Redmap Pty Ltd

(Redmap)

SOC 3 Report

For The Period,
July 01, 2025 to December 31, 2025

Independent Practitioner's Trust Services Report for
Redmap - AP Automation and SCP

Prepared by: **Accorp Partners**

Document Ref: Z6C5N-SBK3M-WQGEO-HM7BG

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

SECTION 2

MANAGEMENT ASSERTION

SECTION 3

DESCRIPTION OF SYSTEM

Background and Overview of Services

Principal Service Commitments and System Requirements

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor's Report

To: Management of Redmap Pty Ltd (Redmap)

Scope

We have examined Redmap Pty Ltd's (Redmap's) accompanying assertion titled "Assertion of Redmap Pty Ltd Management" (assertion) that the controls within Redmap's "Redmap - AP Automation and SCP" (system) were effective throughout the period July 01, 2025 to December 31, 2025, to provide reasonable assurance that Redmap's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

Service Organization's Responsibilities

Redmap 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 Redmap's service commitments and system requirements were achieved. Redmap has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Redmap 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 Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the 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.

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

Our examination included the following:

- 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 Redmap'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 Redmap's service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Redmap's system were effective throughout the period July 01, 2025 to December 31, 2025, to provide reasonable assurance that Redmap's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Accorp Partners CPA LLC

Accorp Partners CPA LLC
License No.: PAC-FIRM-LIC-47383
Kalispell, Montana
January 23, 2026

SECTION 2

MANAGEMENT ASSERTION

Assertion of Redmap Pty Ltd (Redmap) Management

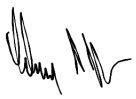
We are responsible for designing, implementing, operating, and maintaining effective controls within Redmap Pty Ltd's (Redmap's) "Redmap - AP Automation and SCP" (system) throughout the period July 01, 2025 to December 31, 2025, to provide reasonable assurance that Redmap's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in Section 3 (Description of System) 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 July 01, 2025 to December 31, 2025, to provide reasonable assurance that Redmap's service commitments and system requirements were achieved based on the applicable trust services criteria. Redmap'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 Section 3 (Description of System).

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 July 01, 2025 to December 31, 2025, to provide reasonable assurance that Redmap's service commitments and system requirements were achieved based on the applicable trust services criteria.

Sincerely,



Johny Andre Ågotnes
Chief Technology Officer

SECTION 3

DESCRIPTION OF SYSTEM

Background and Overview of Services

Background and Description of Services provided

Redmap is as of December 2025 a subsidiary of BASWare. It was founded in 1996 and operates in 4 countries providing Document Automation services, focused on automating the office of the CFO functions.

Many business processes, such as Accounts Payable and Accounts Receivable, rely heavily on the manual keying of data from paper documents. As document automation experts, we have proven methodologies to improve these business processes.

Redmap operates in the mid-tier market with tight integrations across a set of partner ERP providers as well as with a strong focus on the Australian Age Care market due to the recent Support at Home government funding changes, ensuring Age Care operators pay their invoices on time as well as realise all the revenue they are owed.

Significant Changes during the Review Period

No significant changes have occurred to the services provided to user entities during the audit period.

Subservice Organizations

Redmap utilizes the following subservice providers for data center services that are not included within the scope of this examination. However, Redmap's responsibilities for the applications and services run at these cloud services are covered as part of the audit and in scope. The responsibility matrix is defined as part of the SLA and agreements with these sub-service organizations.

Amazon Web Services (AWS)

AWS has provided an Independent Service Auditors Report (SOC2).

The Criteria that relate to controls at the subservice organizations included all criteria related to the Trust Service Principles of Security, Confidentiality, and Availability. The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Redmap include:

- The system is protected against unauthorized access (both physical and logical).
- The system is available for operation and use and in the capacities as committed or agreed.
- Policies and procedures exist related to security and availability and are implemented and followed.

