



## ***Risk Management Policy***

### **INTRODUCTION**

The integrated risk policy (henceforth the Policy) is a high level document outlining Genome Canada's (GC's) approach and strategy towards Integrated Risk Management (henceforth IRM). A Risk Management Policy must be able to 'stand the test of time' and be robust enough to withstand scrutiny from regulatory and/or legislative bodies, as such the Policy is broad in scope. In addition to this Policy, risk management also includes the risk methodology, risk profiles and related actions that will, by nature, change over time to reflect organizational changes and changes in risk profiles. The Policy and related risks and action plans will be applied to all operational aspects of the organization and will consider external strategic risks arising from our external operating environment as well as other internal operational risks. Although Genome Canada is not able to control external factors such as government priorities they will be considered and addressed as much as possible.

### **PURPOSE**

This document sets out the organizations risk policy and includes:

- Policy objectives
- Definitions
- Components
- Responsibilities
- Assurance

### **POLICY OBJECTIVE**

The key objective of the Policy is to provide management with a framework to assist in dealing with the risk inherent in achieving the organizations objectives. IRM will help Genome Canada allocate resources to areas of highest risk and promote a more innovative and less risk averse culture. In addition, the Policy provides a sound basis for IRM and internal control as components of good corporate governance.

### **DEFINITIONS**

The Policy should be formed around a common understanding of risk management. Accordingly the existence of a common language is a key precursor to the understanding and success of risk management. Definitions of key terms used in the Policy can be found in appendix 1.

### **IRM COMPONENTS**

The components contained in this policy will be applied at both corporate and operational levels within the organization. The following components are key to the successful implementation of IRM.

### **INTERNAL ENVIRONMENT**

The internal environment is the foundation for all other components of IRM. It influences the design and use of control activities, how strategy and objectives are established and the design and structure of activities used for reporting, communication and monitoring. In addition the internal environment influences:

- Risk culture;
- Integrity and ethical values;
- Management philosophy and operating style;
- Organizational structure;
- Assignment of authority and responsibility; and
- Human resources policies and procedures.

The board of directors is an important aspect of the internal environment. A board that is actively engaged, committed and qualified is able to raise and pursue difficult issues with management in a confident manner.

### **Objective Setting**

Prior to identifying the risks facing the organization, there must first be objectives against which management can identify possible events (risks) facing their achievement. All risk management activity will be aligned to corporate objectives and organizational priorities. This process begins with Genome Canada's mission. From the mission statement, strategic objectives are set which state, at a high level, what Genome Canada will do to achieve its mission. From these strategies, specific and more detailed objectives are developed. Management's chosen objectives should be aligned with the risk tolerance (appetite) approved by the board.

### **Event Identification**

GC management must identify risks or events that have a potential to undermine the achievement of stated objectives. GC's risk management will be proactive and reasoned. Management will consider a broad range of potential events affecting the achievement of objectives consisting of both internal and external events. Event identification will be supported by quantitative and qualitative techniques and event interdependencies will be considered. For example quantitative techniques may be used if systems support the tracking of historical loss events that may produce projections of future loss events and attempt to measure them. Qualitative techniques may be based upon internal staff perceptions or facilitated workshops and interviews. The interdependency of events refers to how the occurrence of one event may trigger another or two events may happen concurrently. Management's knowledge of the interrelation between certain events may assist in determining where risk management efforts are best directed.

### **Risk Assessment**

Identified risks or events are identified and analyzed against the related objectives which may be affected. Risks are measured in terms of likelihood and impact on both an inherent and residual basis (pre and post controls). Likelihood and impact can be measured in both quantitative and qualitative terms depending upon the risks being considered.

### **Risk Response**

In determining an appropriate response to affect likelihood and impact the cost of the response and the impact of those risks occurring will be balanced with the benefits of reducing risks. Possible risk responses include avoidance, reduction, sharing and acceptance. The appropriateness of responses will be evaluated based on their ability to migrate the anticipated risk to within stated risk tolerance levels based on the resources consumed.

### **Control Activities**

Risk management will be founded on a risk based approach to internal control which is embedded in day to day operations of GC. Control activities are the policies and procedures that help ensure that the risk responses are carried out. Event identification, risk assessment risk response and control activities will provide Genome Canada with a risk profile. The board will maintain a current risk profile as a basis for implementing and monitoring the risk management activities. This profile will include details of the impact and likelihood of each risk identified, indicate ownership/responsibility and specify an action plan for treatment. This will be reviewed and if necessary updated on a semi-

annual basis. Progress of the risk management program will be a standing board agenda item. Management will ensure that organizational policies, procedures and guideline manuals indicate where there are mandatory processes and procedures (i.e. approvals, signing authorities, thresholds, verifications, security of assets, segregation of duties etc.). Full compliance with these standards will be required and confirmation of compliance sought. Non-compliance with specified procedures may constitute an unacceptable risk.

