

Regulatory Readiness Checklist

Essential Steps for Building Compliance Infrastructure That Scales
LAWSEL ADVISORY | WWW.THELAWSEL.COM

How to Use This Checklist

This checklist is designed for founders, COOs, General Counsel, and compliance leads at technology companies operating or expanding across multiple jurisdictions. It covers the foundational elements of a compliance programme that satisfies regulators, investors, and enterprise clients. Items marked [PRIORITY] should be addressed first — particularly if you are preparing for a fundraising round or market entry.

1. Regulatory Landscape Assessment

- [PRIORITY] **Map the regulatory landscape** for every jurisdiction where you operate or plan to operate — identify all applicable laws, regulations, and licensing requirements
- Identify your regulatory classification** in each market: are you a regulated entity (e.g., payments, lending, insurance, healthcare) or subject to horizontal regulations only (data protection, consumer protection, e-commerce)?
- Assess licensing requirements:** determine whether any of your activities require regulatory licences, registrations, or notifications in target markets
- Monitor regulatory developments:** subscribe to regulatory updates in key jurisdictions and track proposed legislation that could affect your business
- Document your regulatory mapping** — this is the foundation that investors and enterprise clients will scrutinise during due diligence

2. Compliance Programme Design

- [PRIORITY] **Define the scope and objectives** of your compliance programme — what regulations it covers, what functions it touches, and what outcomes it aims to achieve
- Assign a compliance owner** — a named individual with authority, resources, and direct access to leadership (this does not need to be a full-time hire at early stage, but accountability must be clear)
- Establish a compliance governance structure:** reporting lines, committee membership, escalation procedures, and board reporting cadence
- Create a compliance policy framework:** overarching compliance policy, supported by topic-specific policies (AML/KYC, data protection, anti-corruption, export control, etc.)
- Implement a compliance risk register:** identify, assess, and prioritise compliance risks with assigned owners and mitigation actions

3. Fundraising & Investor Readiness

- [PRIORITY] **Prepare a compliance due diligence pack** covering: regulatory mapping, licences and registrations, material compliance policies, known regulatory risks, and pending or past regulatory actions
- Document regulatory strategy for expansion markets** — investors want to see that you understand the regulatory path, not just the commercial opportunity

- Address known compliance gaps transparently** — investors prefer a company that knows its gaps and has a remediation plan over one that claims perfection
 - Demonstrate board-level compliance oversight** — include compliance updates in board minutes and maintain a compliance dashboard
 - Prepare for regulatory-related warranty and indemnity provisions** in investment agreements — understand what you are being asked to warrant and whether you can
-

4. Market Entry Compliance

- [PRIORITY] Conduct a regulatory feasibility assessment** before committing to a new market — some regulatory requirements may fundamentally affect your business model
 - Identify mandatory local requirements:** entity establishment, local directors, data localisation, local representative appointments, consumer protection disclosures
 - Assess employment and contractor compliance:** worker classification, local employment law, benefits requirements, and payroll tax obligations
 - Review product and service localisation requirements:** local language, currency, consumer rights, cooling-off periods, and dispute resolution obligations
 - Create a market entry compliance checklist** specific to each target jurisdiction with timelines and responsible owners
 - Budget for compliance costs:** legal, regulatory, licensing, and ongoing compliance operational costs — these are often underestimated in market entry planning
-

5. Anti-Money Laundering & Financial Crime (if applicable)

- Determine whether AML/KYC requirements apply** to your business — they extend beyond banks to payments, lending, crypto, and certain marketplace models
 - Implement a risk-based KYC programme:** customer identification, verification, ongoing monitoring, and enhanced due diligence for higher-risk relationships
 - Establish transaction monitoring** appropriate to your business model and risk profile
 - Appoint a Money Laundering Reporting Officer (MLRO)** or equivalent where required
 - Implement sanctions screening** against relevant sanctions lists (OFAC, EU, UN) for customers, counterparties, and transactions
 - File Suspicious Activity Reports (SARs)** as required — and train staff to recognise red flags
-

