Internal Audit Department

Executive summary:

The audit's scope encompassed the Control Condition Assessment for the period from December 1, 2022, to November 30, 2023, focusing on various operational and compliance areas within the Marketing business group under the CMO-Chief Brand Office. The objective was to evaluate the adequacy and effectiveness of controls related to customer service monitoring, social media content management, marketing material compliance, governance, and information security practices.

The control condition was rated as Unsatisfactory, indicating control weaknesses that require immediate attention.

Two notable issues with high rating was identified concerning the transmission and disposal of customer data with Live Ramp, highlighting incomplete records disposition plans, lack of vendor monitoring controls, and unauthorized data upload methods. The root causes are attributed to ineffective monitoring processes and a lack of management awareness regarding data transmission standards. Remediation is expected by August 30, 2024. It is recommended that remediation actions be taken to address the risks and strengthen the control environment.

In addition a medium rated issue was also identified, Internal Audit (IA) verified that appropriate procedures were not followed, and timely response and escalation occurred by the Social Media Operations team for a sample of 25 cases generated within the scope period.

Audit Overview:

Internal audit has assessed the control conditions of the key control related to "Controls over the transmission to and disposal of customer data in Live Ramp" and "Minimum third-party and privacy standards" in the Marketing department of Abc.

The scope period for this audit is from 12/1/2022 to 11/30/2023.

A control condition audit is designed to provide reasonable assurance as to the design and

effectiveness of the system of internal controls implemented by management.

Internal Audit's testing resulted in the identification of 3 issues. The issue ratings for these identified issues are High and Medium. 2 issues are High rated and 1 Medium rated. The details of the issues identified, and management's action plans can be reviewed in the following pages.

Two notable issues with a high rating was identified concerning the transmission and disposal of customer data with LiveRamp, highlighting incomplete records disposition plans, lack of vendor monitoring controls, and unauthorized data upload methods. The root cause is attributed to ineffective monitoring processes and a lack of management awareness regarding data transmission standards. Remediation is expected by August 30, 2024. It is recommended that remediation actions be taken to address the risks and strengthen the control environment.

This report is confidential and not to be distributed to anyone beyond the individuals indicated. Should copies of this report be requested by any employee of Abc or subsidiaries, the request should be referred to the Internal Audit Department. All requests by external parties, either individual or regulatory entity should be referred to the Law Department.

Another high rated issue identified (IS-0002722) is that minimum third-party and privacy standards were not executed, leading to inadequate information security controls for customer information. The root cause is attributed to various Vendor Engagement Manager (VEM) and organizational changes over the past few years, and inappropriate SaaS configuration during the vendor onboarding process in 2018. The issue is rated as high, with a target resolution date of October 31, 2024.

Control Condition:

Unsatisfactory

Control environment:

Unrated

Rating Rationale:

Based on the results of the work performed, Internal Audit has concluded that certain elements of the system of internal controls implemented by management are not adequately designed [and/or] operating as intended to mitigate the risks of the business [or function].

The project's control condition is unsatisfactory, with ineffective design and operating effectiveness.

Scope:

The Abc Marketing Social Media team, under Tony Hamlett, publishes approved content on social media and monitors customer interactions. A separate team, led by Ealli Chapman, manages the Social Media Customer Look-a-like process. The project's scope covers social media publishing, monitoring, and the customer look-a-like process.

The scope included an assessment of the design and effectiveness of the key controls related to social media systems access, social media response/mentions monitoring, misleading communications and marketing materials, governance over social media posting and monitoring, unauthorized access to systems, and inadvertent data exposure.

The audit focused on certain key risks

including:

- Product, Operations, and Trading - Customer Service/Escalation - Customer Complaints
- Regulatory Compliance - Misleading Communications and Marketing Materials
- People and Governance - Governance and Risk Management
- Information Security - Unauthorized Data Access
- Information Security - Inadvertent Data Exposure

Testing focused on controls in certain key processes including:

This report is confidential and not to be distributed to anyone beyond the individuals indicated. Should copies of this report be requested by any employee of Abc or subsidiaries, the request should be referred to the Internal Audit Department. All requests by external parties, either individual or regulatory entity should be referred to the Law Department.

- Product, Operations, and Trading (12.3.1)
- Customer Service/Escalation and Monitoring – Verify adequate monitoring and escalation controls are in place regarding customer comments, complaints, and service requests.
- Monitoring Reports – Assess management's monitoring controls over social media content.
- Regulatory Compliance (10.5.3)
- Misleading Communications and Marketing Materials – Validate that Marketing Materials presented are not misleading and comply with applicable regulatory requirements.
- People and Governance (14.9.1)
- Governance and Risk Management – Governance over Social-Media posting and monitoring, including the development and maintenance of key standard operating procedures.
- Information Security (8.1.1 & 8.2.1)
- Unauthorized Access to Systems (Sprinklr & LiveRamp)
- Inadvertent Data Exposure - Assess controls and operational frameworks in place to mitigate the risk of unauthorized data transfer, including hashing and uploading of customer data to vendors where applicable.

