Microsoft Corporation – Iris Campaign Communication Service and Iris Communication Platform

Report on Controls at Service Organization Relevant to Security, Availability, and Confidentiality (SOC 2)

October 31, 2018

Deloitte.

Table of contents

Executive summary

Microsoft Corporation—ICCS & ICP	
Scope	Iris Campaign Communication Service (ICCS) and Iris Communication Platform (ICP)
Period of Examination	As of October 31, 2018
Applicable Trust Principles	Security, Availability, and Confidentiality
Locations	Redmond, WA
Subservice Providers	Yes: • Microsoft Azure ("Azure") • Salesforce Marketing Cloud
Opinion Result	Unqualified
Testing Exceptions	0
Complimentary User Entity Controls	Yes – **Page 19**

Section I: Independent service auditors' report

Deloitte & Touche LLP

925 Fourth Avenue, Suite 3300
Seattle, WA 98104-1126
USA

Tel: +1 206 716 7000
Fax: +1 206 965-7000
www.deloitte.com

Section I:
Independent service auditors' report

Microsoft Corporation
Redmond, Washington

Scope

We have examined the attached description of the system of Microsoft Corporation (the "Service Organization") related to Iris Campaign Communication Service (ICCS) and Iris Communication Platform (ICP) which comprises the Iris email campaign service as of October 31, 2018 (the "Description"), based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (American Institute of Certified Public Accountants (AICPA), *Description Criteria*), ("description criteria") and the suitability of the design of controls stated in the Description as of October 31, 2018, to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

The information included in **Section IV**, *Supplemental information provided by the Service Organization*, is presented by management of the Service Organization to provide additional information and is not a part of the Description. This section has not been subjected to the procedures applied in the examination of the description and the suitability of the design of the controls, to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria, and, accordingly, we express no opinion on it.

The Service Organization uses subservice organizations Microsoft Azure to provide Platform-as-a-Service (PaaS) cloud services for hosting the Service Organization applications, and Salesforce Marketing Cloud to provide Software-as-a-Service (SaaS) e-mail management, delivery, and analytics. The Description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls at the Service Organization, to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria. The description presents the Service Organization's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ICCS and ICP's controls. The Description 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 of such complementary subservice organization controls.

The Description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at the Service Organization, to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria. The Description presents the Service Organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the Service Organization's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design of such controls.

Service Organization's Responsibilities

The Service Organization 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 the Service Organization's service commitments and system requirements were achieved. The Service Organization has provided the accompanying assertion titled "Assertion of Service Organization Management" ("assertion") about the description and the suitability of the design of controls stated therein. The Service Organization is also responsible for preparing the description and assertion, including the completeness,

accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria, and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

Service Auditors' Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We applied the statements on quality control standards established by the AICPA and accordingly maintain a comprehensive system of quality control.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. 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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design 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, in all material respects:

a. The description presents the Service Organization's systems that were designed and implemented as of October 31, 2018, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of October 31, 2018, to provide reasonable assurance that the Service Organization's service commitments and system requirements

would be achieved based on the applicable trust services criteria, if the controls operated effectively as of that date, and if the subservice organizations and user entities applied the complementary controls assumed in the design of the Service Organization's controls as of that date.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Restricted Use

This report is intended solely for the information and use of the service organization, user entities of the Service Organization's system related to ICCS and ICP as of October 31, 2018, business partners of the Service Organization subject to risks arising from interactions with the Service Organization's systems, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how they interact with related controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the Service Organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Deloitte & Touche LLP

December 12, 2018

Section II:
Management’s assertion

Section II:
Management's assertion

As of October 31, 2018

Assertion of Service Organization Management

We have prepared the description of the system in Section III of Microsoft Corporation's ("Microsoft" or the "Service Organization") as of October 31, 2018 (the "period"), related to the Iris Campaign Communication Service ("ICCS") and Iris Communication Platform ("ICP") services, collectively referred to as ("Iris") based on criteria for a description of a service organization's system in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report ("description criteria"). The description is intended to provide users with information about our system that may be useful when assessing the risks arising from interactions with Microsoft's system, particularly information about system controls that Microsoft has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy ("applicable trust services criteria").

Iris uses subservice organizations Microsoft Azure to provide Platform-as-a-Service (PaaS) cloud services for hosting the ICCS and ICP applications, and Salesforce Marketing Cloud to provide e-mail management, delivery, and analytics. The description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls for Iris, to achieve Microsoft's service commitments and system requirements related to the Iris services based on the applicable trust services criteria. The description presents Iris's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Iris's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at Microsoft to achieve the service commitments and system requirements related to the Iris services based on the applicable trust services criteria. The description presents Iris's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Iris's controls.

We confirm, to the best of our knowledge and belief, that:

a. The description presents Iris's system that was designed and implemented as of October 31, 2018, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of October 31, 2018, to provide reasonable assurance that Microsoft's service commitments and system requirements related to the Iris services would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Iris's controls as of that date.

Section III:
Description of system

Section III:
Description of the system

Overview of Operations

Business Description

Iris is a collection of Microsoft-internal services that form the engagement platform used at Microsoft to reach existing customers. Iris supports interactions with customers through email as well as through experiences within Microsoft products. Iris supports various teams at Microsoft and is designed to meet their requirements and contractual obligations with regards to security, availability, confidentiality, and compliance.

Iris Push Platform APIs

To allow partners to send email messages to customers, Iris provides two Application Programming Interfaces (APIs), called Iris Campaign Communication Service and Iris Communication Platform. This report applies to the specific instances of these APIs that have been built for email interactions with commercial end-users — such as users of Office 365 Business and Enterprise SKUs — in mind.

Description of Control Activities

This report leverages the 2017 Trust Services Criteria (TSC) for security, availability, and confidentiality as released by the AICPA in April 2017. The description of control activities relevant to the trust services criteria are included below. Additionally, the criteria for each principle and the relevant ICCS and ICP controls in place to satisfy the criteria are included below and are an integral part of the description of the system.

Applicability of Report

This report has been prepared to provide information on Iris's internal controls which are relevant to the requirements of its Microsoft-internal customers to meet the security, availability, and confidentiality trust service criteria.

This report covers the following service components:

- **The Iris Campaign Communication Service (ICCS):** ICCS is responsible for processing metadata provided by our Microsoft-internal partners about who to contact with a given email message (this is provided in the form of metadata and a list of anonymized identifiers) and looking up the email address that is associated with the identifier.
- **Iris Communication Platform (ICP):** ICP takes instructions from ICCS, checks whether the intended recipient may be contacted for a given topic, and dispatches the instructions to the downstream mailing system that the partner has designated for email delivery.

Infrastructure

The Iris services ICCS and ICP leverage Microsoft Azure's ("Azure") Platform as a Service (PaaS). Azure's service offerings enforce operating system protections within the Iris environments. To do so, the Cloud and Enterprise Security team carries out frequent internal and external scans to identify vulnerabilities and assess the effectiveness of the patch management process. In addition, applicable patches are automatically applied to ICCS and ICP Virtual Machines (VM) scale set via the Azure PilotFish[1] service.

Network layer protections, such as Incident Management, Configuration Management, Access Management, and Change Management, related to network devices are managed by Azure in coordination with the ICP and ICCS teams.

---

1 PilotFish: An Azure service which provides an Autopilot cluster co-located with Azure in every Azure data center. PilotFish clusters reside within Azure's compliance boundary, which fall outside of the scope of this report. See section Software for additional information.

Azure also is responsible for physical and environmental security for the infrastructure.

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, and Monitoring

Control Environment

Integrity and Ethical Values

Corporate governance at Microsoft starts with an Independent Board of Directors that establishes, maintains, and monitors standards and policies for ethics, business practices, and compliance that span the company. Corporate governance at Microsoft serves several purposes:

- To establish and preserve management accountability to Microsoft's owners by distributing rights and responsibilities among Microsoft Board members, managers, and shareholders.
- To provide a structure through which management and the Board set and attain objectives and monitor performance.
- To strengthen and safeguard a culture of business integrity and responsible business practices.
- To encourage the efficient use of resources and to require accountability for the stewardship of these resources.

Further information about Microsoft's general corporate governance is available on the Microsoft website.

Microsoft's Standards of Business Conduct

Microsoft's Standards of Business Conduct (SBC) reflect a commitment to ethical business practices and regulatory compliance. They summarize the principles and policies that guide Microsoft's business activities and they provide information about Microsoft's Business Conduct and Compliance Program. The SBC was developed in full consideration of the Sarbanes-Oxley Act of 2002 (SOX) and proposed NASDAQ listing requirements related to codes of conduct. The Office of Legal Compliance (OLC) updates the SBC as necessary and the SBC is made available to all employees on the intranet.

SBC training and awareness is provided to Microsoft employees, contractors, and third parties on an ongoing basis to educate them on applicable policies, standards, and information security practices. Full-time employees must also take a mandatory SBC training course within the first 60 days of their start date and then again on an annual basis thereafter.

Further information about Microsoft's SBC is available on the Microsoft website.

OLC – Business Conduct Hotline

There is a confidential and anonymous Business Conduct Hotline available for employees to report issues. The hotline is accessible 24 hours per day and 7 days per week through email, phone, fax, and mail. The individual may also send a letter or fax reporting the concern to Microsoft's Director of Compliance. Employees are instructed that it is their duty to promptly report any concerns of suspected or known violations of the Code of Professional Conduct, the SBC, or other Microsoft policies or guidelines. The procedures to be followed for such a report are outlined in the SBC and the Whistle Blowing Reporting Procedure and Guidelines in the Employee Handbook. Employees are also encouraged to communicate the issue to their manager, their manager's manager, their Corporate, External, and Legal Affairs (CELA) contact, their Human Resources (HR) contact, or the Compliance Office.

Hiring

Microsoft hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities involved in the job, background characteristics needed to perform the job, and personal characteristics required. Once the requirements are determined, managers create a job description, which is a profile of the job, and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and to make appropriate hiring decisions.

Background Checks

Due to international regulations prohibiting background checks, international employees are exempt from the background check process. For US citizens, backgrounds checks are required before full-time employees and vendors are granted access to the corporate network. Background checks are valid for two years.

Microsoft full-time employees request background checks, when necessary, through the Office Substrate Pulse (OSP) employee portal. A notification is sent to the requesting employee's manager for approval. If approved,

a notification email is sent to Microsoft HR to process a background check for the requesting employee. When the background check is complete, HR enters the results into Employee Cloud Screening (ECS).

