Convictional

Convictional, Inc.

Report on Controls at a Service Organization Relevant to Security, Confidentiality, and Availability

SOC 2 Type 2®

For the Period May 1, 2025 to April 30, 2026

SOC 2 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)

BARR ADVISORY



Contents



Section I

Independent Service Auditor's Report Provided by BARR Advisory, P.A. 2

Section II

Assertion of Convictional Management 6

Section III

Convictional's Description of Its Convictional System 8

Section IV

Description of Criteria, Convictional's Related Controls, and BARR Advisory, P.A.'s Tests of Controls and Results 30

This report is intended solely for use by the management of Convictional, Inc. and its user entities (i.e., customers) that use the services covered by this report during the period. Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Section I

Independent Service Auditor's Report Provided by BARR Advisory, P.A.



Independent Service Auditor's Report

To the Management of Convictional, Inc. ("Convictional"):

Scope

We have examined Convictional's accompanying description of its Convictional System, titled "Convictional's Description of Its Convictional System," throughout the period May 1, 2025 to April 30, 2026 (description), based on the 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* (AICPA, Description Criteria) (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Convictional's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and availability (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).

Convictional uses subservice organizations to provide data center hosting and infrastructure services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Convictional, to achieve Convictional's service commitments and system requirements based on the applicable trust services criteria. The description presents Convictional's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Convictional'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 or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Convictional 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 Convictional's service commitments and system requirements were achieved. Convictional has provided the accompanying assertion titled "Assertion of Convictional Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Convictional 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 Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA.

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 and operated effectively 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.

We are required to be independent of Convictional and to meet our other ethical responsibilities in accordance with relevant ethical requirements related to the engagement.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness 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 or did not operate effectively;
- 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;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and,
- Evaluating the overall presentation of the description.

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

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 and operating 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.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of our tests are listed in Section IV.

In our opinion, in all material respects,

a. The description presents the Convictional System that was designed and implemented throughout the period May 1, 2025 to April 30, 2026, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Convictional's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied any complementary controls assumed in the design of Convictional's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Convictional's service commitments and system requirements were achieved based on the applicable trust services criteria, if any complementary subservice organization controls and complementary user entity controls assumed in the design of Convictional's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Convictional, user entities of the Convictional System during some or all of the period May 1, 2025 to April 30, 2026, business partners of Convictional subject to risks arising from interactions with the Convictional System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators, all of whom 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 those controls interact with the 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; and,
- 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.

BARR Advisory, P.A.

Fairway, KS
June 12, 2026

Section II

Assertion of Convictional Management



©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Assertion of Convictional Management

We have prepared the accompanying description titled "Convictional's Description of Its Convictional System" throughout the period May 1, 2025 to April 30, 2026 (description), based on the 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* (AICPA, Description Criteria) (description criteria). The description is intended to provide users with information about the Convictional System that may be useful when assessing the risks arising from interactions with Convictional's system, particularly information about system controls that Convictional 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, confidentiality, and availability (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).

Convictional uses subservice organizations to provide data center hosting and infrastructure services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Convictional, to achieve Convictional's service commitments and system requirements based on the applicable trust services criteria. The description presents Convictional's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Convictional's controls. The description does not disclose the actual controls at the subservice organizations.

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

a. The description presents the Convictional System that was designed and implemented throughout the period May 1, 2025 to April 30, 2026, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Convictional's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied any complementary controls assumed in the design of Convictional's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Convictional's service commitments and system requirements were achieved based on the applicable trust services criteria, if any complementary subservice organization controls and complementary user entity controls assumed in the design of Convictional's controls operated effectively throughout that period.

Convictional, Inc.

June 12, 2026

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Section III

Convictional's Description of Its Convictional System



©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Overview of Operations

Description of Services Provided

Convictional, Inc. (“Convictional” or the “company”) was founded in 2017 and provides software solutions to companies to help streamline their leadership and business operations.

Convictional’s core product, the Convictional System (the “system”), is a Software as a Service (SaaS) solution that includes the following services:

- **Application:** Customer facing frontend application that allows customers to access Convictional from a non-technical user interface (UI). Features include:
    - Collaborative internal work and communication tools;
    - Users collaborating on company goal tracking, including prioritization, discussing, and linking to other features within the platform;
    - Structure around how decisions are made within user organizations, including AI-powered recommendations, criteria, and resolutions; and,
    - AI-powered context search across integrated context sources.
- **Job Workers:** Process asynchronous work such as waiting for large language model (LLM) responses, search indexing, or scheduled queries.

Principal Service Commitments and System Requirements

Convictional designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Convictional makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that Convictional has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Continuous vulnerability scans over the system and network (Google Cloud Platform (GCP) Security Center), and annual penetration tests (Federacy); and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit;
- Confidentiality agreements with employees and vendors with access to customer data; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between Convictional and user entities.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components;
- Business continuity and disaster recovery (BC/DR) plans that include detailed instructions, roles, and responsibilities; and,
- Operational procedures supporting the achievement of availability commitments to user entities.

Convictional establishes system requirements that support the achievement of service commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements including the following:

- System functional requirements derived from service commitments, published documentation of system functionality, and other descriptions of the system;
- Monitoring of third-party providers to detect failures of those service providers to meet service agreements that could threaten the achievement of the service organization's service commitments and system requirements and respond to those failures; and,
- Business processing rules, standards, and regulations, including:
    - General Data Protection Regulation (GDPR);
    - App Defense Alliance (ADA) Tier 3, and;
    - Privacy laws within the jurisdictions in which it operates including the California Privacy Rights Act (CPRA).

Convictional establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Convictional's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system. Information security policies, including sanctions for policy violations, are approved by management at least annually and published on internal collaboration tools (i.e., Vanta) accessible to all personnel with access to the company systems.

Components of the System Used to Provide the Services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure

The system is hosted on Google Cloud Platform using Google Cloud Run (GCR), a fully managed serverless platform. Convictional employs intrusion detection systems (IDS) at strategic points in its network that complement its Security Policy network settings.

User requests to Convictional's web-based systems are encrypted with Transport Layer Security (TLS) using certificates from an established third party certificate authority.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Convictional does not trust user client machines or provide access based on the network connection. All remote access happens under the zero-trust model where two additional contextual factors (typically Google account single sign-on (SSO) and sometimes two-factor authentication (2FA)) are used to authenticate and authorize user clients.

The hardware components that make up the aforementioned system include servers hosted, managed, and protected by GCP. Production database servers hosted at GCP maintain failover capabilities in the event of physical hardware or logical software failures. This infrastructure is hosted in high-availability data centers with multiple-availability zones.

All infrastructure noted in the Primary Infrastructure and Software table is hosted by subservice organizations, specified in the Complementary Subservice Organization Controls table.

Software

Convictional is responsible for managing the development and operation of the Convictional platform including software components such as applications, operating system, databases, and storage systems, unless noted in the Complementary Subservice Organization Controls table.

