Enterprise Risk

Planning Guide

This document combines **ERM Training (in blue)** with a **Guide on how to complete the Enterprise Risk Plan (in black)** which can be found on the Enterprise Risk Management staff portal website. The Plan form can be used for initiating a risk and for follow-up updates. The Enterprise Risk Plan form contains space for the following:

[Risk Assessment 1](#_Toc57115193)

[Risk Identification 1](#_Toc57115194)

[Risk Analysis 3](#_Toc57115195)

[Risk Evaluation 5](#_Toc57115196)

[Risk Treatment 6](#_Toc57115197)

[Glossary 7](#_Toc57115198)

# Risk Assessment

Risk assessment is the process of ***risk identification, risk analysis*** and ***risk evaluation.*** It forms a key aspect of the overall ERM method, allowing for the documentation and review of risks to prepare for treatment and ongoing monitoring. To effectively complete a risk assessment, a group must undergo three key steps:

* 1. ***Risk identification*** to find, recognize and describe risks
	2. ***Risk analysis*** to comprehend the nature of risk and to determine the level of risk
	3. ***Risk evaluation*** to review results of risk analysis to determine whether the risk and/or its magnitude is acceptable or tolerable (SMT Group’s accountability)

Once the risk assessment is completed, a group will be ready to determine ***risk treatment,*** the strategy to modify the risk that has been assessed.

The following sections provide an overview of the steps that should be followed to complete each of the three key steps of a risk assessment. To facilitate the completion of an assessment, Enterprise Risk Plan and the Risk Register should be utilized; working copies of both tools can be acquired from ERM portal website.

##

## Risk Identification

Identification of risks is the foundational step of any risk assessment, as it establishes the set of Items for analysis and evaluation. When identifying risks, one must consider their lens, gather appropriate information, and organize their thoughts with the aim of being succinct but informative. The following steps should be followed:

#### **Establish Scope**

* + - 1. Ensure that boundaries are placed around the risk assessment; one should not limit the subject matter discussed, but there needs to be attention paid to make sure that topics are appropriate for the group conducting the assessment.
			2. Maintain focus on the things that might impact the achievement of corporate and strategic objectives

#### **Gather Information**

* + - 1. Invite insights from a variety of sources of information; the more varied the view, the greater potential to identify fulsome risks
			2. Use any information available, whether it be documentation, statistics or opinions
			3. As is possible, continue to ask questions to get to the root of an item
			4. Always consider the "so what?" (i.e. what is the implication of the item)
			5. Allow for all thoughts to be heard; even those that are not 'right' add to the dialogue and help the concept to evolve or become more clear

#### **Organize & Group Thematically**

* + - 1. Break information down into manageable themes; remember the scope of the assessment and ensure that the risks are appropriate for the group conducting the work

#### **Document & Refine**

* + - 1. **Utilize the first part of the Enterprise Risk Plan** to document the risks (one form per risk), completing each of the fields as discussed in the Guidelines.
		1. **Make adjustments to information as required**
			1. Remember that no item will be perfect at the first iteration
		2. **Once the risks are documented, send to ERM C to populate the Risk Register**

### Risk Identification – Guidelines

**To be Completed by Divisions (Deans/Directors & Managers) and approved by accountable SMT Member**

The first Section of the Enterprise Risk Plan (found on the ERM portal website) is the Risk Identification.