Principal Service Commitments and System Requirements

Redmap designs its processes and procedures related to the System to meet its objectives. Those objectives are based on the service commitments, related laws and regulations of products and services, and financial, operational, and other compliance requirements that have been established for such services. Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online. Redmap establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Redmap's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach as to how the 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 have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

Specific security, commitments include the following:

- Maintain technical and organizational measures, internal controls, and data security routines to protect customer data.
- Protection of data at rest and in transit.
- Protection of information systems from unauthorized access, use, modification, disclosure, destruction, threats, or hazards.
- Continuous communication of the Redmap platform service availability.
- Ability to recover and restore customer data in the event of a business disruption or disaster.
- Maintain customer data as confidential and not disclose information to any unauthorized party.
- Customer data is removed from Redmap systems upon customer request or as per the agreed terms in the contract.

Redmap has also established system requirements that support the achievement of the principal service commitments relevant to the security trust services categories and relevant laws and regulations. These requirements are communicated internally via the information security policies and procedures and regular security awareness training documentation, and externally via the Redmap public-facing website.

These requirements include, but are not limited to, defined processes around the following:

- Employees undergo background checks as per the requirements
- Employees undergo mandatory security awareness training upon hire, and annually thereafter.
- Roles and responsibilities for Redmap employees who have access to confidential data and the responsibility for protecting the information and information systems.
- Access control policies for employees with access to Redmap’s production environment and source code such that access levels are approved prior to credentials being issued, reviewed at predefined intervals, and based on legitimate business need based on the principle of least privilege.
- Software development lifecycle (SDLC) policies for any changes to the production environment to ensure that key processes and security checks are consistently performed from change initiation through release.
- Risk assessment practices to assist in identifying and managing potential internal or external risks that could negatively affect Redmap’s critical business processes and their ability to provide reliable services to their customers.
- Incident management process to address data breaches and security events related to Redmap’s products and services in an efficient and timely manner.
- Disaster recovery and business continuity plans to prepare Redmap in the event of extended service outages caused by factors beyond their control and to restore services to the widest extent possible in a minimal timeframe.

Components of the System

The System is comprised of the following components:

- Infrastructure including the physical structures, Information Technology (IT), and other hardware.
- Software including application programs and IT system software that support application programs.
- People including executives, sales and marketing, client services, product support, information processing, software development, IT, Finance, and Human resources.
- Procedures (automated and manual).
- Data including transaction streams, files, databases, tables, and output used or processed by the system.

The System boundaries include the applications, databases, and infrastructure required to directly support the services provided to Redmap's clients. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to Redmap's customers are not included within the boundaries of its system.

Boundaries of the System

The specific products, services, and locations that are included in the scope of the report are given below. All other products, services, and locations are not included.

Products and Services in Scope	
Products • Redmap AP Automation and SCP	
Geographic Locations in Scope	
Australia	Level 1 130 Cleveland St Chippendale NSW 2008

All the above material activities and operations in scope are performed from the above office location. Unless otherwise mentioned, the description and related controls apply only to the location covered by the report.

Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information, and Communication

Control Environment

Redmap's internal control environment reflects the overall attitude, awareness, and actions of management concerning the importance of controls, and the emphasis given to controls in the Company's policies, procedures, methods, and organizational structure.

The Chief Executive Officer, the Senior Management Team, and all employees are committed to establishing and operating an effective Information Security Management System in accordance with its strategic business objectives. The Management is committed to the Information Security Management System and ensures that IT Security policies are communicated, understood, implemented, and adhered to at all levels of the organization and regularly reviewed for continual suitability.

Integrity and Ethical Values

Redmap requires directors, officers, and employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Honesty and integrity are core principles of the Company, and all employees are expected to fulfill their responsibilities based on these principles and comply with all applicable laws and regulations. Redmap promotes an environment of open communication and has created an environment where employees are protected from any kind of retaliation should a good-faith report of an ethics violation occur. Executive management has the exclusive responsibility to investigate all reported violations and to take corrective action when warranted.

Management’s Philosophy and Operating Style

The Executive Management team assesses risks prior to venturing into business ventures and relationships. The Executive Management team interacts with operating management on a daily basis.

Risk Management and Risk Assessment

Risk assessments are performed annually to identify current risk levels, with recommendations to minimize those risks that are determined to pose an unacceptable level of risk to Redmap. As part of this process,

security threats are identified and the risk from these threats is formally assessed.