The in-scope Convictional infrastructure and software components are shown in the table below:

Primary Infrastructure and Software			
System/ Application	**Business Function/ Description**	**OS DB**	**Physical Location**
Convictional App	Provides access to the Convictional SaaS application through a web interface and user authentication.	Google Cloud Run Google Cloud SQL Google Cloud Storage	GCP US-Central-1 GCP US-Central-1 (Multi-zone) (Disaster Recovery)
Convictional Job Workers	Provides asynchronous work for long-running operations, such as LLM inference.	Google Cloud Run	GCP US-Central-1 GCP US-Central-1 (Multi-zone) (Disaster Recovery)
Anthropic	Used to access and integrate advanced language models into applications.	Anthropic Proprietary	GCP US-Central-1 GCP US-Central-1 (Multi-zone) (Disaster Recovery)
OpenAI	Used to access and integrate advanced language models into applications.	OpenAI Proprietary	GCP US-Central-1 GCP US-Central-1 (Multi-zone) (Disaster Recovery)
GCP Cloud Run	Serverless computing platform as a service for developing and hosting web applications in Google-managed data centers.	GCP Proprietary	GCP Cloud

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

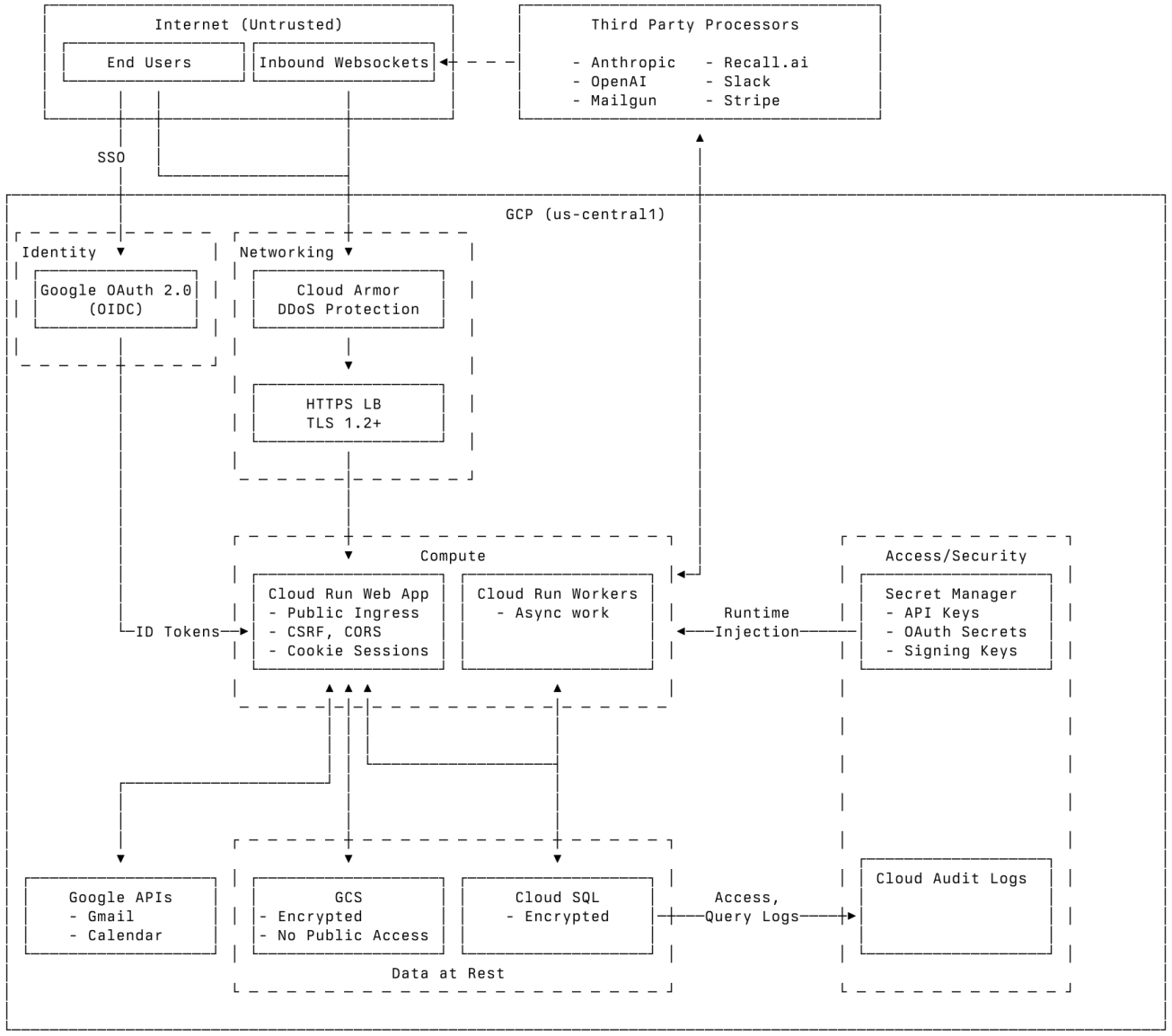
Primary Infrastructure and Software			
System/ Application	**Business Function/ Description**	**OS DB**	**Physical Location**
GCP Firewall (Cloud Armor)	Provides a central way to limit access to backend resources.	GCP Proprietary	GCP Cloud
GCP Cloud Storage	Scalable object storage for data, files, and backups.	Google Proprietary	GCP US-Central-1 GCP US-Central-1 (Multi-zone) (Disaster Recovery)
GCP Cloud Identity and Access Management (IAM)	Identity and access management for GCP services.	Google Proprietary	Google Cloud
GCP Load Balancing	Provides cross-region load balancing including automatic multi-region failover.	Google Proprietary	Google Cloud
GitHub	Source code repositories, version control systems, and build software.	GitHub Proprietary	GitHub Proprietary
Google Kubernetes Engine (GKE)	Manages containerized applications which is how all Convictional written services are deployed.	Google Proprietary	GCP US-Central-1 GCP US-Central-1 (Multi-zone) (Disaster Recovery)
Google OAuth	Authentication in the Convictional app (managed by GCP).	GCP Proprietary	GCP Cloud
Mailgun	Offers application programming interfaces (APIs) that allow users to send, receive, and track emails. Also used for system notifications, email reminders, and email reports.	Mailgun Proprietary	Mailgun Cloud
Recall	Provides an API to get recordings, transcripts, and metadata from video conferencing platforms.	Recall Proprietary	Recall region US-East-1
Stripe	Provides subscription usage billing and customer management.	Stripe Proprietary	Stripe Cloud

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Supporting Tools	
System/Application	**Business Function/Description**
Bitwarden	Password vault for shared secrets for supporting tools.
Certn	Third-party system for employee background checks.
DBT	Transforms data for analytics.
Dependabot	Static code analysis tool for code repositories in GitHub.
Federacy	Provides penetration testing, bug bounty administration, and secure vulnerability reporting to security researchers.
Google Cloud Operations	Suite designed to monitor, troubleshoot, and improve cloud infrastructure, software, and application performance.
GCP Security Center	Provides continuous daily internal vulnerability scanning (e.g., exposure of internal services, ports, and other access methods).
GCP Cloud Tasks	Queuing system service for Google Cloud Platform for managing the execution, dispatch, and delivery of tasks, such as sending transactional emails.
Google Workspace	Office communication services.
HubSpot	Provides customer relationship management (CRM) hosting for customer communication.
ngrok	Provides publicly accessible domains for development.
Rippling	Human resource information system (HRIS).
Squarespace	Provides domain registration and domain name system (DNS).
Terraform	Used to apply changes to Google cloud automatically without applying the changes manually within the console.
Vanta	Provides continuous monitoring of security and compliance posture.
Sentry	Provides error management and anonymized session replay.
Slack	Provides inter-office communications.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Overall Technical Diagram



