



cutting through complexity

Calgary Public Library

Risk Management Leading Practice Overview

KPMG Financial Risk Management

March 24, 2014

Document Contents

Report Topic	Page
1. Executive Summary	2 - 10
Project Overview	2 - 6
Risk Maturity Continuum	7 - 8
2. Leading Practice Analysis	9 - 27
i. Risk Management Framework Gap Analysis	9 - 13
ii. Risk Management Responsibilities and Processes	14 - 17
iii. Risk Assessment and Risk Register	18 - 19
iv. Board Level Risks and CICA Responses	20 - 21
v. Risk Reporting and Monitoring	22 - 23
vi. Alignment with the City of Calgary's Integrated Risk Management Framework	24 - 25
vii. Employee Engagement	26 - 27
3. Next Steps	28 - 30
4. Updated Observations	31 - 32



cutting through complexity

1. Executive Summary

Project Background

Calgary Public Library is working with KPMG to perform a Risk Management assessment, performing a gap analysis to industry and government best practices for risk management and identifying recommendations to close any gaps identified. This will include a review of the risk management responsibilities and processes for the Board, Executive and Senior Management, a plan to address critical (Board level) risks and recommendations to create employee buy in.

The gap analysis presented herein is based on a point in time review. The Executive Leadership Team has commenced implementation of some of the recommendations presented. These are further detailed in section 4 "Updated Observations".

Executive Summary

1. Project Overview

Key Success Criteria

The Calgary Public Library Integrated Risk Management Guideline identifies several risk management success criteria as follows.

Six Success Criteria:

- Proactive approach
- Corporate wide
- Systematic
- Integrated into long term strategic and business
- Informs day to day decision making
- Supported by corporate philosophy and culture



Executive Summary

1. Project Overview

Key Scope Areas:

1. Risk Management Framework Gap Analysis
2. Risk Management Responsibilities and Processes
3. Risk Assessment and Risk Register
4. Board Level Risks and CICA Responses
5. Risk Reporting and Monitoring
6. Alignment with the City of Calgary's Integrated Risk Management Framework
7. Employee Engagement

Executive Summary

1. Risk Maturity Continuum

Risk Maturity Continuum

ERM is not a “One Size Fits All” approach. The key is to determine the degree of maturity that is right for each organization