The following processes were excluded from the scope of the review: "OGIM individually owned accounts are overseen by its own self-contained Social Media Program and Strategy under the leadership of Haley Rubin. OGIM individual accounts will be outside this review however, OGIM Affiliate brand-level accounts (e.g., OGIM Investments, OGIM Fixed Income, OGIM Real Estate, OGIM International, etc.) will be included in this review. AIQ and International social media programs are overseen by their own management team which fall outside of the scope of this function and will be excluded from this review."

This report is confidential and not to be distributed to anyone beyond the individuals indicated. Should copies of this report be requested by any employee of Abc or subsidiaries, the request should be referred to the Internal Audit Department. All requests by external parties, either individual or regulatory entity should be referred to the Law Department.

Internal Audit Department

Issue ID: IS-002722

Issue Name: Minimum third-party and privacy standards were not executed resulting in inadequate information security controls to prevent inappropriate access to customer information by internal or external parties.

Description: Sprinklr is a Software as a Service (SaaS) social media management platform used to implement social media strategy and support the tracking and triage of comments received from consumers (e.g., service requests, customer complaints). The Abc Social Media Listening Program uses Sprinklr to monitor social media content involving Abc across various public platforms (e.g., Facebook, LinkedIn). The Social Media team began collecting Personal Information (PI) to provide further customer assistance since 2018.

Root Cause Description: The root cause can be attributed to both various VEM and organizational changes occurring over the past few years, which over time has impacted clarity regarding the applicable ongoing monitoring standards. Also, during the vendor onboarding process (2018) appropriate SaaS configuration was not performed.

Rating Rationale: A lack of change management discipline and oversight to ensure process enhancements are implemented appropriately and working as intended prior to being operationalized. Failure to execute minimum third-party and privacy standards resulted in inadequate information security controls to prevent inappropriate access to customer information by internal or external parties. The risk is High.

Risk Category: 8. Information Security

Issue Rating: High

Repeat Issue: No

Status: Open

Issue Target Date: 2024-10-31 00:00:00

Action Plan ID: AC-003533

Action Plan Description: Implement single sign on (SSO) authentication for users when accessing Sprinklr through both web and mobile.

Action Plan Closure Target Date: 2024-07-31 00:00:00

Action Plan Status: Open

This report is confidential and not to be distributed to anyone beyond the individuals indicated. Should copies of this report be requested by any employee of Abc or subsidiaries, the request should be referred to the Internal Audit Department. All requests by external parties, either individual or regulatory entity should be referred to the Law Department.

Internal Audit Department

Action Plan ID: AC-003534

Action Plan Description: Explore solutions to implement multifactor authentication (MFA) for Sprinklr access.

Action Plan Closure Target Date: 2024-07-31 00:00:00

Action Plan Status: Open

Action Plan ID: AC-003535

Action Plan Description: Assess enterprise standards for data loss protection and determine whether controls can be configured by the vendor to meet requirements. Implement identified solutions and monitor adherence, as appropriate.

Action Plan Closure Target Date: 2024-07-31 00:00:00

Action Plan Status: Open

Action Plan ID: AC-003536

Action Plan Description: Complete a Privacy Impact Assessment and reclassify the application to Restricted.

Action Plan Closure Target Date: 2024-06-30 00:00:00

Action Plan Status: Open

Action Plan ID: AC-003537

Action Plan Description: Complete the vendor assessment based on current usage of Sprinklr.

Action Plan Closure Target Date: 2024-06-30 00:00:00

Action Plan Status: Open

Action Plan ID: AC-003538

Action Plan Description: Implement access provisioning controls and recertification process through Central Security Service.

This report is confidential and not to be distributed to anyone beyond the individuals indicated. Should copies of this report be requested by any employee of Abc or subsidiaries, the request should be referred to the Internal Audit Department. All requests by external parties, either individual or regulatory entity should be referred to the Law Department.

Action Plan Closure Target Date: 2024-06-30 00:00:00

Action Plan Status: Open

Action Plan ID: AC-003539

Action Plan Description: Oversee a comprehensive assessment of current CMO SaaS vendors to confirm that the following controls are in place where applicable: 1. A Privacy Impact Assessment has been completed. 2. The vendor IRRT has been refreshed in accordance with current VGO standards.

Action Plan Closure Target Date: 2024-06-30 00:00:00

Action Plan Status: Open

Action Plan ID: AC-003610

Action Plan Description: Assess the active SaaS applications within the Marketing organization and determine whether they adhere to relevant Enterprise Information Security Control Standards. Develop a tracking document that lists all SaaS applications and their level of adherence to standards with variables that impact implementation of required configurations. Additionally, document a plan to remediate identified gaps supported by risk and criticality assessments.

Action Plan Closure Target Date: 2024-09-30 00:00:00

Action Plan Status: Open

This report is confidential and not to be distributed to anyone beyond the individuals indicated. Should copies of this report be requested by any employee of Abc or subsidiaries, the request should be referred to the Internal Audit Department. All requests by external parties, either individual or regulatory entity should be referred to the Law Department.

