France: La Poste and ISO 31000
– Case Study –

LE GROUPE LA POSTE

isotc262.org: ***Case Studies draw on real life experiences of businesses and agencies drawing on the ISO 31000 Risk Management Standard to support their objectives. Each story is in its own context and will reflect the pre-existing conditions and management systems experienced by the writers. As a consequence they may not always follow the framework and process line by line. Rather, they show that the philosophy and guidance of ISO31000 can assist you to achieve your objectives in the way that suits you best.***

The project of La Poste described by Françoise Gaucher below has not been to put into place a management system based on requirements but to use the Guidelines of ISO 31000 to enhance the practice(s) in risk management existing at the start of the project within the group and to establish the global approach of the standard. This example shows how an end user applies ISO 31000 in learning and building activities where existing practice is progressively drawn into an innovative global approach to risk management.

This approach demonstrates the adaptive capacity of a more open system approach that meets the needs and culture of an organisation. The approach presented below is not literalist but a part of the Risk Journey, demonstrating the force of ISO 31000 in is its capacity to relate to the reality of an organization and make global risk management an integral part of that reality.

The French group La Poste, a major public company based on a multi-business model (mail, parcel, banking services …), has chosen to refer to ISO 31000 since 2015. Considering the situation of the Group at the outset this was a major and important decision for the Group with about 250,000 employees. Its objective was to develop effectiveness of risk management.

Before 2015, only two subsidiaries out of 300 clearly referred to this standard for risk management. At the same time, the Group already had a charter for Internal Control. This charter was mostly focused on the responsibility of directors (of all the branches) in the implementation of the Internal Control system (1st and 2nd level of control) to guarantee as much as possible the achievement of objectives. This is considered a good way to improve efficiency and global compliance.

Each year, since 2010, a self-evaluation of the maturity of the Internal Control has been carried out, setting out what has been done by each branch of the Group. This is important to ensure that the system is always adapted to changes in the organization or business. Applying ISO 31000 helped capitalizing on this best practice in the Group

by integration in the internal context analysis these different levels of maturity of internal control.

Bank and insurance subsidiaries of course refer to specific rules and mandatory compliance (Basel rules, Solvency, … and the European regulations) but for operational risks (which are not credit risks, or technical insurer risks, …) it appears that similar questions could be asked regarding risks in other branches of activities (human resources, IT, … or for crisis analysis such as natural or technological disasters). It's partly with the creation of a risk and control committee, dedicated to exchanges and discussions about practices between branches at the Group level, that the idea of a global approach for risk management for common risks emerged.

The question was how are common subjects of risk dealt with and good risk management practice optimized when you are a large Group with public and private activities? Use ISO 31000!

The Group complexity, with activities in decline (traditional mail), and others in deep transformation with information and data technologies increasing the new challenges (banking, insurance, e-services, …) as well as new requests for public services (to help seniors continue living at home, to keep public services in small towns, to operate public exams for driving, …) **requires a soft approach which is clear to all in order to manage risk.** Use ISO 31000!

What has been done?

As ISO 31000 is a guideline, we used it to help each branch to structure its own risk management Framework according to its needs.

Risk definition: one definition for all the Group. However, if "the effect of uncertainty on objectives" is the right definition to deal with all kinds of risk, it was not possible to rely on such a short definition which is a bit conceptual. Our definition is focused on the negative aspects of risk due to French tradition. So, the definition chosen is: a risk is all unusual events or uncertain situations whose occurrence could have negative consequences in reaching objectives or for the respect of our values (ethic, public services, …). This differs from the global approach of ISO 310000 as it focuses on threats before opportunities.

Risk management Principles and Framework: To summarize, we can say that the Framework and the global risk management are based on 3 fundamental principles.

- Implication of the Chairman and all the top management in the definition and the monitoring of major Group level risks (20-25).
- Obligation of all branches to take into account major Group risks (if they are concerned directly by them) at all levels as required: analyze, measure and evaluate the components of those major risks and decide (with respect of internal and external mandatory rules) axis for risk treatment to be adapted to local circumstances.
- Each year, all risks (cartographies) have to be updated, strategic as well as large operational risks are re-identified, analyzed evaluated and for all major risks treatment proposed. Risk treatment has to be specified and explained along with the risk treatment from the previous year. It's an iterative way between risk identification and risk analysis first year, and the results of risk treatment of the risk next year: some causes, for example, can be eliminated by risk treatment, so the risk identification is quite the same but the risk analysis shows a diminishing likelihood of events or consequences.

Risk management Process: ISO 31000 has been a help to highlight the fact that the external context has to be clearly examined to determine if all the effects of the actual uncertainties on objectives are negative or positive for our activities. We were very focused on the internal context and the changes in it. We now have to extend our investigations to international markets (for parcels …), demands for new services from citizens, new expectations in secure and reliable digital services.

Risk Assessment: Due to the number of large projects, some branches have created specific project committees to decide to go or not to go, taking into account a more precise risk identification and evaluation, and the cost of risk treatment. This is a better way to compare opportunities and threats for internal and external projects. A more precise identification and evaluation allow to launch new business or new product and to seize opportunities with an adapted supervisory management.

Risk Treatment: The main point for deciding on an option of treatment is to anticipate the effectiveness of the option and to understand the cost of its implementation. A second big challenge with risk treatment, is to elaborate a sustainable solution and to have it implemented sometimes in partner organizations at the same level as for our organization. The treatment plans in our operational organization must suit to the day to day work and business, and be in compliance with all mandatory rules. That is part of the duty for local management to understand, explain, persuade and obtain the commitment of all the employees in working on reducing (mitigating) risks.

Monitoring and Review: Monitoring is essentially part of a manager's job. A manager in charge of a business unit, or a subsidiary, or a division, or a large industrial center, … has the responsibility for taking decisions after local risk assessment and development of local treatment plans. Some actions are compulsory but others have to be planned in accordance with the availability of local resources.

Reviewing the Process: The overall Process and Framework are submitted for internal audit every 2 to 3 years, either by the branch service audit or by the Group service audit. Recommendations from the internal audit is one way to review and improve all the risk management system. The other way is from risk management teams from each branch or corporate level who have the activity of helping, challenging and explaining how to progress from the different feedback from past experience in the Group.

To summarize it: the objective of aligning Groupe La Poste's risk management with ISO 31000 was enhancing the effectiveness of the Groupe's risk management. Applying ISO 31000 helped capitalizing on best practices in the Group by integrating the different levels of maturity on internal controls in the internal context analysis. With the creation of a risk control committee the idea of a global approach for the management of common risks emerged and good risk management practice was optimized. Also, ISO 31000 helped highlighting the fact that the external context must be clearly examined and in risk assessment more precise risk identification and evaluation allowed to launch new business and new products with an adapted supervisory management.

Reported by **Françoise Gaucher**
Risk Manager Expert Groupe La Poste

LE GROUPE LA POSTE