devoteam
Cyber Trust



Case Study

GRC Information Security Maturity Eyewear Sector: Building a Group-Wide GRC Foundation with IntegrityGRC

Client

A global group in eyewear design, manufacturing, and retail, operating a complementary brand portfolio across multiple countries and business entities.

The Challenge

The client needed a single, comparable view of information security maturity across all business units within the group, covering both the applications and the underlying infrastructure used by each entity. Information security assessments had to follow internal controls aligned with the NIST framework, consistently applied across markets such as Italy, France, and the USA. Third-party risk management was considered but largely set aside for the initial phase, with the organisation choosing to focus first on internal application and infrastructure information security maturity before extending the model outward.

The Solution

To address these needs, a phased Proof of Concept of the IntegrityGRC platform was designed, acting as the central tool for compliance and risk assessment. The approach combined technology with the implementation of the following key components:

- **Application & Infrastructure Information Security Assessments:** NIST-aligned assessments covering the applications and infrastructure used by each business unit across the group.
- **Internal Controls Alignment:** Assessment criteria mapped to the organisation's internal controls, themselves aligned with the NIST framework.
- **External Risk Readiness:** Integration with Bitsight to strengthen third-party risk visibility going forward, with adoption planned for a later phase rather than immediate use.
- **AI-Driven Automation:** Use of the platform's AI capabilities to automatically generate activities and outputs from assessment results, reducing manual follow-up.
- **Compliance and Roadmap:** Definition of a compliance programme structure with a clear implementation roadmap and supporting documentation.

The Expected Outcome

The Proof of Concept is designed to give the client one comparable view of maturity across all business units, replacing fragmented, entity-by-entity information security assessments with a consistent, NIST-aligned model spanning both applications and infrastructure. The engagement is still in progress, with results pending as the assessment phases complete across the group's business units.

In summary, the Proof of Concept demonstrates how a phased, technology-led approach can turn fragmented, entity-by-entity assessments into a single, comparable maturity model, with third-party risk integration positioned as a natural next step once the internal foundation is established.