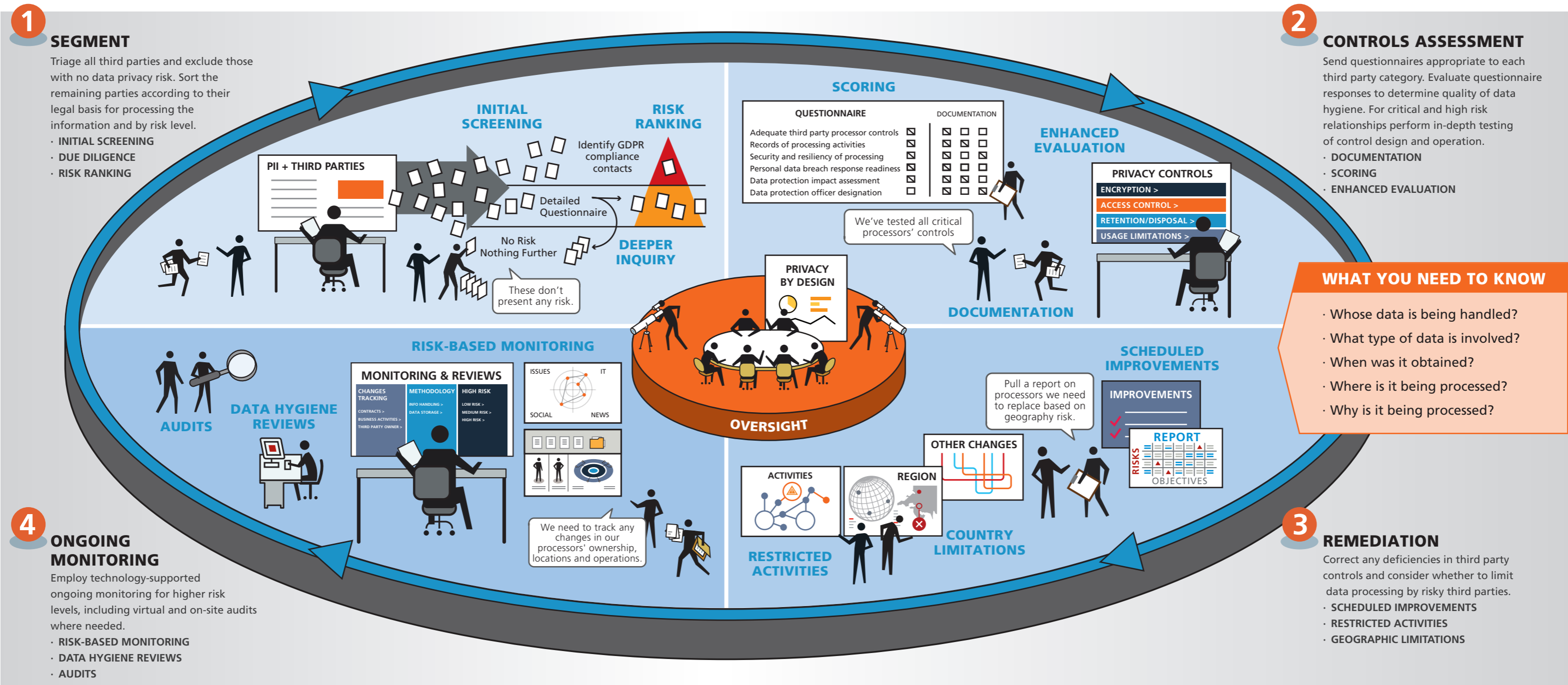


Assessing Third Party GDPR Compliance

The European Union's General Data Protection Regulation (GDPR) comes into force on May 25, 2018 and has been described as the most significant overhaul to data protection laws in a generation. The regulation applies to organizations worldwide that offer goods or services to individuals in the EU, and the penalties for non-compliance are severe. In replacing the outdated 1995 Data Protection Directive, GDPR recognizes the impact that the Internet and other new technologies have had on the data we hold and how we share it. Companies must view this as an opportunity to develop and implement data governance, protection and privacy in line with consumer expectations. This illustration outlines key steps in managing third party data privacy risk under GDPR requirements.

DEVELOPED BY


WITH CONTRIBUTIONS FROM

CONTROLLER OR PROCESSOR?

CONTROLLER:

The data controller is the person (or business) who determines the purposes for which, and the way in which, personal data is processed.

PROCESSOR:

The data processor is anyone who processes personal data on behalf of the data controller (excluding the data controller's own employees).

WARNING!



GDPR applies to both data controllers and data processors and penalties can be imposed on one or both parties depending on their degree of responsibility



Penalties can be severe – up to 20 million Euros or 4% of group worldwide turnover (whichever is greater).