AP 573 – ENTERPRISE RISK MANAGEMENT

PURPOSE

The purpose of the Enterprise Risk Management (ERM) administrative procedure is to establish ERM roles and responsibilities as well as the strategy of Saskatoon Public Schools to manage its risks. The division will identify and manage its enterprise risks in support of its vision, values, guiding principles, goals and strategic plan. The division cannot seek to eliminate risk; rather, it will provide that existing and emerging risks are identified, communicated, and effectively managed.

BACKGROUND

Saskatoon Public Schools is committed to ensuring that risk management practices are embedded into key processes and operations to drive consistent, effective and accountable actions, and decision making in management practice and Board governance. Saskatoon Public Schools has designed its ERM framework to be consistent with the practices suggested by generally accepted global ERM standards frameworks, but at this time has not adopted any particular standard.

ERM is designed to identify potential events/risks that may significantly affect the division's ability to achieve its vision, values, guiding principles, goals, and strategic plan. Through the ERM process, identified risks are assessed based on likelihood and impact. Management processes and controls are used to provide reasonable assurance that significant risks are sufficiently mitigated to support the achievement of the division's objectives.

ERM assists to assess the division's appetite for risk (risk tolerance) and identifies gaps where identified risks are either over or under mitigated. This leads to identification of opportunities and strategies to either close gaps where residual risk is higher than risk appetite or to reallocate resources from areas where residual risk is lower than risk appetite.

The end product of ERM includes a ranked risk register used in developing the annual strategic plan and budget. ERM is an ongoing process with administrative procedure and outcomes revisited and reported at least annually.

Other administrative procedures exist that are related to specific types of risk. For example, the division is committed to education continuity management as outlined in Administrative Procedure 176: Education Continuity Management and Emergency Response Planning. Education continuity management includes the processes, procedures, discussions and activities that help to ensure that the division is able to function throughout a disruptive event such as an emergency, disaster or crisis.

DEFINITIONS

The following definitions will apply for the purpose of this administrative procedure:

Enterprise Risk Management (ERM): ERM is an integrated enterprise-wide risk process established over time which links the management of strategic objectives to risk in order to improve organization performance. It creates a formal process for managing the myriad of risks an organization faces. ERM is not the same as a risk assessment but, the assessment of risk is an integral part of an ERM process.

Risk: An internal or external event, activity or situation that impacts the ability of the division to achieve its vision, mission, outcomes and goals.

Enterprise-wide Risks: For identification purposes, risks may occur in any one of the following categories: financial, facilities, governance, human resources, information technology & support areas, operations, reputation and strategy & vision. Risks rated as high using division tolerance levels will be deemed enterprise-wide risks.

Financial Risk: The ability for the division to achieve its financial objectives.

Legal, Compliance and Reporting Risk: Compliance with applicable laws, regulations, reporting requirements and Board direction.

Reputational Risk: Real or perceived event that has the ability to impact the public confidence in the division.

Inherent Risk: The possibility that risks will prevent an organization from achieving its objectives before the consideration of processes and controls are in place to manage or mitigate the risks.

Impact: Significance of a particular risk to the entity. The significance of a particular risk can range from insignificant to severe/catastrophic. Magnitude of impact is determined with respect to an organization's risk appetite, risk capacity, and organizational objectives.

Likelihood of Occurrence: Probability that a particular risk will occur. These probabilities range from rare to almost certain.

Manage: To control or take charge of a risk in order to avoid or minimize its adverse impact on the division and to maximize its opportunity.

Mitigate: To lessen or minimize the adverse impact of a risk through specific management processes or internal control activities.

Optimize: To balance potential risks versus potential opportunities within the division's stated willingness or appetite and capacity to accept risk. This may require an organization to increase or decrease the amount of risk relative to the potential opportunity.

Residual Risk: Risk remaining after considering the effectiveness of management responses (i.e., processes and controls used to manage or mitigate the risks).

Risk Identification: The process of identifying and understanding potential risks to the division.

