

THIESS INVEST GMBH



THIESS INVEST

CLGF

Compliance-Led Growth Framework (CLGF)

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

By Marcel Thiess

Founder, Thiess Invest GmbH · Creator of the Compliance-Led Growth Framework

Edition 2 · September 2026

About This Playbook

This playbook is the practitioner's edition of the Compliance-Led Growth Framework (CLGF), the operating system I apply with crypto and fintech companies entering the EU under MiCA. It is distilled from more than eight years of operational and advisory work inside major exchanges, market makers, custody providers and infrastructure businesses, and from the same conversation I have had a dozen times with companies that believed a law firm and a nine-month timeline would get them a license.

The full framework runs to thirteen modules, twenty-four control domains and more than 200 pages of procedures, templates, scorecards and checklists. This playbook covers the four strategic pillars that organize it and gives you one working tool for each. 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 losing momentum.

How to use it

Read the executive summary and Section I first. If the pattern they describe matches your company, work through the four pillars in order; each ends with a template you can apply this week. Then score your organization against all twenty-four control domains with the free CLGF diagnostic at framework.thiessinvest.com. It takes about fifteen minutes and produces a maturity score, a severity breakdown and a remediation roadmap on the same scale the framework uses.

Rights and distribution

© 2026 Thiess Invest GmbH. All rights reserved. The Compliance-Led Growth Framework, CLGF, and all associated templates, rubrics and diagrams are the original authorship of Marcel Thiess. This document may be shared in its entirety, unmodified, for non-commercial and internal evaluation purposes. Commercial use, derivative works and training of automated systems require prior written consent.

Nothing in this playbook constitutes legal, tax or investment advice. It is a methodology document. Apply it to your own facts with qualified counsel. References to MiCA, its Level 2 measures and ESMA or EBA guidelines are summarized for operational context; consult the binding text and the guidance of your competent authority.

Executive Summary

I have had the same call at least a dozen times. A crypto exchange, sometimes an infrastructure provider or a market maker, usually based in Asia or the United States, wants to enter Europe. The timeline in their head is six to nine months. They have engaged a law firm and one of the Big Four. They want a little practical guidance on the side.

Then I ask what they have in place. People on the ground with EU regulatory experience? A legal entity? Policies, procedures, controls? Familiarity with MiCA, the 2025 Level 2 package, the ESMA and EBA guidelines? The answer is almost always no, or "we have something from our global setup". The global setup was built for a different supervisory culture. The retainer is already burning, and the internal foundation the competent authority will actually examine does not exist yet.

That gap is where most of the budget disappears, and it is avoidable.

CLGF is the system that closes it. It organizes everything a company has to build, document and evidence for MiCA authorization and ongoing supervision into thirteen operating modules and twenty-four control domains, grouped under four strategic pillars. Every domain maps to a MiCA article, a Level 2 measure, a supervisory expectation or a partnership standard. The framework is deliberately opinionated about where teams under-invest, which is customer support, partner oversight and internal approval design, and where they over-invest, which is legal drafting that never reaches operations.

What you will take away

- A clear picture of how the European authorization sequence works and why "build first, comply later" fails here.
- The four pillars of CLGF, in the order to operationalize them.
- Working tools: the twenty-four-domain readiness map, the complaint severity rubric aligned to MiCA Article 71, the seven-dimension partner scorecard, the three-lane approval flow with the marketing checklist under Articles 66 and 7, and the twenty-week implementation sprint at a glance.
- A next step that costs nothing: the diagnostic at framework.thiessinvest.com.

CENTRAL THESIS

The companies that get authorized under MiCA and scale afterwards run on a compliance operating system that turns controls into an authorization, into partnerships and into product velocity. That system matters more than the size of the compliance budget. CLGF is that system, written down.

I. The Case for Compliance-Led Growth

In Europe, readiness comes first

In many markets, particularly in Asia and the Middle East, companies build first and deal with regulation when it arrives. The product ships, revenue starts, compliance catches up. In those markets it can work.

