GALLUP®

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

STRATEGIC CONSULTING AND DATA ANALYTICS SERVICES SYSTEM

FOR THE PERIOD OF MARCH 1, 2023, TO FEBRUARY 29, 2024

Attestation and Compliance Services

schellman
Quality, above all.

INDEPENDENT SERVICE AUDITOR'S REPORT

To Gallup, Inc.:

Scope

We have examined Gallup, Inc.'s ("Gallup") accompanying assertion titled "Assertion of Gallup Service Organization Management" ("assertion") that the controls within Gallup's strategic consulting and data analytics services system ("system") were effective throughout the period March 1, 2023, to February 29, 2024, to provide reasonable assurance that Gallup's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and privacy ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Gallup uses various subservice organizations for cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Gallup, to achieve Gallup's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Gallup 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 Gallup's service commitments and system requirements were achieved. Gallup has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Gallup 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 systems 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 Gallup's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Gallup's service commitments and system requirements based on the applicable trust services criteria.

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

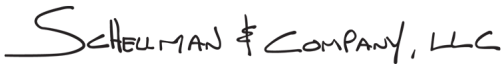
Inherent Limitations

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 Gallup'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 Gallup's strategic consulting and data analytics services system were effective throughout the period March 1, 2023, through February 29, 2024, to provide reasonable assurance that Gallup's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Chicago, Illinois
March 27, 2024

ASSERTION OF GALLUP SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Gallup, Inc.'s ("Gallup") strategic consulting and data analytics services system ("system") throughout the period March 1, 2023, to February 29, 2024, to provide reasonable assurance that Gallup's service commitments and system requirements relevant to security, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented below 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 March 1, 2023, to February 29, 2024, to provide reasonable assurance that Gallup's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Gallup's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 March 1, 2023, to February 29, 2024, to provide reasonable assurance that Gallup's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE STRATEGIC CONSULTING AND DATA ANALYTICS SERVICES SYSTEM

Company Background

Gallup delivers analytics and learning to help leaders and organizations solve their most pressing problems. Combining 89 years of experience with its global reach, Gallup strives to know more about the attitudes and behaviors of employees, customers, students, and citizens than any other organization in the world. Gallup's 1,200 professionals include noted scientists, renowned subject-matter experts, and best-selling authors. The research and consulting teams serve clients in 13 offices around the world. Each office operates under a cohesive set of high standards. Gallup's unified global ownership ensures that clients in each region benefit from the depth of the international experience, industry leadership, innovation, and worldwide operating standards, combined with country-specific expertise.

Gallup works with leaders and organizations to achieve breakthroughs in customer engagement, employee engagement, organizational culture and identity, leadership development, talent-based assessments, entrepreneurship, and well-being.

Description of Services Provided

The following services were included within the scope of the examination.

Customer Engagement, Analytics

Gallup measures a client's customer experience using a structured questionnaire (survey). The client sends their customer contact information by secure protocol. Gallup applies agreed upon sampling criteria prior to contacting the customers. The sampling criteria reduces the sample to adequately fulfill predetermined respondent quotas. Gallup applies the selected sample to either the Survox outbound phone interviewing methodology or to the Gallup e-mail invitation service for the web survey. The responses provided by customers are securely stored in a database from which analysis, aggregation, and reports are conducted and produced. Gallup monitors response rates to ensure a sufficient sample is available to meet the quota. The client also prepares an employee roster which is used to create an organization hierarchy for reporting and authentication purposes. Client users will authenticate to Gallup's web survey and reporting platform, and based on previously determined roles and permissions, will have access to the reports suitable for their role and responsibility. The survey may include an option for a respondent to request contact by the client regarding their experience. This option will report such requests as an "action alert" available through Gallup's web platform. Customer behavior analytics and data are provided to help clients make key business decisions.

