ReguLight

User Manual

Governance, Risk & Compliance Management for macOS

Version: **2.0**

Date: April 2026

Table of Contents

1. Introduction to Governance, Risk & Compliance (GRC)

Governance, Risk, and Compliance (GRC) is an integrated approach to managing an organization's governance structure, enterprise risk management practices, and regulatory compliance activities. Rather than treating these disciplines as separate silos, GRC unifies them into a coherent strategy that helps organizations achieve their objectives reliably, address uncertainty, and act with integrity.

1.1 What is GRC?

GRC stands for Governance, Risk, and Compliance. It is both a discipline and a set of practices that enable organizations to align their information technology with business objectives, manage risk effectively, and meet all industry and government regulations.

The concept of GRC emerged from the recognition that governance, risk management, and compliance are deeply interconnected. A failure in one area often cascades into others: poor governance leads to unmanaged risks, unmanaged risks lead to compliance failures, and compliance failures result in penalties, reputational damage, and operational disruption.

> **Definition**
> GRC is the integrated collection of capabilities that enable an organization to reliably achieve objectives (Governance), address uncertainty (Risk Management), and act with integrity (Compliance).
> — OCEG (Open Compliance & Ethics Group)

1.2 The Three Pillars of GRC

Governance

Governance refers to the system of rules, practices, and processes by which an organization is directed and controlled. It encompasses the mechanisms through which organizations, and those who manage them, are held accountable. Good governance ensures that the organization's strategy aligns with its mission and values, that decisions are made transparently, and that resources are used efficiently.

Key aspects of governance include:

- Setting organizational strategy, objectives, and direction
- Defining roles, responsibilities, and accountability structures
- Establishing policies, standards, and procedures
- Overseeing performance and ensuring alignment with objectives
- Board and management oversight and reporting

Risk Management

Risk Management is the systematic process of identifying, analyzing, evaluating, and treating risks that could affect the achievement of organizational objectives. It involves understanding the threats and opportunities an organization faces, assessing their potential impact and likelihood, and implementing appropriate controls to manage them to an acceptable level.

Risk management involves:

- Identifying potential threats and vulnerabilities
- Assessing the likelihood and impact of risk events
- Designing and implementing controls to mitigate risks
- Monitoring risk levels and control effectiveness over time
- Reporting on risk posture to stakeholders and leadership

Compliance

Compliance is the process of adhering to laws, regulations, industry standards, and internal policies. Organizations must comply with a wide range of requirements depending on their industry, geography, and the nature of their operations. Non-compliance can result in legal penalties, financial losses, reputational damage, and operational disruptions.

Compliance encompasses:

- Meeting legal and regulatory requirements (GDPR, HIPAA, SOX, NIS2, DORA, etc.)
- Adhering to industry standards and frameworks (ISO 27001, SOC 2, NIST, PCI DSS)
- Following internal policies, codes of conduct, and operating procedures
- Preparing for and passing audits and assessments (see Chapter 8 for the Audit module)
- Maintaining documentation and evidence of compliance activities

1.3 Why GRC Matters

In today's complex business environment, organizations face an ever-growing landscape of risks and regulatory requirements. Cyber threats are increasing in sophistication, regulatory frameworks are multiplying, and stakeholders demand greater transparency and accountability.

Without a structured GRC approach, organizations struggle to manage these challenges effectively.

Benefit	Description
Reduced Risk Exposure	Systematic identification and mitigation of threats before they materialize
Regulatory Compliance	Avoid penalties, fines, and legal action through proactive compliance management
Operational Efficiency	Eliminate redundant controls and streamline processes across departments
Better Decision Making	Risk-informed decisions based on accurate, real-time data
Stakeholder Trust	Build confidence with investors, customers, partners, and regulators
Cost Reduction	Prevent costly incidents, breaches, and compliance failures
Competitive Advantage	Certifications and compliance posture open business opportunities

1.4 Benefits of an Integrated GRC Approach

When governance, risk management, and compliance are managed as an integrated program rather than in isolation, organizations realize significant advantages. An integrated GRC approach breaks down silos between departments, enables cross-functional collaboration, and provides a holistic view of the organization's risk and compliance posture.

- **Single Source of Truth:** All GRC data in one place eliminates conflicting information and data silos across departments.
- **Dynamic Risk Assessment:** Risk scores update automatically as controls degrade or improve, providing real-time awareness of your risk posture.
- **Efficient Resource Allocation:** Identify where controls are needed most and avoid duplicating effort across compliance frameworks.
- **Audit Readiness:** Maintain continuous compliance rather than scrambling before audits. Use the Audit module to formally test controls, record findings, and track remediation. Evidence and documentation are always current.
- **Proactive Risk Management:** Detect control degradation early through monitoring dashboards and automated alerts, enabling timely corrective action.
- **Cross-Framework Mapping:** Map a single internal control to multiple framework requirements, reducing the total number of controls needed.

2. The ReguLight GRC Model

ReguLight implements a GRC model that integrates all aspects of governance, risk management, and compliance into a single, dynamic system. The model is designed specifically for small and medium-sized organizations and security and compliance consultants that need professional-grade GRC capabilities without the complexity and cost of enterprise solutions.

2.1 Overview

The ReguLight GRC Model is built around the principle that GRC elements do not exist in isolation. Risks are mitigated by Internal Controls, controls are validated by compliance frameworks, and the effectiveness of controls is influenced by real-world operational factors such as incidents, issues, and task completion. This interconnected approach means that changes in one area automatically propagate throughout the system, giving you a living, breathing view of your organization's GRC posture.

2.2 Key Components

The ReguLight GRC Model centers on nine interconnected components that work together to create a dynamic GRC ecosystem:

Component	Purpose	Key Feature
Risk Register	Identify, assess, and track organizational risks	4x4 matrix with inherent and residual risk scoring
Internal Controls	Define measures that mitigate identified risks	Dynamic effectiveness tracking with CRRF
Compliance Frameworks	Import and map regulatory requirements	CSV import with two-tier architecture
Task Management	Track operational activities maintaining controls	Due date tracking; overdue tasks degrade controls
Incident Management	Record security events and operational failures	Severity-based control degradation (0-50%)
Issue Management	Track audit findings and control gaps	Proportional effectiveness reduction by severity
Document Repository	Manage policies, procedures, and evidence	Review scheduling with overdue degradation
Personnel Directory	Assign ownership and accountability	Link people to controls, tasks, and risks

Audit Management	Examine controls, record findings, drive remediation	Three-level audit structure with finding escalation

2.3 How the Model Works

The ReguLight model operates on a continuous feedback loop. When you create risks and link internal controls to them, the system calculates residual risk based on current control effectiveness. As operational events occur (incidents are reported, tasks become overdue, issues are raised), control effectiveness automatically degrades, which in turn increases residual risk scores. Resolving these operational events restores control effectiveness and reduces risk.