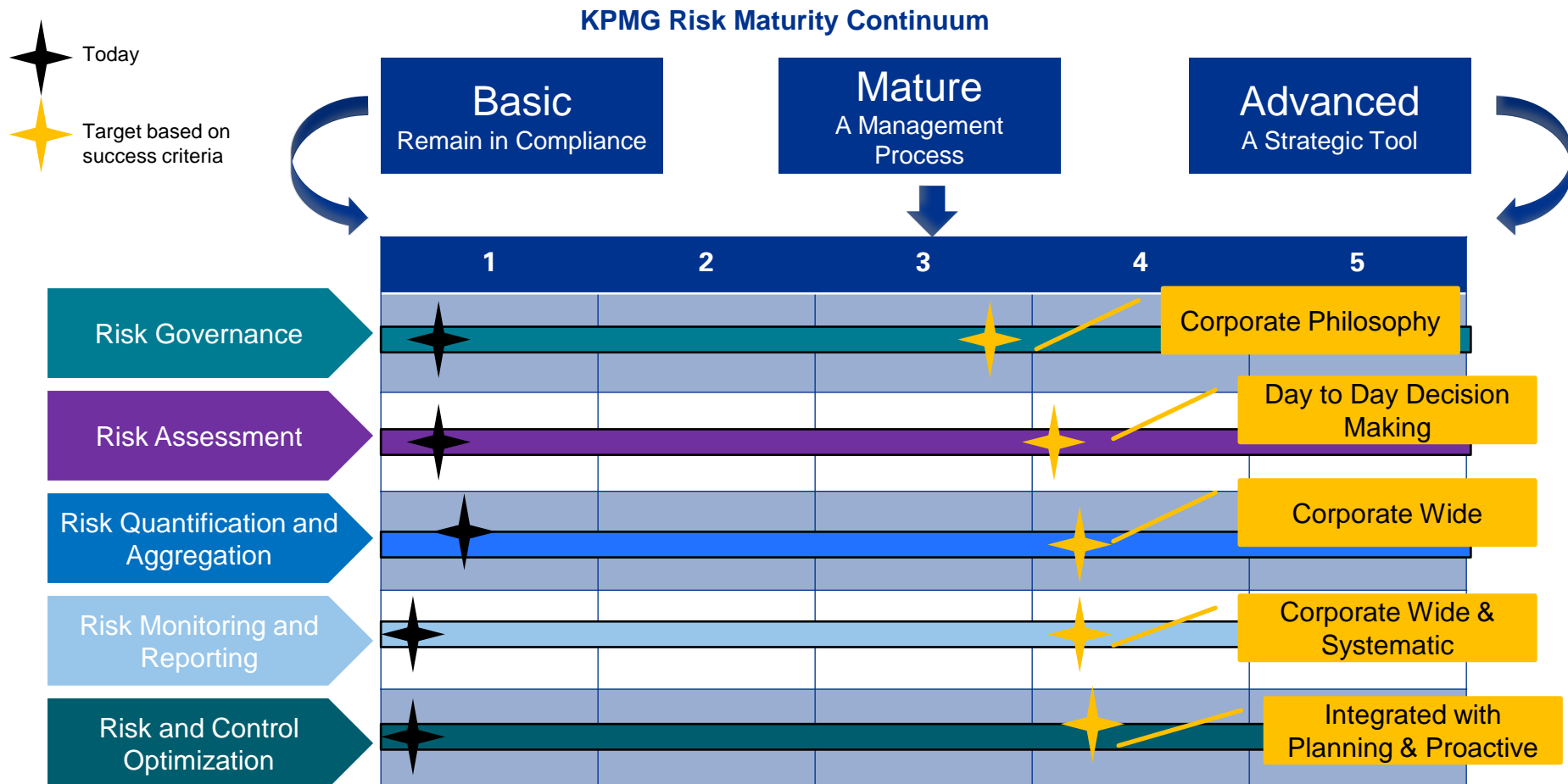
Framework Element	BASIC <i>Remain in Compliance</i>	MATURE <i>A Management Process</i>	ADVANCED <i>A Strategic Tool</i>
Risk Governance	A central Risk Management Policy exists to support external needs	A risk management structure with clear accountabilities exists to support risk management objectives	Risk management accountability integrated with performance management
Risk Assessment	Annual risk assessment with limited analysis and interpretation	Frequent risk assessments and analysis in-line with normal management reporting; minimum annual formal risk assessment for the organization as a whole	Risk and control activities embedded in business processes
Risk Quantification and Aggregation	Quantification of selected risks	Quantification of operational risk; advanced quantification of selected risks	Entity-wide aggregation across all risk areas
Risk Monitoring and Reporting	Business risk reporting designed to support external needs	Comprehensive reporting to the GCT Audit Committee and Board on current and future risks	Alignment of risk reporting to provide a single wide-ranging view of risk
Risk and Control Enhancement	Fewer surprises through management of key risks	Greater stakeholder confidence and improved risk mitigation strategies	Risk adjusted strategy, performance evaluation and approved budget use

Executive Summary

1. Risk Maturity Continuum

Risk Maturity Continuum

Organizations get to decide how far along the maturity continuum they want to progress, and at what rate, depending upon their risk management goals and objectives:





cutting through complexity

2. Leading Practice Analysis

i.) Risk Management Framework Gap Analysis

Leading Practice Analysis

2.i. Risk Management Framework Gap Analysis

Leading practice organizations develop a Risk Management Framework that aligns with the Strategic Objectives of the organization and that includes the following elements: Risk Governance, Risk Assessment, Risk Quantification and Aggregation, Risk Monitoring and Reporting and Risk & Control Optimization.

