Type of document: A Guide to Risk Management in a Census Context

Prepared by Statistics Canada

May 2022

Table of contents

1. Introduction

This guide is based upon the Statistics Canada Integrated Risk Management Guide version 4 released in November 2021. Statistics Canada specific content has been removed and other minor changes made to yield a document more suited to the PRASC audience. Adaptations have been made with a view to application in the context of a population and housing census. Nonetheless the principles and methods are readily applicable to any project or to a national statistical office as a whole.

This document provides guidelines and tools related to the risk management process and is targeted for managers who would be involved with risk management in NSOs of the PRASC countries, and particularly those leading and managing the population and housing census. See Appendix A for the definitions of risk management terms that will be used in this guide.

The population and housing census is a substantial undertaking. It is normally the responsibility of a national statistical office (NSO) which this guide will refer to as the **corporate** level. This guide will refer to the census as being a **programme**. The census is achieved via a number of interacting major elements such as management, data collection, content and questionnaire design, information technology, statistical methods, processing, communications and advocacy, analysis, dissemination, etc. These will be referred to as **projects**.

We live in a world of constant change. This can create uncertainties and opportunities that must be managed or seized. It is the same for organizations which, regardless of their size, are faced with internal or external drivers that could make achieving their objectives uncertain, and therefore must develop mitigation strategies and contingency plans or seize new opportunities.

2. Risk management overview

Risk management takes place in the context of corporate, programme or project governance.

- **Governance** means directing, controlling and evaluating an entity, process or resource to **achieve established objectives.**
- **Risk management** means managing processes and resources to address risks while seeking to **resolve uncertainties.**

This model increases the effectiveness of the internal governance structure by ensuring that governance considers risks and assigns clear responsibilities to appropriate persons or committees so they can implement the strategy(ies) required to achieve the expected strategic outcomes.

It is essential that managers incorporate consideration of risk into their regular management processes. On a daily basis, managers at all levels encounter, analyze and manage risks.

- As a result, they are responsible for understanding these risks and proactively managing them by putting in place internal controls to prevent, detect and contain them.

- They are also required to make trade-offs between risk and control, taking into account the objectives they are expected to achieve, the opportunities they are expected to pursue, and the organization's risk tolerance.

2.1 Census and operational risk

Census and operational risks are expressed in terms of the likelihood and impact of an event, circumstance or condition with the potential to positively (opportunity) or negatively (threat) affect the achievement of objectives.

Census programme risks	Operational risks
They refer to the uncertainty that affects the achievement of objectives for the census as whole	They refer to the uncertainty that affects the achievement of objectives at the **operational or project level and that occurs in day-to-day operations.**
They are identified, assessed, prioritized and treated **at the level of the census programme.**	They are identified, assessed, prioritized and treated **at the level of each project.**
They are monitored, communicated and reported **at the level of the census management team.**	They are monitored, communicated and reported **at the project level**.
Risks are recorded in the **Census Risk Profile.**	Significant operational risks may be raised to the census level.

3. Risk management process

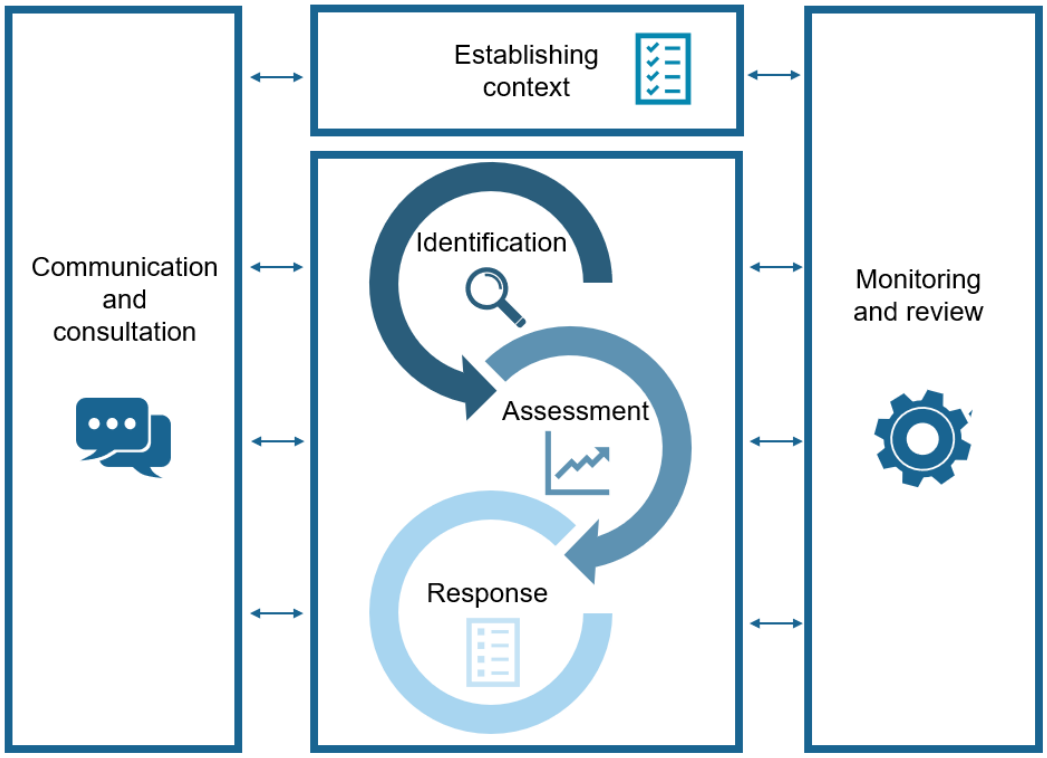
Risk (threat or opportunity) management is a systematic approach to determining the best course of action in uncertain situations by identifying, assessing and understanding risks, and then making and communicating informed decisions.