This dynamic behavior ensures that your risk assessment is always current and reflects the actual state of your organization's defenses, rather than being a static point-in-time snapshot.

> **Tip**
> The interconnected nature of the ReguLight model means that a single action — such as resolving an incident — can simultaneously improve control effectiveness, reduce residual risk scores, and improve your compliance posture across multiple frameworks.

3. Getting Started with ReguLight

ReguLight is a lightweight GRC application for macOS, purpose-built for risk and compliance consultants and SMBs. It turns risk identification, assessment, and mitigation into a structured, auditable process — keeping organizations compliant and in control.

3.1 What is ReguLight?

ReguLight provides an integrated suite of modules and views for managing your, or your client's organization's GRC program:

Module	Description
Risk Management	Identify and assess risks using a 4x4 impact/likelihood matrix. Track inherent vs. residual risk, visualize heatmaps, and monitor risk drift over time.
Internal Controls	Document and manage controls that reduce risk exposure. Track control effectiveness dynamically based on operational factors like incidents and overdue tasks.
Task Management	Assign operational tasks to personnel, set due dates, and track completion. Tasks linked to controls affect their effectiveness when overdue.
Incident Management	Record and track security incidents, breaches, and operational failures. Critical incidents automatically degrade linked control effectiveness to 0%.
Issue Management	Track findings from audits, control gaps, and remediation items. Audit findings can be escalated directly to Issues. Issues reduce control effectiveness proportionally based on severity.
Personnel Directory	Maintain a directory of team members with roles, departments, and contact information. Link people to tasks, controls, and responsibilities.
Document Repository	Track policies, procedures, and compliance documents. Set review schedules and receive alerts for overdue reviews.
Audits & Findings	Create and manage audits with defined scopes, record findings with severity and status tracking, escalate findings to issues, and generate audit analysis reports.
Compliance Frameworks	Import and manage compliance frameworks (ISO 27001, SOC 2, NIST, HIPAA, etc.) via CSV. Map internal controls to framework requirements.

3.2 Navigating ReguLight

The sidebar provides quick access to all major features, organized into five sections:

1. Dashboards

- **Risk Dashboard:** High-level overview with risk heatmaps, control health, and key metrics
- **Compliance Dashboard:** Framework completion tracking and compliance posture
- **Priorities List:** Your personalized to-do list based on urgency and impact

2. Governance

- **Risks:** Browse and manage all risk scenarios
- **Internal Controls:** View and edit all controls
- **Tasks:** Operational tasks and due dates
- **Incidents:** Security incidents and breaches
- **Issues:** Audit findings and control gaps
- **Personnel:** Team directory
- **Documents:** Policies and procedures

3. Compliance

- **Audits:** Audit plans, scope, and execution records
- **Findings:** All audit observations across every audit, with filtering and search

4. Frameworks

- A list of all imported Compliance Frameworks and an All Controls view that lists all controls from all imported Frameworks in one overview.

5. System

- **Reports:** Generate PDF reports for stakeholders, including Audit Analysis Reports
- **Help Center:** Documentation and guides
- **Settings:** Configure organization, import/export data, backup/restore data

Navigation Tips

- **Hide/Show Sidebar:** Use Command + Control + S or View > Toggle Sidebar to maximize your workspace.
- **Multiple Tabs:** Show the tab bar using View > Show Tab Bar. Click + to open new tabs and view different sections simultaneously within the same window.

- **Multiple Windows:** Use Option + Command + N or File > New Window to open additional ReguLight windows. Work with different sections side by side.
- **Right-Click Context Menu:** Right-clicking any item in a list view opens a **context menu** with quick actions: View/Edit, Delete, Notify Owner. For Internal Controls, an additional **Control Map** option opens a graphical overview window.

Tip
Use tabs for quick context switching within a window, or open multiple windows across displays for maximum productivity. Keep your Risk Dashboard visible in one tab while managing controls and tasks in another.

3.3 Loading Demo Data

ReguLight includes demo scenarios to help you explore features without manually creating data. Navigate to Settings > Demo & Testing > Load Demo Data.

Scenario	Complexity	Description
Starter Organization	Low	Small organization starting their GRC journey. Minimal data, basic controls. Perfect for learning. This scenario aligns with the embedded Guided Tour.
Established Enterprise	High	Enterprise with a mature GRC program. Multiple frameworks, complex risk scenarios, full documentation.
Post-Breach Recovery	Medium	Organization recovering from a security incident. Open incidents, remediation tasks, elevated risk scores.
Healthcare Compliance	Medium	Healthcare provider with HIPAA/GDPR requirements. Patient data protection, privacy controls focus.

Loading options include **Add to Existing Data** (supplements current data) and **Wipe Before Loading** (deletes all existing data first, recommended for clean testing).

3.4 Wiping All Data (Fresh Start)

Warning
This action is PERMANENT and cannot be undone. All risks, controls, tasks, incidents, issues, audits, findings, documents, personnel, and frameworks will be deleted. Always create a backup first!

1. **Create a Backup** - Navigate to Settings > System Maintenance > Backup Database. Save the JSON file to a safe location.

2. **Navigate to Wipe Data** - Go to Settings > Demo & Testing > Wipe All Data.
3. **Confirm Deletion** - A confirmation dialog will appear. Read it carefully and click 'Wipe Everything' to proceed.
4. **System Reset Complete** - The app will now be empty. You can load demo data, restore from backup, or start building your GRC program from scratch.

3.5 Understanding the Dashboards

ReguLight provides three specialized dashboards for different aspects of your GRC program:

- **Risk Dashboard:** Your command center for risk management. View risk heatmaps (inherent vs. residual), track risk drift over time, monitor compromised controls, and see key metrics like average risk reduction.
- **Compliance Dashboard:** Track progress across compliance frameworks. See framework completion percentages, control implementation status, and upcoming requirements.
- **Priorities List:** Your personalized action list. Items are prioritized by urgency (due dates) and impact (severity). Focus on what matters most right now.

> **Tip**
> Use the Risk Dashboard as your daily starting point. The heatmaps give you an instant visual snapshot of your organization's risk posture.

