



Enterprise Compliance Policy (ECP)

Document Classification: Confidential – Internal Use Only

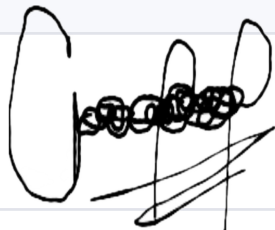
FIELD	VALUE
Policy ID	OG-ECP-001
Version	1.0
Status	Approved
Effective Date	October 8, 2025
Next Review Date	October 8, 2026(annual, or earlier upon regulatory change)
Review Frequency	At least annually; ad hoc upon material change
Document Owner	Oleksii, Chief Security & Compliance Officer (CSCO)
Document Sponsors	CEO; Chief Commercial Officer
Contact (Policy Queries)	compliance@orchestrate.global
Supersedes	N/A (first issue)



Related Documents	Code of Conduct; AML/CFT Framework; Sanctions Standard; Data Protection Policy; Secure SDLC Standard; Incident Response Plan; Third-Party Risk Standard
Distribution	Executive Leadership; All People Managers; All Staff; Relevant Third Parties under NDA
Retention	Maintain most recent approved version + 7 years of history in the Controlled Documents Repository

Approvals

By signing, the undersigned confirm that they have reviewed and approved this policy, and that the organization commits to implementing and maintaining effective compliance controls aligned to all applicable legal, regulatory, and contractual obligations.

Position	Name	Signature	Date
Chief Executive Officer (CEO)	Preston Obadan		8/10/2025
Chief Commercial Officer (CCO)	Kevin Kegera		8/10/2025



Document Owner Acknowledgement

I acknowledge responsibility for maintaining, communicating, and monitoring adherence to this policy and associated standards.

ROLE	NAME	SIGNATURE	DATE
Chief Security & Compliance Officer (CSCO)	Oleksii		8/10/2025

Document Control

Version	Date	Description of change	Author	Reviewed By	Approved By
1.0	2025-10-08	First issue; initial enterprise compliance policy	CSCO	CEO, CCO	CEO, CCO

Table of Contents

1. Purpose & Scope
2. Definitions
3. Governance, Accountability & the Three Lines Model
4. Compliance Risk Management Framework (CRMF)
5. Regulatory Inventory & Obligations Management
6. Regulatory Change Management
7. Policy & Standard Management
8. Training, Awareness & Certification
9. Conduct, Ethics, Conflicts & ABAC (Anti-Bribery/Anti-Corruption)
10. Data Protection & Privacy Compliance
11. Financial Crime & Sanctions Governance (Policy Interface)
12. Third-Party & Outsourcing Compliance
13. Product, Marketing & Customer Communications Compliance
14. Technology, Security & Operational Resilience Compliance
15. Model & Algorithmic Risk Compliance
16. Records Management & Retention
17. Monitoring, Testing & Quality Assurance



- 18. Issues, Incidents & Investigations
- 19. Metrics, KRIs/KPIs & Management Reporting
- 20. Board & Executive Reporting
- 21. Exceptions & Dispensation Management
- 22. Global & Local Alignment; Jurisdictional Addenda
- 23. Audit & Independent Assurance
- 24. Document Control

Appendices

- A. Control Matrix (Controls Page)
- B. RACI for Key Obligations
- C. Training Curriculum Map
- D. Glossary

1. Purpose & Scope

1.1 Purpose

The purpose of this Enterprise Compliance Policy (ECP) is to:

- Establish a unified compliance framework that ensures Orchestrate Global operates ethically, lawfully, and in accordance with all applicable regulatory, contractual, and industry obligations across all jurisdictions.
- Define roles, responsibilities, and minimum standards to identify, assess, monitor, and mitigate compliance risk.
- Embed a culture of integrity, transparency, and regulatory accountability throughout the organization.
- Provide a documented foundation that supports licensing, regulatory approvals, banking relationships, audits, investor due diligence, and third-party partnerships.



1.2 Scope of Application

CATEGORY	IN-SCOPE	OUT OF SCOPE
Legal Entities	All Orchestrate Global parent and subsidiary entities, joint ventures where Orchestrate Global has majority control or brand responsibility	Non-controlled affiliates and minority investments (unless specified by contract)
Functions & Departments	Executive Management, Commercial, Operations, Compliance, Legal, Technology, Finance, Risk, Security, Product, Customer Support, HR	Non-Orchestrate legal entities without operational involvement
Products & Services	Payment processing, treasury and liquidity services, foreign exchange, transaction routing, API-based payment orchestration, stablecoin<>fiat conversion tools, digital compliance services	Legacy, non-operational products, or products not yet approved by Compliance and Risk Committee
Customers	Financial institutions, fintechs, PSPs, marketplaces, merchants, corporates, NGOs	Direct-to-consumer retail services (currently not offered)
Third Parties	Vendors, cloud providers, outsourced service providers, payment facilitators, banking partners, correspondent networks, and agents	Entities without a contractual or operational relationship



1.3 Policy Authority

- This policy is approved by the CEO and Chief Commercial Officer under delegated authority from the Board.
- Compliance is mandatory for all executives, employees, contractors, consultants, interns, and relevant third parties.
- Local procedures may supplement this policy but cannot weaken or contradict it.
- Violations may lead to disciplinary action, contract termination, regulatory reporting, or legal proceedings.

2. Definitions

TERM	DEFINITION
Compliance Risk	The risk of legal or regulatory sanctions, financial loss, or reputational damage arising from failure to comply with laws, regulations, codes of conduct, or internal standards.
Three Lines Model	Governance structure where (1) Business owns risk; (2) Compliance & Risk provide oversight; (3) Internal Audit provides independent assurance.
Regulatory Obligation	A legal, supervisory, licensing, contractual, or industry requirement mandatory for operations.
AML/CFT	Anti-Money Laundering / Counter-Financing of Terrorism; separate policy framework referenced by this policy.
Sanctions	Restrictions imposed by governments or international bodies prohibiting transactions with individuals, entities, or countries.
PEP	Politically Exposed Person – individuals holding prominent public positions or their close associates/family.



ABAC	Anti-Bribery and Anti-Corruption – policies preventing illicit payments, facilitation payments, or improper influence.
Data Subject	An identifiable natural person whose personal data is processed by the organization.
Record	Any data or document generated, received, or maintained as evidence of business activities, regardless of medium.
High-Risk Jurisdiction	Countries identified due to elevated financial crime, sanctions exposure, regulatory deficiencies, or instability.
KRI/KPI	Key Risk Indicator / Key Performance Indicator – metrics used to measure compliance effectiveness and risk exposure.
Incident	A breach, error, data compromise, control failure, or regulatory violation requiring escalation and remediation.
Third-Party Risk	Risk arising when outsourcing or delegating to a vendor or partner who affects regulatory obligations or service delivery.

3. Governance, Accountability & the Three Lines Model

3.1 Governance Structure

Orchestrate Global maintains a formal governance framework that ensures accountability, regulatory oversight, and alignment of compliance activities with strategic objectives. Compliance governance is integrated into corporate governance through documented committees, decision rights, and escalation frameworks.



Key Governance Bodies:

GOVERNANCE BODY	MANDATE	CHAIR	FREQUENCY
Board of Directors	Ultimate oversight of compliance, ethics, and risk culture. Approves policies and receives compliance reports.	Board Chair	Quarterly
Executive Committee (ExCo)	Manages strategic and operational risks; ensures policy implementation.	CEO	Monthly
Risk & Compliance Committee (RCC)	Reviews compliance risks, breaches, regulatory developments, sanctions exposure, and remedial actions.	Chief Security & Compliance Officer (CSCO)	Bi-Monthly
Product & Change Committee	Evaluates new products, features, marketing content, and third-party integrations for compliance impact.	Chief Product Officer	Bi-Weekly
Incident Response & Escalation Group	Activated in security, regulatory, or operational incidents; ensures legal and regulatory notification.	CISO / CSCO	As required
Internal Audit (Independent)	Provides independent assurance over governance, risk, and compliance controls.	Audit Lead	Annual / Per Plan



3.2 Roles & Responsibility – Three Lines Model

LINE OF DEFENSE	DESCRIPTION	KEY RESPONSIBILITIES	STAKEHOLDERS
1st Line – Business & Operations	Own and manage risks; operate controls.	Perform customer onboarding, transaction screening, maintain documentation, follow policies.	Commercial, Operations, Finance, Product, Engineering
2nd Line – Compliance & Risk	Provide oversight, frameworks, and guidance. Monitor control effectiveness.	Develop policies; manage regulatory inventory; advise on compliance risk; monitor and test controls.	CSCO, Legal, Enterprise Risk Management
3rd Line – Independent Audit	Provides independent assurance to the Board.	Conduct audits; validate compliance with laws, licenses, policies; report deficiencies.	Internal Audit, External Auditors

3.3 Accountability Map

SENIOR ROLE	CORE COMPLIANCE ACCOUNTABILITIES
CEO – Preston Obadan	Ensures culture of integrity, regulatory readiness, and enforcement of this compliance policy.
Chief Commercial Officer – Kevin Kegera	Ensures customers, merchants, partners, and revenue activities comply with contractual, licensing, and regulatory requirements.



Chief Security & Compliance Officer – Oleksii	Policy owner; oversees compliance strategy, risk management, regulatory relationships, and incident escalation.
Chief Technology Officer (CTO)	Ensures secure, compliant system architecture, data protection standards, and technology-related regulatory safeguards.
Chief Financial Officer (CFO)	Financial reporting integrity, regulatory filings, licensing renewals, safeguarding client funds where applicable.
Head of Legal / General Counsel	Interprets regulatory requirements, manages regulatory notices, contractual compliance.
Head of Operations	Ensures customer onboarding, transaction monitoring, reconciliation, and operational procedures align with policy.
All Staff & Contractors	Adhere to this policy; complete training; report concerns or breaches immediately.

3.4 Escalation Framework

Compliance issues must be escalated promptly based on severity:

CLASSIFICATION	EXAMPLES	ESCALATE TO	TIMELINE
Level 1 – Minor	Documentation gaps, late training completion	Line Manager / Compliance Officer	Within 5 business days



Level 2 – Moderate	Policy breaches without financial or regulatory impact	CSCO / RCC	Within 48 hours
Level 3 – Major	Data breach, regulatory inquiry, unlicensed activity	CEO / CSCO / Legal Counsel	Within 24 hours
Level 4 – Critical	Sanctions breach, systemic AML failure, widespread outage affecting compliance	Board Chair / Regulators / Law Enforcement	Immediate (≤12 hours)

3.5 Independence of Compliance Function

- The Compliance function (2nd Line) operates independently of commercial and operational teams.
- The CSCO has direct, unrestricted access to the CEO, Board, and regulators.
- Compliance decisions cannot be overridden by revenue or operational teams without formal approval and documented risk acceptance.

4. Compliance Risk Management Framework (CRMF)

The Compliance Risk Management Framework (CRMF) provides a structured, enterprise-wide approach for identifying, assessing, mitigating, monitoring, and reporting compliance risks across Orchestrate Global's operations, products, legal entities, and jurisdictions.

4.1 Objectives of the CRMF

- Ensure compliance with all applicable legal, regulatory, licensing, contractual, and ethical obligations.
- Prevent regulatory breaches, financial penalties, sanctions, reputational damage, and operational disruptions.
- Establish consistent standards for risk identification, control design, monitoring, and remediation.



- Embed compliance considerations into all business decisions, processes, technology deployments, and product development lifecycles.

4.2 Compliance Risk Categories

RISK CATEGORY	DESCRIPTION	EXAMPLE EVENTS
Regulatory & Licensing Risk	Failure to obtain, maintain, or comply with regulatory licenses or approvals.	Operating without a required money transmission license.
Financial Crime & Sanctions Risk	Breaches of AML, CFT, or sanctions laws, or misuse of services for illicit purposes.	Processing a transaction involving a sanctioned entity.
Data Protection & Privacy Risk	Violation of data privacy laws or cross-border data transfer requirements.	Unauthorized disclosure of customer KYC documents.
Customer / Market Conduct Risk	Misleading marketing, unfair practices, or customer misinformation.	Inaccurate disclosure of FX fees leading to customer complaints.
Third-Party Compliance Risk	Reliance on outsourced vendors or partners that fail to meet regulatory obligations.	Cloud provider fails to provide audit logs as contractually required.
Technology & Cyber Compliance Risk	Use of insecure systems that fail mandated compliance standards or certifications.	API encryption failure leading to exposure of transaction data.