Vendors/Contractors: Vendor companies are responsible for providing Microsoft with evidence showing that a valid background check has been performed for each contracted vendor. Once completed, Microsoft receives an attestation letter from the vendor company confirming the validity of the vendor's background check. Once the background check validation is received, Microsoft HR enters relevant information into ECS.

Workload administrators configure requirements, including background check, for eligibilities within each work stream. If no background check is on file, or if a background check has expired, the user receives an error indicating that the employee does not have required background check, thus preventing the employee or vendor from obtaining those eligibilities.

Training

ICCS and ICP leverage the Microsoft Corporate SBC to provide employees with education and resources to make informed business decisions and act on their decisions with integrity. SBC training and awareness is provided to Microsoft employees, contractors, and third parties on an ongoing basis to educate them on applicable policies, standards, and information security practices. Full-time employees must also take a mandatory SBC training course within the first 60 days of their start date and then again on an annual basis thereafter.

In addition, ICCS and ICP personnel are required to participate in Microsoft's mandatory security and privacy trainings including Security 101 and Privacy 101 at a minimum on an annual basis.

Accountability

All ICCS and ICP staff and contingent staff are accountable for understanding and adhering to the guidance contained in the Microsoft Policies and applicable supporting standards. Individuals not employed by these Iris services, but allowed to access, manage, or process information assets of the system are also accountable for understanding and adhering to the guidance contained in the Microsoft Policies and applicable supporting standards.

Performance Reviews

Microsoft employees create individual Core Priorities that align with those of their manager, organization, and Microsoft, and are supported with customer-centric actions and measures so that everyone is working toward the same overarching vision. These Core Priorities are established when an employee is hired, and then updated throughout the year according to business needs.

Periodically, performance reviews, called "Connects", are held between employees and their managers, during which progress is analyzed against accountabilities and accountabilities are adjusted, if needed. The manager evaluates the individual's contributions to the team and business or customer impact, taking into consideration contributions towards creating a high performing team and the demonstration of competencies relevant to their role, which can include an individual's internal control responsibilities.

Microsoft organization guidance requires that "Connects" be performed a minimum of two times a year; however, each group may adjust the timing of these reviews throughout the year to coincide with its business processes.

OLC - Board of Directors and Senior Leadership

The OLC designs and provides reports to the Board of Directors on compliance matters. The OLC also organizes annual meetings with the Senior Leadership team for its compliance review.

Internal Audit Department

Microsoft has an Internal Audit (IA) department that reports directly to the Audit Committee (AC) of the Board of Directors, which is constituted solely of independent directors. IA has a formal charter that is reviewed by the AC and management. The responsibilities of IA include performing audits and reporting issues and recommendations to management and the AC.

Audit Committee

The AC charter and responsibilities are communicated on Microsoft's website, www.microsoft.com. The AC meets privately on a quarterly basis with Microsoft's external auditors and IA. The topics for the quarterly AC meetings are found in the AC Responsibilities Calendar sent out in the charter. In addition, the AC influences the company through the IA function. The AC reviews the scope of IA and advises on the process of identifying and resolving issues. Lastly, the AC monitors itself by completing an annual self-evaluation.

Information and Communication

Internal Communication

Responsibilities concerning internal control are communicated broadly, which includes monthly Controller calls, All Hands Meetings run by the Chief Financial Officer (CFO), and update conference calls held by the financial compliance group with the Sarbanes-Oxley extended project team. Responsibilities for compliance with policies are set out in the SBC for which mandatory training has been stablished for all employees. Additionally, compliance manager meets with the control owners to make sure they understand the controls for which they are accountable and update the controls based on changes in the business environments.

Office of the CFO – Communications External to the Company

CFO communications outside the company occur throughout the year and, where applicable, these external communications include discussions of the company's attitude toward sound internal controls. The office of the CFO is responsible for a few communications outside of Microsoft including quarterly earnings releases, financial analyst meetings, customer visits, outside conferences, and external publications.

Policies

All ICP and ICCS and contingent staff are accountable for understanding and adhering to the guidance provided in Microsoft policies and applicable supporting standards. These policies define accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification, asset management, risk assessment, access control, incident response, business continuity, cryptography, system development, training, and where to go for additional information. These policies are available on the Microsoft intranet.

In addition to the Microsoft-wide Security Policy, the Commerce Engineering Compliance, Governance Risk and Compliance (CEC GRC) team has established the change management policy, which is communicated to the ICCS and ICP team members via CEC GRC's SharePoint site.

Business Planning

The ICCS and ICP planning process is driven by product requirements from our internal partners, specifically for use by commercial workloads (e.g. Office 365 business SKUs). Senior management defines the vision and strategy for the overall Iris product on an annual basis. During this process, senior management considers its high-level commitments and requirements to security and confidentiality in a series of planning meetings and communicates the output to ICP and ICCS teams through email announcements and all-hands meetings. ICP and ICCS's Engineering and Program Management Team Leads also consider their teams' commitments to security and confidentiality on a more specific level, and translate the outcome into scenarios, deliverables and tasks in iteration (RS) planning meetings. Finally, a CEC GRC team has been defined and provides guidance for managing compliance related to security, confidentiality, and availability controls within the ICP and ICCS environments. Each team works to implement and maintain the commitments for security, confidentiality, and availability.

Customer Commitments and Responsibilities

ICP and ICCS communicate their commitments, including those related to security, confidentiality, and availability to their Microsoft-internal customers via email announcements and meetings.

Communication

Information regarding the design and operation of ICP and ICCS including a description of the system, the system's boundaries, roles and responsibilities of internal users, and resources is available on the Microsoft intranet (SharePoint sites). In addition, system description details are available through third-party audit and attestation reports.

System Description

ICP and ICCS (Push Platform APIs are the only systems in scope for SOC 2)

The push platform operates on the list of anonymized user identifiers, provided by Segmentation and the campaign metadata defined in Iris Studio. A campaign worker process calls the ICCS API for each of these

identifiers. Before any further processing, ICCS checks whether there is a delete request for the user identifier in compliance with the European Union's General Data Protection Regulation (GDPR).[2]

If there is a delete request, the identifier is not further processed, and the email interaction request is discarded.

Next, ICCS observes the Frequency Cap[3] table, suppressing the request if the frequency capping criteria is met. Then, ICCS resolves the end-user identifiable information (EUII) such as the email address, first name, last name associated with the anonymized identifier by calling the Customer Master API which in turn calls the Microsoft Online Directory Services (MSODS)[4] to resolve commercial the end-user EUII attributes from Azure Active Directory.

Next, ICCS calls the ICP API with the end-user data enriched information. As a first step, ICP adds the request to an Azure queue. Working off this queue, ICP checks the centralized Contact Permissions Master (CPM) — using the anonymized identifiers — to establish if Microsoft is permitted to send the type of communication that was defined in the campaign metadata (a.k.a. the "topic") to the intended recipient.

If it has been established that the recipient is contactable for the campaign topic, the ICP service processes the request and passes the information to the downstream mailing system configured for the campaign. Entries that are successfully processed are dequeued. If the recipient is not contactable for a given topic, the request is suppressed and dequeued. In case a request fails for any reason, the system will retry the request. However, all requests that haven't been successfully processed within 48 hours will expire.

Delivered, suppressed, or expired requests are logged in the application-level logs using a correlation ID, which is entirely devoid of any commercial personal information and other restricted data.

Supporting Services

The following services are used in a canonical campaign scenario but do process or operate on commercial customer content.

Iris Studio

Iris Studio is a user interface to define campaigns, set up email interactions, and to create the metadata that defines the characteristics of the audience that should receive the email notifications. No end-user identifiable information or other restricted customer content is processed or accessed by Iris Studio.

Segmentation

The segmentation platform pre-computes the audience based on metadata defined in Iris Studio by querying the data source that was selected in Iris Studio. No end-user identifiable information or other restricted customer content is processed or accessed by Iris Segmentation.

Campaign Service

The Campaign Service takes the inputs from Iris Studio and Segmentation and passes these to ICCS at the scheduled time through the Campaign Worker process.

Iris Insights

Authorized staff can view reports on the performance of email campaigns through the Iris Reporting and Insights service. These aggregated reports are based on data that is free of personal data and are created by correlating the application-level log entries generated by ICP and ICCS with the telemetry logs from the mailing system using correlation IDs.

---

2 For more info on GDPR see https://aka.ms/gdpr

3 Frequency cap is a data table that is used to determine whether a user has already received a type of email interaction within a certain time frame. This timeframe is passed as part of campaign metadata and the information is stored against anonymized identifiers.

4 MSODS stands for "Microsoft Online Directory Services", a globally distributed directory, which includes the graph API used to retrieve the user attributes required by Iris to send email

Dataflow Diagram

The following system diagram depicts in-scope ICP and ICCS services as well as the key supporting services, the data flow, and sequence of events:

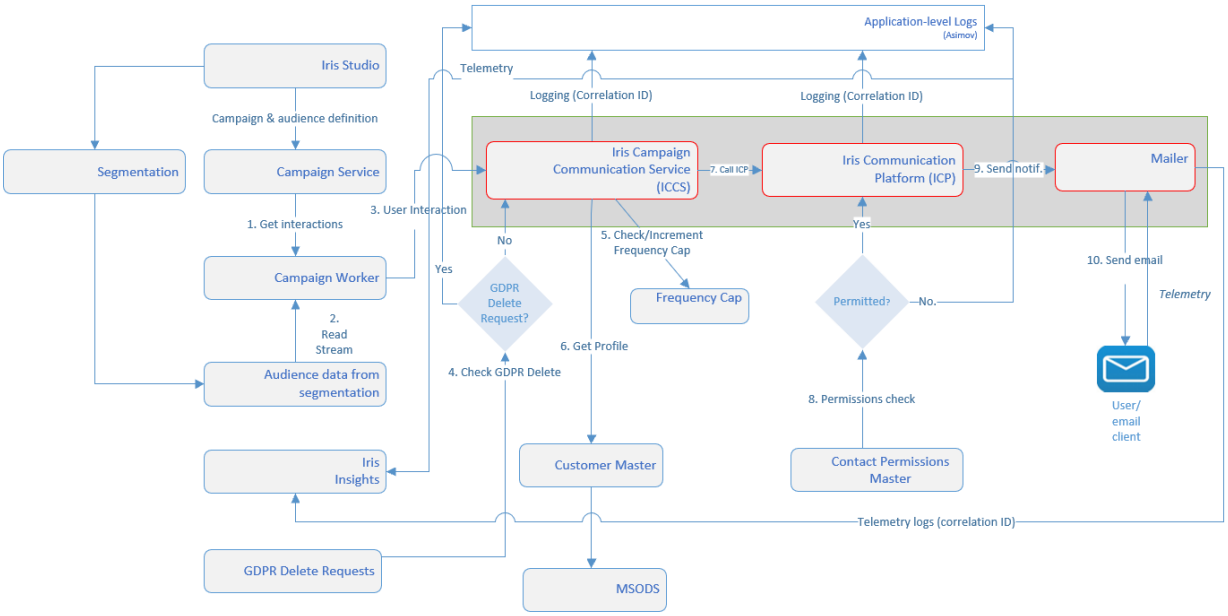

Figure 1: Diagram showing the two APIs called "Iris Campaign Communication Services (ICCS) and "Iris Communication Platform" and the email platform (a capability provided by Salesforce Marketing Cloud)— as well as supporting services. System component in scope for this SOC 2 report are outlined in dark grey.