3.6 Common Workflows

Creating a New Risk

1. Navigate to **Risks > Add Risk**
2. Set Impact and Likelihood (1-4 scale)
3. Assign a Risk Owner
4. Describe the risk scenario and potential consequences
5. Link existing Internal Controls (or create new ones first)
6. Review the Residual Risk calculation

Implementing an Internal Control

1. Navigate to **Internal Controls > Add Control**
2. Describe the Internal Control and assign a Control Owner
3. Choose Control Type (Preventive, Detective, Corrective, Organizational, Technical, or Physical)
4. Set CRRF (target effectiveness, 0-100%)
5. Set the current status to 'Draft', 'Implemented', or 'Managed'
6. Link to relevant Risks, Framework Controls, and Documents

Defining Tasks

1. Navigate to **Tasks > Add Task** (Task IDs are automatically generated)
2. Describe the Task and set a Due Date
3. Assign a Task Owner
4. Link the Task to an Internal Control

Handling an Incident

1. Navigate to **Incidents > Add Incident** (Incident IDs are automatically generated)
2. Set severity (Critical, High, Medium, Low)
3. Link to affected Internal Controls (automatically degrades effectiveness)
4. Link to impacted Frameworks
5. Assign an Incident Owner
6. Record remediation actions taken
7. Monitor risk scores — they may increase until the Incident is resolved

Running an Audit

1. Navigate to **Audits > Add Audit** and fill in audit details (title, type, lead auditor, dates)
2. Click “Define Audit Scope” to select the Internal Controls to be examined
3. Save the audit, then click “Add Finding” to record observations
4. For each finding, set severity, status, and link to in-scope controls
5. Escalate Critical and High findings to Issues for formal remediation tracking
6. Generate an Audit Analysis Report from the Reports section

Importing a Framework

1. Navigate to **Settings > Compliance Frameworks**
2. Download the ReguLight CSV Template (for format reference)
3. Prepare your CSV with framework controls
4. Click **Import Framework (CSV)**
5. Map imported Framework Controls to existing Internal Controls

> **Tip**
> Start registering your IT security and compliance measures right away. Download the free ReguLight Security Framework (www.regulight.eu/docs), import it into ReguLight, and map your existing Internal Controls to the framework's controls — your baseline is ready.

3.7 Tips for Success

- **Start small:** Don't try to document everything at once. Begin with your top 5-10 critical risks.
- **Use realistic CRRF values:** A control rated at 95% effectiveness is rarely achievable. Be conservative (60-80% is typical).
- **Review the Priorities List daily:** It adapts based on open Incidents, Issues, Tasks, Due Dates, and Severity.
- **Link everything:** Connect Internal Controls to Risks, Tasks to Controls, Documents to

Controls. This creates the dynamic effectiveness engine.

- **Monitor control drift:** Check the 'Compromised Controls' tile frequently. Address degrading controls before they become critical.
- **Export and backup data regularly:** Use Settings > Data Export for CSV files and Settings > Backup Database for full backups.
- **Use the Guided Tour:** Click 'Take the Guided Tour' in the Help Center for an interactive walkthrough of ReguLight's features.

4. Risk Management

Risk Management is the systematic process of identifying, assessing, and controlling threats to your organization. ReguLight provides a structured, quantitative approach to managing risk using industry-standard methodologies.

4.1 The 4x4 Risk Matrix

ReguLight uses a 4x4 risk matrix — the most widely adopted standard in enterprise risk management. Every risk is evaluated on two dimensions: Impact (consequence) and Likelihood (probability).

Impact (Consequence) - How severe would the damage be?

Level	Rating	Description
1	Insignificant	Minor inconvenience, no financial loss, no reputational damage
2	Minor	Limited financial loss (<$10K), temporary disruption, minor PR impact
3	Moderate	Significant financial loss ($10K-$100K), service disruption, regulatory notice
4	Major	Severe financial loss (>$100K), prolonged outage, regulatory fines, brand damage

Likelihood (Probability) - How often could this happen?

Level	Rating	Description
1	Rare	May occur only in exceptional circumstances (<5% annually)
2	Unlikely	Could occur at some time (5-25% annually)
3	Possible	Might occur at some time (25-50% annually)
4	Likely	Will probably occur in most circumstances (>50% annually)

Risk Score - Impact x Likelihood (Range: 1 - 16)

Risk Level	Score Range	Action Required
Low	1-3	Acceptable with routine monitoring
Medium	4-6	Requires management attention and controls
High	8-12	Significant concern, immediate action required
Critical	15-16	Unacceptable, escalate to senior leadership

4.2 Inherent vs. Residual Risk

ReguLight calculates risk twice for every scenario, giving you a before-and-after view of your control effectiveness:

- **Inherent Risk** is the risk level assuming **NO** Internal Controls exist. It represents the worst-case scenario if your organization had zero defenses. Inherent risk is based purely on the nature of the threat and its potential consequences.
- **Residual Risk** is the risk level **AFTER** your Internal Controls are applied. It reflects the real-world risk your organization faces today, accounting for all active controls and their current effectiveness.

Key Insight
The gap between Inherent and Residual Risk shows the **VALUE** your controls provide. A large gap means your controls are working well. A small gap means you need stronger controls or better implementation.

4.3 Risk Heatmaps: Visualizing Your Risk Portfolio

The Risk Dashboard displays two interactive heatmaps that provide instant visual insights into your risk landscape:

- **Inherent Risk Heatmap:** Shows the distribution of risks before controls. 4x4 grid with color-coded cells. Click any cell to view specific risks. Useful for strategic planning and control budgeting.
- **Residual Risk Heatmap:** Shows the distribution of risks after Internal Controls are applied. This is your ACTUAL risk posture and what you should report to leadership. Purple/red zones indicate control gaps.

Tip
Compare both heatmaps side-by-side. If they look nearly identical, your controls aren't working effectively.

4.4 Risk Drift: Tracking Changes Over Time

Risk is not static — it changes as controls degrade, incidents occur, and your organization evolves. ReguLight calculates Risk Drift to alert you when risks are getting worse:

Drift Direction	Meaning	Typical Causes
Positive (Worsening)	Risk score has increased	Control effectiveness dropped, new incidents, overdue tasks
No Drift (Stable)	Risk score is unchanged	Controls maintaining their effectiveness
Negative (Improving)	Risk score has decreased	New controls added, incidents resolved, effectiveness improved

Warning
Pay close attention to risks with positive drift! These indicate your controls are failing or degrading. Use the Risk Drift chart on the Risk Dashboard to spot trends.

4.5 Risk Categories & Organization

ReguLight allows you to organize risks into categories for better reporting and analysis:

Category	Examples
Cybersecurity	Cyberattacks, data breaches, system outages, ransomware
Technology	System outages, failing hardware, failing software
Operational	Process failures, human error, supply chain disruption
Legal	Liability claims, contract breaches, lawsuits
Financial	Fraud, market risk, credit default, currency fluctuation
Strategic	Reputation damage, competitive threats, M&A risks

4.6 Linking Controls to Reduce Risk

The most important action in risk management is linking Internal Controls to risks. This is how you demonstrate risk mitigation:

1. **Open a Risk Details View** — Navigate to Risks, select a risk scenario, and open its

details view.

