



comscore

COMSCORE, INC.

Online Market Research Service

System and Organization Controls (SOC) for Service Organizations Report
for the period of June 1, 2019 to May 31, 2020



Report of Independent Service Auditors issued by
Grant Thornton LLP



Contents

I.	Report of Independent Service Auditors	1
II.	Assertion of Comscore, Inc.'s Management	3
III.	Comscore, Inc.'s Description of the Boundaries and Principal Service Commitments and System Requirements of its System.....	4
	A. Overview of Services Provided.....	4
	B. Principal Service Commitments and System Requirements.....	5
	C. Components of the System Used to Provide the Services	6

GRANT THORNTON LLP
201 S College Street
Suite 2500
Charlotte, NC 28244

D +1 704 632 3500
F +1 704 334 7701

I. Report of Independent Service Auditors

Board of Directors and Management
Comscore, Inc.

Scope

We have examined Comscore, Inc.'s ("Comscore") accompanying assertion titled *Assertion of Comscore, Inc.'s Management* ("assertion") that the controls within Comscore's Online Market Research Service, which includes the following brands [www.mobilexpression.com, www.digitalreflectionpanel.com, www.opinionsquare.com, www.relevantknowledge.com, www.permissionresearch.com, www.scorecardresearch.com, www.premieropinion.com, and www.voicefive.com] ("system") were effective throughout the period June 1, 2019 to May 31, 2020, 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*).

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 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 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's Online Market Research Service were effective throughout the period June 1, 2019 to May 31, 2020, 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.



Charlotte, North Carolina
June 26, 2020



The SOC Logo is a proprietary trademark and service mark of the American Institute of Certified Public Accountants, which reserves all rights.

II. Assertion of Comscore, Inc.'s Management

We were responsible for designing, implementing, operating, and maintaining effective controls within Comscore, Inc.'s ("Comscore") Online Market Research Service, which includes the following brands [www.mobileexpression.com, www.digitalreflectionpanel.com, www.opinionsquare.com, www.relevantknowledge.com, www.permissionresearch.com, www.scorecardresearch.com, www.premieropinion.com, and www.voicefive.com] ("system") throughout the period June 1, 2019 to May 31, 2020, 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 sub-sections A and C of Section III, *Comscore, Inc.'s Description of the Boundaries and Principal Service Commitments and System Requirements 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, 2019 to May 31, 2020, 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*). 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 sub-section B of Section III, *Comscore, Inc.'s Description of the Boundaries and Principal Service Commitments and System Requirements 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 its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 1, 2019 to May 31, 2020, to provide reasonable assurance that Comscore's service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Comscore, Inc.’s Description of the Boundaries and Principal Service Commitments and System Requirements of its System

A. 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, which includes the following brands: www.mobileexpression.com, www.digitalreflectionpanel.com, www.opinionsquare.com, www.relevantknowledge.com, www.permissionresearch.com, www.scorecardresearch.com, www.premieropinion.com, and www.voicefive.com, 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, PremierOpinion, and VoiceFive) 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	
q	MobileXpression Privacy Statement
q	Digital Reflection Privacy Statement
q	OpinionSquare Privacy Statement
q	RelevantKnowledge Privacy Statement
q	PermissionResearch Privacy Statement
q	ScorecardResearch Privacy Statement
q	PremierOpinion Privacy Statement
q	VoiceFive Privacy Statement

B. Principal Service Commitments and System Requirements

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 is collected;
- Make commercially reasonable efforts to automatically filter certain personal information collected from Panelists such as password and account numbers; however, information about panelists may inadvertently be collected; 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.