©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

People

Convictional employees are organized in the following functional areas:

- **Executive Leadership:** Responsible for overseeing company wide activities, establishing and accomplishing goals, overseeing objectives, and and key performance indicators (KPIs), and approving internal policies.
- **Information Security:** Responsible for determining the information security program roadmap. This information security function is responsible for the oversight of internal control and includes members independent from control operators. The information security function, under the independent direction of executive leadership, oversees the security activities and communication of its policies and procedures, and includes responsibility over access controls and security of the production environment in conjunction with engineering. Also responsible for business continuity, incident response, and operational monitoring. Additionally, responsible for the risk assessment and risk management processes in partnership with legal and finance. May also include members of the IT and engineering teams.
    - **Incident Managers:** Primarily responsible for incident response and resolution.
- **Information Technology (IT):** Responsible for managing laptops, software, and other technology involved in employee productivity and business operations. Also responsible for third-party management and vendor risk. May include members of the engineering team.
- **Sales and Marketing:** Responsible for sales, account management, customer success, and customer support activities.
- **Engineering:** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Also responsible for the product life cycle, including adding additional product functionality and asset management. Additionally, responsible for vulnerability management, access controls, data deletion procedures, and security of the production environment.
- **Human Resources:** Responsible for recruiting and onboarding new personnel, defining roles and positions for new hires, performing background checks, and facilitating the employee termination process.
- **Legal and Finance:** Responsible for the company finances and legal affairs. Also responsible for controls to mitigate financial fraud and risk management processes in partnership with information security.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Data

Data, as defined by Convictional, constitutes any information collected from employees, candidates, users, customers, vendors, or other parties that provide information to Convictional.

Convictional has a Data Classification Policy in place that defines system and operational requirements for data classification, retention, encryption, storage, and secure disposal. The policy is reviewed and approved on at least an annual basis by members of executive leadership.

Information assets are assigned a sensitivity level based on the audience for the information. The sensitivity level then guides the selection of protective measures to secure the information. All data is to be assigned one of the following sensitivity levels:

Category	Description	Examples
Confidential Data	Valuable and sensitive information where the level of protection is dictated externally by legal requirements and/or by contractual requirements. Access to customer data and information is limited to authorized employees, contractors, and business partners with a specific need.	• User accounts • Customer email addresses • Customer first and last names • Company name • Custom orders • Customer communications
Internal Data	Information that originated or is owned internally, or has been entrusted to Convictional by third parties. Internal data and information may be shared with authorized employees, contractors, and business partners, but it may not be released to the general public.	• Internal system-recorded information • Account creation date • Date of last login
Public Data	Information that has been approved for release to the public and is freely shareable both internally and externally.	• Public website • Press releases

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Processes and Procedures

Convictional has developed and communicated policies and procedures to manage the information security of the system. Information security policies, including sanctions for policy violations, are approved by the executive leadership team at least annually and published on internal collaboration tools (Vanta) accessible to all personnel with access to the company systems. These policies and procedures cover the following key security life cycle areas:

- Acceptable Use
- Asset Management
- Backups
- Business Continuity
- Change Management
- Code of Conduct
- Data Classification, Retention, and Disposal
- Data Deletion
- Data Protection
- Disaster Recovery Plan
- Encryption and Key Management
- Incident Response Plan
- Information Security
- Password
- Physical Security
- Responsible Disclosure
- Risk Assessment and Management
- System Access and Authorization Control
- Vendor Management
- Vulnerability Management

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

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

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of Convictional's description of the system. This section provides information about the five interrelated components of internal control at Convictional, including:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring activities

Control Environment

Integrity and Ethical Values

Convictional has developed a Code of Conduct that addresses acceptable business practices, conflicts of interest, and expected standards of ethical and moral behavior. The company has also developed employee confidentiality agreements that prohibit inappropriate use and disclosure of customer or company information. All employees are required to read and accept the employee confidentiality agreement and information security policies, which include the Code of Conduct and Acceptable Use Policy, during the first 30 days of hire and after a significant modification occurs.

Executive Leadership Oversight

Convictional’s control awareness is significantly influenced by its executive leadership. Attributes that define “tone at the top” include executive leadership’s experience and stature of its members, their involvement and scrutiny of operational activities, and their interaction with independent assessments of the company’s operations and information security posture.

Management’s Philosophy and Operating Style

Convictional’s control environment reflects the philosophy of executive leadership. Convictional's information security function meets frequently and includes at least an annual meeting with executive leadership to review policies and procedures and set the information security program roadmap. The security function, under the direction of executive leadership, oversees the security activities and communication of its policies and procedures. An information security function with roles and responsibilities is documented in the Information Security Policy and approved annually by management. This executive leadership is responsible for the oversight of internal control and includes members independent from control operators.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Authority and Responsibility

Management and employees are assigned levels of authority and responsibility to facilitate internal control. In addition to a dedicated information security function, each policy has an individual owner with accountability and authority over policy enforcement, supported by management.

Human Resources

Convictional maintains formal hiring policies and procedures. Candidates are evaluated through a formal interview process against requirements outlined in documented job descriptions for personnel responsible for designing, developing, implementing, operating, monitoring, and maintaining the system. Background checks are performed on new personnel, prior to employment, as permitted by local laws. These checks are proportional to the business requirements, classification of the information to be accessed, and perceived risk.

Within 30 days of hire and annually thereafter, employees must complete general security awareness training, as required by the Information Security Policy. The general security awareness training is provided and tracked by Vanta. Topics covered during the training include spam, passwords, and data breaches. The training courses are designed to assist employees in understanding security best practices to maintain the security of internal and external data.

Management (i.e., the managers of each employee) conducts annual employee performance evaluations against their job performance, job function and company objectives.

If an employee violates the Code of Conduct in the employee handbook or the company's policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.

Risk Assessment

Convictional regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to the 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).

The information security function assesses security, availability, and confidentiality risks on an ongoing basis. This is done through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual risk assessment in conjunction with company wide risk assessments.

The annual risk assessment is communicated by the information security function and approved by executive leadership. As part of the assessment, risks affecting the organization and recommended courses of action are identified and discussed. Where applicable, mitigating controls are recommended and implemented to address the risks.

Management considers the potential for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws.

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, management considers fraud factors in each risk evaluated during the risk assessment process.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

The information security team, as part of its annual Information Security Policy review, considers developments in technology and the impact of applicable laws and regulations on Convictional's security policies.

Security, availability, and confidentiality risks related to external parties (such as contractors and vendors) are identified and addressed based on the third party risk management program. Designated responsibilities are defined in reviewing risks associated with external parties and establishing relevant agreements.

An annual third party risk assessment is performed by the IT team, including a review of attestation reports (i.e., SOC 2) for critical vendors where user data is shared. Results and action items are communicated to the respective owners and tracked through internal risk management tools.

Changes in security, availability, and confidentiality threats and risks are reviewed by Convictional, and updates to existing control activities and information security policies are performed as necessary.