1. **Department:** the Risk is most closely associated with from the dropdown menu in cell B4. This is usually the department who will have responsibility for the Risk Treatment or Mitigation.
2. **SMT Member Accountable** for the Risk.
3. **Observations** field lists observations about the risk/issue being explored. Use of bullet format is ideal. Research and insights should be included.
4. **Risk Appetite** is outlined for your context information only.
5. **Category:** Reviewing the Risk Analysis Criteria tab and selecting a risk consequence based on the category considerations. Please Note: although there is not a consideration for “Compliance (Legal)” the considerations in any of the categories can be used to determine the rating level. Select a Risk Category from the drop-down Menu. The category is the area that the risk potentially can impact.

|  |  |
| --- | --- |
| **Risk ID** | **Risk Category** |
| EE | External Environment |
| F | Financial |
| HR | Human Resources |
| IE | Internal Environment |
| L | Legal (Compliance |
| OP | Operations (including IT) |
| ST | Strategic |

1. The **Risk** **Statement** has a simple formula to stating the risk precisely:
	* 1. **Formula: A risk of ‘X’ could result in ‘Y’.**
		2. **E.g, A risk of ‘crossing the road on a red signal’ could result in ‘getting hit by a car and sustaining physical injury’.**
2. Provide a **Risk Label** that can be used as a label to refer to the fuller Risk Description.
3. Identify the **Risk Source** and root causes to the risk you may be aware of.
4. **Risk Controls** are Risk Treatments already in place to reduce the risk of likelihood or consequences or impact.

## Risk Analysis

Once a risk has been identified and documented, it is appropriate to determine the extent to which the risk might impact achievement of corporate and strategic objectives. Risk analysis uses a consistent method and set of parameters across all risks to determine a level of risk for each, therefore allowing for the comparison of a variety of risks. The College will use the Likelihood-Consequence (Heat Map) model, which can be executed using the following steps:

#### **Gather Sources** for Input

* + - 1. Having multiple {and differing) viewpoints is always better than a signal viewpoint during analysis

#### Assess **Likelihood & Consequence using the Risk Analysis Criteria Tab**

* + - 1. to determine the risk scores, completing each of the following fields:
				1. ***Likelihood -***the chance of the risk occurring; should be a score between 1 and 5, determined using the Risk Likelihood Criteria
				2. ***Consequence*** - the outcome of the risk if it were to occur; should be a score between 1 and 5, determined using the Risk Consequence Criteria. Estimating is a learned skill, but there are a number of estimating tools and techniques that can be used, this [website](https://www.tutorialspoint.com/top-10-tools-and-techniques-to-estimate-project-cost) explains each .

Expert Judgement

Analogous Estimation

Parametric Estimation

Bottom-up Estimation

Three-Point estimation

Research Analysis

Cost of Quality

Vendor Analysis

Group Decision Making [Techniques](https://toggl.com/blog/6-group-decision-making-techniques-your-team-needs-now)

Brainstorming

Nominal group Technique

Delphi Technique

Voting

Ranking

* + - * 1. When assessing the criteria, it is best to err on the side of caution (i.e. if there is a question of a score of 3 or 4, lean towards the higher score)
				2. There will be risks that have multiple types of consequences, choose the highest level

#### **Review** the Set

* + - * 1. Once scores are documented, review and send to the ERM Committee to populate the Risk Register

### Risk Analysis - Guidelines

**To be Completed by Divisions (Deans/Directors & Managers) and approved by accountable SMT Member**

1. Using the risk analysis criteria tab, determine the likelihood that a risk will occur and the consequence or impact if it did occur.
2. **Likelihood**: Based on your best estimate and using the Likelihood Rating Scale, pick a rating between 1 as the lowest likelihood of occurring and 5 as the most likelihood of occurring.
3. **Consequence**: In using the Consequence Rating Scale, estimate a risk level based on the category considerations criteria. Estimating is a learned skill, but there are a number of estimating tools and techniques that can be used, this [website](https://www.tutorialspoint.com/top-10-tools-and-techniques-to-estimate-project-cost) explains each .
	1. Expert Judgement
	2. Analogous Estimation
	3. Parametric Estimation
	4. Bottom-up Estimation
	5. Three-Point estimation
	6. Research Analysis
	7. Cost of Quality
	8. Vendor Analysis
	9. Group Decision Making [Techniques](https://toggl.com/blog/6-group-decision-making-techniques-your-team-needs-now)
		1. Brainstorming
		2. Nominal group Technique
		3. Delphi Technique
		4. Voting
		5. Ranking

Select a consequence based on your best estimate, pick a rating between 1 as the lowest consequence/impact and 5 as the highest consequence/impact. If there are two categories where you identify risk, select the highest consequence rating of the two.