Risk Assessment

Enterprise Risk Management (ERM) Risk Assessment

The Microsoft Enterprise Risk Management (ERM) team provides management and accountability of Microsoft short- and long-term risks. ERM collaborates with Internal Audit, the Financial Compliance Group, Operations, and Legal and Compliance groups to perform a formal risk assessment. These risk assessments include risks in financial reporting, fraud, and compliance with laws.

Internal Audit (IA) Risk Assessment

IA and other groups within Microsoft perform periodic risk assessments. These assessments are reviewed by senior management. IA specialization area leaders determine high-priority risks across the company, including risks related to financial reporting, operational business processes, and systems controls. Control failures are also analyzed to determine whether they give rise to additional risks.

Commerce Engineering Compliance (CEC) Risk Assessment

In addition to the above Microsoft-wide risk assessments, CEC GRC conducts a risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality and availability commitments specific to the organization. Risks that are identified are reviewed and approved by Commerce Engineering management at least quarterly. In addition, risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis. The results from this risk assessment are rolled into the company-wide risk assessment owned by ERM defined above.

OLC/IA/ERM – Risk Responsibility

The responsibility for risk is distributed throughout the organization based on the individual group's services. OLC, IA, and the ERM team work together to represent enterprise risk management across the company. Through quarter and year-end reviews, the CFO, and Corporate Controller (and respective groups) review the disclosures and issues that may have arisen.

Control Design and Implementation

Based on the risk assessment performed, control activities are put in place within the ICCS and ICP control frameworks. The control frameworks are managed by the CEC GRC group and evaluated at least on an annual

basis. This evaluation includes input from changes to the overall ICP or ICCS environment, the regulatory landscape, and results of control assessments.

Software Development Lifecycle (SDLC Process)

ICP and ICCS follow the standard Microsoft Software Development Lifecycle. The Microsoft SDLC includes the following requirements:

- Project Requirements/Design
- Implementation
- Testing Verification
- Final Approval

Based on established plans for product releases and specifications, features are developed and designed for release. There is an assigned feature crew for each service that includes developers and program managers. Feature crews propose changes, which are submitted for approval by the applicable stakeholders. Features are developed and tested according to the SDLC. Prior to releasing a new feature, the feature must be approved by a Level 65+ level team member and a Technical Lead, which can be the same individual in certain circumstances. If approved, signifying that the release has passed all appropriate testing and that it meets the specifications and requirements, the feature is scheduled to be automatically deployed into the production environment for the ICP and ICCS systems.

Secure Development Lifecycle

ICP and ICCS follow the standard Microsoft Secure Development Lifecycle (SDL) process which includes, at a minimum, risk assessment, testing, approval, and documentation. The SDL process includes security and confidentiality development requirements, which are intended to reduce the number of security-related bugs that appear in the design, code, and documentation associated with a software release, as well as to detect and remove those bugs as early in the SDLC as possible.

For any major change in the system, a risk assessment is performed by CEC GRC and the Microsoft Legal team. Security review is performed by CDG (Cosine, Devices, and Gaming) security. The software development lifecycle is followed for the development, build and test processes. The end-to end process is tracked through Visual Studio Team Services (VSTS).

Source Code Control

The ICP and ICCS code is stored within Microsoft’s instance of VSTS. Access to check in the source code is limited to authorized personnel. In addition, write access to the source code repository is reviewed quarterly.

Asset Management

ICP and ICCS maintain an inventory of Azure subscriptions, service descriptions, and owners through Microsoft's corporate asset management tool, Service Tree. An inventory of all resources residing within each Azure subscription is maintained within the Azure Portal. User access to the Azure subscriptions and services is restricted to appropriate personnel and reviewed quarterly.

Access Management

Access to ICP and ICCS services, data stores, related code base, and deployments must be authorized, conform to Microsoft's access management policies and procedures, and aligned with the Role-Based Access Control (RBAC) Model. RBAC model is implemented within ICP and ICCS systems to enforce the concepts of least-privileged access and the segregation of incompatible duties.

Authentication

ICP and ICCS systems use the Microsoft instance of Azure Active Directory (AAD), which is the corporate active directory infrastructure for centralized authentication and authorization to the systems.

Identity Access Management

ICP and ICCS leverage the Microsoft corporate instance of Microsoft Identity Manager, referred to as IDWEB, which is managed by the Microsoft Core Services Engineering (CSE) group. This tool is leveraged to enforce role-based access (RBAC) permissions and least privilege within the ICP and ICCS environments using AAD security groups.

New User/Modification of User Access

The process to request and to approve new access to ICP and ICCS environments is managed through a manual workflow process by adding users to security groups. Once a user requests access to a security group through IDWeb, the IDWeb automatically notifies the appropriate security group approvers via email that a request is pending for approval. Once the approver approves the request, the tool automatically assigns the user the appropriate membership for that security group.

Termination User Access Removal

When individuals leave the company, Microsoft HR updates the terminated employee's details in the HR system. Through an automated batch process, the terminated employee's access is removed from the Microsoft corporate network and corresponding security groups within 24 hours.

Role change User Access Removal

In the specific case of a team member changing roles within the team or within Microsoft, the team member will be removed from security groups they no longer should be part of within 10 business days.

Periodic User Access Review

Periodic reviews of individual accounts and security group memberships within the ICP and ICCS environment are performed by the ICP and ICCS leads quarterly, to evaluate whether access is still required and appropriate. Any necessary remediating action is taken in a timely manner, as necessary, based on the review.

Just-in-Time Access

Just-in-time (JIT) tools allow individuals to request temporary elevated access privileges on an as-needed basis to privileged areas within the ICP and ICCS production environments. The JIT approvers will review the access request and approve if appropriate. When approved, the requesting user is granted access to the production environment on a temporary basis, typically for under 24 hours, as defined in the request itself, and the tool automatically removes the requested access upon expiration. In general, JIT requestors cannot approve their own individual access. In cases of emergency, principal-level team members that are authorized to request access as well as approve access, can grant their own requests, but will seek additional approval from another authorized approver within 24 hours of the incident.

Developer / Operations Model – Developer Access to Production

ICP and ICCS developers can get temporary access to production using the JIT tools described above. Developer access is limited to specific areas of the environment for operations purposes, such as troubleshooting. Automated configurations are in place within the ICP and ICCS deployment and source code management tool, VSTS, to enforce multiple levels of code-review and approval prior to deploying a change to production. The objective of these controls is to prevent inappropriate changes from being applied to production.

Mobile Devices

For Microsoft employees and other internal users, access to the ICP and ICCS system via mobile device is restricted and the corresponding controls are managed by Microsoft's Core Services Engineering (CSE) organization.

Logical Security

Encryption

Encryption of Commercial Personal Data in Transfer

Restricted data, which in the case of ICP and ICCS is limited to the end-user identifiable information (commercial personal data) necessary to send the notification to the right addressee, is encrypted when transmitted between Microsoft data centers and to the approved mailer/sender, in accordance with Microsoft Security Program Policy (MSPP).

Microsoft leverages Secure Sockets Layer and Azure for establishing an encrypted link between data centers. The encryption protocol is applied in accordance with the MSPP.

Microsoft uses Transport Layer Security for establishing an encrypted link between the ICP and any external mailing applications. At the time of writing, the only mailing application used by our internal partners in conjunction with the covered ICP and ICCS services is Exact Target, a part of Salesforce Marketing Cloud. For Exact Target, a specialized enterprise instance is used that enforces Encrypted Data Sending (EDS).

Using EDS, any data field containing personally identifiable information is encrypted by Microsoft before transmission, ensuring that operators within Exact Target cannot see any personally identifiable data at any time. Only at send time, the data will be decrypted by the underlying mail system.

Encryption of Restricted Data at Rest

ICP leverages Azure to enable the encryption of restricted data at rest within Azure Storage. All data that is written into Azure Storage is automatically encrypted using 256-bit AES encryption, which meets the requirements within the MSPP.

Key Management

ICP and ICCS adhere to Online Services Security Standards (OSSS) for encryption key management. If the content of this policy conflicts with any other Microsoft Security Policy, the stricter of the policies apply.

Any certificates, account secrets, and keys are securely encrypted and stored in PilotFish Secret Store. The encrypted keys are stored in the PilotFish Source Depot and all copies of the key are immediately deleted. Access to decrypt the keys is restricted to authorized personnel and systems.

To ensure compliance with key management, credential monitoring is used to identify a breach in key confidentiality. The production environment uses different encryption keys than those found within Development and/or Test environments.

Encryption keys are rotated on a periodic basis in accordance with OSSS. Where these standards conflict with the Microsoft Security Policy, the stricter of the policies are applied to ensure proper and effective use of cryptographic confidentiality.

In addition to the PilotFish Secret Store, ICP uses Azure Key Vault. The Azure Key Vault is used to store the credentials issued to ICP needed to authenticate with the third-party mailing system.

Azure Virtual Machine Scale Sets

Both ICP and ICCS leverage EAP[5] V2 to deploy the services to PilotFish, using Yabby[6] for cloud deployment automation.

