NAME: Lakshita Rawat

ROLL NO.: 16102

COURSE: B.SC(H)CS-A

Data Privacy Audit Report for Infosys

Audit Date: October 26, 2024
Audit Period: March 2024 – October 2024
Conducted By: Lakshita Rawat

Scope Definition

- **Issues:** A lack of a clearly defined audit scope risks overlooking critical systems, departments, or types of sensitive data, potentially exposing Infosys to unmonitored vulnerabilities.
- **Observations:** Infosys conducts regular data privacy audits, but documentation regarding the scope lacks specifics. Key areas such as HR, customer data, and R&D data handling practices may not be consistently covered across global offices.
- **Recommendations:** Clearly define and document the audit scope to include all sensitive data types, critical departments, and systems. Regularly review the scope to ensure comprehensive coverage and adjust it as new data sources or processing systems are added.

2. Policies and Procedure Review

- **Issues:** Policies and procedures might be outdated, leaving gaps that fail to comply with new data privacy regulations, thereby increasing legal and reputational risks.
- **Observations:** While Infosys has established data privacy policies, they are updated infrequently. The policies cover essential areas but lack specifics regarding the handling of sensitive client data, data deletion, and employee access management.
- **Recommendations:** Conduct an annual review of all data privacy policies and procedures, updating them as necessary to reflect evolving regulations like GDPR, CCPA, and regional laws. Ensure policies comprehensively address the entire data lifecycle and develop a policy review committee to handle emergent regulatory changes swiftly.

3. Compliance Assessment

- **Issues:** Variations in compliance levels across Infosys's international operations may lead to non-compliance with region-specific privacy regulations.
- **Observations:** Compliance measures are inconsistently applied across various geographies. For instance, data retention practices in certain regions may not fully align with local data minimization and retention laws.
- **Recommendations:** Implement a standardized compliance protocol for global operations, tailored to align with regional regulations. Conduct regular compliance audits by region and designate compliance officers in key locations to monitor and manage adherence to laws such as GDPR, CCPA, and APAC privacy requirements.

4. Data Inventory and Classification

- **Issues:** An incomplete data inventory limits Infosys's ability to monitor data usage and manage risks effectively, especially for highly sensitive data like client information or intellectual property.
- **Observations:** Infosys maintains a partial data inventory, but sensitive data is inconsistently classified, leading to discrepancies in data protection measures across departments and projects.
- **Recommendations:** Develop a comprehensive, centralized data inventory system that records all data types collected, processed, or stored by Infosys. Implement a classification framework to label data based on sensitivity (e.g., public, internal, confidential) and automate inventory updates to ensure accuracy. Enforce protection measures based on data classification levels, such as stronger encryption for confidential data.

5. Access Controls Review

- **Issues:** Ineffective access controls could lead to unauthorized data access, posing risks to both client confidentiality and Infosys's intellectual property.
- **Observations:** Infosys uses role-based access control (RBAC) systems, but audits revealed cases where login credentials are shared among team members. Additionally, access permissions are not reviewed regularly, which could allow unauthorized access if employees change roles or leave.
- **Recommendations:** Enforce individualized login credentials and prohibit shared access. Implement a process for automatic role-based access updates, and perform quarterly access reviews to revoke permissions for employees who have changed roles or left the organization. Strengthen authentication measures, such as two-factor authentication, for sensitive data access.

6. Security Measures Assessment

- **Issues:** Outdated security protocols and tools could increase Infosys's exposure to cyber threats and data breaches.
- **Observations:** Infosys employs industry-standard security measures, but some legacy systems lack updated encryption protocols and the latest intrusion detection capabilities, especially for older applications.
- **Recommendations:** Perform a comprehensive security overhaul to ensure that all systems use up-to-date encryption standards (e.g., AES-256) and deploy advanced intrusion detection systems across all IT infrastructure. Schedule regular security assessments, including penetration testing and vulnerability scanning, to proactively identify and address potential threats. Adopt automated patch management for quicker security updates.

7. Third-Party Risk Assessment

- **Issues:** Insufficient oversight of third-party vendors handling Infosys's data could lead to unauthorized data sharing or leaks.
- **Observations:** Some third-party vendors are granted access to sensitive Infosys data, yet few are subject to regular audits to verify compliance with Infosys's data protection standards.
- **Recommendations:** Conduct comprehensive initial and periodic risk assessments for all third-party vendors with access to Infosys's data. Require vendors to demonstrate compliance with Infosys's data privacy policies, including security measures and incident response plans. Update vendor agreements to incorporate data privacy clauses, mandating regular audits and specifying response measures in case of data breaches.

8. Training and Awareness

- **Issues:** Inconsistent employee training across global locations could increase the risk of accidental data breaches or privacy violations.
- **Observations:** Infosys has implemented data privacy training, but the content and frequency of sessions vary by region, and awareness of best practices appears limited among some teams.
- **Recommendations:** Develop a standardized, mandatory data privacy training program that covers key data handling protocols, applicable laws, and incident reporting procedures. Conduct training sessions at least bi-annually for all employees, with role-specific training for departments handling sensitive data.

Integrate scenario-based learning to enhance employee understanding and application of data privacy measures.

9. Incident History Review

- **Issues:** Inadequate analysis of previous data privacy incidents increases the risk of recurring issues.
- **Observations:** Infosys maintains records of past data breaches and security incidents, but incident analyses are inconsistently applied across departments, and recurring issues such as unauthorized access have been observed.
- **Recommendations:** Implement a formal post-incident review process to identify root causes and prevent repeat incidents. Share lessons learned across departments and update relevant policies and training programs accordingly. Establish a centralized incident reporting and analysis team to ensure consistent application of preventive measures across the organization.

10. Risk Assessment and Reporting

- **Issues:** A lack of a formalized risk assessment process may hinder Infosys's ability to prioritize and address data privacy vulnerabilities effectively.
- **Observations:** Infosys conducts some level of risk assessment but does not consistently document or prioritize risks related to data privacy vulnerabilities across departments.
- **Recommendations:** Develop a comprehensive risk assessment framework with standardized criteria for evaluating data privacy risks. Document all identified risks, categorize them by severity and likelihood, and prioritize actions accordingly. Implement regular risk assessments and establish a centralized risk reporting mechanism to keep stakeholders informed and engaged in mitigating high-priority risks.

11. Follow-Up and Continuous Improvement

- **Issues:** Absence of a structured follow-up plan reduces the long-term effectiveness of Infosys's data privacy controls.
- **Observations:** While initial audit findings are addressed, there is no structured process for continuous monitoring or re-evaluation of data privacy practices.
- **Recommendations:** Establish a continuous improvement plan for data privacy, including periodic follow-up audits and reviews. Integrate findings into an ongoing data privacy roadmap, regularly updating policies and procedures as data privacy

laws evolve. Create a monitoring team responsible for tracking compliance and implementing audit recommendations over time