



Working with Frameworks

This document outlines how to implement compliance frameworks within **ReguLight**. By following this workflow, you will transform external regulatory requirements into actionable, measurable internal processes.

1. Core Concepts: Requirements vs. Implementation

In ReguLight, a clear distinction is made between what you *must* do and what you *actually* do:

- **Framework Controls:** These are external requirements (e.g., ISO 27001, DORA, NIS2, or the **ReguLight Security Framework**). They define the standard you are aiming for.
- **Internal Controls:** these are your company's specific measures—policies, automated tools, or manual procedures—that satisfy a Framework Control and mitigate business risks.

ID	Area	Domain	Subdomain	Name	Description	Internal Controls
RGL-AL-001	Govern	Audit & Logging	Governance	Define an Audit Log Management...	Establish and maintain a documented process for collecting, reviewing...	🔴
RGL-AL-002	Detect	Audit & Logging	Log Collection	Enable Comprehensive Audit Logg...	Enable audit logging on all organizational assets that support it. Log ev...	🔴
RGL-AL-003	Protect	Audit & Logging	Log Collection	Protect Audit Log Storage and Inte...	Provision sufficient storage capacity for audit logs to meet retention re...	🔴
RGL-AL-004	Protect	Audit & Logging	Log Collection	Synchronize System Clocks	Synchronize time across all organizational assets using a consistent an...	🔴
RGL-AL-005	Detect	Audit & Logging	Log Collection	Centralize Log Collection	Aggregate audit logs from across the organization into a centralized lo...	🔴
RGL-AL-006	Detect	Audit & Logging	Analysis & Alerting	Deploy SIEM and Configure Alerting	Implement a Security Information and Event Management (SIEM) soluti...	🔴
RGL-AM-001	Identify	Asset Management		Maintain a Comprehensive Asset R...	Create and keep current a thorough register of all organizational assets...	🔴
RGL-AM-002	Respond	Asset Management		Handle Unauthorized Assets	Implement a weekly process to identify and act on unauthorized assets...	🔴
RGL-AM-003	Detect	Asset Management		Deploy Network Asset Discovery	Use both active scanning and passive monitoring solutions to continuo...	🔴
RGL-AM-004	Identify	Asset Management		Leverage DHCP Logs for Asset Tra...	Collect DHCP logs from all DHCP servers or IP address management sy...	🔴
RGL-BR-001	Govern	Backup & Recovery		Define Backup and Recovery Obj...	Establish and maintain a documented process for data backup and rec...	🔴
RGL-BR-002	Protect	Backup & Recovery		Automate and Protect Backups	Configure automated backups for all organizational data within scope o...	🔴
RGL-BR-003	Recover	Backup & Recovery		Test Data Recovery Procedures	Perform regular restoration tests to verify that backed-up data can be...	🔴
RGL-DG-001	Govern	Data Governance	Policy & Classific...	Define a Data Governance Process	Document and maintain a formal data management process covering d...	🔴
RGL-DG-002	Identify	Data Governance	Policy & Classific...	Maintain a Data Inventory	Create and maintain an inventory of organizational data based on your...	🔴
RGL-DG-003	Identify	Data Governance	Policy & Classific...	Classify Data and Map Data Flows	Establish and maintain a data classification scheme using labels such n...	🔴
RGL-DG-004	Protect	Data Governance	Data Protection	Implement Data Access Controls	Define and enforce data access control lists based on the principle of n...	🔴
RGL-DG-005	Protect	Data Governance	Data Protection	Enforce Data Retention and Secur...	Enforce data retention according to your documented data governance...	🔴
