# 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

27th June 2023 – 28th September 2023

Attestation and Compliance Services

CertPro
Effective. Efficient. Economical.

# Table of Contents

# 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 " throughout the period 27 June 2023 to 28 September 2023 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 27 June 2023 to 28 September 2023.

SMB Solutions Cloud Services Pty Ltd uses Microsoft Corporation (Office 365), a subservice organization, to provide office communication, file sharing, collaboration services and Microsoft Office applications like Word, Excel, and PowerPoint etc. 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, and

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 27 June 2023 to 28 September 2023, 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.


**JAY MARU**
Certified Public Accountant
License Number: 41401
5 February, 2024

# Section 2

## Management's Assertion

# MANAGEMENT'S ASSERTION

**SMB Solutions Cloud Services Pty Ltd's Management Assertion for the period 27 June 2023 to 28 September 2023**

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 27 June 2023 to 28 September 2023 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 27 June 2023 to 28 September 2023, 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 27 June 2023 to 28 September 2023, 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**

Richard Duffy 29 January 2024 | 8:54 AM PST Richard Duffy

SMB Solutions Cloud Services Pty Ltd

**Authorized Signatory** CEO

# Section 3

## Description of the Boundaries of the System

# DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM

**Types of Services Provided**

This document provides an overview of the services offered by SMB Solutions Cloud Services Pty Ltd (hereby referred to as SMB Solutions Cloud Services.

SMB Solutions Cloud Services enables small and mid-sized businesses across the world to leverage the power of Cloud Platforms to effectively utilize their SAP Business One solution delivered through SAP Business Partners by providing the required cloud hosting infrastructure and services.

With this structured approach, automated solutions, and people, together with our partners, we provide the Gold Standard in SAP Business One Cloud Hosting.

Our Vision is:

To be considered a trusted strategic partner and the best operational provider of SAP Business One Cloud Services for the business markets we serve through,

- Responsive and responsible delivery of services
- Delivery of services that promote SAP Business One customer business safety and security,
- Provision of operations with integrity and flexibility.
- Utilization of current technologies to deliver client growth focused solutions.
- Focus on SAP certified platforms and products to deliver the services.

Any other services provided by SMB Solutions Cloud Services are not in the scope of this report.

**Principal Service Commitments and System Requirements**

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 standardized and based on some common principles. These principles include but are not limited to, the following:

1. 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.
2. SMB Solutions Cloud Services implements various procedures and processes to control access to the production environment and the supporting infrastructure.
3. Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.

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.

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 networks are managed, and how the staff is hired.

**Infrastructure**

SMB Solutions Cloud Services maintains its infrastructure in a secure colocation data center. This data center is designed to provide optimal physical security, environmental controls, and redundant power and connectivity. It adheres to industry best practices for data center operations, ensuring the availability and reliability of our 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 network is designed to deliver high-speed connectivity, redundancy, and scalable bandwidth to support their clients' diverse needs.

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 employ industry leading storage technologies to ensure data availability, redundancy, and durability.

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 analyze 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 leverages various Microsoft 365 tools, including Outlook, MS Teams, SharePoint, and OneDrive, as well as 3CX, ONE Portal, and OsTicket 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 uses a subservice provider, Sprinto, to provide continuous compliance monitoring of the company's system.

**People**

SMB Solutions Cloud Services has a staff of approximately 5 personnel, organized into various functions. The personnel have also been assigned the following key roles:

**Senior Management:** Senior management carries the ultimate responsibility for achieving the mission and

objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization'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 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 organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, vulnerabilities, and adding controls to mitigate this risk.

**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 effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

**System Users:** The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize 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 management
- Media disposal
- Incident management
- Endpoint security
- Encryption
- Disaster recovery
- Data classification
- Confidentiality
- Business continuity
- Access control
- Acceptable usage
- Vulnerability management
- HR Security Policy

Via the Sprinto platform, 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, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

**Data**

All data that is managed, processed, and stored as a part of the SMB Solutions Cloud Services digital transformation and IT/Business Process outsourcing services is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value, and criticality to achieving the objectives of the organization.

Further, all customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. The access to the customers' critical data is only for a limited time, during their onboarding phase which is revoked after onboarding is successfully completed.

**Physical Security**

SMB Solutions Cloud Services only host and maintain infrastructure physically located in their data center.

**Logical Access**

SMB Solutions Cloud Services use role-based security architecture and require users of the system to be identified and authenticated prior to the use of any system resources. User access to the client's accounts, which is role-based, is controlled manually. Access to the client's accounts is revoked at the end of the engagement with SMB Solutions Cloud Services.

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.

The Information Security Officer is responsible for performing periodic 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 changes. It outlines how changes are reviewed, deployed, and managed. The policy covers all changes made, 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.