Workplace Analytics

Gallup measures a client's employee engagement using a structured questionnaire (survey). With a closed sample, the client sends their employee roster which contains information jointly determined by Gallup and the client to Gallup via a secure protocol. Gallup uses this roster to develop an organization hierarchy, identify supervisors and managers for reporting and authentication purposes, and to assign a unique access code for each invited employee. This unique access code must be used by each of the client's employees to gain access to the unique survey uniform resource locator (URL) created for the client. Once the unique access code is validated by Gallup's application services, it permits the respondent to continue with the survey. Upon submission of the completed survey, the employee's responses are validated, and the access code is flagged as used. Gallup will send a reminder e-mail to those employees who have not yet submitted their individual survey. With an open sample, a client uses a specific link and distributes that link via various distribution channels. Employees then use this link to enter their responses for analysis and aggregation.

Responses provided by employees are securely stored in a database from which analysis, aggregation, and reports are conducted and produced after the survey timeframe is closed. Client users authenticate to Gallup Online using the organization structure (OMS) service or Gallup Access using Security Token Service (STS). Reporting access is restricted based on previously determined roles and permissions.

CliftonStrengths®

Gallup offers the CliftonStrengths® assessment to clients who choose to have a Gallup-managed consulting experience for employee development or select a do-it-yourself approach purchasing the assessment via e-commerce channels. The client will send the assessment to their selected employees who are to complete the assessment by secure protocol. The client may also provide a list of employees who have been identified as strengths coaches, leaders, or managers, thus providing sufficient information to establish an organization hierarchy for CliftonStrengths reporting and coaching purposes. As with Workplace Analytics, Gallup will organize the invited employees and assign a unique access code for participation through Gallup Access. Gallup will send an invitation e-mail to each selected employee with the assessment URL and access code. When an assessment has been completed, a report indicating the employee's top five strengths, or all 34 strengths, is produced. The CliftonStrengths report and summary are made available to the participant and if specified, the client strengths coaches, leaders, and/or managers.

Hiring Analytics (Selection)

Gallup offers clients a talent-based assessment solution that is web-based. The client identifies the position types for which a web assessment would be appropriate. The client typically utilizes their own applicant tracking system (ATS) that is available to candidates who wish to seek employment with the client. The ATS is configured to support the employability characteristics of the position. The candidate completes the ATS application form. The ATS may have qualifying factors which determine if the candidate is qualified to participate in the Gallup assessment. If such an evaluation is positive, the ATS will send an encrypted human resource extensible markup language (HR-XML) payload to Gallup's OMS application. The organization structure will have client employee information to create a hierarchy which identifies the business units that would receive assessment results and provide logon authentication. The payload contains information that identifies the assessment to be used and other information that is unique to the project. The candidate may be presented with a link for the assessment during the application process or the ATS may send an e-mail with a unique access code and assessment URL. Upon completion, the assessment is scored with a predefined algorithm. Assessment results may be available via the ATS or Gallup Online, depending on preferences defined by the client. The requesting manager will be presented with candidates and their classification/score.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

The scope of this assessment was limited to the services provided by Gallup, which represents Gallup, Inc., its subsidiaries, and affiliated entities including, but not limited to, The Gallup Organization Ltd., Gallup GmbH, The Gallup Organization PTY Ltd., and The Gallup Organization PTE Ltd.

Principal Service Commitments and System Requirements

Gallup designs its processes and procedures to meet its objectives for the services it offers. Those objectives are based on the service commitments that Gallup makes to user entities, the laws and regulations that govern the provision of the strategic consulting and data analytics services, and the financial, operational, and compliance requirements that Gallup has established for the services. The strategic consulting and data analytics services of Gallup are subject to the relevant regulatory, industry, and data security requirements in which Gallup operates.

Security, confidentiality, and privacy commitments to user entities are documented and communicated in customer contracts, sales documentation, and the privacy statement. The principal security, confidentiality, and privacy commitments are standardized and include the following:

Security

- Security principles within the fundamental designs of the services offered are designed to permit system users to access the information for their entity while restricting them from accessing information of other entities.
- Encryption technologies are utilized to protect customer data both at rest and in transit.
- Firewalls and network segmentation are utilized to restrict network traffic flow to appropriate and authorized use.
- Logical access controls are implemented along with regular review and monitoring.
- Security monitoring infrastructure is implemented including intrusion detection, centralized log management, and alerting.
- The on-premise data center is architected with multi-layered physical security.
- A vulnerability management program is designed to promptly identify and correct vulnerabilities within the environment.
- An incident response program is designed to minimize the impact of security events and protect resources.
- Physical and logical access controls are implemented to protect confidential information from unauthorized or inadvertent erasure or destruction.

