



# Privacy & Data Protection Risk Assessment

- Ensuring Compliance with GLBA, CCPA, and NIST Privacy Framework
- By: Gerria LeSure | GRC Consultant
- Date: 03/01/2025

# Understanding Privacy Risks in Insurance

Objective: Conduct a privacy & security risk assessment for State Farm.

Industry Focus: Insurance (Auto, Home, Life, Business).

Regulations Applied:

- GLBA (Gramm-Leach-Bliley Act)

- CCPA (California Consumer Privacy Act)

- NIST Privacy Framework

# The Business Impact of Privacy & Security Risks

Why This Matters for State Farm:

- Legal Fines & Compliance Violations: GLBA fines up to \$100,000 per violation.

- Data Breaches Affect Reputation: Insurance companies lose customer trust after breaches.

- Operational Downtime: Cybersecurity incidents cause service disruption & revenue loss.

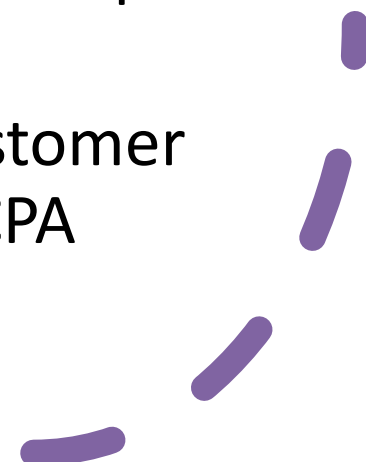
# Regulatory Compliance & Security Standards

- Framework | Key Requirement | Impact on State Farm
- GLBA | Protects consumer financial data | Enforce data encryption & access control
- CCPA | Consumers can request, delete, and opt-out of data sharing | Implement opt-out mechanisms & privacy requests
- NIST Privacy Framework | Best practices for data governance & security | Strengthen incident response & vendor security



A large red circle on the left side of the slide, partially cut off by the edge.

## Identified Data Protection & Security Gaps

- Top Privacy & Security Risks at State Farm:
  - - No encryption for sensitive customer data (GLBA violation).
  - - Employees have excessive access to PII.
  - - Third-party vendors handling PII aren't regularly audited.
  - - No structured incident response plan for data breaches.
  - - Lack of automated customer opt-out mechanism (CCPA violation).
- 
- Four short, thick purple lines of varying lengths and orientations in the bottom right corner.

# Privacy Risk Prioritization – Likelihood & Impact



RISK | LIKELIHOOD (1-5) |  
IMPACT (1-5) | OVERALL  
RISK | RISK LEVEL



UNENCRYPTED  
CUSTOMER DATA | 5 | 5 |  
25 | CRITICAL



EXCESSIVE EMPLOYEE PII  
ACCESS | 4 | 4 | 16 |  
HIGH



LACK OF VENDOR  
SECURITY AUDITS | 5 | 4 |  
20 | HIGH



NO DATA BREACH  
RESPONSE PLAN | 5 | 5 |  
25 | CRITICAL



# How State Farm Can Improve Data Privacy & Compliance

## Recommendations:

- Encrypt sensitive customer data (GLBA compliance).
- Limit access to PII using Role-Based Access Control (RBAC).
- Conduct vendor security audits annually.
- Develop a Data Breach Response Plan (NIST 800-61).
- Implement an automated opt-out mechanism for customers (CCPA compliance).

# Final Recommendations & Roadmap to Compliance

- Key Takeaways:
  - - State Farm must strengthen privacy controls to remain GLBA & CCPA compliant.
  - - Implementing encryption, access controls, and vendor audits is critical.
- Next Steps:
  - - Encrypt all customer data.
  - - Limit employee data access (RBAC).
  - - Develop a structured incident response plan.



# References & Compliance Guides

- Additional Resources & Documentation:
- - GLBA Compliance Guide:  
[https://github.com/GerriaLeSure/Privacy-Data-Protection-Assessment/blob/main/Compliance\\_Guides/GLBA\\_Guide.pdf](https://github.com/GerriaLeSure/Privacy-Data-Protection-Assessment/blob/main/Compliance_Guides/GLBA_Guide.pdf)
- - CCPA Compliance Guide:  
[https://github.com/GerriaLeSure/Privacy-Data-Protection-Assessment/blob/main/Compliance\\_Guides/CCPA\\_Guide.pdf](https://github.com/GerriaLeSure/Privacy-Data-Protection-Assessment/blob/main/Compliance_Guides/CCPA_Guide.pdf)
- For more details, visit the full report in the GitHub repository.

