Category:	**Global Planning & Accountability**
Approved By:	**Senior Administrative Team (SAT)**
Approval Date:	**June 28, 2011**
Effective Date:	**June 28, 2011**
Last Reviewed Date:	**February 17, 2017**
Policy Sponsor:	**Vice President Corporate Services and Chief Financial Officer**
Policy Administrator:	**Vice President People and Planning**

Risk Management Policy

Purpose

The college is committed to building increased awareness and a shared responsibility for risk management throughout the organization. The purpose of this policy is to clarify the college's underlying approach to risk management through an overall framework which includes principles, mandate and commitment, and process. Risk management will further assist the college in improving its management of uncertainty thereby helping to optimize the achievement of objectives.

Scope / Limits

Compliance with this policy extends to all members of the college community.

Definitions

Enterprise-wide risk management framework: A set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the institution.

- The foundations include the policy, objectives, mandate and commitment to manage risk.
- The organizational arrangements include plans, relationships, accountabilities, resources, processes, and activities.
- The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

Members of the College Community: Includes employees, students, contractors, volunteers, and others.

Employees are persons on the payroll of Lethbridge College
Students are persons enrolled at Lethbridge College
Contractors are persons working under a contract or agency relationship
Volunteers are persons who perform an unpaid service for the college
Others are members of the general public on campus for reasons other than outlined above

Risk: The effect of uncertainty on college goals and objectives.

- An effect is a deviation from the expected – positive and/or negative
- Objectives can have different perspectives (such as mission related, financial, health and safety, environmental, etc.).

Risk Management: Coordinated activities to advise and guide an organization with regard to risk.

Risk Management Advisory Committee (RMAC): A sub-committee set up by the College Leadership Council (CLC) that oversees and supports enterprise risk management activities at the institution. Members outside of the RMAC will be invited to participate on an as needed basis.

Policy Statements

1. The college will manage risk using a sustainable enterprise-wide risk management framework that is centered on the achievement of the college's strategic and operational goals and objectives. The system will support proactive, effective actions in the management of all aspects of uncertainty.

2. The management of risk is a shared responsibility.

3. The college's Risk Management Advisory Committee advises and guides the college on risk management issues.

4. The college, when appropriate and cost effective, will seek to share risk with third parties through the use of college policies, insurance policies, waivers and contracts.

5. The college will ensure that risks associated with emergency preparedness and business continuity are addressed in appropriate plans.

A: Policy Supports

Risk Management Framework (Appendix A)
Risk Management Advisory Committee Terms of Reference (Appendix B)
Emergency Management Plan Procedure (Appendix C)

B: Legislated References

C: Other References

CAN/CSA – ISO 31000 - 10

D: Related Policies

College Closures and Service Interruptions
Students Rights and Code of Conduct
Health and Safety
Information Technology Security
Board of Governors:
- EL-1 Treatment of Students
- EL-2 Treatment of Staff
- EL-5 Asset Protection
- EL-14 Environmental Stewardship

Parent Policy:	**Risk Management Policy**
Effective Date:	**June 28, 2011**
Last Reviewed Date:	**February 17, 2017**
Policy Sponsor:	**Vice President Corporate Services and Chief Financial Officer**
Administrative Responsibility:	**Vice President People and Planning**
Appendix A	

Lethbridge College
Risk Management Framework

Risk Management Framework

Table of Contents

Terms and Definitions

For the purposes of this document, the following definitions apply.

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

Control: Any action taken by management to reduce risk exposures to an acceptable level. Control Risk is the possibility of a control failing through poor design or ineffective operation.

Enterprise-wide Risk Management (ERM) framework: A set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the institution.

- The foundations include the policy, objectives, mandate and commitment to manage risk.
- The organizational arrangements include plans, relationships, accountabilities, resources, processes, and activities.
- The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

Establishing the context: Defining the external and internal environments to be taken into account when managing risk, and setting the scope and risk criteria for the Risk Management Policy.

Inability to mitigate: The inadequacy or lack of capability / tools available to fully or partially mitigate risks.

