Kiteworks

EUROPE EXECUTIVE SUMMARY

Data Security and Compliance Risk: 2026 Forecast Report

World-Class Regulations, Second-Tier Operations: Why Europe's Compliance Leaders Are Becoming Operationalisation Laggards

Five Gap-Driven Predictions and Strategic Recommendations

European organisations enter 2026 with strong regulatory foundations but critical operational gaps. Whilst GDPR and the emerging EU AI Act have established comprehensive compliance frameworks, the data reveals European enterprises lag global benchmarks on the capabilities needed to operationalise those frameworks—particularly in AI incident response, software supply chain visibility, third-party risk management, and compliance automation.

The gap isn't in policy. It's in proof. European organisations have built the documentation and governance structures; what they lack are the automated, evidence-generating systems to demonstrate continuous compliance in real time. As AI adoption accelerates across the region and cross-border data flows multiply under increasing regulatory scrutiny, this operational gap will become increasingly untenable.

This regional analysis draws from a survey of 225 security, IT, compliance, and risk leaders globally, with specific breakouts for France, Germany, and the United Kingdom. The findings reveal consistent patterns: European organisations trail global averages on AI-specific incident response capabilities, software supply chain controls, third-party governance mechanisms, and compliance automation. Five predictions emerge from these gaps—not as speculation, but as data-driven projections of where European organisations will find themselves exposed in 2026 if current trajectories continue.

Five Predictions for Europe in 2026

1. AI-specific incident response will lag other regions
2. Software supply-chain controls will remain half-built
3. Third-party controls will stay conservative—especially joint playbooks
4. Compliance operations will remain more manual than global peers
5. European firms will under-weight third-party AI and cross-border AI risks

Europe vs. Global: Key Capability Gaps

Capability	Global	France	Germany	U.K.
AI anomaly detection	40%	32%	35%	37%
Training-data recovery	47%	40%	45%	44%
SBOM management	28%	20%	25%	23%
Joint incident playbooks	13%	**4%**	25%	9%
Cross-border mechanisms	55-62%*	~30%	~28%	~32%

Green *= above global average.* ***Yellow*** *= at or below global average, indicating governance gap.*
**Global benchmark reflects Middle East (Saudi/UAE) leaders.*

Five Gap-Driven Predictions for Europe in 2026

Prediction #1: Europe's AI-Specific Incident Response Will Lag Other Regions

By 2026, many European organisations will still have incomplete AI-specific incident response capabilities, especially around anomaly detection and training-data recovery.

AI IR Capability	Global	France	Germany	U.K.
AI anomaly detection	40%	32%	35%	37%
Training-data recovery	47%	40%	45%	44%

The data tells a consistent story across all three European markets. For AI anomaly detection, France sits at 32%, Germany at 35%, and the U.K. at 37%—all trailing the 40% global benchmark. Training-data recovery shows the same pattern: France at 40%, Germany at 45%, and the U.K. at 44%, all below the 47% global average. These aren't marginal gaps; they represent fundamental incident response capabilities that European organisations haven't prioritised relative to global peers.

The implications are significant. When an AI model behaves unexpectedly—producing biased outputs, accessing data outside its intended scope, or failing in production—European organisations are less equipped than their global counterparts to detect the anomaly and recover the training data needed to diagnose the root cause. Traditional IR playbooks built for conventional IT incidents don't address these AI-specific failure modes.

Key Insight

Traditional backup and logging strategies won't address AI-specific failure modes. European organisations need purpose-built detection and recovery capabilities for model behaviour anomalies.

Opportunity

Build AI-aware IR playbooks that address model-specific failure modes. Invest in anomaly detection specific to model behaviour and establish training-data remediation procedures—not just traditional backups and logs.

Prediction #2: European Software Supply-Chain Controls Will Remain Half-Built

By 2026, European enterprises will still show partial SBOM and supply-chain coverage, trailing more aggressive regions by a significant margin.

Supply Chain Control	Global	France	Germany	U.K.	Leaders*
SBOM management	28%	20%	25%	23%	45%+
Secure SDLC	41%	32%	45%	37%	65%

**Leaders = Australia/UAE*

SBOM management reveals the gap starkly: The global average sits at 28%, but France reaches only 20%, Germany 25%, and the U.K. 23%. For secure SDLC practices, the picture is mixed—Germany performs relatively well at 45%, but France lags at 32% and the U.K. at 37%. Meanwhile, Australia and UAE both achieve 65% on secure SDLC metrics, more than double some European rates.

Europe's supply-chain visibility problem isn't just a gap—it's a generation behind the leaders. As AI models increasingly rely on third-party components, training datasets, and external APIs, the inability to maintain comprehensive SBOMs creates blind spots that compound with every integration. Organisations can't secure what they can't see, and European enterprises see less than their peers.

Opportunity

Close the SBOM gap by pushing continuous dependency monitoring and real-time threat intelligence into the same maturity tier as code scanning and SDLC. Treat supply-chain visibility as critical infrastructure, not a nice-to-have capability.

Prediction #3: Third-Party Controls Will Stay Conservative—Especially Joint Playbooks

By 2026, Europe will still under-invest in continuous vendor risk monitoring and joint incident playbooks, leaving third-party programmes reactive rather than proactive.

Third-Party Control	Global	France	Germany	U.K.
Continuous vendor monitoring	35%	32%	35%	28%
Joint incident playbooks	13%	**4%**	25%	9%

The joint incident playbook numbers are particularly striking. The global average is already low at 13%, but France sits at just 4% and the U.K. at 9%. Even Germany, the regional leader in this category at 25%, represents only one in four organisations with formal joint IR arrangements with their vendors. Continuous vendor risk monitoring shows a similar pattern: France at 32% and the U.K. at 28%, with only Germany matching the 35% global average.

