May Payment SP. Z O.O. MANAGEMENT BODY SUITABILITY ASSESSMENT POLICY

Policy Name	Management Body Suitability Assessment Policy	Version	2.0.
Drafted by	Internal legal and compliance team, strictly confidential and this information can be provided by the official request by the third party (Regulator, External Provider and/or Client)	Approved by Board on: 01.01.2026	
Responsible person	Internal legal and compliance team, strictly confidential and this information can be provided by the official request by the third party (Regulator, External Provider and/or Client)	Scheduled review date: 30.12.2026	

May Payment Sp. z o.o. (hereinafter referred to as "**May Payment**", "**our business**", "**Company**" "**we**", "**our**" or "**business**") Management Body Suitability Assessment Policy (hereinafter referred to as "**Policy**") sets out the procedures and criteria by which the Company assesses the suitability of all personnel – including the management body (board members and senior executives), key function holders (e.g. compliance, risk, security officers), and general staff – to ensure they meet regulatory and internal standards. It is designed to ensure ongoing compliance with the EU Markets in Crypto-Assets Regulation (MiCA), ISO/IEC 27001 (information security) requirements, and Polish AML/CFT laws. The Policy ensures that all persons are of appropriate integrity, competence, and experience for their roles.

1. Scope

This Policy applies to every staff member of the Company, without exception: the Management Board, executive officers, key function holders (including the AML Officer/MLRO, Information Security Officer, Risk Officer, etc.), and all other employees and contractors. It covers all stages of employment: pre-employment screening, onboarding, ongoing employment, and any reassessment triggered by significant incidents or crisis events.

2. Definitions:

1. **Fit and Proper:** As defined under MiCA, requiring members of the management body and key staff to be of "sufficiently good repute" with appropriate knowledge, skills, and experience, and not be convicted of serious offences (e.g. money laundering).
2. **Key Function Holder:** A person entrusted with functions critical to compliance or risk management (e.g. Compliance Officer, Risk Officer, ICT Security Officer).
3. **Politically Exposed Person (PEP):** As defined in the Polish AML Act, a person performing prominent public functions, or their close associates.
4. **High-Risk Personnel:** Roles or individuals identified as having elevated risk (e.g. executives with transaction authority, staff with privileged access, or employees with PEP status or connections).
5. **Information Security Competence:** As per ISO 27001:2022 Clause 7.2, the demonstrated knowledge, experience, and skills of personnel concerning information security tasks. Awareness: Per ISO 27001 Clause 7.3, personnel's understanding of the ISMS policies, their role in security, and response to non-conformance.

3. Fit-and-Proper Criteria (MiCA Compliance)

In accordance with MiCA, the Company requires that members of its management body and relevant staff are fit and proper. In practice, this means:

1. **Honesty and Integrity:** No history of convictions for fraud, money laundering, terrorist financing, or other crimes affecting reputation.
2. **Professional Competence and Experience:** Sufficient relevant qualifications, knowledge, and skills (e.g. financial, technical, legal expertise) for the position, demonstrated via education, certifications, and previous experience.
3. **Financial Soundness:** No recent bankruptcies or insolvency as decision-maker.
4. **Time Commitment:** Ability to devote adequate time to duties.
5. **Governance Standards:** Understanding of sound corporate governance (e.g. absence of conflicts of interest, adherence to company bylaws and regulatory requirements) and no history of regulatory sanctions or compliance breaches.

These criteria align with MiCA's mandate that CASP personnel be of good repute and capable of managing the firm prudently. The Company adopts these fit-and-proper benchmarks for all senior and key staff, ensuring collective competence and integrity in leadership.

4. Pre-Employment and Onboarding Assessments

Prior to hiring, candidates undergo a structured suitability evaluation:

- Background Checks: Verification of identity, education, professional qualifications, and employment history. Criminal record checks are required for senior roles and all positions touching customer funds, as permitted by Polish law. Applicants must disclose any PEP status or related exposures.
- References and Vetting: Collect and review references from previous employers or educational institutions. For key roles, interviews include scenarios testing job-specific knowledge and ethical decision-making.
- AML/PEP Screening: As part of due diligence, HR and Compliance screen candidates against internal PEP/sanctions lists. Any candidate who is a PEP or closely related to one is flagged as high-risk, requiring enhanced assessment. Polish AML/CFT law mandates a risk-based approach, including identifying PEPs and applying enhanced measures. The Company therefore requires all candidates to complete a conflict-of-interest and PEP disclosure form during onboarding.
- Information Security Competence: Assess technical roles for necessary security qualifications or certifications. All new hires must undergo baseline information security awareness training (per ISO 27001 7.3) and demonstrate understanding of Company security policies.

If a candidate passes these checks, HR documents the findings (e.g. background check reports, reference summaries, screening results) in the personnel file and certifies suitability before final offer. This documentation is retained as audit evidence, fulfilling ISO 27001 requirements to "retain evidence of competence" measures.