Reporting & Disclosure Risk

Failure in regulatory reporting, suspicious activity reporting, or financial disclosures.

Late submission of transaction monitoring reports to regulator.

4.3 Risk Management Lifecycle

PHASE	DESCRIPTION	OUTPUTS
1. Identification	Regulatory scanning, risk assessments, incident reports, product reviews.	Risk register entries; compliance impact assessment.
2. Assessment	Evaluate inherent risk, control design, effectiveness, and residual risk.	Risk ratings (Low / Moderate / High / Critical).
3. Control Design & Implementation	Design preventive and detective controls to mitigate risk.	Standard Operating Procedures (SOPs), automated alerts, approvals, segregation of duties.
4. Monitoring & Testing	Ongoing surveillance, thematic reviews, and compliance audits.	KRI dashboards, audit findings, corrective action plans.
5. Reporting & Escalation	Present outcomes to management committees, regulators if required.	Board compliance report; risk metrics; regulatory filings.



6. Remediation & Continuous Improvement

Root cause analysis, corrective actions, retraining, technology updates.

Remediation logs, updated controls, policy improvements.

4.4 Compliance Risk Rating Scale

RATING	DEFINITION	ACTION REQUIREMENT
Low	Minimal regulatory exposure; controls strong.	Monitor through BAU processes.
Moderate	Some regulatory exposure; no imminent breach.	Implement mitigation plan; periodic monitoring.
High	Significant exposure; potential for legal or financial repercussions.	Immediate mitigation; escalate to CSCO and Risk & Compliance Committee (RCC).
Critical	Near-certain or actual breach; potential regulatory or criminal impact.	Escalate to CEO and Board; implement crisis protocol.

4.5 Key Compliance Controls

CONTROL CATEGORY	EXAMPLES OF CONTROLS
Preventive	Segregation of duties, policy enforcement, pre-transaction screening, customer onboarding validation.



Detective	Real-time transaction monitoring, log analysis, reconciliation, sanctions alert systems.
Corrective	Incident response plans, remediation workflows, customer notifications, regulatory reporting.
Directive	Policies, training, compliance checklists, mandatory approvals, risk assessments.

4.6 Compliance Risk Register

A central Compliance Risk Register is maintained by the Compliance Office and includes:

- Risk description and category
- Root cause and exposure
- Inherent and residual risk ratings
- Controls mapped via Control Matrix (see Appendix A)
- Control owner and last review date
- Remediation plan and target close date (if applicable)

The register is reviewed quarterly by the Risk & Compliance Committee and updated in response to incidents, audits, or regulatory changes.

4.7 Integration with Enterprise Risk Management (ERM)

- Compliance Risk is integrated into the enterprise-wide risk taxonomy and reported as part of Orchestrate Global's overall risk profile.
- The CSCO provides monthly updates to the Executive Committee and quarterly reports to the Board.
- Material compliance risks inform the organization's Risk Appetite Statement and influence strategic decisions, product launches, and market entry evaluations.



5. Regulatory Inventory & Obligations Management

This section establishes how Orchestrate Global identifies, documents, interprets, and complies with regulatory, licensing, contractual, and industry obligations across all jurisdictions.

5.1 Purpose

To ensure that all regulatory obligations—current and emerging—are:

- Identified systematically
- Documented in a centralized and controlled repository
- Translated into actionable internal controls, policies, and procedures
- Monitored for compliance and reviewed during regulatory changes

5.2 Regulatory Inventory Structure

Orchestrate Global maintains a Regulatory Obligations Register (ROR) documenting all relevant obligations.

FIELD	DESCRIPTION
Regulation / Requirement	Title of law, regulation, license, supervisory guidance, industry standard, or contractual obligation.
Jurisdiction / Authority	Issuing regulator or standard-setting body.
Applicability	Entity, product, function, or geographic relevance.
Requirement Summary	Key obligation described in clear operational language.



Control Mapping	Associated internal policy, process, or system control.
Responsible Owner	Role accountable for compliance with this obligation.
Evidence	Reports, logs, audits, training completion, certifications.
Review Cycle	Quarterly, annual, or regulatory-triggered.

5.3 Sources of Regulatory Obligations

SOURCE TYPE	EXAMPLE
Statutes & Laws	National payments law, cybersecurity law, data protection law.
Regulators & Central Banks	Licensing conditions, reporting requirements, transaction caps.
International Standards	Financial crime frameworks, data protection standards, payment interoperability norms.
Contracts with Partners	Banking partners, liquidity providers, card networks, cloud service SLAs.
Industry Best Practices	Security certification frameworks, ISO standards, payment integrity guidelines.



5.4 Obligations Lifecycle Management

STAGE	DESCRIPTION	RESPONSIBLE
Identification	Legal/Compliance team scans legislation, regulator notices, industry alerts.	Legal, CSCO
Assessment	Impact assessment on products, licenses, vendors, data flows, operations.	Compliance + Business Owners
Translation	Convert legal text into operational controls or policy requirements.	Compliance
Implementation	Update policies, systems, contracts, training.	Policy Owners / Product / Tech
Monitoring	Periodic control testing, reporting, regulatory audits.	Compliance Monitoring Team
Review & Update	Annual or triggered by regulatory change.	CSCO

5.5 Licensing & Registration Obligations

- No entity may offer financial services in a jurisdiction without approval from the relevant authority.
- A License Register must be maintained with the following fields:



LICENSE FILED	DESCRIPTION
License Type	Money Transfer License, MSB Registration, EMI License, etc.
Jurisdiction	Country / Region
Issuing Authority	Central Bank, Financial Conduct Authority, etc.
Status	Active / Pending / Suspended
Effective & Expiry Dates	Validity period
Renewal Requirements	Documentation, capital requirements, audit
Designated Responsible Officer	Local Compliance Officer / Country Manager

5.6 Responsibility & Oversight

ROLE	RESPONSIBILITY
CSCO (Document Owner)	Maintains Regulatory Inventory & License Register.
Legal Department	Legal interpretation, regulatory correspondence, contractual obligations.



Product & Technology Teams	Ensure system features and data flows align with regulatory conditions.
Country Managers / Local MLROs	Ensure local adaptation of global policies.
Internal Audit	Periodic assurance over completeness and accuracy of the inventory.

5.7 Documentation & Recordkeeping

- All regulatory inventory data is stored in a Controlled Compliance Repository.
- Access is restricted based on the least-privilege principle.
- Version history is retained for at least 7 years.
- Changes to inventory must be approved by the CSCO or delegate.

6. Regulatory Change Management

Regulatory Change Management ensures Orchestrate Global remains compliant with evolving laws, supervisory expectations, licensing conditions, industry standards, and contractual obligations across all jurisdictions.

6.1 Objectives

- Proactively identify regulatory changes affecting Orchestrate Global's operations, products, systems, customers, or third parties.
- Evaluate the impact of these changes in a structured and documented manner.
- Ensure timely implementation of updates to policies, systems, contracts, and training.
- Maintain evidence of compliance for regulators, auditors, and bank partners.



6.2 Regulatory Change Process Overview

PHASE	DESCRIPTION	OUTPUT
1. Scan & Detect	Continuous monitoring of regulatory sources and industry alerts.	Regulatory Change Log Entry
2. Assess Impact	Legal and Compliance assess impact on business, technology, licensing, and data.	Impact Assessment Report
3. Assign Ownership	Designate responsible departments and timelines for implementation.	Change Owner & Action Plan
4. Implement Changes	Update policies, processes, systems, vendor contracts, or licenses.	Updated Documentation & Controls
5. Validate & Test	Confirm effectiveness through testing, QA, legal review.	Test Results & Compliance Sign-off
6. Record & Communicate	Update regulatory inventory, inform staff, train as needed.	Communication Logs, Training Records



6.3 Regulatory Change Sources

SOURCE TYPE	EXAMPLES
Government Legislation	New payments act, digital asset law, privacy amendment.
Regulatory Authorities	Central Bank notices, Financial Supervisory Agency directives.
Industry Bodies & Standards	Global financial crime guidelines, payment messaging standards, data protection frameworks.
Contractual Updates	Banking partner agreements, cloud service terms, liquidity provider mandates.
Enforcement Actions & Fines	Lessons from regulatory penalties issued to peers or competitors.

6.4 Change Classification & Response Time

CHANGE TYPE	DESCRIPTION	EXAMPLE	REQUIRED ACTION TIME
Critical Regulatory Change	High-impact legal change; non-compliance may lead to license revocation or criminal liability.	New licensing requirement; sanctions embargo.	≤30 days or regulator-set deadline



Standard Regulatory Change	Moderate impact; requires internal updates to policies or processes.	New data retention requirement.	≤90 days
Advisory / Best Practice	Non-binding guidance; improves compliance resilience.	New AML guidance by supervisory bodies.	≤180 days or when feasible

6.5 Roles & Responsibilities

ROLE	RESPONSIBILITIES
CSCO	Owns the change management framework; reports significant changes to ExCo and Board.
Legal Counsel	Interprets regulatory texts and advises on legal obligations.
Compliance Officers & MLROs (local/regional)	Assess jurisdiction-specific impact and ensure localization.
Product & Technology Heads	Implement system changes, API updates, encryption, and data storage modifications.
Training & HR	Update training materials and deliver staff certifications on new obligations.



Internal Audit

Perform post-implementation assurance and review control effectiveness.

6.6 Documentation & Evidence Requirements

All regulatory changes must be documented in a Regulatory Change Log including:

FIELD	DESCRIPTION
Change Reference ID	Unique identifier
Source	Regulator, law, contract, memo
Jurisdiction	Country, region, or supranational
Summary of Requirement	Extract of obligation in clear language
Impacted Areas	Product, tech, customer onboarding, data system
Owner	Responsible department/person
Deadline	Compliance date
Implementation Actions	Actions assigned
Status	Open / In Progress / Completed
Evidence	Updated policies, training completion, audit proof



7. Policy & Standard Management

This section defines how compliance-related policies, standards, procedures, and guidelines are created, approved, implemented, communicated, and maintained to ensure consistent and enforceable compliance practices across Orchestrate Global.

7.1 Policy Governance Objectives

- Ensure all internal documents reflect current regulatory, legal, and contractual obligations.
- Provide a structured and traceable document framework with clear ownership.
- Maintain version control, formal approval workflows, and accessibility for relevant teams.
- Prevent outdated, conflicting, or superseded policies from remaining in active use.

7.2 Policy Hierarchy

LEVEL	DOCUMENT TYPE	PURPOSE	APPROVAL AUTHORITY
Level 1	Policies	Mandatory principles defining “what must be done.”	CEO, CCO, CSCO
Level 2	Standards	Minimum mandatory requirements to uphold a policy.	CSCO or relevant Executive
Level 3	Procedures / SOPs	Step-by-step instructions explaining “how to do it.”	Department Heads



Level 4	Guidelines / Work Instructions	Best practices or advisory content (optional but recommended).	Functional Managers
---------	--------------------------------	--	---------------------

All Level 1 and Level 2 documents fall under the formal compliance governance of this Enterprise Compliance Policy and are binding.

7.3 Policy Lifecycle

PHASE	DESCRIPTION	RESPONSIBLE PARTY
1. Drafting	Policy prepared by Compliance or subject-matter experts based on risk assessments, regulatory changes, or audit findings.	Document Owner
2. Review	Cross-functional review by Legal, Risk, Security, Product, and HR as applicable.	CSCO + Stakeholders
3. Approval	Final sign-off via CEO and CCO (or delegated authority).	CEO / CCO
4. Publication	Uploaded to the Controlled Documents Repository with unique ID and version.	Compliance Office
5. Communication & Training	Mandatory acknowledgment or role-based training issued to impacted staff.	Compliance & HR
6. Periodic Review	Reviewed annually or triggered by regulatory change, incidents, or product updates.	CSCO



7. Retirement / Archiving

Superseded policies archived for 7 years and marked "Obsolete."