By developing coordinated and integrated mechanisms, managers can better understand the risks that threaten their objectives, and can therefore manage those risks more systematically.

The risk management process allows risk management to be applied consistently across the entire census programme. **Risk management is ongoing** so that an organization can detect changes in risk factors in a timely manner and take appropriate action, whether to avoid or reduce a risk or to seize an opportunity.

There are six components to the risk management process:

- Communication and consultation
- Establishing context
- Risk identification
- Risk assessment
- Risk response
- Monitoring and review.



The steps in the risk management process are explained in the following sections. Appendix B presents a summary table and associated tools.

3.1 Communication and consultation

Communication and consultation is intended to help relevant stakeholders understand risk, decision-making principles and why certain actions are required. Communication increases awareness and understanding of risk, while consultation obtains feedback and information to strengthen decision-making.

Communication and consultation with relevant internal and external stakeholders occurs at all stages of the risk management process. For example, they take place with census advisory committees, external advisors and NSO senior management.

3.2 Establishing context

Establishing the context involves an analysis of the environment in which an organization operates and identifies internal (weaknesses) and external factors (threats) that could affect the achievement of census priorities or outcomes.

- Threats: Think about potential external pressures that could materialize and impact the census programme or projects. These may include political factors, economic factors, social trends, technological innovations, regulatory obligations, environmental disasters, etc.

- Examples of potential threats: elections, floods, hurricanes, a pandemic, strikes, cyber threats, opposing special interest groups, etc.

- Weaknesses: Think about the internal culture, tools, procedures, practices and behaviours that could prevent the organization from achieving its priorities or outcomes.
  - Examples of potential weaknesses: lengthy and cumbersome approval processes, significant skills shortages, documentation quality, high staff turnover, IT vulnerabilities, infrastructure weaknesses, etc.

Guidance on how to establish context is provided in Appendix C.

To establish the context the team participates in environmental scanning and subsequent strategy sessions. The context is also established by monitoring current events and during discussions with senior programme managers having an understanding of the organization's priorities and outcomes. Any available corporate environmental scan should also be considered when identifying census risks.

3.3 Risk identification

Risk identification is an exercise that seeks to identify, acknowledge and describe risks that may potentially have a significant impact on the ability of the census to meet its commitments, objectives or priorities.

The Risk Management team – usually the census leadership group – reviews census risks and identified mitigation plans. To this end, the team consults various available resources including corporate risks, the environmental scan, key stakeholders and other corporate documents. In addition, discussions are held with key managers not on the core census leadership team to help validate current and emerging risks and mitigation plans.

Census projects and their leaders remain responsible for managing risks for their specific projects. Managers work with their respective teams to identify risks that could affect (negatively or positively) the ability to achieve their objectives. They use their risk registers to update and communicate emerging risks.

Appendix D contains key questions to consider to identify risks (threat or opportunity).

3.4 Risk assessment

Once risks have been identified, the risk assessment process begins.

Risk assessment is an exercise designed to analyze and assess the perceived likelihood of a risk and its perceived impact on the achievement of outcomes.

- Perceived likelihood is the likelihood that the risk will materialize.

- Perceived impact is the impact or consequence that a risk could have on the achievement of an organization's outcomes should it materialize.

The objective of risk assessment is to measure risk based on residual exposure. Residual risk considers the controls and measures that the organization has already put in place to mitigate the risk. These controls and measures can be activities, governance processes, tools, etc.