1. Once you enter a number in the Likelihood Field B24 and the Consequence Field D24. A **Risk Score** will be automatically calculated (DO NOT TYPE IN THIS FIELD). The risk score is calculated by multiplying the likelihood rating (1-5) and the consequence rating (1-5). The **Risk Heat Map** on the Risk Analysis Criteria tab illustrates the scoring and therefore the priority weighting of risks.

## Risk Evaluation

The final step of a risk assessment looks to determine what the next step for the risk(s) should be. During risk evaluation, a target for each risk is established, which sets a marker to drive action out of the results of the assessment. If the score of a risk exceeds the Risk Tolerance, the risk may be subject for mitigation; conversely, if the score is at or below the Risk Tolerance, no action may be required. To complete the evaluation, the following steps should be completed:

#### Gather Sources for Input

* + - 1. Having multiple (and differing) view points is always better than a signal viewpoint during analysis

#### Establish the Risk Tolerance

* + - 1. Document the Risk Tolerance, by completing the following field:
				1. ***Risk Tolerance*** - the risk score that Senior Management can accept as a normal cost of doing business. Anything over this risk tolerance will require a Risk Treatment.
			2. Once scores are documented, send to the ERM Committee to populate the Risk Register

**Risk Appetite**:

* + The amount of **overall risk** in the entire enterprise risk portfolio the **Board** is willing to accept in pursuit of organizational objectives (i.e. value). The Board set the Risk Appetite in 2017 at ≥ 12.

**Risk Tolerance**:

* + The amount of risk for each **individual risk** that the **Senior** **Management Team** feels is acceptable as a ‘cost of doing business’ (i.e. also known as inherent risk, or residual risk).

#### Review Risks that Exceed the Risk Tolerance

* + - 1. Review each of the risks where the risk score exceeds the Risk Tolerance; each of these items should be a consideration for future action to bring the score to within the Risk Tolerance.

### Risk Evaluation - Guidelines

**To be Completed by Divisions (Deans/Directors & Managers) and approved by accountable SMT Member**

**SMT Group – Conduct Final Evaluation of all Enterprise Risk Plans**

This final step of the Assessment looks to determine what the next step for the risks should be.

1. Using the same risk analysis criteria tab and using the highest likelihood that a risk will occur and the highest consequence or impact if it did occur, that is acceptable for this specific and individual risk.
2. **SMT will review the Risk Tolerance** recommended and validate or reset the Risk Tolerance to continually calibrate the risks that add up to Fleming’s Risk Profile.

# Risk Treatment

With the risk assessed, the next step ls to determine the appropriate risk treatment. To determine the path of risk treatment, the following steps should be completed:

#### Gather Sources for Input

* + - 1. Having multiple (and differing) viewpoints is always better than a signal viewpoint during determination of treatment

#### Document and Analyze **Possible Treatment Options**

* + - 1. ***Possible Treatment Options***– see options below based on whether the risk is a threat or an opportunity
			2. ***Accept/Reject******-* SMT Group** todetermine the acceptability of each option

Risk Treatment options for **Threats** include:

* **Avoidance:** We can avoid risks by trying to eliminate the threat or protect the organization from the impact. This is appropriate for risks that have a high probability of occurrence with a large negative impact. Perhaps we decide not to pursue an opportunity at all because the risk is beyond our risk tolerance. This is one strategy.
* **Transfer**: involves shifting ownership of a threat to a third party such as insurance, performance bonds, warranties, and guarantees
* **Mitigation**: action is taken to reduce the probability of occurrence and/or impact of a threat. Early mitigation action is often more effective than trying to repair the damage after the threat has occurred.
* **Acceptance**: acknowledges the existence of a threat, but no proactive action is taken. This may be an appropriate response to a low-priority threat or one where its not possible or cost-effective to address a threat.