### **Information and Communication**

Managers and staff at all levels will have a responsibility to identify, evaluate and manage or report risks and will be equipped to do so. It is imperative that people have the relevant, credible and timely information to effectively carry out their responsibilities.

### **Monitoring**

Management will foster a culture that provides for disseminating best practice, lessons learned and expertise acquired from our risk management activities across the organization. Monitoring will be done through ongoing operations and/or separate evaluations.

## **RESPONSIBILITIES**

Responsibilities of the board of directors, management, risk officer, internal auditors, and other personnel are outlined in appendix 2.

## **ASSURANCE**

The use of this risk management approach assists in the identification of areas for more detailed review and to inform and support Genome Canada and divisional management assurance.

The risk profile will inform internal audit of the work necessary to provide assurance to the audit committee of the board that controls are in place and working to mitigate the areas of highest risk to the achievement of GC objectives. Internal Audit will evaluate the effectiveness of existing controls and risk management responses. Internal Audit assurance will include an assessment of the reliability and effectiveness of GC's overall risk management arrangements.

## **Appendix 1: Definitions**

---

### **Risk Profile**

Provides an overview of the risks inherent to the organization and key internal and environmental factors that influence their mitigation. The Profile provides a common understanding and the impetus for discussion of risks that influence organizational performance and the development of strategies for the management of risk.

### **IRM Framework**

Provides the foundation for establishing a sound IRM function. The Framework builds on what exists and communicates the organization's IRM direction and infrastructure in terms of:

- Roles and responsibilities of managers who are responsible for implementing IRM
- Strategies to integrate IRM in current planning, resources allocation and reporting systems; and
- Learning plans and tools.

### **Action Plan**

After development of the risk profile and the framework, gaps and opportunities related to IRM will be identified within the organization. The action plan outlines the critical next steps for advancing the incorporation and implementation of IRM strategies into decision-making and operations at all levels of the organization.

### **Integrated Risk Management**

IRM is a process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the organization, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

### **Risk Tolerance**

The level of risk GC is willing to accept in pursuit of its objectives. This can be measured qualitatively, with categories such as high, medium or low, or it can take a more quantitative approach. The level of risk acceptable is directly related to the strategy, where the desired return is aligned with the risk tolerance. GC's risk tolerance will be considered by management for resource allocation purposes as it aligns its people, processes and structure to effectively respond to risk.

## Appendix 2: IRM Responsibilities

---

The Policy is to be implemented by Genome Canada and is recommended for each of the Genome Centers. Each Genome Center is responsible for maintaining documented business risk profiles using analytical techniques to identify, evaluate and manage risks in compliance with the Treasury Board of Canada's Integrated Risk Management policy. In addition to those reporting requirements set out in the framework, Genome Center management are asked by the board to provide:

- A Center risk profile which details the priority (impact and likelihood) and ownership within each Center;
- A risk management action plan (mitigation, response, timing, responsibility, expected results; and
- Evidence of regular review and monitoring of the profile and action plan.

In addition to the role of Genome Centers as stated above, management are charged with supporting the successful integration of risk management into Genome Canada processes by undertaking the following general responsibilities:

### *Project Officers*

- Identify risks;
- Propose risk limits;
- Control mechanisms; and
- Reporting.

### *Senior Management*

- Establish policy;
- Establish risk limits;
- Establish risk tolerance (or risk appetite);
- Board reporting; and
- Enforce.

### *Board of Directors*

- Approve policy;
- Approve risk limits;
- Approve risk tolerance; and
- Provide oversight

