Control Environment Narrative

MMF Consulting Grp (Pte. Ltd.)

June 2018

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC1.4, CC2.2, CC2.3, CC4.1, CC4.2, CC5.2, CC6.1, CC6.3, CC6.7, CC6.8, CC7.1, CC7.2, CC9.2

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Control Environment Narrative

The following provides a description of the control structure of MMF Consulting Grp (Pte. Ltd.).

The intent of this description is to enumerate the logical, policy, and procedural controls that serve to monitor MMF Consulting Grp (Pte. Ltd.)'s application and data security. Changes uncovered by these procedures in the logical, policy, procedural, or customer environment are addressed by remediations specific to the noted change.

2 Logical Controls

MMF Consulting Grp (Pte. Ltd.) employs several logical controls to protect confidential data and ensure normal operation of its core product.

- **Data Encryption**: Mandatory data encryption for data at rest (AES-256) and in transit (TLS 1.2+).
- **Access Control**: Strict access control measures are enforced, including:
  - Multi-factor authentication (MFA) for all corporate systems
  - Role-based access control (RBAC) based on predefined job functions and responsibilities
  - Access rights provisioned based on the principle of least privilege
  - Regular reconciliation of user roles against current job responsibilities during quarterly reviews
  - Formal approval process for role changes and privilege escalations
  - Automatic account lockout after consecutive failed login attempts
- **Endpoint Security**: All company-issued workstations are hardened and monitored through a unified endpoint security program. This includes:
  - Mandatory monthly security patching, with critical vulnerabilities patched within 7 days.
  - Enterprise-grade anti-malware solutions with continuous monitoring. Critical alerts are remediated within 7 days, and medium-severity alerts within 30 days.
  - Full disk encryption is enabled on all devices.
  - Automatic screen lock after 5 minutes of inactivity.
- **Audit Logging and Monitoring**: Systems are configured to log access and event activity across company resources. Logs are maintained and routinely reviewed to detect and respond to anomalous or suspicious behavior, in alignment with CIS Control 8.

3 Policy Controls

MMF Consulting Grp (Pte. Ltd.) employs several policy controls to protect confidential data and ensure normal operation of its core product. These policies include, but are not limited to:

- Access Control Policy
- Data Retention and Disposal Policy
- Encryption Policy
- Information Security Policy
- Office Security Policy
- Password Policy
- Third-Party Security Policy
- Workstation Policy

4 Procedural Controls

MMF Consulting Grp (Pte. Ltd.) has numerous scheduled procedures to monitor and tune the effectiveness of ongoing security controls, and a series of event-driven procedures to respond to security-related events.

4.1 Scheduled Security and Audit Procedures

- Review Access [quarterly]
- Review Security Logs [weekly]
- Review Devices & Workstations [quarterly]
- Review & Clear Low-Priority Alerts [monthly]
- Apply OS Patches [monthly]
- Verify Data Disposal per Retention Policy [quarterly]
- Conduct Security Training [annual]
- Review Security Monitoring and Alerting Configuration [quarterly]
- Remediate Anti-Malware Alerts [within 7 days for critical, 30 days for medium]

4.2 Event-Driven Security and Audit Procedures

- Onboard Employee: Includes identity, employment, and criminal background checks prior to onboarding.
- Offboard Employee
- Security Alert Investigate
- Security Incident Investigate

5 Remediations

MMF Consulting Grp (Pte. Ltd.) uses the outcomes of the aforementioned controls and procedures to identify shortcomings in the existing control environment. The remediation process follows these steps:

1. **Deficiency Classification**: Control deficiencies are classified as High, Medium, or Low severity based on potential impact to security, operations, and compliance.
2. **Assignment and Accountability**: Each identified deficiency is assigned to a responsible party with appropriate expertise and authority to implement corrective actions.
3. **Timeframes**: Remediation timeframes are based on severity:
    - High: remediated within 30 days
    - Medium: remediated within 60 days
    - Low: remediated within 90 days
4. **Tracking**: All remediation activities are tracked in a central register, with status updates provided to management on a monthly basis.

Once identified, these shortcomings are remediated by improving existing controls and procedures, and creating new controls and procedures as needed.

6 Communications

MMF Consulting Grp (Pte. Ltd.) maintains formal communication channels for sharing control-related information with both internal and external stakeholders.

6.1 Internal

MMF Consulting Grp (Pte. Ltd.) communicates the following control-related information internally:

- **Control Requirements**: Management communicates security requirements and responsibilities to all employees during onboarding and security training.

- **Control Performance**: Reports summarizing control effectiveness are accessible to Director and System Admin.
- **Control Exceptions**: Security anomalies and incidents are reported to affected teams and management within 3 days of detection.
- **Control Changes**: Updates to control procedures are communicated company-wide before implementation.

These communications are delivered through: - Structured email notifications from helpdesk@mmfgroupinc.com.com - Dedicated Microsoft Teams security channel - Quarterly security briefings for all staff

6.2 External

MMF Consulting Grp (Pte. Ltd.) maintains structured external communication processes for control-related information. Communications to shareholders, customers, contractors, regulators, and government entities are managed according to contractual and statutory requirements as follows:

1. **Regulatory Communications**: Compliance reports are submitted to regulators as required by applicable regulations.
2. **Customer Communications**: Security incidents affecting customer data are communicated within 72 hours of confirmation.
3. **Contractor / Consultant Communications**: Control requirements are formally communicated to contractors / consultants during contracting and annually thereafter.
4. **Audit Communications**: Control information is shared with auditors according to established audit protocols.

All external communications are approved by Legal and documented in the communications register.

7 Third-Party Management

MMF Consulting Grp (Pte. Ltd.) maintains a structured approach to vendor management, even though our core audit services are delivered by internal staff. For technology service providers (such as Microsoft 365 and Box), we implement the following risk management practices:

1. **Vendor Risk Assessment**: All technology vendors undergo security assessment before adoption, including:
    - Review of SOC 2 or equivalent compliance reports
    - Evaluation of security capabilities against our requirements
    - Assessment of business continuity capabilities
2. **Contractual Requirements**: All vendor contracts include specific security requirements, including:
    - Data protection obligations
    - Breach notification requirements
3. **Ongoing Monitoring**: Active vendors are monitored through:
    - Annual review of compliance attestations
    - Quarterly service performance evaluations
    - Monitoring of security incident notifications

For client data handling, MMF Consulting Grp (Pte. Ltd.) does not currently outsource analysis tasks or exchange customer-related data with third parties. Should this change, additional third-party security evaluation controls would be implemented, subject to prior client approval.

8 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.