devoteam
Cyber Trust



Case Study

Maturidade de Segurança da Informação e GRC no Setor da Ótica: Construção de uma Base de GRC para todo o Grupo com a IntegrityGRC

Cliente

Um grupo global no design, fabrico e retalho de artigos óticos, que opera um portfólio complementar de marcas em vários países e entidades empresariais.

O Desafio

O cliente necessitava de uma visão única e comparável da maturidade da segurança da informação em todas as unidades de negócio do grupo, cobrindo tanto as aplicações como a infraestrutura subjacente utilizada por cada entidade. As avaliações de segurança da informação tinham de seguir controlos internos alinhados com a estrutura NIST, aplicados de forma consistente em mercados como Itália, França e EUA. A gestão de risco de terceiros foi considerada, mas essencialmente reservada para uma fase posterior, tendo a organização optado por se focar primeiro na maturidade da segurança da informação das aplicações internas e infraestrutura antes de expandir o modelo para o exterior.

A Solução

Para responder a estas necessidades, foi desenhada uma Prova de Conceito faseada da plataforma IntegrityGRC, atuando como a ferramenta central de conformidade e avaliação de risco. A abordagem combinou tecnologia com a implementação dos seguintes componentes-chave:

- **Avaliações de Segurança da Informação de Aplicações e Infraestrutura:** Avaliações alinhadas com a NIST, cobrindo as aplicações e infraestrutura utilizadas por cada unidade de negócio no grupo.
- **Alinhamento de Controlos Internos:** Critérios de avaliação mapeados com os controlos internos da organização, por sua vez alinhados com a estrutura NIST.
- **Preparação para Risco Externo:** Integração com a Bitsight para reforçar a visibilidade do risco de terceiros no futuro, com adoção planeada para uma fase posterior em vez de utilização imediata.
- **Automação Baseada em IA:** Utilização das capacidades de IA da plataforma para gerar automaticamente atividades e resultados a partir dos resultados da avaliação, reduzindo o acompanhamento manual.
- **Conformidade e Roteiro:** Definição de uma estrutura de programa de conformidade com um roteiro claro de implementação e documentação de suporte.

O Resultado Esperado

A Prova de Conceito foi desenhada para proporcionar ao cliente uma visão comparável da maturidade em todas as unidades de negócio, substituindo avaliações de segurança da informação fragmentadas e de entidade para entidade por um modelo consistente e alinhado com a NIST, abrangendo aplicações e infraestruturas. O projeto ainda se encontra em curso, com resultados pendentes à medida que as fases de avaliação são concluídas nas unidades de negócio do grupo.

Em resumo, a Prova de Conceito demonstra como uma abordagem faseada e liderada pela tecnologia pode transformar avaliações fragmentadas numa visão de maturidade única e comparável, posicionando a integração de risco de terceiros como um passo seguinte natural após o estabelecimento da base interna.