RGL-DG-006	Protect	Data Governance	Data Protection	Encrypt Data on Devices and Rem...	Apply full-disk or volume encryption on all end-user devices containi...	🔴
RGL-DG-007	Protect	Data Governance	Data Protection	Encrypt Sensitive Data in Transit a...	Encrypt all sensitive data during transmission using protocols such as...	🔴
RGL-DG-008	Protect	Data Governance	Data Protection	Segment Data by Sensitivity	Separate data processing and storage environments based on data sen...	🔴
RGL-DG-009	Protect	Data Governance	Data Protection	Implement Data Loss Prevention	Deploy automated DLP tooling to discover, classify, and monitor sensiti...	🔴
RGL-DG-010	Detect	Data Governance	Monitoring	Monitor Sensitive Data Access	Enable logging for all access to sensitive data, including read, modifia...	🔴
RGL-EW-001	Protect	Email & Web Prot...		Maintain Secure Email and Web Br...	Deploy and manage current, supported web browsers and email clients...	🔴
RGL-EW-002	Protect	Email & Web Prot...		Restrict Browser and Email Plugins	Allow only pre-approved browser extensions and email client plugins. R...	🔴
RGL-EW-003	Protect	Email & Web Prot...		Enforce Web Content Filtering	Implement DNS-based and URL-based content filtering to block acces...	🔴
RGL-EW-004	Protect	Email & Web Prot...		Protect Against Malicious Email At...	Use sandbox analysis or similar techniques to inspect email attachmen...	🔴
RGL-EW-005	Protect	Email & Web Prot...		Deploy Email Authentication Contr...	Implement SPF, DKIM, and DMARC records for all organizational email...	🔴
RGL-IA-001	Identify	Identity & Access	Account Manage...	Maintain an Account Inventory	Keep a comprehensive inventory of all accounts in the organization, co...	🔴
RGL-IA-002	Protect	Identity & Access	Authentication	Enforce Strong Password Policies	Require unique passwords across all organizational assets. Apply a min...	🔴
RGL-IA-003	Protect	Identity & Access	Account Manage...	Deactivate Dormant Accounts	Disable or remove accounts that have been inactive for 45 days or mor...	🔴
RGL-IA-004	Protect	Identity & Access	Access Policies	Separate Administrative and Stand...	Restrict administrative privileges to dedicated admin accounts. Ensure...	🔴
RGL-IA-005	Protect	Identity & Access	Access Policies	Centralize Identity and Access Ma...	Use a central directory service, SSO solution, or identity provider to ma...	🔴
RGL-IA-006	Govern	Identity & Access	Access Policies	Define Access Lifecycle Procedures	Document and follow standardized processes for granting and revokin...	🔴
RGL-IA-007	Protect	Identity & Access	Authentication	Enforce Multi-Factor Authentication	Require multi-factor authentication for all externally exposed applica...	🔴
RGL-IA-008	Identify	Identity & Access	Access Policies	Define Role-Based Access Policies	Establish and maintain role-based access control, assigning permisio...	🔴
RGL-IA-009	Govern	Identity & Access	Access Policies	Manage Conditional Access Policies	Define and enforce conditional access rules that evaluate context such...	🔴
RGL-IR-001	Respond	Incident Response		Assign Incident Response Roles a...	Designate a primary and at least one backup person responsible for co...	🔴
RGL-IR-002	Govern	Incident Response		Establish Incident Communication...	Maintain an up-to-date list of parties to notify during incidents, includi...	🔴
RGL-IR-003	Govern	Incident Response		Define Incident Reporting and Res...	Document and publish a clear process for all personnel to report securi...	🔴