The EU runs the sequence in reverse. You demonstrate readiness, then you are authorized, then you operate. Since 1 July 2026, when the MiCA transitional period ended across the Union, there is no grandfathering left: a firm providing crypto-asset services to EU clients needs a CASP authorization, an Article 60 notification as a bank or investment firm, or a compliant white-label arrangement with an authorized provider. The competent authority expects evidence before promises, and it tests substance before it reads policies.

The pattern that keeps repeating

A product ships. A licensing project begins. Counsel is retained. Six to nine months in, momentum stalls. The application comes back incomplete. Partnerships die in due diligence. Marketing slows

because every claim needs three reviews. The team blames regulatory uncertainty. In every case I have seen, the operating model was the problem.

Competent authorities are asking for evidence that the rules already in force are applied consistently, visibly and with a named owner. Under MiCA that evidence has a specific shape: governance arrangements, policies and procedures, the Article 71 complaints procedure, the conflicts register, records under Article 68(9), business continuity, DORA, and the seventeen sections of the application defined in RTS 2025/305. That evidence has to be designed, built and shipped like any other product the company makes.

Three assumptions that cost money

Assumption	What it costs	The CLGF position
Compliance is a cost center	Slower entry, failed partner diligence, lost institutional deals	Compliance unlocks the authorization, the partnerships and the institutional revenue
Legal owns compliance	Policies that never reach operations; controls that exist only as PDFs	Operations own the controls; legal owns the interpretation; both report into one system
We will fix compliance when we scale	Rebuilding under supervisory pressure or in the middle of a deal; three to six months lost	The scale-ready version costs less to build first than to retrofit

The timeline every client asks about

Date	Event
30 December 2024	MiCA Title V applies: CASP authorization and conduct rules
17 January 2025	DORA applies to CASPs
Q1 to Q2 2025	MiCA Level 2 package published: authorization content (RTS 2025/305), complaints (2025/294), conflicts (2025/1142), records (2025/1140), market abuse (2025/885), continuity (2025/299)
30 December 2025	German transitional period ends
1 July 2026	EU-wide transitional period ends
10 July 2027	AMLR applies directly; national AML laws replaced for the harmonized parts; CDD on crypto occasional transactions from EUR 1,000
2028	AMLA direct supervision of selected cross-border entities, including CASPs

The four pillars at a glance

Pillar	Core question	Primary owner	Framework modules
1. Regulatory Readiness	Are we producing the evidence a competent authority can verify under MiCA?	Head of Compliance or MLRO	P02, P03, P06, P11
2. Customer Support as a	Are we resolving complaints inside the	Head of Customer	P12

Pillar	Core question	Primary owner	Framework modules
First-Line Control	company, before they reach the NCA?	Support	
3. Partner-Led Growth	Are we scaling through authorized partners, structured the way MiCA allows?	Head of BD or Partnerships	P07, P13
4. Compliant Growth Operations	Can marketing, product and BD ship without a legal review every time?	COO or Head of Growth	P04, P05, P08, P09, P10

KEY TAKEAWAY

The pillars are ordered deliberately. Regulatory readiness without a first-line control becomes theater. A first-line control without a partner strategy caps growth. A partner strategy without a compliant growth operation becomes a bottleneck inside your own company. Build them in order.

II. Pillar 1: Regulatory Readiness

The thesis

Regulatory readiness is a maturity curve, and most operators sit further down it than they believe. The question a competent authority asks at authorization, and again in supervision, is simple: show me the evidence, in production, today, that the control MiCA requires is operating. If the answer takes more than one meeting to produce, the organization is not ready, whatever the policy manual says.

The twenty-four control domains

This is the map the whole framework runs on. The diagnostic scores every domain on the same 0 to 3 scale.