6. Consumer Protection & E-Commerce

- Review consumer protection requirements** in each market: pre-contractual disclosures, cooling-off rights, complaint handling, and advertising standards
 - Ensure terms of service comply with local consumer law** — many jurisdictions have mandatory terms that cannot be excluded by contract (e.g., EU Consumer Rights Directive)
 - Implement compliant cancellation and refund mechanisms** — particularly for subscription services and digital content
 - Address accessibility requirements** where applicable (e.g., European Accessibility Act, ADA in the US)
 - Review marketing and advertising compliance:** endorsement disclosures, comparative advertising rules, and AI-generated content labelling requirements
-

7. Export Control & Sanctions

- Determine whether your technology is subject to export controls:** US Export Administration Regulations (EAR), EU Dual-Use Regulation, or other national regimes
 - Classify your products and technology** under relevant export control lists (Commerce Control List, EU Control List)
 - Implement screening procedures** to prevent export or provision of services to sanctioned countries, entities, or individuals
 - Address deemed export risks:** providing controlled technology to foreign nationals (even within your own company) may require a licence
 - Include export control provisions in commercial agreements** — particularly for technology licensing and cloud services
-

8. Operational Compliance Playbooks

- Create function-specific compliance playbooks** for teams that handle compliance-sensitive activities: sales (contract terms, regulated claims), marketing (advertising standards, data collection), product (privacy by design, accessibility), and engineering (data handling, security)
 - Define clear escalation procedures:** who to contact when a compliance question arises, with response time expectations
 - Implement compliance checkpoints** in key business processes: product launches, new vendor onboarding, market entry, major commercial deals, and M&A
 - Document decision-making:** when compliance-sensitive decisions are made, record the rationale, alternatives considered, and advice received
-

9. Training & Awareness

- Deliver compliance training to all staff** at onboarding — covering the company's compliance framework, key policies, and how to raise concerns
 - Provide role-specific training** for high-risk functions: sales, customer support, finance, product, and engineering
 - Run annual refresher training** — regulatory requirements evolve, and awareness decays without reinforcement
 - Train the board and leadership team** on their compliance oversight responsibilities
 - Track and document all training:** dates, attendees, content, and completion rates — regulators and investors expect evidence
-

10. Incident Response & Reporting

- Develop a compliance incident response plan:** who is notified, how incidents are assessed, escalation criteria, and regulatory reporting obligations
 - Know your regulatory reporting obligations:** which incidents must be reported, to which regulator, and within what timeframe
 - Establish a confidential reporting channel** (whistleblower mechanism) — required under EU Whistleblower Directive and increasingly expected globally
 - Conduct post-incident reviews** to identify root causes and update controls
 - Maintain an incident register** for regulatory accountability and pattern analysis
-

II. Ongoing Monitoring & Review

- Schedule periodic compliance programme reviews** — at minimum annually, and triggered by material regulatory changes, new markets, or new products
- Monitor regulatory enforcement trends** — enforcement actions against peers reveal regulatory priorities and help calibrate your risk tolerance
- Conduct internal compliance audits** or engage external auditors for independent assessment
- Report compliance programme status to the board** regularly — including risk assessments, incident trends, and programme maturity metrics
- Benchmark your programme** against recognised frameworks (ISO 37301 Compliance Management Systems) and peer practices

Investor Due Diligence: What They Will Ask

Area	Typical Questions
Regulatory mapping	Which regulations apply? Do you have a regulatory register?
Licences	What licences do you hold or need? Any pending applications?
Data protection	GDPR/DPDPA compliance status? DPO appointment? Breach history?
AML/KYC	Is your business subject to AML requirements? Programme maturity?
Litigation & enforcement	Any current or threatened regulatory actions? Past penalties?
Compliance team	Who owns compliance? What resources are allocated?
Insurance	D&O, cyber, professional indemnity coverage?

Next Steps

Compliance infrastructure should be proportionate to your stage, sector, and regulatory exposure — but the foundational elements (regulatory mapping, policy framework, governance, and training) apply at every stage.

Lawssel Advisory builds compliance programmes for technology companies — from seed-stage regulatory strategy to multi-market compliance infrastructure.

Book a consultation: www.thelawsel.com **Email:** rini@thelawsel.com

This document is for informational purposes only and does not constitute legal advice. Regulatory requirements vary by jurisdiction and sector and are subject to change.

Copyright 2026 Lawssel Advisory. All rights reserved.