Compliance Office

7.4 Document Format & Metadata Requirements

Each policy or standard must include the following minimum metadata:

METADATA ELEMENT	REQUIREMENT
Document Title & ID	Clearly labeled (e.g., OG-ECP-001)
Version Number	Incremented with each substantive change
Owner & Approver	Named individuals/roles with contact info
Effective Date	Start date of enforceability
Next Review Date	Typically 12 months from effective date
Scope & Applicability	Clear statement of who/what it applies to
References	Linked laws, regulations, and internal policies
Change Log	Chronological list of revisions, authors, and summaries

Note: Templates for policy creation are maintained by the Compliance Office and must be used for all Level 1–2 documents.

7.5 Access & Distribution

- All policies are stored in a secure Controlled Documents Repository with role-based access.



- Read-only access is granted to all employees and relevant third parties under NDA.
- Critical compliance policies (e.g., AML/CFT Framework, Data Protection Policy, Sanctions Standard) must be accessible via the company intranet or GRC platform.
- Policy versions must never be circulated via email or uncontrolled file shares.

7.6 Non-Compliance with Policy

- Failure to follow mandatory policies may result in:
 - Disciplinary action (up to and including termination)
 - Suspension of system access
 - Contract termination (for third parties)
 - Regulatory reporting or legal proceedings
- All violations must be reported to the CSCO and logged in the Issues & Incidents Register.
- Temporary deviations require formal approval under Section 21: Exceptions & Dispensation Management.

8. Training, Awareness & Certification

This section establishes how Orchestrate Global ensures all employees, contractors, and relevant third parties have the knowledge and skills to comply with regulatory requirements, internal policies, and ethical standards.

8.1 Objectives

- Ensure personnel understand legal, regulatory, and policy obligations relevant to their role.
- Build a culture of compliance, integrity, data protection, security, and ethical conduct.
- Maintain auditable certification records to demonstrate training completion during regulatory reviews, audits, and license applications.



8.2 Training Governance

COMPONENT	REQUIREMENT
Oversight	Chief Security & Compliance Officer (CSCO) owns the training framework.
Development	Done jointly by Compliance, Risk, HR, Legal, Security, and relevant functional teams.
Delivery Methods	e-Learning, live workshops, webinars, tabletop exercises, onboarding sessions.
Tracking System	Centralized Learning Management System (LMS) with completion logs and reminders.
Frequency	At onboarding, annually, or when regulations/policies change.

8.3 Mandatory Training Categories

AUDIENCE	TRAINING MODULES	FREQUENCY
All Employees & Contractors	Code of Conduct, Ethics & Conflicts of Interest, Data Protection & Privacy, Information Security Basics, Anti-Bribery & Corruption	At onboarding + annually
Customer-Facing & Business Teams	Financial Crime Awareness, KYC/KYB Procedures, Complaints Handling, Fair Marketing	At onboarding + annually



Technology & Security Teams	Secure SDLC, API Compliance, Encryption Standards, Incident Response, Data Retention Rules	At onboarding + annually
Compliance, Legal & Risk Staff	Advanced AML/CFT, Sanctions Screening, Regulatory Reporting, Licensing Obligations	At onboarding + annually or role change
Senior Management & Board Members	Regulatory Responsibilities, Governance Duties, Oversight of Compliance Risk	At appointment + annually
Third-Party Service Providers	Data Handling, Confidentiality, Cyber & Compliance Awareness (if accessing systems/data)	Upon contract + renewal

8.4 Training Certification & Recordkeeping

- Training completion is tracked by the LMS or GRC Compliance Portal.
- Certificates of completion must be retained for minimum 5 years (or longer if required by regulation).
- Departments with overdue training receive reminders and are escalated to management after 15 days.
- Employees who fail to complete mandatory courses may face system access suspension or HR disciplinary action.



8.5 Role-Based Training Matrix

ROLE	REQUIRED COURSES	CERTIFICATION TYPES	RENEWAL
Compliance Analyst	AML/CFT Advanced, Sanctions, Regulatory Reporting	Internal Exam & LMS Certificate	Annual
Software Engineer	Secure Coding, API Security, Data Protection	LMS Certification	Annual
Finance & Treasury	Client Fund Safeguarding, Transaction Reporting, Fraud Awareness	LMS Certification	Annual
Sales & Partnerships	Marketing Compliance, Fair Pricing, Third-Party Risk	e-learning Certificate	Annual
Senior Executives	Board Oversight of Compliance, Risk Appetite, Ethics	Executive Workshop Certificate	Annual

8.6 Awareness & Culture Initiatives

- Compliance Awareness Week: Annual campaign with case studies, quizzes, regulatory updates.
- Compliance Bulletins & Alerts: Monthly email or portal update with changes in laws or policies.
- Anonymous Ethics Hotline & Whistleblowing Mechanism: Encourages reporting of misconduct without retaliation.
- Scenario-Based Workshops: Real-case simulations for AML breaches, data leaks, fraud attempts, etc.



9. Conduct, Ethics, Conflicts of Interest & Anti-Bribery/Anti-Corruption (ABAC)

This section establishes the ethical standards, conflict of interest controls, and anti-bribery/anti-corruption principles that all employees, executives, contractors, and third-party partners of Orchestrate Global must adhere to.

9.1 Purpose & Guiding Principles

- Promote a culture of integrity, transparency, accountability, and fairness.
- Prevent bribery, corruption, facilitation payments, conflicts of interest, fraud, or unethical behavior.
- Ensure all activities comply with global anti-corruption laws, contractual obligations, and ethical business conduct standards.
- Protect Orchestrate Global's reputation, licenses, and trust with regulators, partners, and customers.

9.2 Code of Conduct — Core Expectations

All employees and contractors must:

- Act with honesty and professionalism in all internal and external dealings.
- Avoid behavior that could damage the organization's reputation.
- Report known or suspected misconduct, fraud, bribery, or policy breaches.
- Comply with all policies, laws, and regulatory obligations — no exceptions.
- Protect confidential data, customer information, and company assets.



9.3 Conflict of Interest (COI) Management

A conflict of interest occurs when personal, financial, or other interests conflict (or appear to conflict) with the interests of Orchestrate Global.

TYPE OF CONFLICT	EXAMPLES
Personal / Financial	Employee holds shares in a competing or client organization.
Family / Relationship	Hiring or contracting a close relative without disclosure.
External Employment	Consulting or employment outside Orchestrate Global affecting independence.
Gifts & Hospitality	Accepting expensive gifts or travels from vendors/clients.

Conflict Management Requirements:

- All employees must complete a Conflict of Interest Disclosure Form at onboarding and annually.
- Conflicts must be declared to Compliance and line managers.
- Undeclared conflicts may result in disciplinary action or contract termination.
- Compliance maintains a COI Register.

9.4 Gifts, Hospitality & Entertainment Policy

RULE	DESCRIPTION
Acceptable Gifts	Low-value promotional items (e.g., branded notebook, pen) under an approved threshold.



Threshold	Monetary limit is defined (e.g., equivalent of USD 100 per person annually).
Prohibited	Cash, gift cards, personal discounts, luxury travel, or anything creating obligation.
Approval Needed	Any gift or hospitality exceeding the limit must be approved by Compliance or Manager.
Recording	All received or given gifts must be logged in the Gifts & Hospitality Register.

9.5 Anti-Bribery & Anti-Corruption (ABAC)

- Orchestrate Global enforces zero tolerance for bribery, kickbacks, facilitation payments, or improper influence of any kind.
- No employee or third party may offer, promise, give, solicit, or accept anything of value to influence a business decision.
- Donations, sponsorships, or lobbying must receive Compliance and Legal approval.

Prohibited Conduct Includes:

- Paying “speed money” to officials to accelerate approvals.
- Offering internships or business advantages in return for contracts.
- Providing luxury travel or accommodation to influence decisions.



9.6 Political Contributions & Lobbying

REQUIREMENT	DESCRIPTION
Corporate Donations	No political donations without Board approval and legal review.
Personal Political Activities	Allowed but must not be represented as company-sponsored.
Lobbying Activities	Must be transparent, lawful, and pre-approved by Legal & Compliance.

9.7 Whistleblowing & Speak-Up Protection

- Employees, contractors, and third parties may report concerns anonymously via designated email, form, or hotline.
- Retaliation against whistleblowers is strictly prohibited.
- All reports are investigated confidentially by Compliance or an independent investigator.
- Serious allegations may be reported to regulators or law enforcement if required.

9.8 Disciplinary Actions

Violations of this section may result in:

- Verbal/written warnings
- Suspension or dismissal
- Contract termination for vendors/partners
- Regulatory notification or legal action in severe cases



10. Data Protection & Privacy Compliance

This section defines how Orchestrate Global ensures the lawful, fair, secure, and transparent processing of personal and sensitive data across all jurisdictions in which it operates.

10.1 Objectives

- Protect personal, transactional, and confidential data processed by Orchestrate Global or its service providers.
- Ensure compliance with global data protection principles (lawfulness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability).
- Establish a framework for cross-border data transfers, data subject rights, data breach handling, and regulatory reporting.

10.2 Scope of Data Protection Policy

DATE TYPE	COVERED?	EXAMPLES
Personal Data	Yes	Names, email addresses, phone numbers, IP addresses, identity documents
Sensitive / Special Category Data	Yes	Government-issued IDs, biometric data, financial account information
Client Business Data	Yes	Merchant financial statements, KYB documents, contracts



Transaction Data	Yes	Payment details, wallet logs, FX conversion records
Employee Data	Yes	HR files, payroll, performance records
Anonymous / Aggregated Data	No (unless re-identifiable)	De-identified data used for analytics

10.3 Data Protection Principles

All personal data must be processed according to the following core principles:

PRINCIPLE	REQUIREMENT
Lawfulness, Fairness, Transparency	Data must be collected for lawful purposes; individuals informed via privacy notices
Purpose Limitation	Use data only for specified, explicit purposes
Data Minimization	Collect only the minimum required data
Accuracy	Keep data accurate and up to date
Storage Limitation	Retain data only as long as necessary (see Section 16)



Integrity & Confidentiality	Secure data through encryption, access control, and monitoring
Accountability	Demonstrate compliance with documented policies, logs, and assessments

10.4 Roles & Responsibilities

ROLE	RESPONSIBILITY
Chief Security & Compliance Officer (CSCO)	Global Data Protection Officer equivalent; oversees compliance and privacy governance
Data Protection Officer (if appointed by jurisdiction)	Local regulatory liaison for data inquiries and incident reporting
Engineering & Security Teams	Secure architecture, encryption, access management, logging, and breach detection
HR	Manage employee data per this policy
All Employees	Follow data policies and report suspected breaches



10.5 Data Subject Rights (DSR)

Individuals have the right to:

RIGHT	DESCRIPTION
Access	Obtain confirmation and a copy of personal data
Rectification	Correct inaccurate or incomplete data
Erasure (“Right to be Forgotten”)	Request deletion when no legal reason for retention exists
Restriction of Processing	Pause data use while accuracy or purpose is verified
Data Portability	Receive data in a structured, machine-readable format
Objection	Object to data processing for marketing or non-essential purposes

Process:

- Requests must be acknowledged within 5 business days, resolved within 30 days, unless extensions are legally permitted.
- All DSR activities must be logged in the Data Requests Register.



10.6 Cross-Border Data Transfers

- Cross-border transfers are permitted only where adequate protection measures exist.
- Acceptable transfer mechanisms include:
 - Binding Corporate Rules (BCR)
 - Standard contractual clauses in service contracts
 - Local regulatory authorization if required
- Data localization laws must be respected in applicable jurisdictions (e.g., customer and transaction data stored domestically).

