### **GLBA Safeguards Rule Compliance Checklist**

### **Ensure Compliance with 16 CFR 314**

### 

# 1. Designate a Qualified Individual

## Reference: 16 CFR 314.4(a)

* **Appoint a qualified individual responsible for developing, implementing, and maintaining the institution’s information security program. (effective June 2023)**
* **Ensure the coordinator has authority and resources to oversee the program effectively.**

### 

# 2. Conduct a Risk Assessment

## Reference: 16 CFR 314.4(b)(1)

* **Identify Internal and External Risks to the security, confidentiality, and integrity of customer information.**
* **Evaluate risks from unauthorized access, use, or disclosure, including risks posed by third-party vendors.**
* **Assess System Vulnerabilities, including IT systems, physical records, and employee access policies.**
* **Review Safeguards in place and determine their adequacy for risk mitigation.**

### 

# 3. Develop and Implement Safeguards to Control Risks

## Reference: 16 CFR 314.4(c)

* **Technical Safeguards: Implement firewalls, encryption, and intrusion detection systems to protect customer data.**
* **Physical Safeguards: Restrict physical access to areas storing sensitive customer information (e.g., data centers).**
* **Administrative Safeguards: Control access to customer data through role-based permissions and conduct background checks on employees.**
* **Access Controls: Ensure that employees only access information necessary for their roles.**
* **Design and Implementation of Controls**

### 

# 4. Regularly Test and Monitor the Effectiveness of Safeguards

## Reference: 16 CFR 314.4(b)(2)

* **Monitor Systems continuously for unauthorized access and anomalies.**
* **Test Safeguards regularly through penetration testing, vulnerability scans, and security audits.**
* **Adjust safeguards based on test results to respond to emerging threats.**

### 

# 5. Oversee Service Providers (Third-Party Security)

## Reference: 16 CFR 314.4(d)

* **Select Service Providers who maintain appropriate safeguards.  
  Require providers to implement specific security measures in line with your institution’s security program.**
* **Implement a Third-Party Risk Management Program to assess and monitor the security of service providers.**
* **Include specific security requirements in vendor contracts.**

### 

# 6. Stay Agile and Updated

## Reference: 16 CFR 314.4(e)

* **Regularly Update the information security program to address new threats and risks identified through ongoing assessments.**
* **Ensure the program adapts to changes in business arrangements, technologies, or emerging risks.**
* **Conduct Annual Reviews of the security plan and make necessary adjustments based on results from risk assessments and security tests.**

### 

# 7. Prepare for Security Incidents (Incident Response Plan)

## Reference: 16 CFR 314.4(h)

* **Develop and maintain an Incident Response Plan that outlines roles, responsibilities, and response procedures for security incidents.**
* **Ensure the plan addresses communication strategies, including notifications to customers, regulators, and law enforcement.**
* **Include post-incident analysis procedures to identify vulnerabilities and improve safeguards after an incident.**

### 

# 8. Report to the Board or Governing Body

## Reference: 16 CFR 314.4(i)

* **Prepare and present an Annual Report to the board or governing body, summarizing the institution’s compliance status, results of risk assessments, security incidents, and recommendations for future actions.**
* **Ensure the report highlights areas for improvement and provides action plans for addressing deficiencies.**

### 

### 

### **Summary Checklist:**

### **Designate a Compliance Coordinator**

### **Conduct Risk Assessments regularly**

### **Develop, Implement, and Test Safeguards**

### **Oversee Third-Party Service Providers**

### **Stay Agile and Update the Security Program**

### **Prepare for Incidents with a comprehensive response plan**

### **Present an Annual Report to the board on compliance status**

### 