Report on Act!, LLC's Management Assertion Relating to the Customer Relationship Management Solutions System for the Period December 1, 2023 through November 30, 2024 Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy

SOC 3®

Partners
Audits Without Anxiety®

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Act!, LLC:

Scope

We have examined Act!, LLC's accompanying assertion titled "Assertion of Act!, LLC Management" ("assertion") that the controls within Act!'s Customer Relationship Management Solutions System ("system") were effective throughout the period December 1, 2023 through November 30, 2024, to provide reasonable assurance that Act!'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality and privacy ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Act! 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 Act!'s service commitments and system requirements were achieved. Act! has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Act! is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Act!'s service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Act!'s service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion
In our opinion, management's assertion that the controls within Act!'s Customer Relationship Management Solutions system were effective throughout the period December 1, 2023 through November 30, 2024, to provide reasonable assurance that Act!'s service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

IS Partners, LLC

IS Partners, LLC
Certified Public Accountants
Dresher, Pennsylvania
January 29, 2025

Assertion of Act!, LLC Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Act!, LLC's Customer Relationship Management Solutions system ("system") throughout the period December 1, 2023 through November 30, 2024, to provide reasonable assurance that Act!'s service commitments and system requirements relevant to security, availability, processing integrity, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented in this report and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2023 through November 30, 2024, to provide reasonable assurance that Act!'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality and privacy ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Act!'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 1, 2023 through November 30, 2024, to provide reasonable assurance that Act!'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Act!, LLC
January 29, 2025

Act!, LLC's Description of the Boundaries of the Customer Relationship Management Solutions System

Company Background

Act! is a Customer Relationship Management ("CRM") and marketing automation platform provider for small and medium-sized businesses. With over 30 years of experience helping small businesses nurture their customer relationships, Act! combines the power of CRM with marketing automation to enable professionals to initiate and manage long-term customer engagements.

Overview of the Services Provided

Act! develops and supports Act! Premium Cloud – Formally released in early 2021. Act! Premium Cloud is a full-featured CRM Solution for customers that desire a hosted, full featured solution including Marketing Automation.

Principal Service Commitments and System Requirements

Act! designs its processes and procedures related to the cloud-based SaaS Solutions and the underlying system to meet its objectives for its "Professional Services." "Professional Services" shall mean SaaS application development and testing, SaaS application hosting, data collection and storage, data processing and mapping, infrastructure configuration and maintenance, integration and deployment of services supporting SaaS applications, internal support activities like trainings, security, project management, monitoring, sales, marketing, legal and other support services. Those objectives are based on the service commitments that Act! makes to user entities, the laws and regulations that govern the provision of professional services, and the financial, operational, and compliance requirements that Act! has established for the services. The professional services of Act! are subject to the security and privacy requirements of the SOC 2 as specified and amended by the AICPA, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Act! operates.

Security, availability, processing integrity, confidentiality and privacy commitments to user entities are documented and communicated in order forms, proposals, online forms, or other ordering documents, as well as in the terms of use offering provided online. Security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

- Logical and physical access within the fundamental designs of the cloud-based Solutions and Systems that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit
- The terms and conditions of any order for Act! products or services are available to the customer and follow appropriate retention and disposal procedures
- Change Management and Security configuration controls
- Risk Management, monitoring and incident response controls
- Data backup, disaster recovery and business continuity controls

Act! establishes operational requirements that support the achievement of security, availability, processing integrity, confidentiality and privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Act!'s policies and procedures, system design documentation, internal controls, relevant third-party assessments, and contracts with customers. Act! policies define strict guidance governing security, availability, processing integrity, confidentiality and privacy practices and commitments. Related third-party assessments of internal controls and system vulnerabilities help maintain Act!'s commitments and requirements to its customers.

Components of the System

The system is comprised of the following five components:

- Infrastructure (systems and networks)
- Software (web application & utilities)
- People (Engineers, IT project managers, Product Managers)
- Procedures (automated and manual)
- Data (transactions streams, files, databases, and storage)

The following sections of this description define each of these five components comprising Act!'s system and other relevant aspects of Act!'s control environment, risk assessment process, information and communication systems, and monitoring controls.

Infrastructure

User Facility Access

All of Act!'s servers are hosted by AWS, which is classified as a SOC 1, ISAE 3402, SOC 2, SOC 3, ISO 2700, ISO 27017, Cloud Security, ISO 27018, Cloud Privacy and PCI DSS v3.2 compliant facility. In January 2024, Act! decommissioned the QA servers within its data center and solely relies on AWS for physical infrastructure hosting.

