 770 Chapel Street
New Haven, CT 06510
 203-401-8768
 mydae.org

Project Design Documentation Template:

Last updated: July 15th, 2025

1. Project Title & Version Control

Cybersecurity Compliance Checker (with Security Risk Register with Heat Map)

Version Control

Version: DRAFT 1

Date: 07/17/2025

Change Log: N/A

2. Project Summary (2–3 sentences)

This project aims to build a web-based cybersecurity compliance checker that analyzes uploaded policy or configuration files against industry-standard frameworks (e.g., GLBA, NIST CSF, PCI DSS, etc). It automatically identifies non-compliant items, generates a security risk register, and visualizes the risks using a dynamic heat map, helping organizations prioritize and remediate security issues efficiently.


Currently starting project with following:


1. Cybersecurity Compliance for Educational Institutions
(COPPA (Children's Online Privacy Protection Act) and ISO 27001 / NIST CSF)
2. Cybersecurity Compliance for Finance Industry
(GLBA (Gramm-Leach-Bliley Act) + NIST Cybersecurity Framework (CSF))


3. Problem Statement / Use Case

Organizations struggle to consistently monitor and validate cybersecurity compliance across evolving policies, controls, and IT infrastructure. Manual reviews of system configurations, policy adherence, and risk assessment documentation are time-consuming, error-prone, and lack visual prioritization. This tool enables automated scanning of compliance-related files to streamline assessment and support audit readiness.



 770 Chapel Street
New Haven, CT 06510

 203-401-8768

 mydae.org

4. Goals and Objectives

1. Automate the detection of policy violations from uploaded documents (e.g., configs, risk assessments).
2. Create a centralized, editable risk register based on extracted compliance failures.
3. Auto-score and visualize risk impact using a heat map (likelihood × impact).
4. Provide actionable remediation suggestions for failed items.
5. Export compliance reports to PDF/Excel for internal tracking and audit evidence.

