ISO 27001:2022 MINI-ISMS Project

By Victor Beatón

After obtaining the PECB ISO/IEC 27001:2022 Foundation Certificate, I really wanted to test my recently acquired knowledge of this GRC standard. Researched various beginner projects to put into practice all concepts and concluded that an ISO/IEC 27001:2022 aligned Mini-ISMS was the best option in terms of availability. Of course, being a beginner has serious limitations: time (in an industry that continually grows and prepares for new challenges), real-world experience, and the main difficulty: a real company/organization to analyze.

Content of the Project

In this project you will find a fictional case study. In this case, **I used AI (Gemini)** to create a **fictional tech startup located in El Salvador**, with a staff of 25 employees. The company in question: Velo Compute, recognizable for their flag-ship service: VeloAnalytics SaaS Platform. This tool analyses consumer behavior and optimize inventory forecasting for retail enterprises.

As any startup, procedures, policies and practices are (most of the time) not clearly stated as well as documented. In this case, I wanted to highlight the "messy" startup environment. Therefore, you'll find common practices such as not applying MFA, deficient remote-work environment and access rights issues. The project focuses on protecting the company's proprietary machine learning algorithms and the sensitive PII of international retail clients.

Disclaimer:

Warning: This is a lean GRC methodology, ISO 27001:2022 aligned. Not all deliverables of a full ISO 27001:2022 are presented. In this case, prioritizing the 15 most critical ISO 27001:2022 controls to provide maximum risk reduction for a small, high-growth startup. the size of the company also is favorable for a small, but well documented framework.

Deliverables:

- ISMS Scope & Context Document
- Statement of Applicability (SOA)
- Risk Assessment and Risk Treatment Plan
- Audit Checklist (Compliance Indicators and Proof)