Risk Management: The process of identifying, evaluating, selecting and implementing an action plan to avoid or mitigate threats and to leverage and maximize, where possible, risk opportunity.

Risk Monitoring: The process of reviewing and evaluating the effectiveness of the action plan implemented through the risk management process and identifying opportunities to minimize future reoccurrence of similar risk.

Risk Opportunity: The return which may be realized if risk is assumed but managed in a manner that maximizes its potential benefit.

Risk Appetite: Level of risk an organization is prepared to accept to achieve its goals and objectives (i.e., the level of tolerance for risk in a company).

Risk Owner: An individual that has been given the authority to manage a particular risk and is accountable for doing so.

Management Effort: The use of resources and implementation of processes to support the division achieving its strategic objectives.

ROLES AND RESPONSIBILITIES

The following defines roles, accountabilities and responsibilities for:

Identifying and evaluating key risks;

Documenting and managing the response to key risks;

Facilitating appropriate risk/reward decisions at all levels of management;

Communicating risks, and management's responses and priorities to all relevant staff; and,

The following are the roles and responsibilities for governance of risk management at the division:

Role	Responsibilities
Board of Trustees	Has ultimate responsibility for risk. Provides governance oversite of the division's ERM program, as well as its risks and responses to them. This responsibility is demonstrated through review of at least the following items.
	The division's ERM framework (initially with updates as required).
	Management's risk appetite/tolerance levels, if formally developed (annually).
	Management's risk register and risk assessment results for the division's top enterprise-wide risks (annually).
	The Board has delegated certain oversight responsibilities of the ERM program to the Audit and Risk Committee.
Audit and Risk Committee	The Audit and Risk Committee (consisting of at least three Trustees of the Board) has been delegated certain responsibilities for oversight of the ERM program by the Board. The Audit and Risk Committee is responsible for reviewing, and presenting to the Board as required, the following:
	Changes to the division's ERM framework.
	Changes to management's risk appetite/tolerance levels, if formally developed.
	Management's risk register and risk assessment results for the division's top enterprise-wide risks.
	Action plans to address risk mitigations and opportunities identified as high priority by management.
Director of Education	Is accountable to the Audit and Risk Committee and Board of Trustees with respect to ERM, and is responsible for ensuring the ERM framework approved by the Board is implemented and operational through:
	Championing risk management within the division to ensure the division remains focused on risk.

Integration of ERM into the development of strategic, business and operational plans and operational decisions.

Ensuring effective risk identification, risk assessment, risk management and risk monitoring processes within the division.

Consulting, as required, with the division's employees or external consultants to effectively manage all aspects of risk.

Providing ERM status updates (either directly or via a designate) at every Audit and Risk Committee, and at least once per year to the Board of Trustees, on risk management activities, as well as if any significant risk changes or issues arise.

Budget and Audit Manager

Is accountable to the Director of Education and is responsible to managing the implementation and maintenance of the ERM administrative procedure and framework by:

Developing, monitoring and revising the ERM administrative procedure.

Coordinating the risk identification, risk assessment, risk management and risk monitoring processes.

Preparing status updates at least once per year to the Director of Education on risk management activities, as well as if any significant risk changes or issues arise.

Executive and Administrative Councils

Are accountable to the Director of Education and responsible for:

Active participation in the risk assessment process, including promoting the division's ERM Administrative Procedure and Framework as well as expectations for the management of risk.

The formal identification of risks that impact the division's strategic goals and objectives.

Assisting to rank risks, based on the division's impact and likelihood criteria.

Monitoring progress in managing risks and implementing improvement opportunities.

Reporting at Executive or Administrative Council meetings on the status of risk items delegated to specific risk owners.

Communicating the expectations of staff impacted by the identified ERM risks.

Communicating ERM results to all staff.

ENTERPRISE RISK MANAGEMENT FRAMEWORK

All risks are to be identified, assessed, managed, monitored and reported in a thorough and systematic fashion in accordance with the division's Enterprise Risk Management Framework.

Reference:
Date Last Revised: March 17, 2017