Antivirus/Antimalware

ICP and ICCS leverage Azure's PilotFish service to automatically provision all servers with an operating system (OS) image that includes the System Center Endpoint Protection ("SCEP") antivirus/antimalware service. This OS image is applied to the entire Azure VM scale set automatically. The antivirus/antimalware agent is configured to obtain the latest available definition from Azure.

Patch Management

ICP and ICCS both leverage Azure's PilotFish service to enforce patch management for the VM scale set. Autopilot[7]-managed servers run a Windows Server Enterprise SKU as the base OS image. The OS images for all Autopilot managed machines are created, managed, and supported by Autopilot. The Autopilot team is responsible for these OS-related processes, including the base OS image creation and the upgrade of all ICP and ICCS machines into the newly available OS image. This includes upgrading to major OS versions as well as to incremental releases such as service packs and patches.

Vulnerability Scanning and Security Monitoring

Microsoft's CDG Security Operations team uses Qualys to monitor assets and assess vulnerabilities across the CDG organization, including the ICP and ICCS systems. To ensure that ICP and ICCS are appropriately monitored for security vulnerabilities, the CDG Threat Vulnerability Monitoring (TVM) Qualys agent is installed on all ICP and ICCS virtual machines. In addition to Qualys, Microsoft's CDG Security Operations Team leverages additional telemetry collection in the Azure Cloud to identify and monitor operating system related security events. The ICP and ICCS teams periodically review the vulnerability scan report from the CDG Security Operations team, assesses the criticality of the vulnerabilities, and resolves vulnerabilities when

---

5 EAP stands for Elastic Autopilot, and Autopilot version that runs on top of Azure Virtual Machines

6 Yabby is a Microsoft internal service that facilitates the deployment of code to Azure clouds.

7 Autopilot manages datacenter capacity & service quality at internet scale for Microsoft.

appropriate. Additional vulnerability scanning is performed through Azure via the PilotFish service, in which well-known OS and application vulnerabilities are scanned monthly.

Network Management

ICP and ICCS leverage Azure to ensure appropriate controls are in place to protect the network-layer, including but not limited to: Incident Management, Configuration Management, Access Management, and Change Management for network resources.

Data Flow Diagrams

On an annual basis, the system data flow diagrams are reviewed and updated by ICP and ICCS engineering teams with input from the CEC GRC team. This review is performed to provide up to date ICP and ICCS system design information to personnel to support their understanding of their role in addressing security and confidentiality within the systems.

Capacity and Availability Monitoring

Processing capacity and availability are monitored by Service teams through a centralized dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed.

In addition to the above monitoring, on a quarterly basis, Iris teams prepare an overview of the service team's capacity, availability, and resiliency from the prior month for the Iris senior management team. This overview presents the root cause of anomalies or deviations, and based on the meeting, issue remediation plans or changes to capacity and availability are tracked to resolution. Annually, Iris senior management reviews and approves the capacity for Iris and its systems.

Monitoring of Control Health

Security and Compliance Monitoring

ICP and ICCS maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect restricted data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.

The design and operating effectiveness of security, confidentiality, and availability controls are analyzed by independent auditors at least annually. These assessments include external (e.g. SOC2 audits) and internal evaluations (e.g., risk assessments and vulnerability scans). The results and findings from these assessments are addressed with corrective actions, which are tracked by the CEC GRC team to substantiate that they are addressed in a timely manner.

Internal Audit

Microsoft's IA department provides support to management across the company by independently and objectively analyzing whether the objectives of management are adequately performed, as well as facilitating process improvements and the adoption of business practices, policies, and controls governing worldwide operations.

Monitoring of Subservice Organizations

Microsoft ICP and ICCS use the following subservice organizations:

- Microsoft Azure: provides the PaaS services for the ICP and ICCS systems including authentication (AAD) virtual server hosting, and data storage, as well as the physical servers, patch management, and network infrastructure that support those services
- Salesforce Marketing Cloud (formerly ExactTarget): provides e-mail management, delivery, and analytics

The ICP and ICCS teams are responsible for identifying dependencies of each service and monitoring the subservices implementation of agreed-upon security and confidentiality controls. Monitoring includes, but is not limited to, the review of third-party service auditor reports, analyzing the impact of identified deficiencies, evaluating complementary user entity controls (CUECs) and discussions with subservice organization management, where necessary.

Business Continuity and Disaster Recovery

Microsoft has established an organization-wide Enterprise Business Continuity Management (EBCM) framework. The program includes Business Continuity Policy, Implementation Guidelines, Business Impact Analysis (BIA), Risk Assessment, Dependency Analysis, Business Continuity Plan (BCP), Incident Management Plan, and procedures for monitoring and improving the program. The BCM Program Manager also manages the

program for the Azure. Azure datacenter Service Resiliency (SR) program is coordinated through the datacenter SR Program Management Office to ensure that the program adheres to a coherent long-term vision and mission, and is consistent with enterprise program standards, methods, policies, and metrics.

All Datacenters are required to at least annually, exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption.

Data Replication

Data for the Iris system is replicated for redundancy and disaster recovery purposes by Azure. Data redundancy is achieved through fragmentation of data into extents which are copied onto multiple nodes within each used Azure region.

Confidentiality

Any commercial personal data, such as the end-user identifiable information that is processed by ICCS and ICP, is considered confidential in nature and is protected accordingly.

When an email interaction request which includes end-user identifiable information of the intended recipient is processed through the system, it is temporarily queued in an Azure Queue for the minimum required time for the downstream mailer system to receive the information before being dequeued and deleted. However, this time never exceeds 7 days, the default maximum time-to-live for the Azure Queue. After that period, any data still in the Queue is automatically purged and the purge is logged. While queued, the data is encrypted using Azure Storage SDK client-side encryption.

In addition, when an email message request has a big payload size, message extensions are temporarily stored in Azure Blob Storage along with end-user identifiable information of the intended recipient. This again is encrypted by Azure encryption and purged after a maximum of 7 days, in this case explicitly by ICP, and this delete/purge is logged.

Logging

Any logging that happens at the application level is stored against a Correlation ID that is associated with the request. Any log events are free of personally identifiable information or other restricted data.

Software

This report applies to the Iris Push Services APIs ICP and ICCS. In addition to the product software, the following utility software is used by the team to execute controls relevant to the Iris Push Services system:

- **Elastic Autopilot (EAP) -** Autopilot is a datacenter capacity & service quality management application that is part of Azure used by internal Microsoft teams. Elastic Autopilot V2 runs on Azure VMs.
- **IDWeb -** Microsoft's corporate instance of Microsoft Identity Manager. The tool is leveraged to enforce role-based access permissions and least privilege within the ICP and ICCS environments using AAD security groups.
- **PilotFish –**Both ICP and ICCS leverage PilotFish, an Azure service which provides an Autopilot cluster co-located with Azure in every Azure data center. By leveraging PilotFish, ICP and ICCS are able to automate the setup and pre-configuration of new devices within the respective environments. PilotFish is also used to perform vulnerability scanning and patch updates.
- **Azure DevOps -** Automated configurations are placed within the ICP and ICCS source code repository, build, and release management tool, Azure DevOps (formerly Visual Studio Team Services), to enforce multiple levels of code-review and approval prior to deploying and tracking a change to production.
- **xPert -** Incident management monitoring agent that resides on the ICP/ICCS environments. Alerts are customizable to take the necessary steps towards remediation in the case of an event.
- **IcM -** Ticketing tool that resides as a part of the xPert incident management monitoring tool. Incident tickets are created with severity and remediation steps in the case of an event.
- **XTS -** XTS is a tool to manage AP services and includes the functionality to provide Just-in-Time access requests to the ICP and ICCS production environments. JIT access through XTS has a time limit, requires principal-level management approval and is limited to a single virtual machine per request.

- **CodeFlow –** A tool integrated with PilotFish that enforces reviewers to be assigned to a specific code change for review
- **Yabby -** A Microsoft internal service that facilitates the deployment of code to Azure clouds.

  CredScan - Code scanning task to harden security by checking for auth info checked in as part of the code and alert findings.

People

ICP and ICCS personnel are organized into service teams that develop and maintain the application and support teams that provide services for system operations.

Each service and support team has defined responsibilities and accountabilities related to the security and confidentiality of the applications. The teams include the following groups:

- Access Security – includes personnel that maintain Windows Active Directory (AD) services, authentication rules, and user access.
- Change Management – includes development, testing, and project management teams tasked with developing and maintaining the CEC applications and support services.
- Backups and Replication – includes personnel for configuring and monitoring the replication and backup of specified internal and customer content, per customer commitments.

In addition to service teams, centralized support teams provide specialized functions for the services, including the following:

- Business Continuity Management – Provides a single resource to assist Store teams in analyzing continuity and disaster recovery requirements, documenting procedures, and conducting testing of established procedures for the business continuity and disaster recovery of the services.
- CDG Security – Manages cross-platform security functions, such as security incident response, security monitoring, and vulnerability scanning.
- Governance, Risk, and Compliance (GRC) – Identifies, documents, and advises teams in implementing controls to maintain availability and security commitments to its customers.
- Azure - Provides customer authentication infrastructure including Microsoft Online Directory Services (MSODS), Microsoft Organization ID, and Azure Active Directory

Procedures

Iris Services adhere to Microsoft's Security Policy that is owned by the Information Risk Management Council (IRMC), comprising business and security leaders across the company, and approved by the IRMC chair, who is also the Chief Information Security Office (CISO) for Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses:

- Human resources security
- Access control
- Physical and environmental security
- Communications security
- Compliance
- Supplier relationships
- Business continuity management
- Asset management
- Cryptography
- Operations security
- Systems acquisition, development, and maintenance
- Information security incident management

Iris Services use NIST standard 800-53 for baseline control procedures, which are documented in the CEC GRC framework. Control measures above and beyond NIST 800-53 are included to address the full range of Microsoft contractual and regulatory commitments. The framework covers the following areas:

- Access Control
- Accountability, Audit, and Risk
- Authority and Purpose
- Awareness and Training
- Configuration Management
- Contingency Planning
- Data Minimization and Retention
- Data Portability
- Data Quality and Integrity
- Geographic Boundaries
- Identification and Authentication
- Incident Response
- Individual Participation and Redress
- Maintenance
- Media Protection
- Personnel Security
- Physical Access
- Program Management
- Risk Assessment
- Security
- Security Assessment
- Security Planning
- System Access
- System and Communication Security
- System and Information Integrity
- System and Services Acquisition
- Use Limitation

Complimentary User Entity Control Considerations (CUECs)

Microsoft's Iris ICCS and ICP systems, and the controls over these systems, were designed with the assumption that certain controls are in operation within the user entity organizations. This section describes those controls that should be in operation at user entity organizations to complement the controls of Iris ICCS and ICP. The following list contains controls that Iris ICCS and ICP assume their user entities have implemented. User organization auditors should determine whether the user entities have established sufficient controls in these areas:

Complementary User Entity Controls	Relevant SOC 2 Control Criteria
CUEC-01: User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.	**CC6.1, CC6.2, CC6.3**

Complementary Subservice Organization Controls (CSOCs)

Microsoft's Iris ICCS and ICP controls related to the system detailed in this report cover only a portion of overall internal control for each user entity of Iris ICCS and ICP. It is not feasible for the related control criteria to Iris ICCS and ICP to be achieved solely by Microsoft. Therefore, in conjunction with Iris ICCS and ICP's controls, a user entity must take into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as follows.