Internal Audit Department

Issue ID: IS-002723

Issue Name: Controls over the transmission to and disposal of customer data in LiveRamp requires improvement.

Description: LiveRamp, a third-party provider that offers a cloud-based onboarding application designed to collect, organize, and connect customer data to marketing and social media platforms. The Abc Paid Media team provides LiveRamp with customers' personal information (e.g., names, address, phone numbers), to be hashed and anonymized prior to sharing with additional third-party social media platforms for the purposes of creating curated groups of prospective customers.

Root Cause Description: The root cause is primarily attributed to the lack of effective Vendor Engagement Manager's monitoring process and management's awareness of the expected standards, associated controls including the approved data transmission methods.

Rating Rationale: A lack of controls over the transmission to and disposal of customer data in LiveRamp requires improvement. Failure to reduce the exposure of customer data, as well as using an unapproved process to transmit customer data to a vendor, could result in data breaches, as well as reputational and regulatory damages. The risk is high.

Risk Category: 8. Information Security

Issue Rating: High

Repeat Issue: No

Status: Open

Issue Target Date: 2024-08-30 00:00:00

Action Plan ID: AC-003540

Action Plan Description: Revise records disposition plan and contractual agreement with LiveRamp to clearly define data deletion requirements.

Action Plan Owner: Maximilian Stefani - maximilian.stefani@Abc.com

Action Plan Closure Target Date: 2024-06-30 00:00:00

Action Plan Status: Open

This report is confidential and not to be distributed to anyone beyond the individuals indicated. Should copies of this report be requested by any employee of Abc or subsidiaries, the request should be referred to the Internal Audit Department. All requests by external parties, either individual or regulatory entity should be referred to the Law Department.

Internal Audit Department

Action Plan ID: AC-003542

Action Plan Description: Ensure training/communication of EARB approved process for all Social Media team members.

Action Plan Owner: Gregory Aronne - gregory.aronne@Abc.com

Action Plan Closure Target Date: 2024-06-30 00:00:00

Action Plan Status: Open

Action Plan ID: AC-003543

Action Plan Description: Explore methods to disable direct uploads through LiveRamp or assign restricted user permissions with the application.

Action Plan Owner: Ketan Bhanushali - ketan.bhanushali@Abc.com

Action Plan Closure Target Date: 2024-07-31 00:00:00

Action Plan Status: Open

This report is confidential and not to be distributed to anyone beyond the individuals indicated. Should copies of this report be requested by any employee of Abc or subsidiaries, the request should be referred to the Internal Audit Department. All requests by external parties, either individual or regulatory entity should be referred to the Law Department.

Internal Audit Department

Issue ID: IS-002724

Issue Name: Controls to ensure timely response and escalation of customer service-related comments require enhancement.

Description: As part of the Abc Social Media Listening Program, the Social Media Operations team utilizes the Sprinklr platform as the primary tool to support the tracking and triage of comments received involving Abc and its social media accounts across various public platforms (e.g., Facebook, LinkedIn). If customer comments received are specific to service requests or customer complaints, a case is created within Sprinklr and assigned to a member of the Social Media team to ensure timely escalation takes place with the appropriate internal parties for tracking and resolution.

Root Cause Description: The root cause is primarily attributable to a lack of change management discipline and oversight to ensure process enhancements are implemented appropriately and working as intended prior to being operationalized.

Rating Rationale: Controls to ensure timely response and escalation of customer service-related comments require enhancement. Failure to identify and escalate Sprinklr cases related to consumer service requests or complaints in a timely manner increases the likelihood of cases going unaddressed. Unresponsiveness to customer inquiries, coupled with ambiguity in Standard Operating Procedures (SOPs), may result in a negative customer experience, poor quality of service, and operational inefficiencies. The risk is low.

Risk Category: 12. Product, Operations and Trading

Issue Rating: Low

Repeat Issue: No

Status: Open

Issue Target Date: 2024-07-31 00:00:00

Action Plan ID: AC-003544

Action Plan Description: Update procedures to reflect the use of the Meta direct messaging platform as part of the case review and closure process. Implement a management oversight procedure to identify and test process changes prior to the operational go-live date.

Action Plan Closure Target Date: 2024-06-30 00:00:00

Action Plan Status: Open

This report is confidential and not to be distributed to anyone beyond the individuals indicated. Should copies of this report be requested by any employee of Abc or subsidiaries, the request should be referred to the Internal Audit Department. All requests by external parties, either individual or regulatory entity should be referred to the Law Department.

Internal Audit Department

Action Plan ID: AC-003545

Action Plan Description: Explore solutions to the current gap preventing automated responses from feeding directly to Sprinklr to alleviate the need of manual reconciliation.

Action Plan Closure Target Date: 2024-06-30 00:00:00

Action Plan Status: Open

This report is confidential and not to be distributed to anyone beyond the individuals indicated. Should copies of this report be requested by any employee of Abc or subsidiaries, the request should be referred to the Internal Audit Department. All requests by external parties, either individual or regulatory entity should be referred to the Law Department.