THIESS INVEST GMBH

THIESS INVEST

CLGF

The Compliance-Led Growth Framework

A Practitioner's Playbook for MiCA-Regulated Crypto Market Entry

By Marcel Thiess

Founder, Thiess Invest GmbH · Author of CLGF

Edition 1 · 2026

ABOUT THIS PLAYBOOK

This playbook is the practitioner's edition of the Compliance-Led Growth Framework (CLGF), the operating system I use with crypto and fintech companies entering MiCA-regulated markets. It is distilled from more than a decade of operational experience inside major exchanges, infrastructure providers, and early-stage fintechs.

It is written for founders, general managers, compliance leads, and growth executives who already know the rules and now need a system to apply them without killing momentum.

HOW TO USE IT

Read the executive summary first. If the four modules describe the situation you are in, work through the rest of the document in order. Every module ends with at least one fully usable template, a checklist, a rubric, or a scoring grid, that you can apply to your company today.

When you are ready, score your organisation against the full eighteen control domains using the free CLGF Diagnostic at framework.thiessinvest.com. The diagnostic takes roughly fifteen minutes and produces a maturity score, a severity breakdown, and a prioritised finding list referencing the MiCA articles, RTS, and ESMA or EBA guidelines that apply.

RIGHTS AND DISTRIBUTION

CONTENTS

Table of Contents

EXECUTIVE SUMMARY

The operating system for MiCA-regulated crypto market entry.

Most crypto companies treat regulation as a gate. The ones that win treat it as a growth channel. That shift, from defensive compliance to compliance-led growth, is the single biggest predictor of which operators scale under MiCA and which stall at the authorisation stage.

CLGF is the system behind that shift. It organises everything a crypto or fintech company has to get right into four modules and eighteen control domains, each mapped to a concrete MiCA requirement, a supervisory expectation, a partnership standard, or a growth bottleneck. It is deliberately opinionated. It tells you where most teams under-invest, which tends to be customer support, partner oversight, and internal approval design, and where they over-invest, which tends to be template-heavy legal work that never touches operations.

What you will take away from this playbook

- A shared mental model for why compliance is the highest-leverage growth function in a regulated business.
- The four CLGF modules, explained in the order you should operationalise them.
- Workable templates, including a CASP-readiness self-assessment, a complaints handling rubric aligned to MiCA Article 71 and RTS 2025/294, a partner due diligence scorecard, an internal approval flow for marketing communications under Article 7 and Article 66, and a ninety-day sprint plan.
- A clear next step, score your organisation against the full framework in fifteen minutes, for free, at framework.thiessinvest.com.

CENTRAL THESIS

Teams that win under MiCA do not have the biggest compliance budgets. They have the best-designed compliance operating system, one that converts controls into authorisations, partnerships, and product velocity. CLGF is that operating system, written down.

The Case for Compliance-Led Growth

The pattern most operators are getting wrong.

Over the last decade, a predictable pattern has repeated across crypto operators entering EU markets. A product ships. A licensing project begins. Outside counsel is retained. Six to nine months in, momentum stalls. Examinations drag. Partnerships die in due diligence. Marketing slows to a crawl, because every claim has to pass three legal reviews. The team blames regulatory uncertainty, but the actual problem is the operating model.

Competent authorities are not asking for more rules. They are asking for evidence that the rules you already face are being applied consistently, visibly, and with a clear owner. Under MiCA, that evidence takes a specific form, governance arrangements, policies and procedures, complaints handling, conflicts of interest, record-keeping, continuity and regularity, and the list of specified information an applicant must submit under RTS 2025/305. That evidence is a product. It has to be designed, produced, and shipped, exactly like any other product the business ships.

Three myths that keep costing crypto operators money.

Myth	What it costs	The CLGF counter-position
Compliance is a cost centre.	Slower market entry, rejected partner diligence, lost institutional deals.	Compliance is the system that unlocks CASP authorisation, partnerships, and institutional revenue.
Legal owns compliance.	Policies that never touch operations. Controls that exist only in PDFs.	Operations own compliance. Legal owns the interpretation. Both report to the same system.
We will fix compliance when we are ready to scale.	Rebuilding under pressure during examination or a deal. Three to six months of lost velocity.	The scale-ready version is cheaper to build first than to retrofit.

