Fleming College

Procedure Title:	Enterprise Risk Management Procedure
Procedure ID:	#OP 1-108
Manual Classification:	Section 1 – College Policies
Linked to Policy:	#1-108- Enterprise Risk Management
Approved by Senior Management Team:	September 14, 2020
Revision Date(s):	N/A
Effective Date:	October 1, 2020
Next Review Date:	October 2021
Contacts for Policy Interpretation:	Vice-President, Corporate Services & CFO

1.0 – Purpose

ERM is a continuous, proactive and dynamic process to identify, assess, manage and communicate risks that may impact the achievement of the strategic goals of the organization. ERM activities are an integral part of College planning and operations. ERM supports and improves the decision-making, planning and prioritization processes by ensuring that risk is continually assessed and managed. ERM will assist the College in attaining its goals, helping to avoid pitfalls and surprises along the way.

It involves employees at every level of the institution and requires the development of risk profiles across the entire organization. This procedure sets out the structure of how ERM is to be carried out and is intended to operate in harmony with all other policies and strategic operations of the College.

Fleming College's ERM is based on the best practice and standards of ISO 31000:2018. These risk management practices and standards can also be applied to specific initiatives, projects, or activities.

2.0 – Definitions

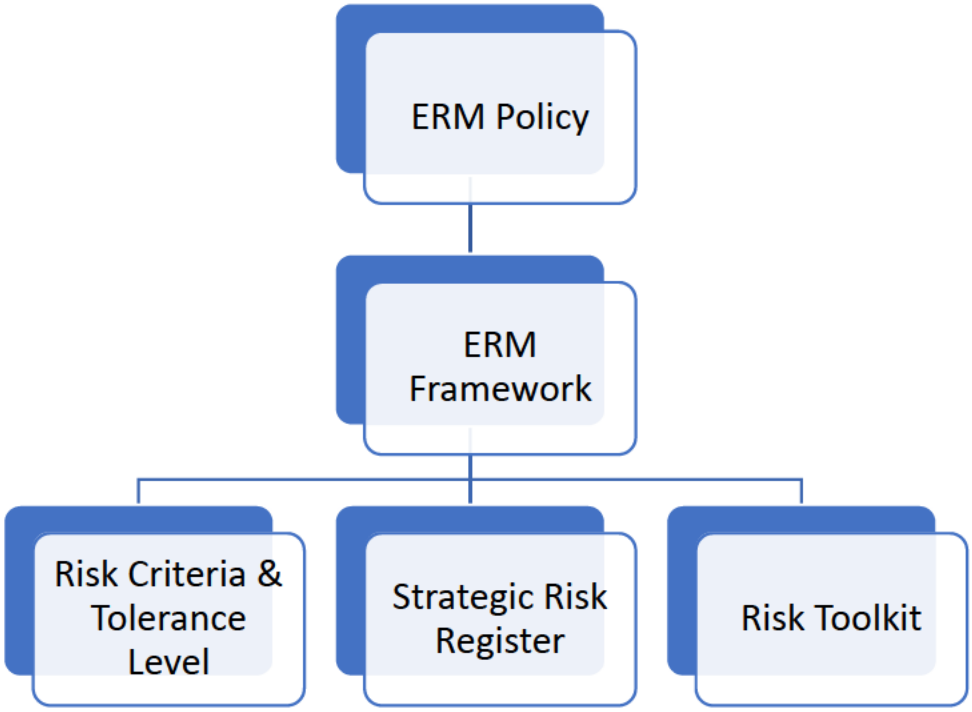
In addition to those terms defined in **College Policy #1-108** (Enterprise Risk Management), the following terms may apply when invoking the present procedure:

Stakeholder Analysis	This involves the identification of internal and external stakeholders and their respective roles, degree of influence, interests and motives and position with respect to value criteria. They can be both bearers of risk, and/or sources of it.
Assumptions and Constraints	These include fixed deadlines, executive directives, resources, or other limiting conditions. Legislation, regulation, and policy are part of the context in which the risk assessment will take place. Not only do they often address the risks identified, but they also guide the implementation of proposed mitigation strategies.

3.0 – ERM Program Structure, Process and Map

The ERM program at Fleming College is structured to facilitate the appropriate management of risk in conjunction with the College's Strategic Plan and its stated goals.

