WHITEPAPER · IMPLEMENTATION GUIDE

Implementing a compliance *strategy*

From the boardroom decision to daily operations — a practical playbook for embedding product compliance, with models and ready-to-use templates.

---

conphora Retailer-ready EU product compliance

EXECUTIVE SUMMARY

Compliance is built, *not bought.*

Most organisations discover compliance the hard way — as a fire to put out when a retailer, marketplace or authority asks for proof. Buying a tool does not fix that; compliance becomes durable only when it is built into how the company decides, staffs, structures its data and runs day-to-day. This paper is a practical playbook for doing exactly that.

It follows the implementation arc that successful programmes share — from the leadership decision, through the business case, people, and data, to operations — and it is grounded in the recognised standards for the field: the ISO 37301 compliance-management-system model and the IIA Three Lines Model for governance. Throughout, you will find models to copy and templates to fill in.

Models & templates in this paper

- **Models:** the implementation arc · the Three Lines governance model · the compliance data model · the continuous-compliance (PDCA) loop · a maturity model · a prioritisation matrix.
- **Templates:** compliance policy · business case · RACI matrix · product-data fields · supplier compliance request · implementation roadmap · KPI scorecard · compliance register.

The implementation arc

Compliance programmes that stick move through five connected stages. Skip one and the others wobble: a tool with no mandate is ignored; a mandate with no data has nothing to act on; data with no operating rhythm goes stale.

The implementation arc — five connected stages, from leadership mandate to daily operations.

The rest of this paper takes each stage in turn. A note on language: we use *compliance management system (CMS)* in the sense of ISO 37301 — the set of policies, roles, data and processes by which an organisation meets its obligations — not a single piece of software.

Stage 1 — The leadership decision

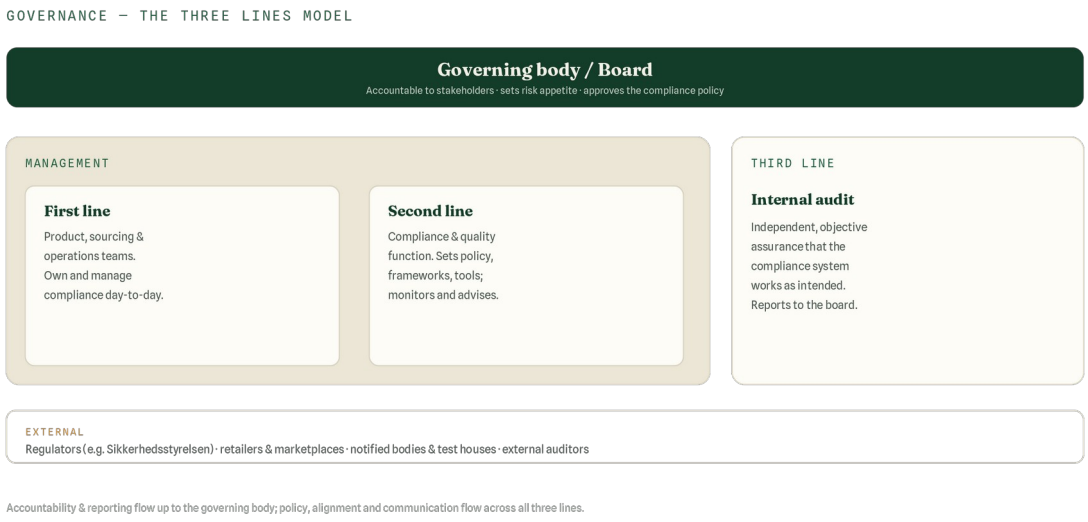
Compliance starts at the top or it does not start at all. ISO 37301 places leadership, governance and culture at the centre of the management system for a reason: without a clear mandate, a stated risk appetite and visible sponsorship, compliance work is always the task that loses to the next deadline.

What leadership must decide

- **A mandate and sponsor.** Name an executive accountable for compliance and give the programme explicit authority and budget.
- **Risk appetite.** State plainly how much non-compliance risk the business will tolerate — by market, channel and product category.
- **A compliance policy.** A short, board-approved statement of commitment, scope, roles and reporting — the constitution everything else hangs from.

