Helping Clients Build Their GRC System with ReguLight

How independent IT Security, Risk and Compliance consultants can use ReguLight to set up — and hand over — a working GRC framework for clients facing NIS2, ISO 27001 or their first structured security program.

If you operate as an independent IT Security, Risk or Compliance consultant, an increasing share of your work probably looks like this: a small or medium-sized client calls because they are suddenly in scope for NIS2, because a customer asked them to demonstrate ISO 27001 alignment, or because they have decided — often after a near-miss incident — to finally start managing their IT security and risk in a structured way.

These organizations rarely have a CISO, a risk manager or a GRC platform. What they have is one IT manager, a few policies in a SharePoint folder, and a deadline. Your job is to bring structure, knowledge and a methodology — and ideally to leave behind a working system that the client can continue to use long after your engagement ends.

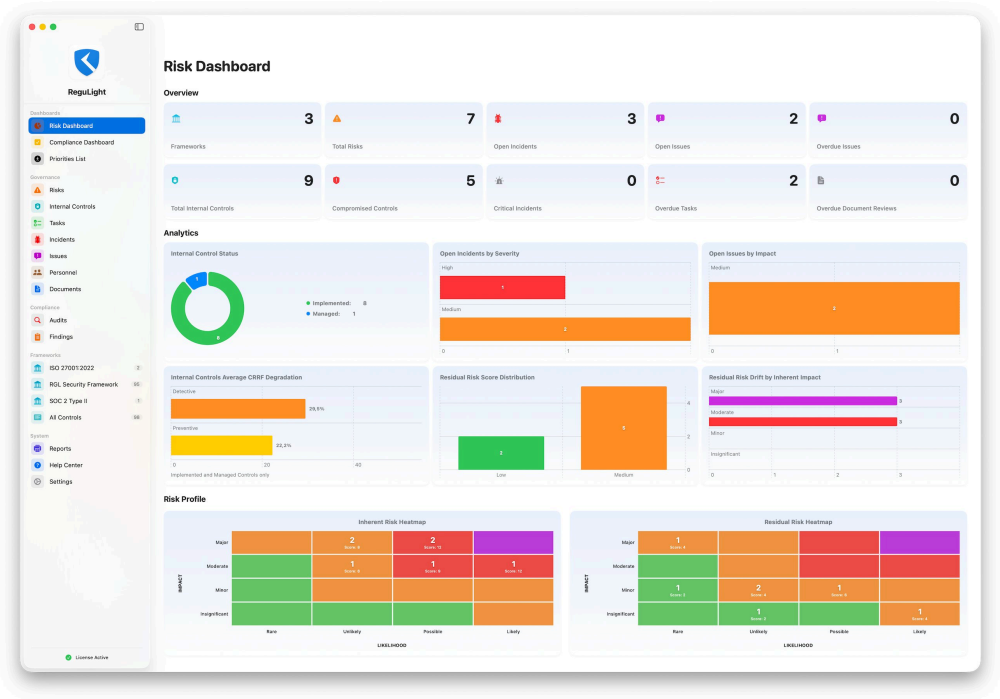
That last part is where most consultants run into the same problem. The artifacts you produce in spreadsheets and Word documents are excellent deliverables, but they are not a system. Once you walk out the door, they age fast. Three months later the risk register is out of date, the control list is no longer maintained, and the client is back where they started — only now with a thicker binder.

ReguLight is designed specifically to break that cycle.

A native macOS app the client can actually adopt

ReguLight is a lightweight, native Mac app that gives an organization a complete GRC environment — risks, internal controls, tasks, incidents, issues, audits, frameworks and reports — running entirely on a MacBook. No cloud tenancy, no implementation project, no IT integration. You install it from the Mac App Store, and within minutes you have a working environment.

For consultants, this can change the engagement model. Instead of building deliverables that live in your own toolset, you build the client's GRC system directly inside the app that will be installed on their Mac. From the very first workshop, the work you do is theirs. When the engagement ends, you do not hand over a folder of documents — you hand over a live, structured, dynamic GRC system that reflects their actual organization, with a methodology and a tool they can keep using.