Control Activities

Convictional's control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Logical Access Control

Access Provisioning

Convictional provides employees access to infrastructure via a role-based access control system to ensure uniform, least-privilege access to identified users and to maintain simple and reportable user provisioning and deprovisioning processes. User access is provisioned and approved by engineering in accordance with the Access Control Policy based on least privilege access principles. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel within the engineering team.

Access Deprovisioning

There is a termination process in place to help ensure access is removed within one business day of termination or if access is no longer required. This process kicks off after a notification from the employee's manager who then notifies engineering and HR. Vanta is utilized to track completion of offboarding and confirmation that offboarding is completed. Additionally, an offboarding checklist is used to document the removal of access to systems.

Access Reviews

User access is reviewed quarterly by members of the engineering team to determine if each individual's access is necessary for their job functions and to identify the existence of inappropriate accounts. Access issues, if any, are resolved as part of the review process.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Privileged Access

Administrative access to systems is restricted to authorized system and security administrators. Powerful service/system accounts and keys are appropriate and are either restricted from direct user authentication or authorized to unique users through a password vault or equivalent security solution.

Authentication

Unique user identification numbers, names, and passwords or tokens are required to authenticate users to the system. Password parameters systematically enforce company policy and require complex passwords that include at least one uppercase letter, one lowercase letter, one number, and one non-alphanumeric character, and are at least 10 characters long. Multi-factor authentication (MFA) is enforced to access cloud services containing company data. In instances where keys are used to authenticate to production, system access keys are rotated at least annually.

Physical Access and Environmental Controls

No servers or computer facilities supporting the Convictional System are hosted on site at Convictional facilities. All servers or computer facilities and physical access thereto are controlled at cloud infrastructure data centers. Therefore, controls related to physical security are the responsibility of the subservice organizations and are described in the complementary subservice organization controls presented in this system description.

Incident Management

Convictional defines a security incident as a violation, or imminent threat of violation, of security policies, acceptable use policies, or standard security practices. An operational incident is an event that impacts the company's ability to meet availability SLAs or impairs processing capabilities. Convictional has procedures in place for preparing, detecting, analyzing, triaging, and performing post-mortem reviews over incidents.

Preparation

Convictional has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. This framework is communicated to internal users, via the incident response plan, which is available on the internal compliance tool (i.e., Vanta). For external users, Convictional communicates the incident reporting and response procedures via customer agreements, the company's website, and ongoing communications.

Convictional prevents incidents via annual risk assessments, effective network security, anti-malware on devices, and security awareness training.

Convictional maintains on-call incident support in the form of rotating incident managers who are the primary and ultimate decision maker during the response period. The incident manager is ultimately responsible for resolving the incident and formally closing incident response actions.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Detection and Analysis

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Monitoring and alarming tools are configured to identify and notify management of incidents when thresholds are crossed on key security and operational metrics. Customer incidents, if any, are reported and resolved through one-to-one communication via the customer ticketing system, HubSpot.

Incidents are prioritized and ranked based on severity. Incident ratings and escalation procedures are as follows:

Incident Rating	Description	Examples	Escalation Procedures
Low	Most issues fall under this category. These do not require someone to be paged or woken up in the middle of the night.	Suspicious emails, outages, strange activity on a laptop	The ticket is filed in the issue management system on GitHub.
High	These are problems where an adversary or active exploitation hasn't been proven yet, and an attack may not have happened, but is likely to happen.	Backdoors, malware, malicious access of business data (e.g., passwords, payment information, vulnerability data, etc.)	The information security team is alerted immediately upon detection; senior engineers with relevant portfolios are notified within one hour.
Critical	The attackers were successful, and something was lost.	Active exploited risk or threat involving a malicious actor.	The information security team and executive leadership are alerted immediately upon detection; response initiated within 15 minutes.

Where required, security incidents are escalated to the information security function, including incident managers.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Containment, Eradication, and Recovery

Containment strategies should be identified and implemented before an incident overwhelms resources or increases damage. Containment strategies vary based on the type of incident. Criteria for determining the appropriate containment strategy include:

- Potential damage to and theft of resources;
- Need for evidence preservation;
- Service availability (e.g., network connectivity, services provided to external parties);
- Time and resources needed to implement the strategy;
- Effectiveness of the strategy (e.g., partial containment, full containment); and,
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, all affected hosts within the organization are identified and remediated.

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security.

Post-incident Activity

Post-mortem activities are conducted for incidents with high severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

Network Operations Monitoring

The network is segmented based on the label or classification level of the information stored on the servers. Firewall rules for the VPC networks are configured to enforce perimeter security including configurations that deny all traffic by default, restrict ingress traffic from sensitive protocols, and restrict authentication to infrastructure systems to trusted IP addresses. Operations and security functions use a variety of security utilities to identify and detect possible security threats and incidents. Utilities include regular security scans, vulnerability assessment reports, irregular login activity, firewall notifications through GCP as well as strict access control to the firewall configuration, operating system event logs; all of which are internally monitored on a regular basis.

Security events requiring further investigation are tracked using internal ticketing systems and monitored until resolved.

Convictional only uses network ports, protocols, and services listening on a system with validated business need to run on each system. Default-deny rules drop traffic except those services and ports that are explicitly allowed.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Cryptography

User requests to the Convictional System are encrypted using TLS using certificates from an established third party certificate authority. Remote system administration access to Convictional web and application servers is available through cryptographic network protocols. Data at rest is encrypted using Advanced Encryption Standard (AES) 256 bit. Data in transit over public networks are encrypted using strong encryption protocols, such as TLS 1.2 or TLS 1.3.

Change Management

Convictional has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning. GitHub issues or discussions can be created to discuss a proposed change. Proposed changes are introduced through a pull request (PR) which are peer reviewed before merging. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed.

Change control, as defined by policy, requires approval and a peer review by an independent developer prior to deployment into a production release to help ensure change requirements are met and security issues are resolved. This happens during the PR process and is enforced through branch protection settings on GitHub.

Changes to infrastructure and software are developed and tested in a separate development or test environment before implementation. Static analysis tools are used to verify secure coding practices are adhered to for internally developed software, including linting, continuous integration, checks, and security scans. Issues identified during testing are remediated prior to production release and documented within the change tool.

Customer content and personal information are not used in non-production environments. Additionally, changes require one or more independent peer review from a developer prior to being merged to the main branch. Access to migrate code changes to production is restricted to authorized engineering personnel. Access to override branch protection settings is limited based on the principle of least privilege to admins.

GitHub Dependabot and GitHub Advanced Security are used to ensure code dependencies are up to date and code vulnerabilities are identified and addressed prior to release. In addition, automated software update tools are in place to ensure production infrastructure is running the most up to date version.

All software is version controlled and synced between contributors (developers). Access to the central repository is restricted based on an employee's role. Using a decentralized version control system allows multiple developers to work simultaneously on features, bug fixes, and new releases.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. Convictional uses tagging tools (i.e., Vanta) to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Vulnerability Management and Penetration Testing

Vulnerability scanning tools in GitHub (Dependabot) and GCP (GCP Security Center) are used to automatically scan the Convictional environment on a continuous basis. Issues, if any, are routed through incident and risk management processes for resolution and resolved in accordance with the service-level agreements for high, medium, and low risk rankings.