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant SOC 2 Control Criteria
Platform as a Service (PaaS) logical access	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting Iris ICCS and ICP.	**CC6.6**
Platform as a Service (PaaS) change management	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over physical access to the facilities, including data centers, supporting ICCS and ICP.	**CC6.4, CC6.5, and CC6.7**
Platform as a Service (PaaS) physical security	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over protection of the network environment, including perimeter firewalls and restricting access to network devices.	**CC6.7**
Platform as a Service (PaaS) physical security	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over environmental protection of systems, including natural disasters and man-made threats, for infrastructure supporting ICCS and ICP.	**CC6.7**

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant SOC 2 Control Criteria
Platform as a Service (PaaS) physical security	Microsoft Azure	Microsoft Azure is responsible for monitoring and addressing security events and incidents related to the ICCS and ICP systems hosted on Azure platform services.	**CC7.3**
Platform as a Service (PaaS) physical security	Microsoft Azure	Microsoft Azure is responsible for controlling that all Datacenters are required to at least annually, exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption.	**CC7.5 and A1.3**
Platform as a Service (PaaS) data security	Microsoft Azure	Microsoft Azure is responsible for the encryption of data at rest and data in motion for ICCS and ICP systems hosted on Azure platform services.	**CC6.1, CC6.6, CC6.7 and C1.1**
Platform as a Service (PaaS) physical security	Microsoft Azure	Microsoft Azure is responsible for geographic replication and backups for ICCS and ICP systems hosted on Azure platform services.	**CC7.2 and A1.2**
Platform as a Service (PaaS) physical security	Microsoft Azure	Microsoft Azure is responsible for the maintenance and change management of the infrastructure and supporting systems that support their platform as a service where ICCS and ICP are hosted.	**CC6.5, CC7.1, and CC8.1**
Platform as a Service (PaaS) network security	Microsoft Azure	Microsoft Azure is responsible for antimalware protection related to the ICCS and ICP systems hosted on Azure platform services.	**CC6.1, CC6.6, CC6.8, CC7.1, and CC7.2**
Platform as a Service (PaaS) network security	Microsoft Azure	Microsoft Azure is responsible for the encryption of the Remote Desktop Connection used for administrator access to the ICCS and ICP systems hosted on Azure platform services.	**CC6.6 and CC6.7**
Platform as a Service (PaaS) network security	Microsoft Azure	Microsoft Azure is responsible for network filtering implementation to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components.	**CC6.6 and CC6.7**
Software as a Service (SaaS) physical security	Salesforce Marketing Cloud	Salesforce Marketing Cloud is responsible for maintaining controls over physical access to the facilities, including data centers, supporting ICCS and ICP.	**CC6.4, CC6.5, and CC6.7**
Software as a Service (SaaS) physical security	Salesforce Marketing Cloud	Salesforce Marketing Cloud is responsible for maintaining controls over protection of the network environment, including perimeter firewalls and restricting access to network devices.	**CC6.7**
Software as a Service (SaaS) physical security	Salesforce Marketing Cloud	Salesforce Marketing Cloud is responsible for maintaining controls over environmental protection of systems, including natural disasters and man-made threats, for infrastructure supporting ICCS and ICP.	**CC6.7**
Software as a Service (SaaS) physical security	Salesforce Marketing Cloud	Salesforce Marketing Cloud is responsible for monitoring and addressing security events and incidents related to their Software-as-a-Service supporting ICCS and ICP.	**CC7.3**
Software as a Service (SaaS) physical security	Salesforce Marketing Cloud	Salesforce Marketing Cloud is responsible for the maintenance and change management of the infrastructure related to their Software-as-a-Service supporting ICCP and ICP.	**CC6.5, CC7.1, and CC8.1**
Software as a Service (SaaS) network security	Salesforce Marketing Cloud	Salesforce Marketing Cloud is responsible for antimalware protection over their Software-as-a-Service supporting ICCS and ICP.	**CC6.1, CC6.6, CC6.8, CC7.1, and CC7.2**

Principal Commitments and Requirements

Microsoft makes commitments and has established requirements for its products and services. The principal commitment for Iris ICCS and ICP is to conform to internal organizational commitments for products and services to create a consistent level of compliance across all Microsoft environments. These commitments include the areas of logical and physical access security, system operations, change management, risk mitigation, and availability that are met through this report. These internal commitments when met, allow the Iris ICCS and ICP environments to interact with other environments across Microsoft in a compliant manner.

Trust Services Criteria and Control Activities provided by Microsoft

Criteria Common to All Security, Availability, and Confidentiality Principles

CC1.0 – CONTROL ENVIRONMENT

Criteria	IRIS Control Activity
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	**CCL-01** – Iris has implemented Microsoft governance policies reflecting requirements of the current business, regulatory and compliance environments. The policies are reviewed and approved at least annually or more frequently, as necessary. **CCL-02** – On an annual basis, Office of Legal Compliance (OLC) reviews the Standards of Business Conduct and updates the standards as necessary. The Code is made available to all employees internally on CELAWeb and externally at microsoft.com/compliance. **CCL-03** – Values are accessible to employees via the Values SharePoint site. The Values govern employees' interactions in their workgroup, across teams, with partners, and with customers. **CCL-117** – OLC provides an annual Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	**CCL-05** – The Audit Committee (AC) reviews its Charter and Responsibilities as listed in its calendar on an annual basis. The AC responsibilities include meeting privately with the external and internal auditors on a quarterly basis; reviewing and discussing the Company's quarterly financials; and completing an annual self-evaluation. **CCL-28** – Internal Audit Charter directs them to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment. **CCL-30** – Internal Audit has open access to the Audit Committee members and attends regular meetings with the Audit Committee to maintain a close working relationship and adheres to professional standards of conduct.

Criteria	IRIS Control Activity
CC1.3 - COSO Principle 3: Management establishes with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	**CCL-07** – MS Policy enables users to access documents such as policies and guidelines quickly via a central repository. Unifying the location of the policies is designed to provide users with greater access to consistent information and powerful search capabilities. Policies are defined by function, region, and product, as needed. In addition, there are over-arching corporate policies that apply for the extended enterprise (i.e., anti-corruption, confidential information, insider trading, whistleblowing, global trade, etc.). Policies are located at the Company's MS Policy SharePoint site and are readily available. Policies are reviewed and approved on an annual basis. **CCL-08** – Iris adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDL policies, Microsoft Mobile Device Security Policy and Standards, Microsoft Policy and Standards related to protection of information asset processed or stored at teleworking sites, Microsoft Privacy policy, Cryptography Standard and Online Services Security Standards (OSSS), Tools and Removable Media Security Procedure which are reviewed and approved on an annual basis or if significant changes occur. These policies are communicated with teams and are available on the intranet. **CCL-15** – Iris has a defined security organization structure for the Information Security Program for security governance, accountability, and oversight. This structure includes clearly defined roles and responsibilities.
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**CCL-09** – Outsourced providers are expected to meet certain levels of skills and experience, depending on role. **CCL-10** – The candidate's job descriptions are created and documented for open positions at Microsoft. Job descriptions include desired candidate competencies and expected job roles and responsibilities. **CCL-11** – Microsoft Human Resources works with organizations and vendor companies to perform a background check on new or transferred US personnel before they are granted access to the Microsoft corporate network. **CCL-118** – Training is provided as needed (i.e., LOB apps, Microsoft Office, etc.). In addition, all outsourced providers are trained to understand and comply with Microsoft's code of conduct. **CCL-119** – Management holds all outsourced service providers accountable to achieving specific deliverables, as outlined in a Statement of Work. **CCL-13** – HR maintains an Employee Handbook and HR Web that orient employees on topics like equal employment opportunity, avenues to raise employee compensation and benefits, employee security, and safety and health. http://hrweb/lifeatmicrosoft/Handbook/Employee **CCL-14** – Annual and Mid-Year Reviews - Employees hold midyear check in discussions with their managers to validate they are on the expected Career Path. They also review their performance against their commitments at that time. Additionally, employees and managers discuss overall performance and results against commitments relative to peers in the organization during the annual performance review. **CCL-15** - Iris has a defined security organization structure for the Information Security Program for security governance, accountability, and oversight. This structure includes clearly defined roles and responsibilities.

Criteria	IRIS Control Activity
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	**CCL-08** – Iris adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDL policies, Microsoft Mobile Device Security Policy and Standards, Microsoft Policy and Standards related to protection of information asset processed or stored at teleworking sites, Microsoft Privacy policy, Cryptography standard and Online Services Security Standards (OSSS), Tools and Removable Media Security Procedure which are reviewed and approved on an annual basis or if significant changes occur. These policies are communicated with teams and are available on the intranet. **CCL-14** – Annual and Mid-Year Reviews - Employees hold midyear check in discussions with their managers to validate they are on the expected Career Path. They also review their performance against their commitments at that time. Additionally, employees and managers discuss overall performance and results against commitments relative to peers in the organization during the annual performance review. **CCL-15** – Iris has a defined security organization structure for the Information Security Program for security governance, accountability, and oversight. This structure includes clearly defined roles and responsibilities. **CCL-16** – A security education and awareness training program has been formally defined and all employees and contractors are required to attend this training on an annual basis. Employees and contractors are made aware of their roles and responsibilities with regard to information security.

