Security Architecture Narrative

MMF Consulting Grp (Pte. Ltd.)

June 2018

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC3.2, CC6.1, CC6.3, CC6.4, CC6.7, CC6.8

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document
Jun 24 2025	Enhanced narrative and updated TSC controls

1 Security Architecture Narrative

This document outlines the security architecture of MMF Consulting Grp (Pte. Ltd.), demonstrating how our organizational structure, control environment, and service delivery processes work together to protect client data and ensure the integrity of our audit services. As a Taiwan-based consulting firm specializing in contract compliance auditing, our security architecture is designed to support our unique operational needs and risk profile.

2 Service Architecture

MMF Consulting Grp (Pte. Ltd.)'s service architecture is built around a secure workflow for delivering our core services, including Royalty Audits, Channel Inspections, and Supplier Reviews. This process is supported by a robust set of logical, policy, and procedural controls rather than a traditional software product stack.

The key stages of MMF Consulting Grp (Pte. Ltd.)'s service delivery are:

1. **Data Ingestion:** The journey of client data begins with secure reception through official encrypted channels, creating a protected pathway for sensitive information to enter our environment. Once received, this data finds a home in Box, our designated secure collaboration platform, where it remains protected by enterprise-grade security controls.
2. **Data Analysis:** The data's journey continues as authorized auditors—and only those specifically assigned to the engagement—access and analyze it using secured tools within the Microsoft 365 ecosystem (e.g., Excel, Power BI) on company-managed workstations. Throughout this analytical phase, the data remains within our protected environment.
3. **Reporting:** As insights emerge, they're transformed into comprehensive reports that encapsulate our findings while maintaining security. These reports complete their journey when they're securely transmitted back to the client through official encrypted channels, maintaining protection from origin to destination.

Security is deeply integrated into this workflow through multiple layers of controls:

- **Logical Controls**: We employ a layered defense approach to protect our information assets. At the core of this strategy is mandatory data encryption, using industry-standard AES-256 for all data at rest and TLS 1.2+ for data in transit. This encryption shield surrounds all client and company information, ensuring that even if other security measures are compromised, the data remains protected. Surrounding this encrypted core is a comprehensive access management system built on strict Role-Based Access Control (RBAC) and reinforced by Multi-Factor Authentication (MFA), creating multiple barriers that potential attackers must overcome. These logical protections extend to all company workstations, which form the outer perimeter of our security architecture. Each workstation acts as a security outpost, hardened with full-disk encryption, enterprise-grade anti-malware, and continuously monitored patching to seal potential security gaps as they emerge.
- **Policy & Procedural Controls**: Our operations are governed by comprehensive policies, including the Access Control Policy, Data Retention and Disposal Policy, and Encryption Policy. Regular procedures such as quarterly access reviews and weekly security log analysis ensure these policies are effectively implemented and monitored.

3 Service Infrastructure

MMF Consulting Grp (Pte. Ltd.)'s service delivery infrastructure is entirely cloud-based, relying on industry-leading SaaS providers. This approach eliminates the need for on-premises servers and the associated physical security and maintenance overhead.

3.1 Core Infrastructure and Access Control

Our core infrastructure for both internal operations and service delivery relies on two primary cloud platforms:

- **Microsoft 365 (M365):** This suite is used for all internal and external communication (Outlook), data analysis (Excel, Power BI), and real-time collaboration (Microsoft Teams).
- **Box:** This platform serves as our central, secure repository for all client data and internal documentation.

Access to these platforms is granted based on the principle of least privilege and is strictly controlled through our formal onboarding/offboarding procedures. Permissions are managed by IT and reviewed quarterly to ensure alignment with employee job functions. Access to specific client data within Box is further restricted to only the audit team members assigned to that engagement.

4 Workstations

MMF Consulting Grp (Pte. Ltd.)'s workstations represent the primary interface between our team members and client data. As such, they form a critical component of our overall security architecture. We've developed a comprehensive approach to workstation security that creates a trusted, resilient environment for sensitive work.

Each workstation in our ecosystem is fortified against both logical and physical threats through multiple security layers:

- Operating systems are kept within one generation of current releases, balancing security updates with stability needs
- Full-disk encryption serves as an ever-present guardian, protecting data even if devices are lost or stolen
- Enterprise-grade antivirus and antimalware solutions actively monitor for and defend against malicious software threats
- Automatic updates for both operating systems and security software ensure protection against newly discovered vulnerabilities

This isn't a set-and-forget approach—our security team evaluates workstation compliance with these measures quarterly, ensuring that our protective measures remain effective in an evolving threat landscape.

4.1 Remote Access

MMF Consulting Grp (Pte. Ltd.) does not operate an on-premises corporate network. All employees, whether remote or in-office, access production and systems for work directly through encrypted connections to our cloud service providers. It is the employee's responsibility to ensure that only authorized personnel use MMF Consulting Grp (Pte. Ltd.) resources and access MMF Consulting Grp (Pte. Ltd.) systems.