2. **Enter Edit Mode** — Click Edit to enter edit mode and scroll down to the Mitigating Controls section.
3. **Select Relevant Controls** — Choose controls that directly address the risk. You can link multiple controls (defense in depth).
4. **Review Residual Risk** — The system automatically recalculates the Residual Risk based on control effectiveness.

Control Type	Risk Dimension Affected
Preventive	Reduces Likelihood (prevents threats from occurring)
Detective	Reduces Impact (identifies issues early to minimize damage)
Corrective	Reduces Impact (fixes problems after they occur)
Organizational	Reduces Likelihood (through policies, procedures, and training)
Technical	Reduces both Impact and Likelihood (through technology)
Physical	Reduces Likelihood (through physical barriers and access restrictions)

4.7 Risk Management Best Practices

- **Review risks quarterly:** Risk assessments should be living documents, not one-time exercises.
- **Be realistic about Impact/Likelihood:** Avoid inflating scores to get attention. Use objective criteria.
- **Document your assumptions:** In the risk description, explain WHY you chose those scores.
- **Don't ignore low risks:** Even low-scored risks should be monitored. Context changes over time.
- **Link multiple controls:** Defense in depth is stronger than single controls. One control failing shouldn't leave you exposed.
- **Monitor drift religiously:** Set a weekly reminder to check the Risk Drift chart. Early detection prevents crises.
- **Use risk categories for reporting:** Generate category-specific exports for different departments.
- **Escalate critical residual risks:** If a risk remains critical after controls, escalate to leadership immediately.

4.8 Common Risk Management Pitfalls

Warning
Avoid these common mistakes that undermine risk management programs:

- **Set-It-and-Forget-It:** Creating risks once and never updating them. Risk is dynamic. Incidents, new threats, and control changes require continuous updates.
- **Over-Rating Everything as Critical:** If every risk is 'critical', nothing is critical. Use the matrix honestly to enable proper prioritization.
- **Linking Irrelevant Controls:** Don't link controls just to reduce scores. Controls must genuinely address the risk threat vector.
- **Ignoring Control Degradation:** A control showing 100% effectiveness with 10 overdue tasks is a red flag. Investigate why effectiveness hasn't dropped.
- **No Risk Owner Accountability:** Every risk should have a designated owner responsible for monitoring and reporting.

5. Risk Calculation Engine (Deep Dive)

ReguLight uses a sophisticated risk calculation engine that models how Internal Controls reduce risk exposure. This chapter explains the complete methodology, including how control effectiveness degrades based on operational factors.

5.1 Inherent Risk: The Starting Point

Inherent Risk represents the risk level before any controls are applied:

Inherent Risk Score = Impact x Likelihood

- **Impact (1-4):** Severity of consequences if risk occurs
- **Likelihood (1-4):** Probability of occurrence
- **Score Range:** 1 (lowest) to 16 (highest)

5.2 Internal Controls: Your Defense Mechanism

Each Internal Control has two critical properties:

1. **Control Type:** Determines whether the control reduces Impact or Likelihood (Preventive/Organizational/Physical reduce Likelihood; Detective/Corrective reduce Impact; Technical reduces both).
2. **CRRF (Control Risk Reduction Factor):** The target effectiveness (0-100%) the control should achieve when operating perfectly. This represents the control's design capability.

5.3 Dynamic Control Effectiveness

The **Current Effectiveness** of a control is not static — it degrades based on real-world operational factors:

Current Effectiveness = CRRF x Worst Degradation Factor

Factor	Degradation	Effect
Critical/High Incidents	0%	Complete control failure — effectiveness drops to zero
Medium/Low Incidents	50%	Partial control failure — effectiveness reduced by 50%

Critical Issues	50%	Severe control gap — effectiveness reduced by 50%

Factor	Degradation	Effect
High Issues	30%	Significant control gap — effectiveness reduced by 30%
Medium Issues	20%	Moderate control gap — effectiveness reduced by 20%
Low Issues	10%	Minor control gap — effectiveness reduced by 10%
Overdue Operational Tasks	20%	Control maintenance neglected — effectiveness reduced by 20%
Overdue Document Reviews	20%	Document review neglected — effectiveness reduced by 20%

Warning
The system uses WORST CASE logic: if any factor completely fails (e.g., Critical Incident), the entire control's effectiveness becomes 0%, regardless of other factors.
Example: A control with CRRF of 80% and one overdue operational task would normally be at 64% $80% x 0.8). But if it also has a Critical incident, effectiveness becomes 0% immediately.

5.4 Residual Risk Calculation

Once Internal Controls are linked to a risk, ReguLight calculates the Residual Risk through a six-step process:

1. **Convert and Classify Controls:** Convert Current Effectiveness to decimal (80% becomes 0.80) and classify by type: Preventive/Organizational/Physical affect Likelihood; Detective/Corrective affect Impact; Technical affects both dimensions.
2. **Calculate Average Effectiveness:** For each dimension, calculate the average effectiveness of relevant controls. Using averages makes degradation visible — one failing control reduces the average significantly.
3. **Apply Diminishing Returns Multiplier:** Multiple controls provide layered defense with diminishing returns.
   Formula: 1.0 + (0.5 x extra controls), capped at 2.0x maximum. Example: 3 controls = 2.0x multiplier.
4. **Apply 90% Maximum Reduction Cap:** No control set can reduce risk by more than 90%. This prevents a 'zero risk' illusion and accounts for unknown threats and black swan events.

5. **Apply 85% Dampening Factor:** Real-world controls never work perfectly. A 0.85 dampening factor accounts for implementation gaps, human error, configuration drift, and integration issues.
6. **Calculate New Risk Values:** For each dimension: Residual = Inherent x (1 - (Reduction x 0.85)), rounded to nearest integer (1-4 range).