What compliance-led growth actually means.

It is the operating principle that every growth lever in a regulated business, licensing, partnerships, product launches, marketing, user acquisition, is gated by a small number of controls that, once built correctly, make growth faster, not slower. The framework is designed to identify those

controls, operationalise them, and route every commercial decision through them in a way the business actually tolerates.

The four modules at a glance.

Module	Core question it answers	Primary owner
1, Regulatory Readiness	Are we building the evidence a competent authority or counterparty can verify under MiCA?	Head of Compliance or MLRO
2, Customer Support as First-Line Defence	Are we resolving customer complaints internally, before they become regulator-filed complaints?	Head of Customer Support
3, Partner-Led Growth	Are we scaling through authorised partners instead of rebuilding every licence ourselves?	Head of BD or Partnerships
4, Compliant Growth Operations	Can marketing, product, and BD ship without asking legal every time, within MiCA marketing rules?	COO or Head of Growth

KEY TAKEAWAY

The modules are ordered deliberately. Regulatory readiness without a first-line defence turns into theatre. A first-line defence without a partner strategy caps your growth. A partner strategy without a compliant growth operation becomes a bottleneck inside your own company. Build them in order.

II Module 1, Regulatory Readiness

The thesis.

Regulatory readiness is not a binary, it is a maturity curve, and most operators sit further down the curve than they think they do. The question a competent authority asks during CASP authorisation, or during ongoing supervision afterwards, is simple. Show me the evidence, in production, today, that the control MiCA requires is operating effectively. If the answer takes more than one meeting to produce, the organisation is not ready, regardless of what the policy manual says.

The ten control domains in this module, mapped to MiCA.

#	Domain	What "ready" looks like (MiCA reference)
P01	Governance and oversight	Management body suitability assessed against the Joint Guidelines on suitability, documented minutes, clear charter, and a signed risk-appetite statement. Article 68 MiCA.
P02	Fit and proper, qualifying holdings	Suitability evidence for management body and for direct or indirect qualifying holders, aligned with the Joint Guidelines on qualifying holdings. RTS 2025/414 for the assessment information.
P03	Policies and procedures	Policies for all required areas, versioned, with evidence the front line has been trained on the latest version, and a review cadence.
P04	Continuity and regularity of services	Business continuity, disaster recovery, and operational resilience evidenced in production. RTS 2025/299 on continuity and regularity in cryptoasset services, and the interplay with DORA.
P05	Custody and safekeeping of client assets and funds	Segregation of client cryptoassets and client funds, reconciliation cadence, and custody policy evidencing protection of client rights. Articles 70 and 75 MiCA.
P06	Conflicts of interest	Conflicts policy, register, and disclosure workflow meeting RTS 2025/1142 for CASPs, or RTS 2025/1141 for ART issuers.
P07	AML, CFT, and sanctions	Full AMLD framework, transaction monitoring, sanctions screening, and SAR filing. Addressed under the AML package and national law alongside MiCA.
P08	Record-keeping	Records of all cryptoasset services, activities, orders, and transactions kept for at least five years, extendable to seven years at the competent authority’s request. Article 68(9) MiCA and RTS 2025/1140.
P09	Market abuse prevention	Arrangements, systems, and procedures to prevent, detect, and report market abuse, with notification templates. Title VI MiCA and RTS 2025/885.
P10	Prudential and own funds	Ongoing own funds calculation, monitoring, and adjustment procedures. Article 67 MiCA, plus RTS 2025/415 and RTS 2025/419 where applicable to ART or EMT issuers.

WHERE MOST OPERATORS UNDER-INVEST

P04 (operational continuity and DORA interplay), P08 (record-keeping that actually produces extractions on demand), and P09 (market abuse monitoring on-chain and on-

venue). These are the three domains competent authorities and institutional counterparties consistently probe first, and they are almost always the ones found weakest.

Template, Regulatory Readiness Self-Assessment.

For each domain, score your organisation on the four-point maturity scale below. Anything under a 2.0 average across the module is not ready for a MiCA CASP application or a top-tier partner diligence review.