Administrative Access

All access to production resources is accessed through a combination of the AWS cloud platform console and a VPN connection. Access to the AWS cloud platform console is controlled by a strong password policy and multi-factor authentication. Access to the VPN server is controlled using a VPN client and multi-factor authentication. All access is done using unique user accounts, no shared user accounts are used to access the servers in the production environment.

Servers and network devices must be hardened based on the following guidelines:

- Unnecessary files, services, and ports should be removed or blocked. Hardening guides, which are available from the respective vendor or standards from Center for Information Security/NIST are to be used for hardening.
- Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.

- If possible, a standard installation process should be developed for the company's network servers. This will provide consistency across servers no matter what employee or contractor handles the installation.
- Access control lists must be implemented on network devices that prohibit direct connections to the devices. Connections to the router should be limited to the greatest extent possible. Exceptions to this are management connections that can be limited to known sources.
- Access to administrative ports on networking hardware must be restricted to known management hosts and otherwise blocked with a firewall or access control list.

Only those who are deemed necessary are granted access to Act!'s infrastructure. All access is granted through the new hire request process and management approval is necessary. Access is granted using a role-based model to ensure that personnel only have the rights to access the necessary services to perform their explicit job.

Access is revoked in accordance with the employee termination process for any employee that is terminated or leaves the company.

The operations team at Act! has access to the necessary infrastructure in order to run the Act! environment. Access to the infrastructure is restricted to only the employees that require it to maintain the service**.**

All access to the infrastructure is logged and audited including but not limited to access attempts, infrastructure changes and command executed. Act! provides security awareness and enforces strong passwords through the use of minimum password lengths, password complexity rules, unique and non-repeat rules. Passwords are periodically changed due to password expiration rules or can be reset on an ad-hoc basis. Password policies and practices are in place to provide guidance to users to ensure the integrity of their passwords when securing user and company assets. Users are instructed on the following:

- The current password must not be the same as the previous four passwords (password history of four passwords).
- Passwords expire every 90 days.
- Complexity requirement for passwords
  - Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters
  - Dictionary words should not be set as passwords.
  - User account passwords must be of minimum eight characters.
  - Administrator/root passwords must be at least eight or more characters long.
  - Passwords must be a mix of alpha-numeric characters and at least one special character

Since compromise of any single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the IT Helpdesk. Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported. When a password is suspected to have been compromised the IT Helpdesk will request that the user, or users, change all his or her passwords.

The Act! network has several mechanisms and controls in place to minimize intrusion, improve accountability and enable tracing of incidents and events. For example, Act! centralized logging for network devices and servers. Applications may be configured with separate logging facilitates since they may be designed for more in-depth analysis of the application behavior. Logs are to be configured for all events which are of significance such as errors, warnings, security alerts, access logs, application events etc. Act! may undertake any normalization process to optimize logging.

Systems Operations

Act! may use either an IDS or IPS on critical or high-risk network segments. If an IDS is used, procedures must be implemented to review and act on the alerts expediently. If an IPS is used, procedures must be implemented that provide a mechanism for emergency unblocking if the IPS obstructs legitimate traffic.

By implementing network zones, which is separating the network into different segments, the Company reduces its network-wide risk from an attack or virus outbreak. Further, security can be increased if traffic must traverse additional enforcement/inspection points. The company requires the following with regard to network compartmentalization:

AWS servers are guarded by the AWS security policies. AWS security profiles typically refer to role-based security configurations that define access permissions, identity management and compliance settings for users, applications, or workloads within AWS. They encompass multiple AWS services and best practices. Here's a breakdown of key AWS security components that make up security profiles:

1. Identity & Access Management (IAM)
   - IAM Users: Individual users with specific permissions
   - IAM Groups: Collections of users with shared policies
   - IAM Roles: Assignable permission sets for AWS services or external entities
   - IAM Policies: JSON-based documents that define allowed/denied actions
2. AWS Organizations & Service Control Policies (SCPs)
   - Used in multi-account AWS environments
   - Define guardrails on what actions accounts can perform
3. AWS Security Hub and Compliance Frameworks
   - Provide security findings across AWS services
   - Maps configurations to standards like CIS, PCI-DSS and HIPAA
4. AWS Key Management Services (KMS)
   - Manages encryption keys to protect sensitive data
   - Works with AWS services like S3, RDS and Lambda
5. AWS Security Groups & Network Policies
   - Security Groups: Stateful firewalls controlling inbound and outbound traffic at the instance level
   - Network ACLs (NACLs): Stateless, subnet-level traffic filtering
6. AWS Configuration & Audit Logging
   - AWS Configuration: Tracks resource configurations and changes
   - AWS CloudTrail: Logs all API calls for security auditing
   - Amazon GuardDuty: Detects security threats using machine learning
7. AWS Secrets Manager & Parameter Store
   - Securely stores API keys, credentials and secrets