Residual Risk Score = Residual Impact x Residual Likelihood

5.5 Worked Example

Scenario: Unauthorized Access to Customer Database

Inherent Risk
Impact: 4 (Major) | Likelihood: 3 (Possible) | **Inherent Risk Score: 4 x 3 = 12 (High)**

Control ID	Name	Type	CRRF	Current	Reason
AC-001	Multi-Factor Authentication	Preventive	85%	85%	No issues
AC-002	Access Review Process	Detective	70%	56%	Overdue task (70% x 0.8)
IR-001	Incident Response Plan	Corrective	60%	48%	Medium issue (60% x 0.8)

Calculation Process

- **Likelihood Controls (Preventive):** AC-001: 85% = 0.85 | Average: 0.85 | Multiplier: 1.0 | Reduction: 0.85
- **Impact Controls (Detective + Corrective):** AC-002: 56% = 0.56 | IR-001: 48% = 0.48 | Average: 0.52 | Multiplier: 1.5 | Reduction: 0.78
- **Apply Caps:** Both under 90% cap
- **Apply Dampening (x0.85):**
  Likelihood: 3 x (1 - 0.85 x 0.85) = 0.83, rounded to 1
  Impact: 4 x (1 - 0.78 x 0.85) = 1.35, rounded to 1
- **Result:** Residual Impact: 1 (Insignificant) | Residual Likelihood: 1 (Rare) | Residual Risk Score: 1 x 1 = 1 (Low)

Result
The risk was reduced from High (12) to Low (1) by implementing three controls, even though two controls are operating below their target effectiveness due to operational issues.

5.6 Key Takeaways

- Control effectiveness is DYNAMIC — it changes as incidents, issues, and tasks evolve
- Different control types work on different dimensions (Impact vs. Likelihood)
- The system uses AVERAGE effectiveness (not sum), making control degradation immediately visible
- Multiple controls provide layered defense with diminishing returns (capped at 2x multiplier)
- 90% reduction cap prevents unrealistic 'zero risk' scenarios
- 85% dampening factor accounts for real-world implementation gaps and human error
- Monitor the 'Compromised Controls' tile on the Dashboard to catch degrading controls early
- Use the Risk Drift chart to identify risks worsening due to control effectiveness degradation

6. Internal Controls

Internal controls are the processes, policies, procedures, and technology that organizations put in place to ensure the integrity of information, promote accountability, and prevent fraud. They are fundamental to organizational governance and risk management. Think of Internal Controls as the checks and balances that help organizations achieve their objectives by minimizing risks.

6.1 What Are Internal Controls?

Internal controls are technical measures, policies, processes, and procedures designed to:

- Safeguard assets and resources
- Ensure accuracy and reliability of data (client information, financial records, etc.)
- Promote operational efficiency
- Ensure compliance with laws and regulations
- Prevent and detect fraud and errors

Every organization, regardless of size, needs internal controls to operate securely, effectively, and maintain stakeholder trust.

6.2 The Five Components of Internal Controls (COSO Framework)

#	Component	Description
1	**Control Environment**	The foundation for all other components. Includes the organization's integrity, ethical values, and competence of its people.
2	**Risk Assessment**	The process of identifying and analyzing relevant risks to achieving objectives, forming a basis for determining how risks should be managed.
3	**Control Activities**	The policies and procedures that help ensure management directives are carried out. Includes approvals, authorizations, verifications, and reconciliations.
4	**Information & Communication**	The systems that identify, capture, and communicate relevant information to enable people to carry out their responsibilities.
5	**Monitoring Activities**	Ongoing evaluations to ascertain whether each component of internal control is present and functioning.

6.3 Types of Internal Controls in ReguLight

ReguLight categorizes internal controls into six types based on their purpose and implementation:

Type	Purpose	Risk Dimension
Preventive	Stop errors or fraud before they occur (e.g., segregation of duties, access controls, input validation)	Reduces Likelihood
Detective	Discover errors or fraud after they occur (e.g., reconciliations, monitoring, reviews)	Reduces Impact
Corrective	Fix problems that have been identified (e.g., backup/ recovery, incident response)	Reduces Impact
Organizational	Prevent issues through structure and culture (e.g., security training, code of conduct)	Reduces Likelihood
Technical	Technology-based controls that both prevent and detect (e.g., firewalls, encryption, monitoring)	Reduces Both
Physical	Physical barriers and access restrictions (e.g., locks, cameras, badge readers)	Reduces Likelihood

Important
Understanding control types is crucial: they determine whether a control reduces the Likelihood or Impact dimension of a risk. Choose the type that matches your control's primary function.

6.4 Common Control Activities

Here are some fundamental control activities found in most organizations:

- **Segregation of Duties:** No single person should control all phases of a transaction. This reduces the risk of errors and fraud.
- **Authorization and Approval:** Transactions and activities must be authorized by appropriate personnel before execution.
- **Reconciliations:** Regular comparison of records to ensure data accuracy and identify discrepancies.
- **Physical Controls:** Securing assets through locks, safes, restricted access, and security systems.
- **Reviews and Verifications:** Regular management reviews of performance reports, exception reports, and key metrics.

6.5 Why Internal Controls Matter

Strong internal controls provide multiple benefits:

- **Risk Reduction:** Minimize financial losses and operational disruptions
- **Improved Accuracy:** Ensure reliable financial reporting and decision-making
- **Regulatory Compliance:** Meet legal and regulatory requirements
- **Fraud Prevention:** Deter and detect fraudulent activities
- **Operational Efficiency:** Streamline processes and reduce waste
- **Stakeholder Confidence:** Build trust with investors, customers, and regulators

6.6 Working with Internal Controls in ReguLight

ReguLight provides a sophisticated system for managing internal controls with dynamic effectiveness tracking:

- **CRRF (Control Risk Reduction Factor):** The target effectiveness (0-100%) your control should achieve when operating perfectly. Be realistic: 60-80% is typical for most controls.
- **Control Types:** Each type affects risk differently. Preventive/Organizational/Physical reduce Likelihood; Detective/Corrective reduce Impact; Technical reduces both dimensions.
- **Control Status:** Track implementation progress: Draft > Implemented > Managed > Depreciated. Only Implemented and Managed controls actively reduce risk.
- **Control Owner:** Assign a responsible person to each control. Owners are accountable for monitoring effectiveness and responding to degradation.

6.7 Linking Controls to Other GRC Elements

Internal Controls don't exist in isolation. ReguLight enables linking to create a dynamic GRC ecosystem:

Link To	Purpose	Effect on Effectiveness
Risks	Controls mitigate risks. Link to calculate Residual Risk.	More effective controls = lower residual risk
Tasks	Operational tasks maintain control effectiveness.	Overdue tasks reduce effectiveness to 80%
Incidents	Incidents reveal control failures.	Critical/High: 0%, Medium/Low: 50%

Link To	Purpose	Effect on Effectiveness
Issues	Issues are control gaps or weaknesses.	Critical: 50%, High: 30%, Medium: 20%, Low: 10%
Documents	Policies and procedures support controls.	Overdue reviews reduce effectiveness to 80%
Framework Controls	Map to compliance requirements.	Demonstrates regulatory compliance
Audits	Audits examine control effectiveness through formal testing.	Findings can be escalated to Issues, which degrade effectiveness

6.8 Monitoring Control Health

ReguLight provides multiple ways to monitor your controls and catch degradation early:

Tool	Location	Purpose
Compromised Controls Tile	Risk Dashboard	Shows controls with degraded effectiveness. Check weekly.
Risk Drift Chart	Risk Dashboard	Tracks changes in risk scores over time. Upward trends indicate control degradation.
Priorities List	Sidebar Navigation	Personalized to-do list showing overdue tasks and high-severity issues.
Control Detail View	Internal Controls View	Shows current effectiveness, CRRF, and all linked entities.
Internal Control Map	Right-Click > Control Map	Graphical overview showing all linked GRC components and degradation factors with clickable drill-down circles.