Group	Domain	Primary legal basis
Core Compliance	1. Governance and oversight	MiCA Art. 68; AMLR Art. 11 from 2027
Core Compliance	2. AML/CFT policies	National AML law; AMLR Art. 9 from 2027
Core Compliance	3. Business-wide risk assessment	National AML law; AMLR Art. 10 from 2027
Core Compliance	4. KYC and customer due diligence	National AML law; AMLR Art. 19 and 20 from 2027
Core Compliance	5. EU restrictive measures screening	EU sanctions regulations
Core Compliance	6. Transaction monitoring	National AML law; AMLR Art. 26 from 2027
Core Compliance	7. Wallet and blockchain screening	TFR; EBA risk factor guidelines for CASPs

Group	Domain	Primary legal basis
Core Compliance	8. STR reporting to the FIU	National AML law; AMLR Art. 69 from 2027
Core Compliance	9. Travel Rule compliance	TFR (EU) 2023/1113; EBA Travel Rule guidelines
Core Compliance	10. Recordkeeping and retention	MiCA Art. 68(9); RTS 2025/1140
Core Compliance	11. Conflicts of interest	MiCA Art. 72; RTS 2025/1142
Core Compliance	12. Market abuse prevention	MiCA Title VI; RTS 2025/885
Core Compliance	13. Client asset segregation	MiCA Art. 70
Core Compliance	14. Own funds and prudential	MiCA Art. 67 and Annex IV
Operations and Oversight	15. Training and certification	MiCA Art. 68; national AML law
Operations and Oversight	16. Independent testing	MiCA Art. 68; national AML law
Operations and Oversight	17. Customer support and complaints handling	MiCA Art. 71; RTS 2025/294
Growth and Partnerships	18. Marketing compliance	MiCA Art. 66 and Art. 7
Growth and Partnerships	19. Licensed partner compliance	MiCA Art. 73
Infrastructure and Governance	20. Outsourcing governance	MiCA Art. 73
Infrastructure and Governance	21. Data protection	GDPR
Infrastructure and Governance	22. Vendor management	MiCA Art. 73; DORA Art. 28
Infrastructure and Governance	23. Regulator engagement	Supervisory practice
Infrastructure and Governance	24. Operational resilience	DORA (EU) 2022/2554

The maturity scale

Score	Label	Operational definition
0	Nothing in place	No documented policy or control
1	Informal only	A practice exists but is not written down, not assigned, not auditable
2	In place, not tested	Documented and operating, but no independent review or evidence of effectiveness
3	Fully tested	Documented, operating, independently reviewed, evidenced with metrics, retrievable within 24 hours

An average below 2.0 is not ready for a CASP application or a serious partner diligence. The framework does not submit an application with any applicable domain below 2.

What the application actually contains

Most companies underestimate the application because they have never seen its structure. RTS 2025/305 fixes it at seventeen sections. The full framework (module P06) maps each one to the document that satisfies it, the owner, and what the NCA is testing. The outline:

RTS 2025/305	Section	What the NCA is testing
Art. 1	General information	Identity, LEI, corporate documents
Art. 2	Programme of operations	Services, clients, member states, three-year operational capacity, and every marketing channel you intend to use, including influencers and affiliates
Art. 3	Prudential requirements	Own funds by class; fixed overheads; three-year forecasts with stress scenarios
Art. 4	Governance and internal control	Three lines of defense, compliance authority, conflicts policy and register, outsourcing register
Art. 5	Business continuity	Plan, recovery objectives, test results
Art. 6	ML/TF prevention	The full AML/CFT program and MLRO
Art. 7	Management body	Repute, competence, time commitment, interview
Art. 8	Qualifying holdings	Repute and origin of funds for every holder of 10 percent or more
Art. 9	ICT and security	DORA framework, incident process, register of information, cybersecurity staffing
Art. 10	Segregation of client assets	On-chain and in the books; applies to every CASP
Art. 11	Complaints handling	The Article 71 procedure and template
Art. 12 to 17	Service-specific sections	Custody policy, trading platform rules and market abuse, exchange policy, execution policy, advice and portfolio management, transfer services

WHERE MOST OPERATORS UNDER-INVEST

Three domains draw the first questions from competent authorities and institutional counterparties, and they are almost always the weakest: operational resilience under DORA (domain 24), recordkeeping that can actually produce an extraction on request (domain 10), and market abuse surveillance on-chain and on-venue (domain 12). The fourth is not a domain but a test: substance. Two nominee directors and a compliance officer in another time zone fail it.

