Governance, Risk & Compliance (GRC)

Navigating Complexity, Incorporating Privacy

In today's data-driven world, organisations must manage a multitude of regulations, internal controls, and risks. Robust governance to manage risk and compliance are three interwoven disciplines and referred to as GRC. However, for organisations handling personal information, a traditional GRC approach might not be enough. Here's where incorporating privacy becomes crucial.

GRC and Privacy: A Symbiotic Relationship

Traditionally, GRC focuses on ensuring organisational effectiveness, managing risks, and adhering to regulations. However, when it comes to privacy, GRC has taken on a new dimension. Each element of GRC—Governance, Risk, and Compliance—needs to address specific privacy elements.

- **Privacy Governance:** This involves establishing clear governing guidelines on how personal information is collected, used, stored, and disposed of. Data governance, which sets rules for managing all data assets, must consider personal information handling practices. Ensuring a privacy lens is applied to governance of data sharing arrangements and the use of AI is also a key aspect.
- **Privacy Risk Management:** Identify and assess the risks associated with your organisation's use of personal information. Risk events to consider could include data breaches, unauthorised access, or accidental disclosure. Integrate privacy-specific risks into your risk management framework for a holistic view.
- **Privacy Compliance:** The web of privacy jurisdictional laws such as GDPR and frameworks such as ISO27701 becomes increasingly complex. Mapping the obligations of all these that apply and ensuring they are integrated and complied with, can be a significant challenge.

Building a Robust GRC Framework to Include Privacy

Here are some key steps you can take to strengthen your GRC program for effective privacy management:

- **Embed Privacy into Governance:** Don't treat privacy as a poor cousin. Integrate it into your overall organisational governance framework: e.g. consider developing data governance policies and processes that address the handling of personal information, include privacy as a specific component of AI governance frameworks
- **Develop and Enforce Clear Policies:** Create easy-to-understand privacy policies that outline how you handle personal information. Don't just write them; enforce them across your business and IT functions. Automated tools can enforce policies, monitor for policy breaches and enable swift remediation.
- **Real-Time Compliance Monitoring:** Ditch manual compliance tracking. Utilise technology solutions to monitor compliance with relevant privacy regulations and framework in real, or near real time. This allows for quick adaptation to evolving regulatory requirements and use of data with confidence.
- **Integrate Privacy Risk:** Business and IT risk assessments should include a privacy risks. These risks should be linked to your specific holdings of personal information and seamlessly integrated with existing risk management processes.

Partnering for Success in a Complex World

Navigating the intricate world of GRC with privacy in mind can be overwhelming. We understand the challenges and can help you develop a comprehensive GRC program tailored to your needs. Contact us today to discuss how our expertise and technology solutions can empower you to build a robust and integrated approach to GRC, ensuring a solid privacy posture in the face of ever-changing regulations.

TRUSTWORKS360 PYT LTD

Email: Contact@trustworks360.com

LinkedIn: Trustworks360 LinkedIn

Website: Trustworks360 Website