6.9 Best Practices for Internal Controls

- **Set realistic CRRF values:** 60-80% is typical. Controls rated at 95%+ effectiveness are rarely sustainable.
- **Assign owners to every Internal Control:** Accountability is critical for maintaining effectiveness.
- **Link controls to risks:** Unlinked controls don't reduce risk scores. Show the value of your controls.
- **Create maintenance tasks:** Regular reviews, audits, and updates keep controls operating effectively.

- **Monitor the Compromised Controls tile:** Weekly checks help you catch degradation before it becomes critical.
- **Document your controls thoroughly:** Explain HOW the control works, not just WHAT it does.
- **Link to supporting documents:** Attach policies, SOPs, and evidence to demonstrate implementation.
- **Close Incidents and Issues promptly:** Open incidents/issues degrade effectiveness. Resolve them quickly.
- **Use the right control type:** The type determines which risk dimension is affected.
- **Review control effectiveness quarterly:** Adjust CRRF values based on actual performance and testing.

6.10 Common Pitfalls to Avoid

> **Warning**
> Avoid these mistakes when managing Internal Controls:

- **Ignoring Effectiveness Degradation:** A control showing 100% effectiveness with 5 overdue tasks is broken. Investigate why it's not updating.
- **Setting Unrealistic CRRF Values:** Rating every control at 95-100% effectiveness creates false confidence. Be honest about control limitations.
- **Not Linking Controls to Risks:** Unlinked controls don't reduce residual risk scores. If controls aren't mitigating risks, why do they exist?
- **No Control Owner Assigned:** Controls without owners lack accountability. When effectiveness degrades, who's responsible for fixing it?
- **Leaving Incidents/Issues Open:** Open incidents degrade control effectiveness to 0-50%. Close them promptly to restore effectiveness.
- **No Maintenance Tasks:** Controls require ongoing maintenance. Create recurring tasks to ensure controls stay effective.

7. Compliance Frameworks

Compliance frameworks are structured sets of requirements, controls, and best practices that help organizations meet regulatory, industry, or security standards. ReguLight enables you to import, manage, and map these frameworks to your Internal Controls.

7.1 Why Frameworks Are Integral to GRC

- **Regulatory Compliance:** Meet legal and industry requirements (HIPAA, SOC 2, ISO 27001, GDPR, NIS2, NIST, etc.) by demonstrating adherence to established control frameworks.
- **Best Practice Guidance:** Leverage industry-proven controls rather than building everything from scratch. Frameworks represent decades of collective expertise.
- **Audit Readiness:** Auditors expect framework alignment. Mapping controls to requirements streamlines audits and demonstrates due diligence. Use the Audit module (Chapter 8) to formally record audit evidence and findings.
- **Customer Trust:** Certifications like SOC 2 Type II or ISO 27001 are often prerequisites for enterprise contracts.
- **Progress Measurement:** Frameworks provide clear completion metrics with percentage-based progress indicators.
- **Gap Identification:** Mapping controls to requirements instantly identifies gaps where controls are missing or incomplete.

7.2 How Frameworks Work in ReguLight

ReguLight uses a two-tier architecture that separates framework requirements from your operational Internal Controls:

Framework Controls (Tier 1) - The 'What'

These are the control requirements defined by external standards bodies (ISO, DORA, NIST, AICPA, etc.). They describe **WHAT** needs to be done to comply. They include reference IDs, control descriptions, and are grouped by domain/category. Framework controls can be edited after import by double-clicking the first column or using the right-click context menu.

Internal Controls (Tier 2) - The 'How'

These are **YOUR** organization's specific policies, procedures, technology, and processes that fulfill the framework requirements. They describe **HOW** you meet the standard. They are fully customizable, track effectiveness dynamically, and can map to multiple framework controls.

Key Concept
Framework Controls define requirements. Internal Controls implement solutions. Mapping connects them.

7.3 Importing Frameworks via CSV

ReguLight allows you to import any compliance framework using a standardized CSV template:

1. **Download the CSV Template** - Navigate to Settings > Compliance Frameworks > Download CSV Template for the correct format.
2. **Prepare Your Framework Data** - Populate the CSV with framework controls. Each row represents one control requirement.
3. **Required CSV Columns** - Your CSV must include 6 columns: ID (control reference), Area (high-level category), Domain (subcategory), Subdomain (optional), Name (short title), Description (full requirement text).
4. **Import the Framework** - Go to Settings > Compliance Frameworks > Import Framework (CSV), select your file. The framework name matches your CSV filename.
5. **Verify Import** - Check the Frameworks section in the sidebar to see your newly imported framework.

CSV Format Example (ISO 27001):

ID	Area	Domain	Subdomain	Name	Description
A.9.1.1	Access Control	Business Req.		Access Control Policy	An access control policy shall be established
A.9.2.1	Access Control	User Access Mgmt		User Registration	A formal user registration process shall be implemented
A.9.2.2	Access Control	User Access Mgmt		Privileged Access	Allocation of privileged access rights shall be controlled

7.4 Mapping Internal Controls to Framework Requirements

Mapping is how you demonstrate compliance. It connects your implementation to framework requirements:

1. **Navigate to a Framework Control** - In the sidebar Frameworks section, select a framework, click on a specific control. Double-click in the first column or right-click 'View/Edit' to open details. Press 'Edit' to enter edit mode.
2. **Enter the Link Internal Controls View** - Press the 'Link Controls' button in the Internal Control Mapping section.
3. **Select Relevant Internal Controls** - Choose one or more controls that implement the requirement. Use the Search function to quickly find controls. Click 'Save'.
4. **Review Mapping Status** - The framework control's status automatically updates: Unmapped (no controls linked), Partially Mapped (some controls linked), Fully Mapped (controls linked and Implemented/Managed).

> **Tip**
> You can also quickly access the Link Internal Controls view by clicking the icon in the 'Internal Controls' column of the Framework view, or map from Internal Control detail views by linking them to framework controls.