Confidentiality

- Classification policies and supporting procedures are utilized to identify and designate confidential information when it is received or created.
- Destruction procedures are implemented to identify confidential information requiring destruction.

Privacy

- Personal information is collected and used only for the particular purpose stated at the point of collection.
- Personal information is retained in accordance with guidelines or contractual requirements and disposed of upon request or in accordance with contractual requirements.
- Reasonable and appropriate security procedures are maintained to protect personal information from loss, misuse and unauthorized access, disclosure, and alteration and destruction.
- Requests to correct, update, amend, suppress, delete, or otherwise modify personal information are responded to and processed.

Gallup establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. This includes using encryption technologies to protect system user data both at rest and in transit, implementing background screening for personnel, performing periodic vulnerability scans and penetration tests, authenticating personnel using strict password enforcement mechanisms, revoking access to personnel upon termination, and ongoing monitoring to ensure the achievement of the related objectives.

Such requirements are communicated in Gallup's customer contracts, sales documentation, and the privacy statement. 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, trained, and managed. 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 strategic consulting and data analytics services.

In accordance with the assertion and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

The infrastructure and software supporting the strategic consulting and data analytics services system is housed in primary and secondary locations. The primary locations include a Gallup owned and operated data center located in Omaha, Nebraska; Amazon Web Services, Inc. (AWS) data centers located in Virginia (US East (Northern Virginia)), and Frankfurt, Germany (EU (Frankfurt)); and Microsoft Azure (Azure) data centers located in Iowa (Central US), Illinois (North Central US), Ireland (North Europe), and Singapore (Southeast Asia). The secondary locations include a Scott Data Center colocated data center located in Omaha, Nebraska; an AWS data center located in Oregon (US West (Oregon)); and Azure data centers located in Virginia (East US 2) and the Netherlands (West Europe).

People

Personnel involved in the operation and use of the system include the following:

Operation Teams

- Project Implementation, Implementation Analyst – An Implementation Analyst designs, programs, and implements a list of survey participants per client specifications for outbound, paper, and web methodologies. They advise client teams of potential problems with client supplied lists and propose actionable solutions. They serve as the first and central point of contact for a Gallup Consultant or client team to start the process for survey creation and editing. They format the survey into Gallup's internal methodology templates. They clean, organize, and aggregate data for internal and external use. They are responsible for running routine data processing or analysis tasks with data sets to be used in reporting or for research and analytics.
- Project Implementation, Implementation Quality Assurance – An Implementation Quality Assurance employee ensures the quality of instruments for data collection and reporting through detailed checklist items and their knowledge and documentation of practice and systems requirements. They work with the Instrument Specialist, Instrument Specification Writers, and Consulting Specialists to help ensure the surveys are created correctly and that the programming works as designed. They are also responsible for running sophisticated checks on organizational structures to minimize the risk of structure errors on projects.
- Consulting Specialists – A Consulting Specialist is responsible for helping clients customize tools and integrate them into the client organization. They offer strategic insights through analytical analysis and the creation of meaningful executive presentations. A Consulting Specialist provides input and direction on the various facets of a client project, including questionnaire design and delivery, sample and organizational structure design, and report design and delivery.
- Project Manager – A Project Manager is responsible for managing their projects from the point of proposal and study design through client delivery of the data and/or discoveries and recommendations, on time, on budget, and with perfection. They communicate, facilitate, arrange, and motivate the individuals and teams that support the delivery of Gallup's consulting projects.

Talent Resources – Talent Acquisition

- Director of Talent Sourcing – A Director of Talent Sourcing finds and recruits individuals with world-class talent to become Gallup associates. They accomplish this by building relationships with campus leaders, students, faculty, administrators, and community leaders to promote the Gallup brand within colleges, universities, and communities. They typically focus their efforts on a specific department or region.