The governance model

Use the IIA Three Lines Model to assign who does what. The first line (product, sourcing and operations) owns and manages compliance in daily work. The second line (a compliance/quality function) sets policy, frameworks and monitoring. The third line (internal audit) provides independent assurance. The governing body sits above all three, accountable to stakeholders and external bodies — regulators, retailers and notified bodies — sit outside.



Governance — the IIA Three Lines Model adapted for product compliance.

Template — Compliance policy (one page)

Purpose. Why the organisation is committed to product compliance.

Scope. Which products, brands, markets and channels the policy covers.

Commitment. A statement that the organisation will meet all applicable EU product requirements and act on breaches.

Roles & responsibilities. Sponsor, compliance owner, first/second/third-line duties (see RACI).

Risk appetite. The level of risk tolerated, by category and market.

Reporting & escalation. How issues are raised, to whom, and how fast.

Review. Cadence of review (e.g. annually) and trigger events.

Approval. Approved by [governing body] on [date]; owner [name].

Stage 2 — The business decision

With a mandate in place, compliance becomes a business case like any other: scope it, prioritise it, choose how to resource it, and define what success looks like.

Prioritise where it matters

You cannot do everything at once. Rank products and markets by exposure — combining regulatory/recall risk with revenue at stake — and start where both are high.

	High revenue	Lower revenue
High risk	Prioritise first — most to lose. Validate and document now.	Schedule next — material risk, protect proactively.
Lower risk	Quick wins — easy coverage, visible progress.	Monitor — automate and review periodically.

Build, buy or outsource

Three resourcing models, usually combined: build an in-house function (control, but slow and costly to hire); buy a platform that automates classification, validation and documentation (fast, scalable); or outsource to a managed service (capability without headcount). Most brands buy the platform and add managed support where judgment is needed.

Template — Compliance business case

Field	What to capture
Objective	The outcome (e.g. retailer-ready across top 3 markets in 90 days).
In scope	Products, brands, markets and channels covered first.
Options considered	Build in-house · buy a platform · outsource (managed).
Recommended option	The choice and why.
Budget	One-off and ongoing cost (capex / opex).
Expected benefits	Faster onboarding, fewer delistings/recalls, trust premium.
Success metrics	See KPI scorecard.
Risks & assumptions	Key risks and how they are mitigated.
Decision & owner	Approved by [name] on [date].

Stage 3 — People & responsibilities

Compliance fails quietly when everyone assumes someone else owns it. Make ownership explicit, give people the skills, and build a culture where raising an issue is rewarded, not punished.

Assign ownership with a RACI

A RACI matrix maps each activity to who is Responsible, Accountable, Consulted and Informed. Adapt the template below to your structure — the point is that every row has exactly one Accountable.

Activity	Sponsor	Compliance	Product team	Audit
Set policy & risk appetite	A	R	I	I
Classify products to rules	I	A	R	—
Validate vs requirements	I	A	R	—
Remediate gaps	I	C	R	—
Generate documentation	I	A	R	—
Appoint responsible person	A	R	C	I
Monitor regulatory change	I	A	C	I
Independent assurance	I	I	I	A/R

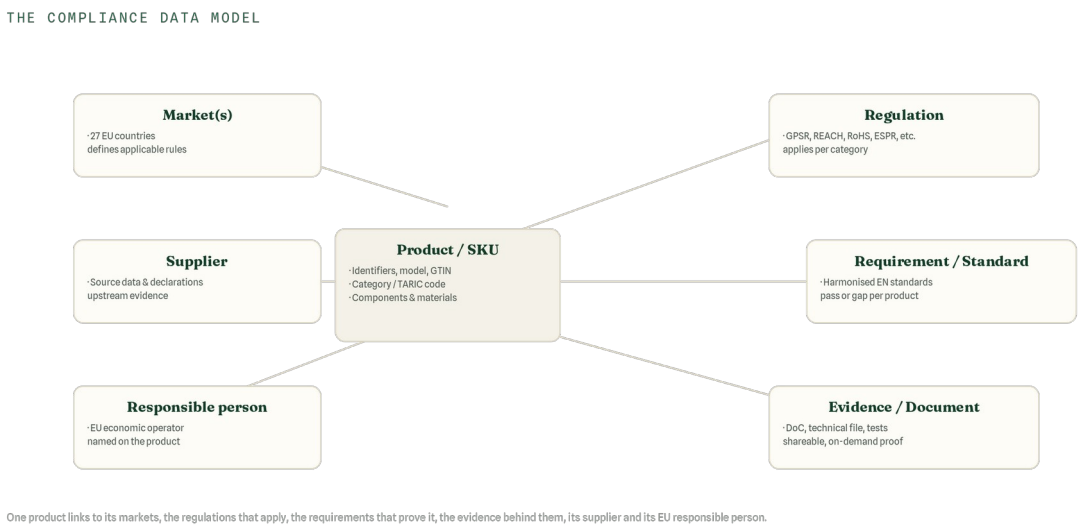
R = Responsible · A = Accountable · C = Consulted · I = Informed. Where you lack in-house capacity, a platform or managed service can hold the Responsible role while your team stays Accountable.

