GRC104: The "GlobalSync Inc." Compliance Crisis

Exercise Goal: To test your comprehensive understanding of compliance frameworks, audit processes, data privacy laws, and the legal implications of non-compliance in a realistic, high-stakes scenario.

Total Points: 100
Target: Achieve a 70% (70 points) or higher to successfully "save" the company.

Scenario Introduction:

Welcome, newly appointed **Chief Compliance Officer (CCO)**. You have just been hired by **GlobalSync Inc.**, a fast-growing multinational technology company headquartered in California, with significant operations in the European Union and Brazil.

GlobalSync's core product is a cloud-based collaboration platform used by businesses worldwide. The company has experienced rapid growth, but its compliance programs have not kept pace. The Board of Directors has hired you following a tip from a whistleblower about potential serious compliance failures. They are nervous, as a major merger with a European company is scheduled in six months, and any significant compliance issues could derail the deal.

Your Mission: Conduct a rapid but thorough compliance assessment, manage the immediate crisis, and present a strategic remediation plan to the Board.

Part 1: The Initial Discovery & Risk Triage (25 Points)

Task 1.1: The Whistleblower Email (10 Points)
You receive an anonymous email from an employee with the following allegations:

- **Allegation A:** Customer data from EU clients is being transferred to and processed in GlobalSync's main US data center without a proper legal mechanism.
- **Allegation B:** The sales team in Brazil has been offering significant "incentives" to secure large government contracts.
- **Allegation C:** There is no centralized process for handling customer requests to delete their data, and many requests are ignored or lost.
- **Allegation D:** The company cannot reliably prove that its financial reporting controls are effective.

Your Questions:
For each allegation (A, B, C, D), identify:

1. **The Primary Regulation/Framework at Risk** (e.g., GDPR, SOX, FCPA, etc.).
2. **The Potential Legal Implication** (e.g., Financial Penalty, Criminal Liability, Civil Lawsuit, Administrative Action).
3. **The "Key Dimension" of this Non-Compliance** (Is it Intentional/Unintentional? Systemic/Isolated?).

Task 1.2: Risk Assessment Matrix (15 Points)
Using the risk matrix methodology from the audit course, create a 5x5 Risk Matrix (Likelihood: Rare, Unlikely, Possible, Likely, Almost Certain; Impact: Insignificant, Minor, Moderate, Major, Catastrophic).

Plot each of the four allegations (A, B, C, D) on your matrix. Justify your placement for each one based on the potential financial, legal, and reputational impact to GlobalSync.

Part 2: The Compliance Audit Deep Dive (35 Points)

The Board has approved your request for an immediate, targeted compliance audit. Your team has assembled initial findings.

Task 2.1: Scoping the Audit (10 Points)
Based on the allegations, outline the **Scope and Objectives** for this audit. Be specific. Which business units, processes, and data flows will you examine? What are the key audit questions you need to answer?

Task 2.2: Evidence Gathering Plan (15 Points)
For allegation A (Improper EU-US data transfers), describe the specific evidence-gathering techniques you would use. Create a mini-plan:

- **Document Review:** Which 3 specific documents would you request first?
- **Interviews:** Which 3 job roles would you interview, and what are 2 key questions for each?
- **Testing:** Describe a control test you would perform to verify the data transfer mechanism.

Task 2.3: Drafting the Audit Finding (10 Points)
Your team has confirmed Allegation C is true. GlobalSync has no formal process for data subject requests (DSRs), and a sample shows 40% of deletion requests were never actioned.

Draft a formal audit finding using the required structure:

- **Condition:** What is the problem? (State the fact)
- **Criteria:** What should be happening? (Quote the relevant law/framework principle)
- **Cause:** Why is this happening? (Root cause analysis)
- **Effect:** What is the impact/risk? (Link to legal/financial/reputational consequences)
- **Risk Rating:** Assign a risk rating (Critical, High, Medium, Low) and justify it.

Part 3: Navigating the Legal & Regulatory Maze (25 Points)

The situation has escalated. You have discovered more information.

Task 3.1: The Regulator Knocks (10 Points)
The French Data Protection Authority (CNIL) has sent a formal inquiry about GlobalSync's EU-US data transfers. They are referencing the **Schrems II** ruling and asking what legal mechanism you are using.

- **Question:** What are the possible mechanisms for legal data transfer under the GDPR post-Schrems II? Which one is the most robust, and what must GlobalSync do to implement it?

- **Question:** If found in violation, what is the **maximum potential fine** GlobalSync could face from the CNIL under GDPR?

Task 3.2: The Lawsuit (10 Points)
A class-action lawsuit has been filed in California on behalf of users whose data deletion requests were ignored.

- **Question:** Under which California law (CCPA/CPRA) does this lawsuit fall? What specific "consumer right" has been violated?
- **Question:** What is a key difference between the private right of action in the CCPA/CPRA vs. the GDPR?

Task 3.3: The Settlement Dilemma (5 Points)
The DOJ has begun investigating the bribery allegations in Brazil. They have offered GlobalSync a **Deferred Prosecution Agreement (DPA)**.

- **Question:** What is a DPA, and what are the two key benefits for GlobalSync in accepting it?
- **Question:** What is one major obligation the company will likely have to fulfill under this DPA?

Part 4: The Strategic Roadmap & Board Presentation (15 Points)

You have 10 minutes to present your findings and plan to the Board of Directors.

Task 4.1: The Remediation Plan (10 Points)
Create a **high-level Corrective Action Plan (CAP)** for the data subject request failure (Allegation C). Use the structure from the audit course:

- **Specific Action Items** (at least 3)
- **Assigned Department/Owner**
- **Target Completion Date** (set realistic deadlines)
- **Metric for Success** (How will you know it's fixed?)

Task 4.2: The "Tone at the Top" (5 Points)
In one paragraph, draft the opening statement for your Board presentation. Your goal is to convince them that compliance is not just a cost center but a strategic imperative for the company's future survival and the pending merger. Use language that demonstrates leadership commitment.

Bonus Challenge: The Future-Proofing Question (Extra 5 Points)

The Board is impressed but asks: "What one emerging trend in privacy or compliance should we invest in now to avoid such a crisis in the future?" Based on the "Future Trends" from your materials, recommend one trend (e.g., Privacy-Enhancing Technologies, AI Governance, Continuous Auditing) and briefly explain why it's a strategic investment for GlobalSync.