Template: readiness self-assessment

Pull the team into a ninety-minute working session and score each of the twenty-four domains. Domains at 0 or 1 go onto a thirty-day remediation sprint; domains at 2 go onto a sixty-day audit-readiness sprint; domains at 3 become the case studies you use with partners and supervisors. Ten checks that predict the score:

- The management body has been assessed against the EBA and ESMA joint guidelines on suitability and can explain the control environment without notes.
- Every policy has a named owner, a version number and a training record per employee.
- The business-wide risk assessment was drawn up by the compliance officer, approved by the management body and updated in the last twelve months.
- Transaction monitoring has tuning evidence: threshold rationale, alert-to-case conversion, closure within SLA.
- Client crypto-assets and funds are segregated on-chain and in the books, with daily reconciliation and client funds at a credit institution.
- Records of services, orders and transactions can be extracted within 24 hours.
- The conflicts register is live and disclosure to clients works where prevention is not possible.
- The DORA incident path has been tested against the four-hour, 24-hour, 72-hour and one-month clocks, and the register of information exists.
- Own funds are calculated at the higher of the Annex IV class minimum and one quarter of fixed overheads, monitored monthly.
- Management, compliance and ICT decisions are demonstrably taken in the home member state.

III. Pillar 2: Customer Support as a First-Line Control

The thesis, stated precisely

Most operators will tell you their first line of defense is "the front line". That is too vague to be operational. Customer support is the first-line control owner for complaints handling and customer-facing communication, and a detection channel that feeds the risk surfaces owned elsewhere: KYC operations, transaction monitoring, sanctions screening, fraud, treasury. Framed that way, support reduces regulatory escalation and produces evidence. Framed as a universal first line for everything, it dilutes the accountability that the three-lines model gives to compliance.

Here is why it matters. Most complaints that land on a competent authority's desk start as ordinary tickets: a delayed withdrawal, a confusing KYC request, a misunderstood fee, an outage. The company resolved them too slowly, so the client went to the regulator instead. That is where day-to-day supervisory exposure comes from, and MiCA now regulates it directly. Article 71 requires effective and transparent procedures for the prompt, fair and consistent handling of complaints, free of charge, and RTS 2025/294 specifies the template, the languages and the records.

What Article 71 and the RTS require

Requirement	Implementation
A published complaints procedure	On the website, clear and current
The standard complaint template	From the RTS annex, on the website and on request; complaints accepted in any form
Free of charge	No fee at any step
Languages	Every language you use to market or communicate with clients
Acknowledgement and	Prompt written acknowledgement with a reference and the expected timeline; final

Requirement	Implementation
timelines	written response within the published period; interim explanation where longer
Register	Every complaint and the measures taken, retained under Article 68(9), available to the NCA
Analysis	Root-cause analysis; complaints data reported to the management body; feedback into product, support and compliance

The three control mechanisms in this pillar

Mechanism	What to build
Complaints handling under Article 71	The procedure, the template, the register with supervisory-grade metadata, and the timelines, owned by support with compliance as Tier 3
Support-to-compliance handoff	A tagging taxonomy and keyword triggers that route regulator references, legal threats, fund-access complaints, fraud signals and data-protection requests to Tier 2 or 3 in real time, with an audit trail
Incident response and disclosure	A joint playbook for support, security and compliance with decision trees for the first 24 hours, aligned with DORA incident classification and GDPR breach notification

Template: complaint severity and response rubric

Severity	Definition	Response standard
S0	Informational query	Standard support SLA; no register entry
S1	Service complaint, no regulator mentioned	Acknowledge within one business day; final response within the published timeline; register entry
S2	Regulator, ombudsman, lawyer or consumer authority mentioned	Same-day escalation to the complaints owner; Article 71 clock running; root cause within ten business days
S3	Allegation of misconduct, fraud, or a sanctions or AML signal	Handoff to compliance within four hours; evidence preserved; STR assessment. For AML-driven restrictions, neutral approved script only: the tipping-off prohibition applies
S4	Market abuse signal, ICT incident, or data breach indication	Incident playbook; DORA classification within the four-hour window where major; GDPR notification within 72 hours where applicable

Keyword triggers worth configuring on day one, in English and in every market language: the names of the NCAs (BaFin, AMF, AFM, CBI, CSSF), "regulator", "ombudsman", "lawyer", "complaint", "cannot withdraw", "funds locked", "hacked", "unauthorized", "GDPR", "my data".