Level of risk: Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood to occur.

Likelihood: The chance of something happening.

Monitoring: Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.

Review: Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

Risk: The effect of uncertainty on college goals and objectives.

- An effect is a deviation from the expected – positive and/or negative
- Objectives can have different perspectives (such as mission related, financial, health and safety, environmental, etc.).

Risk analysis: The process to comprehend the nature of the risk and to determine the level of risk.

Risk appetite: The amount of risk exposure the college is willing to assume and can vary depending on the driver.

Risk assessment: Overall process of risk identification, risk analysis, and risk evaluation.

Risk capacity (tolerance): The maximum amount of risk the college can assume after all mitigating factors have been implemented and can vary depending on the driver (e.g. financial, reputation, etc.).

Risk clockspeed: The rate at which the information necessary to understand and manage a risk becomes available. Assessment of time available to anticipate and react to an occurrence.

Risk criteria: The terms of reference against which the significance of a risk is evaluated and rated (e.g. college objectives, internal and external context, laws, regulations etc.)

Risk evaluation: The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk identification: The process of finding, recognizing, and describing risks.

Risk management: Coordinated activities to advise and guide an organization with regard to risk.

Risk management advisory committee (RMAC): A sub-committee set up by the College Leadership Council (CLC) that oversees and supports enterprise risk management activities at the institution. Members outside of the RMAC will be invited to participate on an as needed basis.

Risk management maturity scale: The level of maturity of risk management ranging on a continuum from unaware, informal, formal, to embedded and optimized within an organization.

Risk management process (risk process): The systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.

Risk owner: The person or entity with the accountability and authority to manage a risk.

Risk profile: The description of any set of risks. May be a collection of Institutional risks or a set of risks associated with a single decision or activity.

- Risk Heat Map is a graphical presentation of a set of risks color coded to depict the severity of the risks.
- Risk Report is any type of report that is designed to provide risk information to stakeholders.

Risk register: A comprehensive list of risks identifying the risk description, potential consequence(s), likelihood and impact levels, risk score, risk clockspeed, inability to mitigate, risk trend, controls, risk owner, and risk action plan.

Risk treatment: The process to modify risk by:

