Magma Tech Solution Co., Ltd.

BUSINESS GOVERNANCE AND OPERATIONAL CONTROLS FRAMEWORK

Governance • Accountability • Operational Assurance

MAGMA TECH SOLUTION CO., LTD.

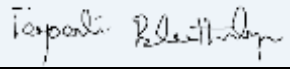
Version 1.0 | Effective 1 January 2026

Document control	Details
Document owner	Magma Tech Solution Co., Ltd. – Management
Version	1.0
Effective date	1 January 2026
Review frequency	At least annually and following material changes
Approver	Tapati Bhattacharya – Managing Director

Approval and Effective Date: This Framework has been approved by Management and is effective from 1 January 2026. Management is responsible for overseeing its implementation and ensuring that it remains relevant to the Company's business operations and applicable requirements.

Document Control and Approval

Version	Date	Change / reason	Prepared / reviewed by	Approved by
1.0	1 January 2026	Initial issue – approved by Management	Management	Tapati Bhattacharya – Managing Director

Approval item	Record
Document owner	Magma Tech Solution Co., Ltd. – Management
Review responsibility	Management, with input from relevant functional owners
Approver	Tapati Bhattacharya – Managing Director
Signature	
Approval date	Date of signature: 24th December 2025
Next review date	By 1 January 2027, and annually thereafter or earlier if material changes occur.

1. Purpose and Scope

This Internal Control Framework (Framework) describes the governance arrangements and practical controls Magma Tech Solution Co., Ltd. uses or is to implement to support reliable operations, protect company and client interests, maintain accurate records, and manage operational, financial, personnel, information-security and compliance risks. It is proportionate to the company's size, structure and IT outsourcing / consulting activities. It is not an independent audit, certification or assurance opinion.

It applies to relevant company activities and personnel, including Management, employees, recruitment, HR / Administration, Finance / Payroll, Account Management / Operations, IT support and, where relevant, consultants, contractors and third parties acting on behalf of Magma Tech Solution Co., Ltd.

- Recruitment, candidate screening and consultant deployment.
- Employment / engagement administration, onboarding, assignment changes and offboarding.
- Client contracts, work orders, purchase orders, timesheets and invoicing.
- Payroll, expenses, payments and financial recordkeeping.
- Company and client information, personal data, systems and access.
- Legal, statutory, immigration and contractual obligations, where applicable.
- Risk monitoring, incident escalation, corrective action and business continuity.

2. Internal Control Principles

- Accountability: material activities have an identified responsible role.
- Authorization: transactions and commitments are approved by an appropriately authorized person.
- Verification: important information and transactions are checked before processing or release.
- Segregation / compensating review: where staffing does not permit full separation of duties, a management or other independent review is used where practicable.
- Evidence: approvals, reconciliations, checklists and material decisions are retained as appropriate.
- Confidentiality: access to company, client and personal information is limited to legitimate business needs.

- Escalation: significant errors, suspected misconduct, security incidents and compliance concerns are promptly raised to Management.
- Proportionality: controls are scaled to the size, risk and complexity of the activity.

3. Governance, Roles and Responsibilities

Role / function	Key control responsibilities
Management / Managing Director	Approves this Framework and material policies; oversees significant risks; authorizes matters within delegated authority; reviews material incidents, exceptions and corrective actions.
HR / Administration	Maintains personnel and engagement records; supports onboarding and offboarding; tracks work authorization dates where applicable; protects employee and candidate records.
Recruitment	Checks candidate information and role suitability; maintains recruitment records; obtains required permissions / consents where applicable; communicates accurate candidate information.
Finance / Payroll	Checks payroll inputs and calculations; maintains payment, invoice and expense records; monitors receivables and statutory payment obligations; escalates discrepancies.
Account Management / Operations	Monitors client contracts, work orders, POs, consultant deployment, timesheets, assignment changes, client feedback and end-of-assignment coordination.
IT support / designated IT contact	Coordinates company-system access, security practices, access changes and removal, backups and IT incident escalation within assigned authority.
All personnel / consultants	Follow applicable policies and client requirements; protect information and assets; use access only for authorized work; report concerns and incidents.

4. Key Internal Controls

4.1 Financial, Invoicing and Payment Controls

- Client invoices should be checked against the applicable contract / work order, approved rates, billing period and supporting timesheet or service evidence, where relevant.
- Material invoice adjustments, credit notes, refunds and unusual payments should be reviewed and approved by an authorized person.
- Company expenses should have a business purpose, supporting documentation and appropriate approval before reimbursement or payment.
- Bank and payment records should be reviewed periodically; unexplained differences should be investigated and escalated.
- Financial records should be retained in accordance with applicable legal, tax, contractual and company requirements.