Risk Dashboard — the live picture the client keeps after you leave.

How a typical SMB engagement unfolds

Phase 1 — Setting it up together

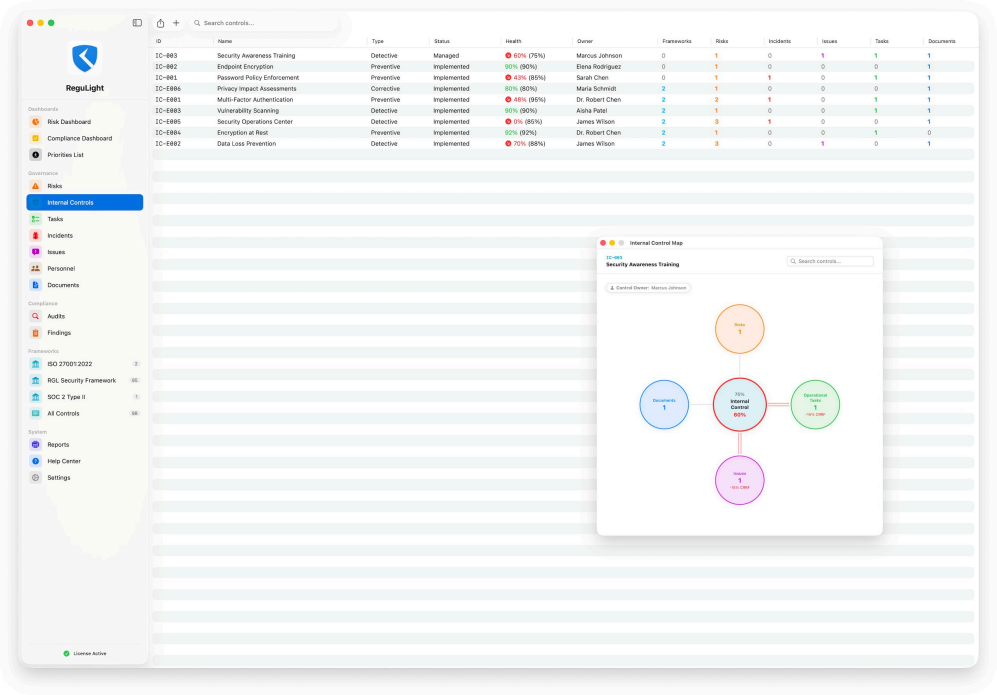
The first phase typically happens on your own MacBook. You set up a fresh ReguLight database for the client, import the RGL Security Framework as a baseline (more on that below), and start modeling: documenting the organization's first set of risks, defining internal controls, registering key personnel, and mapping the controls to ISO 27001:2022, NIS2 or whichever frameworks apply. Doing this on your own machine means you can prepare offline between sessions, demo the working model in the next workshop, and refine the structure without disrupting the client's environment.

Once the initial model is in good shape, you simply back up the ReguLight database and restore it on the client's Mac. From that moment on, the work continues in the client's own environment — and it has been theirs from the start. This is, in practice, the most natural way to run an SMB engagement: model on your Mac, hand over to theirs.

Because everything runs locally, there are no procurement hurdles, no DPAs, no IT change requests on either side. You are productive on day one.