Skills & culture

- Train product and sourcing teams on the basics: what a DoC is, what a responsible person does, what triggers a regulation.
- Make compliance status visible in the tools people already use, so it is part of the workflow — not a separate chore.
- Reward early flagging of gaps. A culture that hides problems is the single biggest risk to any compliance system.

Stage 4 — Data & systems

Compliance is, underneath, a data problem. You cannot prove what you cannot describe. The foundation is a single source of truth that connects each product to the markets it sells in, the rules that apply, the requirements that prove it, and the evidence behind them.



The compliance data model — one product linked to its markets, rules, requirements, evidence, supplier and responsible person.

Get the product data right

Classification is where most programmes stall. Capture a consistent set of fields per product so the system can match each SKU to the regulations and harmonised standards that apply.

Template — Product data fields

Field	Example / note
Product ID / SKU	Internal identifier
Model name & GTIN/EAN	For traceability and labelling
Category & TARIC code	Drives which rules apply
Target markets	Which of the 27 EU countries
Components & materials	Bill of materials
Substances	For REACH / RoHS screening
Supplier	Source of upstream evidence
Responsible person	EU economic operator
Applicable regulations	Auto-matched (GPSR, REACH, …)
Status & evidence	% complete; links to DoC, tests

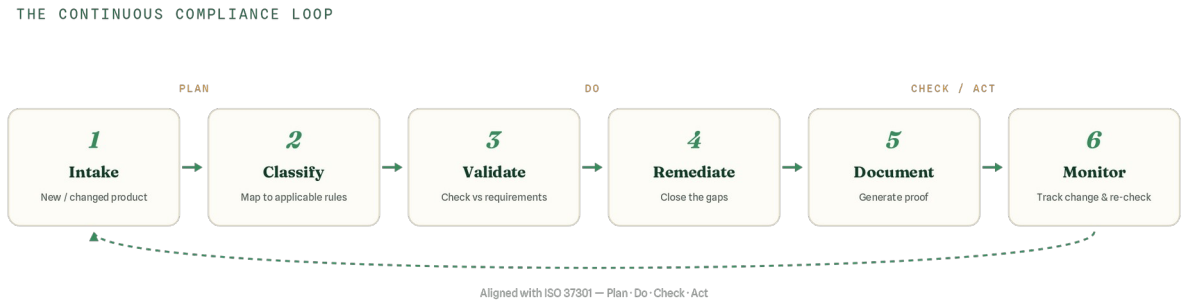
Template — Supplier compliance request

Send this checklist to suppliers at onboarding; prefer third-party-verified documents over self-declarations.

Item to request from supplier	Required?
Declaration of Conformity (DoC)	Yes
Test reports (accredited lab)	Yes, risk-based
Material declarations (REACH/RoHS)	Yes
Bill of materials	Yes
Conformity to harmonised standards	Yes
Country of origin / EUDR data	If applicable
Responsible-person details	Yes
Labelling & marking artwork	Yes

Stage 5 — Operations & continuous compliance

Compliance is not a project that ends; it is an operating rhythm. ISO 37301 is built on the Plan-Do-Check-Act cycle, and a working programme runs the same loop continuously for every product.



The continuous-compliance loop — intake to monitoring, aligned with ISO 37301's Plan-Do-Check-Act.

Run the loop

- **Intake & classify.** Every new or changed product enters the system and is matched to applicable rules.
- **Validate & remediate.** Check against requirements, see the gaps, and close them.
- **Document.** Generate the DoC, technical file and a shareable compliance status — ready before a retailer asks.
- **Monitor.** Track regulatory change and re-validate automatically, so a new requirement is an alert, not an emergency.