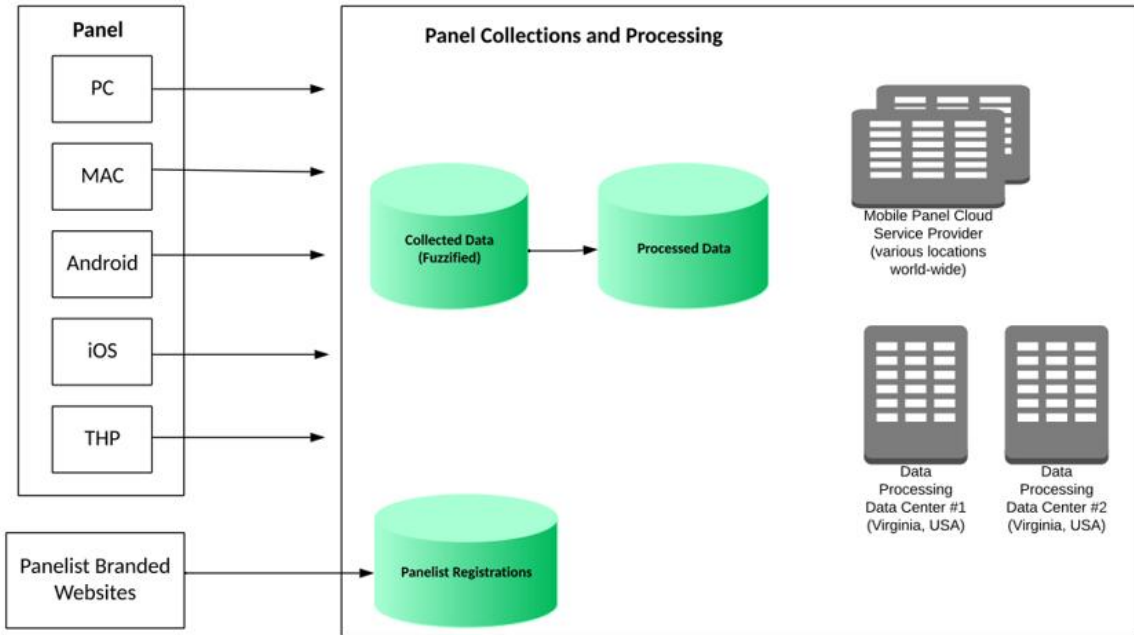
These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out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

C. Components of the System Used to Provide the Services

1. Infrastructure

Below is a high level overview of the infrastructure supporting the service.

Panel Infrastructure Overview



2. Software

Comscore has three main types of panels.

- PC/Mac: Panelists install software to measure digital activity on their computers;
- Mobile: Panelists install software to collect browser and app activity on mobile devices, typically using a VPN to route traffic; and
- Total Home: Panelists plug hardware into home routers in order to collect Internet traffic on home networks.

Brand	Type
OpinionSquare (OS)	PC Panel, has a login
PermissionResearch (PR)	PC Panel, has a login
Relevant Knowledge (RK)	PC Panel, no login
PremierOpinion (PO)	PC Panel, no login
MobileXpression (MXP)	Mobile Panel, has a login
Digital Reflection (DR)	Total Home Panel, has a login
ScorecardResearch	Not a panel, used for tagging

3. People

Management of the Company is responsible for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Importance is placed on maintaining sound internal controls and the integrity and ethical values held by the Company. As detailed within the Employee Handbook, organizational values and behavioral standards are communicated to personnel through policy statements and formal codes of conduct.

Individuals associated with each job function are responsible for training, execution of established processes and procedures, and other tasks associated with maintaining the Company's control environment. Each department maintains an organizational chart that indicates its reporting structure and area of responsibility. The charts are kept up-to-date and are available to department personnel. These organizational charts are developed in sufficient depth to indicate the responsibility, authority, and interrelationship of personnel who support the control environment. Each Senior Officer of the Company has accountability and supervisory authority for his/her assigned area in each of the operating business units.

4. Data

The types of data related to the system can be broken down into three categories: information collected automatically, information provided via the Meter, and information provided by third parties.

Information collected automatically from Comscore's websites

Comscore's Website and application automatically create logs regarding user entities' activities on Comscore's Website. These logs may identify the features that user entities use, the actions that user entities take, and the information that user entities access while on our Website or mobile app.

The personal information collected from user entities may include online identifiers (e.g., IP address) and Internet or other electronic network activities, including information about browsing history, operating system, browser type, website preferences, and use of the website or application (e.g., time accessed, duration of visit, etc.).

