



comscore

COMSCORE, INC.

Online Market Research Service

System and Organizational Controls (SOC) for Service Organizations Report
for the period of June 1, 2018 to May 31, 2019



Grant Thornton

Report of Independent Service Auditors issued by
Grant Thornton LLP

Contents

I.	Report of Independent Service Auditors	1
II.	Comscore, Inc.'s Assertion	4
III.	Comscore, Inc.'s Description of the Boundaries of its System.....	5
	A. Scope and Purpose of the Report	5
	B. Overview of Services Provided.....	5
	C. Principal Service Commitments and System Requirements.....	6

GRANT THORNTON LLP

1100 Peachtree St. NE, Suite 1200
Atlanta, GA 30309

D +1 404 330 2000

F +1 404 330 2047

I. Report of Independent Service Auditors

Board of Directors and Management
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, www.opinionsquare.com, www.relevantknowledge.com, www.permissionresearch.com, www.scorecardresearch.com, www.voicefive.com, and www.premieropinion.com (the "System") were effective throughout the period June 1, 2018 to May 31, 2019 (the "specified period"), to provide reasonable assurance that Comscore's service commitments and system requirements were achieved based on the trust services criteria relevant to security and privacy (Applicable Trust Services Criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). 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 statement of privacy practices 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 its assertion and its description in Section III includes only the controls of the Company and excludes the controls of these subservice organizations. Management's assertion indicates that certain AICPA Applicable Trust Services Criteria specified by management in Section III, *Comscore, Inc.'s Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved 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 AICPA Applicable Trust Services Criteria specified in Section III, *Comscore, Inc.'s Description of the Boundaries of its System*, under the section *User Entity Controls*, can be achieved 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 its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Comscore's service commitments and system requirements were achieved. Comscore has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Comscore is responsible for selecting, and identifying in its assertion, the Applicable Trust Services 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 service organization's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria. 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 and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve Comscore's service commitments and system requirements based on the Applicable Trust Services Criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Comscore's service commitments and system requirements based the Applicable Trust Services Criteria.

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

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 service organization's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria. Also, the projection to the future of any conclusions about the effectiveness of controls 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, Inc.'s System were effective throughout the period June 1, 2018 to May 31, 2019, to provide reasonable assurance that Comscore's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria is fairly stated, in all material respects.

Grant Thornton LLP

Atlanta, Georgia
June 12, 2019



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, www.opinionsquare.com, www.relevantknowledge.com, www.permissionresearch.com, www.scorecardresearch.com, www.voicefive.com, and www.premieropinion.com (the "System") throughout the period June 1, 2018 to May 31, 2019 (the "specified period"), to provide reasonable assurance that Comscore's service commitments and system requirements relevant to security and privacy were achieved. Our description of the boundaries of the system is presented in *Comscore, Inc.'s Description of the Boundaries of its System* and identifies the aspects of the system covered by our assertion. We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2018 to May 31, 2019, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security and privacy (Applicable Trust Services Criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). 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 presented in *Comscore, Inc.'s Description of its System*.

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 AICPA Applicable Trust Services Criteria, specified in Section III, *Comscore, Inc.'s Description of the Boundaries of its System*, under the section *Subservice Organizations* can be achieved 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. Management's assertion and the related description of the boundaries of the system in Section III of this report includes only the controls of the Company and excludes the controls performed by these subservice organizations.

Certain AICPA Applicable Trust Services Criteria, specified in Section III, *Comscore, Inc.'s Description of the Boundaries of its System*, under the section *User Entity Controls* can be achieved 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. Management's assertion and the related description of the boundaries of its System in Section III of this report includes only the controls of the Company and excludes the controls performed by User Entities.

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 its service commitments and system requirements are achieved.

We assert that the controls within the System were effective throughout the period June 1, 2018 to May 31, 2019, to provide reasonable assurance that Comscore, Inc.'s service commitments and system requirements were achieved based on the Applicable Trust Services Criteria

III. Comscore, Inc.’s Description of the Boundaries 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”) for the period of June 1, 2018 to May 31, 2019 (the “specified period”) for the trust services criteria relevant to security and privacy (Applicable Trust Services Criteria) as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *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.

At the core of Comscore’s control environment is its statement of policies and procedures. Each Online Marketing Research Service brand publicly displays its privacy statement for all panelists to view. Links to the privacy statement for each brand in the Online Marketing Research Service are included within the table below.

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

C. Principal 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 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. The SOC 3 examination 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.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. Each user entity's internal control must be evaluated in conjunction with the Company's controls, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

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

Subservice Organization	Services Provided	Associated Criteria
Lightspeed Research	<p>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:</p> <ul style="list-style-type: none"> • Controls around the logical access of internal and external users to the Digital Reflection system. • Controls around the change management process regarding the registration portal for Digital Reflection. <p>In addition, the Company has identified the following controls to help monitor the subservice organization:</p> <ul style="list-style-type: none"> • 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. 	CC5.2*, CC6.1*, CC6.3*, CC6.6*, CC6.7, CC6.8*, and CC 8.1*
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"> • Controls around the physical security of the Data Centers hosting the in-scope applications. <p>In addition, the Company has identified the following controls to help monitor the subservice organization:</p> <ul style="list-style-type: none"> • On an annual basis, management reviews employee access to the third-party Data Center. • 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. 	CC6.4*
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"> • Controls around the physical security of the Data Centers hosting the in-scope applications. 	CC6.4*

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

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"> • On an annual basis, management reviews employee access to the third-party Data Center. • 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. 	
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"> • Controls around the physical security of the Data Centers hosting the in-scope applications. <p>In addition, the Company has identified the following controls to help monitor the subservice organization:</p> <ul style="list-style-type: none"> • On an annual basis, management reviews employee access to the third-party Data Center. • 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. 	CC6.4*
Cyxtera Technologies, Inc.	<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"> • Controls around the physical security of the Data Centers hosting the in-scope applications. <p>In addition, the Company has identified the following controls to help monitor the subservice organization:</p> <ul style="list-style-type: none"> • On an annual basis, management reviews employee access to the third-party Data Center. • 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. 	CC6.4*

* 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

Comscore’s controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company’s service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity’s internal control must be evaluated in conjunction with the Company’s controls, taking into account the related complementary user entity controls identified in the table below, where applicable. Complementary user entity controls and their associated criteria are included within the table below.

In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine if the identified complementary user entity controls have been implemented and are operating effectively.

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.	CC2.3*, P6.6*, 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*, P3.1*, P3.2*, P6.1*
Individuals are responsible for giving the Company explicit consent at or before the time that personal information is collected.	P1.1*, P2.1*, 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.	P1.1*, P2.1*, P6.1*
Individuals are responsible for informing the Company if they wish to access their personal information which is maintained by the Company.	CC5.2*, P1.1*, P5.1*, P5.2*, P6.2*, P6.7*, P6.8*, P7.1*
Individuals are responsible for following up with the Company if their requests are not responded to timely.	P5.1*, P5.2*, P6.7*, P7.1*
Individuals are responsible for challenging denials of access to their personal information, as specifically permitted or required by law or regulation.	P1.1*, P5.1*, P5.2*, P6.7*, P7.1*
Individuals are responsible for updating and/or correcting their personal information.	P1.1*, P5.2*, P6.7*, P7.1*
Individuals are responsible for appealing denials of requests for correction of personal information if so desired.	P1.1*, P5.2*, P6.7*, P7.1*

* 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.