10.7 Third-Party Data Processors

Before onboarding third-party data processors:

REQUIREMENT	DESCRIPTION
Due Diligence	Assess security controls, privacy certifications, and sovereignty risks
Contractual Clauses	Include confidentiality, breach notification, deletion, audit rights
Continuous Monitoring	Annual risk assessments, SLAs, monitoring of breaches or exposure

10.8 Data Breach Management

STEP	REQUIREMENT
Detection	Breaches must be identified through monitoring tools (SIEM, DLP systems) or employee reports



Containment & Investigation	Compliance, Security, and Legal coordinate investigation within 24 hours
Notification	If legally required, regulators notified within mandated timeframes (typically ≤72 hours)
Customer Communication	Impacted clients notified promptly if high risk to their rights or finances
Documentation	All breaches logged in the Incident & Breach Register with root cause analysis

10.9 Data Retention & Disposal

- Data is retained according to legal, regulatory, or contractual limitations (Section 16).
- Secure deletion methods include cryptographic wiping, secure API-based purging, and certified destruction for physical media.

11. Financial Crime & Sanctions Governance (Policy Interface)

This section defines how Orchestrate Global governs its obligations relating to financial crime prevention—including Anti-Money Laundering (AML), Counter-Financing of Terrorism (CFT), fraud, sanctions compliance, and suspicious activity reporting—through integration with this Enterprise Compliance Policy. It establishes governance oversight and formal interfaces with dedicated AML/CFT and Sanctions policies, which are maintained as Level 1 documents under this framework.



11.1 Purpose

- Ensure that Orchestrate Global does not facilitate money laundering, terrorist financing, fraud, sanctions violations, or other illicit financial flows.
- Embed robust financial crime controls into customer onboarding, transaction monitoring, product design, and third-party relationships.
- Define clear accountability, escalation pathways, and reporting obligations for financial crime risks.
- Ensure full alignment with international standards (e.g., FATF Recommendations), licensing conditions, and local financial crime laws.

11.2 Financial Crime Governance Structure

COMPONENT	RESPONSIBILITY
Board of Directors	Ultimate accountability for AML/CFT and sanctions compliance; approves risk appetite and receives quarterly reporting.
Chief Security & Compliance Officer (CSCO)	Enterprise policy owner; ensures integration of AML, sanctions, and fraud controls into all business functions.
Money Laundering Reporting Officer (MLRO) or Regional AML Officers	Receive internal suspicious activity reports (SARs); file external reports with Financial Intelligence Units (FIUs); serve as primary liaison with regulators on AML matters.
Sanctions Officer / Compliance Team	Maintain real-time sanctions screening protocols; manage match investigations; ensure blocked assets are frozen and reported.



Internal Audit

Conducts annual or risk-based independent assurance over AML/CFT and sanctions control effectiveness.

11.3 Scope of Financial Crime Controls

AREA	DESCRIPTION
Customer Due Diligence (KYC/KYB)	Identity verification of customers, beneficial owners, directors, and authorized signatories using reliable, independent sources.
Enhanced Due Diligence (EDD)	Applied to high-risk clients, including Politically Exposed Persons (PEPs), entities in High-Risk Jurisdictions, and complex ownership structures.
Transaction Monitoring	Automated and rules-based systems monitor real-time transaction patterns for structuring, layering, unusual geographies, or high-risk counterparties.
Sanctions & Watchlist Screening	Real-time screening of customers, counterparties, and transactions against global lists (e.g., OFAC, UN, EU, HMT, local regulators).
Fraud Prevention	Controls to detect and prevent account takeover, synthetic identities, chargebacks, and merchant fraud.
Suspicious Activity Reporting (SAR/STR)	Confirmed suspicious activity is escalated to the MLRO and, where legally required, filed with the relevant FIU.



Recordkeeping

Full retention of KYC files, transaction records, screening logs, and SAR documentation per Section 16.

11.4 Financial Crime Risk Assessment (FCRA)

- A comprehensive Financial Crime Risk Assessment is conducted annually or upon entry into new jurisdictions, launch of new products, or significant changes in customer risk profile.
- The FCRA evaluates risk across:
 - Customer types (e.g., fintechs, NGOs, corporates)
 - Geographic exposure (High-Risk Jurisdictions per FATF or local regulator)
 - Product/service risk (e.g., cross-border payments, FX, stablecoin conversion)
 - Delivery channels (API vs. manual)
- Outputs drive:
 - Risk-based customer onboarding thresholds
 - EDD triggers
 - Transaction monitoring rules
 - Resource allocation for compliance monitoring

11.5 Sanctions Compliance Requirements

REQUIREMENT	DESCRIPTION
List Management	Sanctions and watchlists are updated at least every 24 hours, or in real time when critical updates are issued.
Real-Time Screening	All customers and payment counterparties screenedpre-transaction; transactions screenedpost-transactionfor retroactive list additions.



Blocking & Rejecting	Any confirmed match with a sanctioned entity or individual must result in immediate transaction blocking and asset freezing.
Reporting	Blocked transactions must be reported to relevant authorities within mandated deadlines (e.g., 10 business days for OFAC; immediate for EU/UN).
Zero Tolerance	No exceptions or overrides are permitted for knowingly processing a transaction involving a sanctioned party.

11.6 Escalation & Reporting Mechanism

STAGE	ACTION
Level 1 – Frontline Alert	Transaction monitoring or screening system flags potential match or anomaly.
Level 2 – Initial Review	Compliance analyst performs triage; dismisses false positives or escalates confirmed risks.
Level 3 – MLRO/Sanctions Officer Review	Determines if SAR/STR is warranted or if funds must be blocked; documents rationale.
Level 4 – External Reporting	SAR/STR filed with FIU; sanctions breach reported to competent authority; RegTech logs preserved.



11.7 Interface with Enterprise Compliance Policy

- The AML/CFT Framework and Sanctions Standard are classified as Level 1 Policies under this Enterprise Compliance Policy (ECP).
- All financial crime controls are subject to:
 - Training requirements (Section 8)
 - Policy governance (Section 7)
 - Record retention (Section 16)
 - Monitoring and audit (Sections 17, 23)
 - Board reporting (Section 20)
- Any deviation from financial crime controls requires explicit Board-level risk acceptance and is not eligible for standard exception pathways (Section 21).

12. Third-Party & Outsourcing Compliance

This section defines how Orchestrate Global ensures that all third parties, service providers, agents, cloud platforms, vendors, and outsourced partners comply with applicable regulatory, contractual, security, and ethical requirements.

12.1 Purpose

- Ensure third-party relationships do not expose Orchestrate Global to regulatory, operational, financial, legal, cybersecurity, or reputational risks.
- Maintain oversight and accountability even when business activities are outsourced.
- Meet regulatory expectations for third-party risk management and outsourcing oversight.

12.2 Scope

This policy applies to all external parties engaged by Orchestrate Global, including:



THIRD PARTY TYPE	EXAMPLES
Critical Service Providers	Cloud infrastructure providers, transaction processors, banking partners, liquidity providers
Outsourced Operational Functions	Customer support, KYC screening vendors, compliance analytics partners
Technology Vendors	API services, cybersecurity firms, encryption key management platforms
Consultants & Contractors	Legal advisory, risk consultants, audit firms
Agents & Resellers	Payment agents, merchant onboarding partners

12.3 Third-Party Risk Management Lifecycle

PHASE	KEY ACTIVITIES	OWNER
1. Identification & Classification	Identify vendor need, define service scope, classify based on risk (critical/non-critical).	Business Unit / Procurement
2. Due Diligence & Risk Assessment	Assess financial stability, regulatory status, data protection, security, sanctions screening.	Compliance / Risk / Legal



3. Contracting & Legal Review	Contracts must include confidentiality, data protection, audit rights, SLAs, termination clauses.	Legal / Compliance
4. Onboarding & Integration	Provide training, assign relationship manager, ensure secure integration.	Business Unit
5. Ongoing Monitoring	Conduct periodic risk reviews, performance monitoring, compliance checks.	Compliance / Vendor Owner
6. Renewal or Exit	Reassess risk before renewal; ensure data return or secure destruction at termination.	Legal / Compliance / IT Security

12.4 Minimum Due Diligence Requirements

DUE DILIGENCE AREA	EVALUATION CRITERIA
Legal & Regulatory Status	Licensed/registered where applicable; no regulatory sanctions
Financial Stability	Audited financial statements; no insolvency risk
Information Security	ISO 27001 alignment, encryption, access controls, breach history
Data Protection	GDPR-equivalent standards, data residency compliance, DPIA if required



Sanctions & Adverse Media Screening	Screening of ownership, directors, and beneficial owners
Operational Resilience	Disaster recovery plans, service continuity measures
Sub-Outsourcing Controls	Disclosure of subcontractors; must meet same obligations

12.5 Contractual Compliance Clauses (Minimum Requirements)

Each third-party contract must include:

- Confidentiality, IP protection, and data ownership clauses
- Compliance with applicable laws, privacy rules, and financial crime regulations
- Right-to-audit provisions for Orchestrate Global or its regulators
- Incident notification timelines (e.g., within 24 hours for data or regulatory breaches)
- Data retention, deletion, and return clauses upon termination
- Termination rights for compliance violations or regulatory instructions

12.6 Ongoing Monitoring & Performance Reviews

MONITORING TYPE	FREQUENCY	PERFORMED BY
Compliance Review	Annually or risk-triggered	Compliance / Legal
Security Audit (External or Internal)	Annually	IT Security
Service Level Performance Check	Monthly / Quarterly	Vendor Owner



Financial Health Check	Annually	Finance / Risk
Onsite Assessment (Critical Providers)	As required	Compliance / Risk

12.7 Exit & Termination

Upon termination of services, the vendor must:

- Securely return all Orchestrate Global data
- Confirm destruction of retained data (Certificate of Destruction)
- Support transition to a new provider if required
- Continue confidentiality obligations post-termination

12.8 Accountability

ROLE	RESPONSIBILITIES
Chief Commercial Officer (Kevin Kegera)	Ensures commercial partnerships adhere to compliance obligations.
CSCO (Oleksii)	Oversees third-party compliance framework and sanction screening obligations.
Legal Team	Ensures contractual compliance, liability protections, SLA enforcement.
Procurement / Vendor Manager	Coordinates due diligence, onboarding, ongoing monitoring.



IT Security

Validates technical security, encryption, and access controls.

13. Product, Marketing & Customer Communications Compliance

This section ensures that all products, features, marketing materials, and customer-facing communications are lawful, accurate, non-misleading, and aligned with regulatory standards and ethical expectations across all jurisdictions.

13.1 Purpose

- Prevent unfair, deceptive, or misleading practices in product development and marketing.
- Ensure clear, accurate, and compliant communication with clients, partners, regulators, and the public.
- Embed compliance checks into the lifecycle of every product and communication.

13.2 Scope

This section applies to:

CATEGORY	EXAMPLES
Products & Features	APIs for FX, treasury management tools, payment gateways, digital wallets, fiat<>stablecoin conversion
Customer Communications	Website content, platform dashboards, emails, pricing pages, contracts, FAQs



Marketing & Sales Materials	Brochures, social media posts, investor decks, paid ads, pitch materials
Disclosures & Terms	Service agreements, consent forms, risk warnings, fee disclosures

13.3 Product Compliance Lifecycle

Compliance must be embedded in all product development phases:

PHASE	COMPLIANCE REQUIREMENT	OWNER
1. Concept & Feasibility	Regulatory impact assessment, licensing requirements, cross-border considerations	Product + Compliance
2. Design & Development	Secure architecture, data privacy by design, AML/CFT requirements, audit logging	Product + Tech + Compliance
3. Pre-Launch Review	Compliance sign-off, legal review of terms, risk evaluation	Compliance + Legal
4. Go-Live Approval	All controls in place (monitoring, reporting, customer disclosures)	CSCO / CRO / Legal
5. Post-Launch Monitoring	Customer feedback, regulatory updates, incident tracking	Product + Compliance



6. Product
Retirement

Customer notification, contractual closure, data
retention/deletion

Product + Legal +
Compliance

13.4 Marketing & Communication Compliance Rules

RULE	DESCRIPTION
Truthful & Non-Misleading	All claims must be accurate, supported by evidence, and avoid exaggeration
Transparent Pricing	Fees, FX rates, transaction charges, and settlement times must be clearly disclosed
No Unlicensed Claims	Do not state regulatory approvals that are not yet granted
Risk Disclosures	Required for financial products (e.g., FX volatility, blockchain risks, transaction delays)
Language Standards	Clear, professional, culturally appropriate — avoid discriminatory or unethical wording
Comparisons	Must be factual and backed by data; avoid defamation of competitors



13.5 Approval Workflow – Marketing Materials

STEP	REQUIREMENT	OWNER
Draft Creation	Prepared by marketing/sales teams	Marketing
Initial Review	Checked for accuracy and branding	Marketing Lead
Compliance Review	Verified for legal accuracy, no misleading statements, correct risk disclosures	Compliance
Legal Review (if required)	For contracts, disclaimers, new jurisdictions	Legal
Final Sign-off	CSCO or delegated officer approves	Compliance

No advertising or marketing content may be published without documented approval.

