SecureWatch for GDPR

Solution:

RiskWatch offers risk and compliance management software that provides an easy-to-manage platform that will keep track of all GDPR risk and compliance efforts.

SecureWatch

A GDPR Compliance Solution

RiskWatch works with companies of all sectors to ensure the successful compliance of GDPR.

Key Features:

- ✓ **Turn key** solution for GDPR compliance. Comes complete with GDPR content library to identify areas of non-compliance in systems holding PII.
- ✓ **Comprehensive** high-level audit criteria to ensure regulation is being met.
- ✓ Compliance analysis that **determines risk score** and detects alarming abnormalities for further investigation.
- ✓ Ability to **consolidate all compliance and risk assessments** into one platform.
- ✓ Identify gaps in compliance, make recommendations and assign action plans to **avoid penalties**.
- ✓ Assessment workflows and reports that make it easy to collect, track, and **provide proof of compliance**.
- ✓ Guaranteed encryption and protection for your data through AES 256bit encryption.
- ✓ Provides a **centralized storage of documents** that can be used as evidence of

Realized Time Savings:

RiskWatch

Model Inputs**	Current Program	SecureWatch
Hours needed to communicate (email) and interview client, perform survey or request documents to review	1	0
Hours required to gather assessment data*	3	1
Hours required to analyze data gathered	4	2
Hours required to perform remediation	3	1
Hours required to write report	20	4
Total Hours	31	8
Total Reduction of Time	**74%** (23 hours per assessment)	

** The time saved can be multiplied by the amount of people that are involved in each step of the assessment process. We have only included a single person for each step in the model inputs above.
* SecureWatch can provide data not available in current assessment program.

RiskWatch's solution, ***SecureWatch***, can not only help prevent non-compliance consequences for GDPR, but also increases your ability to detect, predict and appropriately respond to any red flags.

GDPR indicates that organizations should implement appropriate technical and organizational measures to **ensure a level of security appropriate to the risk**. ISO 27001 is an ideal standard for organizations to follow in order to meet these GDPR requirements. **SecureWatch provides tools** to ensure your controls and measures align with the ISO 27001 standard.

- ISO 27001 allows for a documented process for regularly evaluating the effectiveness of security controls, identifies personal data and manages the details of data such as how it's stored, the location at which it's stored and the duration of the storage.
- ISO 27001 provides an approach to handling information security incidents which falls in line with GDPR's 72-hour breach notification requirement, as well as a set of controls to ensure the availability of critical data and associated business processes in the event of an incident.

The SecureWatch Process:

Additional Features:

- Access to GDPR *and* other regulation and standards' content.
- The ability to measure compliance with preloaded questions.
- Task tracking.
- Recommendations are automatically offered to mitigate non-compliance and vulnerabilities identified.
- Real-time risk profiles and scores that update as changes occur.
- Subject matter expertise built in.
- Control requirements are re-worded into questions people can answer.
- Can be implemented immediately—saving time and money—avoiding a prolonged compliance process.

RiskWatch offers ***free trials*** and a service to assist in performing a ***proof of concept*** using any of its assessment platforms.

Free Trial

Security:

SecureWatch was built aiming to provide highly secured data transactions between the client's browser and the server. Data between the customer's browser and our server is encrypted using AES 256bit encryption. All information contained in the database has AES-256 encryption and PBE with MD5 & Triple DES, to which RiskWatch controls the encryption key. This database is also backed up daily and sent to an offsite location in Amazon S3 where it is re-encrypted and stored for Disaster Recovery and Business Continuity.