Onboarding: Upon hiring, new employees are formally briefed on compliance, security, and AML policies. They must sign confidentiality/conflict-of-interest agreements and complete role-specific compliance training (e.g. AML training, security protocols) within the first 30 days. These steps ensure that newcomers immediately understand expectations for integrity and competence.

Ongoing Suitability Assessments

The Company maintains continuous oversight of personnel suitability through the following procedures:

- Periodic Reviews: Annually (at minimum), each employee's continued fitness for role is assessed. For executives and key holders, review cycles may be more frequent (e.g. semi-annual). Reviews include:
- Performance Appraisals: Evaluation of job performance, including adherence to ethical and security standards. Managers verify that staff maintain required qualifications and licenses.
- Training and Competence Updates: Confirmation that staff have completed mandatory refresher courses. Information-security-critical roles must attend annual advanced security training and pass periodic awareness quizzes or simulations (e.g. phishing tests) in line with the Company's ISO 27001-based training program.
- Background and AML Re-Screening: At least annually for high-risk positions, HR/Compliance re-checks criminal records and updates PEP/sanctions screening lists. Any change in circumstances (marriage into a political family, inheritance of wealth, etc.) is disclosed and evaluated.

- Ongoing Fit Assessment: Review of any changes in personal circumstances (bankruptcy, legal proceedings, regulatory investigations). Employees must promptly notify HR of events that could affect their status.
- Governance Oversight: The Board (or a designated Board committee) periodically validates that management demonstrates good governance. It ensures no conflicts of interest exist and that governance roles (e.g. internal audit head) meet fitness standards. In line with MiCA Article 68, the board ensures that policies and procedures are "sufficiently effective" and conducts annual management assessments.
- Documentation: All review outcomes, training records, and attestations are documented in personnel records. This audit trail supports both internal compliance checks and external audits. For example, ISO 27001 requires retaining evidence of training and competence measures.

Crisis-Triggered Reassessment

Certain events may trigger immediate reassessment of personnel suitability:

- Regulatory Breach or Compliance Incident: If the Company experiences a material regulatory violation (e.g. an AML lapse or MiCA rule breach), the Compliance Officer conducts a targeted review of involved staff and decision-makers. The Board may re-evaluate the fitness of responsible executives and key staff to prevent recurrence.
- Cybersecurity Incident: A serious information security breach or cyber-attack prompts an urgent review of IT and security personnel's actions and competencies. The Company may require incident-response staff to undergo refresher training or assessment of practical skills. If a failure is traced to inadequate expertise, personnel changes or additional training are immediately enacted.
- Significant Organizational Change: Major business changes (e.g. mergers, new product lines) can raise suitability issues. Relevant managers must then re-confirm their qualifications and availability for new duties.

In any crisis scenario, the Company's Compliance and Risk units jointly oversee reassessments. Findings and corrective actions (such as re-training, role reassignments, or disciplinary action) are recorded. If breaches reflect on an individual's integrity or competence, the Company may suspend or remove them, in accordance with employment law and in some cases notify regulators as required.

Information Security Competence (ISO 27001 Alignment)

Consistent with ISO/IEC 27001:2022, the Company adopts a risk-based approach to ensure staff competence and awareness:

- Role-Based Training Plans: Based on risk assessment, the Company defines required security competencies for each role. For example, developers must be trained in secure coding, while operations staff must know incident response procedures.
- Competence Verification: In line with ISO 27001 Clause 7.2, the Company verifies that personnel are competent through review of qualifications, certifications, or practical tests. Where gaps are found, targeted training or mentoring is provided. The effectiveness of competence-building actions is evaluated (e.g. test scores, practical drills), and records are kept as evidence.
- Awareness Programs: As required by ISO 27001 Clause 7.3, all employees receive regular security awareness training. Content covers the Company's security policies, individual responsibilities, and consequences of non-compliance. Management ensures that staff know how to report incidents and the basics of threat recognition (phishing, social engineering, etc.). Metrics from simulated attacks inform where refresher sessions are needed.

These measures ensure that information security is integrated into suitability assessments: personnel handling sensitive systems are scrutinized for their security expertise and commitment to continuous improvement. The Company documents all training completion and testing outcomes for auditability.

AML/CFT Considerations

To comply with the Polish AML/CFT Act (2018) and FATF standards, the Policy includes AML-specific suitability checks:

- PEP and Sanctions Screening: HR/Compliance verify that no employee or their close relatives hold positions defined as PEP under Article 2(2)(11) of the Polish AML Act. If a candidate or employee is identified as a PEP (or becomes one), the Company classifies them as high-risk. Enhanced measures (e.g. increased managerial oversight, additional disclosures, and possibly exclusion from certain decision-making) are applied to mitigate risk. This aligns with the requirement for risk-based procedures and additional scrutiny of PEPs.
- Conflict of Interest: Staff must declare any connections to customers or counterparties, especially involving family members in politics or public office. Such declarations are reviewed by Compliance to prevent potential money-laundering schemes or undue influence.
- High-Risk Role Monitoring: Employees in roles dealing with customer funds or transactions (e.g. traders, cashiers) are subject to extra diligence. The Company conducts enhanced due diligence on these employees analogous to customer due diligence – for example, reviewing their financial background and travel history to detect any undeclared cross-border exposures.
- Whistleblowing and Reporting: All staff are reminded of their duty to report suspicious behavior (by themselves or others). The Company's whistleblower mechanism provides safe channels to flag internal misconduct. Any reports trigger immediate suitability review of implicated individuals.