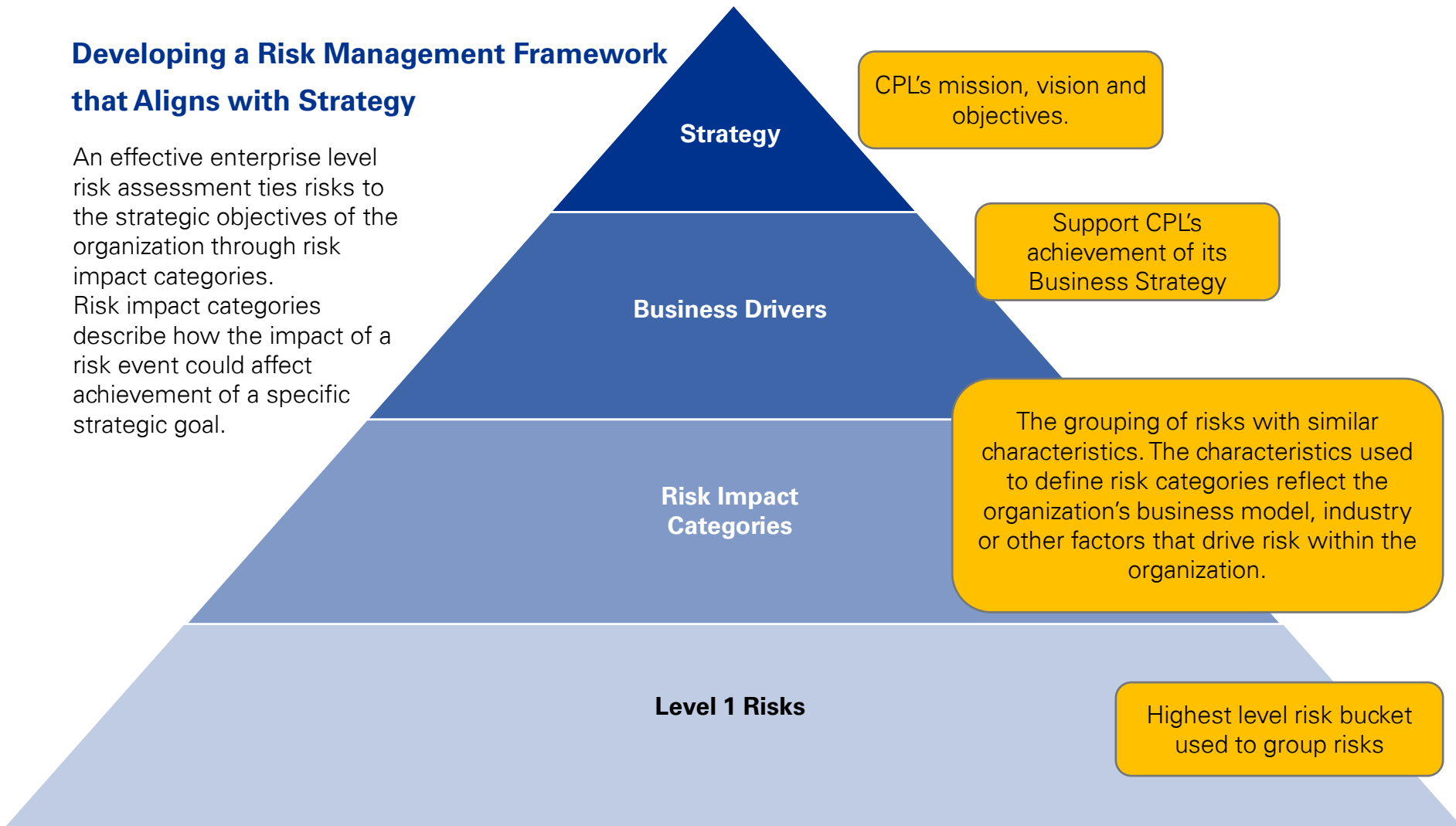
Theme #1	Risk Management Framework
Summary Observations	<ul style="list-style-type: none"> ■ Impact categories do not include specific or measurable impact thresholds. ■ Impact categories as defined may be too broad resulting in difficulty assessing specific impacts to the organization. ■ Risk tolerances are not specific or measurable.
Suggested Improvements	<ul style="list-style-type: none"> ■ Define specific and measurable impacts ("Critical," "High," "Medium," "Low," "Negligible") for each impact category and include a 5 level rating system. ■ If a measureable and specific impact cannot be define, consider re-defining the impact category. ■ Define specific risk tolerances.
Anticipated Potential Benefits	<ul style="list-style-type: none"> ■ Ease of consistent application and risk assessment across the organization and improved differentiation between impact categories. ■ Impact categories align with strategic objectives and can be clearly communicated and understood by the organization. ■ Board risk tolerances are well understood which may facilitate executive decision making, accountability and defined process for reporting and escalation of risk events.