Score	Label	Operational definition
0	Nothing in place	No documented policy or control. Ad-hoc at best.
1	Informal only	A practice exists but is not written down, not assigned, and not auditable.
2	In place, not audited	Documented and operating, but no independent review or evidence of effectiveness.
3	Fully tested	Documented, operating, independently reviewed, and evidenced with metrics.

Self-assessment checklist

☐ Management body suitability is assessed and documented per the Joint Guidelines on suitability.

☐ Qualifying holders, direct and indirect, have been assessed per the Joint Guidelines on qualifying holdings.

☐ Every policy has a named owner, a version number, and a training record per employee.

☐ A business continuity plan has been tested within the last 12 months and evidence is on file.

☐ Client cryptoassets and client funds are segregated, with reconciliation frequency defined and evidenced.

☐ Conflicts of interest register is live, and disclosure workflow meets RTS 2025/1142 for CASPs.

☐ Transaction monitoring has tuning evidence, false-positive rate, alert-to-case conversion, and threshold rationale.

☐ Records of services, orders, and transactions are kept for at least five years and can be extracted on request.

☐ Market abuse arrangements are documented with notification templates aligned to RTS 2025/885.

☐ Own funds calculation is refreshed on the documented cadence, with adjustments procedure per RTS 2025/419 where relevant.

WORKABLE NEXT STEP

Pull your team into a 90-minute working session. Score each of the ten domains above using the four-point scale. Any domain scored 0 or 1 goes onto a 30-day remediation sprint. Any domain at 2 goes onto a 60-day audit-readiness sprint. Domains at 3 become the case studies you use in partner and supervisor conversations.

III Module 2, Customer Support as First-Line Defence

The thesis, and what it does not mean.

Most crypto operators will tell you their first line of defence is front-line employees. That is too vague to be operational. I treat customer support as a first-line defence in a very specific sense, and it is worth being precise about what that means.

When compliance freezes an account for AML, sanctions, or fraud reasons, compliance is first-line, of course. Support is downstream of that decision. The reason I still put customer support into the first line of defence is different. Most regulatory complaints that land on a competent authority's desk do not start as compliance issues. They start as ordinary customer complaints, a delayed withdrawal, a misunderstood fee, a KYC request the customer found confusing, an outage, a mismatched trade, that the company never resolved fast enough. So the customer escalates to the regulator instead. That is where the regulatory exposure actually comes from, day to day.

Efficient customer support, structured correctly, prevents those complaints from ever leaving the company. That is its first-line role, and MiCA recognises it explicitly. Article 71 MiCA requires CASPs to establish and maintain effective and transparent procedures for the prompt, fair, and consistent handling of complaints, and RTS 2025/294 specifies the templates, timeframes, and

information CASPs must maintain. Meeting that bar is not a customer-care nicety, it is a direct regulatory control.

The three control domains in this module.

#	Domain	What to build
P11	Complaints handling under MiCA Article 71 and RTS 2025/294	A documented procedure, free of charge for the complainant, with acknowledgement, investigation, and substantive response within the timeframes set by your competent authority. A complaints register with regulator-grade metadata.
P12	Support-to-compliance handoff	A tagging taxonomy that routes regulatory-relevant contacts (fraud reports, sanctions concerns, market abuse tips) into the compliance queue in real time, with audit trail.
P13	Incident response and disclosure	A joint playbook run by support, security, and compliance, with pre-agreed decision trees for the first 24 hours of an incident, aligned with DORA incident reporting where applicable.

The four categories of complaint every support team should be tagging.

Category	Typical surface	Where it should escalate
Service quality (non-compliance)	Delayed withdrawals, fee disputes, UX confusion, app downtime.	Resolve inside support SLA. Track recurrence as a product input.
Regulatory complaint risk	Customer threatens to contact the competent authority, ombudsman, or consumer authority.	Immediate escalation to the complaints officer. Response clock starts under Article 71.
Fraud and sanctions signal	Customer reports account takeover, social engineering, or a counterparty sanctions concern.	Real-time handoff to fraud and compliance. Tag for transaction-monitoring re-tuning.
Market abuse signal	Customer reports suspected manipulation, insider dealing, or misleading disclosures.	Real-time handoff to the market abuse officer per Title VI MiCA and RTS 2025/885.

Template, complaint severity and response rubric.