2. Importing the ReguLight Security Framework

The quickest way to start is by importing the ReguLight Security Framework.

1. Download the RGL Security Framework.csv from regulight.eu/docs.
2. In ReguLight, navigate to **Settings** → **Compliance Frameworks**.
3. Click the **Import Framework (CSV)** button.
4. Once loaded, the Framework is added to the App's menu bar. Framework Controls are organized into **Areas** (e.g., *Identify, Protect, Detect*) and **Domains** (e.g., *Asset Management*) and **Subdomains** (e.g., *Log Collection*).

Note: Initially, the **Internal Controls** column for these new requirements will show 0, indicating a compliance gap (no mapped Internal Controls).

3. Creating and Mapping Internal Controls

To bridge the gap between a requirement and your operation, you must **map the Framework Control to an Internal Control**.

The 'Add Control' form is divided into several sections:

- Identification:** Fields for ID (IC-001), Name (Use of NTP server for time synchronization), and Description (For accurate time synchronization, the IT department has deployed a centralized Network Time Protocol (NTP) server that is used by all computer systems).
- Responsibility:** Field for Control Owner (Search person...).
- Classification:** Dropdowns for Type (Technical), Nature (Automated), Frequency (Continuous), and Status (Implemented). A slider for Target Effectiveness (CRRF) is set to 90%.
- Risk Mapping:** Search risks... field.

Buttons for 'Cancel' and 'Save' are at the bottom.

The 'Add Control' form continues with the following sections:

- Framework Mapping:** Search framework controls... field. A list of controls is shown, with 'RGL-AL-004: Synchronize System Clocks' highlighted in blue.
- Document Mapping:** Search documents... field.

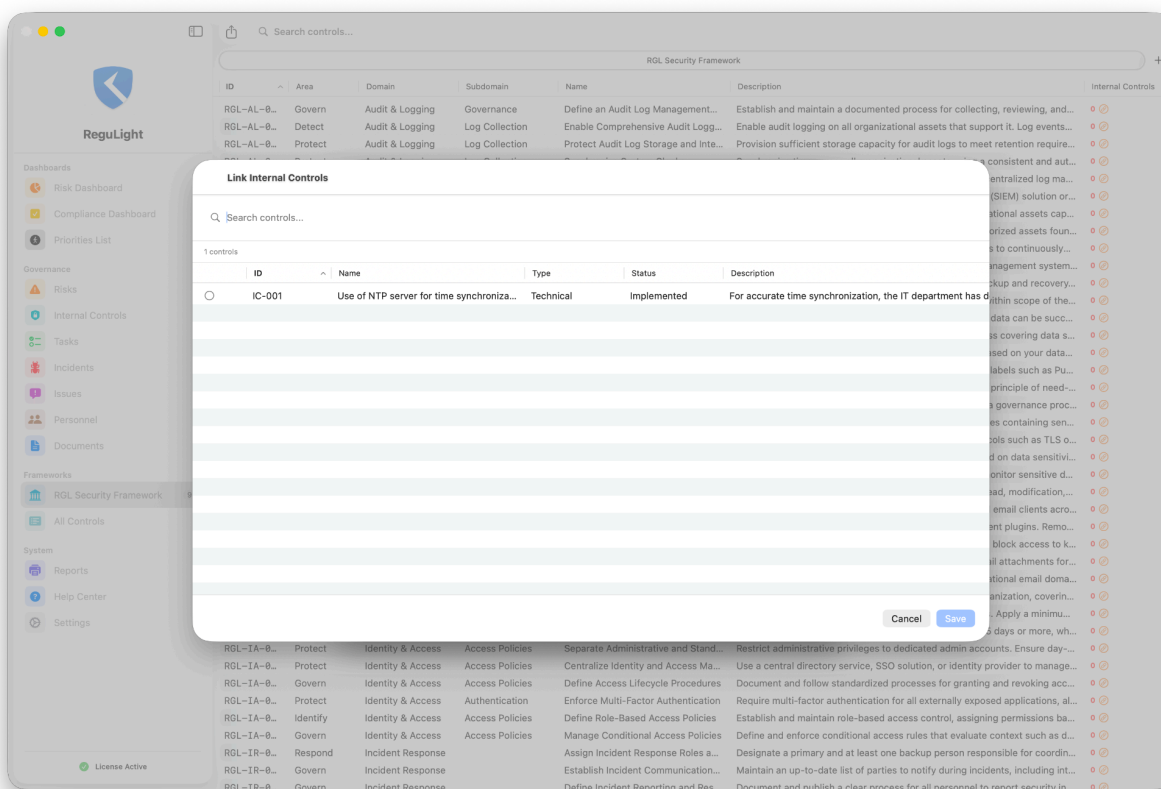
Buttons for 'Cancel' and 'Save' are at the bottom.