7.5 The Compliance Dashboard

The Compliance Dashboard provides a framework-by-framework overview of your compliance status:

Metric	Description
Total Controls	The total number of framework controls in the compliance framework. Click to view all.
Controls Mapped	Framework controls with at least one Internal Control mapped. Click to view mapped controls.
Unmapped Controls	Framework controls with no Internal Controls — your compliance gaps. Click for targeted remediation.
Average Effectiveness	Average Current Effectiveness of all mapped Internal Controls, based on the highest-effectiveness control per framework control.

Framework Health
Each framework tile displays a colored health indicator: green = good coverage and effectiveness, orange = moderate, red = needs attention, gray = no controls mapped.

7.6 Popular Compliance Frameworks

Framework	Focus Area	Best For
ISO 27001:2022	Information security management (93 controls, 4 themes)	Companies needing formal certification for clients/regulators
SOC 2 Type II	Trust Service Criteria (Security, Availability, etc.)	SaaS companies and service providers processing customer data
NIST CSF	Cybersecurity (Identify, Protect, Detect, Respond, Recover)	Organizations seeking flexible, risk-based cybersecurity approach
HIPAA	Healthcare data protection (Administrative, Physical, Technical safeguards)	US healthcare providers and business associates handling PHI
GDPR	EU data protection (consent, data rights, breach notification)	Any organization processing personal data of EU residents
NIS2	EU critical infrastructure cybersecurity	Essential/important service operators in critical EU sectors
PCI DSS	Payment card data security (12 requirements, 6 objectives)	Organizations storing, processing, or transmitting credit card data

7.7 Framework Management Best Practices

- **Start with one framework:** Don't try to implement multiple frameworks simultaneously. Focus on one until it's mature.
- **Map incrementally:** Prioritize high-risk or audit-critical controls first.
- **One Internal Control, multiple framework requirements:** Design controls that satisfy multiple requirements to avoid duplication.
- **Document your rationale:** Explain HOW each Internal Control satisfies the framework requirement. Auditors will ask.
- **Review mappings quarterly:** As your controls evolve, ensure mappings remain accurate.
- **Use the Compliance Dashboard for reporting:** Generate overviews showing framework completion for executives and auditors.
- **Track control effectiveness:** Framework compliance isn't binary — effectiveness matters. Monitor your mapped controls' health.

7.8 Framework Implementation Pitfalls

Warning
Avoid these common mistakes when working with compliance frameworks:

- **Checkbox Compliance:** Mapping controls just to show 100% completion without actual implementation. Auditors will test your controls.
- **Copy-Paste from Framework Text:** Using framework language verbatim as your internal control. Describe YOUR specific implementation.
- **Ignoring Control Effectiveness:** Mapping a control and forgetting about it. If it degrades, your compliance suffers.
- **Over-Mapping:** Linking every control to dozens of framework controls. Be specific - only map genuine implementation relationships.
- **No Evidence Trail:** Mapping without documenting evidence. Link documents and tasks to prove implementation.

7.9 ReguLight Security Framework

The ReguLight Security Framework is available as a free download from the ReguLight website (www.regulight.eu/docs). Consisting of 95 distinct requirements, it is designed to enhance the security posture of your ICT systems and IT operations.

Importing this framework into ReguLight enables you to map your existing Internal Controls and risk assessments, providing a structured foundation for registering and managing compliance measures.

8. Audits & Findings

The Audit module in ReguLight brings structured evidence collection to your GRC program. Audits let you formally examine whether your controls are working as intended, document what you find, and drive remediation through the Issue management system — creating a closed loop from observation to resolution.

8.1 The Three-Level Audit Structure

ReguLight organizes audit work into three nested levels. Understanding this hierarchy is key to using the module effectively:

Level	Description
Audit	The execution record. An Audit is a specific audit event that records who audited (lead auditor), the audit type, start and end dates, the overall conclusion, and the status of the audit itself. The scope (Audit Set) is defined as part of creating the audit.
Audit Set	The scope definition. An Audit Set is created inside the audit creation form. It defines which Internal Controls will be examined. Each audit has its own dedicated scope — defined once, when the audit is created.
Audit Finding	The individual observation. A Finding is a specific observation, deficiency, or non-conformity discovered during the audit. Each finding is assigned a severity and status (required), an optional due date, and can be linked to controls in the audit's scope.

Tip
The hierarchy flows as: Audit → Audit Set → Findings. The scope is defined during audit creation, and many findings can be recorded per audit.

8.2 Creating and Running an Audit

Start by creating a new audit. Fill in the audit details, then use the "Define Audit Scope" button in the Audit Scope section to set up the Audit Set. Each audit captures a complete picture of the audit event:

Field	Description
Title	A clear, descriptive name for the audit event (required)
Scope Description	Narrative description of what is being examined and how

Type	Internal · External · Regulatory · Self-Assessment
Status	Planning · In Progress · Review · Closed
Lead Auditor	Selected from your People register
Start Date	The start date of the audit (required)
End Date	Optional — enable with the “Set End Date” toggle
Conclusion	Free-text field for the overall audit opinion and observations

Tip
Findings can only be added after the audit is first saved. Once saved, an “Add Finding” button appears in the Findings section of the audit form.

The Findings column in the Audit list shows how many findings exist for each audit. Click the count to jump directly to the Findings panel filtered to that audit.

8.3 Audit Sets — Defining the Scope

The scope of an audit is defined as part of creating the audit itself. Click “Define Audit Scope” inside the audit creation form to open the scope builder, where you select the Internal Controls that will be examined in this audit:

1. Name the scope — Give the scope a meaningful name (e.g., “Q2 2026 IAM Assessment”) so it is clear what this audit examines.
2. Select in-scope controls — Tick the specific Internal Controls to be tested. Use the search bar to filter by control ID, title, or type. Use “Select All” to select all currently visible controls. The selected count is shown in the header.
3. Confirm Scope — Click “Confirm Scope” to apply the selection. The button is disabled until a name is entered and at least one control is selected.

Tip
Each audit has its own dedicated scope. To run a similar audit again, create a new audit and redefine the scope in the scope builder. The scope can also be edited later via the “Edit Scope” button in the audit form.

8.4 Recording Audit Findings

Findings are the heart of the audit. Each finding documents a specific observation with enough detail to drive remediation. Add findings from within the audit form after saving the audit. Each finding has the following fields:

Field	Description
Title	Short, specific description of the observation (required)
Description	Detailed narrative: what was tested, what was expected, what was found
Severity	Low · Medium · High · Critical (see below)
Status	Open · Accepted · Remediated (default: Open)
Due Date	Optional — enable with the “Set Due Date” toggle
Linked Controls	Select from controls in the audit’s scope. Only visible if an Audit Set with controls has been defined.

