Individuals are responsible for updating and/or correcting their personal information.	P5.2*, P7.1*

comScore, Inc.

**SOC 3® Report – SOC for Service Organizations: Trust Services Criteria for General Use  
Online Market Research Service**

---

User Entity Control	Associated Criteria
Individuals are responsible for appealing denials of requests for correction of personal information if so desired.	P5.2*

\* This is a complementary control and is required to achieve design and operating effectiveness for this particular criterion.



© Grant Thornton LLP  
All rights reserved.  
U.S. member firm of Grant Thornton International Ltd.

This report is confidential. Unauthorized use of this report in whole or in part is strictly prohibited.