**GRC Opensource Platforms Evaluation**

**A diagram of a system

AI-generated content may be incorrect.**

*https://www.mermaidchart.com/app/projects/266f0b65-8df4-4c5b-804d-078d92524b63/diagrams/5e5302ae-e90e-48ef-ae9e-bcf7c5cb3174/version/v0.1/edit*

The following table summarizes the scores assigned to each repository across all criteria.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Repository | Tech  Stack | Modern Stack | Microservices | Updates | Community | Data  Automation | Total Score |
| CISO-Assistant | Python/Django, SvelteKit, PostgreSQL, Docker | 5 | 5 | 5 | 5 | 5 | 25 |
| GRC4CISO | Odoo, Wazuh, OpenZiti, GPT | 5 | 5 | 1 | 3 | 3 | 17 |
| Eramba | PHP, MySQL, Redis, Apache, Docker | 3 | 0 | 4 | 5 | 5 | 17 |
| ComplianceAsCode | Python, Go, CMake, SCAP, Bash, Ansible | 4 | 0 | 4 | 4 | 2 | 14 |
| Auditree | Python | 4 | 0 | 3 | 3 | 2 | 12 |
| gapps | Python, JavaScript | 4 | 0 | 3 | 3 | 4 | 14 |
| OpenGRC | PHP, Laravel, Filament, MySQL, Tailwind | 3 | 0 | 3 | 2 | 1 | 9 |
| SimpleRisk | PHP, MySQL | 2 | 0 | 1 | 4 | 5 | 12 |
| GRC (GRCbit) | Python, web2py | 2 | 0 | 1 | 1 | 1 | 5 |

**Integration Considerations**

* CISO Assistant as Central Hub: Use CISO Assistant’s APIs to integrate with Auditree for automated evidence collection and with gapps for compliance tracking. Its decoupling principle allows reusing past assessments, facilitating evidence consistency.
* Auditree for Evidence Automation: Auditree can collect evidence and export it in formats compatible with CISO Assistant, enhancing evidence management workflows.
* gapps for Specialized Compliance: gapps can be used independently or integrated with CISO Assistant for detailed compliance tracking, leveraging its support for multiple frameworks.
* Custom Development: Since all tools are open-source, custom integrations can be developed if needed (e.g., API connections between CISO Assistant and gapps), though this may require development effort.

**Key URLs**

* [CISO Assistant GitHub Repository](https://github.com/intuitem/ciso-assistant-community)
* [GRC4CISO GitHub Repository](https://github.com/grcbit/grc4ciso)
* [Eramba Official Website](https://www.eramba.org/)
* [ComplianceAsCode GitHub Repository](https://github.com/ComplianceAsCode/content)
* [OpenGRC GitHub Repository](https://github.com/LeeMangold/OpenGRC)
* [SimpleRisk GitHub Repository](https://github.com/simplerisk/code)
* [GRC (GRCbit) GitHub Repository](https://github.com/grcbit/grc)
* [ComplianceAsCode Organization GitHub](https://github.com/ComplianceAsCode)
* [OpenGRC Installation Documentation](https://docs.opengrc.com/installation/)
* [CISO Assistant Documentation](https://intuitem.gitbook.io/ciso-assistant)
* [Intuitem Official Website](https://intuitem.com)
* [SimpleRisk Official Website](https://www.simplerisk.com/)
* [Auditree Documentation for Compliance Automation](https://auditree.github.io/)
* [OpenGRC Documentation for Cyber GRC Web Application](https://docs.opengrc.com/)

**Avalible Online Demos**

1. CISO Assistant <https://intuitem.com/trial> ==> Register  
2. SimpleRisk <https://demo.simplerisk.com/> ===> user / user  
3. Gaaps <https://gapps.darkbanner.com/> ===> Register  
4. GRC4CISO <https://democommunity.grc4ciso.com/> ===> guest / guest123



**Example Use Cases for GenAI/LLM in GRC**

* Automated Compliance Checklists: GenAI can generate compliance checklists for frameworks like HIPAA or SOC 2, ensuring that all necessary controls are in place and easily accessible for audits.
* Incident Response Documentation: When an incident occurs, GenAI can assist in documenting the response process, pulling relevant logs and communications to create a comprehensive report that can be used for future audits and compliance assessments.
* Risk Scoring Models: Organizations can develop risk scoring models using historical incident data analyzed by GenAI, allowing for more informed decision-making regarding resource allocation for risk mitigation.
* Policy Generation and Updates: GenAI can automate the drafting and updating of policies to reflect changes in regulations or organizational practices, ensuring that compliance documents are always current and relevant.
* Anomaly Detection in Logs: By analyzing logs from various systems, GenAI can identify anomalies that may indicate compliance issues or security threats, enabling quicker responses to potential risks.

**Open-Source GenAI/LLM Options**

Seevral options are available that can be integrated with CISO Assistant:

* **Hugging Face Transformers**: A popular library for implementing various LLMs that can be fine-tuned for specific GRC tasks.
* **GPT-Neo and GPT-J**: Open-source models that can be adapted for generating compliance documentation and parsing regulatory texts.
* **Haystack**: An open-source framework for building search systems that can be used to retrieve and analyze compliance-related documents efficiently.