Penetration tests are performed at least annually and include a full scope of blended attacks, such as client-based and web-application attacks. Issues, if any, are tracked through risk management processes and tools to resolution.

Vulnerabilities identified are risk-ranked from low to critical to prioritize the remediation of discovered vulnerabilities. All vulnerabilities are initially handled by senior engineers who assign tickets to appropriate team members to resolve. The vulnerability tickets follow Convictional's change management process to implement necessary patches and, once the change is applied, exceptions are noted in the company's Risk Register. Senior engineers check the source from which the vulnerability originated to ensure the change performed has addressed the vulnerability detected. The patched vulnerability ticket is then closed.

Endpoint Management

Endpoint management solutions are in place that include policy enforcement on both company issued devices (i.e., mobile phones and laptops) that could connect to or access data within the system boundaries.

Policies enforced on endpoints include controls such as:

- Anti-malware protection
- Enforce encryption on devices for data at rest

Availability

Convictional has a documented business continuity plan (BCP), which includes an annual test of the disaster recovery plan. At a minimum, daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are monitored and alerted by Google Cloud Operations or Datadog. Backups are restored regularly as part of operational activities and included as part of the BCP test plan. Critical system components are replicated across multiple availability zones or regions to permit the resumption of critical operations in the event of loss of a critical facility.

Confidentiality

Convictional is committed to the confidentiality of customer data. Convictional has confidentiality commitments with their customers as described in terms and conditions set forth within master service agreements, which must be signed before services start. Service agreements define service levels, rules of use, and additional terms for governing use of the system. Customer data is stored in encrypted volumes and retained per the executed master service agreements (MSAs) and Data Classification, Retention, and Disposal Policy. Per the Data Deletion Policy, Convictional disposes of all customer data within 30 days of request by customers. Once completed, a confirmation is sent back to the customer to notify them that the disposal is complete. Data deletion is the responsibility of the engineering team. Unless a deletion is requested, customer data is retained. Confidentiality agreements are executed with employees and vendors with access to Convictional or customer data.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Information and Communication

Convictional has an Information Security Policy to help ensure employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

Descriptions of the system and its boundaries are available to external users via ongoing communications with customers and official blog posts. Customers report issues by emailing decide@convictional.com. These issues are triaged to the appropriate team to address and fix any incidents or issues.

Monitoring Controls

In addition to the daily oversight, ongoing vulnerability assessments, and use of security information and event management (SIEM), management provides further security monitoring through the security function, which performs periodic audits, ongoing monitoring of KPIs, and information security assessments.
The company selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. KPIs are monitored continuously using automated tools (i.e., Vanta) that are configured to alert system administrators of activity that falls outside of predefined thresholds.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of how the system is used to provide the service during the period from May 1, 2025 to April 30, 2026.

Disclosure of Incidents

There were no system incidents during the period from May 1, 2025 to April 30, 2026, requiring disclosure that either:

- Were the result of controls failing; or,
- Resulted in a significant impairment to the achievement of systems requirements or service commitments to customers.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Complementary User Entity Controls and Responsibilities

Complementary User Entity Controls

There are no controls at the user entity that are necessary, in combination with Convictional's controls, to provide reasonable assurance that Convictional's service commitments and system requirements were achieved based on the applicable trust services criteria (complementary user entity controls).

User Entity Responsibilities

There are, however, certain responsibilities that users of the system must fulfill for the user entity to derive the intended benefits of the services of the system. The user entity responsibilities presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. User entities are responsible for their own control environments and their operational effectiveness.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

User Entity Responsibilities	Criteria
User entity is responsible for protecting established user IDs within their organizations.	Logical Access
User entity is responsible for reviewing customer access to the Convictional System periodically to validate appropriateness of access levels.	Logical Access
User entity is responsible for approving and creating new user access to the Convictional System.	Logical Access
User entity is responsible for removing terminated employee access to the Convictional System.	Logical Access
User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the Convictional System.	Data Classification
User entity is responsible for sending data to Convictional via a secure connection and/or the data should be encrypted.	Cryptography
User entity is responsible for notifying Convictional if they detect or suspect a security incident related to the Convictional System.	Incident Management
User entity is responsible for reviewing email and other forms of communications from Convictional related to changes that may affect Convictional customers and users, and their security, confidentiality, and availability obligations.	Information Communication
User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the system.	Information Security
User entity is responsible for endpoint protection of workstations used to access the system.	Endpoint Management
User entity is responsible for developing their own business continuity and disaster recovery plan.	Business Continuity and Disaster Recovery
User entity is responsible for requesting their data to be deleted.	Data Management
User entity is responsible for the development, content, operation, maintenance, and use of data in AI features.	Data Management

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Complementary Subservice Organization Controls

Convictional uses subservice organizations in support of its Convictional System. Convictional's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Convictional System to be achieved solely by Convictional. Therefore, user entity controls must be evaluated in conjunction with Convictional's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Convictional periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC reports
- Regular meetings to discuss performance
- Non-disclosure agreements

Control Activity Expected to be Implemented by Subservice Organizations	Subservice Organizations	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	GCP	CC6.1, CC6.2, CC6.3
Physical access to the data center facility is restricted to authorized personnel.	GCP, GitHub, Mailgun, Recall, Stripe	CC6.4
Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	GCP, GitHub, Mailgun, Recall, Stripe	CC6.4, A1.2
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	GCP	A1.3
Servers are hardened, including baseline hardening, and maintained by the subservice organizations, as applicable.	GCP, GitHub, Mailgun, Recall, Stripe, Anthropic, OpenAI	CC6.1, CC6.2, CC6.3
Patching is performed and updates are applied for servers and databases.	GCP, GitHub, Mailgun, Recall, Stripe, Anthropic, OpenAI	CC6.8, CC7.1, CC8.1
The company has a defined Data Classification, Retention, and Disposal Policy, which specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality.	GCP, Anthropic, Stripe	C1.1
The company has a defined process to sanitize and destroy hard drives and backup media containing customer data prior to leaving company facilities.	GCP, Anthropic, Stripe	C1.2

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Section IV

Description of Criteria, Convictional's Related Controls, and BARR Advisory, P.A.'s Tests of Controls and Results



©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample-based testing), BARR Advisory, P.A. performed a combination of the following procedures, where possible, based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

1. Inspect the source of the IPE;
2. Inspect the query, script, or parameters used to generate the IPE;
3. Tie data between the IPE and the source; and/or,
4. Inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of controls (e.g., periodic reviews of user access lists), BARR Advisory, P.A. inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Convictional Controls Mapped to the Security, Confidentiality, and Availability Criteria