CC2.0 - COMMUNICATION AND INFORMATION

Criteria	IRIS Control Activity
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	**CCL-08** – Iris adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDL policies, Microsoft Mobile Device Security Policy and Standards, Microsoft Policy and Standards related to protection of information asset processed or stored at teleworking sites, Microsoft Privacy policy, Cryptography standard and Online Services Security Standards (OSSS), Tools and Removable Media Security Procedure which are reviewed and approved on an annual basis or if significant changes occur. These policies are communicated with teams and are available on the intranet. **CCL-12** – FCG reviews the Section 302 survey responses, the CFO Questionnaire, and the Policies and Controls Matrix responses as they come into the survey tools and assesses their ICFR significance. Survey responses help inform future risk assessments. Also, if deficiencies are identified, remediation may drive change to control activities and progress is monitored and reported to senior management. **CCL-21** – The Office of Enterprise Risk Management (ERM) uses a risk-based approach that factors in management's tolerance for risk in determining how to allocate resources to address entity level risks. When assessing risks, management evaluates the potential significance of risks in each ERM pillar, effectiveness of internal controls and considers the acceptable levels of risk relative to achievement of objectives. The ERM process is driven by a central team that engages with management across the company to identify and manage risks. Where risks exceed acceptable thresholds, remediation plans are developed, and reported to the Board of Directors on behalf of senior management.

Criteria	IRIS Control Activity
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	**CCL-01** – Iris has implemented Microsoft governance policies reflecting requirements of the current business, regulatory and compliance environments. The policies are reviewed and approved at least annually or more frequently, as necessary. **CCL-08** – Iris adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDL policies, Microsoft Mobile Device Security Policy and Standards, Microsoft Policy and Standards related to protection of information asset processed or stored at teleworking sites, Microsoft Privacy policy, Cryptography standard and Online Services Security Standards (OSSS), Tools and Removable Media Security Procedure which are reviewed and approved on an annual basis or if significant changes occur. These policies are communicated with teams and are available on the intranet. **CCL-20** – The company maintains several mechanisms that permit employees and non-employees to communicate confidential and/or anonymous reports concerning Business Conduct. Compliance concerns may be communicated several ways: sending an e-mail to msft.buscond@alertline.com, accessing an external website, www.microsoftintegrity.com and using the web allegation tool to communicate concerns to OLC, calling the Business Conduct Line 24-hour number at 1-877-320-MSFT (6738) or International Toll Free number at 1-704-540-0139, and emailing the Business Conduct and Compliance alias at buscond@microsoft.com. The individual may also send a letter or confidential fax (425) 705-2985 reporting the concern to Microsoft's Director of Compliance. **CCL-21** – The Office of Enterprise Risk Management (ERM) uses a risk-based approach that factors in management's tolerance for risk in determining how to allocate resources to address entity level risks. When assessing risks, management evaluates the potential significance of risks in each ERM pillar, effectiveness of internal controls and considers the acceptable levels of risk relative to achievement of objectives. The ERM process is driven by a central team that engages with management across the company to identify and manage risks. Where risks exceed acceptable thresholds, remediation plans are developed, and reported to the Board of Directors on behalf of senior management.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**CCL-20** – The company maintains several mechanisms that permit employees and non-employees to communicate confidential and/or anonymous reports concerning Business Conduct. Compliance concerns may be communicated several ways: sending an e-mail to msft.buscond@alertline.com, accessing an external website, www.microsoftintegrity.com and using the web allegation tool to communicate concerns to OLC, calling the Business Conduct Line 24-hour number at 1-877-320-MSFT (6738) or International Toll Free number at 1-704-540-0139, and emailing the Business Conduct and Compliance alias at buscond@microsoft.com. The individual may also send a letter or confidential fax (425) 705-2985 reporting the concern to Microsoft's Director of Compliance. **CCL-27** – Effectiveness of the internal controls are assessed by independent auditors on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner.

CC3.0 - RISK ASSESSMENT

Criteria	IRIS Control Activity
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**CCL-21** – The Office of Enterprise Risk Management (ERM) uses a risk-based approach that factors in management's tolerance for risk in determining how to allocate resources to address entity level risks. When assessing risks, management evaluates the potential significance of risks in each ERM pillar, effectiveness of internal controls and considers the acceptable levels of risk relative to achievement of objectives. The ERM process is driven by a central team that engages with management across the company to identify and manage risks. Where risks exceed acceptable thresholds, remediation plans are developed, and reported to the Board of Directors on behalf of senior management. **CCL-22** – Services adhere to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability and process integrity commitments.
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	**CCL-11** – Microsoft Human Resources works with organizations and vendor companies to perform a background check on new or transferred US personnel before they are granted access to the Microsoft corporate network. **CCL-22** – Services adhere to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability and process integrity commitments.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	**CCL-21** – The Office of Enterprise Risk Management (ERM) uses a risk-based approach that factors in management's tolerance for risk in determining how to allocate resources to address entity level risks. When assessing risks, management evaluates the potential significance of risks in each ERM pillar, effectiveness of internal controls and considers the acceptable levels of risk relative to achievement of objectives. The ERM process is driven by a central team that engages with management across the company to identify and manage risks. Where risks exceed acceptable thresholds, remediation plans are developed, and reported to the Board of Directors on behalf of senior management. **CCL-25** – Corporate, External, and Legal Affairs (CELA) reports confirmed or potential fraud matters to external auditors, Deloitte, in the Quarterly Fraud Certification meetings. In addition to the representatives of Deloitte, these meetings are attended by the Corporate VP of Finance, Assistant Corporate Controller, VP Deputy General Counsel for Corporate Finance, CVP of Internal Audit, Senior Director of the Financial Integrity Unit (FIU), and representatives of CELA, including the CVP Deputy General Counsel for CELA Litigation, Competition and Compliance Group and the Director of OLC Investigation. At the meetings, the Microsoft attendees disclose and discuss any matter that may a fall under the 302 definition and confirm that any such matters have been or will be further disclosed by CELA to the Audit Committees of the Board of Directors. **CCL-26** – Anti-Corruption Program Management Office (ACPMO) considers the potential incentives, pressures, attitudes, and the potential opportunities related to different types of anticorruption fraud when evaluating and prioritizing risk. ACPMO's mission is to design, implement and manage an effective global anticorruption program for Microsoft which includes driving business and functional accountability, oversight, monitoring, guidance, training, reporting and the development & coordination of a worldwide community across LCA, Finance, Controls & Compliance, AI/FUI, GPG, RE&F, SMSG and other pertinent organizational partners relative to the company's anticorruption effort. The risk assessment covers the extended enterprise and considers the inherent risks related to outsource service providers. Anticorruption polices can be found at: http://lcaweb/policies/anticorruption/Pages/Anticorruption-landing-page.aspx

Criteria	IRIS Control Activity
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	**CCL-12** – FCG reviews the Section 302 survey responses, the CFO Questionnaire, and the Policies and Controls Matrix responses as they come into the survey tools and assesses their ICFR significance. Survey responses help inform future risk assessments. Also, if deficiencies are identified, remediation may drive change to control activities and progress is monitored and reported to senior management. **CCL-22** – Services adhere to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability and process integrity commitments.

CC4.0 - MONITORING ACTIVITIES

Criteria	IRIS Control Activity
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	**CCL-22** – Services adhere to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability and process integrity commitments. **CCL-27** – Effectiveness of the internal controls are assessed by independent auditors on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner. **CCL-28** – Internal Audit Charter directs them to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	**CCL-22** – Services adhere to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability and process integrity commitments. **CCL-27** – Effectiveness of the internal controls are assessed by independent auditors on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner. **CCL-28** – Internal Audit Charter directs them to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.

CC5.0 - CONTROL ACTIVITIES

Criteria	IRIS Control Activity
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	**CCL-21** – The Office of Enterprise Risk Management (ERM) uses a risk-based approach that factors in management's tolerance for risk in determining how to allocate resources to address entity level risks. When assessing risks, management evaluates the potential significance of risks in each ERM pillar, effectiveness of internal controls and considers the acceptable levels of risk relative to achievement of objectives. The ERM process is driven by a central team that engages with management across the company to identify and manage risks. Where risks exceed acceptable thresholds, remediation plans are developed, and reported to the Board of Directors on behalf of senior management. **CCL-22** – Services adhere to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability and process integrity commitments. **CCL-27** – Effectiveness of the internal controls are assessed by independent auditors on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner.
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**CCL-22** – Services adhere to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability and process integrity commitments. **CCL-27** – Effectiveness of the internal controls are assessed by independent auditors on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner.
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	**CCL-01** – Iris has implemented Microsoft governance policies reflecting requirements of the current business, regulatory and compliance environments. The policies are reviewed and approved at least annually or more frequently, as necessary. **CCL-08** – Iris adheres to Microsoft Security Policy, Physical Security for Assets Standards, Microsoft Access Management, Asset Management, Change Management, Data Management, Security Management, SDL policies, Microsoft Mobile Device Security Policy and Standards, Microsoft Policy and Standards related to protection of information asset processed or stored at teleworking sites, Microsoft Privacy policy, Cryptography standard and Online Services Security Standards (OSSS), Tools and Removable Media Security Procedure which are reviewed and approved on an annual basis or if significant changes occur. These policies are communicated with teams and are available on the intranet. **CCL-16** – A security education and awareness training program has been formally defined and all employees and contractors are required to attend this training on an annual basis. Employees and contractors are made aware of their roles and responsibilities with regard to information security.

CC6.0 - LOGICAL AND PHYSICAL ACCESS CONTROLS

Criteria	IRIS Control Activity
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	**CCL-148** – JIT activity is documented within a VSO or ICM ticket describing the reason for and changes made during the login session. **CCL-167** – Commercial personal data is encrypted within SFMC (Encrypted Data Send). Access to the encryption key is restricted to authorized individuals. **CCL-113** – An anti-malware scanner is integrated with the build definition to ensure the integrity of the build prior to deployment. **CCL-40 (network only)** – User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within 2 business days or as per policy whichever is earlier. Upon a user's termination or role change, the user's access at the application level should be removed/adjusted within 10 business days of the termination/change. **CCL-42** – To access the Service's systems, users must have a valid and unique Microsoft account. Password configuration is in accordance with Microsoft security policy and the password configuration is managed by CSE. **CCL-45** – Encryption keys are rotated on a periodic basis in accordance with Online Services Security Standards (OSSS). Where these standards conflict with the Microsoft Security Policy, the stricter of the policies are applied to ensure proper and effective use of cryptographic confidentiality. **CCL-46** – Access to encryption keys storage is restricted to authorized personnel. **CCL-47** – Credential monitoring is performed in each build to prevent credentials from existing in the Service's source code. **CSOC** - Microsoft Azure is responsible for antimalware protection related to the ICCS and ICP systems hosted on Azure platform services. **CSOC** – Microsoft Azure is responsible for the encryption of data at rest and data in motion for ICCS and ICP systems hosted on Azure platform services. **CSOC** – Salesforce Marketing Cloud is responsible for antimalware protection over their Software-as-a-Service supporting ICCS and ICP.