Method A: Via the Internal Control Dialog

If you are creating a new Internal Control from scratch:

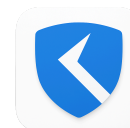
1. Go to the **Internal Controls** section in the sidebar.
2. Click **Add Internal Control** (or click the + sign in the ReguLight tool bar).
3. In the **Framework Mapping** section of the Add Control dialog, locate the **ReguLight Security Framework** (controls all start with RGL-).
4. Select the relevant Framework Control (e.g., *RGL-AM-004: Synchronize System Clocks*).



Method B: Via the Framework View

If you are reviewing a specific framework and want to assign existing measures:

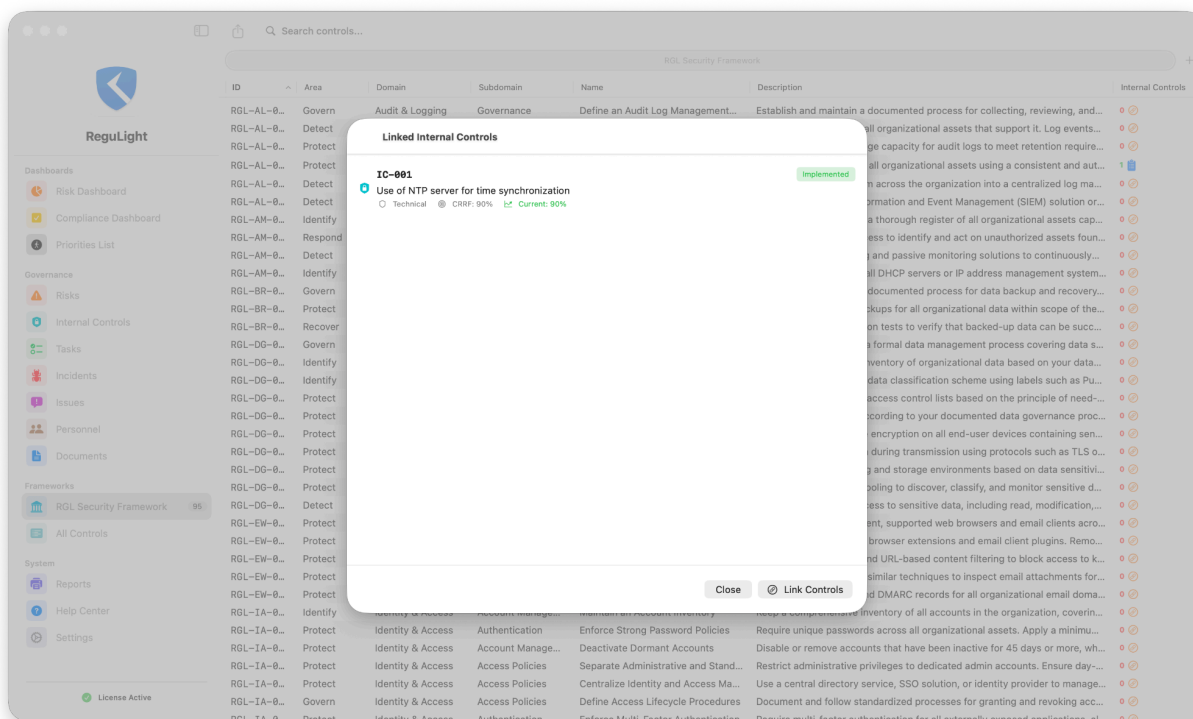
1. In the **Framework View**, select a control.
2. Click the **Link** icon in the **Internal Controls** column.
3. Select the appropriate internal measure from the list.



4. Reviewing Compliance Coverage

Once mapped, the **Framework View** becomes your primary verification tool.

- The **Internal Controls** column now displays the number of measures linked to each Framework Control.
- Clicking on the number in the Internal Controls column within this view will take you directly to the **Linked Internal Controls** overview where more Internal Controls can be linked (or removed) and you can drill-down to a filtered view of the Internal Controls list.

