IMPRESAPROGETTO
ELECTRONIC JOURNAL OF MANAGEMENT

Scenario planning as an element of strategic risk management

Carlo De Matteo, Paolo Cova, Alessandra Fissore[1]

Summary and list of contents: 1. Introduction - 2. Enterprise Risk Management as a founding element of strategic planning processes - 3. Enterprise Risk Management as a managerial lever for creating value - 4. Enterprise Risk Management and the cognitive distortions associated with risk assessment - 5. Enterprise Risk Management in Iren – 6. Conclusions

Abstract

Enterprise Risk Management of a company is a founding element of the strategic planning processes and must be applied to the determinants of the choices of the strategy itself and to the consistency matrix of the organization's mission, vision and values. This becomes always more essential in a generalized context in which the contraction of the duration of life cycles of business models, determined by destructive exogenous factors, originated by the development of technology, often leads to a scenario in which the life cycle of investments based on a certain strategy is longer than that of the underlying business model.
Enterprise Risk Management is also a managerial lever for creating value. The attitude to a risk based approach is usually due to regulatory or soft law prescriptions while it would be better considered as a third dimension, other than "what" and "how", of the paradigms and management schemes. A well working risk management process could also help to avoid the cognitive distortions produced by the limited rationality of human beings, which can lead to destruction of value. In this paper, the concepts above will be discussed in a theoretical way and in the context of a multiutility business like Iren.

Key words: Enterprise Risk Management, strategic planning, managerial lever, value creation, cognitive distortion, Iren

[1] **Carlo De Matteo**, Former Chief Risk Officer - Iren S.p.A.; e-mail: carlo.dematteo@fastwebnet.it
Paolo Cova, Risk Manager – Head of ERM System Management Iren S.p.A.; e-mail: paolo.cova@gruppoiren.it
Alessandra Fissore, Risk Manager Specialist - Iren S.p.A.; e-mail: alessandra.fissore@gruppoiren.it

DOI: 10.15167/1824-3576/IPEJM2018.3.1156

1. Introduction

Enterprise Risk Management (ERM) is a founding element of the strategic planning processes, essential to identify, assess and manage strategic risks. If ERM is integrated in the strategic planning processes, it represents an essential lever for creating value; in addition, it allows managers to avoid value destruction, due to exogenous risky events.

The article deals with the ERM approach, in a general context, and its application in IREN Group, one of the most important multi-utility companies in Italy.

2. Enterprise Risk Management as a founding element of strategic planning processes

The new Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s framework, named "Enterprise Risk Management - Integrating with Strategy and Performance", affirms that "Enterprise risk management, as it has typically been practiced, has helped many organizations identify, assess, and manage risks to the strategy. But the most significant causes of value destruction are embedded in the possibility of the strategy not supporting the entity's mission and vision, and the implications from the strategy.[2]"

Therefore, Enterprise Risk Management is a founding element of the strategic planning processes. It must be applied to the determinants of the choices that found strategy itself and to the consistency matrix of the organization's mission, vision and values. Moreover, the phenomenon of the business models' life cycles contraction, due to destructive exogenous factors (e.g. technology), is leading to a scenario in which life cycles of investments are longer than those of the underlying business models. Consequently, to predict and attenuate this value destruction, it is essential for Enterprise Risk Management to become a founding element of strategic planning processes.

The issue above is far from being abstract: the business models' life cycles contraction and the consequent risk of impairment and value destruction are real[3].

In addition, the Society of Actuaries confirms that strategic planning and strategic risk management are deeply connected. In fact, they can be considered effectively one integrated process: strategic planning is a response to strategic risks to the business model. It is essential to have disciplined and different processes to identify, assess and deal with strategic risks, because they are different in type and nature from business risks that involve threats within business model. Strategic risk management

[2] Committee of Sponsoring Organizations of the Treadway Commission, "Enterprise Risk Management - Integrating with Strategy and Performance", June 2017, Executive Summary.
[3] See e.g. the case of the generation companies in Italy.

processes represent an integral part of company's value proposition; therefore, they are a vital part of a comprehensive ERM framework.[4]

3. Enterprise Risk Management as a managerial lever for creating value

Enterprise Risk Management also represents a managerial lever for creating value.

The attitude to a risk based approach often derives from regulatory or soft law prescriptions, while it would be better to consider it as a third dimension, other than "what" and "how", of the paradigms and management schemes.