13.6 Customer-Facing Terms & Agreements

- All customer agreements (MSAs, API Terms of Service, Merchant Agreements) must be reviewed and approved by Legal & Compliance.
- Agreements must contain:
 - Service description and limitations
 - Fees, chargebacks, settlement timelines
 - Data usage, confidentiality, liability limitations
 - Termination rights and jurisdiction of governing law



13.7 Recordkeeping Requirements

- Final approved versions of all marketing communications, campaigns, and product documentation must be stored for a minimum of 5 years.
- Compliance must retain approval evidence, disclaimers, and risk assessment documents.

13.8 Monitoring & Testing

CONTROL TYPE	ACTIVITY	FREQUENCY
Website Monitoring	Ensure live site content matches approved versions	Monthly
Sales Call Audits	Random sampling of sales calls or demos for compliance	Quarterly
Social Media Checks	Ensure posts comply with communication policy	Ongoing
Customer Complaints Review	Identify marketing misrepresentation or misinformation issues	Continuous

14. Technology, Security & Operational Resilience Compliance

This section defines the compliance expectations for technology operations, cybersecurity, infrastructure management, and operational resilience to ensure confidentiality, integrity, availability, and regulatory compliance of systems supporting Orchestrate Global's services.



14.1 Objectives

- Ensure that all systems, networks, APIs, and data centers meet regulatory, contractual, and industry security requirements.
- Maintain resilience against cyberattacks, system failures, disasters, and operational disruptions.
- Ensure secure development, testing, deployment, and ongoing monitoring of technology assets.
- Align technology operations with compliance, licensing, data protection, and financial service obligations.

14.2 Scope

DOMAIN	INCLUDED COMPONENTS
Infrastructure	Cloud platforms, data centers, disaster recovery sites, network architecture
Application Layer	Payment gateway, orchestration APIs, admin consoles, FX engines
Data & Security	Encryption, secure storage, access management, key management
Operational Resilience	Incident response, service availability, backup & recovery
Development & Deployment	Secure SDLC, DevSecOps, change management



14.3 Technology Compliance Control Areas

CONTROL AREA	MANDATORY REQUIREMENTS
Access Control	Role-based access, least privilege, MFA for privileged accounts, central IAM system
Encryption	Data in transit and at rest must be encrypted using strong cryptographic standards (e.g., AES-256, TLS 1.3)
Logging & Monitoring	Centralized log collection (SIEM), real-time alerting of anomalous or privileged activities
Secure Development Lifecycle (SDLC)	Code review, dependency scanning, API security testing, vulnerability management integrated into CI/CD
Change Management	All system changes require documented approval, testing evidence, rollback plans, and post-deployment validation
Incident Response	24/7 incident detection and response capability; documented playbooks; mandatory reporting to Compliance if regulatory or customer impact

14.4 Operational Resilience Requirements

COMPONENT	REQUIREMENT
Business Continuity	Systems supporting core services must align with the Business Continuity Plan (BCP), tested annually



Disaster Recovery (DR)	DR sites with Recovery Point Objective (RPO) ≤15 minutes and Recovery Time Objective (RTO) ≤4 hours for critical applications
Redundancy & Failover	Multi-region cloud deployment, load balancing, automated failover capabilities
Backups	Encrypted backups of databases and logs, tested quarterly for integrity and restorability

14.5 Incident & Breach Management Interface

SEVERITY	DESCRIPTION	ESCALATION
Low	Minor disruption, no data exposure	IT Ops
Medium	System errors impacting small customer group	IT + Compliance
High	Service outage, financial loss, or suspected unauthorized access	CSCO + CISO + ExCo
Critical	Confirmed data breach, regulatory impact, or full regional outage	CEO + Board + Regulators (within required timeframes)

All technology-related incidents with compliance implications must be logged in the central Incidents & Breaches Register and linked to Section 18.



14.6 Vendor Technology Compliance

- Technology vendors must meet minimum security requirements as defined in Section 12 (Third-Party & Outsourcing Compliance).
- Cloud providers must support encryption, audit logging, multi-region redundancy, and contractual right-to-audit provisions.
- Penetration testing must be conducted annually or after major architectural changes, with findings remediated based on risk severity.

14.7 Secure API & Platform Compliance Requirements

REQUIREMENT	DESCRIPTION
Authentication & Authorization	OAuth 2.0 or equivalent token-based access; no shared static credentials
Input Validation	All endpoints must sanitize inputs to prevent injection attacks (SQLi, XSS, CSRF)
Rate Limiting & Abuse Prevention	API throttling to control traffic spikes, DDoS attempts, and brute-force attacks
Data Segmentation	Client data must be logically segregated in multi-tenant architecture using robust tenant isolation
Audit Logging	Every API request must be logged with: timestamp, authenticated user ID, source IP, endpoint, payload hash, and response status



14.8 Evidence & Certification

- System architecture diagrams, network maps, penetration test reports, vulnerability assessments, and compliance attestations must be retained for a minimum 5 years.
- Certifications (e.g., ISO 27001, SOC 2 Type II, or jurisdictional equivalents) must be maintained and made available to regulators and banking partners under NDA.
- Cryptographic standards must comply with globally accepted practices (e.g., NIST, ETSI) and be reviewed annually by the CSCO and CTO.

15. Model & Algorithmic Risk Compliance

This section governs the responsible use, development, deployment, and monitoring of models and algorithms—including AI/ML systems—used in risk scoring, fraud detection, pricing, FX routing, credit risk assessment, sanctions screening, and operational automation.

15.1 Purpose

- Ensure all algorithmic and machine-learning models are accurate, explainable, unbiased, secure, and compliant with regulatory expectations.
- Prevent discriminatory outputs, incorrect decisioning, or systemic model failures that could impact customers, financial integrity, or regulatory standing.
- Establish a structured framework for model development, validation, documentation, deployment, monitoring, and retirement.

15.2 Scope

This policy applies to all models that influence:



CATEGORY	EXAMPLES
Financial Risk	FX pricing algorithms, liquidity routing engines
Fraud & AML	Machine-learning models for transaction anomalies, behavioral analytics, sanctions screening
Credit & Scoring	Merchant eligibility scoring, onboarding risk scores
Operational Automation	Automated onboarding decisions, rule-based API approvals/rejections
AI/ML Systems	Neural networks, predictive classifiers, natural language processing models

Excluded: Static, non-adaptive business rules not based on statistical or machine-learning techniques (e.g., fixed fee calculators).

15.3 Model Risk Management (MRM) Lifecycle

PHASE	KEY ACTIONS	OWNER
1. Design & Development	Define objectives, data sources, fairness constraints, regulatory boundaries	Data Science / Product



2. Validation & Testing	Back-testing, bias detection, accuracy metrics, stress testing; independent pre-deployment review	Independent Validator / Compliance
3. Documentation	Create a Model Card: purpose, methodology, inputs, thresholds, known limitations	Model Owner
4. Deployment & Change Control	Approved via Change Management Board; version-controlled; rollback plan in place	Technology / DevOps
5. Monitoring & Performance Review	Track accuracy, false positives/negatives, concept drift, fairness metrics, downtime	Data Science + Compliance
6. Retirement	Decommission outdated models; archive documentation and outputs securely	Model Owner + Compliance

15.4 Model Documentation Standards

Every model must have a Model Governance File containing:

- Model purpose, type, and version
- Data sources and preprocessing logic
- Algorithm(s) used (e.g., XGBoost, logistic regression, transformer)
- Validation results (accuracy, precision, recall, AUC)
- Business rules, decision thresholds, and override mechanisms
- Bias and fairness assessment (e.g., disparate impact analysis)
- Regulatory interpretation or limitations (e.g., “not used for final credit denial”)
- Change log and version history
- Model owner and key stakeholders



All documentation must be stored in the Controlled Model Repository with access restricted to authorized roles.

15.5 Fairness, Ethics & Bias Controls

REQUIREMENT	DESCRIPTION
No Discrimination	Models must not intentionally or unintentionally discriminate based on protected attributes (e.g., nationality, gender, ethnicity).
Bias Detection	Training and inference data must be tested for representational and measurement bias; skewed datasets must be corrected.
Explainability	Models used in customer-impacting decisions (e.g., onboarding rejection, transaction blocking) must support post-hoc explanations (e.g., SHAP values, rule extraction).
Transparency	Customers must receive clear, non-technical statements when automated decisions materially affect them (e.g., "Your application was declined based on automated risk scoring").

15.6 Security & Data Integrity

- Training and production data must be pseudonymized or anonymized where feasible.
- Model training environments must be isolated and secured against data poisoning, model inversion, or adversarial attacks.
- All API calls and automated decisions must be logged with:
 - Timestamp
 - Input features (hashed or masked if sensitive)
 - Output score/decision
 - Decision rationale (if explainable)



- User or system identifier

15.7 Validation & Assurance

VALIDATION TYPE	DESCRIPTION	FREQUENCY
Pre-Deployment Validation	Independent testing for accuracy, bias, robustness, and regulatory alignment	Before go-live
Ongoing Monitoring	Track KPIs: false positive rate, prediction drift, latency, throughput	Daily/Weekly
Periodic Review	Full revalidation of performance, data quality, and fairness	At least annually
Regulatory or Audit Review	Respond to inquiries from regulators, auditors, or banking partners	As required

15.8 Accountability Matrix

ROLE	RESPONSIBILITY
Model Owner (Product/Data Science)	Develops model; ensures business logic validity and performance
Compliance & Legal	Assess regulatory impact, fairness, explainability, and customer rights



Chief Technology Officer (CTO)	Ensures secure deployment, logging, versioning, and system integration
Chief Security & Compliance Officer (CSCO)	Approves high-risk models; oversees ongoing monitoring and governance
Internal Audit	Conducts periodic independent reviews of model governance, documentation, and outcomes

Note: Models classified as High or Critical Risk (e.g., those impacting licensing, sanctions, or customer onboarding) require CSCO and ExCo approval before deployment.

16. Records Management & Retention

This section sets out the requirements for the creation, classification, retention, protection, and secure disposal of records to ensure legal, regulatory, and business obligations are met across all jurisdictions.

16.1 Purpose

- Ensure all records—digital or physical—are stored, retained, and disposed of in accordance with legal, regulatory, contractual, and operational requirements.
- Enable transparency, audit readiness, legal defensibility, and regulatory compliance.
- Minimize data retention risks by securely disposing of outdated records when no longer needed.



16.2 Scope

Applies to all records generated or received by Orchestrate Global, including:

RECORD TYPE	EXAMPLES
Customer & Transaction Records	KYC/KYB documents, transaction logs, FX trades, settlement files
Financial Records	General ledger, balance sheets, statements, invoices
Compliance & Legal Records	AML reports, sanctions logs, regulatory filings, licenses
Data & System Logs	API logs, access logs, audit trails, incident reports
HR & Employee Data	Employment agreements, payroll, performance reviews
Contracts & Agreements	Vendor contracts, banking agreements, NDAs
Model & Algorithm Documentation	Model cards, validation reports, testing logs



16.3 Record Retention Schedule

RECORD CATEGORY	MINIMUM RETENTION PERIOD	NOTES
KYC/KYB Documents & Customer Files	5–10 years after relationship ends	Subject to financial crime regulations
Transaction Records & Payment Data	5–7 years	Must support regulatory audits and investigations
Suspicious Activity Reports (SAR/STR)	5–10 years	Never disclosed to customer per law
Sanctions Screening Logs	5 years	Required under international sanctions regulations
Contracts & Vendor Agreements	Active duration + 7 years	Includes termination records
Board & Committee Minutes	Permanently	Regulatory and legal requirement
Employee HR Records	Employment duration + 6 years	Longer if mandated by local law
System Access & Security Logs	1–2 years minimum	Longer if involved in an incident
Incident/Breach Reports	7 years	Must include root cause and corrective actions



Note: If multiple regulations apply, retain for the longest required period.