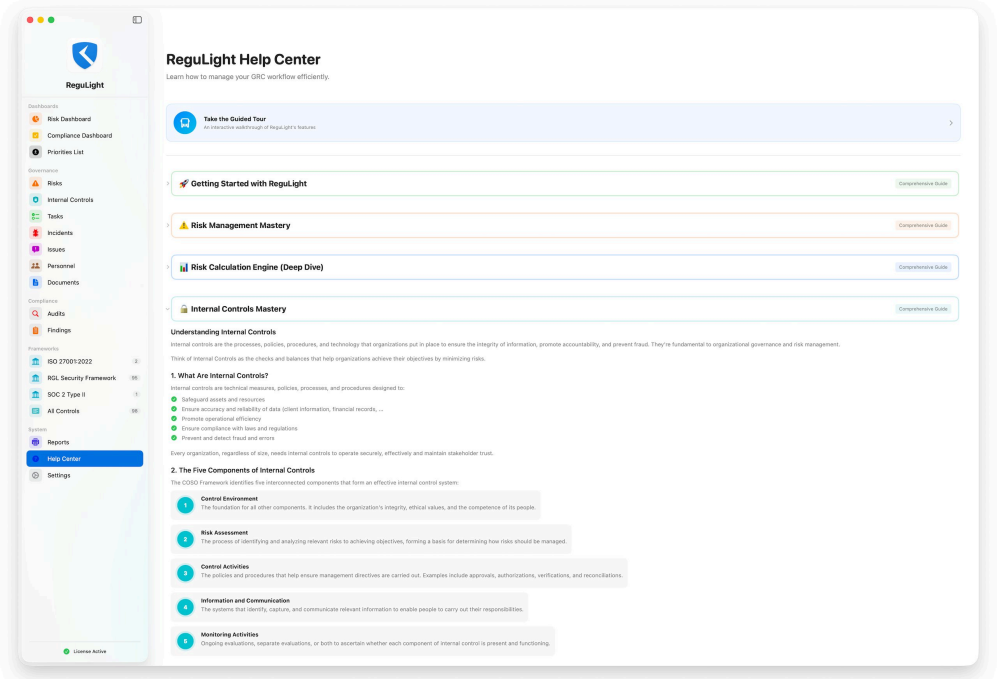
Phase 2 — Bringing the client into the work

With the database now installed on the client's Mac, the second phase is where ReguLight earns its keep as a consultant's tool. You shift from doing the work for the client to doing it with them, side by side at their machine. The Internal Controls module, with its visual Control Map, becomes a teaching aid: you walk the control owner through the relationships between a control, its risks, its tasks and any open incidents or issues. The conversation stops being abstract and starts being operational.



Internal Controls and Control Map — a visual teaching aid for control owners.

This is also where the learning curve flattens. ReguLight has an extensive built-in Help Center with comprehensive guides on Risk Management, the Risk Calculation Engine, Internal Controls, Frameworks and the Audit module. The accompanying documentation on www.regulight.eu adds further depth. Clients who have never thought systematically about GRC suddenly have a structured reference at their fingertips, written in plain language and linked directly to the screens they are working in.



Help Center — comprehensive in-app guides that make GRC concepts accessible.

Phase 3 — The hand-over

By the end of the engagement, the client is no longer dependent on you for routine GRC work. They open ReguLight, see their dashboard, work their priorities list, close their tasks, log their incidents, and run their reports. You move into an advisory role — a quarterly review, an audit, a strategic refresh — instead of being the only person who can keep the system alive. That is the right relationship for both sides, and it is the relationship most SMB clients actually want.

Why ReguLight is also a learning system

One of the quieter strengths of ReguLight is how much GRC knowledge it embeds in the product itself. For clients new to the field, this matters as much as the functionality.

The RGL Security Framework — a free, ready-to-use baseline

The RGL Security Framework is a 95-control framework, freely downloadable from www.regulight.eu and importable directly into ReguLight. It is organized around the familiar Identify, Protect, Detect, Respond, Recover and Govern areas, with clear domain groupings and original control wording. For an SMB starting from scratch, this is a defensible, sensible baseline on day one — no need to invent a control set, no license concerns, no months of debate. As a consultant, you can map it onto whichever regulatory framework the client is facing, and you have a starting point that the client can read, understand and own.