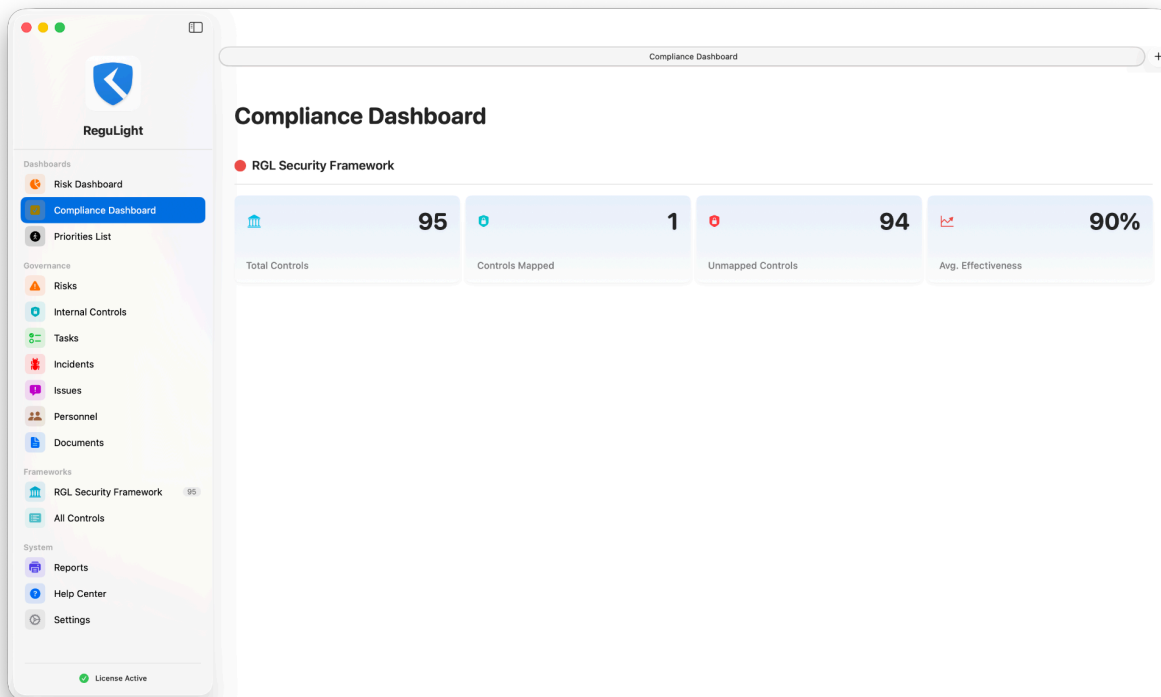
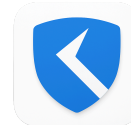


5. Visualizing Status via the Compliance Dashboard

The **Compliance Dashboard** provides a real-time summary of your posture. It tracks:

- **Mapped Controls:** How many requirements have an assigned internal measure.
- **Avg. Effectiveness:** The average effectiveness of linked Internal Controls.

Clicking on the tiles will take you to the filtered lists in the Frameworks section of the App.



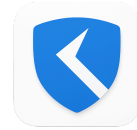
6. Understanding Dynamic Effectiveness

A Framework Control - **and therefore compliance** - is only as strong as the Internal Controls supporting it. ReguLight calculates the Internal **Control Effectiveness** dynamically.

The Effectiveness of an Internal Control (percentage) is automatically influenced by:

- **Overdue Tasks:** Are recurring actions (e.g., "Review Asset Log") being completed in time?
- **Issues:** Are there unresolved gaps or failures found during audits?
- **Incidents:** Are there any open incidents related to Internal Controls?
- **Overdue Document Reviews:** Are document review tasks completed in time?

Failure to complete a task or the occurrence of a related incident will automatically lower the effectiveness of the Internal Control, which in turn flags the Framework Control as "At Risk" on your dashboard.



7. Further Learning

The ReguLight App and website are designed to be explored. For deep dives into specific functions and logic:

- **In-App Help Center:** Take the Guided Tour and access detailed articles on *Getting Started*, *Risk Management*, *Working with Frameworks*, *Internal Control Logic* and *Risk Mapping*.
- **Documentation Site:** Visit regulight.eu/docs for general GRC information, ReguLight manuals, diagrams and documentation, and the ReguLight Security Framework CSV file.