16.4 Record Storage & Security

- Records must be stored in secure, access-controlled repositories (e.g., Document Management System, encrypted databases, secure cloud vaults).
- Access must follow the principle of least privilege and be logged for auditability.
- Physical records must be stored in locked cabinets or accredited archive facilities with environmental controls.
- Backup copies of critical records must be maintained in geographically separate, encrypted locations.

16.5 Secure Disposal & Destruction

RECORD TYPE	DESTRUCTION METHOD
Paper Records	Cross-cut shredding or certified destruction vendor with certificate
Digital Files	Cryptographic wiping, secure erasure software, or API-triggered logical purge
Hardware (e.g., disks, SSDs)	Degaussing, physical shredding, or certified e-waste destruction with audit trail

All destruction activities must be pre-approved and logged by Compliance and IT Security. Destruction is prohibited if a legal or regulatory hold is active.

16.6 Litigation & Regulatory Holds

- When litigation, audit, or regulatory investigation is anticipated or underway, the Legal Department issues a Legal Hold Notice.



- Upon receipt of a legal hold:
 - All related records must not be deleted or altered.
 - Relevant employees must acknowledge the hold.
 - The hold remains in effect until formally released in writing by Legal.

16.7 Responsibilities

ROLE	RESPONSIBILITIES
Chief Security & Compliance Officer (CSCO)	Ensures retention schedules meet global regulatory obligations
Legal Department	Issues legal holds; advises on jurisdiction-specific retention laws
IT Security & Infrastructure Teams	Implements technical controls for secure storage, backup, and destruction
HR	Manages employee record lifecycle and archival
All Employees	Adhere to retention/disposal procedures; report violations

17. Monitoring, Testing & Quality Assurance



This section defines how Orchestrate Global continuously evaluates the effectiveness of its compliance framework, internal controls, risk management processes, and adherence to legal and regulatory obligations.

17.1 Objectives

- Detect control weaknesses, policy breaches, or emerging risks before they escalate into regulatory issues.
- Provide assurance to management, auditors, and regulators that controls operate as designed and remain effective.
- Ensure that identified deficiencies are promptly corrected with documented remediation and verified closure.

17.2 Three Layers of Compliance Assurance

ASSURANCE LEVEL	DESCRIPTION	PERFORMED BY
1st Line – Business Self-Monitoring	Process owners monitor their own controls and report incidents or control gaps.	Business Units / Operations
2nd Line – Compliance Monitoring & Testing	Structured, independent testing of controls (e.g., KYC file reviews, sanctions alert validation, policy adherence checks).	Compliance / Risk Teams
3rd Line – Internal Audit (Independent)	Objective, risk-based audits of compliance frameworks, including AML, data privacy, cybersecurity, and third-party risk.	Internal Audit / External Auditors

17.3 Compliance Monitoring Activities



MONITORING ACTIVITY	DESCRIPTION	FREQUENCY
KYC/KYB File Reviews	Sample-based validation of completeness, accuracy, and timeliness of onboarding documentation.	Monthly
Sanctions Alert Review	Review of sanctions screening alerts for timely escalation, resolution, and false-positive tuning.	Daily
Transaction Monitoring Quality Checks	Evaluate performance of transaction monitoring rules (e.g., false positives/negatives, coverage gaps).	Weekly
Policy Adherence Reviews	Spot-check adherence to internal procedures (e.g., approvals, sign-offs, training completion).	Quarterly
Third-Party Compliance Audits	Assess vendor adherence to contractual, security, and regulatory obligations.	Annually (or risk-triggered)

17.4 Formal Testing Program (2nd Line)

Compliance conducts structured, evidence-based testing using the following phases:

PHASE	ACTIVITY
Planning	Identify high-risk areas using risk assessments; define scope, methodology, and sampling criteria.
Fieldwork	Collect evidence (e.g., system logs, customer files, policy attestations); conduct interviews and process walkthroughs.



Evaluation	Compare control design and operating effectiveness against policy and regulatory requirements.
Reporting	Issue findings with severity rating, root cause, and actionable recommendations.
Follow-Up	Track remediation until verified closure; escalate overdue actions to RCC or ExCo as needed.

17.5 Quality Assurance (QA) Framework

- The Compliance function is subject to internal quality reviews to ensure accuracy, consistency, and independence.
- QA activities include:
 - Peer reviews of monitoring reports and findings
 - Documentation completeness checks
 - Accuracy validation of regulatory filings and risk metrics
- Independent external or internal audit reviews of the Compliance function are conducted at least every 2–3 years.

17.6 Issues Classification & Severity

SEVERITY LEVEL	DESCRIPTION	ESCALATION PATH
Low	Minor documentation gap or isolated procedural lapse; no regulatory or financial impact.	Line Manager
Medium	Repeated or systemic weakness in a non-critical control; limited operational impact.	Compliance Officer
High	Significant control failure affecting customer data, transactions, or reporting; potential regulatory finding.	CSCO + Risk & Compliance Committee (RCC)



Critical

Confirmed regulatory breach, data exposure, sanctions violation, or criminal exposure.

CEO, Board, and Regulators (as required)

17.7 Remediation & Action Tracking

- All issues are recorded in the Compliance Issues Register with the following fields:
 - Issue description
 - Severity rating
 - Root cause
 - Action owner
 - Remediation plan
 - Target completion date
 - Status (Open / In Progress / Closed)
- Remediation progress is reviewed weekly by Compliance and reported to the Risk & Compliance Committee monthly.
- Unresolved Critical or High issues are escalated to the Executive Committee and Board until closed.

18. Issues, Incidents & Investigations

This section establishes the framework for identifying, reporting, managing, escalating, investigating, and remediating compliance-related issues and incidents at Orchestrate Global.

18.1 Purpose

- Ensure all compliance breaches, control failures, data/privacy incidents, regulatory violations, and ethical misconduct are logged, investigated, and resolved.



- Provide a consistent approach to root cause analysis, accountability, and remediation.
- Ensure timely regulatory reporting where required by law, licensing, or contractual obligations.

18.2 Definitions

TERM	DESCRIPTION
Issue	A control weakness, non-compliance with policy, documentation gap, or audit finding.
Incident	A specific event causing disruption, risk, or breach (e.g., data leak, transaction error).
Breach	Confirmed violation of legal, regulatory, contractual, or internal policy requirements.
Investigation	Formal review to determine cause, responsibility, and required actions.

18.3 Issue & Incident Reporting Channels

Employees, contractors, and third parties may report issues via:

- Compliance Incident Reporting System (Internal Portal)
- Email: compliance@orchestrate.global
- Whistleblowing / Anonymous Hotline (for ethical or legal concerns)
- Escalation to Line Managers or CSCO directly

All employees are obligated to report potential or actual violations immediately.

18.4 Incident Classification & Initial Response



INCIDENT LEVEL	EXAMPLE	RESPONSE TIME	ESCALATION TO
Low	Minor documentation error, delayed filing	Within 5 business days	Line Manager
Medium	Repeated KYC gaps, failed internal audit test	Within 48 hours	Compliance Officer
High	System outage, suspicious activity, internal data leak	Within 24 hours	CSCO + Legal
Critical	Sanctions breach, major fraud, regulatory inquiry or notice	Immediate (≤12 hours)	CEO, CSCO, Legal, Board

18.5 Incident Management Workflow

STAGE	ACTION	OWNER
1. Detection & Logging	Issue recorded in Compliance Issues & Incident Register with timestamp.	Employee / Manager
2. Classification	Severity assigned based on impact and risk.	Compliance Officer
3. Containment	Limit impact (e.g., freeze account, block transactions, isolate systems).	Operations / Security
4. Investigation	Collect evidence; perform root cause analysis; determine breach source.	Compliance + Legal + IT (if technical)



5. Remediation Plan	Assign corrective actions, deadlines, responsible owners.	CSCO
6. Reporting	Internal report to ExCo/Board; external reporting to regulator if required.	CSCO / MLRO / Legal
7. Closure	Verified completion of corrective actions with approval.	Compliance
8. Lessons Learned	Document findings; update policies/training if needed.	Compliance + Risk

18.6 Root Cause Analysis (RCA)

Investigations must determine underlying causes, not just symptoms. RCA must address:

- What failed? (Process, control, system, human error)
- Why did it fail? (Training gap, flawed design, negligence, vendor failure)
- How to prevent recurrence? (Policy update, retraining, automation, architectural change)

18.7 Regulatory & Law Enforcement Notifications

Regulators must be notified when required by law or licensing conditions, such as:



TRIGGER EVENT	NOTIFICATION REQUIREMENT
Data breach affecting personal data	Notify data protection authority within legal timeframe (typically ≤72 hours).
AML / Suspicious activity	File SAR/STR with FIU promptly (timelines vary by jurisdiction).
Sanctions breach	Freeze transaction; notify competent authority immediately.
Material operational outage	Notify supervisory authority and banking partners without delay.

18.8 Confidentiality & Evidence Handling

- All investigation documents must be stored securely in a controlled folder accessible only to Compliance, Legal, and authorized investigators.
- Evidence must be preserved in original format; audit trails must not be altered.
- Employees involved are prohibited from destroying, modifying, or sharing investigation details externally.

18.9 Employee Protections

- Anyone who reports a concern in good faith is protected from retaliation.
- Retaliation may result in disciplinary action or termination.
- Whistleblower identities are kept confidential unless disclosure is required by law.

19. Metrics, KRIs/KPIs & Management Reporting



This section defines how Orchestrate Global tracks compliance performance using measurable indicators—Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs)—and ensures timely, accurate reporting of these metrics to senior management, executive committees, and the Board.

19.1 Purpose

- Provide transparent, data-driven visibility into compliance health, emerging risks, and control effectiveness.
- Enable proactive intervention before risks escalate into regulatory breaches or operational failures.
- Support regulatory, audit, and stakeholder assurance through reliable, consistent metrics.
- Align operational outcomes with the organization's Risk Appetite Statement and strategic objectives.

19.2 Key Compliance Metrics (KRIs & KPIs)

DOMAIN	EXAMPLE KRIs/ KPIs	THRESHOLD/ ESCALATION TRIGGER
KYC/KYB Compliance	% customer files complete % periodic reviews overdue	>5% overdue → Escalate to CSCO
Sanctions & Screening	Unresolved alerts >24h False positive rate	Any open alert >24h → High risk
Transaction Monitoring	SAR/STR filed per quarter % alerts unresolved after 30 days	>10% unresolved → Remediation plan required



Training & Awareness	% staff completing mandatory training on time	<95% completion → HR/Compliance intervention
Policy Breaches	Number of policy violations Repeat offenders	≥3 repeat breaches/quarter → ExCo review
Third-Party Compliance	% critical vendors with overdue audits Average vendor risk rating	Critical vendor audit overdue → RCC escalation
Data Protection	Data subject requests resolved on time Number of reportable breaches	Any breach → Immediate incident protocol
Incident Management	Avg. time to close High/Critical issues	>30 days for High issues → CEO notification

19.3 Reporting Cadence & Audience

REPORT TYPE	FREQUENCY	PREPARED BY	PRIMARY AUDIENCE
Daily Operational Dashboards	Daily	Compliance / Tech Ops	Department Heads
Monthly Compliance Report	Monthly	Compliance Office	Executive Committee (ExCo)
Quarterly Board Compliance Report	Quarterly	CSCO	Board of Directors / Audit & Risk Committee



Regulatory Filings & Incident Summaries	As required	MLRO / CSCO / Legal	Regulators, Banking Partners
Annual Compliance Effectiveness Report	Annually	CSCO + Internal Audit	Board

19.4 Quarterly Board Compliance Report – Core Components

Each quarterly report to the Board must include:

- Executive Summary: Material developments, breaches, or regulatory shifts
- Compliance KRI/KPI Dashboard: Visual status (Green/Amber/Red) with trend analysis
- Incident Log Summary: High/Critical incidents, root causes, remediation status
- Regulatory Change Impact: New laws, licensing updates, jurisdictional risks
- Audit & Testing Outcomes: Internal/external findings and closure rates
- Financial Crime Metrics: SARs filed, sanctions screening efficacy, fraud losses
- Third-Party Risk Overview: Critical vendor status, due diligence gaps
- Forward-Looking Risks: Emerging threats, control enhancements, resource needs

19.5 KRI/KPI Dashboard Example (Simplified)

METRIC	TARGET	CURRENT	STATUS
Training Completion Rate	≥95%	94%	⚠ Monitoring
Open Sanctions Alerts (>24h)	0	2	! Action Required
KYC Periodic Review Overdue	≤5%	7%	! Escalated
Critical Issues Closed in 30 Days	≥90%	85%	⚠ Remediation Plan Active



Data Breaches (QTD)

0

0

✓ Compliant

19.6 Escalation Protocol for Metric Threshold Breaches

RISK LEVEL	CONDITION	ESCALATION PATH
Level 1 – Minor Deviation	KPI variance <10%	Business Owner → Line Manager
Level 2 – Threshold Breach	KPI variance ≥10%; no immediate harm	Compliance Officer → CSCO
Level 3 – Sustained Non-Conformance	Repeated breaches over 2 cycles	CSCO → Risk & Compliance Committee (RCC)
Level 4 – Systemic Failure	Regulatory exposure, financial loss, or reputational harm	CSCO → CEO → Board

19.7 Data Integrity & Auditability

- All metrics must be generated from source systems (e.g., GRC platform, LMS, SIEM, transaction monitoring engine).
- Reports must include metadata: data source, extraction date, preparer, reviewer, and approval signature.
- Historical metric data must be retained for a minimum 7 years in the Controlled Documents Repository for audit and regulatory purposes.