The Help Center — built-in GRC education

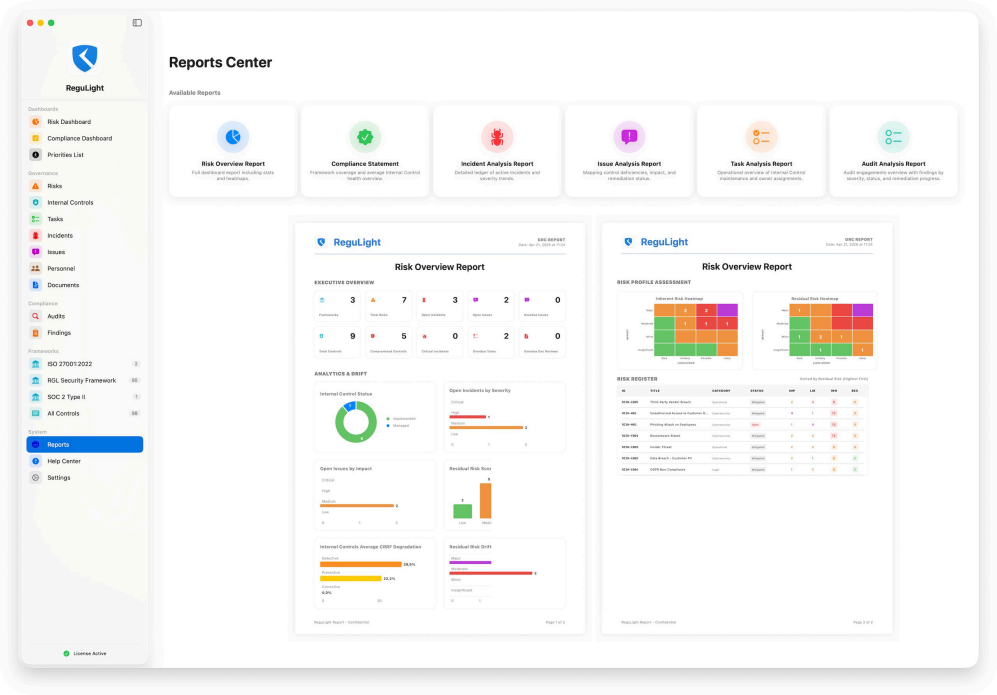
The Help Center inside the app is not an afterthought. It contains structured guides — Getting Started, Risk Management Mastery, Risk Calculation Engine (Deep Dive), Internal Controls Mastery, Frameworks, Audits — written specifically for people who are new to GRC. Clients who would never read a 400-page ISO standard will read these. They learn the concepts in the same place they apply them, which is the most efficient form of professional learning there is.

The website documentation

Beyond the in-app material, www.regulight.eu hosts further documentation and reference content. As a consultant, you can point a curious control owner there between sessions and trust that what they read aligns with what they will see on screen. The terminology, the methodology and the calculations are consistent across the app, the Help Center and the public documentation.

Reports the client can take to the board

From the Reports Center you generate branded PDF reports — Risk Overview, Compliance Statement, Incident Analysis, Issue Analysis, Task Analysis and Audit Analysis — that the client can take straight into a management meeting or a customer due-diligence review. After your engagement, the client can produce these themselves, with the same professionalism. That continuity is exactly what gives an SMB the confidence to keep going.



Reports Center — six PDF report types the client can generate themselves.

What it costs and how to evaluate it

ReguLight is free to download from the Mac App Store, with full functionality available against four built-in demo scenarios. As a consultant, you can spend an afternoon exploring every module — risks, controls, audits, reports, the Help Center — before deciding whether it fits your practice. For active use with real client data, the subscription is €49.99 per month or €549.99 per year. For the client's own continued use after hand-over, the same pricing applies — and for an SMB, that is a meaningful step down from anything resembling an enterprise GRC seat.

The natural way to start is to install ReguLight on your own MacBook, run through the demo data, generate a Risk Overview and an Audit Analysis Report, and judge it against the way you currently deliver. If it fits, the next client engagement is the right place to put it to work.

Closing thought

The most valuable thing a consultant can leave behind at an SMB is a system the client will actually keep using. ReguLight is built around that idea: structured enough to look professional in a board pack, simple enough that a non-specialist risk or compliance owner can maintain it, and complete enough — with its built-in Help Center, public documentation and free RGL Security Framework — to function as both a working tool and a learning environment.

Download ReguLight from the Mac App Store and have a look. More information and the free RGL Security Framework at **www.regulight.eu**.