Group Risk Consulting® LTD

Governance. Risk. Compliance.

Payments Services Directive 2 (PSD2) Compliance – Gap Analysis / Review

The speed of change within the electronic payments industry has been immense. With this change and the adoption of these new technologies / payment processes comes a corporate responsibility to protect the customer. Firms are now required to have a deep understanding of this risk and prove how it is mitigated. The PSD2 standards came into force on 13 January 2018.

The Payment Services Regime (PSR) 2017 and European Banking Authority (EBA) guidelines have mandated a number of obligations on Account Servicing Payments Service Providers (ASPSP), Account Information Service Providers (AISP), Payment Initiation Service Providers (PISP) to comply with the PSD2 regulation such as:

- 15 Business day rule (issuing final response) for PSD Complaints handling - Does your complaints handling process cater to closing the PSD complaints in 15 business days as opposed to 8 weeks as per DISP rules?
- Allowing customers' payment accounts access to other third-party providers
- Allowing customers to share their security credentials (bank provided) to third party payment service providers
- Providing access to Payment accounts/systems to payments service providers via risk-based criteria
- Secure communication through Strong Customer Authentication and Open APIs
- APIs for third party payment service providers to connect and obtain customers' data securely
- Allowing access to customers' payment accounts through screen scraping methods (until the APIs are published)
- The Business Continuity & Disaster Recovery plans assess a range of extreme but plausible scenarios which include consideration for failure of key systems, the loss of key data, inaccessibility of premises and loss of key persons
- Monitor and seek assurance on the outsourcing providers' level of compliance
- Risk assessments - Under PSD2, all PSPs must, at least annually, send their competent authorities an updated and comprehensive assessment of the operational and security risks to their payment services
- Also at least every year, PSPs must send their competent authorities statistical data on fraud affecting different types of payment
- New reporting and notification requirements - Fraud reporting, complaints response reporting, AIS/PIS denial, payment account rejections/withdrawals.

GRC

Group Risk Consulting® LTD

Governance. Risk. Compliance.

Risks of non-compliance:

There are a number of risks and potential impacts that may arise as a result of failure to adequately comply with the PSD2 regulations. These may include:

- Regulatory fines and censures for not being PSD2 compliant with the requirements of PSR 2017 and EBA guidelines
- Reputation damage and loss of customer confidence resulting in a shrinking customer base and diminishing balance sheet
- The firm's license for payments services may get revoked
- The firm may face litigation from its customers and shareholders due disputes in relation to; fraud, data theft, cyber crime / misrepresentation etc.

How GRC can help:

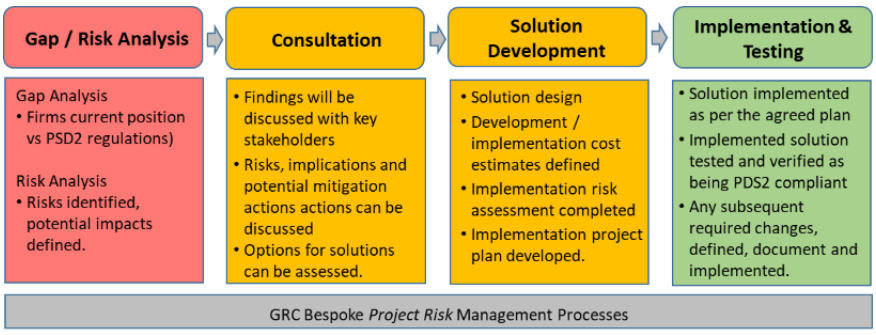
At GRC, we can help you comply with PSD2. Our experts convert the compliance overhead into a workable solution for you.

GRC's PSD2 business impact assessment:

- Identifies the gaps in payments services against your current position
- Consults you regarding the required risks / changes / enhancements and implements the optimal future state as per PSD2 regulation.

PSD2 Operational Environment

Example – Project Delivery Structure



For assistance, or an obligation free discussion, please contact:

Babu Chellappa (Head of Payments & Financial Crime Compliance)

T: +44 (0) 7794930963

E: babu.chellappa@grouprisk consulting.com

GRC