Severity	Definition	Response standard
S0	Informational query, no complaint.	Resolve within standard support SLA. No register entry required.
S1	Service complaint, no regulator mentioned.	Acknowledge within 1 business day. Substantive response within the firm-defined SLA. Register entry per RTS 2025/294.
S2	Complaint with regulator, ombudsman, or consumer authority mentioned.	Escalate to complaints officer same day. Treat as Article 71 complaint. Root-cause analysis within 10 business days.
S3	Allegation of misconduct, fraud, or sanctions concern.	Handoff to compliance within 4 hours. Preserve evidence. Trigger SAR review if thresholds met.
S4	Market abuse signal, incident, or data breach indication.	Invoke incident response playbook. Notify competent authority and data protection authority within statutory deadlines where applicable.

Implementation checklist

☐ Article 71 complaints procedure is published in a customer-accessible place in each required language.

☐ Complaints register contains the fields required by RTS 2025/294, including receipt date, category, resolution, and root cause.

☐ Tagging taxonomy in the support tool routes S2 and above to compliance automatically.

☐ Support team is trained on the S0 to S4 severity rubric and re-tested annually.

☐ Monthly complaints MI is shared with the management body, with themes and root causes.

☐ Product inputs from recurring S1 complaints are tracked to closure.

WHAT THIS GETS YOU

Two outcomes that matter. First, fewer complaints reach the competent authority, because they were resolved inside the company within the statutory window. Second, when a supervisor does inspect your complaints file, the register is already in the form the RTS expects, which is one of the easiest ways to build credibility with your regulator.

IV Module 3, Partner-Led Growth

The thesis.

Rebuilding every licence in every market is slow, expensive, and often unnecessary. Most crypto operators scale faster, and with less regulatory drag, by partnering with already-authorised CASPs, EMIs, custodians, and distribution partners, and then governing those relationships rigorously. MiCA does not penalise outsourcing, but it does hold you fully responsible for it. Article 73 MiCA requires a CASP that outsources operational functions to take all reasonable steps to avoid undue additional operational risk, and to ensure that outsourcing does not materially impair the quality of internal control or the competent authority's ability to supervise.

The two control domains in this module.

#	Domain	What to build
P14	Partner selection and due diligence	A scorecard that evaluates regulatory posture, financial stability, operational maturity, and strategic fit before contracting.
P15	Partner oversight and outsourcing governance	Ongoing oversight under Article 73 MiCA, including a service-level agreement, audit rights, exit plan, and evidence of periodic review.

Build versus partner, a decision grid.

Capability	Build yourself if...	Partner if...
Custody of client cryptoassets	It is core to your product and you have the capital and expertise to meet Article 70 and related safeguarding standards.	You can contract with an authorised custodian that meets segregation and reconciliation standards, with audit rights.
EUR on- and off-ramp	You already hold or can realistically obtain EMI or PI authorisation.	You can partner with an authorised EMI or PI whose passporting covers your target markets.
Trading venue operation	You have a long-term volume thesis and the prudential and market-abuse controls to match.	You can route flow through an authorised trading platform with a clear allocation of Title VI MiCA obligations.
Distribution into new member states	You have direct go-to-market capacity and local language coverage.	You can use an authorised CASP's passporting footprint or a regulated distribution partner.

Template, the seven-dimension partner scorecard.

Use this scorecard before contracting with any regulated partner. Score each dimension 0 to 3. A partner scoring below 2.0 on average, or a zero on any single dimension, is not ready.

Dimension	What you are checking	Evidence required
1. Authorisation status	Is the partner authorised for the exact services they will provide you?	Public register entry, authorisation letter, passport notifications.
2. Management and ownership	Are management body and qualifying holders fit and proper?	Suitability documentation per Joint Guidelines, UBO register check.
3. Capital and financial stability	Can the partner absorb operational shocks?	Audited financials, own funds report, capital adequacy evidence.
4. Operational maturity	Does the partner operate at the service level you need?	SLA history, uptime reports, incident log, BCP test results.
5. AML and sanctions framework	Are AML, sanctions, and travel-rule controls at or above your own?	Policy set, risk assessment, independent audit or SOC report.
6. Data protection and security	GDPR, DORA, and ICT risk posture?	DPA, SOC 2 or ISO 27001, penetration test summary, incident history.
7. Exit and continuity	Can you exit the relationship without operational breakage?	Documented exit plan, data portability clauses, transition support commitment.