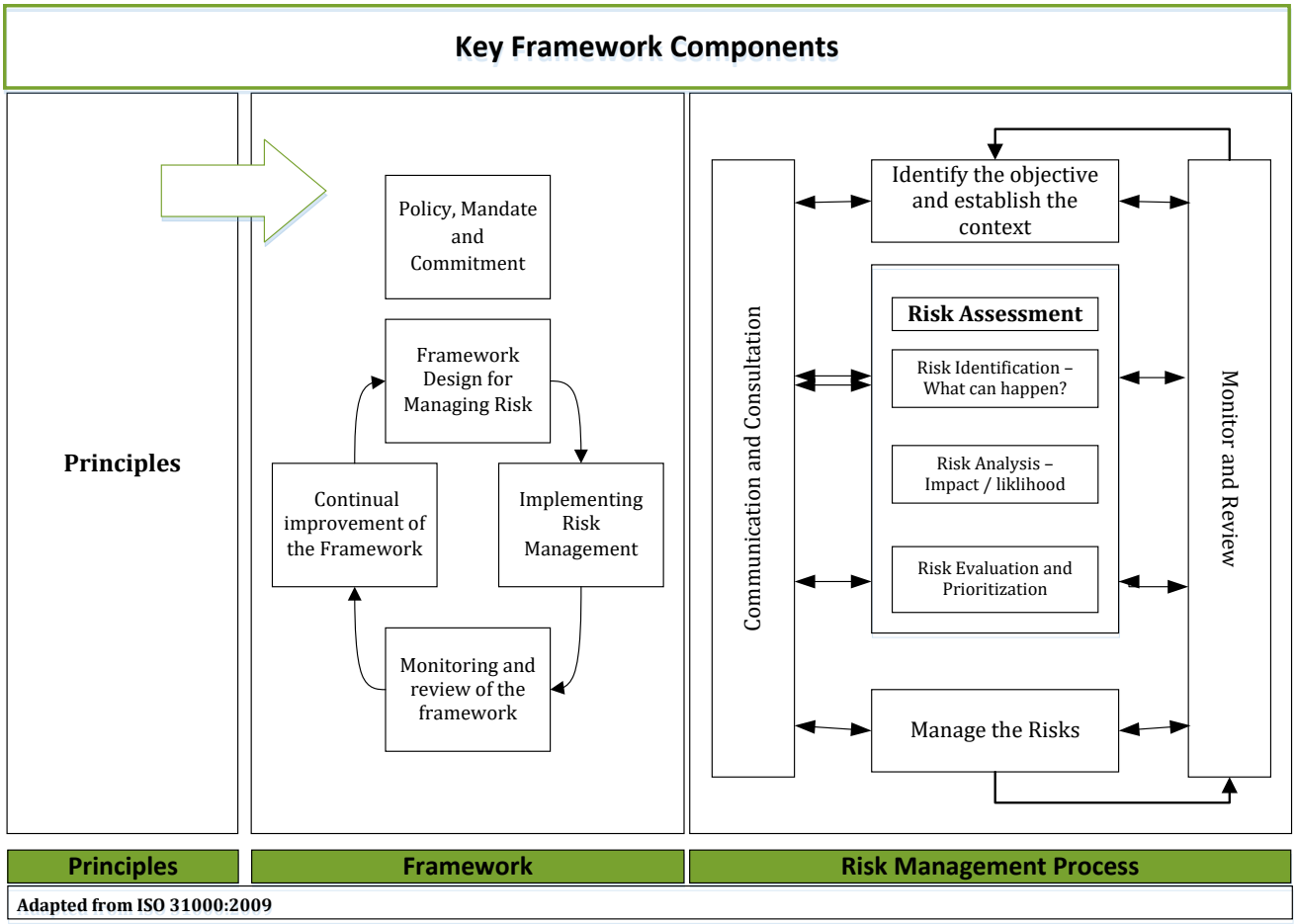
- not starting or stopping the activity
- removing the risk source
- changing the likelihood
- changing the consequences
- sharing the risk with other parties (contracts, insurance companies, etc.)
- taking or increasing risk in order to pursue an opportunity
- retaining the risk by informed decision

Stakeholder: Person or entity that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

Uncertainty: The state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

Risk Management Framework Objective

The Risk Management Framework sets out the general mandate and commitment, overview and guiding principles, roles and accountabilities, for managing, monitoring and improving risk management practice within Lethbridge College. This framework aligns with ISO 31000:2009, Risk



Management Principles and Guidelines, Mandate and Commitment.

Mandate and Commitment

Lethbridge College's College Leadership Council (CLC) is committed to fostering an environment that creates and preserves value. Risk-informed decision-making balanced with innovation is encouraged as the college explores and develops opportunities, set priorities, resolve issues and improves the way work is done to achieve business objectives.

All existing and new risk management activities in the college will align to this framework. Employees should incorporate risk management into governance, decision-making and key business and operational processes as set out in this framework.

Risk Management Principles

The college's Risk Management Framework is based on the following key principles. All employees are expected to apply these principles in their work.

- Risk management is an integral part of how we do business. All managers understand that management of risk is one of their core responsibilities.
- Risk management is aligned with the mission and values of the college and seeks to create or protect the college's value. Risk management adds value to our work by helping us to be dynamic and responsive to change, facilitating continuous learning and improving the way we work with each other and our partners as we serve our students. Our continuous application of the risk process safeguards stakeholder interests.
- Risk management is an integral part of key decision making at the college. Risk-informed decisions provide more robust information on the potential outcomes of decisions. The college strives to build decision making processes that will minimize potential losses, improve the management of existing uncertainty and the approach to new opportunities, thereby helping to maximize the achievement of the college's objectives.
- Risk management will be transparent, documented and inclusive. Risk information, policy and framework will be communicated to all affected internal and external stakeholders. The risk process will include consultation with stakeholders where appropriate.
- Risk management is tailored and responsive to the college's external and internal context; including objectives, priorities, public service ethics and values, cultural orientation to risk, college stakeholders, and the capacity to manage risk.