How to conduct a risk assessment?

See Appendix E for examples of questions to ask when conducting a risk assessment. Risks are then assigned a rating on the risk scale (matrix) based on likelihood and impact.

Management must decide which risks it will accept and which ones it will manage more tightly. In both cases, the risk management decision is made in an uncertain context and is always guided by judgement linked to the strategic and operational imperatives of the organization and its stakeholders.

Once the level of each risk is determined, different approaches are expected based on the organization's risk tolerance and appetite.

Risk appetite refers to the amount and type of risk an organization is willing to assume to ensure it has ample opportunity to achieve its objectives.

Risk tolerance is the willingness of an organization to accept or reject a given level of residual risk. Essentially, risk tolerance is the degree of risk an organization can afford to take given the resources it is willing to devote to reduce negative risks or to capitalize on positive risks.

Once a risk is assessed, it is important to clearly describe the key ideas inherent in a risk in a statement called a **risk statement**.

A traditional risk statement is written to highlight three main ideas:

1. The risk or opportunity
2. The key drivers (factors) that contribute to the risk or opportunity
3. The consequences of the risk if not mitigated

A typical risk (or opportunity) statement could be written as follows: "There is a risk (or opportunity)] that...because [the main drivers], which could lead to [the consequences]."

For example: There is a risk that the Census experiences wrongful disclosure of information because enumerators are new and inexperienced which could lead to public loss of confidence, reduced census success and reputational damage for the NSO.

Alternatively one could write a shorter statement that focuses on the risk itself followed by a short paragraph detailing the drivers and consequences.

For example,: "There is a risk that the Census may experience a wrongful disclosure of information.

Field data collection staff are mostly new, inexperienced and unfamiliar with the requirements of the Statistics Act and procedures to protect the confidentiality of respondent provided data and

so are at increased risk of allowing or causing a material disclosure. This could have consequences for the Census of reduced public confidence, reduced response, increased cost and reputational damage for the NSO."

Appendix F presents a five-level risk and opportunity assessment scale that can be used to understand where risks lie relative to each other and to illustrate the likelihood of a risk materializing and the impact it could have on the ability to fulfill its mandate.

3.5 Risk response

At this step, management has a thorough understanding of its risks and their context (What could go wrong or well and why?), the measures to mitigate existing risks (What are we already doing about this?), and the level of their residual risk (How are we exposed to this risk now?).

What is a risk response?

Risk response is an approach to determine whether additional strategic options should be put in place to respond to risk. Management must therefore review the risks assessed, determine their acceptability and develop their risk responses.

This requires asking a few questions: *Is the current level of risk acceptable or not given the organization's risk appetite and tolerance?*

If not, *can we do anything about it?*

If yes, *what should we do?*

The objective is to respond more proactively to risks rather than responding reactively. Planned and existing risk responses are developed using one or more of the following strategies:

THREATS	OPPORTUNITIES
• **Reduce**: Implement new mitigation measures to reduce likelihood or impact to an acceptable level. • **Accept**: Tolerate, keep mitigation measures already in place. • **Share**: Share the risk with other partners, transfer the risk using a third party to do the work when internal expertise is not developed. • **Avoid**: Eliminate, withdraw or do not participate	• **Exploit**: Eliminate uncertainty by making opportunity possible. • **Improve**: Increase likelihood and/or impact, identify and maximize key opportunity drivers. • **Accept**: Ignore, adopt a reactive approach without taking action. • **Share**: Share with partners to maximize likelihood and increase potential benefits if opportunity arises.

It may be acceptable for an organization (depending on its risk tolerance levels) to accept some or all low risks. Thus, it may not be necessary to include a response for all risks. The focus should be on **medium to high risks** and seizing opportunities that arise by focusing on those with medium to high assessments.

It is important to allocate appropriate resources to risk responses. Generally, the higher the risk (threat or opportunity), the more likely senior management is to act as the risk owner and assume management of the response. Conversely, the lower the risk, the more likely a manager is to act as the risk owner and manage the response.

During this process, it is important to remember that risks are interrelated. The interrelationship between risks is the influence that risks have on each other. Taking these interrelationships into account provides a horizontal view of risk exposure and risk response options. Analyzing the interrelationship between risks provides important benefits such as avoiding unintended impacts on other risks and unnecessary duplication of effort by focusing on integrated risk responses and common strategies.

Identifying common root causes for a group of risks, for instance, may reveal both the magnitude of the risk event for the group as a whole along with effective strategies that might address several risks simultaneously. Alternatively, some risks may be linked with others in a causal chain, and understanding the chain of risks may lead to a better understanding of the implication of risk.