Implementation checklist

- Article 71 procedure and template published in every required language.
- Complaints register configured with the RTS fields: receipt, acknowledgement, response, category, root cause, outcome, external escalation.
- Keyword routing sends S2 and above to Tier 2 or 3 automatically.

- Support trained on the S0 to S4 rubric and on the two handling paths for restrictions (AML-driven: neutral script; non-AML: specific resolution steps).
- Monthly complaint intelligence report to compliance, product and the CEO; standing section in the quarterly compliance report.
- External escalation rate tracked; target under 2 percent of tickets.

WHAT THIS GETS YOU

Fewer complaints reach the competent authority because they were resolved inside the company within the published window. And when a supervisor inspects the complaints file, the register is already in the form the RTS expects, which is one of the cheapest ways there is to build credibility with your regulator.

IV. Pillar 3: Partner-Led Growth

The thesis, and what MiCA actually allows

Rebuilding every authorization in every market is slow, expensive and usually unnecessary. Most operators scale faster by working with already-authorized CASPs, credit institutions, EMIs and distribution partners, and governing those relationships properly.

One point most market entrants get wrong, and it decides whether the structure survives supervisory review: MiCA has no agent, tied-agent or appointed-representative regime for crypto-asset services. ESMA confirmed in its Q&A that a CASP cannot designate a third party to provide crypto-asset services on its behalf; a party that receives or transmits orders, advises or holds client assets must itself be a CASP. The MiFID II tied-agent model does not carry over. What MiCA does allow is a CASP outsourcing operational functions under Article 73 while remaining fully responsible, and using third parties for marketing under Articles 66 and 7. Every workable white-label structure in the EU is built on those two provisions.

Permitted and not permitted for the unauthorized partner

The company may	Only the authorized CASP may
Build and operate the technology and user interface under the CASP's oversight	Contract with the client and be the provider of record
Market the CASP's service under its approval and with the agreed wording	Decide to onboard, restrict or terminate a client
Collect identity data through the CASP-approved flow	Approve or reject KYC; apply enhanced due diligence
Run monitoring rules configured by the CASP and surface alerts	Decide on alerts and file STRs with the FIU
Provide first-line support and the first step of the complaints process	Own the Article 71 procedure and the final response
Prepare data and draft reports	Report to the NCA, the FIU and the AML supervisor
Provide ICT services as a third party in the CASP's DORA register	Own the DORA framework and notify major incidents

The company may	Only the authorized CASP may
Refer institutional prospects	Receive, transmit or execute orders; advise; manage portfolios; hold client assets

The three-stage model

Stage	Objective	Partner	Outcome
1. White-label CASP	Start regulated operations within weeks	An authorized CASP with the permissions the product needs, under an Article 73 outsourcing agreement	Clients onboarded as the CASP's clients; revenue; a supervised track record
2. Banking-grade partner	Raise credibility with the NCA and the market	A credit institution providing crypto-asset services under Article 60	A supervised bank has run due diligence on the company and put its name on the operation
3. Own authorization	Operate independently	None	Clients migrated; partner relationships continue commercially where useful

Template: the seven-dimension partner scorecard

Score each dimension 0 to 3 before contracting. Below 2.0 on average, or a zero on any dimension, means the partner is not ready.