Criteria	IRIS Control Activity
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	**CCL-132** – The baseline configuration for Security Groups (SGs) enforce a requirement for SG Owner's approval for adding new users to the SG. **CCL-149** – Services maintain an inventory of all Azure subscriptions in the Service Tree. An inventory of all resources residing within each Service's Azure subscription is maintained within the Azure Portal. Access to service tree and Azure portal is restricted to authorized individuals. **CCL-152** – Quarterly, services validate that Azure Subscription security is properly configured. Any changes in the Azure portal security configuration follows the Commerce Services change management process. **CCL-32** – Quarterly, services validate the servers are appropriately mapped to the Service Tree ID. **CCL-35** – Access to Services must be authorized, conform to Microsoft access management policies and procedures, and aligned with the Role-Based Access Control (RBAC) Model. Role Based Access Control (RBAC) is implemented within the Service's systems to enforce the concepts of the least privilege access and segregation of the incompatible duties. **CCL-36** – On a quarterly basis, the list of users with access to the Service's systems, including the Service tree admins, Azure subscriptions and resources, security groups, Load balancer Tool, source code repository, encryption keys repository and in-scope third party tools are reviewed. Any inappropriate access identified through the review process is removed from the resource in a timely manner. **CCL-40 (network only)** – User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within 2 business days or as per policy whichever is earlier. Upon a user's termination or role change, the user's access at the application level should be removed/adjusted within 10 business days of the termination/change.
CC6.3- The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	**CCL-132** – The baseline configuration for Security Groups (SGs) enforce a requirement for SG Owner's approval for adding new users to the SG. **CCL-152** – Quarterly, services validate that Azure Subscription security is properly configured. Any changes in the Azure portal security configuration follows the Commerce Services change management process. **CCL-35** – Access to Services must be authorized, conform to Microsoft access management policies and procedures, and aligned with the Role-Based Access Control (RBAC) Model. Role Based Access Control (RBAC) is implemented within the Service's systems to enforce the concepts of the least privilege access and segregation of the incompatible duties. **CCL-36** – On a quarterly basis, the list of users with access to the Service's systems, including the Service tree admins, Azure subscriptions and resources, security groups, Load balancer Tool, source code repository, encryption keys repository and in-scope third party tools are reviewed. Any inappropriate access identified through the review process is removed from the resource in a timely manner. **CCL-40 (network only)** – User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within 2 business days or as per policy whichever is earlier. Upon a user's termination or role change, the user's access at the application level should be removed/adjusted within 10 business days of the termination/change.
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	**CSOC** – Microsoft Azure is responsible for maintaining controls over physical access to the facilities, including data centers, supporting ICCS and ICP. **CSOC** – Salesforce Marketing Cloud is responsible for maintaining controls over physical access to the facilities, including data centers, supporting ICCS and ICP.

Criteria	IRIS Control Activity
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	**CCL-40 (network only)** – User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within 2 business days or as per policy whichever is earlier. Upon a user's termination or role change, the user's access at the application level should be removed/adjusted within 10 business days of the termination/change. **CSOC** – Microsoft Azure is responsible for maintaining controls over physical access to the facilities, including data centers, supporting ICCS and ICP. **CSOC** – Microsoft Azure is responsible for the maintenance and change management of the infrastructure and supporting systems that support their platform as a service where ICCS and ICP are hosted. **CSOC** – Salesforce Marketing Cloud is responsible for maintaining controls over physical access to the facilities, including data centers, supporting ICCS and ICP. **CSOC** – Salesforce Marketing Cloud is responsible for the maintenance and change management of the infrastructure related to their Software-as-a-Service supporting ICCP and ICP.
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**CCL-113** – An anti-malware scanner is integrated with the build definition to ensure the integrity of the build prior to deployment. **CCL-167** – Commercial personal data is encrypted within SFMC (Encrypted Data Send). Access to the encryption key is restricted to authorized individuals. **CCL-29** – Security threat modeling is performed when any new service is spun up and then is performed annually, or after any significant changes in the system design and/or infrastructure. The Service's Security Champ and CDG Security team review the result including security and availability of the Service's systems. Corrective action, if required, is performed in a timely manner. **CCL-47** – Credential monitoring is performed in each build to prevent credentials from existing in the Service's source code. **CCL-70** – Services conduct an annual review of the system's data flow to validate its accuracy, and update it if necessary. **CSOC** – Microsoft Azure is responsible for the encryption of the Remote Desktop Connection used for administrator access to the ICCS and ICP systems hosted on Azure platform services. **CSOC** – Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting Iris ICCS and ICP. **CSOC** – Microsoft Azure is responsible for antimalware protection related to the ICCS and ICP systems hosted on Azure platform services. **CSOC** – Microsoft Azure is responsible for the encryption of data at rest and data in motion for ICCS and ICP systems hosted on Azure platform services. **CSOC** – Microsoft Azure is responsible for network filtering implementation to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components. **CSOC** – Salesforce Marketing Cloud is responsible for antimalware protection over their Software-as-a-Service supporting ICCS and ICP.

Criteria	IRIS Control Activity
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	**CCL-167** – Commercial personal data is encrypted within SFMC (Encrypted Data Send). Access to the encryption key is restricted to authorized individuals. **CCL-46** – Access to encryption keys storage is restricted to authorized personnel. **CSOC** – Microsoft Azure is responsible for maintaining controls over physical access to the facilities, including data centers, supporting ICCS and ICP. **CSOC** – Microsoft Azure is responsible for maintaining controls over protection of the network environment, including perimeter firewalls and restricting access to network devices. **CSOC** - Microsoft Azure is responsible for maintaining controls over environmental protection of systems, including natural disasters and man-made threats, for infrastructure supporting ICCS and ICP. **CSOC** – Microsoft Azure is responsible for network filtering implementation to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted service components. **CSOC** – Microsoft Azure is responsible for the encryption of data at rest and data in motion for ICCS and ICP systems hosted on Azure platform services. **CSOC** – Microsoft Azure is responsible for the encryption of the Remote Desktop Connection used for administrator access to the ICCS and ICP systems hosted on Azure platform services. **CSOC** – Salesforce Marketing Cloud is responsible for maintaining controls over physical access to the facilities, including data centers, supporting ICCS and ICP. **CSOC** – Salesforce Marketing Cloud is responsible for maintaining controls over protection of the network environment, including perimeter firewalls and restricting access to network devices. **CSOC** – Salesforce Marketing Cloud is responsible for maintaining controls over environmental protection of systems, including natural disasters and man-made threats, for infrastructure supporting ICCS and ICP.

Criteria	IRIS Control Activity
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	**CCL-148** – JIT activity is documented within a VSO or ICM ticket describing the reason for and changes made during the login session. **CCL-113** – An anti-malware scanner is integrated with the build definition to ensure the integrity of the build prior to deployment. **CCL-29** – Security threat modeling is performed when any new service is spun up and then is performed annually, or after any significant changes in the system design and/or infrastructure. The Service's Security Champ and CDG Security team review the result including security and availability of the Service's systems. Corrective action, if required, is performed in a timely manner. **CCL-54** – OS patching is automatically deployed to all Service's system resources through Pilotfish. CDG runs the scan to determine that all VMs have updated security patches. CDG will notify services regarding any outdated security patches. **CCL-59** – The JIT access to production environment is logged, and on a quarterly basis, log is reviewed to determine only appropriate users logged into production environment. Users have read-only access to the JIT log. **CCL-60** – An incident management (ICM) ticket is opened for incidents and issues are addressed in a timely manner. **CCL-92** – For teams utilizing the Developer / Operations model, system configurations are in place to prevent implementation of unapproved changes to production. **CSOC** – Microsoft Azure is responsible for antimalware protection related to the ICCS and ICP systems hosted on Azure platform services. **CSOC** – Salesforce Marketing Cloud is responsible for antimalware protection over their Software-as-a-Service supporting ICCS and ICP.

CC7.0 - SYSTEM OPERATIONS

Criteria	IRIS Control Activity
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities and (2) susceptibilities to newly discovered vulnerabilities.	**CCL-148** – JIT activity is documented within a VSO or ICM ticket describing the reason for and changes made during the login session. **CCL-152** – Quarterly, services validate that Azure Subscription security is properly configured. Any changes in the Azure portal security configuration follows the Commerce Services change management process. **CCL-113** – An anti-malware scanner is integrated with the build definition to ensure the integrity of the build prior to deployment. **CCL-29** – Security threat modeling is performed when any new service is spun up and then is performed annually, or after any significant changes in the system design and/or infrastructure. The Service's Security Champ and CDG Security team review the result including security and availability of the Service's systems. Corrective action, if required, is performed in a timely manner. **CCL-59** – The JIT access to production environment is logged, and on a quarterly basis, log is reviewed to determine only appropriate users logged into production environment. Users have read-only access to the JIT log. **CCL-60** – An incident management (ICM) ticket is opened for incidents and issues are addressed in a timely manner. **CCL-92** – For teams utilizing the Developer / Operations model, system configurations are in place to prevent implementation of unapproved changes to production. **CCL-94** – Quarterly, services validate that the Qualys agent is running on in-scope VMs. **CSOC** – Microsoft Azure is responsible for antimalware protection related to the ICCS and ICP systems hosted on Azure platform services. **CSOC** – Microsoft Azure is responsible for the maintenance and change management of the infrastructure and supporting systems that support their platform as a service where ICCS and ICP are hosted. **CSOC** – Salesforce Marketing Cloud is responsible for the maintenance and change management of the infrastructure related to their Software-as-a-Service supporting ICCP and ICP. **CSOC** – Salesforce Marketing Cloud is responsible for antimalware protection over their Software-as-a-Service supporting ICCS and ICP.