Criteria	Supporting Control	Criteria Description
1.0 – Common Criteria Related to Control Environment		
CC1.1	HR-01, HR-02, IS-02, IS-03	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
CC1.2	IS-01, RC-01	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	HR-03, IS-01, IS-02, IS-03, IS-04	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	HR-01, HR-02, HR-03, IS-01, IS-02, IS-03, IS-04	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	HR-02, HR-03, IS-01, IS-02, IS-03, IS-04, RC-03	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
2.0 – Common Criteria Related to Information and Communication		
CC2.1	AM-01, RC-01, RC-03, TV-01, TV-02	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	HR-03, IS-01, IS-02, IS-03, IS-04, OM-01, RC-03	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	IS-05, OM-02, OM-03	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
3.0 – Common Criteria Related to Risk Assessment		
CC3.1	IS-01, RC-01, RC-03	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	AM-01, RC-01, RC-02, RC-03, TV-01, TV-02	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.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Criteria	Supporting Control	Criteria Description
CC3.3	IS-03, RC-01, RC-02	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	IS-03, RC-01, RC-02, RC-03	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
4.0 – Common Criteria Related to Monitoring Activities		
CC4.1	OM-01, RC-01, RC-02, RC-03, TV-01	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.
CC4.2	RC-01, RC-02, RC-03, TV-01	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.
5.0 – Common Criteria Related to Control Activities		
CC5.1	IS-01, IS-03, RC-01, RC-03	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.
CC5.2	IS-01, IS-03, RC-01	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	HR-02, IS-01, IS-03, RC-03	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
6.0 – Common Criteria Related to Logical and Physical Access		
CC6.1	AC-01, AC-02, AC-03, AC-04, AC-05, AC-06, AC-07, AM-01, CR-02, SC-01	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.
CC6.2	AC-01, AC-03, AC-04, AC-05, AC-06	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.
CC6.3	AC-02, AC-03, AC-05, AC-06, AC-07, AC-08	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.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Criteria	Supporting Control	Criteria Description
CC6.4	N/A - See complementary subservice organization controls	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5	AC-05, AM-01, TV-03	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.
CC6.6	AC-02, AC-03, AC-04, CR-01, CR-02, OM-01, SC-01, TV-01, TV-03	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	AC-04, AM-01, CR-01, CR-02, OM-01, SC-01, TV-03	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.
CC6.8	AM-01, CR-01, OM-01, TV-01, TV-03	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
7.0 – Common Criteria Related to System Operations		
CC7.1	AM-01, OM-01, OM-02, TV-01, TV-02	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.
CC7.2	AM-01, OM-01, OM-02, RC-03, TV-01, TV-02, TV-03	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.
CC7.3	OM-01, OM-02, RC-03, TV-01, TV-02	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.
CC7.4	BC-01, OM-01, OM-02, TV-01, TV-02	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Criteria	Supporting Control	Criteria Description
CC7.5	BC-01, IS-01, OM-01, OM-02, TV-01	The entity identifies, develops, and implements activities to recover from identified security incidents.
8.0 – Common Criteria Related to Change Management		
CC8.1	AC-07, CM-01, CM-02, CM-03, CM-04	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
9.0 – Common Criteria Related to Risk Mitigation		
CC9.1	BC-01, BC-02, OM-01, RC-01	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	IS-01, RC-01, RC-02, RC-04	The entity assesses and manages risks associated with vendors and business partners.
Additional Criteria for Confidentiality		
C1.1	CM-03, CR-01, CR-02, IS-03, IS-06, OM-04	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2	IS-03, OM-04	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.
Additional Criteria for Availability		
A1.1	BC-01, BC-02, BC-03, OM-01	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.
A1.2	BC-01, BC-02, BC-03, RC-01	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.
A1.3	BC-01	The entity tests recovery plan procedures supporting system recovery to meet its objectives.

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

Security, Confidentiality, and Availability Criteria Mapped to Convictional Controls, BARR Advisory, P.A.'s Tests, and Test Results

No.	Description of Controls	Criteria	Tests of Controls and Test Results
AC-01	Powerful service/system accounts and keys are appropriate and are authorized to unique users through a password vault or equivalent security solution.	CC6.1 CC6.2	Inquired of management and inspected the Access Control Policy, password configuration records, and system-generated user lists for systems listed in the Primary Infrastructure and Software table to determine if powerful service/system accounts and keys were appropriate and were authorized to unique users through a password vault or equivalent security solution in accordance with company requirements. **No exceptions noted.**
AC-02	Administrator access is restricted to authorized system and security administrators.	CC6.1 CC6.3 CC6.6	Inquired of management and inspected the System Access and Authorization Control Policy and system-generated lists of administrator access privileges from systems listed in the Primary Infrastructure and Software table to determine if administrator access was restricted to authorized system and security administrators in accordance with company requirements. **No exceptions noted.**
AC-03	User access is approved by management in accordance with the Access Control Policy based on least privilege access principles.	CC6.1 CC6.2 CC6.3 CC6.6	Inquired of management and inspected the Access Control Policy and provisioning documentation for a selection of new users to determine if user access was approved by management based on least privilege access principles in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
AC-04	Password configurations are documented and systematically enforced in compliance with the Password Policy. Access to cloud services or remote access systems requires multi-factor authentication.	CC6.1 CC6.2 CC6.6 CC6.7	Inquired of management and inspected the Password Policy and authentication configurations from systems listed in the Primary Infrastructure and Software table to determine if password configurations were systematically enforced in compliance with company policy, and access to cloud services or remote access systems required MFA in accordance with company requirements. **No exceptions noted.**
AC-05	Terminated user access to production systems, tools, and the network is removed within one business day.	CC6.1 CC6.2 CC6.3 CC6.5	Inquired of management and inspected the Access Control Policy, termination tickets, and system-generated access removal logs for a selection of terminated users to determine if terminated user access to production systems, tools, and the network was removed within one business day in accordance with company requirements. **No exceptions noted.**
AC-06	User profile and access reviews are performed each quarter and include active user accounts for employees and contractors. Access issues, if any, are resolved.	CC6.1 CC6.2 CC6.3	Inquired of management and inspected the Access Control Policy and access review documentation for a selection of quarters to determine if user profile and access reviews were completed each quarter for systems in the Primary Infrastructure and Software table, that the reviews included active user accounts for employees and contractors, and access issues, if any, were resolved in accordance with company requirements. **No exceptions noted.**

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

No.	Description of Controls	Criteria	Tests of Controls and Test Results
AC-07	Access to migrate changes to production is restricted to authorized personnel. Code management tools enforce branch protection to restrict users from bypassing standard change controls.	CC6.1 CC6.3 CC8.1	Inquired of management and inspected the Change Management Policy and a system-generated list of users with access to migrate changes to production to determine if access to migrate changes to production was restricted to authorized personnel in accordance with company requirements. Inspected code management tools to determine if branch protection settings were enforced that restricted users from bypassing standard change control and restricted access to migrate changes to production to authorized personnel in accordance with company requirements. **No exceptions noted.**
AC-08	Access keys with production privileges are rotated annually.	CC6.3	Inquired of management and inspected the Encryption and Key Management Policy, access key credentials established, and key ages from the infrastructure environment to determine if access keys with production privileges were rotated annually in accordance with company requirements. **No exceptions noted.**
AM-01	Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels to help ensure assets were classified appropriately and tracked as part of configuration management.	CC2.1 CC3.2 CC6.1 CC6.5 CC6.7 CC6.8 CC7.1 CC7.2	Inquired of management and inspected the Asset Management Policy and current asset inventory to determine if assets used in the system were inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets were classified appropriately and tracked as part of configuration management in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
BC-01	A documented business continuity and disaster recovery plan is in place, and is tested and approved on an annual basis.	A1.1 A1.2 A1.3 CC7.4 CC7.5 CC9.1	Inquired of management and inspected the Business Continuity Policy, DRP, and results of the most recent BC/DR test scenario to determine if they were tested and approved on an annual basis in accordance with company requirements. **No exceptions noted.**
BC-02	Critical system components are replicated across multiple availability zones or regions to permit the resumption of critical operations in the event of loss of a critical facility.	A1.1 A1.2 CC9.1	Inquired of management and inspected the disaster recovery plan and system configuration settings for a selection of critical system components to determine if critical system components were replicated across multiple availability zones or regions to permit the resumption of critical operations in the event of loss of a critical facility in accordance with company requirements. **No exceptions noted.**
BC-03	Backups of critical system components are performed at least daily. Alerts are configured to notify key personnel of backup failures, if any.	A1.1 A1.2	Inquired of management, inspected the Backup Policy, configuration settings, backup history, and alert settings to determine if backups of critical system components were performed at least daily, and if alerting was configured to notify key personnel of backup failures, if any, in accordance with company requirements. **No exceptions noted.**
CM-01	Change control, as defined by policy, requires a peer review and approval prior to implementation to help ensure change requirements are met and security issues are resolved.	CC8.1	Inquired of management and inspected the Change Management Policy and documentation for a selection of code changes to determine if change control required a peer review and approval prior to implementation to help ensure change requirements were met and security issues were resolved in accordance with company requirements. **No exceptions noted.**

