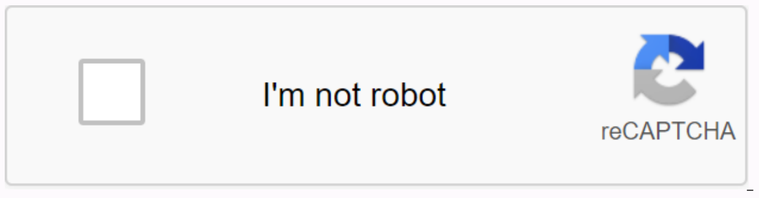

Continue

Operational risk management is known as what type of process

Graph 19. Operational risk management structure: Three lines of defense Table 20. Characteristics of bbva's operational risk management model Operational risk stems from the likelihood of human error, inadequate or defective internal processes, system failures, or external events. This definition includes legal risk, but excludes strategic and/or business risks and reputational risk. Operational risk is inherent in all banking activities, products, systems and processes. Its origins are diverse (processes, internal and external fraud, technology, human resources, business practices, disasters and suppliers). Operational risk management is integrated into the bbva Group's overall risk management structure. The Group has in place an integrated methodology of internal control and operational risk. This methodology identifies risks in organizational areas, generates analyses that prioritize risks according to the estimated residual risk (after the incorporation of control effects), links risks to processes and establishes an objective level of risk for each type of risk to identify and manage gaps, comparing it with the residual risk level. The Group has developed an enterprise application to provide the necessary support for this methodology: STORM (Operational Risk Management Support Tool), which includes indicator modules and scenarios. The operational risk management framework defined for the BBVA Group includes a governance structure based on: three lines of defense with clear specification of responsibilities; policies and procedures common to the whole Group; systems for identifying, measuring, monitoring, controlling and mitigating operational risks and losses; and tools and methodologies that quantify operational risk in terms of capital. BBVA's operational risk management model is designed and coordinated by the Corporate Operational Risk Management function, which is part of Global Risk Management, and by the Operational Risk Management Units (ORM Country), located in the Risk units of different countries and business areas. The business or support areas have operational risk managers (ORM Business) who report functionally to ORM Country, and are responsible for implementing the model in the day-to-day operations of the areas. This gives the Group an insight into the risks at the process level, where risks are identified and prioritized and mitigation decisions are made. Following a bottom-up approach, this system allows an overview at each level. To accomplish this task, BBVA has several tools already in place that cover qualitative and quantitative aspects of operational risk: Operational risk management tool: The STORM corporate tool was implemented throughout the Group in 2013. Identification the most relevant risk management have been key aspects discussed at meetings of the Operational Operational Risk Management Committee business units and support carried out throughout the year. Indicators. The indicators anchored in the main residual risks and their controls were consolidated in 2013. This model is included in STORM. Indicators measure risk development and controls over time, generate warning signals, and provide continuous measurement of the effectiveness of controls. These indicators are defined and monitored by experts. Siro. Operational risk events almost always have a negative impact on the Group's income statements. To keep these events under control, they are logged into a database called SIRO. To ensure reliability, 95% of your entries are fed directly from accounting data through automatic interfaces. Siro's internal data is supplemented with information from an external database in the Operational Risk Exchange (ORX) consortium. ORX is a non-profit association founded by twelve international banks in 2002 and currently has 65 members in 18 countries. The Group has additional tools to assist in the handling of data for the calculation of capital and in the realization of other necessary estimates. Operational risk events are classified according to the risk categories established by Basel II: processes, fraud (internal and external), IT, human resources, business practices, disasters and suppliers. Spain and Mexico quantify operational risk using internal models based on the Loss Distribution Approach methodology: loss distribution determined by the evolution of frequency and severity distribution of operational events, considering a one-year period and a confidence level of 99.9%. The capital calculation methodology using internal models involves internal operational event databases, external databases, scenarios, and various business environment and internal control factors. In 2010, the Bank of Spain authorized the Advanced Measurement Approach (AMA) to calculate capital requirements, consolidated by operational risk in Spain and Mexico, where most of the Group's assets are allocated. BBVA is, from this date, the only bank authorised by the Bank of Spain to apply advanced models to calculate capital requirements for operational risk. Although the basic model is still applied exceptionally, the standard model is used to calculate capital in the rest of the geographic areas. The capital resulting from the application of advanced models is adjusted by factors related to the country's environment and by internal control factors that depend on the level of mitigation of weaknesses identified by the controls. Operational risk admission As part of its continuous improvement of the operational risk admission phase, the CORM function has implemented a new for approval of new business, products and services. It was put in place in 2013 and will be completed in 2014 with the implementation of a workflow tool to management and documentation, providing the procedure and decision-making process with greater reliability and monitoring capacity. With this procedure, BBVA further integrated operational risk management into the Group's day-to-day operations and adopted the best practices and recommendations recently made by European bodies and regulators. The improvements introduced for the approval of companies, products and services are: A clearer distinction between business and products and/or services. Simpler governance, composed of committees with a broader level of representation that combines the global vision of companies and products in the business and geographical areas. A definition of the steps and tasks that approval processes must fulfill, as well as the persons responsible for carrying them out. Stronger monitoring of new business and products after their approval. Fundamental role for the operational risk function, as coordinator and guarantor of the application of criteria and processes, and for the different specialists involved, who make decisions within