



SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON
MANAGEMENT'S DESCRIPTION OF ITS

CanIPhish Cloud Platform

Relevant to Security, Availability, and Confidentiality

For the period 1 June 2025 to 30 November 2025

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:



Table of Contents

1. Independent Service Auditors' Report	1
Scope	1
Service Organization's Responsibilities	1
Service Auditors' Responsibilities	1
Inherent Limitations	2
Opinion	2
2. Assertion of CanIPhish Management	3
3. Description of CanIPhish's Cloud Platform	4
Company Background	4
Services Provided	4
Principal Service Commitments and System Requirements	4
Components of the System	4

1. Independent Service Auditors' Report

To the Management of Can I Phish Pty Ltd (CanIPhish)

Scope

We have examined CanIPhish's accompanying assertion titled "Assertion of CanIPhish" (assertion) that the controls within CanIPhish's Platform (system) were effective throughout the period 1 June 2025 to 30 November 2025, to provide reasonable assurance that CanIPhish's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in SP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)* in AICPA, *Trust Services Criteria*.

Service Organization's Responsibilities

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

Service Auditors' Responsibilities

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

- Assessing the risks that controls were not effective to achieve CanIPhish's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve CanIPhish's service commitments and system requirements based on the applicable trust services criteria

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

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

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements 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.

Opinion

In our opinion, management's assertion that the controls within CanIPhish's Cloud Platform were effective throughout the period 1 June 2025 to 30 November 2025, to provide reasonable assurance that CanIPhish's services commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



San Jose, California
22 January 2026

2. Assertion of CanI Phish Management

We are responsible for designing, implementing, operating and maintaining effective controls within Can I Phish Pty Ltd's (CanI Phish) Cloud Platform throughout the period 1 June 2025 to 30 November 2025 to provide reasonable assurance that CanI Phish's service commitments and system requirements relevant to Security, Availability and Confidentiality were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of CanI Phish's Cloud Platform" (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period 1 June 2025 to 30 November 2025, to provide reasonable assurance that CanI Phish's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

CanI Phish's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period 1 June 2025 to 30 November 2025, to provide reasonable assurance that CanI Phish's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by CanI Phish Management

22 January 2026

3. Description of CanIPhish's Cloud Platform

Company Background

Can I Phish Pty Ltd ('CanIPhish') was founded in February 2021 with the objective of providing a simulated phishing and security awareness training Cloud Platform. The CanIPhish mission is simple yet essential: to provide organizations with a training experience that engages learners through immersive real-world scenarios and interactive learning. This mission is fueled by the desire to ensure every business has access to a cost-effective platform to train their employees.

Services Provided

CanIPhish's product, the CanIPhish Cloud Platform (the System), provides phishing simulation and training capabilities. The System delivers simulated phishing scenarios and tracks user responses to support security awareness training activities within a controlled environment.

Principal Service Commitments and System Requirements

CanIPhish has established processes, policies, and procedures to meet its objectives related to its Cloud Platform (the 'System'). Those objectives are based on the purpose, vision, and values of CanIPhish as well as commitments that CanIPhish makes to user entities, the requirements of laws and regulations that apply to CanIPhish's activities, and the operational requirements that CanIPhish has established.

Commitments are documented, and communicated in customer agreements, as well as in public descriptions of the System. The operational requirements are communicated in CanIPhish's processes, policies and procedures, system design documentation, and customer agreements. This includes policies around how the System is designed and developed, how the System is operated, how the system components are managed, and how employees are hired, developed, and managed to support the System.

Components of the System

CanIPhish utilizes industry-leading cloud service providers to ensure data integrity and availability.

People

CanIPhish's personnel are organized into the following functional areas:

- **Leadership:** The executive level responsible for corporate governance.
- **Product:** Responsible for managing the roadmap of requirements and balancing the Engineering team priorities.
- **Engineering:** Responsible for building and maintaining the infrastructure and software.

- Customer Success: Responsible for the customer experience, support, and services.
- Operations: Responsible for monitoring and supporting robust and effective company and system operations.
- Risk and Compliance: Responsible for identification, assessment, treatment and monitoring to manage risks and support compliance.
- Partnerships: Responsible for managing partnerships with complementary service providers.
- Sales: Responsible for onboarding new customers and aligning requirements.
- Marketing: Responsible for branding, market positioning and attracting customers.

Data

The data collected and processed by CanIphish includes the following types:

- Basic personal details: name, email, contact details.
- User activity: user activity within the software.
- Campaign statistics: employee phish click statistics, training statistics, and computed risk score

Processes, Policies and Procedures

Processes, policies, and procedures are established that set the standards and requirements of the System. All personnel are expected to comply with CanIphish's policies and procedures that define how the System should be managed. The documented policies and procedures are shared with all CanIphish's employees and can be referred to as needed.