Leading Practice Analysis

2.i. Risk Management Framework Gap Analysis

Developing a Risk Management Framework that Aligns with Strategy

An effective enterprise level risk assessment ties risks to the strategic objectives of the organization through risk impact categories. Risk impact categories describe how the impact of a risk event could affect achievement of a specific strategic goal.



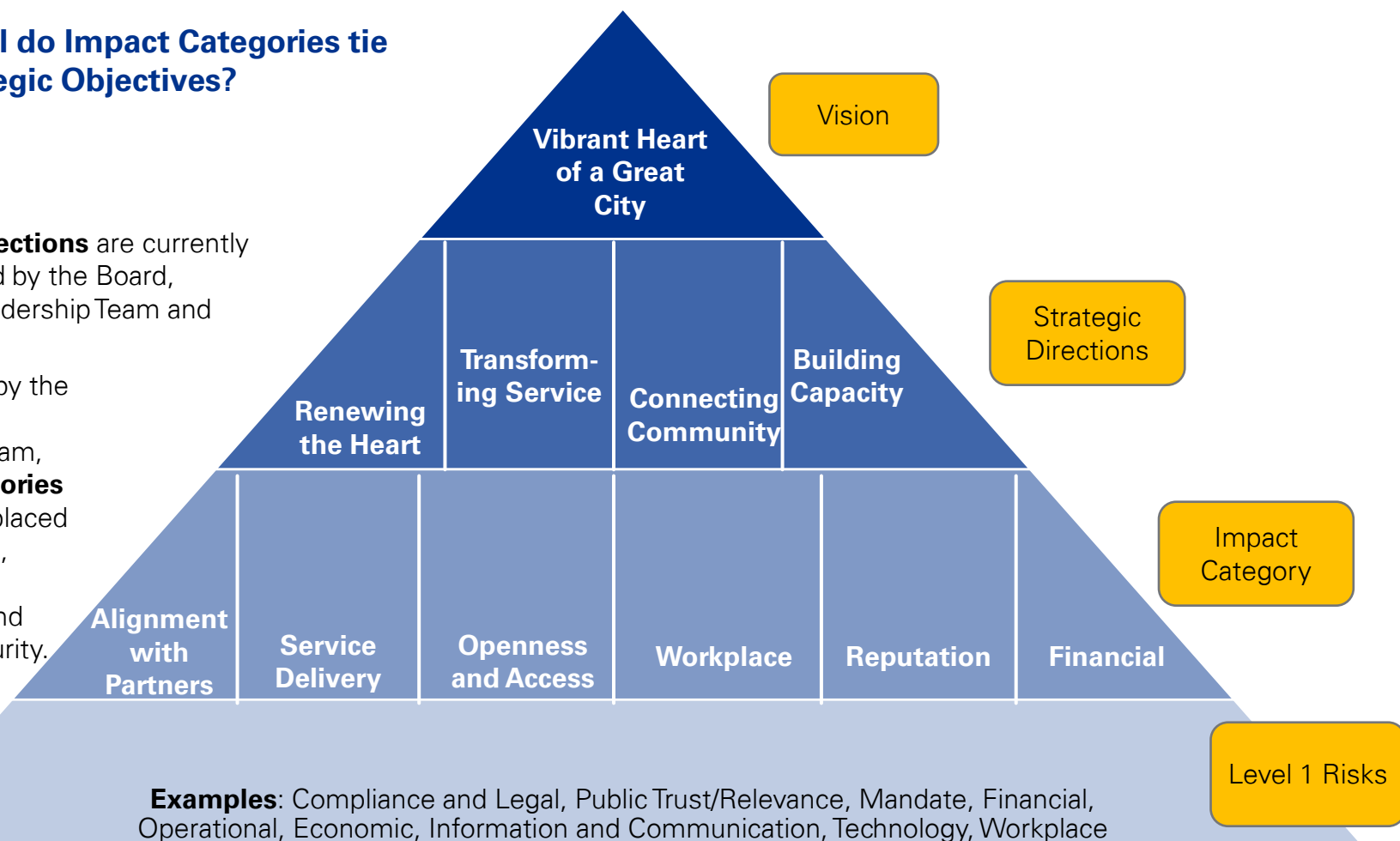
Leading Practice Analysis

2.i. Risk Management Framework Gap Analysis

How well do Impact Categories tie to Strategic Objectives?