their area of expertise. Page 2 Graph 19. Operational risk management structure: three lines of defense Figure 20. Characteristics of BBVA Operational Risk's operational risk management model stem stems from the probability of human error, inadequate or defective internal processes, system failures and as a result of external events. This definition includes legal risk and excludes strategic and/or business risks and reputational risks. Operational risk is inherent to all activities, products, systems and processes, and their origins are varied (processes, internal and external fraud, technology, human resources, business practices, disasters, suppliers). Operational risk management is integrated into the bbva Group's overall risk management structure. There is an integrated methodology of internal control and operational risk throughout the Group. This methodology allows identifying risks in organizational areas, generating analyses in which risks are prioritized according to their estimated residual risk (after incorporating the effect of controls), linking risks to processes and establishing for each risk an objective level that, compared to residual risk, identifies gaps for its management. To provide the necessary support for this methodology, the Group has a corporate application: STORM (Operational Risk Management Support Tool), which includes modules of indicators and scenarios. The operational risk management framework defined for the BBVA Group includes a governance structure based on: three lines of defense with clear delimitation of responsibilities; common policies and procedures to Group; systems to identify, measure, monitor, control and mitigate operational risks and losses; and tools and methodologies to quantify operational risk in terms of capital. Operational risk management at BBVA is designed and coordinated from the Corporate Operational Risk Management function, belonging to Global Risk Management, and the Operational Risk Management Units (GRO Country), located in Risks from different countries and business areas. The business or support areas have, in turn, operational risk managers (GRO Business) who are functionally dependent on GRO Country, and who are responsible for implementing the model in the day-to-day of the areas. Thus, the Group has a process-level view, which is where risks are identified and prioritized and mitigation decisions are made, and which by aggregation allows a macro view at different levels. To accomplish this task, BBVA has several tools already in place that cover the qualitative and quantitative aspects of operational risk: Operational Risk Management Tool. During 2013, the implementation throughout the STORM Corporate Tool Group was completed. The identification and management of the most relevant risks have been the reference for the focus on the Operational Risk Management Committees of the business and support units carried out during the year. Indicators. During 2013, the indicators anchored in the main residual risks and their controls were consolidated. This model is located in STORM. The indicators allow to measure the evolution of risks and their controls over time, generate warning signals and measure the effectiveness of controls continuously. These indicators are defined and followed by SIRO experts. Operational risk events almost always have a negative impact on the Group's accounts. To have a thorough control of them, they are registered in a database called SIRO. To make it reliable, it is fed directly from accounting through automatic interfaces at 95% of its inputs. SIRO's internal data is complemented by information from an external database that comes from the Operational Risk Exchange (ORX) consortium. This consortium is a non-profit association founded by twelve international banks in 2002 and currently has sixty-five members in eighteen countries. The Group has additional tools that facilitate the processing of data for the calculation of capital and the completion of the necessary calculations. Operational risk events are classified according to the risk categories established by Basel II: processes, fraud (internal and external), human resources, business practices, disasters and suppliers. The quantification of operational risk is performed, for Spain and Mexico, by internal models based on the Methodology Approach of Loss Distribution: distribution of losses determined by the evolution of distributions of frequency and severity of operational events for the period of one year and confidence level of 99.9%. Internal operational event databases, external databases, business environment and internal control scenarios and factors are used for capital calculation by internal models. In 2010, the Bank of Spain approved the use of the advanced method (AMA Method) to calculate consolidated own resources requirements for operational risk in Spain and Mexico, countries that accumulate most of the Group's assets. To date, BBVA is the only bank authorized by the Bank of Spain to apply advanced models in the calculation of own resources requirements for operational risk. With the exception of some exception where we apply the basic model, capital calculation for all other geographies is obtained by applying the default model. The capital resulting from the application of advanced models is corrected by both the country's environmental factors and internal control factors that are based on the degree of mitigation of weaknesses identified in the controls. Operational risk admission GCRO's role has been implemented as part of its work, part of the continuous improvement of the operational risk admission phase, a new procedure for approving new business, products and services. It was implemented throughout 2013 and will be completed in 2014 with the implementation of a workflow tool that facilitates the management and documentation of the procedure, providing greater reliability and monitoring and facilitating decision making. In this way, BBVA deepens the integration of operational risk management into the Day-to-Day of the Group, adopting the best practices and recommendations recently made by European bodies and regulators. Improvements in business approval, products and services are: A clearer distinction between business and product and/or service. Simpler governance, created by committees with a higher level of representation, which unifies the global view of companies and products in the areas of business and geographies. A definition of the steps and tasks that approval processes must overcome, as well as those responsible for carrying them out. Strengthening the monitoring of new business and products after approval. A leading role in the operational risk function, as coordinator and guarantor of the criteria and processes, and the intervention of the different specialists who make decisions in their areas of activity. Specialty.