DEVELOPING AN ORGANIZATION'S RISK TAXONOMY

An organization's risk taxonomy is specific to its organizational culture. The presented tool suggests a way to establish a comprehensive, common and stable taxonomy. The tool also aims to provide analytical leads to assess an organization's overall risks.

1. Identify organizational risks

With the help of the various actors in the organization, identify the various risks it faces. Below are examples of possible risks for organizations to develop their taxonomy according to their needs.

Examples[1]:

- **Business processes:** Threats associated with business process design or implementation.
- **Capital infrastructure:** Threats associated with an organization's capital infrastructure including hard assets (e.g., buildings, vessels, scientific equipment, fleet), but excluding IT.
- **Communications:** Threats associated with an organization's approach and culture of communication, consultation, transparency and information-sharing, both within and outside the organization.
- **Conflict of interest:** Threats associated with perceived or potential conflicts between private and public interests.
- **Financial management:** Threats associated with the structures and processes of an organization to ensure sound management of financial resources and its compliance with financial management policies and standards.
- **Funding**: Threats associated with the commitment of various financial backers and stakeholders in terms of funding the organization's operations and programming.
- **Governance and strategic direction:** Threats associated with an organization's approach to leadership, decision-making and management capacity.
- **Human resources management:** Threats associated with staff/management turnover; employment/work culture; recruitment, retention and staffing processes and practices; succession planning and talent management; and employee development, training and capacity building.
- **Information management:** Threats associated with an organization's capacity and sustainability of information management procedures and practices.
- **Information technology:** Threats associated with an organization's capacity and sustainability of information technology, both the infrastructure and utilization of technological applications.
- **Knowledge management:** Threats associated with an organization's collection and management of knowledge, including intellectual property, organizational or operational information and records, and scientific data.
- **Legality:** Threats associated with an organization's management of its legislative, advisory and litigation activities, including the development and renewal of, and compliance with, laws, regulations, international treaties/agreements and policies.

[1] Inspired from the website, Guide to Risk Taxonomies, https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/taxonomies.html, (May 11, 2020).

- **Organizational transformation and change management:** Threats associated with significant structural or behavioural change within an organization related to mandate, operating context, leadership and strategic direction.
- **Policy development and implementation:** Threats associated with an organization's design, implementation and compliance with the government-wide policy suite as well as its own internal policies and procedures.
- **Privacy:** Threats associated with an organization's protection of personal information.
- **Program design and delivery:** Threats associated with an organization's design and delivery of specific programs, which may impact the organization's overall objectives.
- **Project management:** Threats associated with an organization's process and practice of developing and managing major projects in support of its overall mandate, as well as risks associated with specific projects that may require ongoing management.
- **Political situation:** Threats associated with the political climate and operating context of an organization.
- **Reputation:** Threats associated with an organization's reputation and credibility with its partners, stakeholders and the public.
- **Occupational health and safety:** Threats associated with the safety of the work environment in which the organization's employees work, as well as the health of employees.
- **Resource management:** Threats associated with the availability and level of resources of an organization to deliver on its mandate, as well as the organization's management of these resources.
- **Stakeholders and partnerships:** Threats associated with an organization's partners and stakeholder demographics, characteristics and activities.
- **Values and ethics:** Threats associated with an organization's culture and capacity to adhere to the spirit and intent of the Values and Ethics Code.

The organization can identify other risks specific to their organizational culture.

2. Define each risk

After identifying organizational risks, it is important to develop a definition for each.

Examples:

Human resources management: There is a risk that organization effectiveness may be compromised by an inability to substitute for key personnel lost unexpectedly (death, illness, special family situations, etc.).

Funding: There is a risk that funding patterns may be disrupted (interest rates, financial backer's strategic direction, competition, etc.).

Political situation: There is a risk that the party or parties in power in Canada or at destination may have an impact on the organization's work strategy (elections, orientations, corruption, etc.).

Legality: There is a risk associated with a legal dispute (formal notice, lawsuit, etc.) that would impact the organization's reputation.

3. Group risks in broad categories

The identification of a risk taxonomy requires defining broad categories of identified risks throughout the organization. In general, small and medium-sized organizations working in international cooperation and development would establish the following broad categories:

1. Operational risks
2. Financial risks
3. Strategic risks
4. Reputational risks

Below is a generic taxonomy example of a small or medium-sized organization.

OPERATIONAL	FINANCIAL	STRATEGIC	REPUTATIONAL
Human resources management	Funding	Political situation	Legality*
Information technology	Financial management	Governance and strategic direction	Reputation
Occupational health and safety	Resource management	Program design and delivery	Values and ethics
	Legality*		Stakeholders and partnerships

*Depending on the organization's definition of a risk, it can fall into various categories. For example, legal risks (ex: lawsuits) can have significant financial impacts given the financial resources required for a defence and this same risk can have a negative impact on the organization's reputation.

4. Analyze each listed risk

For each of the risks listed, identify the level of risk (impact x probability) and the mitigation measures to be implemented in order to meet the organization's risk tolerance.

From the website: https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/taxonomies.html