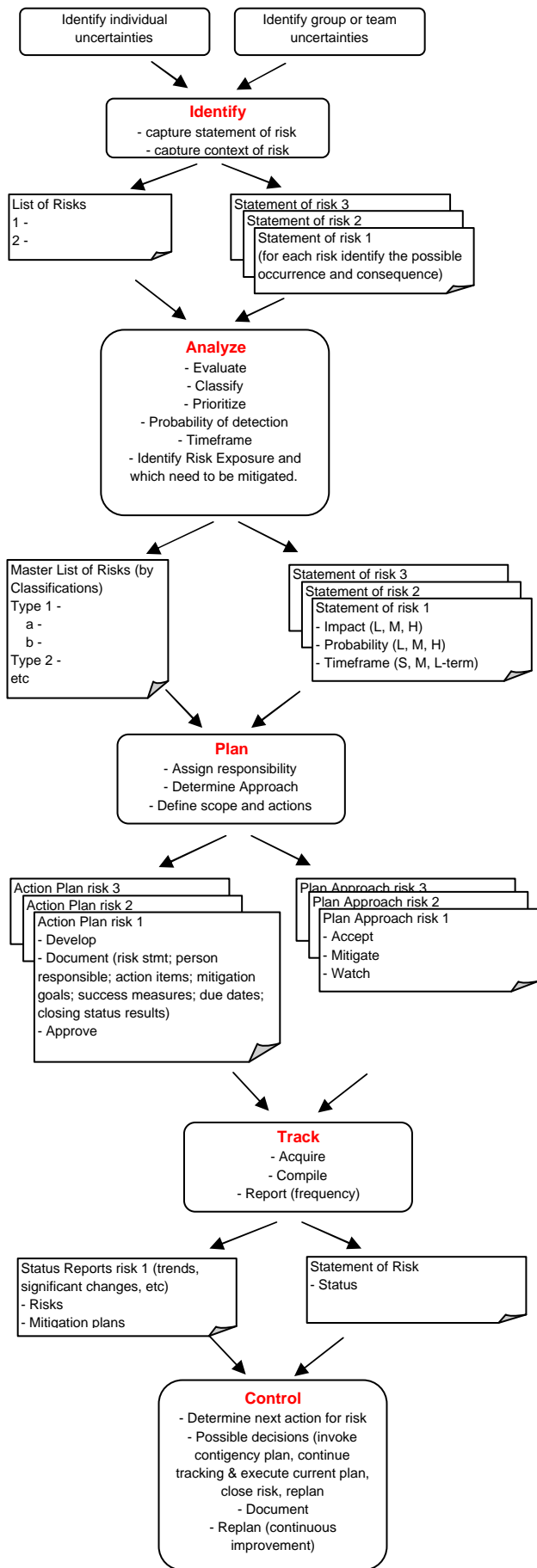
### *Risk Champion (Chief Risk Officer or designate)*

- Monitor, coordinate and teach;
- Measure – benchmark;
- Report to board; and
- Enforce.

### *Internal Audit*

- Monitor the quality of performance of IRM initiatives;
- Assist management and the board by monitoring, examining, evaluating, reporting on and recommending improvements to the adequacy and effectiveness of IRM processes.

# Appendix 3: Risk Management Framework Overview



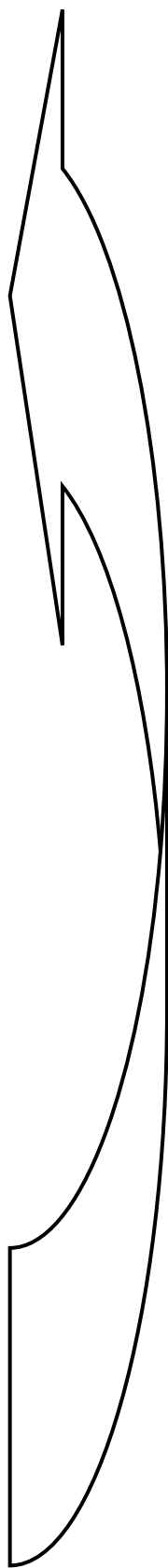
Step 1 - IDENTIFY

Step 2 - ANALYZE

Step 3 - PLAN

Step 4 - TRACK

Step 5 - Control

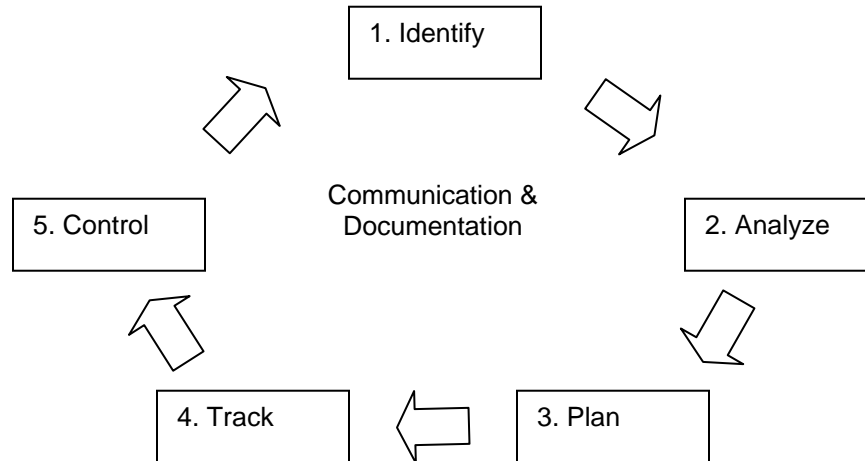


## Appendix 4: Risk Management Framework Guidelines

---

### Introduction

These guidelines provide additional guidance to assist with the implementation of the five-step Genome Canada Risk Management Framework.



