RADARFIRST COMPLIANCE MATURITY BENCHMARK

This benchmark helps you see where your program stands today across Privacy, Control management, and AI Risk. Proactively building maturity now (like creating incident and AI system inventories) will make you more resilient and ready for governance tomorrow.

For each area, review the descriptions across the maturity levels and check the box that best represents your current state. If helpful, bring this worksheet to a follow-up meeting with RadarFirst to explore your path forward.

Compliance Area	Ad Hoc	Foundational	Operationalized	Predictive
Executive Confidence	No formal ownership; reactive board responses (high risk exposure)	Basic executive awareness; some reports shared	Regular compliance updates to executives/board	Proactive leadership; compliance drives strategic decisions (board-ready, competitive advantage)
Cross-Functional Alignment	Teams work in silos with unclear roles	Roles defined for privacy teams	Cross-functional reviews and collaboration norms	Integrated collaboration across privacy, legal, IT, risk (enterprise-wide resilience)
System of Record / Auditability	Documents stored in spreadsheets/emails (inconsistent, hard to defend)	Centralized storage for key decisions and records	Dedicated system of record for privacy/AI decisions (consistent, scalable, auditable)	Full audit trails with traceable logic and timestamps (trusted, board-ready)
Real-Time Visibility	Visibility only during audits or incidents	Basic dashboards or summaries updated quarterly	Live dashboards tracking core compliance areas	Predictive alerts for risk hotspots and compliance gaps
Clause-Level Mapping (Controls)	Manual mapping (if any), often inconsistent	Manual mapping in spreadsheets with some consistency (defensible coverage)	Mapped to frameworks like NIST, GDPR, CCPA	Fully automated clause-level mapping across domains (continuous readiness)

RADARFIRST COMPLIANCE MATURITY BENCHMARK

Compliance Area	Ad Hoc	Foundational	Operationalized	Predictive
AI Governance Readiness	No clear plan or framework (high exposure)	Initial exploration of frameworks (EU AI Act, NIST)	Documented AI policies, draft governance playbooks (scalable, defensible)	AI systems designed with a governance-by-default approach (future-proof)
Automation of Compliance Tasks	Compliance tasks handled manually (slow, error-prone)	Some processes are templated or checklist-driven	Automation in monitoring, reporting, and task assignment	AI-powered orchestration and predictive risk scoring (efficiency)
Defensibility Under Regulatory Review	Inconsistent documentation; hard to defend (penalty risk)	Basic defensibility for critical processes	Can respond to regulator queries in days, with evidence (confidence grows with external stakeholders)	Board-ready insights delivered in real time (compliance as a strategic asset)

WHAT'S NEXT?

You can use the above as a blueprint for what comes next. If your organization is strong in Privacy, the next step is to expand to Controls management.
If you're strong in both, you're well-positioned to bridge into AI Risk.
Together, these stages help form a connected compliance journey.

After completing the above, check out our Compliance Readiness Checklist to test your readiness and identify quick wins.

RadarFirst