Departmental Go-Tos (managers)

- Manager of Operations – A Manager of Operations is responsible for recruitment, hiring, retention, and engagement of associates and ensuring they adhere to global best practices. They lead others to help ensure timelines, scope, quality, and customer needs are met or exceeded.

Legal

- Data Protection Officer (DPO) – A DPO is responsible for overseeing Gallup's data protection strategy and implementation. They ensure that Gallup is compliant with all applicable privacy legislation requirements, train Gallup employees on privacy legislation compliance requirements, and conduct regular assessments and audits to ensure applicable privacy legislation compliance. A DPO serves as the point of contact between Gallup and relevant supervisory authorities, maintains records of data processing activities conducted by Gallup, and responds to data subjects to inform them about how their personal data is being used and what measures Gallup has in place to protect their data.
- The Legal team has global responsibility for legal matters including contracts, intellectual property, litigation, and defense of the company's future, including such things as new legislation and rules and regulations that will affect the businesses.

Information Technology (IT) – Software Development

- Systems Application Development – A Systems Applications Developer is responsible for writing programming code to create, maintain, and support approved software applications for Gallup. Development includes application design, unit and functional testing, implementation, and following the software development product lifecycle.
- Technical Project Manager – A Technical Project Manager leads Gallup technology projects from design through development, testing, and implementation. They are responsible for meeting stakeholder expectations while keeping projects on time, in scope, and within budget.
- Technology Client Solutions Manager – A Technology Client Solutions Manager supports clients using Gallup products and provides feedback to Gallup Developers and Technical Project Managers with suggested application improvements.

IT – Infrastructure

- Network/Systems Administrator – A Systems Administrator is responsible for designing, planning, monitoring, and maintaining systems within Gallup Technology. They also work to expand and improve the system while providing communication and education about the system to the global organization.
- Database Administrator – A Database Administrator develops, maintains, and implements the policies and procedures necessary to help ensure the security and integrity of a corporate database. They establish and maintain sound backup and recovery policies, develop and maintain database documentation, maintain user roles, assign privileges, and provide 24x7 support when required.
- Gallup Security Advisory Team (GSAT) – The GSAT team is responsible for managing the ongoing maintenance, monitoring, and support of the security guidelines, standards, and best practices adopted by Gallup. The team serves as a leading advisory partner to the Gallup enterprise and as an expert on issues of compliance, governance, data privacy, and technical security trends requested by clients and/or prospects around the world.

Procedures

Access Authentication and Authorization

Access to system information, including confidential data, is protected by authentication and authorization mechanisms. User authentication is required to access the in-scope systems.

Authorized systems administration personnel are responsible for assigning and maintaining access rights to the production environment. Access to production systems varies by system and is ultimately restricted either via Active Directory (applicable to domain controllers, servers, certain databases, certain applications, and remote access),

OMS (applicable to certain applications), or directly to the system/device (applicable to certain databases, network and storage infrastructure, cloud hosting vendor consoles (i.e., AWS and Azure), and certain applications).

Access Requests and Access Revocation

Internal and external user access requests are initiated by a manager and are documented via e-mail or ticket. Employee role transfers are initiated by a manager, documented in the Payroll accounting system, and are communicated via e-mail. Once an employee's manager triggers an employee or contractor termination, automated tasks are utilized to notify systems owners via e-mail of certain tasks that include the revocation of access. A review of system access privileges is additionally performed for prioritized systems at least semi-annually to help ensure that access to systems is restricted to authorized personnel.

Device and Network Security

A firewall system is in place to filter unauthorized inbound network traffic from the Internet. The firewall system configurations are reviewed on a quarterly basis to help ensure that only necessary connections are configured. Additionally, an intrusion detection system (IDS) is utilized to analyze and report network events to relevant personnel.

Policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted. Data in transit utilizes transport layer security (TLS) encryption for the secure transfer of information. Encrypted VPNs requiring two-factor authentication are utilized for remote access for the security and integrity of the data passing over the public network.