8. AWS Web Application Firewall (WAF) & Shield
    - Protects against common web threats and DDoS attacks

Protected Zone

Internal Servers which are to be protected such as Active Directory and Database Servers are to be placed in this zone. The servers in this zone will not have any direct inbound or outbound access to the internet. They can only be accessed from specific trusted sources in the internal network.

Software

Act! maintains a list of applications, operating systems and all critical software needed to run the system and its operations. The list is kept up to date. Software and hardware assets are tracked and managed in order to reconcile compliance with licensing agreements. Adequate controls are in place to ensure that all software being used by Act! is in compliance with the terms and conditions for the software and applicable regulations as they pertain to the laws that govern the use of software.

Software Sources

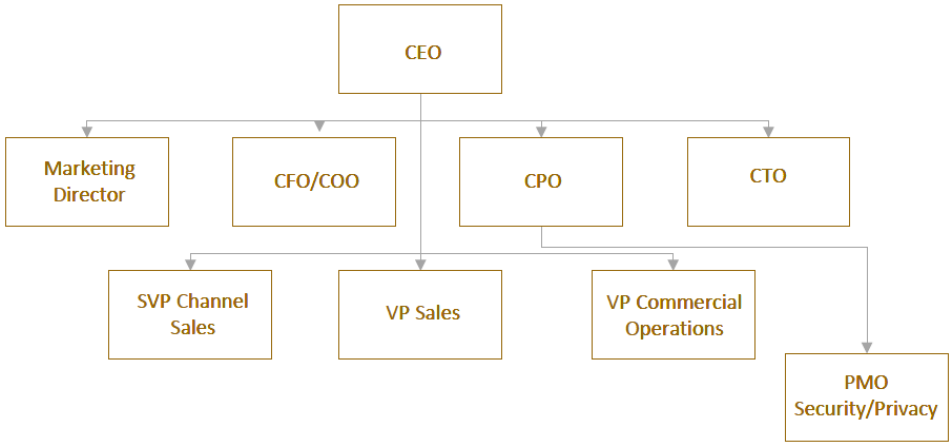
Software utilized by Act! to manage and support the system includes:

- Microsoft Windows, Microsoft SQL Server, Microsoft Active Directory, Jenkins, Datadog, PagerDuty, Pingdom, Glacier, and custom Cloud Tooling Apps.

Microsoft Windows, and Microsoft SQL Server running on cloud based virtual machines are licensed through the cloud providers agreement. Administrative devices not running in the cloud (user laptops) are running Microsoft Windows and Microsoft SQL Server licensed under the Act! MCSA agreement. All other supporting applications are licensed directly by the manufacture and are either dynamically accounted for and charged by use or have limits that cannot be exceeded until additional licenses are purchased.

People

The following diagram outlines the organizational structure within the organization:



Processes and Procedures

Act! has documented policies and procedures to support the operation and controls over the system. Specific examples of the relevant policies and procedures include the following:

- Acceptable Usage Policy
- Access Management Policy
- Access Termination Policy
- Backup and Recovery Policy
- Building Security Policy
- Change Management Policy
- Data Archival and Retention Policy
- Data Classification Policy
- Data Disposal Policy
- Email Policy
- Incident Management Policy
- Mobile Computing Policy
- Network Security Policy
- Onsite Customer Data Policies and Procedures
- Password Policy
- Patch Management Policy
- PCI Policy
- Physical Security Policy
- Risk Management Policy

Network Documentation

Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that the company's IT Staff has a firm understanding of the network architecture at any given time. The intangible benefits of this are immeasurable.

At a minimum, ACT!'s network documentation must include:

- Network diagram(s)
- System configurations
- Firewall rule set
- IP Addresses with VLAN information
- Access Control Lists
- Switch port documentation on the mapping of data points to switch ports

The company requires that network documentation be performed and updated on a semi-annual basis.

Data

This component of the system definition is limited to the information used and supported by the system for the services outlined in this description. The Act! data classification system is based on the concepts of need to know and least privilege. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information, and when disclosure is appropriate only the minimum necessary amount of such information is disclosed. These concepts, when combined with security policies, will protect Act! information from unauthorized disclosure, use, modification, and deletion.