The ERM Framework (ISO 31000:2018) was used to develop this Procedure which details how the College will properly manage Risk Criteria and Tolerance Level(s), its Strategic Risk Register, and its Risk Toolkit.



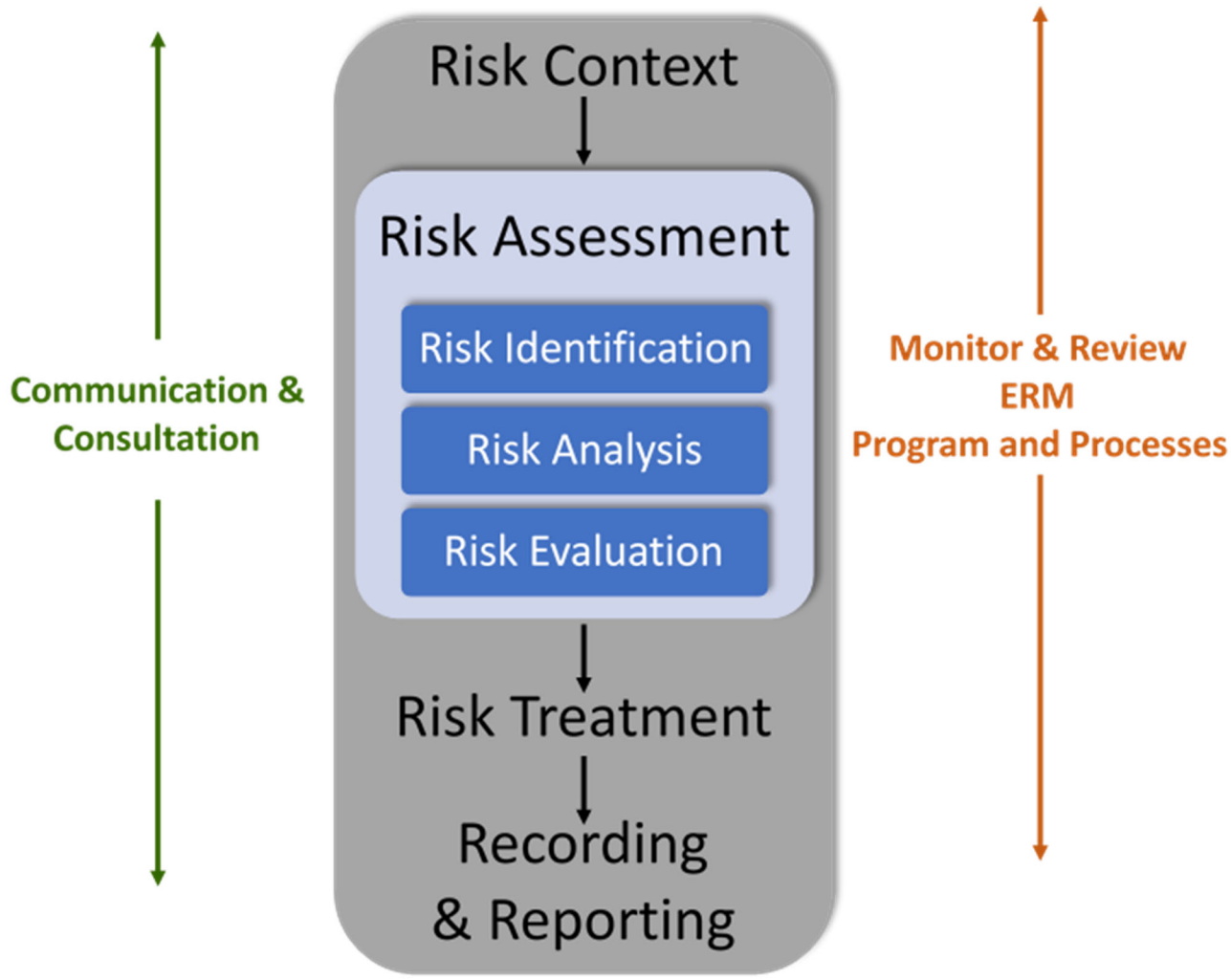
The **ERM Procedure Map** (below) gives a general idea of how information and decisions are made when the College follows the present Procedure.

Communication & Consultation: Communication and Consultation are important to assist stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication and consultation should take place within and throughout all steps of the risk management process. Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making.