Hereinafter, some examples of regulatory and soft law contexts that regard the risk based approach:

1) the Corporate Governance Code, written by the Corporate Governance Committee of Italian Stock Exchange, whose adoption is optional for listed companies[5]. It sets out the "Internal control and risk management system" in article 7. In particular, the Code specifies the corporate bodies involved in this system, depending on their related responsibilities. In particular, Risk Management is specified among the tasks of the Board of Directors: "[the Board] shall define the risk profile, both as to nature and level of risks, in a manner consistent with the issuer's strategic objectives, taking into account any risk that may affect the sustainability of the issuer's business in a medium-long term perspective.[6]" Moreover, the Code establishes the designation of a Director in charge of the Internal Control and Risk Management System, as well as a Control and Risk Committee, whose task is to support the assessments and decisions of the Board of Directors related to the internal control and risk management system;

2) the new international standard ISO 9001: 2015[7] provides a risk-based thinking approach that involves top management in the entire risk identification and mitigation process;

3) the Legislative Decree no. 254/2016, which transposes the EU Directive no. 95/2014, concerns rules on non-financial reporting that apply to large public-interest companies, as defined in article 2. In the non-financial reporting, as established in article 3, first clause, companies have to provide information about the main risks, generated or suffered, and the underlying policies implemented. Relevant risks concern environment, social responsibility and treatment of employees, respect for human rights, anti-corruption and bribery, diversity on company boards (in term of age, gender etc…);

[4] Society of Actuaries, Integrating ERM with Strategic Planning, https://www.soa.org/Library/Newsletters/The-Actuary-Magazine/2007/August/int2007aug.pdf, August 2017.
[5] As explained above, the adoption of the Corporate Governance Code is voluntary for listed companies; however, if companies do not adopt it, they have to explain the reasons of each non-compliance, in line with the "comply or explain principle" set out in art. 123-bis of the legislative decree no. 58/1998.
[6] Borsa Italiana, Corporate Governance Committee, "Corporate Governance Code", July 2015.
[7] ISO 9001:2015 - Quality management systems. Requirements.

4) the information security standard ISO/IEC 27001[8] on cybersecurity represents a guideline to define, realize, maintain and improve information security. It provides a risk assessment aimed at defining acceptable levels of risk. In accordance with ISO/IEC 27001 on cybersecurity, the Italian Legislative Decree no. 65/2018, which transposes the EU Directive no. 1148/2016 (the so-called NIS Directive), states that operators in essential services (as defined in article 1) have to adopt measures that aim at reducing IT risks and minimizing the impact on service continuity;

5) the EU General Data Protection Regulation 2016/679 (G.D.P.R.) regards the processing of personal data in the EU by an individual, a company or an organization. The G.D.P.R. emphasizes the importance of monitoring risks in terms of impact and probability. Indeed, it promotes the concept of "privacy by design", i.e. the potential privacy risks deriving from a specific project or initiative that risk assessment activities have to identify, as required by article 24. This means a risk based approach that aims at identifying risks that could compromise the privacy and security of data, which transit through company information systems, defining the correct risk/benefit ratio and preparing the adoption of appropriate measures to mitigate risks. The G.D.P.R. requires that this process is continuous and takes into account not only the evolution of threats and technologies, but also the evolution of business.

These and other exogenous contexts interact in a quite prescriptive way with the corporate governance and management system. The intrinsic risk consists in the individual management of these instances in terms of compliance, without having a strategic approach to risk management. This attitude generates inefficiency, because different corporate bodies with heterogeneous non-integrated methodologies examine the same risks; in addition, it is ineffective, because it is not an integrated risk management aiming at creating value, but it becomes a "compilation exercise", i.e. a fair copy of spreadsheets more or less extracted from the line structures. If Enterprise Risk Management is not embedded in the business processes, in particular in strategic planning processes, the role of the Chief Risk Officer (CRO) becomes merely formal and useless. The main issue is culture: the paradigms and managerial schemes applied to business management can be traced back to two macro dimensions: that of the "what" (business models, strategies, plans, objectives) and that of the "how" (resources used, control, results, deviations, etc.). Within these two Cartesian axes, managers move the levers that create or destroy value. A third dimension is needed: "risk", which according to ISO 31000[9] is the "effect of uncertainty on objectives". Risk is also defined by the CoSo[10] as: "The possibility that events occur and affect the achievement of strategy and business objectives". Therefore, top managers who do not integrate this third dimension into business processes, deprive themselves of a powerful managerial lever to mitigate the risks of value destruction, generated by events that, in some cases, may also have impact on business continuity.