The Gap

Only 4% of French organisations have joint incident playbooks with third-party vendors. When a vendor incident occurs—and with AI-enabled supply chains, it will—**96%** will be improvising their response in real time.

Opportunity

Use Europe's strong regulatory culture to justify formal joint playbooks and shared tabletop exercises with critical vendors. GDPR already requires vendor oversight; extending that to joint IR planning is a natural evolution that's clearly under-implemented.

Prediction #4: Compliance Operations Will Remain More Manual Than Global Peers

By 2026, many European organisations will still lean on manual or semi-manual compliance processes, limiting their ability to prove near real-time control effectiveness.

Compliance Approach	Global	France	Germany
Automated/policy-as-code	43%	40%	35%
Continuous/partial automation	32%	36%	40%
Periodic manual	10%	12%	15%

The pattern shows European organisations clustering in "continuous but manual" compliance rather than true automation. Whilst this approach maintains oversight, it doesn't scale to meet the demands of EU AI Act enforcement or expanding GDPR scope. Manual compliance processes can't generate the real-time evidence that regulators increasingly expect.

Opportunity

Shift from "continuous but manual" to actual policy-as-code implementations, particularly around AI systems and cross-border data processing. Automated compliance evidence generation will be essential as regulatory scrutiny intensifies.

Prediction #5: European Firms Will Under-Weight Third-Party AI and Cross-Border AI Risks

By 2026, many European organisations will still underestimate vendor AI risk and cross-border AI exposure relative to other regions—despite operating under the world's most comprehensive data protection regime.

Cross-Border AI Governance	Europe	Middle East*
Cross-border mechanisms in workflows	28-32%	55-62%
Third-party AI vendor risk (top concern)	26-30%	30% (global avg.)

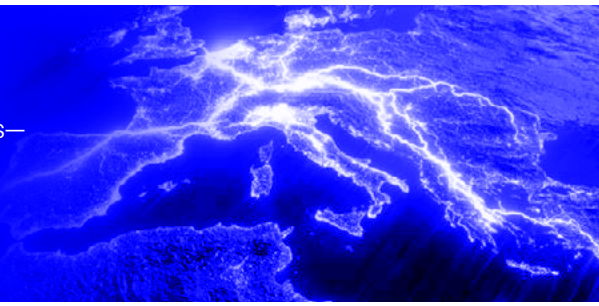
**Middle East = Saudi Arabia/UAE*

European organisations rank third-party AI vendor risk as a top concern at rates near the global average (France 28%, Germany 30%, U.K. 26% vs. 30% global). Recognition of the risk isn't the problem. Operationalisation is.

On implementing cross-border data mechanisms, European organisations sit at just 28-32% adoption—whilst Middle East regions (Saudi Arabia, UAE) reach 55-62%. This gap is striking given GDPR's extensive cross-border provisions. European organisations operate under regulations that demand cross-border data governance, yet they aren't operationalising those requirements at rates their regulatory environment demands. As AI systems increasingly process data across jurisdictions, this implementation gap becomes a compliance liability.

Opportunity

Treat AI vendors and cross-border AI processing as first-class risk domains—not just extensions of general GDPR compliance. The EU AI Act will require this approach regardless; organisations that move early gain operational advantage and avoid the scramble when enforcement begins.



Strategic Recommendations for European Organisations

The data points to five priority investments for European organisations preparing for 2026. These aren't aspirational goals—they're gap-closing measures required to reach parity with global peers and meet the operational demands of Europe's evolving regulatory landscape.

1. Build AI-Specific Incident Response Capabilities

Traditional IR playbooks don't address AI failure modes. Invest in anomaly detection specific to model behaviour, establish training-data recovery procedures, and build response protocols for AI-specific incidents. The 5-8 point gap versus global averages represents real exposure that conventional IT security measures won't address.

2. Close the SBOM Gap Aggressively

At 20-25% SBOM adoption versus 65% in leading regions, European organisations face a visibility deficit that compounds with every AI model and third-party integration. Make SBOM management a prerequisite for new AI deployments. Require dependency documentation as a procurement condition. Treat supply-chain visibility as critical infrastructure.

3. Formalise Third-Party IR Relationships

Joint incident playbooks at 4-9% (France/U.K.) versus 13% global is a liability waiting to be exposed. Use existing GDPR vendor management requirements as leverage to establish formal joint playbooks. Conduct annual tabletop exercises with critical vendors. Document escalation paths and communication protocols before incidents occur.

4. Automate Compliance Evidence Generation

"Continuous but manual" compliance won't survive EU AI Act enforcement or expanding GDPR scope. Prioritise policy-as-code implementations that generate audit evidence automatically, particularly for AI governance and cross-border data flows. Invest in systems that can prove continuous compliance, not just document point-in-time assessments.

5. Operationalise Cross-Border AI Controls

The 28-32% vs. 55-62% gap on cross-border mechanisms is striking given Europe's regulatory leadership on data protection. Treat cross-border AI data flows as a first-class risk domain with dedicated controls, monitoring, and governance. Don't rely on existing GDPR processes designed for conventional data transfers—AI systems require purpose-built cross-border governance.

The Bottom Line

Europe has built the regulatory frameworks that the world is now emulating. The gap isn't in policy—it's in operational proof. European organisations must now build the infrastructure to demonstrate continuous compliance before AI adoption and data sovereignty demands make that gap impossible to close. The organisations that invest now will be positioned for competitive advantage. Those that wait will face a compliance scramble when enforcement begins in earnest.

For the complete report with detailed methodology, industry breakdowns, and regional analysis, download it now.

Download the Report

Kiteworks