



ReguLight - Easy Risk & Compliance Management

In the current business climate, characterized by increasing cyber threats and a constant stream of new regulations such as GDPR, CCPA/CPRA, MAS TRM, DORA, and NIS2, it is essential for organizations to implement demonstrable and robust risk management. However, many companies, particularly Small and Medium-sized Enterprises (SMEs), find traditional GRC (Governance, Risk, and Compliance) solutions to be **overly complex** and **expensive** in terms of implementation and maintenance.

ReguLight has been developed as a focused, **affordable**, and **accessible** application that supports SMEs and organizations with limited GRC knowledge or capacity in the structural setup, execution, and maintenance of their risk and compliance processes. The focus is on providing the necessary functionality for effective management, without the unnecessary bulk and complexity of *enterprise* systems.

Key Features of ReguLight

Independent, Secure Architecture

ReguLight offers maximum control over sensitive data:

- **Standalone Operation:** The application is available on the Apple Mac App Store and runs locally on a **Mac computer**. This makes the solution manageable and suitable for single-user operation.
- **Local Data Storage:** All data, including risk analyses, controls, and uploaded compliance documentation, is stored **exclusively locally** on the user's device.
- **No Internet Connectivity:** There is **no data exchange** via the internet, ensuring the security and privacy of the GRC data is protected by the security mechanisms of the MacOS operating system.

Fundamental Risk Management

The application facilitates the structured documentation of your risk and compliance management processes:

- **Identification and Linking:** Users can identify and record risks and link them to the relevant **Internal Controls** defined and implemented within the organization. This is applicable to both IT and cybersecurity risk management, as well as broader forms of *Business Risk Management*.
- **Documentation and Follow-up:** Internal Controls can be linked to supporting documents (such as policies, procedures or other types of relevant information), and to **tasks, issues, and incidents** (such as improvement points, concerns or reported disruptions). This ensures comprehensive administration and improves the maintainability of the system.
- **Control Effectiveness:** ReguLight provides a direct and practical mechanism for managing Internal Control **Risk Effectiveness** and quantifying the impact of active remediation efforts. When an organization defines an **Internal Control** and links it to an identified risk, the application establishes the control's intended risk mitigating effect. However, the true effectiveness of that control is continuously influenced by the presence of **open Tasks, Issues, and Incidents** linked to it.

- **Live Risk Status:** ReguLight's **mechanics of Risk Reduction** operate on the principle that unresolved items—whether they are tasks to implement a new measure, issues highlighting a deficiency in an existing control, or incidents representing a failure of the control—directly degrade the control's perceived **effectiveness**. By tracking the status and urgency of these linked items, ReguLight dynamically adjusts the calculated residual risk. For example, a high-priority open incident linked to a backup procedure will significantly increase the *live* residual risk associated with data loss, even if the written control is documented.
- **Risk Dashboard:** The live **Risk Status Dashboard** aggregates the available data, offering users immediate, **visual feedback on the health** of their risk posture. The dashboard converts GRC data into clear, actionable insights, highlighting whether risks are elevated due to unresolved issues and enabling **drill-down access** to detailed underlying information. This focused approach ensures that attention is directed precisely to where control deficiencies (delayed tasks, open issues and incidents) are actively undermining the risk reduction strategy, enabling quick intervention and continuous improvement of the organization's overall risk management maturity.

Compliance and Framework Integration

ReguLight assists in translating Internal Controls into external requirements:

- **Mapping Capabilities:** The application offers the functionality to **map** Internal Controls to the individual requirements of common international standards and regulations, such as **ISO 27001/27002, CCPA/CPRA, MAS TRM, NIST, and DORA**.
- **Demonstrable Compliance:** Through this linking, and through the live **Compliance Dashboard**, organizations can present their **compliance status** to regulators and auditors. The option to **import frameworks** of choice is available as a standard feature.

Built-in dynamically generated PDF Reports

ReguLight includes dynamically generated PDF reports that deliver clear insight into the organization's risk posture and compliance status, including task progress, open incidents, and outstanding issues.

Accessibility and Knowledge Development

ReguLight is designed to **get started**, shorten the learning curve and strengthen internal capacity:

- **Easy Start:** The application is low-threshold and includes a '**Getting Started Wizard**' and a help system to quickly guide users.
- **Step-by-Step Methodology:** Users can follow a structured methodology while working to learn and build the organization of risk management and Compliance.
- **Insight and Monitoring:** Dashboards, dynamic PDF Reports, and an up-to-date, auto generated Priorities List provide continuous insight into the risk and compliance status and show the concrete, necessary actions to maintain and improve risk status or compliance levels.

ReguLight provides SMEs with an accessible way to establish structured risk and compliance management, helping them effectively meet risk management and regulatory compliance requirements.