These AML/CFT provisions ensure that personnel suitability is also viewed through an anti-financial crime lens, thereby protecting the Company's integrity and complying with Polish law. All AML-related assessments are documented as part of the suitability record.

Roles and Responsibilities

- Board of Directors: Ultimately responsible for approving this Policy and ensuring its effectiveness. The Board (or a suitable committee) periodically reviews aggregate suitability results and approves any policy changes.
- Human Resources (HR): Conducts background checks, organizes onboarding screenings, maintains personnel records, and initiates periodic assessments (in coordination with managers). HR ensures documentation of all evaluation steps.
- Compliance Officer: Oversees the suitability program, especially AML/CFT aspects. Validates PEP/sanctions screening, reviews conflict-of-interest disclosures, and audits suitability processes for regulatory compliance. The Compliance team also ensures MiCA fit-and-proper criteria are met by management, notifying regulators of any changes as required by Article 69 of MiCA.
- Information Security Officer (ISO): Ensures that information security competence and awareness components of the assessments are carried out. Provides training resources, conducts security drills, and reports on ISO 27001 compliance.
- Line Managers: Assess their team members' ongoing competence and integrity, conduct performance reviews, and report any issues to HR/Compliance. Managers also confirm that staff complete required trainings.
- Employees: Must cooperate by providing accurate information (e.g. during vetting), completing training, and self-reporting any changes affecting their suitability. They are required to uphold the Company's ethical standards at all times.

Each unit keeps records of its activities to enable internal or external auditors to verify compliance with this Policy.

Documentation, Auditability, and Review

The Company maintains strict documentation for all suitability assessments: background check reports, interview notes, training completion certificates, PEP/COI declarations, assessment matrices, and review outcomes. These records are retained securely (in compliance with data protection laws) and are made available for audits. The policy itself, and its implementation, are subject to periodic audit (internal and/or by regulators) to ensure effectiveness and compliance with evolving standards.

This Policy will be reviewed at least annually, or whenever there are significant legal or organizational changes (e.g. updates to MiCA, AML laws, ISO standards, or the Company's business model). Any amendments are approved by the Board. This review process satisfies MiCA's requirement that providers adopt "effective policies and procedures" and continually improve them.

Role-Based Assessment Table

Role/Position	Assessment Criteria	Review Frequency	Responsible Unit	Evaluation Method(s)
Board of Directors	MiCA fit & proper (repute, experience, no ML/TF record), governance expertise, time commitment. No conflicts.	At appointment and annually	Nomination Committee (Board); Compliance	Background check, regulatory screening, reference checks, Board interviews, ongoing self-declarations
Chief Executive / Officers (C-level)	Leadership track record, sector experience, integrity, absence of sanctions, AML/CFT awareness.	At hiring and annually	HR; Compliance; CEO	CV verification, interviews, reference checks, annual performance & conflict-of-interest review

Key Function Holders (e.g. AML, Risk, InfoSec)	Relevant certifications, technical competence, adherence to laws/policies, integrity.	At assignment and annually	HR; Compliance; ISO	Verify qualifications, role-specific interviews, periodic skills tests (e.g. compliance case studies, security drills)
IT & Security Personnel	Technical certifications (e.g. CISSP), secure coding/systems experience, clean record.	At hiring and annually (after major projects)	HR; ISO; CTO	Skills assessment, certification check, phishing/social-engineering test results, code review audits
Finance/AML Staff	Accounting/AML qualifications, track record in compliance tasks, integrity.	At hiring and annually	HR; Compliance; CFO	Qualification verification, transaction-monitoring simulations, AML case exercises
Other Managers/Supervisors	Appropriate management experience, legal awareness, no conflicts of interest.	At hiring and annually	HR; Dept. Head	Reference checks, managerial experience review, conflict declarations
General Employees	Basic suitability (ID, no disqualifying record), role-specific aptitude, completion of required trainings (security, AML).	At hiring and every 1–3 years (or on role change)	HR; Line Manager	

This table supplements the Policy by clarifying how different roles are evaluated, how often reviews occur, and which departments carry out the checks. It exemplifies our risk-based approach: higher-

impact roles have more stringent criteria and oversight. Each evaluation is documented and subject to audit, ensuring transparency and compliance with MiCA and ISO principles.