Strategic Directions are currently being updated by the Board, Executive Leadership Team and organization.

Upon review by the Executive Leadership Team, **impact categories** have been replaced with Strategic, Financial, Operational and Safety & Security.



Leading Practice Analysis

2.i. Risk Management Framework Gap Analysis

Alignment of Strategic Directions with Impact Categories

- Alignment with Funders, Partners and Customers to ensure we continue to be a visible symbol of democracy, a community builder, connector and gathering place
- Service Delivery, including supporting learning and growth at every life stage
- Ensuring openness and universal access
- Strengthening the workplace
- Reputation
- Financial

STRATEGIC DIRECTIONS				
KEY ACTIONS	RENEWING THE HEART	TRANSFORMING SERVICE	CONNECTING COMMUNITY	BUILDING CAPACITY
	New Central Library	Make it Fun	Everywhere You Are	Strengthen the Core
	Laying a Foundation for a Second Century of Service	Make it Easy	A Community Story-Teller	Leverage Opportunity
		Make it Yours	Making New Friends	Sustainable Choices
		Make it Matter	Telling Our Story	Governance Matters
OUTCOMES	An Inspired and Inspiring Catalyst	Delighted Customers	Engaged Citizenry	A Resilient Organization

*Upon review by the Executive Leadership Team, **impact categories** have been replaced with Strategic, Financial, Operational and Safety & Security.



cutting through complexity

2. Leading Practice Analysis

ii.) Risk Management Responsibilities and Processes

Leading Practice Analysis

2.ii. Risk Management Responsibilities and Processes

Leading risk management programs have clearly defined risk management roles and responsibilities and accountabilities to facilitate ownership of work, alignment to common risk management objective(s), individual performance measurement, encourage collaboration, reduce inefficiency and enhance training.

Theme #2	Roles and Responsibilities
Summary Observations	<ul style="list-style-type: none"> ■ Board risk tolerances are not specific or measurable. ■ Risk management responsibilities are not specific. ■ Lack of process to communicate risk responsibilities and risk tolerances to employees.
Suggested Improvements	<ul style="list-style-type: none"> ■ Document Board level thresholds for escalation and reporting. ■ Define a delegation of authority that clarifies risk management accountabilities. ■ Annual Risk Management Policy review with all employees.
Anticipated Potential Benefits	<ul style="list-style-type: none"> ■ Board risk tolerances are well understood which may facilitate executive decision making, accountability and defined process for reporting and escalation of risk events. ■ Improved risk management accountability at all levels of the organization. ■ Improved buy in and engagement through better alignment with strategic objectives.