At the project level, managers work with their respective teams to assess risks and seek guidance from the Census Management team to support them in their analysis. Managers must ensure that their leadership group reviews outcomes and that they perform the challenge function. Threats and opportunities are documented in a register. The level of risk will determine the frequency of updating, whether quarterly, semi-annually or annually. The risk assessment form in Appendix G can be valuable to document the statement, assessment, existing controls, and risk responses.

3.6 Monitoring and review

Ongoing monitoring and review are key elements of the risk management process and should be included in each component. Risk monitoring and review allows the census management team to:

- analyze and learn from events, changes and trends;
- detect changes in external and internal environments and identify new risks arising from them;
- identify risk interdependencies;
- ensure that risk responses and control measures are effective in terms of design and function;
- identify new or emerging risks.

Risks are monitored at three levels. It starts at the project level where risks are identified and managed. Project managers monitor the environment in which risks evolve and escalate significant issues to the census level. Significant risks are monitored at the census level.

Risk reporting takes place at least annually to provide a complete and transparent picture of progress in implementing risk mitigation strategies; to assist management in assessing the

effectiveness of risk responses and control measures; and to understand the nature and scope of any changes to key risks, including any new or emerging risks. The frequency of monitoring and review may be influenced by the likelihood and impact of risks, the organization's planning cycle, the meeting agendas of key committees, or a decision of an individual group.

Appendix H presents a monitoring model that may be used as part of the census risk exercise.

APPENDICES

Appendix A: Definitions

The **Census Risk Profile** describes a set of key risks. This set of risks may contain risks to the organization as a whole, to a part of the organization or to a project, or risks based on a different definition. Typically, the profile includes an environmental scan, risk statements, risk assessment methodology and results, risk responses and accountabilities, and monitoring and reporting requirements.

Integrated risk management is the systematic development and use of all types of valid risk assessment information as inputs to inform operational planning, decision-making, investment planning, project, program and operational management, and financial and resource management. It is conducted across an organization, at all levels, to support corporate, program, operational or project management.

An **opportunity** is a time, event, or set of conditions or circumstances permitting or favourable to taking a particular action or achieving a particular purpose.

A **threat** is a time, event or set of conditions or circumstances that impair or are unfavourable to taking a particular action or achieving a particular purpose.

Risk refers to the uncertainty around the achievement of objectives. It is generally expressed in terms of the likelihood and impact of an event, circumstance or condition with the potential to positively (an opportunity) or negatively (a threat) affect the achievement of objectives.

Risk appetite is the amount and type of risk an organization is willing to pursue, retain or take on.

A **risk culture** is the set of assumptions, beliefs and values about integrated risk management principles and practices and how they manifest within an organization's governance, compliance and risk management frameworks, and guide the organization in achieving its objectives.

Risk-informed refers to building risk management into existing governance and organizational structures, including business planning, decision-making and operational processes. It also ensures that the workplace has the capacity and tools to be innovative while protecting the public interest and maintaining public trust.

Risk management is a systematic approach to setting the best course of action under uncertainty by identifying, assessing and understanding risks, and then making and communicating informed decisions about those risks.

Risk response refers to the risk mitigation, control or treatment measures developed and implemented to address an identified risk. This can include avoiding the risk, seeking an opportunity, eliminating the risk, changing the likelihood of a risk, changing the consequences of a risk, sharing the risk with another party, and retaining the risk. It is based on a decision-maker's propensity for risk tolerance.

Risk tolerance is the willingness of an organization to accept the residual risk after applying a risk response to achieve its objectives.

Uncertainty refers to the state of having limited knowledge or understanding of a future event or outcome, its consequences or likelihood.

Appendix B: Risk management process checklist

Step	Considerations	Tools and resources
Communication and consultation	• Identify key internal and external stakeholders • Establish protocols for ongoing communication with key stakeholders • Establish approval protocols within the organization	
Establishing context	• Define the organizations' s main objectives • Identify internal and external factors; conduct environmental scan • Define the organization's risk tolerance • Communicate with and gain support from key stakeholders	*Appendix C: Establishing the Context*
Risk identification	• Develop a systematic method to identify risks • Establish a method for agreeing on risks • Have risks approved at the appropriate management level • Create a risk profile that includes threats and opportunities • Communicate with and gain support from key stakeholders	*Appendix D: Sample Risk Identification Questions*
Risk assessment	• Use risk analysis table approach to determine likelihood and impact of risks • Consider threats and opportunities • Communicate with and gain support from key stakeholders	*Appendix E: Sample Risk Assessment Questions* *Appendix F: Risk Assessment Scale*
Risk response	• Identify measures currently in place and corresponding risk ratings	
Monitoring and review	• Update the Corporate Risk Profile • Identify the frequency required for risk monitoring • Update risks and risk responses by plan • Develop process to identify emerging risks; apply risk management process to new risks • Identify committees that can be used to report on risk response progress • Develop new reporting mechanisms as required; obtain approval at the appropriate management level • Align reporting with business planning cycle	*Appendix G: Monitoring and review model and Guidance on action plan implementation measurement*