Dimension	What you are checking	Evidence required
1. Permissions	Authorized for the exact services and member states you need	ESMA register entry, authorization decision, passport notifications
2. Management and ownership	Management body and qualifying holders fit and proper	Suitability documentation, transparency register check
3. Capital and stability	Can absorb operational shocks	Audited financials, own funds report
4. Operational maturity	Operates at the service level you need	SLA history, uptime, incident log, continuity test results
5. AML and sanctions	Controls at or above your own	Policy set, risk assessment, independent review
6. Data protection and resilience	GDPR, DORA and ICT posture	Processor agreement, SOC 2 or ISO 27001, penetration test summary
7. Substance and exit	Retains the competence to oversee the arrangement; you can leave without breakage	Named oversight staff at the partner; documented exit plan; data portability; transition support

Outsourcing and oversight checklist, Article 73

- Outsourcing policy covering approval, oversight and termination.
- Outsourcing register listing every arrangement: provider, function, criticality, contract reference, notification status, audit rights, exit plan, last review.

- Written agreement with scope, service levels, audit rights for the CASP and its NCA, sub-outsourcing controls, data protection terms and exit assistance.
- NCA notified where the home member state requires it for critical or important functions.
- Substance retained: the CASP's own staff understand, monitor and can take back every outsourced function.
- Responsibility matrix annexed to the agreement, with a "permitted for the unauthorized partner" column for every function.
- Exit plan tested or tabletop-exercised at least once a year.

THE LEVERAGE

Partner-led growth works only where the oversight is real. Firms that do it badly end up owning every failure of a partner without the authority to fix it, and a supervisor that concludes the CASP has outsourced its business rather than its functions will act. Firms that do it well turn every partner into a controlled channel that scales with their brand.

V. Pillar 4: Compliant Growth Operations

The thesis

This is where most frameworks give up. Marketing wants to ship a campaign, product wants to list a token, BD wants to sign an institutional partner by Friday, and all three end up in a weekly escalation queue with legal. CLGF replaces the queue with a three-lane approval flow: routine work never touches legal, elevated work runs through compliance, and only novel work reaches counsel.

MiCA makes this buildable because it states what marketing has to get right. Article 66(2) requires information to clients, including marketing communications, to be fair, clear and not misleading and identified as marketing; Article 66(3) requires a risk warning; Article 7 requires marketing for a crypto-asset offer to be consistent with the whitepaper and, where the NCA asks, notified in advance. Encode those into a checklist and the growth team has a rule set it can run on.

Growth by authorization phase

Phase	Status	What is permitted
Pre-authorization, no partner	Nothing regulated	Audience, education, waitlist with GDPR consent. No onboarding, no transactions, no promotion of regulated services
White-label under a partner	An authorized CASP is provider of record	Real clients and revenue as the partner's clients; full marketing within the partner's approval and with the partner named as provider
Own authorization	CASP authorization and passports	Full flexibility within the scope of the authorization; own authorization on every client surface

A plan that relies on reverse solicitation to delay authorization does not survive review. The ESMA guidelines treat any marketing with EU reach as solicitation.

The three-lane approval flow

Lane	What it covers	Who approves
Green	Routine marketing within pre-approved templates; minor product updates; existing partner renewals; complaint responses on standard templates	Line manager; no legal review
Amber	New campaigns, new member states, new partners, new product features, complaints with a regulator mentioned	Compliance officer, 24-hour SLA (plus partner review in the white-label phase)
Red	New product classifications, token listings requiring a whitepaper, institutional deals above a defined threshold, anything requiring management body attention	Counsel and the relevant management body member

Template: the marketing pre-publish checklist

- The communication is identifiable as marketing (Art. 66(2)).
- Information is fair, clear and not misleading on risks, fees and past performance (Art. 66(2)).
- The risk warning is present and visible, in the wording confirmed with the home NCA (Art. 66(3)).
- Where a whitepaper exists, the communication is consistent with it and, where required, notified to the NCA (Art. 7).
- No yield, return or performance claim; no comparison with banks or securities; no urgency or scarcity language.
- No targeting of member states outside the authorization or passport.
- Influencer and affiliate content is disclosed and pre-approved; any affiliate performing onboarding steps sits in the outsourcing register.
- Every channel used appears in the programme of operations filed with the NCA.
- Approver signature from the correct lane, and the asset archived with its approval chain.