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.

**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 centralized 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 analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating.

- **Low severity incidents** are those that do not require immediate remediation. These typically include a partial service of SMB Solutions Cloud Services being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.
- **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium-severity incidents usually cover the large majority of incidents found.
- **High severity incidents** are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, and malicious access to business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed, and immediate remediation steps should begin.
- **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

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

**Cryptography**

When users send requests to SMB Solutions Cloud Services' systems, these requests are encrypted using Transport Layer Security (TLS). TLS ensures that the communication between the user's device and SMB Solutions Cloud Services' systems is secure. Remote system administration access to SMB Solutions Cloud Services web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using Advanced Encryption Standard (AES) 256-bit.

**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. SMB Solutions Cloud Services uses tagging tools to automatically

facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technological assets with the potential to store or process information is maintained.

**Vulnerability Management and Penetration Testing**

Vulnerability scanning tools are used to automatically scan systems on the network at least monthly to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities.

**Endpoint Management**

Endpoint management solutions are in place that includes policy enforcement on company issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include but are not limited to enabling screen lock, OS updates, and encryption at rest on critical devices/workstations.

**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**

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.

.

**Management Philosophy and Operating Style**

SMB Solutions Cloud Services' management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to monitoring business risks, and management's attitudes toward personnel and the processing of information.

Specific control activities that the service organization has implemented in this area are described below:

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment, and high severity security incidents annually.

**Risk Assessment**

SMB Solutions Cloud Services' risk assessment process identifies and manages risks that could potentially affect its ability to provide reliable services to its customers. All staff, but in particular the CEO, are expected to identify significant risks inherent in products and services as they oversee their areas of responsibility. SMB Solutions Cloud Services identifies the underlying sources of risk, measures the impact to organization,

establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the SMB Solutions Cloud Services, and the management has implemented various measures designed to manage these risks.

**Scope**

The Risk Assessment and Management program applies to all services and data that are a part of the SMB Solutions Cloud Services. The SMB Solutions Cloud Services risk assessment exercise evaluates its services to its clients. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high-level or detailed to a specific organizational or technical change as the stakeholders and managers see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of SMB Solutions Cloud Services' Information Security Officer and the department or individuals responsible for the area being assessed. All SMB Solutions Cloud Services staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

**Vendor Risk Assessment**

SMB Solutions Cloud Services uses a number of vendors to meet its business objectives. SMB Solutions Cloud Services understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

SMB Solutions Cloud Services employs several activities to effectively manage its vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, SMB Solutions Cloud Services assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support SMB Solutions Cloud Services' commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, SMB Solutions Cloud Services management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

**Integration with Risk Assessment**

As part of the design and operation of the system, SMB Solutions Cloud Services identifies the specific risks that service commitments may not be met, and designs controls necessary to address those risks. SMB Solutions Cloud Services' management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity, and mitigating action.

**Monitoring**

SMB Solutions Cloud Services management monitors controls to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken 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. Staff activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

**Information and Communication Systems**

SMB Solutions Cloud Services maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, SMB Solutions Cloud Services also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff via the company intranet.

**Significant Events and Conditions**

SMB Solutions Cloud Services has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with all relevant information for any impact on the services.

**Trust Services Categories**

The following Trust Service Categories are in scope. **Common Criteria (to the Security, Confidentiality and Availability Categories)**.

1. **Security** refers to the protection of:
    a. Information during its collection or creation, use, processing, transmission, and storage and
    b. Systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removals of information or system resources, misuse of the software, and improper access to or use of, alteration, destruction, or disclosure of information.

2. **Confidentiality** addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

3. **Availability** refers to the accessibility of information used by the entity’s systems, as well as the products or services provided to its customers. The availability objective does not set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs)

or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

**Complementary Customer Controls**

SMB Solutions Cloud Services' controls related to SMB Solutions Cloud Services cover a subset of overall internal control for each user of their service. The control objectives related to SMB Solutions Cloud Services cannot be achieved solely by the controls put in place by SMB Solutions Cloud Services; each customer's internal controls need to be considered along with SMB Solutions Cloud Services' controls. Each customer must evaluate its own internal control to determine whether the identified complementary customer controls have been implemented and are operating effectively.

| Complementary Customer Control List | Related Criteria |
|---|---|
| Customers are responsible for managing their organization's account, where SMB Solutions Cloud Services is given access to, as well as establishing any customized security solutions or automated processes through the use of setup features | CC5.1, CC5.2, CC5.3, CC6.1 |
| Customers are responsible for communicating relevant security and availability issues and incidents to SMB Solutions Cloud Services through identified channels during their engagement. | CC7.2, CC7.3, CC7.4 |