Appendix C: Establishing context

To establish the context, the census identifies its objectives and the external and internal factors to be considered in risk assessment and management. These factors can be identified through analysis, which can then be used to shape the design of the risk management approach and process.

Environmental scan
When conducting an internal and external analysis, organizations may wish to consider:

- the results of audits, evaluations, reviews or other documentation containing information on the organization's risk management, strategic leadership, values and ethics, integrated performance information, stewardship, and accountability;
- NSO and Census strategic planning documents such as mandate letters, integrated business plan, submissions to government, the NSO departmental plan,;
- input from interested parties such as Parliament, Census Advisory Committee, audit committees, clients, the public, and other stakeholders;
- key external analytical drivers (social, economic, legislative, etc.)

Proposed sources for the environmental scan:

- Internal announcements on new frameworks, policies and procedures;
- Internal communication tools;
- Interviews and meetings with subject-matter experts;
- Reports on newspaper articles, Internet articles or other media, and television programs;
- Sources from other NSOs and partner agencies like CARICOM, UNFPA, ECLAC, IADB, etc.

Key questions to consider for the environmental scan:

- What trends in the internal or external environment could affect a strategy or initiative?
- What assumptions do we make when planning our strategy? Are they consistent with the internal and external environments?
- Are there any anticipated new policies that could impact a program, initiative or process?
- What keeps you awake at night?
- Does the strategy or initiative depend on other current strategies or initiatives?

Appendix D: Sample risk identification questions

A. Census level

At the census level, risks (threat or opportunity) typically stem both from corporate-like risks as well as from the overall design of the census programme and the extent to which the census relies on human or manual elements. Risks can also arise from the interaction between census projects. During the high level design phase, risk control ensures that all residual risks are minimal and acceptable for threats, and maximized and favourable for opportunities. For this reason, census management should identify someone as risk management coordinator. It may be reasonable for this to be the same person responsible for coordination of change management.

What are the census programme's key priorities and expected outcomes?

Each priority and expected outcome will have a distinct set of risks. It is important to see the big picture, to keep in mind the context, and to know whether key priorities and expected outcomes depend on internal or external initiatives.

- How do the census' priorities and expected outcomes fit into the bigger picture or align with NSO and government priorities?
- Are these priorities and expected outcomes dependent on other strategies or initiatives in the agency? If so, how?
- What are the most urgent or important priorities and expected outcomes?
- What are the potential advantages or disadvantages of the strategy or initiative?
- What activities are required to respect priorities and achieve expected outcomes?
- Who owns the risk (threat or opportunity)?

How do NSO and government broader priorities and pressures affect census strategy or initiative?

- How do emerging NSO government priorities affect your strategies or initiatives?
- How do domestic and international pressures on a new government affect your ability to achieve expected outcomes?

Can you say which risks (threat or opportunity) are likely to threaten or enhance your ability to respect priorities and achieve expected outcomes, depending on the scenarios? (Focus on the most likely and worst case scenarios.)

- Which of the initiatives and projects will contribute most to respecting priorities and achieving expected outcomes?
- What recent adverse events could have been avoided?
- What internal and external factors impact the ability to respect priorities and achieve expected outcomes?

Are the census and NSO able to implement the strategy or initiative? Does it have the capacity?

- What are the key issues that may arise during implementation?

- How might the current initiative or strategy address internal or external changes that will occur?
- What continuity or contingency plans, existing or not, would enable recovery from a disaster or failure?
- Do you have the human resources to manage and implement the strategy or initiative?
- Do they have the skills and abilities to manage the strategy or initiative?
- If the answer to the above two questions is no, do you have a plan to train existing human resources or recruit new employees?

Have you identified any ethical risks or other factors that might arise during implementation?

B. Project level

At the project level, risks (threat or opportunity) typically stem from the design of the project and the extent to which the project relies on human or manual elements. During the project design phase, risk control ensures that all residual risks are minimal and acceptable for threats, and maximized and favourable for opportunities.