Confidential data maintained within the production environment is stored in an encrypted format, and third-party software is configured to encrypt backup media. Backup media is secured in a tamper resistant case within the data center.

Physical Security

The infrastructure supporting the strategic consulting and data analytics services system is housed in an internal data center located in Omaha, Nebraska, and in AWS and Azure data centers located in the US, Europe, and Asia. The Gallup data center utilizes the following physical protection controls:

- Badge access authentication mechanisms
- Two-factor authentication system required for access to the data center
- Real-time and archived digital video surveillance system
- Visitor badges
- Visitor logs for the facilities
- Visitor escort required
- No exterior windows within the data center
- 24x7x365 guards
- Alarmed doors with response upon activation
- Locked device cages

Securing Gallup services using the AWS virtual private cloud and/or Azure virtual network is a joint responsibility between Gallup, AWS, and Azure, respectively. AWS and Azure are responsible for physical and environmental security, hypervisor security, and providing the underlying infrastructure of databases, firewalls, load balancers, user management services, queuing services, e-mail, and other services. Gallup is responsible for securely configuring and managing the operating systems and applications required for the strategic consulting and data analytics services system.

Change Management

Documented policies and procedures are in place to guide personnel in the change management process which includes documentation, testing, and change approval requirements. Changes to systems are documented within a centralized ticketing system to document, manage, and monitor changes from request through implementation. The change request process enforces and records the change description, request authorization, due date, affected systems, testing, and approval. Changes are tested when applicable, approved prior to implementation, and verified post-implementation. The ability to implement changes into the production environment is restricted to authorized personnel.

Development and testing activities are performed in distinct environments that are logically separate from production in order to ensure that changes made within the test environments do not affect changes in the production environment. The software development platforms enable development personnel to check-out different versions of the code for editing. Once users are ready to update the code repository, they check-in the version and after a code review is performed, and if approved, then merge the changes into the code branch. The software development platforms assign a different version number to iterations. The ability to modify source code within the software development platforms is restricted to user accounts accessible by authorized development personnel.

Automated systems and scripts are in place to monitor for changes to production systems and are configured to notify systems administration and security personnel when changes are detected. Additionally, application logs, including build details, are configured to send events to a log aggregation tool, which is reviewed by security analysts as part of their day-to-day responsibilities. Administrative access privileges to the systems and scripts used for notifying personnel when changes to applications occur are restricted to user accounts accessible by authorized security personnel.

Emergency changes are subject to the standard change management procedures; however, implementation is expedited, and documentation can be performed in arrears.

Incident Response

Documented incident response policies and procedures are in place to guide personnel in the investigation and resolution of security incidents and are communicated to employees via the company intranet. These policies and procedures include, but are not limited to, the following incident management process components:

- Roles and responsibilities
- Documentation
- Incident response plan activation
- Notification and escalation procedures
- Legal requirements
- Containment and remedial actions

The incident response plan supplements the incident response policy and establishes procedures to report and handle physical and IT-related incidents. The goal of the plan is to minimize the impact due to disruption of critical computing services when incidents occur. The plan is tested on an annual basis and includes an incident response process walkthrough using real world scenarios.

IT system users, including employees and contractors, are required to contact client support or the help desk when an information security incident is suspected or discovered. The incident is escalated to predefined groups for further analysis and are acted upon based on the priority given to the initial findings associated with the incidents. The incidents are rated on a scale of priority 1 – priority 4 in which priority 1 is a possible life-threatening activity or affects critical information and priority 4 is an unintentional violation of the security policy. Security personnel document incidents that require follow-up or a change within the ticketing system. Information documented within the ticket includes names of personnel that discovered the incident, steps taken to resolve the incident, and lessons learned. Additionally, a root cause analysis is performed as a component of the incident review process that includes actions to prevent or address security incidents. Gallup separately documents security incidents which it retains for investigation, corrective actions, and potential disciplinary actions/or prosecution.

Furthermore, the GSAT team meets on a monthly basis to discuss any security incidents that occurred during the past month to analyze the impact, resolution, lessons learned, and action items. The GSAT team utilizes the knowledge gained from analyzing and resolving incidents to reduce the likelihood or impact of future incidents.