Physical Security

The critical infrastructure and data of the System are hosted by AWS. There are no trusted local office networks. As such, AWS is responsible for the key physical security controls that support the System.

Logical Access

CanIphish's logical access processes restrict access to the infrastructure, software, and data to only those that are authorized for access. Access is based on the concept of least privilege that limits the system components and access privileges to the minimum level required to fulfil job responsibilities.

The in-scope systems require approval and individual authentication practices prior to gaining access. Microsoft Entra ID authentication software is used for identity management and multi-factor authentication. Access management processes are followed to ensure new and modified access is approved, terminated users access is removed, and access rights are quarterly reviewed and adjusted when no longer required. Additional information security policies and procedures require CanIphish employees to use the systems and data in an appropriate and authorized manner.

Automated and manual security practices are used to protect the perimeter security and network to prevent unauthorized access attempts and tampering from third-party actors with malicious intent. Those include applying encryption of data and communications, continuous scanning for and remediation of technical vulnerabilities and applying network controls like firewalls and event monitoring to prevent and detect unauthorized activity.

CanIphish employee workstations are required to follow defined security practices to mitigate the risks of data leakage and malware that may compromise the devices, system access and sensitive data. Microsoft Intune mobile device management software is used to monitor, systematically enforce device requirements, and provide remote management capabilities for the workstations.

System Operations

Backup and restoration procedures for the System are defined and followed. The System is monitored through a combination of automated and manual processes to prevent and detect any issues with the infrastructure, software, and data. Alerts and logs are monitored with incident management processes defined for handling and resolving adverse events.

CanIphish's critical infrastructure and data are hosted by AWS with multiple availability zones to provide failover capability in the event of an outage of one of the data centers. Redundancy, disaster recovery in continuity considerations are built into the system design of AWS to support CanIphish's availability objectives. These are supported by the system monitoring, incident management processes and defined recovery and continuity plans.

Change Control

CanIphish operates a defined process for software development with supporting policies and procedures. Change requests and requirements are logged and prioritized for development. Changes include those related to functionality improvements, bug fixes, security and reliability-related enhancements, and other updates to the GitHub software to support CanIphish's System and objectives.

Separate environments are used to support development and testing activities in isolation from the production environment. GitHub version control software is used for the code repository that tracks all changes to the GitHub software, including managing versions and roll-back capability in the event of a failed change release.

Data Governance

CanIphish uses data to support the System objectives and services. An approach to effective data governance has been established to understand and communicate the data that's used in the System, the objectives and requirements of that data, and the commitments of CanIphish.

Established processes, policies, procedures define the operational requirements for data governance, including how data is classified, handled, and used by the System in supporting the objectives and services.

Control Environment

Integrity and Ethical Values

The effectiveness of controls is dependent on the integrity and ethical values of the people who implement, manage, and monitor them. Integrity and ethical values are important foundations of CanIphish's control environment, affecting the design, implementation, and monitoring of the controls. Integrity and ethical behavior are supported by CanIphish's culture, governance, hiring and onboarding practices, ethical and behavioral standards, the way those are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Commitment to Competence

CanIphish's competence of employees includes the knowledge and skills necessary to accomplish employees' roles and responsibilities, in support of CanIphish's objectives and commitments. Management's commitment to competence includes careful consideration of the competence levels required for each role, the requisite skills, knowledge, and experience, and the actual performance of individuals, teams and the company as a whole.

Management's Philosophy and Operating Style

CanIphish's management philosophy and operating style is a purpose-driven, risk-based approach to pursuing the company objectives and satisfying CanIphish's commitments. Risk taking is an essential part of pursuing the objectives. A formal approach is taken to understanding those risks and being deliberate about which risks are acceptable, and where risk mitigation actions are required.

Organizational Structure and Assignment of Authority and Responsibility

CanIphish's organizational structure provides the framework within which its activities for achieving the objectives are planned, executed, managed, and monitored. An organizational structure has been developed to suit CanIphish's needs and is revised over time as the company grows and requirements change.

Roles and responsibilities are further established and communicated through documented policies, and job descriptions, as part of individual performance review processes, reviewing and communicating team and functional performance, and the various operational team and governance meetings.

Human Resource Policies and Practices

CanIPhish's employees are the foundation for achieving the objectives and commitments. CanIPhish's hiring, onboarding and human resource practices are designed to attract, develop, and retain high-quality employees. That includes training and development, performance evaluations, compensation, and promotions, providing personal support and perks for individuals, recognizing team and company success, and building a culture of alignment to a shared purpose and vision. It also includes disciplinary processes and business planning to avoid single-person dependencies to ensure the objectives and commitments are not reliant on individuals.