Key questions

- Are the project objectives clearly defined?
- Are there unrealistic operational constraints (such as deadlines)?
- Have all parameters (liability, legal, financial, etc.) been considered?
- Are different versions of the project being conducted elsewhere?
- How does the project depend on other projects, or do other projects rely on this project?
- Are controls in place throughout the project? Are these controls directly related to the risks?
- At each decision point during the project, does the decision maker have access to sufficient information to enable them to make decisions with confidence? Could internal or external pressures affect how decisions are made?
- What impact could a new or modified project have on stakeholders?
- During this project, is there a time when an unforeseen event might occur that would derail the project?
- Does each employee involved in the project have a clear understanding of how the project aligns with the objectives of the agency, regional branch or region?

Appendix E: Sample risk assessment questions

Likelihood

What criteria will you use to determine the likelihood of the risks (threat or opportunity) you have identified occurring?

- Is the risk internal or external?
- Has the risk ever materialized in the past? Has an event occurred recently?
- How likely is the risk to occur in the future?

Based on the answers to these questions, assess the likelihood of the risk (threat or opportunity):

- High (almost certain): The event is expected in almost all circumstances, within a given period;
- Medium to high (likely): The event should occur;
- Medium (possible): The event could occur at some point;
- Low to medium (unlikely): The event should not occur;
- Low (rare): The event should only occur in exceptional circumstances.

Impact (severity)

What criteria will you use to determine the impact of the risks you have identified?

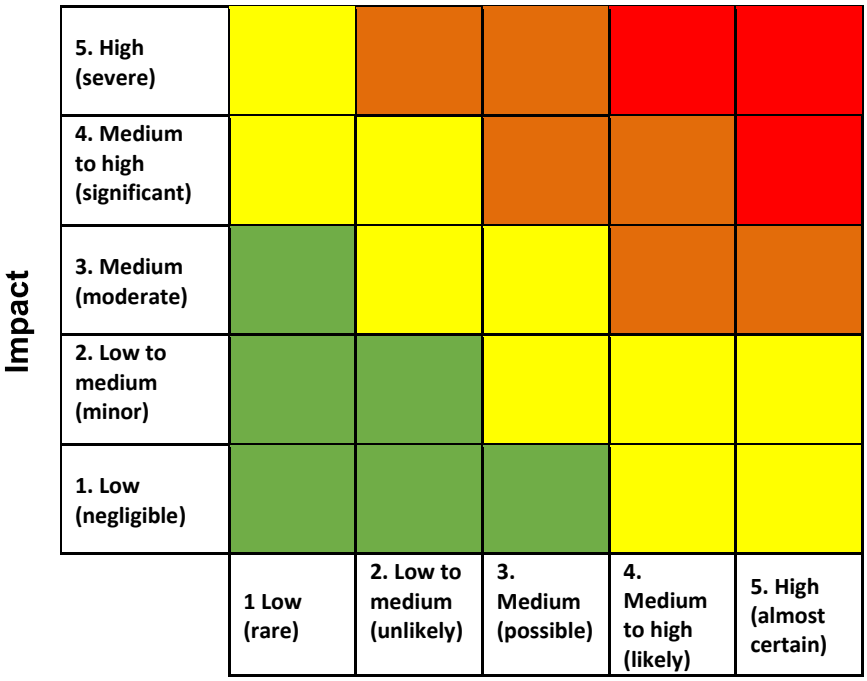
- What can go wrong? What could go well?
- What are the opportunities associated with the risk? What are the threats?
- Who will be affected? How will it affect them? How will the affected people react (positively or negatively)?
- Will the impact strengthen the ability of the agency, branch or region to meet its objectives?
- Will the impact interfere with the ability of the agency, branch or region to meet its objectives?

What measures (responses) are in place to prevent or mitigate the risks?

- Are too many of the risk responses considered weak?
- Are we maximizing risks that could benefit the organization?
- Are there too few or no responses to the risks deemed high?
- Are we maximizing an opportunity (beneficial risk)?