Outsourcing and oversight checklist, Article 73 aligned

- ☐ Outsourcing policy is in place, covering approval, oversight, and termination of outsourcing arrangements.
- ☐ Outsourcing register lists all material arrangements, with owner and review cadence.
- ☐ Written SLA covers scope, performance metrics, audit rights, sub-outsourcing, and termination.
- ☐ Competent authority notification is in place where the outsourced function is critical or important.
- ☐ Business continuity plan covers failure of each material outsourcing partner.
- ☐ Annual oversight review is documented, with findings and remediation tracked to closure.
- ☐ Exit plan is tested or tabletop-exercised at least once per year.

THE LEVERAGE

Partner-led growth is not a shortcut, but only if the oversight is real. The firms that do this badly end up owning every failure of a partner without the authority to fix it. The firms that do it well turn every partner into a controlled channel that scales with their brand, not at the expense of it.

V Module 4, Compliant Growth Operations

The thesis.

The last module is where most frameworks give up. Marketing wants to ship a campaign. Product wants to launch a new token listing. BD wants to sign an institutional partner by Friday. In most crypto companies, all three end up in a weekly escalation queue with legal, which grinds everyone down. CLGF replaces that escalation queue with a three-lane approval flow, so that routine work does not touch legal at all, elevated work runs through compliance, and only genuinely novel work reaches the general counsel.

MiCA makes this easier to build, because it tells you exactly what you have to get right on the marketing side. Article 7 and Article 66 require that marketing communications are fair, clear, not misleading, identifiable as marketing, and consistent with the white paper. Article 66 also covers general obligations for CASPs acting honestly, fairly, and professionally in the best interests of clients. Once you encode those standards into a marketing checklist, you have a rule-set the growth team can run on without phoning legal every time.

The three control domains in this module.

#	Domain	What to build
P16	Marketing communications control	A pre-publish checklist aligned with Article 7, Article 66 MiCA, and your white paper, with approver routing by severity.
P17	Product and launch readiness	A launch readiness review that covers classification, white paper (if required), conflicts of interest, market abuse, and complaints handling readiness.

#	Domain	What to build
P18	Conflicts of interest and inducements	Conflicts policy, register, and disclosure workflow per RTS 2025/1142, with annual attestation for all client-facing staff.

The three-lane approval flow.

Lane	What it covers	Who approves
Green	Routine marketing within pre-approved templates. Minor product updates. Existing partner renewals. Complaints responses per standard template.	Line manager. No legal review required.
Amber	New campaigns, new markets, new jurisdictions, new partners, new product features, complaints with regulator mentioned.	Compliance officer with 24-hour SLA.
Red	New product classifications, token listings requiring a white paper, institutional deals over defined threshold, anything triggering management body attention.	General counsel and relevant management body member.

Template, the marketing pre-publish checklist (Article 7 and 66 aligned).

- ☐ The communication is clearly identifiable as a marketing communication.
- ☐ Information is fair, clear, and not misleading, including on risks, fees, and past performance.
- ☐ The communication is consistent with the white paper, where a white paper is required.
- ☐ No marketing communication is disseminated before the white paper has been published, where required.
- ☐ Any risk warnings required by your competent authority are present and visible.
- ☐ Target market is appropriate and the communication is not directed at prohibited audiences.
- ☐ All claims are substantiated and the evidence is saved on file.
- ☐ The communication has an approver signature from the correct lane (Green, Amber, Red).

Launch readiness checklist, pre-launch, launch week, post-launch

Pre-launch:

- ☐ Classification memo complete (cryptoasset type, ART, EMT, other, financial instrument under MiFID II).
- ☐ White paper drafted and notified to the competent authority, where required.
- ☐ Marketing materials vetted through Article 7 and Article 66 checklist.
- ☐ Complaints handling procedure updated with new product in scope.
- ☐ Market abuse monitoring scope extended to the new product.

Launch week:

- ☐ Support team briefed on the new product and severity rubric updates.
- ☐ Compliance on-call coverage scheduled for the first 72 hours.
- ☐ Incident decision tree live with named on-call owners.