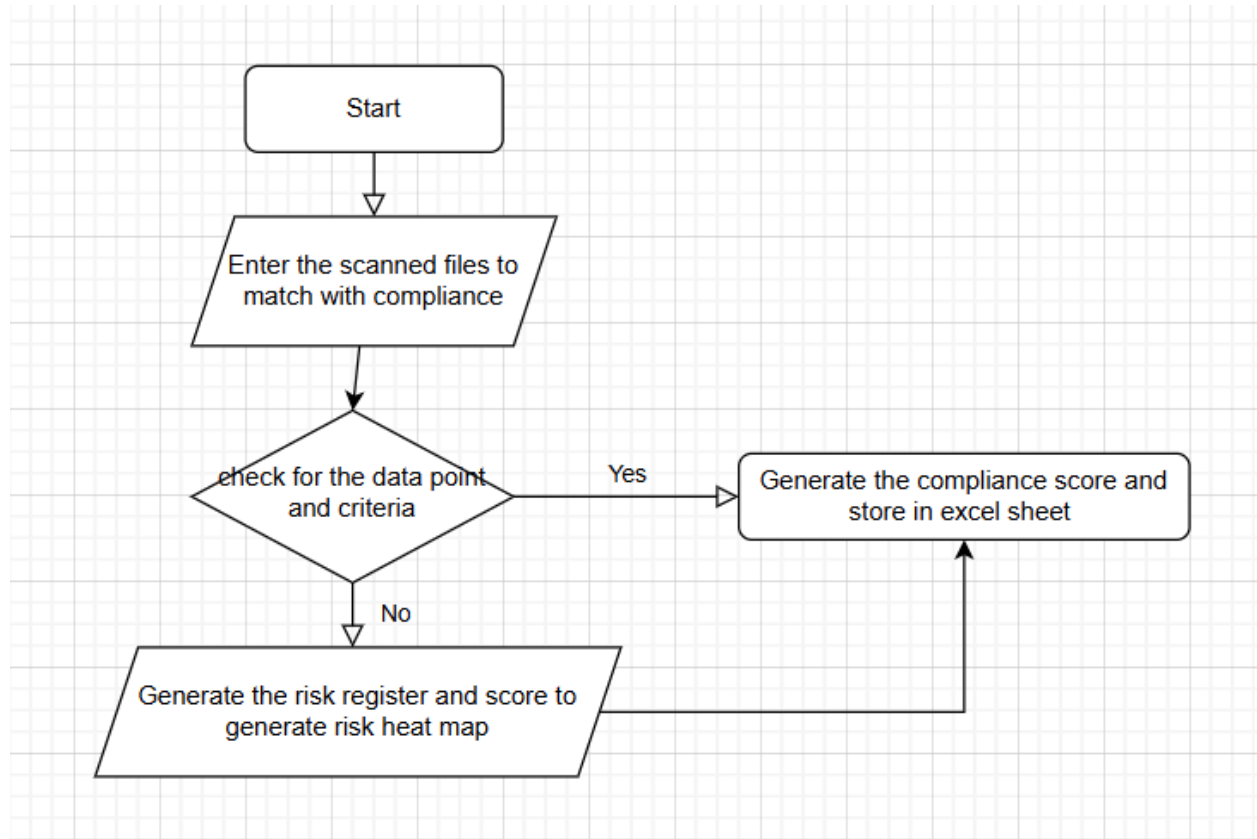
5. Key Features / Functions

1. Upload system configuration or policy files (.txt, .json, .yaml, etc.)
2. Framework-based compliance scanning (GLBA + NIST Cybersecurity Framework (CSF), etc.)
3. Automated extraction of data points using regex/NLP
4. Policy compliance scoring (pass/fail with % summary)
5. Risk register with fields: likelihood, impact, owner, control
6. Auto-calculation of risk score and dynamic heat map visualization
7. Remediation suggestions and export to PDF/Excel

6. Tech Stack and Tools

Component	Technology
Frontend	HTML, CSS, JavaScript, Bootstrap (or React for dynamic UI)
Backend	Python (Flask)
Compliance Engine	Custom parsers using Python, Regex, NLP (spaCy or NLTK optional)
Visualization	Plotly or Dash (for heat maps and dashboards)
Data Storage	JSON/YAML for uploads; SQLite/PostgreSQL for metadata
Reporting	pdfkit, pandas, or openpyxl for export to PDF/Excel
Authentication (optional)	Flask-Login or Firebase Auth

7. Architecture / Workflow Diagram



8. Timeline / Weekly Milestones+

Week	Outcome
Week 1	Finish Landing page
Week 2	Define GLBA compliance frameworks, policies, and data points to check
Week 3	Define COPPA compliance frameworks, policies, and data points to check along with the company policies
Week 4	Build document parser for GLBA + COPPA config checks (regex/NLP)
Week 5	Generate risk entries based on failed policies
Week 6	Implement auto risk score + build editable risk register table
Week 7	Add functionality to fetch and save the compliance score
Week 8	Add functionality to fetch and save the risk score
Week 9	Export compliance report to PDF/Excel
Week 10	Create dynamic heat map using Plotly
Week 11	Enhance with NIST CSF/ISO 27001 compliance which is common for both the above industries and test



Week 12	Project documentation
---------	-----------------------

9. Risks and Risk Mitigation

Risk	Mitigation
Parser may miss data points in diverse formats	Use consistent config formats or NLP fallback
Heat map scores may lack context	Allow user overrides for likelihood/impact
File parsing may introduce security risks	Sanitize file inputs and restrict extensions
Time constraints on implementing all frameworks	Start with GLBA + NIST Cybersecurity Framework (CSF), then modularize others

10. Evaluation Criteria

Metric	Description
Accuracy	% of correct data point extractions and compliance results
Usability	Intuitive UI for file uploads, filtering, and editing risks
Completeness	Full support for at least 2 frameworks and document types
Visualization Quality	Clear, interactive heat map and dashboard
Automation	Degree of effort reduced compared to manual reviews
Exportability	Clear, formatted reports for audit or compliance teams

11. Future Considerations

1. Support for additional frameworks (e.g., SOC 2, ISO 27001, NIST 800-53)
2. Role-based user access and multi-tenant capabilities for MSSPs