2.ii. Risk Management Responsibilities and Processes

Risk Management Roles

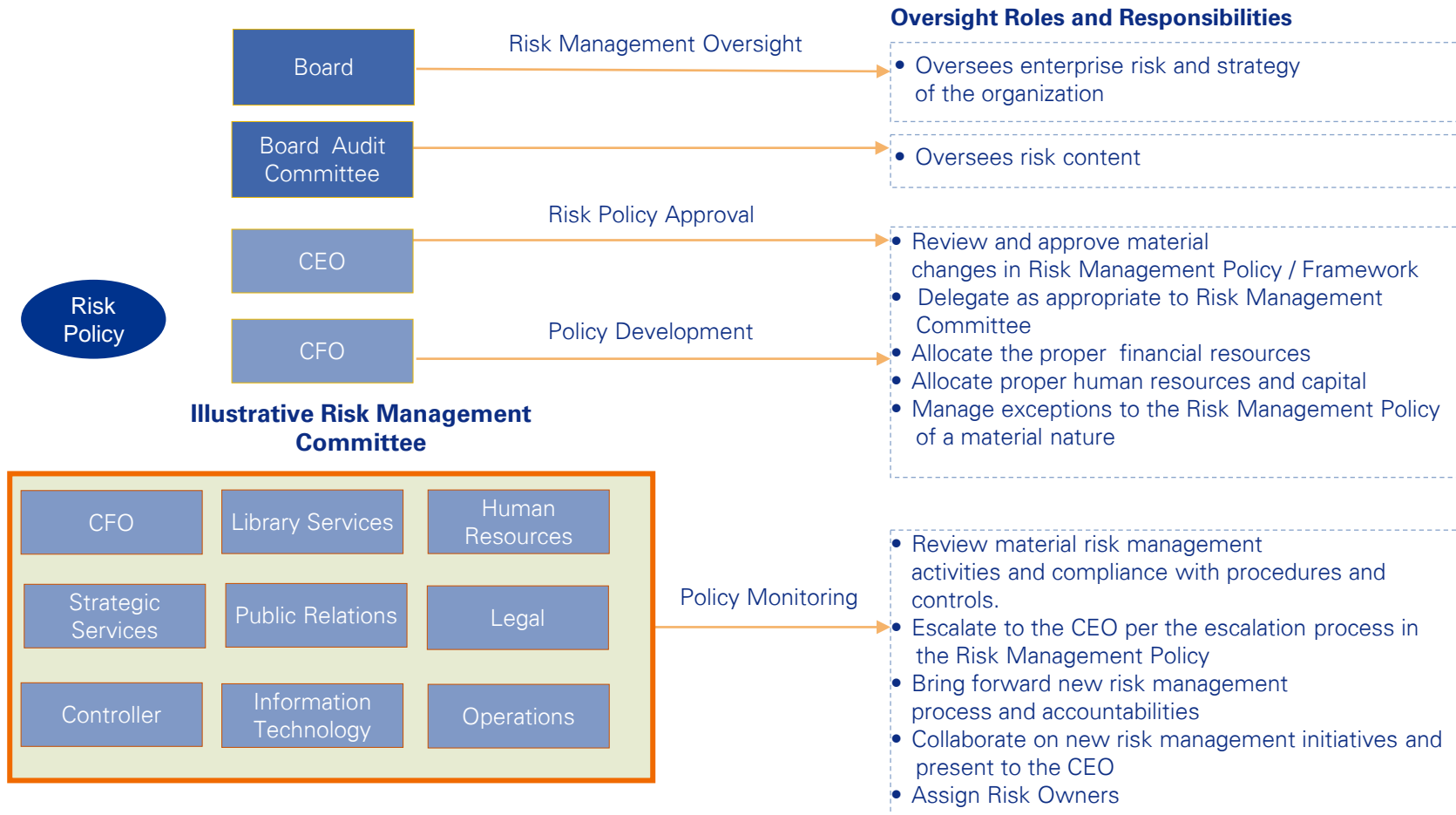
The following pages describe risk management roles and responsibilities for the Board (as represented through the Board Audit Committee), Executive Leadership Team and Risk Management Committee.

Leading Practice Analysis

2.ii. Risk Management Responsibilities and Processes

Leading Practice Governance Structure

A key decision with regards to IRM process is determining the ownership and oversight of the IRM process.





cutting through complexity

2. Leading Practice Analysis

iii.) Risk Assessment and Risk Register

Leading Practice Analysis

2.iii. Risk Assessment and Risk Register

Leading risk management programs use risk registers at all levels of the organization to document risks, risk assessment and risk mitigation activities. Those risks that meet the criteria for inclusion into an Enterprise risk register are aggregated onto an Enterprise risk register for management and Board reporting and monitoring.