Appendix F: Risk assessment scale

Negative risk (threat) assessment scale

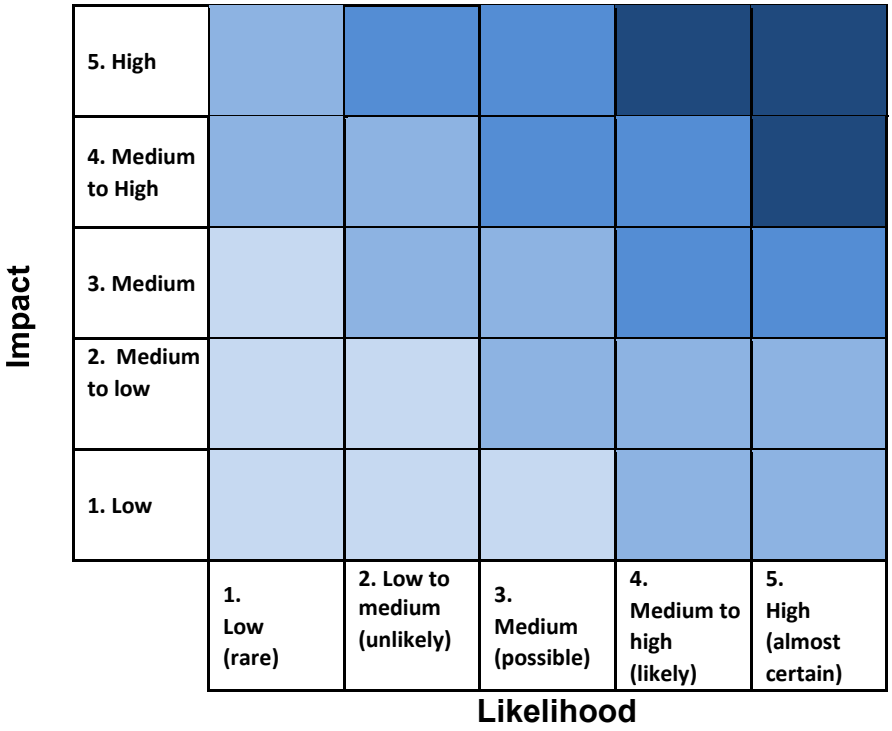


The horizontal axis shows the likelihood of a given risk occurring, that is, the likelihood that the risk will materialize and become an issue. The vertical axis shows the potential impact that the risk will have on priorities or the unachieved objective should it materialize. The colours are zones of risk (green boxes are in the low zone, yellow boxes the medium zone and red boxes the high zone). Risks are plotted on the scale based on potential impact and potential likelihood of occurring.

The table below explains the different risk levels in detail.

	Likelihood	Impact
5	**High (almost certain)**: The event could occur under most circumstances.	**High (severe)**: The event could prevent the achievement of organizational goals or objectives.
4	**Medium to high (likely)**: The event could likely occur.	**Medium to high (significant)**: The event could threaten the achievement of organizational goals or objectives.
3	**Medium (possible)**: The event could occur at some point in time.	**Medium (moderate)**: The event may require significant adjustments to overall organizational goals or objectives.
2	**Low to medium (unlikely)**: The event should not occur.	**Low to medium (minor)**: The event could limit an element of organizational goals or objectives.
1	**Low (rare)**: The event could only occur in exceptional circumstances.	**Low (negligible)**: The event could have little impact on the achievement of organizational goals or objectives.

Positive risk (opportunity) assessment scale



The horizontal axis shows the probability that an opportunity will occur, that is, the probability that the opportunity will materialize and become an event. The vertical axis shows the potential impact the opportunity will have on priorities or the objective should it materialize. Colors represent zones of opportunity, shifting from light blue, which represents a rare (low) opportunity, to dark blue, which represents a high opportunity. Opportunities are plotted on the scale based on potential impact and potential likelihood of occurring.

	Likelihood	Impact
5	**High (almost certain)**: The event could occur under certain conditions.	**High:** An opportunity that could have a high positive impact on the achievement of organizational goals or objectives.
4	**Medium to high (likely)**: The event could likely occur.	**Medium to high**: An opportunity that could have a moderate to high positive impact on the achievement of organizational goals or objectives.
3	**Medium (possible)**: The event could occur at some point in time.	**Medium**: An opportunity that could have a moderate positive impact on the achievement of organizational goals or objectives.
2	**Low to medium (unlikely)**: The event should not occur.	**Medium to low**: An opportunity that would have a moderate to low positive impact on the achievement of organizational goals or objectives.
1	**Low (rare)**: The event could only occur in exceptional circumstances.	**Low**: An opportunity that would have a low positive impact on the achievement of organizational goals or objectives.

Appendix G: Risk Assessment Form

Risk Assessment Form
Formulaire d'évaluation des risques

Field / Secteur :	
Prepared by / Préparé par :	
Date:	

Step 1: Identify risk & Context / **Étape 1 :** Identifier le risque & contexte
Provide relevant information to understand the causes and drivers of the risk / Veuillez fournir les informations importantes afin de comprendre les causes et les facteurs de risque

Step 2: Provide Risk Statement / **Étape 2:** Fournir l'énoncé de risque
Please use the following terminology: There is a risk (...) / S'il vous plaît suivre la terminologie suivante: Il y a un risque (...)