Redmap has operationalized a risk assessment process to identify and manage risks that could adversely affect their ability to provide reliable processing for User Organizations. This process consists of the Information Security team identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks.

The following steps are involved in performing risk assessments

- Risk identification for each asset in a process and at the Organizational level.
- Risk analysis & evaluation for each asset in a process & at the Organizational level.
- Risk treatment & residual risk.

Risk assessment comprises calculating the level of risk associated with assets belonging to a particular business process. It is done in a manner to assess and evaluate the criticality of impact on business by a particular risk and also to identify the areas where the organization needs to focus on information security. Apart from the asset-based risk assessment, the Company has also conducted organization-based risk assessment which is based on internal as well as external issues, needs, and expectations of interested parties, etc. The threats, and vulnerabilities associated with every asset are evaluated along with threat impact, probability of occurrence, and chances of detection (on a rating basis) of the threat. This determines the Risk Factor, which is then put into an equation to derive a risk value. The risk value is then compared to the organizational threshold (i.e., accepted risk value) which is treated appropriately (i.e., treat, transfer, avoid, accept). The identified risks will be treated (mitigated) so that risk levels are reduced. The output of a risk assessment will include a complete risk register and risk treatment plan. Any action plans are tracked to completion. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in business conditions. Management and Information Security personnel monitor the quality of internal control performance as a routine part of their activities. Performance monitoring reports cover server parameters such as disc space, incoming/outgoing network traffic, packet loss, CPU utilization, etc. These system performance reports are reviewed by management on a periodic basis. In addition, a self-assessment scan of vulnerabilities is performed prior to every release to the production or on a yearly basis. Vulnerabilities are evaluated and remediation actions are monitored and completed. Results and recommendations for improvement are reported to management.

Information and Communication

Redmap has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated based on suggestions from security personnel and approval by management. Departmental managers monitor adherence to policies and procedures as part of their daily activities. The management holds departmental status meetings, along with strategic planning meetings, to identify and address service issues, customer problems, and project management concerns. The CTO is the focal point for communication regarding the IT environment. Additionally, there are personnel that have been designated to interface with the customer if processing or systems development issues affect customer organizations. Electronic messaging has been incorporated into many of Redmap's processes to provide timely information to employees regarding daily operating activities and to expedite management’s ability to communicate with employees.

Electronic Mail (e-Mail)

Communication to Customer organizations and project teams is through e-mail. Important corporate events, employee news, and cultural updates are some of the messages communicated using e-mail. E-mail is also a means to draw the attention of employees towards adherence to specific procedural requirements. Redmap requires two-factor authentications from employees to access their e-mails.

Components of the System

Infrastructure

The infrastructure comprises physical and hardware components of the System including facilities, equipment, and networks.

Network Segmentation Overview

Redmap's offices are equipped with the latest hardware, software, and networking infrastructure. All the offices are linked through high-speed internet based communication channels.

Software

Firewalls

The production system at AWS is protected by security group rules (virtual firewall) set up for the virtual private cloud (VPC) provided by AWS. VPC is used to protect all Production systems hosted at AWS. Any change to configuration is overseen by the IT Security team. All configurations, backups, and rules have been documented for compliance.

Network & Endpoint Protection

All systems and devices are protected by the comprehensive endpoint protection system. The endpoints include antivirus, anti-malware, and Trojan protection from any source. This also includes the e-mail scanning of the systems which prevents malicious scripts and viruses from the e-mails. Apart from this, all systems are restricted to the internet with the content filtering system routed through the proxy server.

Monitoring

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Redmap’s management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Redmap’s management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management’s close involvement in Redmap’s operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control’s weakness is made based on whether the incident was isolated or requires a change in the company’s procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Redmap’s personnel.

Capacity Management

Capacity management controls are put in place so as to monitor, tune and project certain Redmap’s resources to ensure system performance meets the expected service levels and minimize the risk of systems failure and

capacity-related issues. The addition of new information systems and facilities, upgrades, new versions, and changes are subject to formal system analysis, testing, and approval prior to acceptance.