Establish Context: Take into consideration the internal and external environments, as well as the purpose, goals, and objectives of the ERM program and key relationships that may impact or be impacted by the risk management process.

Risk Assessment: Three main steps will result in understanding the risk exposure present. The steps are detailed below in the **ERM Procedure Map**.

ERM Procedure Map



---

1. **Risk Identification:** identification of risks which arise from the internal and/or external environment. It is important to ensure that the full range of risks is identified, including both threats and opportunities.

2. **Risk Analysis**: consider the extent to which potential risks might have an impact on the achievement of strategic priorities. Risks are assessed for likelihood of occurring as well as consequences of occurrence. The analysis is documented within a Risk Register.

3. **Risk Evaluation:** A Risk Register is developed as the primary tool for articulating Fleming's risk profile. Where risk exceeds acceptable level of tolerance, additional risk treatment strategies may be applied to reduce the level of risk.

Risk Treatment: Identification of the range of options available for treating risk and assessing the appropriateness of each alternative.

Monitor & Review: regular monitoring and review of risks are essential to understanding the changing dynamic of risk and the ERM program.

4.0 – ERM Responsibilities

Employee responsibilities under the College's ERM program are established in the College's ERM Policy (**#1-108**).

5.0 – Risk Assessment

Risks are assessed by identifying the likelihood and consequences of a risk event occurring ('likelihood' is not synonymous with 'probability'), categorizing the risks, and identifying existing treatments for those risks.

Risks are often identified using surveys, loss histories, process flowcharts, and expert advice (both from internal and external sources). Other methods include:

- Interviews and focus group discussions,
- Environmental scans and competitor analyses,
- Audits and physical inspections,
- Questionnaires and the Delphi technique,
- Networks of peers, industry groups and/or professional associations,
- Subject Matter Expert consultations – speculative, conjectural and intuitive,
- Historical records, failure analyses, 'lessons-learned' reports,
- Incident, accident and injury investigations/reports,
- Scenario analyses,
- SWOT (Strength, Weakness, Opportunity, Threats) analyses,
- System design reviews and system analysis,
- Scenario analysis and simulation (including mathematical/statistical modelling).

Once identified, the College groups risks into the following categories:

- **Reputational** risk is a hidden threat or danger to the good name or standing of an organization – the realization of these risks often happens without warning.

- **Human Resource** risk includes (but is not limited to) threats that effect: staffing/skill(s) levels, professional development, performance, succession, recruitment/retention, compensation, labour relations, employee satisfaction, and health and safety.

- **Strategic** risk is associated with the strategic direction of an organization. Strategic risks are often a function of uncertainties that may be driven by strategic and market direction, government policy, competition, court decisions or a change in stakeholder requirements.

- **Financial** risk relates to losing/gaining financial resources which may include market risk, liquidity risk, budgeting risk, insurance risk and capital management risk.

- **Compliance** risk relates to various regulatory requirements such as accessibility, funding compliance, legal compliance, privacy law and procurement practices.

- **Operational** risk pertains to how we deliver programs and services to students and members of the College Community, as well as to the internal and external processes and systems the College utilizes.

Once you have identified all relevant sources of risks and their categories, you should 'state' the risks by detailing the following three elements for each: Event, Causes and Consequences. Clearly articulating these three elements for each risk helps to develop tangible, treatable strategies for each.

For an effective process, it is important to define the Event as something that could prevent achievement of an objective, milestone or target, or create an opportunity to exceed them. From there, the causes and consequences of realizing that risk should become more apparent.

To do so, follow these three steps:

1. Identify the risk event (using one of the above methods) that is related to an in-scope objective. General, unfavourable conditions, in and of themselves, are not risk events.

2. List the potential causes of such an event. There are often multiple potential causes for any given risk event. To determine the specific 'why' for the identified risk, consider the use of a root cause analysis method (such as the Five Whys tool).

3. Identify the consequences of the event. Do not just consider the immediate consequences of its occurrence – would more consequences be realized after the primary consequences?

Once a risk is clearly identified, you must also identify existing mitigations (if any).

All Risk Assessments are documented in the Risk Register, including existing mitigations (if any). Additional/proposed mitigations (if required) are not detailed in the Risk Register until approved and implemented.

6.0 – Risk Analysis

Risk analysis is the process of calculating the likelihood of an event and the consequence if it were to occur. The product of these two variables is the Risk Score. See **Risk Criteria (Appendix I)** for the impact and likelihood tables.