### Step 1 - Identify risks

In the first step of Risk Management Framework all of the possible risks associated with individual project/platform as well as normal operations should be identified. The focus in this step is on capturing and not necessarily evaluating the risks. In addition, the consequence of an incident (risk) occurring should be identified.

It is also important to note that there may be significant cross-functional value-added input from different individuals, for example, soliciting the input from project managers, project leaders, coordinators from host organizations, GE3LS specialist may provide valuable insight.

At a minimum, an organization's risk profile should address risks in the following risk classes: strategic; functional (operational); project-related; and, platform-related.

Some of the perils that threaten operations and assets and create risks include fire, collision, theft, fraud, security leaks, violence, climate and earthquakes.

Factors influencing risks should be identified. They include: acts of nature; human inefficiency, negligence, error and wilfulness; and physical factors such as the availability and quality of materials and the state of a particular technology.

Each risk should be identified as one that is either: strictly internal to the Genome Canada or Genome Centre; or partly or wholly related to the actions or omissions, and property of other parties such as host organizations, collaborators, funding partners or suppliers, either by design or by chance.

This distinction has important implications for determining the respective obligations or potential liabilities, the degree of control that can be exercised over the probability of chance occurrences, the effect these occurrences may have, and the selection of the appropriate mitigation action.

Examples of possible risks include:

- Regulatory compliance, requirements
- Toxic operations and waste
- Technology requirements
- Business (misappropriation of assets, funds)
- Political
- Resources (Equipment; HR; Skills; funding)
- Development & Support (Infrastructure in place)
- Integration
- Maintenance and enhancement
- Design
- Ethical
- Disclosure of vital information (privacy of personal information)
- Back-up & Recovery - Electronic data, record keeping, computer & mail systems

## **Step 2 - Analyze risks**

For those risks that are deemed to require further analysis two main components, impact and probability, should be considered in determining the acceptability of a risk and their risk exposure index. These risk components should be analyzed separately.

Impact can be described as follows:

HIGH – expected to have a very significant negative impact. The impact could be expected to have significant long-term effects and potentially catastrophic short-term effects.

MEDIUM – Expected to have moderate impact. The impact could be expected to have medium-term detrimental effects.

LOW – Expected to have minor negative impact. The damage would not be expected to have a long-term detrimental effect.

Probability can be described as follows:

HIGH – The frequency of the event occurring is perceived to be once per hundred transactions.

MEDIUM – The frequency of the event occurring is perceived to be once per thousand transactions.

LOW – The frequency of the event occurring is perceived to be once per ten thousand transactions.

***[TO BE TAILORED]***

To simplify the analysis of the various risks it may be appropriate to group or classify the various by categories that would be considered appropriate by source or nature of risks, for example, scientific, technology, ethical, for financial.

The assessment of the impact and probability will result in a risk exposure index that will determine the extent of actions required. The risk exposure index will also guide the prioritization of the identified risks. Other considerations in the prioritization could include the probability of detection and the possible timeframe within which this event may occur.

**Risk Exposure Index Matrix**

	M	H	VH
Impact	L	M	H
	VL	L	M
	Probability		

Risk Exposure Index	Action
Very High	Unacceptable – requires (further) mitigation
High	Acceptable only with executive sign-off
Moderate	Acceptable with project leader sign-off
Low	Acceptable with no review
Very Low	No further documentation required

### Step 3 - Plan

This step requires the determination of the following:

- Responsibility (designate person)
- Approach (Accept, Mitigate or Watch/Monitor)
  - Keep the risk
  - Transfer to a third-party (may require a contingency plan which identifies a contingency trigger)
  - Delegate (internally)
- Scope of Actions
  - Develop mitigation plan – required for critical risks (those with Risk Exposure Indexes greater than X)
  - Document
  - Approval by appropriate level of management or Board

As a general rule, high risk events require a plan that avoids transfers or prevents the risks. Moderate risk events require inspection and correction controls and monitoring processes (for downstream risks). Low risk events may be deemed acceptable and not require further documentation.

In establishing the plan certain constraints may need to be considered such as performance requirements, cost, schedule (timing) or safety.

### Step 4 - Track

This step will require that relevant tracking data be collected. The frequency (weekly, monthly, quarterly, annually) of the data collection would be defined in the risk action plans.

Once the data has been compiled, the risk attributes (probability, impact, probability of detection and timeframe) should be re-evaluated.

Pre-defined reports should be prepared and distributed and should include:

- Status of the risk
- Status of mitigation efforts
- Trends
- Significant changes

### **Step 5 - Control**

This last step is actually the beginning of a continuous improvement process that determines the next action of the risks, strategy and possibly the overall risk management approach.

Possible decisions associated with the identified risks include:

- Re-plan
- Close the risk
- Invoke a contingency plan
- Continue tracking & execute current plan

In any event all decisions need to be adequately documented and approved by the appropriate level of authority.