This is a classic high-stakes project for a Big Four firm, where the integrity of the compliance program directly impacts investor confidence and legal exposure. The key is establishing a sustainable, technology-enabled control environment, moving beyond simple manual compliance.

Here is the comprehensive action plan for **Global Regulatory Compliance and Control Overhaul**.

Comprehensive Action Plan: Global Regulatory Compliance and Control Overhaul

Section	Content
Preamble/Role	Senior Partner, Big Four Consulting Firm. The company is a multinational pharmaceutical firm facing a new, major global data privacy regulation (similar to GDPR or CCPA) that mandates specific data handling controls, auditing, and reporting, alongside existing Sarbanes-Oxley (SOX) compliance needs.
Core Mandate	Design a comprehensive action plan for achieving Global Regulatory Compliance with the new mandate and SOX. The plan must include a control framework redesign, implementing necessary system configuration changes (especially in ERP and data platforms), and setting up a continuous monitoring solution.
Objective	Achieve 100% compliance readiness for the new regulation across all Tier 1 markets and pass the external audit without any material weaknesses or significant deficiencies by the regulatory deadline (Q4, Year 1).
Compelling Why	The strategic imperative is Risk and Reputation Preservation. Failure to comply exposes the company to fines of up to 4% of global revenue (in the case of privacy breaches) and a loss of investor confidence (in the case of SOX deficiencies). The implementation of a Continuous Control Monitoring (CCM) solution will reduce external audit costs by 15% annually and lower the risk of material misstatement or a major data breach, directly stabilizing the company's risk-adjusted valuation.

Section	Content
Approach	Phase 1: Impact Assessment & Gap Analysis (Months 1-2): Conduct a line-by-line review of the new regulation against the current control environment and key system configurations. Prioritize gaps based on risk severity (e.g., probability x impact). Phase 2: Control Framework Design & Documentation (Months 3-4): Redesign the end-to-end control framework, defining To-Be automated and manual controls, and updating all control documentation (narratives, flowcharts). Phase 3: System Configuration & Remediation (Months 5-8): Execute required changes in ERP and key data systems (e.g., implementing segregation of duties (SoD) rules, configuring automated logs). Build the CCM solution/dashboards. Phase 4: Testing, Certification, and Continuous Monitoring Setup (Months 9-12): Execute internal testing (SIT and UAT on controls), achieve formal management certification, and operationalize the CCM solution for go-forward assurance.
Organization	Executive Risk Committee (ERC): Chaired by the CFO and Chief Risk Officer. Meets monthly to review residual risk, approve funding for remediation, and endorse the final certification. Compliance PMO: Led by a VP of Internal Controls/Risk Assurance. Responsible for project tracking, documentation integrity, and coordinating all testing. Functional Process Owners: Business leaders (e.g., VP of P2P) responsible for implementing and owning the redesigned controls within their processes. Internal Audit Liaison: Internal Audit is embedded in the PMO from day one to ensure controls are testable and to facilitate the final external audit sign-off.
Processes & Governance	Annual Compliance Training Certification: Mandatory, tailored annual training for all employees on the new regulation and SOX controls, with testing and executive sign-off required for all key control performers. Control Testing Cadence: Implement a Quarterly Attestation Process where control owners formally certify the design and operating effectiveness of their controls. Reporting Deficiencies: Establish a clear workflow for logging CCM alerts/deficiencies, root-cause analysis by the Process Owner, and mandatory remediation tracking by the PMO, reported weekly to the ERC.
Key Deliverables	Phase 1: Regulatory Gap Analysis Report, Risk-Prioritized Remediation Backlog. Phase 2: Updated Global Controls Matrix (detailing manual vs. automated controls), Process Narrative and Flowchart Documentation (To-Be). Phase 3: Remediated System Configuration Scripts (e.g., ERP SoD rules), Continuous Control Monitoring (CCM) Solution Dashboard (Pilot). Phase 4: Management Control Certification Letter (Final Attestation), 90-Day Monitoring Report, and External Audit Readiness Package.

Section	Content
Critical Risks & Mitigation	1. Misinterpretation of Complex Regulatory Language Risk: Incorrectly designing controls based on faulty understanding of the new mandate. Mitigation: Mandate 3rd-party Legal Review of the Gap Analysis and Control Design in Phase 2, utilizing external counsel with deep, multi-jurisdictional expertise in the regulation. 2. Lack of Budget for Control Automation Risk: Over-reliance on inexpensive, less reliable manual controls. Mitigation: Quantify the 3-year TCO of manual control performance (labor costs) versus the CapEx for CCM automation, justifying the automation investment based on ROI and audit efficiency. 3. Failure to Enforce Controls Consistently Across Global Sites Risk: Regional Business Units implement local workarounds. Mitigation: Tie 20% of the Regional VP's annual bonus to the Control Compliance Score as tracked by the CCM system, mandating zero tolerance for critical control bypasses.
Change Management Plan	Strategy: Focus on the non-negotiable nature of compliance: "Control is Mandatory; Efficiency is Expected." Training: Implement role-specific, modular training (e.g., P2P staff only train on P2P controls), using short, interactive modules tested for comprehension. Communication: CEO and CFO must issue a Joint Mandate at the beginning, emphasizing that regulatory compliance is a key performance indicator for every leader.
Crucial Additional Element	Scope and Methodology for Internal Control Testing: Scope: 100% coverage of all key SOX controls (ITGCs and BPCAs) and all controls addressing the five most critical requirements of the new data privacy regulation. Methodology: Implement 70% Automated Testing Target via the CCM tool for all high-volume transactional controls (e.g., SoD, payment limits). The remaining 30% (judgmental/manual controls) are tested Quarterly by the Internal Audit Liaison team.