Severity Levels

Severity	Description
Critical	Control is completely failing or absent. Immediate escalation required. Should always be raised as an Issue.
High	Significant deficiency. The control is ineffective or frequently bypassed. Escalation strongly recommended.
Medium	Partial control effectiveness. Notable gaps in design or operation. Remediation required within the agreed due date.
Low	Minor observation. The control mostly works but could be strengthened. Address in the next review cycle.

Finding Status

Status	Description
Open	The finding is acknowledged and awaiting remediation. This is the default status on creation.
Accepted	The residual risk has been formally accepted — no remediation will be performed. Requires documented justification in the description.
Remediated	The control failure has been addressed and the finding is resolved. Evidence of remediation should be noted.

Warning
Do not mark a finding as Remediated without verifying the fix. Premature closure of findings undermines audit credibility and gives a false sense of security.

8.5 Escalating Findings to Issues

When a finding requires formal remediation tracking with ownership, deadlines, and management visibility, escalate it to an Issue. This links the audit observation directly into your Issues register:

1. Raise Issue on Save (new findings) — When creating a new finding, enable the “Raise Issue on Save” toggle. ReguLight automatically creates a linked Issue of type “Finding” when the finding is saved — no need to reopen the finding afterwards.
2. Escalate from an existing finding — Open any finding that has not yet been escalated, then click “Escalate to Issue” in the Escalation section. A confirmation dialog appears; confirm to create the Issue immediately.
3. Navigate to the linked Issue — In the Findings panel, the Issue column shows the linked issue’s reference ID. Click it to navigate directly to the Issues view filtered to that specific issue.

When escalating, ReguLight auto-populates the following Issue fields:

Issue Field	Auto-populated Value
Type	Always set to “Finding”
Title	Copied from the finding title
Description	Finding description plus the audit reference
Impact Level	Critical → 4 · High → 3 · Medium → 2 · Low → 1
Due Date	Copied from the finding due date (if set)
Linked Controls	Copied from the finding’s linked Internal Controls

Tip
Escalating Critical and High findings ensures they are tracked with the same rigour as other issues — with an assigned owner, due date, and status visible in dashboards and reports.

Independent lifecycle: deleting an Issue does not delete its source Finding, and deleting a Finding does not delete its linked Issue. Only the link between them is removed.

8.6 The Findings Panel

The Findings panel (under Compliance in the sidebar) provides a global view of all audit findings across every audit. Use it to monitor the overall state of audit observations organization-wide:

- **Filter by Audit:** Filter by Audit — click the bold findings count in the Audit list to open the

Findings panel pre-filtered to that audit.

- **Hide Remediated:** Enable the checkbox to focus only on open and accepted findings requiring action.
- **Search:** Find findings across title, description, severity, status, or linked audit in real time.
- **Issue Drill-Down:** Click a linked issue reference in the Issue column to navigate directly to that Issue.
- **Sort by Any Column:** Click a column header to sort findings by ID, severity, status, audit, due date, or linked issue.

8.7 Audit Analysis Report

Generate a formal PDF Audit Analysis Report from the Reports section. The report is structured for professional use and includes:

- Executive metrics: Total Audits (with closed count), Total Findings (with open count), Critical Findings, and Remediation Rate
- Charts: Findings by Severity (bar chart) and Findings by Status (donut chart)
- Audit Ledger table: Audit ID, title, type, status, and findings count (open / total)
- Findings Ledger table: severity, finding title, linked audit ID, status, and due date

> **Tip**
> Generate the report immediately after completing an audit to capture the findings at a point in time. Finding statuses change as remediation progresses.

8.8 Audit Best Practices

- **Keep Audit Sets stable:** Keep Audit Sets stable: only change the in-scope controls when the scope genuinely changes, not between cycles. Consistency enables trend analysis.
- **Assign a lead auditor:** Every audit should have a named responsible person. This ensures accountability and is required for formal audit reports.
- **Set realistic due dates on findings:** An aggressive due date that cannot be met is worse than a realistic one that drives actual remediation.
- **Escalate Critical and High findings immediately:** Do not wait until the audit is complete. Raise issues as findings are recorded so remediation can start early.
- **Use Accepted status deliberately:** Only accept a finding if the risk has been formally reviewed and signed off by a risk owner. Document the justification in the description.
- **Review findings from previous audits:** Before starting a new audit cycle, check whether prior findings have been remediated. Repeat findings indicate systemic control failures.
- **Link findings to controls:** Always link a finding to the relevant Internal Control(s). This creates traceability and enables reporting on which controls have the most findings.
- **Close the loop via Issues:** A finding marked Remediated should correspond to a closed

Issue. If there is no linked Issue, document the remediation evidence in the finding description.

8.9 Common Audit Pitfalls

> **Warning**
> Avoid these common mistakes that reduce the value of your audit programme:

- **Closing Findings Too Quickly:** Marking a finding Remediated before the fix is verified and tested gives a false picture of your control environment. Verify before closing.
- **Audit Without a Set:** Creating audits without a defined Audit Set makes scope unclear. Always define what is in scope before starting fieldwork.
- **Ignoring Repeat Findings:** A finding that appears in two or more consecutive audits indicates the root cause was never addressed. Investigate underlying process failures, not just symptoms.
- **Not Escalating Critical Findings:** A Critical finding that sits as Open for weeks without an Issue and owner defeats the purpose of the audit. Escalate immediately and assign ownership.
- **Vague Finding Descriptions:** “Control not effective” is not a useful finding. Describe exactly what was tested, what was expected, and what was observed. Findings without evidence cannot be actioned.

9. Support & Resources

ReguLight is provided to help businesses manage their Governance, Risk, and Compliance needs. This chapter outlines the available support channels and resources.

9.1 Getting Help

Your primary source of information is built directly into the application. ReguLight includes demo data sets, an embedded Guided Tour and Help Center that guides you through all features and functionality.

9.2 Additional Resources

The ReguLight website offers additional documentation covering general GRC topics and specific guidance on using ReguLight. These resources are available to all users and are regularly updated.

Resource	URL
Documentation	www.regulight.eu/docs
Online Support Page	www.regulight.eu/support
Privacy Policy	www.regulight.eu/privacy
End User License Agreement	www.regulight.eu/eula

9.3 Contact Information

For:	Email	Purpose
Technical Support	support@regulight.eu	Problems, questions, issues, or comments about ReguLight
General Inquiries	info@regulight.eu	General questions about ReguLight
Company Inquiries	info@itsecuconsult.com	Information about the company behind ReguLight
Privacy & Data Protection	privacy@itsecuconsult.com	Questions about privacy, data collection, and data protection