Template — Compliance register

Maintain a living register so status is auditable at any moment.

Product	Market	Regulation	Status	Owner
Desk lamp (SKU-1042)	DE	LVD / RoHS / GPSR	Compliant	Product
Night light (SKU-3391)	FR	GPSR / EN 71	Gap — labelling	Product
[add row]	—	—	—	—

Be ready for the bad day

Operations also means readiness: a defined process for a recall or a Safety Gate alert, with the responsible person, documentation and corrective-action steps already in place. The brands that survive an incident are the ones that prepared for it before it happened.

Know where you stand

Before you plan, locate yourself. The jump that matters most is from Compliant to Retailer-ready — the point where compliance stops being a bottleneck and becomes a sales tool.

Stage	What it looks like	Outcome
1 · Reactive	Handled per crisis; spreadsheets and last-minute calls.	Stalled listings, surprise costs, exposure.
2 · Compliant	Products meet the rules, but proof is manual and slow.	Survives audits; compliance is a bottleneck.
3 · Retailer-ready	Complete, current documentation per product and market.	Faster onboarding, fewer stalls, reliable reputation.
4 · Advantaged	Continuous, data-driven; transparency used in marketing.	Speed-to-shelf, trust premium, first-mover on new rules.

The roadmap

A pragmatic sequence gets a brand from reactive to retailer-ready in about a quarter, then into continuous improvement. Adapt the timing to your size and catalogue.

Phase	Timing	Focus	Output
0 · Mobilise	Week 0–2	Mandate, sponsor, policy, scope, risk appetite.	Approved policy; named owner.
1 · Foundation	Week 2–6	Data model, product import, RACI, supplier requests.	Single source of truth; roles set.
2 · Operationalise	Week 6–12	Validate priority products, close gaps, generate docs.	Priority catalogue retailer-ready.
3 · Optimise	Ongoing	Monitor change, audit, extend coverage, use in sales.	Continuous compliance; KPIs tracked.

Measuring success

What gets measured gets done. Track a small set of KPIs that link compliance to the business.

KPI	Definition	Target
Coverage	Share of catalogue validated against applicable rules.	→ 100%
Time-to-documentation	Avg. days to produce a retailer-ready pack.	< 2 days
Open gaps	Number of unresolved requirement gaps.	Trending to 0
Audit pass rate	Share of products passing internal/external audit.	> 95%
Speed-to-shelf	Avg. days from buyer request to listing-ready.	Falling
Change actioned	Regulatory changes assessed within SLA.	100%

Pitfalls & success factors

Avoid

- Buying a tool with no mandate, owner or operating rhythm behind it.
- Trying to cover the whole catalogue at once instead of prioritising by risk and revenue.
- Treating documentation as a one-off, not a living, monitored register.

Do

- Start at the top, scope tightly, and show a retailer-ready win fast.
- Make one person Accountable for every activity, and make status visible.
- Automate the repeatable work so people spend their time on judgment, not admin.

From obligation to *capability*

Implementing a compliance strategy is an operating change, not a purchase. Decide it at the top, make the business case, assign clear ownership, build the data foundation, and run the loop. Do that, and compliance stops being the thing that slows you down — and becomes the thing that gets you on the shelf, keeps you there, and turns every new regulation into a feature you already have.

How Conphora helps

Conphora is the platform and managed service behind this playbook. It gives you the compliance data model out of the box, validates your catalogue against 48 EU regulations across 27 countries, runs the continuous-compliance loop, and generates the documentation and shareable status retailers require. Use it self-service, or let our team operate it for you. Learn more at conphora.com.

Sources & references

1 ISO 37301:2021 — Compliance management systems: requirements with guidance for use (PDCA; replaces ISO 19600:2014). ISO

2 The Institute of Internal Auditors — The Three Lines Model (2020 update of the Three Lines of Defense). IIA

3 Regulation (EU) 2023/988 — General Product Safety Regulation (GPSR). EUR-Lex

4 Regulation (EU) 2024/1781 — Ecodesign for Sustainable Products Regulation (ESPR) & Digital Product Passport. EUR-Lex

5 European Commission — Safety Gate Rapid Alert System (annual report). EC