Risk Treatments options for **Opportunities** include:

* The **Exploitation:** increasing the likelihood of occurrence. This strategy may be used for high-priority opportunities where the College wants to ensure the opportunity is realized; that it definitely happens. When SMT was looking at public private partnership opportunities, as an SMT we discussed how we could act to increase the likelihood that a certain partnership would happen.
* **Sharing**: This speaks to the partnering strategy where two or more organization have a better change of achieving the opportunity together rather than apart.
* **Enhancing**: focuses on increasing the probability and/or impact of an opportunity to drive the size of the potential benefit. An example may be adding more resources to an activity to finish early if there were some benefits to an early finish.
* **Acceptance**: like for threats, is about acknowledging the existence of the opportunity but no proactive measures.

#### Document a **Risk Mitigation Plan**

* + - 1. If risk is above the Risk Tolerance, document the plan to mitigate the risk, completing the following fields:
				1. ***Action Item***- the specific actions to be taken for the mitigation
				2. *Action by-* the individual assigned to complete (or lead the completion of) the action
				3. *Timeline* - the timeframe during which the action is to be completed
				4. *RASCI - a* listing of the resources needed to complete the actions

**RASCI Stands for: R**esponsible, **A**ccountable; Supporting; **C**onsulted; **I**nformed; if **S**upports are added it is RASCI

See RASCI Guidelines Tab in the Enterprise Risk Plan

* + - * 1. *Reporting and Monitoring Required* - the manner in which the progress towards the action plan is to be monitored (e.g. quarterly status updates, KPI reports, etc.)
				2. *Mitigation Status and Date* – to understand where the mitigation is at
				3. *Completed By-* the name of the individual leading the completion of the Detailed Risk Plan
				4. *Completed Dote* - the date when the Detailed Risk Plan was developed

### Risk Treatment - Guidelines

**To be Completed by Divisions (Deans/Directors & Managers) and approved by accountable SMT Member**

**SMT Group – Conduct Final Evaluation of all Enterprise Risk Plans**

1. If the Risk Score is under the Risk Tolerance, then skip to “completed By” section.
2. If the Risk Score exceeds the Risk Tolerance, then enter Risk Treatment options.
	1. If one of the Risk Treatment Options is to Mitigate the risk (by trying to reduce the likelihood of occurrence or the consequence/impact if it occurs) then complete the Risk Mitigation Section.
	2. Also complete RASCI section by reviewing each role on the RASCI Guidelines and naming the individuals and title.

# Glossary

C

**Communication and consultation** - continual and iterative processes that an organization conducts to provide, share or obtain information and engage in dialogue with stakeholders regarding the management risk

**Consequence** - outcome of an event affecting objectives

**Control** - measures that is modifying risk

**E**

**Establishing the context-** defining the external and internal parameters to be taken into account when

**managing** risk, and setting the of risk criteria

**Event-** occurrence or change of a particular set of circumstances

**External context** - external environment in which the organization seeks to achieve its objectives

**I**

**Internal context** - internal environment in which the organization seeks to achieve its objectives

L

**Level of risk-** magnitude of *a* risk or combination of risks, expressed in terms of the combination of consequences and their likelihood

**Likelihood** - chance of something happening

M

**Monitoring** - continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

R

**Risk-** effect of uncertainty on objectives, deviation from the expected {positive and/or negative)

**Risk analysis** - process to comprehend the nature of risk and to determine the level of risk

**Risk appetite** - the amount of risk, at the broad level, the organization is willing to accept in pursuit of value

**Risk assessment** - overall process of risk identification, risk analysis and risk evaluation

**Risk criteria** - terms of reference against which the significance of a risk is evaluated

**Risk evaluation** - process of reviewing result of risk analysis to determine whether the risk and/or its magnitude is acceptable or tolerable