4.2 Payroll Controls

- Payroll should be prepared from authorized employee / consultant records and verified inputs, including attendance, timesheets, approved changes, deductions and allowances, as applicable.
- Payroll calculations and payment totals should be checked by an appropriate reviewer before disbursement.
- Changes to salary, bank details, allowances or deductions should be supported by documented authorization.
- Payroll information is confidential and access is limited to personnel who require it for their duties.
- Errors, late inputs or payment exceptions should be documented, corrected and escalated where material.

4.3 Recruitment and Personnel Controls

- Candidate CVs, qualifications, experience and relevant role information should be reviewed for consistency and suitability before submission to a client.
- Candidate personal data should be collected, used, shared and retained only for legitimate business purposes, with appropriate notice / consent or other lawful basis where required.

  Recruitment activities must not involve forced labour, human trafficking, deceptive recruitment, unlawful worker-paid recruitment fees or coercive retention of identity documents. Recruitment partners should be informed of these expectations where relevant.

- Employment or consultant engagement terms should be documented before commencement, as applicable.
- Onboarding should confirm required documentation, assignment details, client requirements and access arrangements.
- Offboarding should include return of company / client property, closure of relevant access, final payroll / timesheet checks and record updates.

4.4 Consultant Deployment and Client Service Controls

- Deployment should be supported by an agreed role, rate, start date, work location / arrangement and applicable client approval or work order.
- Account Management / Operations should maintain a record of active consultants, assignment dates, client contacts and material assignment changes.
- Timesheets or attendance records should be reviewed and approved in accordance with the client's process before billing and payroll, where applicable.
- Client feedback, performance concerns, absence, resignation and replacement needs should be documented and escalated to the relevant owner.
- At assignment end, the responsible team should coordinate return of assets and removal of client-system access with the client.

4.5 Contract, PO and Compliance Controls

- Executed client agreements, work orders, purchase orders, amendments and relevant correspondence should be stored in an authorized location.
- Contract, PO, work permit and other relevant expiry dates should be recorded and monitored, with advance reminders where practicable.
- Changes to rates, scope, personnel, assignment dates or commercial terms should be documented and approved before implementation where required.
- Management / Administration should monitor relevant company registration, tax, labour, immigration, BOI-related and other statutory requirements applicable to the company and its activities.
- Legal or regulatory questions outside internal competence should be referred to an appropriately qualified adviser.

4.6 IT, Information Security and Data Privacy Controls

- Company and client systems should be accessed only by authorized users for approved business purposes.
- Access should be granted according to role and need; access changes and termination should be coordinated promptly when personnel join, change roles or leave.
- Passwords, authentication credentials, devices and access tokens must not be shared or exposed to unauthorized persons.
- Company, client and personal information should be stored and transferred using appropriate approved channels and safeguards.
- Suspected loss, unauthorized access, malware, data disclosure or other security incidents should be reported promptly to Management and the designated IT contact; client notification should follow applicable contractual and legal requirements.

The incident coordinator or Management should assess the incident, take reasonable containment steps, preserve relevant evidence, record the known facts and actions taken, and determine whether client, affected-person or regulator notification is required by applicable law or contract.

- Personal data should be handled in accordance with applicable privacy laws, including Thailand's PDPA where it applies.

  AI and other digital tools may be used only for legitimate business purposes. Confidential client information, personal data, CVs, payroll information, credentials and restricted records must not be entered into public or unauthorized AI tools. AI-generated outputs must be checked by an appropriate person before use, including for accuracy, confidentiality, bias and intellectual-property concerns.

4.7 Procurement and Third-Party Controls

- Purchases and third-party engagements should have a legitimate business purpose and appropriate approval.
- Supplier selection should consider capability, cost, reliability, conflicts of interest and relevant compliance / confidentiality requirements.

  For material suppliers or subcontractors, proportionate due diligence should be performed before engagement and periodically where warranted. Checks may include business identity, service capability, conflicts of interest, confidentiality commitments, data-protection and security arrangements, and relevant legal or contractual compliance. The extent of screening should reflect the nature and risk of the services.