5 Access Review

Access to MMF Consulting Grp (Pte. Ltd.) infrastructure, both internal and product, is reviewed quarterly and inactive users are removed. Any anomalies are reported to the security team for further investigation. When employees start or depart, an onboarding/offboarding procedure is followed to provision or deprovision appropriate account access.

6 Physical Security

MMF Consulting Grp (Pte. Ltd.)'s security architecture extends beyond the digital realm to encompass our physical workspace. Our headquarters in Singapore and offices located Taipei and Hsinchu are designed with a security-first approach that complements our digital protections. Physical access to our facilities follows a controlled distribution model where only employees receive access keys, creating a clear boundary between authorized and unauthorized personnel.

The journey of these physical access credentials is carefully managed throughout the employee lifecycle. Human Resources oversees the issuance and retrieval of keys, maintaining a living record of who can access our physical spaces. When team members depart, their physical access credentials are immediately revoked as part of our comprehensive offboarding process, ensuring former employees cannot re-enter secure areas. This physical access ecosystem isn't static—management conducts regular reviews of physical access privileges, ensuring that access rights continue to align with current responsibilities and security needs.

7 Risk Assessment

Understanding the threats that could impact our ability to protect client data is fundamental to MMF Consulting Grp (Pte. Ltd.)'s security architecture. Rather than approaching security reactively, we maintain a living understanding of our threat landscape through a comprehensive Cyber Risk Assessment process. This assessment is refreshed annually, ensuring our security posture evolves alongside emerging threats and changing business objectives.

Our risk assessment methodology follows a structured narrative that helps translate abstract threats into concrete security controls:

1. **Threat Identification:** We systematically catalog potential threats from both adversarial and non-adversarial sources
2. **Impact Analysis:** Each identified threat is evaluated for its potential impact on client data confidentiality, integrity, and availability
3. **Likelihood Determination:** We assess the probability of each threat materializing based on industry intelligence and our specific environment
4. **Risk Prioritization:** Threats are prioritized based on their combined likelihood and potential severity
5. **Control Mapping:** Specific security controls are mapped to mitigate each prioritized risk

This cyclical process ensures that our security architecture remains responsive to the evolving risk landscape while maintaining focus on our highest-priority objectives: protecting client data and maintaining service integrity.

7.1 Adversarial Threats

Our analysis has identified the following key adversarial threats that inform our security architecture:

Threat	Source	Vector	Target	Likelihood	Severity
Phishing / Social Engineering	External Attacker	Email, Instant Messaging	Employee Credentials, Client Data	Medium	High
Malware / Ransomware	External Attacker	Email Attachment, Malicious Link	Workstations, Client Data	Low	High

Threat	Source	Vector	Target	Likelihood	Severity
Unauthorized Data Access	External/Internal	Compromised Credentials, Insider Abuse	Client Data in Box/M365	Low	High
Insider Threat (Malicious)	Internal Employee	Direct Access	Client Data, Intellectual Property	Low	High

7.2 Non-Adversarial Threats

While malicious actors represent a significant concern, our risk assessment also accounts for accidental or environmental threats that could impact our security objectives:

Threat	Vector	Target	Likelihood	Severity
Human Error	Accidental Deletion, Misconfiguration	Client Data, System Availability	Medium	Medium
Service Provider Outage	M365/Box Failure	Service Availability, Productivity	Low	Medium
Data Corruption	Software/Hardware Failure	Client Data Integrity	Low	Medium

This balanced view of both intentional and unintentional threats allows us to develop a holistic security architecture that addresses the full spectrum of risks to our data and services.

8 References

The following documents complement this Security Architecture Narrative, providing additional context and detailed guidance for implementing the security controls described herein.

8.1 Narratives

- **Organizational Narrative** - Describes our company structure, management approach, and ethical foundations that form the basis for our security architecture
- **Control Environment Narrative** - Outlines the broader control environment that enables effective implementation of our security controls

8.2 Policies

- **Encryption Policy** - Defines standards and requirements for encrypting sensitive information
- **Log Management Policy** - Establishes practices for generating, collecting, and analyzing security logs
- **Office Security Policy** - Details physical security requirements referenced in this narrative
- **Remote Access Policy** - Specifies requirements for secure remote connections to company resources

- **Security Incident Response Policy** - Defines procedures for identifying, reporting, and responding to security events
- **Workstation Policy** - Establishes minimum security standards for company workstations

8.3 Procedures

- TODO: Add relevant procedures

9 Authorship and Approval

Last edit made by Bill Li (yushengli.tw@gmail.com) on Mon, 18 Aug 2025 18:37:06 +0800.

Approved by Yusheng Li (YushengLi@users.noreply.github.com) on Thu, 21 Aug 2025 11:54:21 +0800 in commit 8e0c1296a6a80185ef11d1631bbf6ca59ccc896b.