



SMB SOLUTIONS CLOUD SERVICES PTY LTD

SOC 3 REPORT

FOR

**SMB Solutions Cloud Services – A
SAP Business One Cloud Hosting Provider**

**INDEPENDENT SERVICE AUDITOR'S REPORT ON
CONTROLS RELEVANT TO SECURITY, CONFIDENTIALITY & AVAILABILITY**

August 30, 2024 – August 29, 2025

Attestation and Compliance Services

CertPro

TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2	MANAGEMENT'S ASSERTION	4
SECTION 3	DESCRIPTION OF THE SYSTEM	6

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Board of Directors

SMB Solutions Cloud Services Pty Ltd

Scope

We have examined the accompanying "Description of SMB Solutions Cloud Services, a SAP Business One Cloud Hosting Provider" provided by SMB Solutions Cloud Services Pty Ltd throughout the period August 30, 2024 to August 29, 2025 and the suitability of the design and operating effectiveness of controls to meet SMB Solutions Cloud Services Pty Ltd's service commitments and system requirements based on the criteria for Security, Confidentiality, Availability, Processing Integrity & Privacy principles set forth in TSP Section 100 Principles and Criteria, Trust Services Principles and Criteria for Security, Confidentiality and Availability (applicable trust services criteria) throughout the period August 30, 2024 to August 29, 2025.

The description of boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SMB Solutions Cloud Services Pty Ltd, to achieve SMB Solutions Cloud Services Pty Ltd's service commitments and system requirements based on the applicable trust service criteria. 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

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

Our examination included:

- a. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- b. Assessing the risks that controls were not effective to achieve SMB Solutions Cloud Services Pty Ltd's service commitments and system requirements based on the applicable trust services criteria.
- c. Performing procedures to obtain evidence about whether controls within the system were effective to achieve SMB Solutions Cloud Services Pty Ltd'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 SMB Solutions Cloud Services Pty Ltd'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 SMB Solutions Cloud Services Pty Ltd were effective throughout the period August 30, 2024 to August 29, 2025, to provide reasonable assurance that SMB Solutions Cloud Services Pty Ltd's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Certified Public Accountants
License Number: CF-0010928
October 21, 2025

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

SMB Solutions Cloud Services Pty Ltd's Management Assertion for the period August 30, 2024 to August 29, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within "SMB Solutions Cloud Services, a SAP Business One Cloud Hosting Provider" throughout the period August 30, 2024 to August 29, 2025 to provide reasonable assurance that SMB Solutions Cloud Services Pty Ltd's service commitments and system requirements relevant to Security, Confidentiality, and Availability were achieved. Our description of the boundaries of the system is presented below 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 August 30, 2024 to August 29, 2025, to provide reasonable assurance that SMB Solutions Cloud Services Pty Ltd'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, Trust Services Criteria for Security, Confidentiality, Availability, Processing Integrity, and Privacy (AICPA, Trust Services Criteria). SMB Solutions Cloud Services Pty Ltd's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 August 30, 2024 to August 29, 2025, to provide reasonable assurance that SMB Solutions Cloud Services Pty Ltd's service commitments and systems requirements were achieved based on the applicable trust services criteria.

For SMB Solutions Cloud Services Pty Ltd

Authorized Signatory

SECTION 3

DESCRIPTION OF THE SYSTEM

Types of Services Provided

Types of Services Provided

SMB Solutions Cloud Services enable small and mid-sized businesses across the world to leverage the power of Cloud Platforms to effectively utilise their SAP Business One solution delivered through SAP business partners.

With this structured approach, automated solutions and people, together with our partners, SMB Solutions Cloud Services provide secure and reliable SAP Business One cloud hosting services.

SMB Solutions Cloud Services designs its processes and procedures to meet objectives for its digital transformation and IT/Business Process outsourcing services. Those objectives are based on the service commitments that SMB Solutions Cloud Services makes to customers and the compliance requirements that SMB Solutions Cloud Services has established for its services.

Security commitments to user entities are documented and communicated in SMB Solutions Cloud Services' customer agreements, as well as in the description of the service offering provided online. SMB Solutions Cloud Services' security commitments are standardised and based on some common principles.

These principles include but are not limited to, the following:

- The fundamental design of SMB Solutions Cloud Services' digital transformation and IT/Business Process outsourcing services address security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
- SMB Solutions Cloud Services implements various procedures and processes to control access to the production environment and the supporting infrastructure.
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilisation metrics.

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 and non-disclosure agreements with employees, contractors, and third parties.
- Confidential information must be used only for the purposes explicitly stated in agreements between SMB Solutions Cloud Services Pty Ltd and user entities.

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.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans are tested on a periodic basis.
- Operational procedures supporting the achievement of availability commitments to user entities.

SMB Solutions Cloud Services establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in SMB Solutions Cloud Services' system policies and procedures, system design documentation, and contracts with customers.

Components of the System used to Provide Services

Infrastructure & Network Architecture

SMB Solutions Cloud Services maintains its infrastructure in a secure colocation data centre. This data centre is designed to provide optimal physical security, environmental controls, and redundant power and connectivity. It adheres to industry best practices for data centre operations, ensuring the availability and reliability of services.

SMB Solutions Cloud Services network infrastructure comprises robust routers, switches, firewalls, and other networking equipment. SMB Solutions Cloud Services have implemented network segmentation to isolate client environments and protect data confidentiality and integrity.