**Risk Identification** - process of finding, recognizing and describing risks

**Risk owner-** person or entity with the accountability and authority to manage a risk

**Risk profile** - description of any set of risks; the set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined

**Risk source** - elements which alone or in combination has the intrinsic potential to give risk to risk

**Risk treatment** - process to modify risk

**Risk Tolerance** - The amount of risk for each **individual risk** that the **Senior** **Management Team** feels is acceptable as a ‘cost of doing business’ (i.e. also known as inherent risk, or residual risk).

S

###### **Stakeholder-** person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

|  |
| --- |
| **Detailed Risk Plan – Template** (from ERM Staff Portal) |
| **Risk Identification** |
| **Department** |   | **SMT Member Accountable** | SMT Member Accountable for the risk |
| **Observations** | Use this field to gather your thoughts, simply list observations, research and/or statistics about the issue being explored. Use of bullet format is ideal. |
|  |
|  |
|  |
|  |
| **Risk Appetite (FOR YOUR INFORMATION ONLY)** | The college is willing to accept risk in pursuing opportunities, excellence in teaching, innovation, community partnerships, etc., as long as the following considerations within its key risk categories are observed:- Strategic Risk will not adversely impact the student experience, recruitment, enrolment and retention.- Reputation Risk (external and/or internal) will not significantly impact the college's reputation or compromise the fundamental of its mission, vision and values.- Operational Risk will not materially disrupt service delivery- Financial Risk when aggregated will not negatively materially impact college overall financial integrity and health- People Risk (Human Resources) will not significantly discourage trust, engagement, inclusion and empowerment, but should support and enable the College's people and communities.- Compliance risk - the college will operate with prudence within all legislation, regulation and policy-based requirements to the extent that it will not knowingly put itself in a position that results in significant non-compliance, or significantly delay its ability to take appropriate corrective actions. |  |
| **Risk ID** | TEMPLATE | **Risk Category** |   |  |
| **Risk Statement** | Keep this to a sentence to outline the risk, using the following statement format - **a risk of "X" that could result in "Y"** |  |
|  |
|  |
| **Risk Label** | provide short relevant name |  |
| **Risk Source(s)** | List elements giving rise to risk - root cause(s). Again bullet format is ideal. |  |
|  |
|  |
|  |
| **Controls** | list controls currently in place to mitigate the issue identified |  |
|  |
|  |
|  |
| **Risk Analysis** |  |
| **Likelihood** | key chance of risk occurring (1 - 5) | **Consequence** | impact of the outcome should risk occur ( 1 - 5) |  |
| **Risk Score** | #VALUE! |  |
| **Rationale for Likelihood / Consequence** | Use this field to express your thoughts and rationale for the risk analysis scoring including conclusion on desired target risk below. Tie your thoughts to the risk critieria guidelines. |  |
|  |
| **Risk Evaluation** |  |
| **Risk Tolerance** | What is the desired overall risk that should be tolerated for the issue described? |  |
| **Risk Treatment** |  |
| **Risk Type** |  |  |  |  |
| **Possible Treatment Options** | **SMT Group (Accept/Reject)** |  |
|   |   |  |
|   |   |  |
|   |   |  |
|   |   |  |
| **Risk Mitigation Plan** |  |
| **Action Item** | **Action by** | **Targeted Timeline** |  |
| 1. - |   |   |  |
| 2. - |   |   |  |
| 3. - |   |   |  |
| 4. - |   |   |  |
| 5 - |   |   |  |
| 6 - |   |   |  |
| **Reporting and Monitoring Required** |  |  |
|  |
| **RASCI** |  | **Name** |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Mitigation Status** |  | **Date** |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Completed (or Updated) By** |  | **Date** |  |  |
|  |  |  |  |
|  |   |  |  |