[8] ISO/IEC 27001:2013 – Information technology -- Security techniques -- Information security management systems – Requirements.
[9] ISO 31000:2018, Risk management – Guidelines.
[10] CoSo, Enterprise Risk Management Integrating with Strategy and Performance, Committee of Sponsoring Organizations of the Treadway Commission, June 2017, Executive Summary.

A well working risk management process could also help to avoid the cognitive distortions produced by the limited rationality of human beings, which can lead to destruction of value.

4. Enterprise Risk Management and the cognitive distortions associated with risk assessment

In 2017, Richard Thaler awarded the Nobel Prize in Economics for his studies on behavioural science and economics. Even before, in 2002, Daniel Kahnemann won the Nobel Prize for his works on behavioural finance. In his studies, Thaler explored the interactions between economics and psychology, by analyzing the psychological effects on market players' decisional processes. Most of risk assessments rely on deterministic quantitative models (e.g. profit at risk, probability of occurrence, etc.), but it is necessary to take into consideration the human factor. Indeed, our evaluations and consequent decisions move within a limited rationality that, in some cases, is conditioned by cognitive distortions.

For instance, within a risk assessment on major investments or merger and acquisition (M&A) transactions, which aims at identifying, assessing strategic risks and taking action for managing them, the impacts of risks are often underestimated if people involved have a positive bias on that operation. In the organization, the top management itself can induce this prejudice, with sentences like "the CEO believes in it". In this way, people involved in the risk assessment processes tend to overestimate the information that confirms this choice and to minimize any purposes of discussion. In psychology, this phenomenon is called cognitive bias.

To support strategic decisions and mitigate the "cognitive bias", there are quantitative models (financial models, risk assessment etc.). However, they may generate the so-called "illusion of control", i.e. the cognitive bias that leads to assume a complete control over the outcome of a situation. The cognitive distortions in planning, control and decision-making processes represent a significant risk in terms of value destruction. In case of initiatives of great financial importance, the illusion of control could also compromise the business continuity; there are some cases of companies wiped out by wrong investments or acquisitions. Hence, the risk manager has to perform a top organizational position that guarantees an impartial judgement, without being extraneous to the key processes.

5. Enterprise Risk Management in Iren

IREN is a top player in the Italian multi-utilities sector with a leading position in its business areas (mainly Torino, Vercelli, Genova, La Spezia, Parma, Piacenza, Reggio Emilia). IREN Group operates in the following sectors: electricity, gas, district heating, integrated water service and waste, and it provides other public utility services (public lighting, traffic light services and facility management). It is a diversified business model, characterized by a mix of market-based activities, regulated and

semi-regulated activities (the last two generated more than 70% of 2018 EBITDA[11]) which ensures solidity, development prospects and reduced risk levels. IREN is one of the main examples in Italy of a multi-utility oriented towards the provision of services and the creation of infrastructures for enriching and enhancing the territory, with respect for the environment and its customers.

IREN Group is oriented towards strengthening its position in the energy market and in the local public services by exploiting the advantages and benefits of economies of scale and integrating the value chain.

The Group' strategy is based on the following development guidelines[12]:

- DEVELOPMENT: structural increase in Group's profitability that leads to a significant growth (about 200 mln euro growth in 6 years);
- CLIENTS: development of the client-base (from consumer to prosumer) in reference areas through innovation digitalization and the offer of a wide range of high value added services: e-mobility, new downstream, energy efficiency etc.;
- EFFICIENCY: further improvement in efficiency, through 65 million euro synergies in 6 years (2023) linked to Performance Improvement projects. Reduction in cost-to-serve, thanks to digitalization and billing process/CRM improvement and a continuous improvement in workforce management systems in Waste and Networks sectors to optimize maintenance and management processes;
- SUSTAINABLE RESOURCES: key factors are decarbonization, circular economy, water sources, resilient town;
- PEOPLE: innovation, care and new ideas to be prepared to the challenges of the future, e.g. by 2023 the number of IREN employees under 30 years old will double.

In terms of Corporate Governance, Iren Group adopts a traditional system, compliant with the principles of the Code of Conduct for listed companies. The shareholders have attributed to the Board of Directors the widest powers for the ordinary and extraordinary management of the company. In particular, the Board of Directors has the power to take any action it consider appropriate to implement and achieve the corporate purpose, excluding only actions that the law and the articles of association assign to the shareholders' meeting.

In Iren Group, the Risk Management Department depends on the Vice President, who is also the Director in charge of monitoring the System of Internal Control and Risk Management.

