🛡️ Third-Party Risk Management Suite

This repository contains a full set of GRC-aligned documentation designed to evaluate, onboard, and manage third-party vendors securely and responsibly. It demonstrates key stages of vendor due diligence, contract alignment, and operational accountability — all grounded in real-world frameworks like SOC 2, ISO 27001, GDPR, and NIST.

📂 Included Sections & Tools

`questionnaires/`
📄 **Third_Party_Security_Questionnaire_Template.md**
📄 **Sample_Vendor_Response.md**
Vendor-facing forms to assess security posture and data protection practices.

`data-processing-agreements/`
📄 **Data_Processing_Agreement_Template.md**
📄 **DPA_Terminology_Glossary.md**
Templates to define controller/processor roles, compliance terms, and personal data handling expectations.

`risk-assessments/`
📄 **Third_Party_Risk_Assessment_Template.md**
📄 **Sample_Risk_Assessment_for_AcornCloud.md**
Internal scoring templates for evaluating risk across data sensitivity, access controls, and incident response.

`vendor-security-addendum/`
📄 **Vendor_Security_Addendum.md**
Add-on agreement outlining minimum security controls, breach timelines, and audit rights.

`service-level-agreements/`
📄 **SLA_Template_for_Vendors.md**
📄 **SLA_Response_Timeline_Chart.md**
Documents service availability, breach response expectations, and performance penalties.

🌐 Why This Matters

Vendor security isn’t just a checkbox — it’s a core part of digital trust.
This suite reflects my hands-on understanding of Governance, Risk, and Compliance (GRC), and my ability to operationalize security expectations in clear, enforceable language.

> Because risk is shared — but responsibility must be clear.