Patch Management

The respective vertical team ensures that all patches to network device/servers operating systems are tested for stability & availability issues before deploying to the production environment. The patch management activity is done regularly or as and when any critical event occurs and required updates or patches are installed to ensure efficient working of the servers, desktops, and critical network devices. Operating system patches related and marked critical, and security are managed and applied as they become available, windows systems are managed through the patch management system, and the network device's OS patching is managed automatically while renewing.

Vulnerability Scans & Security Audits

As per the Audit calendar, all the network devices and services are audited for vulnerabilities by doing periodic vulnerability scans. These scans are done by the internal IT Infrastructure team.

Virus Scans and Endpoint Security

Redmap ensures antivirus is installed with the feature of scanning the device automatically in all the systems and log reports are reviewed by the IT Head. Updates to the virus definition files are managed and downloaded by the software itself on a daily basis from the vendor website at specific intervals.

People

Organizational Structure

The organizational structure provides the overall framework for planning, directing, and controlling operations. It has segregated personnel and business functions into functional groups according to their job responsibilities. This approach helps to enable the organization to define responsibilities, lines of reporting, and communication and helps facilitate employees to focus on the specific business issues impacting clients.

The management team meets regularly to review business unit plans and performances. Meetings with the CEO and department heads are held to review operational, security, and business issues, and plans for the future.

Redmap's Information Security policies define and assign responsibility/accountabilities for information security. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

The following are the responsibilities of key roles.

- **Executive management** - Responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- **Human resources (HR)** - Responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- **IT and DevOps** - Responsible for installation, configuration, operation, monitoring, and maintenance of IT and DevOps.
- **IT Security** – Responsible for Information Security including implementing, managing, and monitoring the information security program along with IT Risk Management.
- **Development** - Responsible for the development, testing, deployment, and maintenance of code for internally developed applications.

Processes and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Redmap policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Redmap team member.

Administrative Level Access

Administrative rights and access to administrative accounts are granted to individuals that require that level of access in order to perform their jobs. All administrative level access, other than to IT team, must be justified to and approved by IT team.

Confidentiality

Secure procedures are established to ensure safe and secure disposal of media when no longer required. The level of destruction or disposal of media would depend on the information or data stored in the media and the criticality of the information as per the information classification guideline.

Backup and Recovery of Data

Redmap has developed formal policies and procedures relating to backup and recovery. Backup is defined in the Backup Policy. Suitable backups are taken and maintained. The backup processes are approved by the business owners and comply with the requirements for business continuity, and legal & regulatory requirements. All backup and restoration logs are maintained for retention periods as defined in the "Backup Policy".

Applicable Trust Services Criteria and related Controls

The Security trust services categories have been identified by Redmap as applicable to its system.

Complementary User-Entity Control Considerations

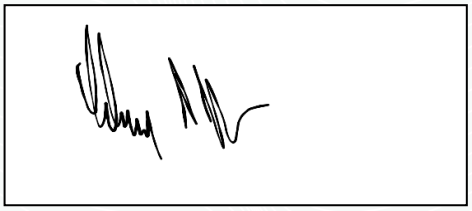
The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities'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

1. User entities are responsible for understanding and complying with their contractual obligations to Redmap.
2. User entities are responsible for notifying Redmap of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Redmap services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Redmap services.
6. User entities are responsible for providing Redmap with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Redmap of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

CERTIFICATE *of* SIGNATURE

REF. NUMBER
Z6C5N-SBK3M-WQGEO-HM7BG

DOCUMENT COMPLETED BY ALL PARTIES ON
23 JAN 2026 21:17:03
UTC

SIGNER	TIMESTAMP	SIGNATURE
JOHNY AGOTNES EMAIL JAGOTNES@REDMAP.COM	SENT 23 JAN 2026 09:59:52 VIEWED 23 JAN 2026 10:23:51 SIGNED 23 JAN 2026 21:17:03	 IP ADDRESS 104.28.35.18 LOCATION BRISBANE, AUSTRALIA

RECIPIENT VERIFICATION

EMAIL VERIFIED
23 JAN 2026 10:23:51