Overview and Risk Appetite

Overview

The college's Risk Management Framework requires that we understand uncertainties that may impact the achievement of objectives. Doing so ensures we are continuously focused on the most important risks and opportunities as we identify priorities and allocate resources.

Navigating uncertainty effectively will help to strengthen our performance in creating and preserving value by ensuring that the way we facilitate program and service delivery is innovative and responsible. Managing risk well ensures that we are proactive and resilient as we sense and respond to uncertainty. At the core of managing risk is the college's Statement of Risk Appetite which strives to reduce unwanted or unexpected outcomes and engender the trust and confidence of stakeholders.

The college's risk appetite is further expressed in terms of a continuum to guide employees in their actions and ability to accept and manage risks. Risk appetite also forms the basis for the college's Risk Rating Criteria identified in Schedule 1 - Risk Management Process and Tools.

Risk Capacity/Tolerance is the maximum amount of risk the college can assume after all mitigating actions have been implemented and varies depending on the driver (e.g. financial, reputation, etc.). Risk appetite is "How willing the college is to accept the mitigated risk related to key value drivers". Risk appetite is set somewhere within the capacity/tolerance limits. The following is a guide to the college's risk appetite and tolerance within each value driver.
The Statement of Risk Appetite is fundamental to risk management and will be reviewed annually within the context of the current operating environment. Adjustments will be made as required.

Lethbridge College Statement of Risk Appetite
Lethbridge college will continuously seek out innovation in the way we deliver our mandate, while ensuring that all decisions we make are informed by an understanding of the uncertainties we face as an organization. We have a low risk tolerance for any risks that compromise our academic integrity, the health and safety of our students and employees, our reputation and brand, or risks that may impact our ability to be regarded by our stakeholders as trustworthy and credible. We will continuously seek out those opportunities that can best build on our strengths and core values.

Risk Apetite			
Innovation Risk	Reputation Risk	Health and Safety Risk	People Risk
3	2	2	2
We will strive for innovation and excellence in our operations.	The college will continue to maintain its high standards of conduct and academic integrity (excellence in teaching, leadership and research and respect for intellectual property). Ethics and critical thinking will be required of all employees and students. Student recruitment, admission and retention practices will support student success. We will strive to provide quality learning opportunities and life experiences.	The college is committed to providing and maintaining a safe and healthy work and learning environment, in accordance with industry standards and in compliance with legislative requirements.	We will continue to hire and retain employees who meet high standards in ethics, leadership, and professional abilities. We will strive to have succession plans in place for key positions.
Relationships Risk	Financial and Physical Resources Risk	Information Management Risk	
3	2	2	
The college will create and maintain positive relationships with external stakeholders (e.g. business, industry, funders, donors, government) in pursuit of the college's mandate.	We will maintain high stewardship standards for our financial and physical resources. We will continue to ensure financial commitments do not exceed available resources and that college activities do not cause undue exposure. Capital budgets will be prioritized in the area of deferred maintenance and renewal of learning and operational resources.	The college will maintain security, integrity and availability of information management systems as it pertains to core processes and activities including, students, financial management, human resources, intellectual property, and key performance indicators.	

Assessment	Description
Very High Risk Appetite 5	The college **accepts opportunities that have an inherent very high risk** that may result in damage to our academic and/or general reputation, financial loss or exposure to liability, major breakdown in information system or information integrity, significant incident(s) of regulatory non-compliance, potential risk of injury to employees and students.
High Risk Appetite 4	The college **is willing to accept risks** that may result in damage to our academic and/or general reputation, financial loss or exposure to liability, major breakdown in information system or information integrity, significant incident(s) of regulatory non-compliance, potential risk of injury to employees and students.
Moderate Risk Appetite 3	The college **is willing to accept some risks in certain circumstances** that may result in damage to our academic and/or general reputation, financial loss or exposure to liability, major breakdown in information system or information integrity, significant incident(s) of regulatory non-compliance, potential risk of injury to employees and students.
Low Risk Appetite 2	The college **is not willing to accept risks in most circumstances** that may result in damage to our academic and/or general reputation, financial loss or exposure to liability, major breakdown in information system or information integrity, significant incident(s) of regulatory non-compliance, potential risk of injury to employees and students.
Very low Risk Appetite 1	The college **is not willing to accept risks under any circumstances** that may result in damage to our academic and/or general reputation, financial loss or exposure to liability, major breakdown in information system or information integrity, significant incident(s) of regulatory non-compliance, potential risk of injury to employees and students.

