

# Compliance.

---

LBBW defines compliance as the preventative management of risk arising from failure to comply with the applicable laws, standards and processes, which damages the bank's business model, reputation and success and disappoints the expectations of owners, customers, employees and the public.

The requirements of LBBW's compliance are set out in a compliance management system (CMS). This system combines requirements of the corporate culture and internal guidelines, a compliance organization, information systems, controls, employee training and reciprocal reporting to create an instrument for risk-oriented management. The goal is to implement an end-to-end culture of prevention in which all agents of the bank commit to comply with the law and act accordingly, thereby achieving risk transparency and ultimately the trust of business partners.

## Capital Market Compliance.

The transfer of the EU's Markets in Financial Instruments Directive (MiFID) into national law and the procedures and processes introduced after this were monitored in 2009 by LBBW's capital market compliance. Compliance also supervised the implementation of the tightened regulations on recording investment advice, which have been in force since January 1, 2010.

Employee training was also provided in 2009 to raise awareness of individuals holding insider information and the resulting prohibitions on trading. In addition to advice for specialized divisions on issues of capital market compliance, the focus was again on continual monitoring of securities transactions with regard to adherence to legal regulations (control room).

---

---

## Money Laundering Prevention.

The requirements of the money laundering law, which was amended in 2008, continued to necessitate significant adjustments to processes, both in the field of money laundering prevention and in distribution. The money laundering law concentrates on a risk-oriented approach that is specific to the institution, which can be determined through a detailed analysis of the bank's risk situation. As a result, multi-level companies, correspondent banks and foreign customers who exercise an important public function are subject to stricter reviews and must meet increased transparency and integrity standards. These requirements applicable to natural persons are supplemented by an obligation to verify the identity of decision-makers and economic beneficiaries and to verify ownership structures in the case of legal entities.

## Financial Sanctions/Embargoes.

LBBW's customers and all incoming and outgoing payment transactions by LBBW and its savings bank partners that are processed through LBBW's cross-border payment activities are continually reviewed. The embargo unit of the Compliance department at LBBW provides recommendations on issues relating to foreign trade legislation, such as adjustments or amendments to financing plans with regard to sanctioned countries, such as Iran and Uzbekistan at present.

## Financial Intelligence Activities.

Financial fraud represents a significant potential threat that, in addition to material damage, can involve incalculable risks to reputation. As in previous years, LBBW placed particular emphasis on raising awareness and informing employees about the modus operandi of perpetrators. A joint information campaign was organized with the police headquarters in Karlsruhe to protect elderly people against criminals posing as long-lost relatives. All branches of BW-Bank were also provided with relevant information material. In order to better counteract the anticipated increase in organized fraud, LBBW will implement additional measures based on the results of the risk analysis for financial fraud. These include the creation of a bank-wide »Fraud Prevention Board« and the gradual introduction of plausibility checks to prevent fraud in bank units that are at particular risk.

---

---

## Data Protection.

Three amendments were made to the Federal Data Protection Act in 2009: the first amendment changed how the activities of credit agencies and their contractual partners (particularly banks) and scoring are regulated. The second amendment concerns, among other things, new regulations on market research and opinion polls, address trading, employee data protection and the processing of data relating to orders. The third amendment relates to consumer credit rights.

While the guidelines of the second amendment have had to be observed since September 2009, the fulfillment of the requirements of the first and third amendments will become compulsory during the first half of 2010.

The implementation of the guidelines of the second amendment in conjunction with the revised version of the law against unfair competition is of practical relevance to the distribution and marketing units. The extension of obligations relating to verification, monitoring and documentation in connection with awarding contracts to external service providers leads to additional costs before the contract is concluded and during its term. New processes have been designed for this and their implementation has begun.

Increasing interest in issues relating to data protection legislation was reflected in 2009 in a higher number of customer queries and requests for information.

As in previous years, subsidiaries were checked within the Group on the basis of a standard introduced by the Federal Office for Information Security. The action taken as a result of the findings of these checks ensured a comparably high level of data protection at all subsidiaries in Germany.

Random checks were also carried out by Data Protection on internal organizational units at the LBBW Group. In 2009, checks focused on concepts of roles and rights, the storage of third-party and partner products, content filtering of incoming emails, video surveillance, security in the computer center, ordering processes for Extend checking accounts and spot checks to ensure the operation of branches in compliance with data protection law. LBBW also conducted audits at the premises of external service providers involved in business with credit cards, the destruction of files and data carriers and PC services.

In addition, a risk analysis was carried out regarding opportunities for third parties to gain unauthorized access to personal data. The results of this will serve as a basis for future checks.

---