1. Maintain Governance Structure

- Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures

2. Maintain Internal Data Inventory

- Maintain an inventory of the location of key personal data storage or personal data flows with defined classes of personal data

3. Maintain Data Privacy Policy

- Maintain a data privacy policy that meets legal requirements and addresses operational risk

4. Embed Data Privacy Into Operations

- Maintain operational policies and procedures that reflect the data privacy policy, legal requirements, and operational risk management objectives

5. Maintain and Awareness Program

- Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks

6. Manage Information Security Risk

- Maintain an information security program based on legal requirements and ongoing risk assessments

7. Manage Third-Party Risk

- Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance

8. Maintain Notices

- Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance

9. Maintain Procedures for Inquiries and Complaints

- Conduct periodic testing of breach protocol and document findings and changes made
- Engage a breach response remediation provider
- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage
- Maintain a record preservation protocol to protect relevant log history

10. Monitor for New Operational Practices

- Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles

11. Maintain Data Privacy Breach Management Program

- Maintain an effective data privacy incident and breach management program

12. Monitor Data Handling Practices

- Verify operational practices comply with the data privacy policy and operational policies and procedures

13. Track External Criteria

- Track new compliance requirements, expectations, and best practices