No.	Description of Controls	Criteria	Tests of Controls and Test Results
CM-02	Changes are tested according to the nature of the change in an environment separate from production prior to deployment into a production release.	CC8.1	Inquired of management and inspected Change Management Policy and change documentation for a selection of code changes to determine if changes were tested in an environment separate from production prior to deployment into a production release in accordance with company requirements. **No exceptions noted.**
CM-03	Customer content and personal information are not used in non-production environments.	C1.1 CC8.1	Inquired of management and inspected the Change Management Policy, non-production data samples, and non-production environment configurations to determine if customer content and personal information were not used in non-production environments in accordance with company requirements. **No exceptions noted.**
CM-04	A security analysis is performed to verify secure coding practices are followed during change control. Vulnerabilities identified, if any, are tracked to resolution.	CC8.1	Inquired of management and inspected the Change Management Policy and change documentation for a selection of code changes to determine if a security analysis was performed to verify secure coding practices were followed during change control, and vulnerabilities identified, if any, were tracked to resolution in accordance with company requirements. **No exceptions noted.**
CR-01	Data in transit over public networks are encrypted using strong encryption protocols such as TLS 1.2 or TLS 1.3.	C1.1 CC6.6 CC6.7 CC6.8	Inquired of management and inspected the Encryption and Key Management Policy and cryptography and security protocols to determine if strong encryption, such as TLS 1.2 or TLS 1.3, was used for data transmission over open, public networks in accordance with company requirements. **No exceptions noted.**

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

No.	Description of Controls	Criteria	Tests of Controls and Test Results
CR-02	Strong cryptography standards for the storage of data are enforced in accordance with policy.	C1.1 CC6.1 CC6.6 CC6.7	Inquired of management, inspected the Data Protection Policy, Encryption and Key Management Policy, and encryption protocols in place for stored data to determine if strong cryptography standards for the storage of data were enforced in accordance with company policy and requirements. **No exceptions noted.**
HR-01	Background checks are performed on personnel prior to employment, as permitted by local laws.	CC1.1 CC1.4	Inquired of management and inspected the Information Security Policy and background check records for a selection of new hire personnel to determine if background checks were performed on personnel prior to hire, as permitted by local laws and in accordance with company requirements. **No exceptions noted.**
HR-02	New hires are required to read and acknowledge an employee confidentiality agreement and information security policies, which include the Code of Conduct and Acceptable Use Policy, during the first 30 days of hire and after a significant modification occurs.	CC1.1 CC1.4 CC1.5 CC5.3	Inquired of management and inspected the Information Security Policy and policy acceptance records for a selection of new hires and current employees to determine if new hires were required to read and acknowledge an employee confidentiality agreement and information security policies, which included the Code of Conduct and Acceptable Use Policy, during the first 30 days of hire and after a significant modification occurs in accordance with company requirements. **No exceptions noted.**

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

No.	Description of Controls	Criteria	Tests of Controls and Test Results
HR-03	Convictional has defined job descriptions for personnel responsible for designing, developing, implementing, operating, monitoring, and maintaining the system. To fill these job roles, candidates are evaluated against job requirements through a formal interview process.	CC1.3 CC1.4 CC1.5 CC2.2	Inquired of management and inspected interview notes and job descriptions for a selection of personnel to determine if Convictional had defined job descriptions for personnel responsible for designing, developing, implementing, operating, monitoring, and maintaining the system and, to fill these job roles, candidates were evaluated against job requirements through a formal interview process in accordance with company requirements. **No exceptions noted.**
IS-01	An information security function with roles and responsibilities is documented in the Information Security Policy and approved annually by management. The executive leadership team is responsible for the oversight of internal control and includes members independent from control operators.	CC1.2 CC1.3 CC1.4 CC1.5 CC2.2 CC3.1 CC5.1 CC5.2 CC5.3 CC7.5 CC9.2	Inquired of management and inspected the Information Security Policy to determine if an information security function with roles and responsibilities was documented in the Information Security Policy and approved annually by management, and the executive leadership team was responsible for the oversight of internal control, and included members independent from control operators, in accordance with company requirements. **No exceptions noted.**
IS-02	The company provides security awareness training to employees within 30 days of hire and annually thereafter, as required by the Information Security Policy.	CC1.1 CC1.3 CC1.4 CC1.5 CC2.2	Inquired of management and inspected the Information Security Policy and security awareness training records for a selection of new hires and current employees to determine if Convictional provided security awareness training to employees within 30 days of hire and annually thereafter, as required by the Information Security Policy and company requirements. **No exceptions noted.**

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

No.	Description of Controls	Criteria	Tests of Controls and Test Results
IS-03	Information security policies, including sanctions for policy violations, are approved by management at least annually and published on internal collaboration tools accessible to all personnel with access to the company systems.	C1.1 C1.2 CC1.1 CC1.3 CC1.4 CC1.5 CC2.2 CC3.3 CC3.4 CC5.1 CC5.2 CC5.3	Inquired of management and inspected information security policies to determine if the policies included sanctions for policy violations, were approved by management annually, and were published on internal collaboration tools accessible to company personnel with access to the company systems in accordance with company requirements. **No exceptions noted.**
IS-04	Management conducts annual employee performance evaluations against company objectives.	CC1.3 CC1.4 CC1.5 CC2.2	Inquired of management and inspected documentation for the most recent employee performance evaluations for a selection of current employees to determine if management conducted annual employee performance evaluations against company objectives in accordance with company requirements. **No exceptions noted.**
IS-05	Descriptions of the system and its boundaries are available to external users via ongoing communications with customers, official blog posts, and status portals. Customer-reported issues, if any, are routed through internal processes.	CC2.3	Inquired of management and inspected system descriptions and communications to determine if descriptions of the system and its boundaries were available to external users via ongoing communications with customers, blog posts, and status portals in accordance with company requirements. Inspected a selection of customer-reported issues to determine if they were routed through internal processes in accordance with company requirements. **No exceptions noted.**