Theme #3	Risk Register
Summary Observations	<ul style="list-style-type: none"> ■ Calgary Public Library has an enterprise level risk register that links inherent risks to the strategic impact categories identified. The strategic impact categories identified may be difficult to tie back to the strategic directions of the organization. ■ Risk Register impact category definitions and thresholds may not have the detail required to facilitate consistent understanding and application across the organization. ■ Mitigation activities may not refer to specific action plans, policies or processes.
Suggested Improvements	<ul style="list-style-type: none"> ■ Perform a review of impact categories to ensure they can be easily linked back to the strategic directions of the organization and perform a risk assessment for both inherent and residual risk. ■ Identify and define 5 impact thresholds for each impact category. ■ Refer to specific actions in the mitigation plans and identify risk owners for each action.
Anticipated Potential Benefits	<ul style="list-style-type: none"> ■ Ease of adoption across the organization as personal interpretation of impact thresholds is removed and improved differentiation between impact levels. ■ Assessment of residual risk to identify strength of mitigation processes. ■ Risk owners understand the specific actions and processes for which they are responsible.



cutting through complexity

2. Leading Practice Analysis

iv.) Board Level Risks and CICA Responses

Leading Practice Analysis

2.iv. Board Level Risks and CICA Responses

The Canadian Institute of Chartered Accountants (CICA) has defined a list of “20 Questions Directors Should Ask about Risk”. The Calgary Public Library Board Audit Committee was presented with management answers to these questions in the October 23, 2013 Audit Committee Meeting.

Theme #4	Board Risks
Summary Observations	<ul style="list-style-type: none"> ■ Board and senior management risk management accountabilities are not defined in specific or actionable terms. ■ IRM Framework implementation is scheduled for 2014. ■ Board has focused largely on financial risk to date (per Board member responses to the CICA questions).
Suggested Improvements	<ul style="list-style-type: none"> ■ Defined risk management responsibilities through a Delegation of Authority, Board risk tolerances and guidance from the Board on what is viewed as a critical risk will strengthen the IRM framework. ■ Board discussion on risk tolerances and identification of critical risks in addition to Financial risk.
Anticipated Potential Benefits	<ul style="list-style-type: none"> ■ Senior management and Board aligned with respect to risk management accountabilities. This will facilitate annual CEO performance reviews. ■ Board alignment with respect to acceptable risk for Calgary Public Library and alignment on critical risks that may require frequent discussion and review by the Board.



cutting through complexity

2. Leading Practice Analysis

v.) Risk Reporting and Monitoring

Leading Practice Analysis

2.v. Risk Reporting and Monitoring

Risk reporting is a motivator for management to demonstrate progress with regard to risk-related action and is an effective way of enabling risk governance. Risk reporting is used to track the status of risks, activities / controls, mitigations, and losses. Risk reports expedite the flow of critical information and decision making.

Risks rarely remain static, so it is imperative that the risk owner arranges for a deliberate or formal review of risk trends to be performed. This may include an independent study of a key risk, whereby the circumstances, potential root causes, and key assumptions of a risk are reevaluated to understand where there has been change.

Theme #5	Risk Reporting and Monitoring
Summary Observations	<ul style="list-style-type: none"> ■ Process yet to be defined for regularly scheduled risk assessments. ■ Process yet to be defined for reporting and escalating newly identified risk and risk incidents to Executive Leadership Team and Board Audit Committee. ■ Escalation protocols based on the severity of the risk incident yet to be defined.
Suggested Improvements	<ul style="list-style-type: none"> ■ Establish a process for incorporating risk management activities into day to day operations, such as regular risk assessments and risk discussions in already established communication forums. ■ Establish a process including defined escalation thresholds based on the severity of the risk for reporting and escalating newly identified risks and risk incidents.
Anticipated Potential Benefits	<ul style="list-style-type: none"> ■ Employee engagement through regular workshops. ■ Employee confidence when reporting and escalating risks as a result of a predetermined process.



cutting through complexity

2. Leading Practice Analysis

vi.) Alignment with the City of Calgary's Integrated Risk Management Framework

2.vi. Alignment with the City of Calgary's Integrated Risk Management Framework

The Calgary Public Library has aligned its risk management framework with the City of Calgary's Risk Management Policy and Integrated Risk Management Framework. This includes mentorship by the City of Calgary in developing risk factors and in formalizing risk management processes.