Launch readiness checklist

Pre-launch: classification memo (crypto-asset, ART, EMT, financial instrument); whitepaper notified where required; marketing through the checklist; complaints procedure updated for the new product; market abuse surveillance extended; DORA impact assessed.

Launch week: support briefed on the product and the severity rubric; compliance on call for 72 hours; incident decision tree live with named owners.

Post-launch: first complaint report reviewed within fourteen days; market abuse alerting tuned to actual behavior; any supervisory query closed out with actions tracked.

THE OUTCOME

When the flow works, marketing, product and BD ship without waiting on legal, legal handles only the novel questions, and compliance runs the green lane at full speed.

VI. Implementation: The Operator Sprint

Twenty weeks, four phases, signed gates

CLGF is installed through a twenty-week operator sprint (module P05 in the full framework) with a signed gate at the end of each phase, so the company owns a working operation at the end rather than a report about one.

Phase	Weeks	Focus	Gate
1. Diagnostic	1 to 3	Gap analysis across the twenty-four domains; licensing roadmap and reverse solicitation gate; KPI baseline; partner shortlist; scope	Scope document signed by the CEO
2. Design	4 to 6	Policy pack in draft including the MiCA control domains and DORA; funnel and marketing design; support design; partner agreement; vendors contracted; application index	All designs approved
3. Execution	7 to 16	Eight parallel workstreams: compliance, authorization application, licensed partner, growth, support, localization, DORA, monitoring and reporting. Mid-sprint review at week 12	Application filed; systems live
4. Transition	17 to 20	Training and certification; SOP library; ownership matrix; handover sessions; governance calendar	Final report and ownership matrix signed

KPIs from day one

KPI	Owner	Target
Complaints acknowledged within one business day and answered within the published timeline	Head of Support	100 percent
S2 and above escalated to compliance same day	Head of Support	100 percent
External complaint rate	Head of Support	Under 2 percent of tickets
Partners covered by a current scorecard and outsourcing register entry	Head of BD	100 percent
Marketing shipped through the green lane without rework	Head of Growth	80 percent after month three
Gap analysis maturity score	Head of Compliance	2.5 of 3.0 or higher; no applicable domain below 2 before submission
DORA major-incident path tested; register of information current	CTO	Before the sprint exits

A NOTE ON SEQUENCE

The companies that stall are the ones that start with Pillar 4 because it is the most visible. Without the first three pillars, the growth lane approves activity the company cannot defend in front of a supervisor. 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 forward.

1. Score your readiness in fifteen minutes, free

The CLGF diagnostic at framework.thiessinvest.com walks you through all twenty-four control domains and produces a maturity score, a severity breakdown and a prioritized remediation roadmap on the same scale the full framework uses. Your answers stay in your browser until you choose to send them.

2. Run the framework with Thiess Invest

When you are ready to build, we run the operator sprint with you: the gap analysis, the authorization application pack, the compliance stack, the partner structure, the support operation, the growth workflow and the handover. Engagements are scoped to what the company actually needs, and I work directly with founders and management bodies rather than through layers of junior consultants.

Start a conversation at thiessinvest.com or marcel.thiess@thiessinvest.com.

A CLOSING NOTE

Six to nine months of legal work will not get you into Europe. Entering the EU under MiCA is a multi-quarter operational project: the control environment, the documentation, the team knowledge and the operating culture that competent authorities require. The companies that understand this early spend less, move faster and get authorized. CLGF is the system I built to get them there.

About the Author

Marcel Thiess

Marcel Thiess is a crypto and fintech executive with more than eight years of operational and advisory experience across major exchanges, market makers, custody providers and infrastructure businesses. He has led compliance and customer-facing functions at scale, worked on authorization across EU member states, and advises companies preparing for CASP authorization and ongoing MiCA supervision. He is the creator of the Compliance-Led Growth Framework.

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

Thiess Invest GmbH

Thiess Invest GmbH is the advisory practice behind CLGF. It works with exchanges, infrastructure providers and fintechs on regulatory readiness, partner-led growth and compliant growth operations under MiCA, engaging directly with founders and management bodies.

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