Likelihood is the chance that the identified risk will actually occur. When available, statistical data can support estimates of likelihood and impact. In practice, when historical data is not available, consultation(s) with Subject Matter Expert(s) is often required. As a result of this, likelihood assessments rarely imply mathematical certainty but, rather, a subjective estimate.

Using likelihood and consequence, risk types are then scored by the Dean or Director. It is not necessary to use all the different risk scores for any particular risk assessment, but as a minimum, the rating of initial risk is required, and residual risk is recommended.

> **Inherent risk:** involves rating the exposure in the absence of existing controls. When seeking to understand inherent risk, we are considering a hypothetical condition free of all controls, like locks, rules, procedures, ethics and so forth. This can be difficult to imagine. However, there is value in assessing risk this way as it can identify whether an exposure is over- or under-controlled. Strategic risk assessments often benefit from an assessment of inherent risk.
>
> **Initial risk:** involves rating the exposure within its current control environment (i.e. now). Initial risk is a baseline against which you can measure progress. Reviews of loss histories, reviews of similar sectors' loss histories, and consultation with stakeholders can support the assessment process.
>
> **Residual risk:** involves rating the exposure after the development of additional mitigation/treatment strategies. It is important to establish a residual risk score because it is a prediction of the efficacy of proposed mitigations. It also serves as a start point for an informed discussion of acceptable risk with senior decision-makers.
>
> **Current risk:** is a measure of progress. Later, regular updates on the progress of risk mitigation strategies can be valuable in helping to demonstrate progress or to secure additional resources for stalled mitigation efforts. The tracking of current risk over time allows efficient shifting of resources to problem areas or to areas of opportunity. In addition, tracking the progress of current risk can help demonstrate the effectiveness of the organization's risk management program.
>
> Risk scoring must always consider the College's established risk tolerance.

7.0 – Risk Evaluation

Risk Evaluation consists of considering the scored risks in relation to existing mitigations and the College's risk tolerance for the particular risk. This process enables the risk lead (SMT member who is **accountable** for the risk) to arrive at a decision – guided by specific criteria and consideration of costs and benefits. There are three considerations when evaluating existing

mitigations and controls – and details for each should be entered into the risk register as follows:

1. Characterize, in qualitative terms, the existing mitigations/controls as one of the below and include additional information as describe:

    a. **Non-existent, Inadequate, Adequate, Robust, Excessive** (Excessive indicated that a risk is over-controlled/over-mitigated, resulting in over-spending or lost opportunity).

    b. How would you describe the process, policy, device, practice or other action already in place that mitigates the risk in question?

2. Characterize the risk in relation to the College's degree of tolerance:

    a. **Unacceptable, Acceptable with Treatment, Acceptable**.

    b. It is possible to have 'zero' tolerance for certain risks (assuming one can avoid them completely). A risk may be 'Acceptable' either because it is inevitable and too prohibitively costly to treat or, because it is immaterial and not worthwhile to treat.

3. Determine consequent action based on steps 1 and 2:

    a. **Avoid, Treat, Monitor, Tolerate**

    b. You may avoid risk entirely, if unacceptable for the College's risk tolerance, by not engaging in any activity that would cause the risk event. We tolerate and monitor risk when mitigation is impracticable or prohibitively costly. We monitor risks that are inconsequential but whose status might change.

When risks cannot be avoided, but require actions beyond monitoring/tolerating, the College will treat the risk.

8.0 – Risk Treatment

Risk treatments work to prevent the event by addressing the causes or decrease its consequences by treating the negative effects and preparing for post-event recovery.

Existing legislation, regulation, policies, and procedures effectively mitigate many organizational risks. These legal and administrative controls effectively reduce to tolerable levels most risks associated with routine activities. The first risk management priority should therefore be a review of procedural controls and remedial action to educate and encourage compliance. Internal Audit is an excellent resource to assist in assessing compliance with policy.

Should existing treatments be inadequate, new, or need to change, a risk assessment and consideration of additional treatments may be appropriate.

Treatments (risk mitigations) can consist of virtually any sort of administrative action, as well as the application of specialized disciplines – where a separate analysis may be required; e.g.,

emergency planning, business continuity planning, security planning, risk financing; financial controls; human resources management. Grouping risks in categories can help in the design of cost-effective treatments. If the current level of risk is unacceptable or acceptable with treatment a treatment strategy should be recommended.