- Where a third party may access client or personal information, appropriate confidentiality, data protection and security obligations should be agreed before access is provided.
- Material supplier issues or suspected misconduct should be escalated and corrective action documented.

5. Internal Control Responsibility Matrix

Control area	Responsible function	Review / oversight
Recruitment and candidate checks	Recruitment	HR / Management, as appropriate
Employment records and onboarding / offboarding	HR / Administration	Management
Consultant deployment and timesheets	Account Management / Operations	Management
Client contracts, work orders and PO tracking	Account Management / Operations	Management
Invoicing, expenses and payments	Finance / Accounts	Authorized Management reviewer
Payroll preparation and verification	Finance / Payroll	Authorized reviewer / Management
Work authorization tracking, if applicable	HR / Administration	Management
IT access and information security	Designated IT contact / system owner	Management
Privacy and data handling	Relevant process owner	Management
Risk register and corrective actions	Relevant risk owners	Management

6. Risk Management and Control Monitoring

Magma Tech Solution Co., Ltd. should maintain a Risk Register covering material operational, financial, personnel, client-service, information-security and compliance risks. Each risk should have a likelihood rating, impact rating, risk score, mitigation / monitoring action, responsible owner and current status.

Rating	Likelihood	Impact
1	Rare	Insignificant
2	Unlikely	Minor
3	Possible	Moderate

4	Likely	Major
5	Almost certain	Severe

Risk score = Likelihood × Impact. Risk bands should follow the approved Risk Management Policy. Management should review high risks and material changes, and ensure actions have an owner and target date.

7. Incident, Exception and Corrective Action Management

- Personnel should promptly report suspected fraud, bribery, conflicts of interest, payroll errors, unauthorized disclosure, system-access issues, workplace concerns, regulatory issues or material client-service failures.
- Management or the designated responsible person should assess the issue, determine immediate containment steps, identify who needs to be informed and preserve relevant records.
- Where appropriate, record the issue date, description, impact, owner, action taken, target date and closure evidence.
- Corrective actions should address the cause of the issue where practicable and be checked for completion.
- Reports should be handled sensitively and confidentially to the extent reasonably possible. Retaliation against good-faith reporting is not permitted.

8. Business Continuity and Operational Resilience

Management should identify critical activities and maintain proportionate continuity arrangements. These may include backup management / client contacts, access to essential company records, alternative payroll processing arrangements, backup personnel for key responsibilities and a process to identify replacement consultants where feasible. Significant disruption should be escalated to Management and affected clients in accordance with contractual obligations.

9. Records, Evidence and Retention

Records supporting the operation of controls should be maintained securely and be retrievable by authorized personnel. Examples include approvals, contracts, work orders, POs, timesheets, payroll review records, invoice checks, onboarding / offboarding checklists, access records, risk reviews, incident reports and corrective-action records. Retention and disposal should follow applicable legal, contractual and company requirements. Personal and confidential information must not be shared externally unless authorized and appropriate.

Retention periods should be determined by record category and applicable statutory, tax, employment, privacy, immigration and contractual requirements. Candidate CVs and other personal data should not be retained longer than necessary for the relevant recruitment or business purpose, unless a lawful basis or legal requirement supports continued retention. Records reaching the end of their retention period should be securely deleted or destroyed, subject to any legal hold or ongoing claim.

10. Review and Continuous Improvement

Management should review this Framework at least annually and when there is a material change in operations, legal requirements, client obligations, technology environment or risk profile. Reviews should consider incidents, client-assessment findings, overdue actions, changes in risk ratings and whether controls remain practical and effective. Changes should be recorded in the document history.

Appendix A – Control Evidence Checklist

Use this checklist to identify evidence that can be provided to a client. Mark a status only after checking the relevant records. Redact personal, salary, banking and confidential client information unless disclosure is authorized.