System Monitoring

A security information and event management (SIEM) tool is utilized to monitor security events according to internal prioritization. These security events consist of activities on the in-scope systems, including the network, firewalls, routers, IDS, servers, databases, and applications. The SIEM tool analyzes the log results and alerts security personnel via e-mail alerts in the event suspicious or unauthorized activities are identified. Upon receipt of the alerts, security personnel review the alerts to determine if any additional action should be taken. Regular security reviews and vulnerability assessments are also performed by IT personnel and third-party vendors to identify new vulnerabilities and susceptibilities to new vulnerabilities. Such reviews include, but are not limited to, quarterly internal and external network vulnerability scans and an annual penetration test.

Enterprise antivirus software and a cloud native endpoint detection and response (EDR) tool are utilized to protect registered production servers and workstations. Production servers and workstations are configured to scan for updates to virus definitions and update registered clients on a continuous basis.

Privacy Practices

As a component of Gallup's strategic consulting and data analytics services system, Gallup provides services to user entities in the capacity of a Data Processor. Gallup serves in the function of a Processor in cases where it processes personal data only as instructed by user entities (Data Controllers) to fulfill the requirements of an agreement associated with the provisioning of the services. Additionally, Gallup retains personal information in accordance with established guidelines or contractual requirements, and personal information is disposed of either upon customer request or in accordance with contractual requirements.

User entities are responsible for providing their privacy statement to individuals. Gallup communicates its privacy statement to user entities via its company website. The privacy statement is inclusive of how the organization addresses privacy from both the Data Controller and Data Processor perspectives; however, only areas that the service organization acts as the latter are applicable to this review.

A comprehensive information security program is maintained that contains technical and organizational safeguards designed to ensure customer data is not lost, accidentally destroyed, misused, or disclosed, and is not accessed except by authorized employees and partners in the performance of their duties. Gallup maintains a privacy program and has appointed a DPO to provide advice and guidance around compliance with various privacy regulations. Gallup (as a Data Processor) supports its clients (as the Data Controller) to complete any/all necessary privacy and legal agreements as requested, including but not limited to, Privacy Impact Assessments and Data Processing Agreements. A Record of Processing Activities (ROPA) is additionally maintained by Gallup to verify that personal information is collected, used, maintained, and processed in a manner consistent with the entity's objectives related to privacy.

Gallup customers are responsible for ensuring that (i) they will comply with all applicable data protection legislation and (ii) they have the right to transfer, or provide access to, the personal data to Gallup for processing in accordance with the terms of the agreement.

Gallup tracks unauthorized disclosures of personal information in a ticketing system. Additionally, management meetings are held monthly to discuss incidents and corrective measures to ensure incidents are resolved. In the event of complaints, disputes, or data deletion requests, Gallup has a dedicated privacy e-mail account and resolution process in place. Data subject access requests (DSARs) received via the privacy e-mail account are recorded in an access-restricted data subject access log and are assigned to the appropriate team to fulfill the request.

Data

Documented data retention and destruction policies are in place to define retention periods and the disposal process for confidential data. Confidential data is retained in accordance with established guidelines or contractual requirements. Confidential data maintained within the production environment is stored in an encrypted format. Upon customer request or in accordance with contractual requirements, confidential data is disposed of using approved sanitization or disposal procedures.

[Intentionally Blank]

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Client's "customer" contact information includes: • Outbound phone data – includes customer name, telephone number, and services experienced. • Web survey data – includes customer or employee name, e-mail address, and services experienced. • Paper surveys – includes a unique predetermined respondent identifier. • Client provides organizational hierarchy for reporting purposes. Client contact data provided for their customers do not include primary account numbers or other identifiers which might reveal transactions and activities of a specific "customer."	Gallup aggregates respondent data with a reporting requirement of five or more. No individual respondent's data is reported. Aggregated reports (scorecards) are available to authorized client users via Gallup's client platforms (Gallup Online and Gallup Access). Permissions for access to such reports are defined by the client to ensure that "Store 1" gets only "Store 1" reports. This is managed by Gallup's organization structure application and the rollup reporting hierarchy is jointly defined by the client and Gallup. If the respondent, during the interview process, indicates that they wish to have contact with the client for problem-solving or positive feedback, the respondent must give consent for their name and contact information to be provided by Gallup to the client. Such contact information is sent by an "action alert".	Confidential