Step 3: Assess Likelihood / **Étape 3**: Évaluer la probabilité *See instructions Tab for more details / Voir l'onglet instructions pour plus de détails*	
Step 4: Assess Impact / **Étape 4**: Évaluer l'incidence *See instructions Tab for more details / Voir l'onglet instructions pour plus de détails*	
Overall inherent risk assessment / Évaluation du risque inhérent	#N/A

Step 5: Existing Controls / **Étape 5:** Contrôles existants
What are you already doing to prevent this risk from happening? / Que faites-vous déjà pour éviter que ce risque se produise?

Step 6: Mitigation Strategy / **Étape 6:** Stratégie d'atténuation

Actions *What actions will you put in place to mitigate this risk? / Quels actions allez-vous prendre pour atténuer ce risque?*	Level of Implementation / Niveau de mise en œuvre	Appropriateness of risk response / Convenance de la réponse au risque	Niveau de risque estimée après la mise en œuvre complète de la réponse au risque (risque résiduel) (probabilité/incidence)

Approved by / Approuvé par :	
Date:	

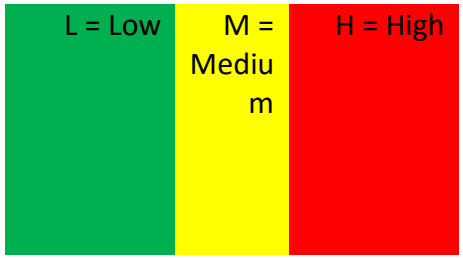
Appendix H: Monitoring and review template and Guidance on measuring the implantation of action plans

Monitoring and review template

Risk	Estimated risk rating before mitigation (inherent risk) (likelihood/impact)	Mitigation measures	Level of implementation (Note 1)	Risk rating as at dd/mm/yy	Appropriateness of risk response (Note 2)	Estimated risk level after full implementation of risk response (residual risk) (probability/impact)
Example: Public trust – There is a risk that STC may not be perceived as a trusted national Statistical Office	Medium-High/High	Work with stakeholders, partners and collaborators through various channels to promote and discuss Statistics Canada activities.	Level 4: Substantial implementation	01/12/21	Risk response 1: Risk response is appropriate as is	Medium-Low/High
Transformation— There is a risk that STC's transformation activities may not transform fast enough to meet the expectations of users	Medium/Medium	Update and implement branch modernization roadmap	Level 4: Substantial implementation	01/12/21	Risk response 1: Risk response is appropriate as is	Low/Medium

Alternate Risk Review Template - PROJECT NAME - DATE

The colour code for the overall risk is based on Impact and Likelihood:



Overall risk colour coding: High risk (H-H, H-M, M-H), Medium risk (M-M, L-H, H-L), Low risk (L-L, L-M, M-L)

Description	Probability	Impact	Inherent Risk Level (probability +impact)	Mitigation Plan	Residual Probability	Residua l Impact	Residual Risk Level (probability+ impact)	Contingency Plan	Contingency Triggers	Responsible

Guidance on implementation measurement

Note 1: Level of implementation:
When assessing the level of implementation of an action plan, select the highest level achieved. For example, if you feel that implementation efforts did not fully meet the criteria for Level 4 but were close to it, assign a Level 3 to the action plan.

Level 1: Minimal progress

Actions such as creating a new committee, holding meetings and developing informal plans should be seen as minimal progress.

Level 2: Planning stage

You have created formal plans for organizational changes and had them approved by the appropriate level of management (at a sufficiently high level, usually executive level or equivalent) with appropriate resources and a reasonable timeline.

Level 3: Initial preparation or implementation

You have concrete preparations for implementing a mitigation plan by hiring or training employees and/or developing or acquiring the necessary resources to implement the mitigation plan.

Level 4: Substantial implementation

Controls and processes are in place and integrated in at least some areas, and some results have been identified. You have a short-term plan and timeline for full implementation.

Level 5: Full implementation

Controls and processes are fully implemented. The risk has been reduced to an acceptable level or eliminated.

Level 6: Obsolete

You consider the strategy obsolete or no longer applicable because of unforeseen events or because the issue has been superseded by the introduction of a new process or program.

Note 2: Appropriateness of risk response
Determine if the planned risk response continues to be the appropriate response:
Risk response 1: Risk response is appropriate as is
Risk response 2: Risk response needs revision
Risk response 3: Risk response is no longer applicable
Risk response 4: Backtrack/New risks have emerged