The Chief Risk Officer is responsible for integrated management and monitoring system of the Group Enterprise Risk Management (ERM), the development of Risk Analyses according to risks related to the Business Plan, the Operational Plan and

[11] IREN Financial Statement 2017, https://www.gruppoiren.it/documents/21402/91033/Annual+Report+at+31+december+2017_DEF.pdf/e7215f58-0c07-48b4-9696-4fa003fc58b3

[12] IREN Business Plan 2018-2023, https://www.gruppoiren.it/documents/21402/146880/BP_IREN_2018_ITA.pdf/5bf50278-a344-429d-a8b8-91c0ea8826ec

strategic initiatives, the development of specific Risk Assessments and its Risk Matrix. Moreover, he has to monitor the application of the Risk Policies, the integrated process of risk and standardization of controls, definition of standards and information to Risk Owners.

Through specific reports the CRO upgrades to the management involved in the "Internal Control System and Risk Management" on the state of the situation and highlight any unresolved issues within their competence; he manages the insurance programs and the claims of the Group. As regards Risk Policies, Risk Management assesses the first proposals of change of the individual classes of risk management strategies; the Vice President submit them to the Control and Risk Committee, "Control, Risk and Sustainability Committee" in order to analyze them in conjunction with Statutory Auditors. Later, the Board of Directors approves Risk Policies and the Audit Plan.

Iren Group adopts a risk management system that considers three levels of control. The first level of control regards risk owners that hold and manage risk every day. The second level concerns the players of the Enterprise Risk Management system (not only Risk Management department but also Compliance, Financial Risk Management, HSE and other lines of defense). Finally, the third level of control regards Internal Auditing that relies on the Board of Directors. Above all, the Governance bodies, i.e. the Board of Directors, the Control and Risk Committee, the Statutory Auditors provide the strategic guidance and evaluation on the overall internal control and risk management system.

In Iren Group, the most important risks, regulated by specific policies, regard energy and commodity, financial, credit, operational and reputational risks. The ERM system follows the CoSo ERM Framework and defines the Group Risk Model and the strategies against the risk factors that could threaten business continuity. Furthermore, risk analyses of specific strategic initiatives (e.g. M&A operations) are conducted: for this purpose, Risk Management prepares the Risk assessments and related risk matrices, by identifying and evaluating risks and associating the identified risks to mitigation measures. Moreover, it identifies and supervises specific KRIs (key risk indicators) related to each risk and the relevant risk owners. In particular, Risk Management builds the risk analysis of the Business Plan by drawing a risk map that identifies the macro drivers of the plan (efficiency and organization of Group's processes, development etc. …). Successively, it quantifies the contribution of the target values of each macro driver to the operating results and the balance sheet at the final year of the plan. After that, the top risks associated with each macro drivers are identified; Risk Management calculates a sensitivity compared to target values during the time frame of the plan and quantifies the percentage of change in target values. Therefore, an analysis of possible risk mitigation actions and the level of management controls for risk minimization is conducted[13].

[13] ANRA (Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali) and Protiviti confirm, in their Position Paper (Protiviti – ANRA, "Da Insurance Risk Manager a Chief Risk Officer: un

6. Conclusions

In this paper, we have discussed about the importance of the rising role of risk management in business strategy. Only a proper identification, evaluation and management of risks enable the business to achieve its targets and create value.

In the strategic planning, every development driver must be evaluated according to the dimension of "risk", in order to verify if and how risks could affect the business and compromise the desired and planned performance. The input must rise inside the Board of Director, the corporate body that approves the strategy and supervises the governance of the company.

Regulatory, soft laws and literature underline the growing importance of risk management culture at every company level. For instance, the CoSo Framework starts with the principles related to Governance and Culture: "An entity with a culture that is risk-aware stresses the importance of managing risk and encourages transparent and timely flow of risk information. It does this with no assignment of blame, but with an attitude of understanding, accountability, and continual improvement"[14]. This implies that information can be managed in a proper way, by limiting cognitive bias and misunderstandings.

An effective Risk Management department should help diffusing the risk culture inside the company and provide the instruments and the framework to allow risk owners and management to turn uncertainty and risks into knowledge and value. It does not replace people in taking decision, but it helps them to be aware of the implication of their decision. Risk evaluations must be not just an exercise, but an integrating part of business decision.

percorso di evoluzione nella gestione dei rischi", September 2016), that modern ERM approaches aim at identifying risks and opportunities deriving from Industrial Plan and quantify the impacts of risky events on expected results of the plan.

[14] See reference in footnote 10.