Post-launch:

- ☐ First complaints report reviewed within 14 days, with themes logged.
- ☐ Market abuse alerting tuned against actual product behaviour.
- ☐ Post-mortem on any supervisory queries, with actions tracked to closure.

THE OUTCOME

When this flow works, marketing, product, and BD stop waiting on legal. Legal stops getting dragged into routine questions. Compliance stops being the function that says no, and becomes the function that lets the Green lane run at full speed.

VI Implementation, the 90-Day CLGF Sprint

How to roll CLGF out without disrupting the business.

CLGF is not a one-weekend installation. On the other hand, it does not need six months of consulting either. The companies that adopt it fastest break the rollout into six phases across a single quarter, with a clear deliverable at the end of each phase.

Phase	Window	Focus	Deliverable
1	Days 1 to 10	Diagnostic and alignment. Run the free CLGF diagnostic. Socialise the results with the management body.	Baseline score and heatmap by module.
2	Days 11 to 25	Module 1, regulatory readiness remediation for all P01 to P10 domains scored below 2.	Domain-level remediation plan and owners.
3	Days 26 to 45	Module 2, stand up MiCA Article 71 complaints handling, severity rubric, and support-to-compliance handoff.	Live complaints register and tagging taxonomy.
4	Days 46 to 60	Module 3, run the seven-dimension scorecard on every material partner. Close oversight gaps under Article 73.	Updated partner register and outsourcing oversight plan.
5	Days 61 to 80	Module 4, implement the three-lane approval flow and marketing pre-publish checklist.	Approval flow live in tooling, with training complete.
6	Days 81 to 90	Independent review and board sign-off. Re-run the diagnostic for a post-sprint score.	Board-approved CLGF operating model.

KPIs to track from day one.

KPI	Owner	Target
Complaints resolved within Article 71 SLA	Head of Support	95 percent or higher
S2 complaints escalated to compliance within 1 business day	Head of Support	100 percent
Material outsourcing partners covered by a current scorecard	Head of BD	100 percent, refreshed annually
Marketing pieces shipped without legal re-work	Head of Growth	80 percent Green-lane after month three
Domains scored 3 in the module self-assessment	Head of Compliance	Increase by 3 per quarter until full maturity

A NOTE ON SEQUENCE

The companies that stall tend to be the ones that try to do Module 4 first, because it is the most visible. Do not. Without the first three modules, the growth operations lane will be approving activity you cannot defend. Build them in order.

Next Steps and Working With Thiess Invest

If the patterns in this playbook look like your company today, there are two ways to move forward.

1. Score your readiness in fifteen minutes, free.

The CLGF diagnostic walks you through all eighteen control domains and produces a maturity score, a severity breakdown, and a prioritised finding list, each mapped to the MiCA articles, RTS, and ESMA or EBA guidelines that apply to your business model.

Start here, framework.thiessinvest.com

2. Run a structured engagement with Thiess Invest.

When you are ready to implement, we run the ninety-day sprint with you. That includes independent assessment, module-level remediation, supervisor-grade documentation, and board-ready reporting. Engagements are scoped to what you actually need, not to a fixed retainer.

Start a conversation, thiessinvest.com

A CLOSING NOTE

You do not need more legal advice. You need a system. CLGF is the system I built so that compliance stops being the reason you missed the quarter, and starts being the reason you made it.

About the Author

THIESS INVEST

Marcel Thiess

Marcel is a crypto and fintech executive with over a decade of operational experience across major exchanges, infrastructure providers, and early-stage fintechs. He has led compliance and customer-facing functions at scale, worked directly on licensing and authorisation across EU member states, and advised companies preparing for CASP authorisation and ongoing MiCA supervision.

He writes on crypto, compliance, and the intersection of AI and financial services, with a focus on practical operating models rather than policy theory.

Thiess Invest GmbH

Thiess Invest GmbH is the advisory practice behind CLGF, working with exchanges, infrastructure providers, and fintechs on regulatory readiness, partner-led growth, and compliant growth operations under MiCA. We engage directly with founders and management bodies, not through layers of junior consultants.

Contact, marcel.thiess@thiessinvest.com · thiessinvest.com