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Client employee information includes: The content of a client's employee roster is designed to provide personal and organizational information to support the project. The data can include: employee name, employee identification (ID), employee e-mail address, manager name, manager ID, organizational elements that include division, department, team, work location, job classification, primary language, country code and length of service. A client may also wish to include additional demographic data (full-time/part-time status, hire date, job title, department, etc.) about each employee roster. There are two categories of demographics available with Gallup's client platforms: dispositional and positional: • Dispositional demographics include age, gender, and race/ethnicity – essentially anything that describes a person regardless of his or her position as an employee. Both Gallup and the client's legal department must sign a Demographic Authorization Letter to gain permission to collect and present these employee level demographics. • Other demographics, such as length of service, job title, job function, location/facility, and department are positional and do not require an authorization letter. If the client wishes to have an open-ended question, Gallup requires that both Gallup and the client's legal department sign a verbatim authorization letter. Gallup requests that clients avoid providing social security numbers, driver's license identifiers, international identifiers, credit card numbers, etc.	Gallup aggregates respondent data with a reporting requirement of five or more. No individual respondent's data is reported. Aggregated reports (scorecards) are available to authorized client-users via Gallup's client platforms (Gallup Online and Gallup Access). Permissions for access to such reports are defined by the client to ensure that "Dept. 1" gets only "Dept. 1" reports. Gallup can produce reports based upon any employee attribute, variable, or reporting relationship (including matrixed).	Highly Confidential

Subservice Organizations

The cloud hosting services provided by AWS and Azure were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS and Azure, alone or in combination with controls at Gallup, and the types of controls expected to be implemented at AWS and Azure to meet those criteria.

Control Activities Expected to be Implemented by AWS and Azure	Applicable Trust Services Criteria
AWS and Azure are responsible for implementing controls to manage logical access to the underlying network and virtualization management software for their cloud hosting services where production systems reside.	CC6.1 – CC6.3 CC6.6 – CC6.7
AWS and Azure are responsible for implementing controls to restrict physical access to facilities and protected information assets.	CC6.4
AWS and Azure are responsible for implementing controls to render data unreadable, when directed by Gallup, prior to the decommissioning of physical assets.	CC6.5

Gallup has not delegated any responsibility of the personal information life cycle to AWS or Azure.

Trust Services Criteria Not Applicable to the In-Scope System

The Trust Services criteria presented below are not applicable to the strategic consulting and data analytics services system within the scope of this examination. As a result, an associated control is not required to be in place at the service organization for the omitted applicable trust services criteria. The following table presents the trust services criteria that are not applicable for the strategic consulting and data analytics services system at Gallup.

Criteria #	Reason for Omitted Criteria
P1.1	Providing notice to data subjects regarding privacy practices, including changes in the use of personal information, is the responsibility of the data controller and not Gallup given its role as a data processor.
P2.1	Communicating choice and obtaining consent regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects is the responsibility of the data controller and not Gallup given its role as a data processor.
P3.2	Obtaining consent and communicating the need for consent, as well as the consequences of a failure to provide consent for the request for personal information, to data subjects is the responsibility of the data controller and not Gallup given its role as a data processor.
P5.1	Providing access to data subjects is the responsibility of the data controller and not Gallup given its role as a data processor.
P5.2	Correcting, amending, or appending personal information is the responsibility of the data controller and not Gallup given its role as a data processor.
P6.1	Obtaining consent from data subjects for purposes of third-party disclosure is the responsibility of the controller and not Gallup given its role as a data processor.
P6.7	Providing an accounting to the data subject of the personal information held and disclosing a data subject's personal information is the responsibility of the data controller and not Gallup given its role as a data processor.