Risk Assessment Process

CanIPhish's risk assessment process identifies and manages risks that threaten achievement of the objectives and commitments. This includes risks that may affect the security, reliability or integrity of the services provided to user organizations and other interested stakeholders.

A formal process is followed to identify, assess, treat, and monitor the risks to ensure the risks are aligned to the risk appetite and objectives of CanIPhish, and mitigated or avoided where appropriate. Risks identified in this process include:

- Operational risk – changes in the environment, staff, or management personnel, reliance on third parties, and threats to security, reliability, and integrity of CanIPhish's operations.
- Strategic risk – new technologies, changing business models, and shifts within the industry.
- Compliance risk – legal and regulatory obligations and changes.
- Financial risk – the sustainability of CanIPhish and resources supporting the objectives.

These risks are identified by CanIPhish management, employees, and third-party stakeholders, and updated in the risk register as a single source of monitoring the risks. The formal risk assessments ensure the ongoing commitment of management, and support completeness and an evolving view of the risk landscape in CanIPhish's context.

Integration with Risk Assessment

Established internal controls include CanIPhish's policies, procedures, automated system functions and manual activities. The controls are designed and implemented to address the identified risks, and to meet the obligations and criteria set by laws, regulations, customer commitments and other compliance obligations. The controls follow a continual improvement methodology in consideration of the costs and benefits of such control improvements and recognizing the changing landscape and requirement of those controls as CanIPhish grows, and the associated risks change.

Information and Communications Systems

Information and communication are a core part of CanIPhish's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control CanIPhish's operations effectively. The information and communication systems consider the internal control requirements, operating requirements, and the needs of interested parties including employees, customers, third-party vendors, regulators, and shareholders.

The information and communication systems include central tracking systems that support CanIPhish's established processes, as well as various meetings, and documented policies, procedures, and organizational knowledge.

Monitoring Controls

Management monitors the controls to ensure that they are operating as intended and that controls are modified and continually improved over time. Leadership, culture, and communication of the controls are important enablers to the effectiveness of the controls in practice. This ensures buy-in amongst the employees and empowers CanIPhish's team and individuals to prioritize the performance and continual improvement of the controls. Evaluations are performed during the course of business, in management reviews, and by independent auditors to assess the design and operating effectiveness of the controls. Deficiencies that are identified are communicated to responsible control owners to agree remediation actions or re-enforce the control requirements and importance. Corrective actions are tracked with agreed timelines and ownership for remediation with ownership of management and the board, for ensuring appropriate actions are completed in a timely manner.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the examination period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the examination period.

Criteria Not Applicable to the System

All Security, Availability, and Confidentiality Trust Services Criteria were applicable to CanIPhish's Cloud Platform.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS.

CanIphish's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the Agreed Criteria related to CanIphish's services to be solely achieved by CanIphish control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of CanIphish.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Agreed Criteria described within this report are met.

Subservice Organization – AWS		
Category	Criteria	Control
Security	CC6.1- CC6.8	Logical access measures are established and followed to ensure access to systems and data is restricted to authorized personnel with technical safeguards and ongoing assessments to reduce the risk of system and data breaches.
Security	CC6.4	Policies and procedures are established and followed to restrict physical access to data center facilities, backup media, and other system components, including firewalls, routers, and servers.
Security	CC7.1- CC7.5	Incident management and response policies and procedures are established and followed to identify, analyze, classify, respond to and resolve adverse events.
Security	CC8.1	Formal processes are established and followed to ensure system changes are documented, tracked, prioritized, developed, tested and approved prior to deployment into production.
Availability	A1.2	Procedures are established and followed to manage environmental protections within the data centers that house network, virtualization management, and storage devices supporting cloud hosting services where the system resides.

CanIphish management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Agreed Criteria through written contracts and published terms of service. In addition, CanIphish performs monitoring of the subservice organization controls by reviewing attestation reports and monitoring the performance of the subservice organization controls.

Complimentary User Entity Controls

CanIPhish's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Agreed Criteria related to CanIPhish's services to be solely achieved by CanIPhish control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of CanIPhish's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Agreed Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

User entities are responsible for:

- Understanding and complying with CanIPhish's terms of service.
- Notifying CanIPhish of changes made to technical or administrative contact information.
- Administering their users' access rights including approval, removal, and periodic review to ensure access is appropriate.
- Ensuring multi-factor authentication is applied by personnel, if required.
- Performing any required risk assessments and approvals when using pre-built integrations available with CanIPhish's services.
- Performing any required risk assessments and approvals for using CanIPhish's open application programming interface (API), and notifying CanIPhish of any identified vulnerabilities, security breaches or system failures when using the APIs.
- Ensuring the supervision, management, and control of the use of CanIPhish's services by their personnel.
- Developing their own disaster recovery and business continuity plans that address the inability to access or utilize CanIPhish services for any critical reliance on these services.