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

No.	Description of Controls	Criteria	Tests of Controls and Test Results
IS-06	A Data Classification Policy and Data Protection Policy is in place that defines system and operational requirements for data classification, retention, encryption, storage, and secure disposal. The policy is reviewed and updated at least annually.	C1.1	Inquired of management and inspected the Data Classification Policy and Data Protection Policy to determine if they defined system and operational requirements for data classification, retention, encryption, storage, and secure disposal, and if the policies were reviewed and updated accordingly within the past year in accordance with company requirements. **No exceptions noted.**
OM-01	Monitoring and alarming are configured to identify and notify management of incidents when thresholds are crossed on key security and operational metrics. Issues are resolved in accordance with incident management processes.	A1.1 CC2.2 CC4.1 CC6.6 CC6.7 CC6.8 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5 CC9.1	Inquired of management and inspected the incident response plan, monitoring and alarming tool configurations, and documentation for a selection of security alerts generated by monitoring and alarming tools to determine if monitoring and alarming were configured to identify and notify management of incidents when thresholds were crossed on key security and operational metrics, and issues were resolved in accordance with incident management processes and company requirements. **No exceptions noted.**
OM-02	Policy and procedure documentation for incident management, which includes the responsibility and escalation levels for reporting operational failures, security incidents, system problems, and user complaints, and the process for doing so, is made available to internal and external users.	CC2.3 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	Inquired of management and inspected the incident response plan and procedures and evidence of communication of the incident response policies and procedures to determine if policy and procedure documentation for incident management, which included the responsibility and escalation levels for reporting operational failures, security incidents, system problems, and user complaints, and the process for doing so, was made available to internal and external users in accordance with company requirements. **No exceptions noted.**

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

No.	Description of Controls	Criteria	Tests of Controls and Test Results
OM-03	Customers are required to read and accept the Convictional terms of service when signing up for services. Service agreements define service levels, rules of use, and additional terms for governing use of the system.	CC2.3	Inquired of management and inspected the terms of service and account creation process to determine if customers were required to accept the Convictional terms of service when signing up for services, and that service agreements were in place that defined service levels, rules of use, and additional terms for governing use of the system in accordance with company requirements. **No exceptions noted.**
OM-04	Customer data is disposed of within 30 days of request by customers. For disposal requests, a confirmation is sent back to the customer to notify them that the disposal is complete.	C1.1 C1.2	Inquired of management and inspected the Data Deletion Policy and completed data deletion requests, along with communication of completion back to the client, for a sample of customer data deletion requests to determine if customer data was disposed of within 30 days of request by customers and, for disposal requests, a confirmation was sent back to the customer to notify them that the disposal was complete in accordance with company requirements. **No exceptions noted.**
RC-01	A formal risk assessment is performed on an annual basis where relevant risks to the organization, including fraud, are identified and evaluated. Identified risks and mitigation strategies, including risk owners, are documented within a centralized risk register.	A1.2 CC1.2 CC2.1 CC3.1 CC3.2 CC3.3 CC3.4 CC4.1 CC4.2 CC5.1 CC5.2 CC9.1 CC9.2	Inquired of management and inspected the Risk Assessment and Management Policy and most recent risk assessment to determine if a risk assessment was performed within the last year, relevant risks, including fraud, were identified and evaluated, mitigation strategies were documented, and risk owners were identified within a centralized risk register in accordance with company requirements. **No exceptions noted.**

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

No.	Description of Controls	Criteria	Tests of Controls and Test Results
RC-02	An annual third-party risk assessment is performed including a review of attestation reports (e.g., SOC 2 attestations) when available. Results and action items are communicated to the respective owners and tracked through internal risk management tools.	CC3.2 CC3.3 CC3.4 CC4.1 CC4.2 CC9.2	Inquired of management and inspected the Vendor Management Policy and results of the most recent third-party risk assessment to determine if: • It was completed within the last year; • It included all third party providers; • It included a review of attestation reports (e.g., SOC 2 attestations) if available; and, • Results and action items were communicated to the respective owners and tracked through internal risk management tools in accordance with company requirements. **No exceptions noted.**
RC-03	Information security KPIs are monitored continuously using automated tools that are configured to alert system administrators of activity that falls outside of predefined thresholds.	CC1.5 CC2.1 CC2.2 CC3.1 CC3.2 CC3.4 CC4.1 CC4.2 CC5.1 CC5.3 CC7.2 CC7.3	Inquired of management and inspected KPI monitoring and alerting configurations to determine if information security KPIs were monitored continuously using automated tools that were configured to alert system administrators of activity that falls outside of predefined thresholds in accordance with company requirements. **No exceptions noted.**
RC-04	Confidentiality agreements are in place for vendors with access to customer data.	CC9.2	Inquired of management and inspected the Vendor Management Policy, as well as executed agreements for a selection of vendors with access to customer data, to determine if confidentiality agreements were in place for vendors with access to customer data in accordance with company requirements. **No exceptions noted.**

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

No.	Description of Controls	Criteria	Tests of Controls and Test Results
SC-01	Firewall rules for the VPC networks are configured to enforce perimeter security, including configurations that deny all traffic by default, restrict ingress traffic from sensitive protocols, and restrict authentication to infrastructure systems to trusted IP addresses.	CC6.1 CC6.6 CC6.7	Inquired of management and inspected the firewall rules for the VPC networks to determine if firewalls were configured to enforce perimeter security, including configurations that deny all traffic by default, restrict ingress traffic from sensitive protocols, and restrict authentication to infrastructure systems to trusted IP addresses, in accordance with company requirements. **No exceptions noted.**
TV-01	Vulnerability scans are performed on a continuous basis. Identified vulnerabilities are risk ranked and routed through incident and risk management processes for remediation.	CC2.1 CC3.2 CC4.1 CC4.2 CC6.6 CC6.8 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	Inquired of management and inspected the Vulnerability Management Policy, vulnerability scan configurations, vulnerability SLA compliance history for the audit period, and remediation evidence for a selection of current vulnerabilities to determine if vulnerability scans were performed on a continuous basis and identified vulnerabilities were risk ranked and routed through incident and risk management processes for remediation in accordance with company requirements. **No exceptions noted.**
TV-02	External penetration testing is performed at least annually. Issues, if any, are routed through incident and risk management processes for resolution.	CC2.1 CC3.2 CC7.1 CC7.2 CC7.3 CC7.4	Inquired of management and inspected the Vulnerability Management Policy and most recently completed penetration test report to determine if external penetration testing was performed at least annually and issues, if any, were routed through incident and risk management processes for resolution in accordance with company requirements. **No exceptions noted.**

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |

No.	Description of Controls	Criteria	Tests of Controls and Test Results
TV-03	Encryption and antivirus software is installed on mobile devices (e.g., workstations, laptops) with access to production systems.	CC6.5 CC6.6 CC6.7 CC6.8 CC7.2	Inquired of management and inspected the Acceptable Use Policy and configuration settings for a selection of mobile devices with access to production to determine if antivirus software was installed on mobile devices and if devices were encrypted in accordance with company requirements. **No exceptions noted.**

©2026 Convictional, Inc. | All rights reserved | CONFIDENTIAL |