SMB Solutions Cloud Services use a combination of physical and virtual servers to host client applications, databases, and storage systems. SMB Solutions Cloud Services servers are regularly patched and hardened to mitigate security risks.

SMB Solutions Cloud Services have implemented a comprehensive set of security controls to protect their infrastructure. This includes firewalls, intrusion detection and prevention systems and security information. SMB Solutions Cloud Services regularly monitor and analyse network traffic and system logs to detect and respond to potential security incidents promptly.

SMB Solutions Cloud Services has implemented data protection mechanisms, including data encryption, access controls, and regular data backups. These measures ensure the confidentiality, integrity, and availability of their clients' data. Backups are stored in geographically separate locations to protect against data loss due to unforeseen events.

SMB Solutions Cloud Services have established comprehensive business continuity and disaster recovery plans to mitigate the impact of potential disruptions. These plans include regular testing and validation to ensure their effectiveness in quickly restoring services in the event of an incident.

Software

SMB Solutions Cloud Services is responsible for managing the development and operation of the SMB Solutions Cloud Services platform including infrastructure components such as servers, databases, and storage systems. SMB Solutions Cloud Services leverages various Microsoft 365 tools, including Outlook, MS Teams, SharePoint, and OneDrive, as well as 3CX, Autotask for client communication. These tools are deployed across a combination of cloud-based services and SMB Solutions Cloud Services' secure colocation data center, which they manage and maintain.

SMB Solutions Cloud Services does not produce software.

People

SMB Solutions Cloud Services staff have been organised into various functions like Sales, Support, Engineering, Product Management, etc. The personnel have also been assigned to the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organisation. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organisation's mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required to run an effective risk management program that assesses and mitigates IT-related mission risks.

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organisation. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls to mitigate these risks. Additionally, they also summarise remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager: The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organisation.

System Users: The organisation's staff members are the users of the IT systems. The organisation understands that use of the IT systems and data according to an organisation's policies, guidelines, and rules of behaviour is critical to mitigating risk and protecting the organisation's IT resources. To minimise risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

Procedures and Policies

Formal policies and procedures have been established to support SMB Solutions Cloud Services. These policies cover:

- Code of Business Conduct
- Change Management
- Data Retention
- Data Backup
- Information Security
- Vendor Management
- Physical Security
- Risk Management
- Password
- Media Disposal
- Incident Management
- Endpoint Security
- Encryption
- Disaster Recovery
- Confidentiality
- Business Continuity
- Access Control
- Acceptable Usage
- Vulnerability Management
- HR Security

All policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

SMB Solutions Cloud Services also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the SMB Solutions Cloud Services, in the event there are problems, and takes actions within an appropriate timeframe as and when issues

are raised.

Data

Data, as defined by SMB Solutions Cloud Services, constitutes the following:

- Transaction Data
- Electronic Interface Files
- Output Reports
- Input Reports
- System Files
- Error Logs

All data that is managed, processed and stored as a part of the SMB Solutions Cloud Services' service is classified as per the Data Classification Policy which establishes a framework for categorising data based on its sensitivity, value, and criticality to achieving the objectives of the organisation.

Further, all customer data is treated as confidential. The availability of this data is also limited by job function. All customer data storage and transmission follow industry-standard encryption. The data is also regularly backed up as documented in the Data Backup Policy.

Physical Security

The in-scope system and supporting infrastructure are hosted by a third-party hosting provider. As such, they are responsible for the physical security controls of the in-scope system. SMB Solutions Cloud Services reviews the SOC 2 report provided by its provider on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the SMB Solutions Cloud Services' service.

Logical Access

The SMB Solutions Cloud Services' service uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the service and authenticates to the database.

SMB Solutions Cloud Services has identified certain systems that are critical to meet its service commitments. All-access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role-based access matrix prior to being issued system credentials and granted the ability to access the system.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assessing the appropriateness of the access and permission levels and making modifications based on the principle of least privilege, whenever necessary.

Change Management

A documented Change Management Policy guides all staff members in documenting and implementing service and infrastructure changes. It outlines how changes to the SMB Solutions Cloud Services system are reviewed, deployed, and managed. The policy covers all changes made to the SMB Solutions Cloud Services' service, regardless of their size, scope, or potential impact.

The Change Management Policy is designed to mitigate the risks of:

- Corrupted or destroyed information.
- Degraded or disrupted software application performance.
- Productivity loss.
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

A change to the SMB Solutions Cloud Services' service can be initiated by a staff member with an appropriate role.

The ability to implement changes in the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities. Further audit logs are configured to track all changes to the production infrastructure.

Incident Management

SMB Solutions Cloud Services 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. Customers are directed to contact SMB Solutions Cloud Services via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralised tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analysed for anomalous or suspicious activity.

Availability

SMB Solutions Cloud Services has a documented Business Continuity Plan (BCP) and testing performed against the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

Boundaries of the System

The scope of this report includes the SMB Solutions Cloud Services' service. It also includes the people, processes, and IT systems that are required to achieve our service commitments toward the customers of this service.

SMB Solutions Cloud Services depends on a number of vendors to achieve its objectives. The scope of this report does not include the processes and controls performed by the vendors. The management understands that risks exist when engaging with vendors and has formulated a process for managing such risks, as detailed in the Risk Assessment section of this document.