20. Board & Executive Reporting

This section describes the structure, frequency, and content of compliance-related reports delivered to the Board of Directors and Executive Committee (ExCo) to ensure effective oversight of regulatory, financial crime, data protection, and operational compliance risks.

20.1 Objectives of Executive & Board Reporting

- Enable informed decision-making on compliance, ethics, and risk exposure.
- Provide visibility into high-risk issues, breaches, regulatory developments, and remediation progress.
- Ensure the Board meets its fiduciary and regulatory oversight responsibilities.
- Demonstrate proactive governance to regulators, auditors, and strategic partners.

20.2 Reporting Structure

REPORT TYPE	PREPARED BY	SUBMITTED TO	FREQUENCY
Monthly Compliance Operations Report	Compliance Team	Executive Committee (ExCo)	Monthly
Quarterly Compliance & Risk Report	Chief Security & Compliance Officer (CSCO)	Board of Directors / Audit & Risk Committee	Quarterly
Regulatory Incident Report	CSCO / MLRO	CEO, ExCo, Board (if severe)	Within 24–72 hours of incident



Annual Compliance Effectiveness Report	CSCO, Internal Audit	Board	Annually
Ad-hoc Briefings	CSCO / Legal / CCO	Board / CEO	As required (e.g., new regulation, major enforcement action)

20.3 Minimum Contents – Quarterly Compliance & Risk Report

SECTION	DESCRIPTION
Executive Summary	Key developments, emerging risks, material breaches, significant trends.
Regulatory Environment Update	Upcoming laws, licensing conditions, regulator communications.
Compliance Dashboard (Metrics)	KRIs/KPIs on AML, sanctions, KYC reviews, incidents, training, vendor compliance.
Incidents & Breaches	Summary of high/critical incidents, root causes, corrective actions.
Audit & Monitoring Findings	Internal audit results, thematic reviews, outstanding remediation tasks.
Licensing & Registrations Status	Status of license renewals/approvals across jurisdictions.



Financial Crime Report	SAR/STR statistics, sanctions screening performance, fraud cases.
Data Protection & Privacy	Breach notifications, data subject requests, cross-border transfer updates.
Third-Party Compliance	Vendor risk updates, due diligence results, critical failures.
Risk & Controls Outlook	High-risk areas, control improvements, required board decisions.

20.4 Escalation Triggers to Board / Regulators

ESCALATION TRIGGER	ACTION
Confirmed sanctions breach	Immediate escalation to CEO, Board, and regulator (where required).
Major data breach involving personal or payment data	Notify the regulator within the mandated timeframe and inform the Board.
Regulatory enforcement notice / investigation	Board must be informed within 24 hours.
Failure to meet licensing conditions	Immediate CEO & Board review; remediation plan required.
Reputational risk or media exposure	CEO and CSCO to brief Board promptly.



20.5 Board Responsibilities (Compliance Oversight)

- Approve the Enterprise Compliance Policy and Risk Appetite Statement.
- Review quarterly compliance reports and challenge management where needed.
- Ensure adequate resourcing of compliance, risk, and security teams.
- Monitor remediation of critical issues and regulatory requests.
- Support a tone-from-the-top culture of integrity and accountability.

21. Exceptions & Dispensation Management

This section outlines how Orchestrate Global manages exceptions or dispensations where adherence to a policy, standard, control, or regulatory requirement is temporarily impractical, while ensuring risks are documented, approved, mitigated, and time-bound.

21.1 Purpose

- Provide a formal and controlled process for approving temporary deviations from established policies or standards.
- Ensure all exceptions are risk assessed, approved by the appropriate authority, remediated within a defined timeframe, and monitored to closure.
- Prevent unapproved or undocumented deviations that could create regulatory, operational, legal, or security risks.



21.2 When an Exception May Be Requested

Exceptions may be considered in the following circumstances:

SITUATION	EXAMPLE
Operational Limitation	A newly onboarded market or vendor cannot fully meet encryption or documentation requirements immediately.
Technology Constraint	The legacy system cannot support mandatory logging until upgraded.
Regulatory Transition Period	New regulation enforced with insufficient implementation time.
Emergency / Incident Response	Temporary bypass of normal approval processes due to outage or cyber incident (must be documented post-event).

Note: Exceptions are not allowed for core financial crime controls (AML, sanctions), fraud prevention, or knowingly violating law.

21.3 Exception Request Workflow

STEP	ACTION	RESPONSIBLE
1	Submit Exception Request Form (including risk assessment, reason, duration, compensating controls)	Requesting Manager / System Owner
2	Initial Review	Compliance / Risk Officer



3	Risk Assessment	CSCO evaluates residual risk and regulatory impact
4	Approval Decision	Based on severity matrix (see below)
5	Documentation	Record in Exception & Dispensation Register
6	Monitoring	Owner tracks progress and remediation plan
7	Closure	Exception expires or is formally closed after remediation

21.4 Exception Approval Matrix

RISK LEVEL	EXAMPLE	APPROVAL REQUIRED
Low	Delay in policy training completion	Department Head + Compliance Officer
Medium	Missing non-critical log fields in system	Chief Security & Compliance Officer (CSCO)
High	Delay in full KYC procedure for low-risk customer type	CSCO + CEO
Critical	Control gap that could cause regulatory breach	CEO + Board notification



Critical exceptions require Board-level awareness and must include a formal risk acceptance statement.

21.5 Exception Documentation Requirements

Every approved exception must include:

- Description of the rule being waived
- Reason and justification for the exception
- Affected system, process, vendor, or jurisdiction
- Risk assessment and impact analysis
- Compensating or temporary controls in place
- Approval authority and date
- Start and end date (maximum 6 months, unless renewed with re-approval)
- Remediation plan and responsible owner

21.6 Monitoring & Review

- Compliance maintains an Exception & Dispensation Register.
- Expiration alerts must be sent 30 days before the end date.
- Renewals require reassessment and re-approval—no automatic extensions.
- Exceptions not remediated on time are escalated to the Risk & Compliance Committee and CEO.

22. Global & Local Alignment; Jurisdictional Addenda

This section establishes how Orchestrate Global maintains a unified global compliance framework while adapting policies, procedures, and controls to meet specific local regulatory requirements in each jurisdiction where it operates.

22.1 Purpose



- Ensure global compliance standards are consistently applied across all countries and legal entities.
- Allow localized procedures only where required by law or regulator, without weakening core global standards.
- Provide a formal structure for managing jurisdiction-specific variances through documented Jurisdictional Addenda.

22.2 Global vs. Local Compliance Governance

ASPECT	GLOBAL STANDARD(MANDATORY)	LOCAL ADAPTATION(PERMITTED ONLY IF LEGALLY REQUIRED)
Policy Requirements	Enterprise Compliance Policy applies uniformly to all entities.	Local addendum may supplement, but never weaken , global controls.
AML/KYC Standards	Core framework defined globally (risk-based onboarding, EDD triggers, ongoing monitoring).	Local ID types, reporting thresholds, or record retention periods may be adjusted per national law.
Data Privacy & Transfers	Global data protection principles (lawfulness, purpose limitation, encryption, DSR handling).	Data localization, cross-border transfer restrictions, or DPA appointment may be added per jurisdiction.
Licensing & Reporting	Central tracking of all licenses, renewals, and regulatory filings.	Country Manager responsible for local regulator engagement and submission of jurisdiction-specific reports.
Training	All staff complete global baseline compliance training.	Local modules may be added for language, consumer law, or market-specific rules.

22.3 Jurisdictional Addenda Structure



Each operational jurisdiction must maintain a formally approved Jurisdictional Addendum, reviewed and signed annually by the Country Manager and CSCO, containing:

SECTION	REQUIRED CONTENT
1. Local Regulatory Authorities	Names, mandates, and contact details (e.g., Central Bank, FIU, Data Protection Authority).
2. Licensing Requirements	License type(s), numbers, renewal dates, capital/audit requirements.
3. Local AML/CFT Rules	Customer identification standards, PEP definitions, suspicious activity reporting timelines.
4. Data Protection Requirements	Local privacy laws, data subject rights process, transfer mechanisms (e.g., SCCs, BCR).
5. Reporting Obligations	Transaction reporting, fraud disclosures, operational incident notices.
6. Record Retention Variances	Jurisdictional retention periods that differ from global baseline (Section 16).
7. Product or Service Restrictions	Activities prohibited or requiring pre-approval (e.g., crypto, cross-border remittance).
8. Language & Disclosure Rules	Mandatory local language for contracts, dashboards, or customer notices.



9. Local Compliance Contacts

Designated MLRO, Data Protection Officer (if required), legal representative, escalation path.

All addenda are stored in the Controlled Documents Repository with version control and 7-year retention.

22.4 Roles & Responsibilities

ROLE	RESPONSIBILITY
Chief Security & Compliance Officer (CSCO)	Approves all jurisdictional addenda; ensures global standards are not diluted.
Country Manager / Local Compliance Officer	Maintains addendum; implements local compliance; acts as regulatory liaison.
Legal Department	Provides interpretation of local law; flags conflicts with global policy.
Internal Audit	Tests adherence to both global policy and local addenda during audits.

22.5 Conflict Resolution: Global Policy vs. Local Law



1. If local law is stricter → Local law prevails; global policy is supplemented (not replaced).
2. If global policy is stricter and not prohibited locally → Global standard applies in full.
3. If direct contradiction exists → Legal and Compliance escalate to CSCO and CEO for risk-based resolution.
4. Regulator instructions always override internal policy.

22.6 Local Regulatory Engagement

- All regulatory interactions (filings, inspections, correspondence) must be logged in the Regulatory Engagement Register.
- Country Managers must notify the CSCO within 24 hours of any regulatory inquiry, inspection, or enforcement action.
- Regulatory findings or remediation orders are treated as Critical Incidents under Section 18.

23. Audit & Independent Assurance

This section defines how Orchestrate Global ensures objective, independent evaluation of its compliance framework, internal controls, data protection practices, financial crime defenses, and operational integrity.

23.1 Purpose

- Provide assurance to the Board, regulators, banking partners, and stakeholders that compliance and risk controls are effective, reliable, and consistently implemented.
- Detect control weaknesses, policy deviations, or systemic risks that frontline and second-line monitoring may miss.
- Support regulatory licensing, investor due diligence, and partnership assessments.