Information provided via the Meter

Personal and other information is collected when user entities choose to participate in Comscore's Panels by voluntarily downloading and enabling the software which allows Comscore to monitor the digital consumption behavior on the computer on which user entities install it. The software collects this information regardless of whether you the user is connected to the Internet at the time.

The following types of computer and device information are collected:

- Online identifiers (e.g., cookie ID, device ID, etc.);
- IP address and geolocation inferred by the IP address;
- General hardware, software, computer, or device configuration information about the computer on which user entities install the Company's software or any connected device,
- Operating system;
- Browser information, such as type and version;
- Speed of the computer processor, its memory capacity, Internet connection speed, and device type and configuration; and
- Information about the devices connected to user entities' computers or networks, such as the type of printer or router used.

Information about web browsing activities and use of the applications on user entities' devices are also collected, such as the following:

- Internet or other network activities,
- What is clicked on and what is typed,
- Time spent on a particular website,
- The content on the websites visited and within the applications used,

- The context and location in which certain content is displayed on individual web pages,
- Any information that is available through these websites or applications,
- Any information submitted to these websites and applications (e.g., search queries),
- Select e-mail header information from web-based e-mails,
- Information about any software that downloaded or used, and
- Information about use of video streaming services.

Information Provided by Third Parties

Comscore may also collect information from third parties and service providers collecting the information of user entities on Comscore's behalf, as well as companies such as, information resellers, search engines, e-mail providers, social networks, and other application service providers whose Internet sites or applications are used by user entities.

Comscore uses the information collected through the software and the survey responses from user entities, combined with information from other sources, to make predictions and evaluations about current and future digital consumption behavior based on inferences drawn from the information collected.

5. Processes and Procedures

Management has developed and communicated procedures to restrict logical access and protect the privacy of information related to the Online Market Research Service. Security obligations of internal users and the Company's security and privacy commitments to users are documented within the Data Security Policy and, as such, are communicated to internal users through the Company's intranet.

The Company has developed and implemented formal, documented security and privacy policies and procedures which are approved on an annual basis; include administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction; and address the following:

- Risk assessment and treatment;
- Security policies;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development, and maintenance;
- Information security incident management;
- Business continuity management; and
- Compliance.

The Company's formal documented privacy policies addresses the following:

- The purpose for collecting personal information,
- Notice,
- Choice and consent,
- Disclosure to third parties,
- Collection,
- Use and retention,
- Access,
- Onward transfer and disclosure,
- Security for privacy,
- Quality,

- Disposal, and
- Monitoring and enforcement.

6. Subservice Organizations

The Company uses various subservice organizations as follows:

Company Name	Service(s) Provided
Amazon Web Services	The Company uses Amazon Web Services for the hosting of the collection servers for census data pertaining to Scorecard Research.
Lightspeed Research	The Company uses Lightspeed Research for the management and hosting of the registration/new panelist recruitment process for Digital Reflection.
Anexia, Inc.	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.
CenturyLink, Inc.	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.
QTS Realty Trust, Inc.	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.
Cyxtera Technologies, Inc.	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.

Our description of the boundaries of the system and the principal service commitments and system requirements related to the applicable trust services criteria do not include the services provided by the subservice organizations.

Our conclusion regarding effectiveness of controls within the system to achieve Comscore's service commitments and system requirements based on the applicable trust services criteria assumes that the complementary subservice organization controls assumed in the design of Comscore's Online Market Research Service operated effectively throughout the period June 1, 2019 to May 31, 2020.

7. Complementary User Entity Controls

Our description of the boundaries of the system and the principal service commitments and system requirements related to the applicable trust services criteria do not include complementary user entity controls.

Our conclusion regarding the effectiveness of controls within the system to achieve Comscore's service commitments and system requirements based on the applicable trust services criteria assumes that complementary user entity controls assumed in the design of the Comscore's controls operated effectively throughout the period June 1, 2019 to May 31, 2020.



© 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.