Criteria	IRIS Control Activity
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	**CCL-148** – JIT activity is documented within a VSO or ICM ticket describing the reason for and changes made during the login session. **CCL-113** – An anti-malware scanner is integrated with the build definition to ensure the integrity of the build prior to deployment. **CCL-29** – Security threat modeling is performed when any new service is spun up and then is performed annually, or after any significant changes in the system design and/or infrastructure. The Service's Security Champ and CDG Security team review the result including security and availability of the Service's systems. Corrective action, if required, is performed in a timely manner. **CCL-59** – The JIT access to production environment is logged, and on a quarterly basis, log is reviewed to determine only appropriate users logged into production environment. Users have read-only access to the JIT log. **CCL-60** – An incident management (ICM) ticket is opened for incidents and issues are addressed in a timely manner. **CSOC** – Microsoft Azure is responsible for antimalware protection related to the ICCS and ICP systems hosted on Azure platform services. **CSOC** – Microsoft Azure is responsible for geographic replication and backups for ICCS and ICP systems hosted on Azure platform services. **CSOC** – Salesforce Marketing Cloud is responsible for antimalware protection over their Software-as-a-Service supporting ICCS and ICP.
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	**CCL-29** – Security threat modeling is performed when any new service is spun up and then is performed annually, or after any significant changes in the system design and/or infrastructure. The Service's Security Champ and CDG Security team review the result including security and availability of the Service's systems. Corrective action, if required, is performed in a timely manner. **CCL-60** – An incident management (ICM) ticket is opened for incidents and issues are addressed in a timely manner. **CSOC** – Microsoft Azure is responsible for monitoring and addressing security events and incidents related to the ICCS and ICP systems hosted on Azure platform services. **CSOC** – Salesforce Marketing Cloud is responsible for monitoring and addressing security events and incidents related to their Software-as-a-Service supporting ICCS and ICP.
CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	**CCL-29** – Security threat modeling is performed when any new service is spun up and then is performed annually, or after any significant changes in the system design and/or infrastructure. The Service's Security Champ and CDG Security team review the result including security and availability of the Service's systems. Corrective action, if required, is performed in a timely manner.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	**CCL-17** – The Service has a geo-redundant design and it runs in an active/passive (or active/active) configuration. Services' fail over requirements are configured in a fail-over tool and access is limited to authorized administrators to modify the configurations. **CSOC** – Microsoft Azure is responsible for controlling that all Datacenters are required to at least annually, exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption.

CC8.0 - CHANGE MANAGEMENT

Criteria	IRIS Control Activity
CC8.1 - The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	**CCL-148** – JIT activity is documented within a VSO or ICM ticket describing the reason for and changes made during the login session. **CCL-152** – Quarterly, services validate that Azure Subscription security is properly configured. Any changes in the Azure portal security configuration follows the Commerce Services change management process. **CCL-47** – Credential monitoring is performed in each build to prevent credentials from existing in the Service's source code. **CCL-55** – Development of new features and major changes to Services follow a defined approach based on the Microsoft Security Development Lifecycle (SDL) methodology. **CCL-56** – Changes are tested and technical specifications and/or configurations are validated for appropriateness. Testing results and Technical signoff are retained within the appropriate TFS record depending on the type of change as outlined in the Commerce Services change management Policy. **CCL-57** – Changes are appropriately approved prior to release to production, as defined in the Commerce Services change management Policy, indicating their approval of the production readiness of the tested code. **CCL-59** – The JIT access to production environment is logged, and on a quarterly basis, log is reviewed to determine only appropriate users logged into production environment. Users have read-only access to the JIT log. **CCL-64** – System is configured to retain campaign data records in SFMC for no more than 4 days. **CCL-76** – The Global Traffic Management (GTM) or Azure Traffic Manager (ATM) activity log is reviewed on quarterly basis to determine changes to the Service's properties were appropriate and authorized. **CCL-92** – For teams utilizing the Developer / Operations model, system configurations are in place to prevent implementation of unapproved changes to production. **CCL-98** – The Production and Pre-Production environment (PPE) are separated. New features and major changes are developed and tested in separate environments prior to production implementation. Production data is not replicated in test or development environments. **CSOC**– Microsoft Azure is responsible for the maintenance and change management of the infrastructure and supporting systems that support their platform as a service where ICCS and ICP are hosted. **CSOC** – Salesforce Marketing Cloud is responsible for the maintenance and change management of the infrastructure related to their Software-as-a-Service supporting ICCP and ICP.

CC9.0 - RISK MITIGATION

Criteria	IRIS Control Activity
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**CCL-22** – Services adhere to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability and process integrity commitments. **CCL-27** – Effectiveness of the internal controls are assessed by independent auditors on an annual basis. Findings are addressed with corrective actions, which are tracked and completed in a timely manner. **CCL-78** – Iris adheres to the Enterprise Business Continuity Management and Standard. The Service's business continuity plans (BCPs) are reviewed and tested at least annually.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.	**CCL-22** – Services adhere to ERM and performs an information systems risk assessment on an annual basis to assess potential risks that would impair system security, confidentiality, availability and process integrity commitments. **CCL-65** – Services monitor their dependencies on third parties through obtaining and evaluating attestation reports when available.

Additional Criteria for Availability

Criteria	IRIS Control Activity
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	**CCL-66** – Processing capacity and availability are monitored by Service teams. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed. **CCL-67** – Quarterly, Service management reviews and discuss system availability and reliability and addresses any issues.
A1.2 - The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	**CCL-17** – The Service has a geo-redundant design and it runs in an active/passive (or active/active) configuration. Services' fail over requirements are configured in a fail-over tool and access is limited to authorized administrators to modify the configurations. **CCL-69** – Services have an architecture in place that supports the recovery of services through tools and services supporting the overall Service. **CCL-76** – The Global Traffic Management (GTM) or Azure Traffic Manager (ATM) activity log is reviewed on a quarterly basis to determine changes to the Service's properties were appropriate and authorized. **CSOC** – Microsoft Azure is responsible for geographic replication and backups for ICCS and ICP systems hosted on Azure platform services.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.	**CCL-78** – Iris adheres to the Enterprise Business Continuity Management and Standard. The Service's business continuity plans (BCPs) are reviewed and tested at least annually. **CSOC** – Microsoft Azure is responsible for controlling that all Datacenters are required to at least annually, exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption.

Additional Criteria for Confidentiality

Criteria	IRIS Control Activity
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	**CCL-120** – The Service's secret keys are encrypted and stored in a restricted access storage. The encryption key storage is backed up. **CCL-167** – Commercial personal data is encrypted within SFMC (Encrypted Data Send). Access to the encryption key is restricted to authorized individuals. **CCL-72** – Services Production environment uses different encryption keys than those for the Pre-Production environment (PPE). **CCL-98** – The Production and Pre-Production environment (PPE) are separated. New features and major changes are developed and tested in separate environments prior to production implementation. Production data is not replicated in test or development environments. **CSOC** – Microsoft Azure is responsible for the encryption of data at rest and data in motion for ICCS and ICP systems hosted on Azure platform services.
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	**CCL-64** – System is configured to retain campaign data records in SFMC for no more than 4 days.

Section IV: Supplemental information provided by Microsoft

Section IV: Supplemental information provided by Service Organization

The information included in Section IV of this report is presented by Microsoft to provide additional information to user entities and is not part of the ICCS and ICP System description. The information included here in Section IV has not been subjected to the procedures applied in the examination of the description of the system related to ICCS and ICP services, and accordingly, Deloitte & Touche LLP expresses no opinion on it.

Business continuity planning

The ICCS and ICP services incorporate resilient and redundant features in each service and utilize Microsoft's enterprise-level datacenters. These data centers use the same world-class operational practices as Microsoft's corporate line of business applications and provide a comprehensive solution for the company's online services with the ability to meet the high standards of its customers.

The company's online services designs include provisions to quickly recover from unexpected events, such as hardware or application failure, data corruption, or other incidents that may affect a subset of the user population. The company's service continuity solutions and framework are based on industry best practice and are updated on a regular basis to support Microsoft's ability to recover from a major outage in a timely manner.

Cloud service continuous improvements

Features and functionality are regularly being added to these services. The risk-based controls applied to the new components are expected to remain consistent with the risk-based controls applied to the existing ICCS and ICP services.

Controls not subject to this examination

The following controls have been put in place by Microsoft, but have not occurred, and were not tested as part of this examination.

Control Activity	Management's Note
CCL-40 (ICCS and ICP) – User terminations are handled in a timely manner. Upon receipt of a termination notification, user access is removed from Microsoft active directory within 2 business days or as per policy whichever is earlier. Upon a user's termination or role change, the user's access at the application level should be removed/adjusted within 10 business days of the termination/change.	There were no occurrences of terminations for the ICCS or ICP systems.
CCL-61 – CDG Security receives security and incident alerts on an ongoing basis. Notification of required actions and response efforts are communicated internally. Corrective action, if required, is performed in a timely manner.	There were no occurrences of security incidents relating to the ICCS or ICP systems. Monitoring procedures are in place to alert and process security incidents as part of CCL-60.
CCL-101 – Failover procedures are defined and at least annually, integrity checks are performed through standard restoration activities.	There was no occurrence of this control for these workstreams during the examination period.
CCL-68 – Annually, Services senior management reviews and approves the capacity for Service's systems.	The IRIS team's annual budget and capacity had not yet been performed since IRIS is a newly implemented system.

Control Activity	Management's Note
CCL-23 – The identified risks that would impair system security, confidentiality, availability and poses integrity are reviewed and approved by Service's management team. The status of the risk mitigation strategies and control gaps are monitored by the assigned owners.	The IRIS team undergoes a risk assessment as part of CCL-22. Findings from the risk assessment are triaged according to risk level. Any risks that are deemed as 'High' become subject to the review and monitoring of control CCL-23. Management noted that there were no high risks as part of the annual risk assessment. As a result, there were no occurrences for this control.
CCL-169 – Services maintain and communicate the confidentiality and related security obligations for customer data via the Microsoft Trust Center.	There was no occurrence of this control for these workstreams during the examination period.
CCL-111 - A root cause analysis of the incidents will be performed to reduce the likelihood or impact of future incidents; if applicable.	There was no occurrence of this control for these workstreams during the examination period.