23.2 Types of Independent Assurance



ASSURANCE TYPE	DESCRIPTION	PERFORMED BY
Internal Audit	Independent assessment of compliance, financial, IT, and operational controls.	Internal Audit Department
External Audit	Financial or compliance assessment (e.g., statutory audit, SOC 2, ISO certification).	Independent Audit Firm
Regulatory Audits / Inspections	Mandatory reviews by supervisory authorities (e.g., central bank, FIU, data protection agency).	Regulators
Third-Party Reviews	Assessments requested by banking partners or strategic clients under NDA.	Approved external firms
Penetration Testing & Security Audits	Technical validation of infrastructure, API, and application security.	Certified cybersecurity providers

23.3 Audit Coverage & Planning

- Internal Audit develops an annual risk-based audit plan, approved by the Board Audit & Risk Committee.
- High-risk domains (e.g., AML/CFT, sanctions, data privacy, transaction monitoring, cloud infrastructure) are audited at least annually.
- Medium-risk domains are reviewed every 24–36 months or triggered by incidents, regulatory changes, or material control failures.
- Unannounced or thematic audits may be conducted based on emerging threats, whistleblower reports, or regulatory mandates.

23.4 Audit Independence & Authority



- The Internal Audit function reports directly to the Board Audit & Risk Committee, ensuring organizational independence from operational management.
- Auditors have unrestricted access to:
 - Personnel (including executives and third parties)
 - Systems, logs, and transaction data
 - Policies, risk registers, incident reports
 - Vendor contracts and due diligence files
- Any interference with or obstruction of audit activities is considered a serious policy violation and may result in disciplinary action.

23.5 Audit Findings & Remediation

STAGE	REQUIREMENT
Issuance of Report	Findings are classified as Low / Medium / High / Critical, with root cause analysis and actionable recommendations.
Management Response	Business or control owners must provide a formal response within 10 business days, including remediation plan and timeline.
Tracking & Follow-Up	All findings logged in the Audit & Compliance Issues Register; progress reviewed monthly by Compliance and Internal Audit.
Closure Validation	Internal Audit validates evidence of remediation before formally closing the finding.
Escalation	Unresolved High/Critical findings after 60 days are escalated to the CEO and Board.

23.6 Documentation & Recordkeeping



- All audit engagements (internal, external, regulatory) are recorded in the Audit & Assurance Register, including:
 - Scope and objective
 - Dates and participants
 - Findings and severity
 - Management responses
 - Closure evidence
- Audit reports and supporting documentation must be retained for a minimum of 7 years in the Controlled Documents Repository.
- Regulatory inspection outcomes must be summarized in the Quarterly Board Compliance Report (Section 20).

23.7 Regulatory & External Stakeholder Access

- Regulators, banking partners, or auditors may request access to systems, data, or personnel as part of due diligence or oversight.
- All such requests must be:
 - Logged in the Regulatory Engagement Register
 - Reviewed by Legal and Compliance
 - Processed within legally mandated or contractually agreed timeframes
- Refusing or delaying legitimate regulatory access constitutes a breach of this policy and may trigger immediate escalation to the CEO and Board.

24. Document Controls



This section governs the management, versioning, approval, distribution, and archival of all compliance-related documentation to ensure accuracy, integrity, and regulatory defensibility across Orchestrate Global.

24.1 Purpose

- Maintain authoritative, up-to-date versions of all compliance policies, standards, procedures, and related documentation.
- Prevent the use of obsolete, unapproved, or conflicting documents.
- Ensure traceability of changes, approvals, and historical versions for audits and regulatory reviews.

24.2 Controlled Documents Scope

The following document types are subject to formal document control under this policy:

- Enterprise Compliance Policy and all referenced Level 1–2 policies
- Standards, procedures, and risk frameworks (e.g., AML/CFT Framework, Sanctions Standard)
- Regulatory obligation registers, licensing records, and jurisdictional addenda
- Training curricula, certification records, and awareness materials
- Audit reports, monitoring findings, issue logs, and remediation plans
- Model governance files, data protection impact assessments, and third-party due diligence records

24.3 Document Lifecycle Management



PHASE	REQUIREMENT
Creation & Drafting	Documents must use approved templates; include metadata (ID, owner, version).
Review & Consultation	Cross-functional input required from Legal, Risk, Security, and relevant business units.
Approval	Formal sign-off by designated approvers (per policy hierarchy in Section 7).
Publication	Final version published to the Controlled Documents Repository with unique ID and timestamp.
Distribution	Access granted per role-based permissions; distributed only via secure internal channels.
Review & Update	Reviewed annually or when triggered by regulatory change, incident, or audit finding.
Retirement	Marked “Obsolete,” archived, and retained per Section 16 retention requirements.



Each controlled document must include the following meta

FIELD	REQUIREMENT
Document Title	Clear and descriptive
Document ID	Unique identifier (e.g., OG-ECP-001, OG-AML-002)
Version Number	Incremented for each material change (e.g., 1.0 → 1.1)
Effective Date	Date the document becomes enforceable
Next Review Date	Typically 12 months from effective date
Document Owner	Named individual with contact details
Approver(s)	Roles and names of signatories
Status	Draft / Approved / Obsolete
Classification	Confidential – Internal Use Only (default)
Related Documents	Hyperlinks or references to supporting policies



24.5 Controlled Documents Repository

- All controlled documents are stored in a secure, access-controlled GRC or Document Management System (DMS).
- Access is governed by least privilege: only authorized personnel may view, edit, or approve.
- Editing rights are restricted to Document Owners and designated delegates.
- The system maintains a full audit trail of all actions (creation, modification, approval, download).

24.6 Change Control & Versioning

- No document changes may be made outside the formal change process.
- Minor edits (e.g., typo fixes) may be made without re-approval if they do not alter meaning; version number incremented (e.g., 1.0 → 1.1).
- Material changes (e.g., control updates, scope expansion) require full re-review and re-approval; version major number incremented (e.g., 1.0 → 2.0).
- A Change Log must be maintained within each document, listing:
 - Version number
 - Date of change
 - Summary of change
 - Author
 - Approver

24.7 Obsolescence & Archiving

- When a document is superseded or retired:
 - It is marked “Obsolete – For Reference Only”.
 - It is moved to the Archived Documents section of the repository.
 - It remains accessible for audit, regulatory, or legal purposes.
- Obsolete documents must not be used for operational guidance.



24.8 Accountability

- Chief Security & Compliance Officer (CSCO): Overall accountability for document control integrity.
- Document Owners: Responsible for ensuring timely reviews, updates, and approvals.
- Compliance Office: Maintains repository structure, metadata standards, and archival processes.
- All Staff: Must use only the latest approved version of any controlled document.

Appendix A: Control Matrix

This matrix maps core compliance obligations to specific controls, owners, and verification methods across Orchestrate Global.

#	REGULATORY POLICY DOMAIN	CONTROL DESCRIPTION	CONTROL TYPE	CONTROL OWNER	VERIFICATION METHOD	FREQUENCY
A1	AML / Financial Crime	Customer identity verified via reliable, independent source (KYC/KYB)	Preventive	Head of Operations	File review + system log audit	Per onboarding + annually
A2	Sanctions Compliance	Real-time screening of customers and transactions against OFAC, UN, EU, and local lists	Detective	Compliance Analyst	Alert log review, false positive analysis	Daily



A3	Data Protection	Personal data encrypted at rest and in transit using AES-256 / TLS 1.3	Preventive	CTO / Security Team	Architecture review, penetration test	Quarterly
A4	Training & Awareness	All staff complete mandatory compliance training within 30 days of hire	Directive	HR + Compliance	LMS completion report	Per hire + annually
A5	Third-Party Risk	Critical vendors undergo annual security and compliance due diligence	Preventive	Vendor Manager	Due diligence package, audit report	Annually
A6	Incident Response	Breach response initiated within 24 hours of detection	Corrective	CISO / CSCO	Incident log, post-mortem report	Per incident
A7	Model Risk	High-risk AI/ML models undergo independent pre-deployment validation	Preventive	Data Science Lead	Model validation report	Per model launch
A8	Record Retention	KYC records retained for 7 years post-relationship termination	Directive	Compliance	Repository audit	Ongoing



A9	Product Compliance	New product features require Compliance sign-off before launch	Preventive	Product + CSCO	Change ticket, approval log	Per release
A10	Conduct & Ethics	Gifts >\$100 logged and approved	Directive	All Staff	Gifts Register audit	As incurred
A11	Operational Resilience	DR failover tested annually with RTO ≤4 hours	Corrective	CTO / Ops	DR test report	Annually
A12	Regulatory Reporting	SAR/STR filed within statutory deadlines	Detective	MLRO	FIU submission logs	Per case
A13	Access Control	Role-based access with quarterly access reviews	Preventive	IAM Team	Access review certification	Quarterly
A14	Policy Management	Enterprise policies reviewed annually or upon material regulatory change	Directive	CSCO	Policy version history, approval log	Annual / event-driven

Control Types:

- Preventive: Stops risk before it occurs
- Detective: Identifies risk after it occurs
- Corrective: Mitigates impact post-event



- Directive: Sets expectations via policy, training, or procedure

Appendix B: RACI for Key Compliance Obligations

OBLIGATION	BOARD	CEO	CSCO	LEGAL	CTO	CCO	HR	INTERNAL AUDIT
Approve Enterprise Compliance Policy	A	A	R	C	I	C	I	I
Ensure AML/CFT Program Effectiveness	A	A	R	C	I	I	I	C
Manage Data Subject Rights (DSR)	I	I	A	C	R	I	I	I
Oversee Third-Party Risk Program	I	A	R	C	C	R	I	C
Conduct Compliance Training	I	I	A	I	I	I	R	C
Report to Regulators (e.g., SARs)	I	C	R	C	I	I	I	I
Review Audit Findings & Remediation	A	A	C	I	I	I	I	R
Manage Model & Algorithmic Risk	I	C	A	C	R	C	I	C



Maintain Records per Retention Policy	I	I	A	C	R	I	R	C
Handle Sanctions Screening & Blocking	I	I	R	C	C	I	I	I

RACI Legend:

- R = Responsible (does the work)
- A = Accountable (ultimate approval)
- C = Consulted (provides input)
- I = Informed (kept up to date)

Appendix C: Training Curriculum Map

ROLE	CORE MODULES	OPTIONAL/CONTEXTUAL MODULES	CERTIFICATION VALIDITY
All Employees	Code of Conduct, Data Privacy Basics, ABAC, Security Awareness, Whistleblowing	—	1 year
Customer Ops / Sales	KYC/KYB Procedures, Fair Marketing, Customer Complaints, AML Red Flags	FX Risk Disclosure, Stablecoin Compliance	1 year
Engineers / DevOps	Secure SDLC, API Security, Encryption Standards, Incident Response	Model Risk Basics, Logging Requirements	1 year



Compliance / Risk	AML/CFT Advanced, Sanctions Screening, Regulatory Change Mgmt, FCRA	Jurisdictional Addenda Deep Dive	1 year
Product Managers	Product Compliance Lifecycle, Model Governance, DSR Process	Third-Party Integration Compliance	1 year
Executives / Board	Board Oversight of Compliance, Risk Appetite, Regulatory Responsibilities	—	1 year
Third-Party Vendors (with data access)	Confidentiality, Incident Notification, Data Handling	—	Per contract term

Delivered via LMS with automatic reminders and manager dashboards.

Appendix D: Glossary

TERM	DEFINITION
ABAC	Anti-Bribery and Anti-Corruption
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
BCP	Business Continuity Plan



CISO	Chief Information Security Officer
CSCO	Chief Security & Compliance Officer
DSR	Data Subject Request
EDD	Enhanced Due Diligence
FCRA	Financial Crime Risk Assessment
FIU	Financial Intelligence Unit
GRC	Governance, Risk, and Compliance
KRI	Key Risk Indicator
KPI	Key Performance Indicator
KYC/KYB	Know Your Customer / Know Your Business
MLRO	Money Laundering Reporting Officer



PEP	Politically Exposed Person
RCC	Risk & Compliance Committee
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAR/STR	Suspicious Activity Report / Suspicious Transaction Report
SDLC	Secure Software Development Lifecycle

END OF ENTERPRISE COMPLIANCE POLICY