Control area	Examples of evidence	Status / reference
Corporate governance	Approved Code of Conduct; approval record; policy review record	Maintained by the responsible function, as applicable; provided when relevant and authorized.
Financial controls	Invoice approval records; expense approvals; payment review records; reconciliations	Maintained by the responsible function, as applicable; provided when relevant and authorized.
Payroll controls	Payroll verification checklist; approved payroll inputs; statutory payment records	Maintained by the responsible function, as applicable; provided when relevant and authorized.
Recruitment / HR	Candidate screening records; engagement documents; onboarding / offboarding checklist	Maintained by the responsible function, as applicable; provided when relevant and authorized.
Consultant management	Deployment register; approved timesheets; client feedback / issue records	Maintained by the responsible function, as applicable; provided when relevant and authorized.
Contract / PO management	Executed agreements; work orders; PO and expiry tracker	Maintained by the responsible function, as applicable; provided when relevant and authorized.
IT / access management	User access list; access request / removal evidence; incident records	Maintained by the responsible function, as applicable; provided when relevant and authorized.
Privacy / confidentiality	Privacy notice or procedure; NDA / confidentiality clauses; data handling instructions	Maintained by the responsible function, as applicable; provided when relevant and authorized.
Risk management	Risk Register; risk review record; corrective-action register	Maintained by the responsible function, as applicable; provided when relevant and authorized.
Business continuity	Backup contact list; continuity arrangements or plan	Maintained by the responsible function, as applicable; provided when relevant and authorized.

Appendix B – Internal Control Review Checklist

Review question	Result / notes	Action owner / target date
Are key client contracts, work orders and POs recorded and expiry dates monitored?	[To be completed during the periodic review.]	[To be assigned if required]
Are consultant deployment details and approved timesheets maintained?	[To be completed during the periodic review.]	[To be assigned if required]
Are invoices checked against agreed terms and supporting records?	[To be completed during the periodic review.]	[To be assigned if required]
Are payroll inputs and calculations reviewed before payment?	[To be completed during the periodic review.]	[To be assigned if required]
Are recruitment, onboarding and offboarding records maintained?	[To be completed during the periodic review.]	[To be assigned if required]
Are access rights changed or removed when personnel leave or assignments end?	[To be completed during the periodic review.]	[To be assigned if required]
Are personal and client data handled through appropriate channels and access controls?	[To be completed during the periodic review.]	[To be assigned if required]
Are incidents, exceptions and corrective actions recorded and followed up?	[To be completed during the periodic review.]	[To be assigned if required]
Have material risks and overdue actions been reviewed by Management?	[To be completed during the periodic review.]	[To be assigned if required]

Appendix C – Corrective Action Register

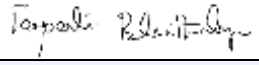
Ref.	Issue / control gap	Action required	Owner	Target date	Status / closure evidence
CA-01	[To be recorded if a control gap or deficiency is identified.]	Define and document the corrective action required.	Responsible Manager / Assigned Personnel	[Date to be assigned]	[Open / In progress / Closed] Evidence to be recorded upon completion.
CA-02	[Describe issue, if any]	Define and document the corrective action required.	Responsible Manager / Assigned Personnel	[Date to be assigned]	[Open / In progress / Closed] Evidence to be recorded upon completion.

Appendix D – Management Review Record

Review item	Record
Review date	24 December 2025
Reviewed by	Tapati Bhattacharya – Managing Director
Scope of review	Internal controls, incidents, risk register, client requirements and corrective actions
Material changes since previous review	Initial issue. Material changes will be recorded at subsequent reviews.
Control gaps / overdue actions	Any identified gaps are recorded in Appendix C with an assigned owner and target date; material issues are escalated to Management.
Decisions / escalation required	Management adopts this Framework and requires relevant function owners to operate the controls applicable to their responsibilities.
Next review date	By 1 January 2027, and annually thereafter or earlier if material changes occur.

Approval and Authorization

By signing below, the authorized approver confirms that this Framework has been reviewed and approved by the Management of Magma Tech Solution Co., Ltd. for implementation within the Company and circulation to clients, business partners and other relevant stakeholders, as appropriate. The Framework reflects the Company's governance principles, internal control arrangements and operational practices, subject to applicable laws, contractual obligations and the Company's actual operating procedures.

Approval field	Details
Approved by	Tapati Bhattacharya – Managing Director
Title	Managing Director
Signature	
Date	Date of signature: 24th December 2025
Effective date	1 January 2026

Important implementation note

This Internal Control Framework has been established and approved by Magma Tech Solution Co., Ltd. to define the Company's governance responsibilities, operational controls and risk-monitoring practices.

Management is responsible for overseeing the implementation and ongoing effectiveness of this Framework, reviewing the adequacy of the controls described and identifying opportunities for improvement in line with the Company's business operations and applicable requirements.

Where further enhancements or improvements to existing controls are identified, appropriate responsibilities shall be assigned, and progress shall be monitored by Management to support continuous improvement.

This Framework represents the Company's internal management and control arrangements. It does not constitute an ISO certification, independent audit report, external assurance opinion or certification against any particular control standard.