To frame Risk Treatment activities, consider, “what might be done to prevent the event from happening”, then ask, “If it were to happen, how can we limit the damage done and get back to business?”

For negative risks (threats), treatment options include:

1. Avoidance (eliminate the risk by avoiding event-causing activities)

2. Transference (shifting the negative consequences and ownership of response to a third-party)

3. Mitigation (reducing the likelihood and/or consequences of occurrence through purposeful planning and actions)

4. Acceptance (continue operating as ‘normal’ but create contingency plan(s) to address occurrence)

For positive risks (opportunities), treatment options include:

1. Exploitation (ensuring the realization of the risk)

2. Sharing (partnerships and joint ventures to increase the likelihood of occurrence)

3. Enhancement (maximize key ‘drivers’ of the positive impact of the occurrence)

4. Acceptance (preparations to take advantage of the occurrence of the risk event but not actively pursuing/facilitating its occurrence)

Once approved and implemented, risk treatments must be catalogued in the risk register.

9.0 – Risk Register, Monitor and Review

College risks should be monitored by managing and reviewing your risk information and register, as a regular practice. Risks themselves undergo change and can require revision in terms of their description and ranking - new risks also ‘appear’ regularly and old risks may require ‘striking through’ (not deleting) and archiving. Therefore, periodic updating of risk information is recommended, using the risk register as a management tool.

When used to track the implementation of mitigation strategies and the resultant consequence on risk ratings, the risk register becomes a valuable communication tool by informing every one of the progress or lack thereof, and any additional resources required.

In a mature practice of risk management, a growing body of information can inform analysis of the risks themselves, their most common sources, their frequency and consequences /costs of actual occurrence, the efficacy of treatments, and the occurrence of unforeseen events. All of this serves to better manage risks and inform planning. Audits, complaints investigations, legal

judgements, and retrospective cost/benefit analysis are some sources of historical risk information.

The Risk Register is managed by the ERM Committee. This group is responsible for ensuring risks are being processed appropriate, for reporting on the Risk Register as required and for monitoring the performance of the ERM processes and outcomes.

10.0 – Related Documents

- Policy #1-108, Enterprise Risk Management
- Risk Planning Guide
- Enterprise Risk Management Training Video
- ERM Committee Terms of Reference – To Be Developed.

11.0 – History of Amendments & Reviews

Approved by SMT on September 14, 2020

Appendix I: Risk Criteria (page 1 of 2)

Risk **likelihood** is classified using the following table:

Assessment	Rating	Description	Indicator	Immediate chance of occurring
Very likely	5	expected in most circumstances	multiple times a year	> 99%
Likely	4	will probably occur in most circumstances	once a year	> 50%
Possible	3	might occur at some time	once within 3-5 years	> 30%
Unlikely	2	could occur occasionally	within 10 years	< 30%
Rare	1	may occur in exceptional circumstances	within 25 years	<1%

Appendix I: Risk Criteria (page 2 of 2)

Risk **impact** (consequence) is classified using the following table:

		Considerations				
Assessment	**Rating**	**Finance**	**Compliance**	**People**	**Reputation**	**Operations**
			Breach resulting in:			not inclusive
Severe	5	> $3.5 M	Material sanctions, fines, penalties	Loss of several key leaders and/or multiple critical staff Long term impact on staff engagement	Long -term wide spread media coverage, major long-term impact	Complete disruption unplanned outage > 2 weeks widespread staff/visitor safety at risk
Major	4	> $1 M	Significant sanctions etc	Loss of few key leaders and/or a critical staff Medium term impact on staff engagement	Medium -term wide spread media coverage, short-term impact	widespread disruption unplanned outage > 5 days some staff/visitor safety at risk
Moderate	3	~ $500 K - $1.0 M	some penalties/fines	Loss of one key leader Medium term impact staff engagement	Short -term localized media coverage, Short-term impact	minimal disruption unplanned outage > 1 day local staff/visitor safety at risk
Minor	2	~ $100K - $500K	Immaterial fines	Loss of identified successor of key leader, minimal impact staff engagement	Medium -term localized media coverage, medium-term impact	local disruption unplanned outage couple hours minimal staff/visitor safety at risk
Insignificant	1	< $100K	nothing	Nominal impact staff engagement	No media coverage, minimal impact	no risk