Theme #6	Alignment with the City of Calgary's Integrated Risk Management Framework
Summary Observations	<ul style="list-style-type: none"> ■ The Calgary Public Library IRM framework and terminology adopted from the City of Calgary IRM. ■ The accountabilities and risk tolerances defined in the Calgary Public Library IRM align with those as outlined in the City of Calgary IRM. ■ The impact categories defined by the Calgary Public Library are unique to the strategic plan of The Library.
Suggested Improvements	<ul style="list-style-type: none"> ■ The City of Calgary IRM framework provides the basis for establishing a common risk terminology and Basic framework between the City of Calgary and the Calgary Public Library. Calgary Public Library can strengthen and customize the framework in the area of specific accountabilities, specific risk tolerances and specific risk thresholds that align with the unique strategies of The Library.
Anticipated Potential Benefits	<ul style="list-style-type: none"> ■ A custom framework that provides relevant risk management information to support the unique challenges and opportunities faced by CPL.



cutting through complexity

2. Leading Practice Analysis

vii.) Employee Engagement

Leading Practice Analysis

2.vii. Employee Engagement

Risk Management is the responsibility of all employees. Creating an awareness of the specific Risk Management processes, terminology and importance in achieving strategic goals is critical to success. Employee engagement and buy in the result of formal training, creating an open dialogue and risk management culture and through the implementation of a simple and effective plan.

Theme #7	Employee Engagement
Summary Observations	<ul style="list-style-type: none"> ■ Risk Management Training programs have not yet been developed and Training has not yet been rolled out to Calgary Public Library employees. ■ Executive Leadership Team is educated in Risk Assessment and has aligned its program to the City of Calgary's Integrated Risk Management Plan.
Suggested Improvements	<ul style="list-style-type: none"> ■ Develop formal Risk Management training programs that leverage the training and education materials developed by the City of Calgary. Focus on a common understanding of terminology, importance in achievement of strategic objectives and focus on employee engagement for success. ■ Participate in City of Calgary enterprise risk management training to further align employee understanding and common terminology. ■ More specific definition of risk impact categories, action plans and risk owners.
Anticipated Potential Benefits	<ul style="list-style-type: none"> ■ Employee engagement and accountability.



cutting through complexity

3. Next Steps

Questions to Facilitate a Risk Assessment Discussion

- How acceptable is the level of risk compared to Board tolerance limits?
- Who are the risk owners?
- What level of quality of information do we have about the risk?
- Could this risk affect stakeholders?
- What is the likely financial impact of a risk event?
- Which business objective would be affected by a risk event?
- How would a risk event impact on value creation?
- How does the risk impair performance?
- What is the risk's impact on strategy?
- Which business process generates the risk?
- What should we report to the Board and when?

3. Next Steps

Governance

- Define Board risk tolerances and impact thresholds for each Impact Category.
- Implement quarterly reporting to the Board as well as a process for immediate escalation of risks outside Board tolerances.
- Allocate appropriate resources that aligns with the level of risk management maturity desired.

Process

- Further delegate and assign risk ownership as required to Responsibility Unit managers.
- Define detailed Risk treatment plans with reference to specific mitigation policy, process or for highest risks.
- Implement a risk reporting tool for all enterprise level risks and Responsibility Unit risks.

People

- Perform risk management training of Responsibility Unit leaders and staff.
- Develop IRM user reference material for Responsibility Unit level risk management activities.
- Conduct an Executive Leadership Team high level risk assessment at the enterprise level followed by a functional risk assessment one department at a time.



cutting through complexity

4. Updated Observations

4. Updated Observations (March 12, 2014)

Governance

- The Executive Leadership Team will present the top enterprise risks and four revised risk impact categories to the Board Audit Committee on March 24th. The risks were identified through an Executive Leadership Team risk assessment and review of Board identified risks.
- Board to define desired risk maturity and compliance reporting requirements.

Process

- Executive Leadership Team has updated the IRM risk register as follows to align with KPMG recommendations:
 - Executive Leadership team has identified the top 4 risk categories and associated specific risks to each risk category.
 - Risk register has been updated to include both inherent and residual risk.
 - Specific risk mitigation action plans and owners have been identified.
 - Risk ownership has been delegated to specific Responsibility Units and Committees.



cutting through complexity

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2013 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.