Roles and Accountabilities

Finance, Audit and Risk Committee (FAR)

- endorsement and monitoring of the effectiveness of the Risk Management Policy and Framework

President and Chief Executive Officer

- ensures effective risk management performance within this Risk Management Framework

College Leadership Council (CLC)

- responsible for approving the Risk Management Policy
- overseeing and supporting the use of the Risk Management Framework for all business processes and key decision making within the college

Executive Director People and Planning

- administrative responsibility for supporting effective risk management
- enabling the practical implementation of this Risk Management Framework

Employee with Delegated Authority for Decision Making

- ensuring the Risk Management Policy and Framework is applied to all key decisions and business processes and supporting guidance, tools and training,
- participating in the development, review and update of the Institutional and departmental Risk Registers,
- addressing, monitoring and reporting on the status of key risks which they are accountable, and
- fostering a risk aware culture.

Vice President Corporate Services and Chief Financial Officer

- ensuring an effective Risk Management Policy and Framework is in place
- chair of Risk Management Advisory Committee
- reports to FAR on risk management

Risk Management Advisory Committee (RMAC)

- recommend the Risk Management Policy to CLC
- approve the Risk Management Framework
- assist the College in identifying and quantifying fundamental risks affecting the College, and ensuring that appropriate arrangements are in place to manage those risks
- at least annually do a full review of significant risks and their controls
- embed a risk management culture into major decisions through risk education, high level controls and risk process
- at least annually evaluate risk management processes and the reporting of key risks
- identifying risks and controls that should be included in the reporting and communication

All Employees

- the proactive engagement of internal stakeholders (e.g. Managers/Supervisors, Human Resources, Finance, Risk Management, etc) in identifying, documenting and escalating risks and opportunities using appropriate business processes
- being aware of the top risks affecting your business area
- applying Lethbridge College risk management resources (guidance, tools and training)

Applying the Risk Management Framework

The Risk Management Framework is applied to all key decisions and business processes as we plan, execute, measure, monitor and report on our work.

Strategic risks are explicitly identified through planning systems, periodic strategic assessments, and/or as new initiatives and issues arise and are appropriately managed. Operational and project risks are managed as an ongoing and integral part at all levels of the Institution including program and project management, service delivery levels, review and reporting activities.

What We Do	Our Key Business Processes	Risk Management Expectation	Guidance and Tools To Help
Planning our work	➢ Organizational planning/design ➢ Strategic planning ➢ Operational planning ➢ Policy development ➢ Program planning ➢ Project/initiative planning	➢ Consider how our key risks will be impacted ➢ Identify new or changed risks and opportunities using appropriate consultation with stakeholders	➢ Risk Management Framework ➢ Risk Process and Risk Criteria ➢ Risk Register ➢ Risk management training
Executing our work	➢ Key decisions that affect resource allocation and work priorities within the college ➢ Change management	➢ Consider how our key risks will be impacted by the decision ➢ Apply the risk process	➢ Risk Management Framework ➢ Risk Process and Risk Criteria ➢ Risk Register
Measuring, monitoring and reporting on our work	➢ Measuring and tracking performance	➢ Track, measure and report on progress made in addressing key risks ➢ Communicate key risks to stakeholders	➢ Risk Management Framework ➢ Risk Process and Risk Criteria ➢ Risk Register ➢ Risk Report/Profile
Improving the way we work	➢ Independent assessments ➢ Process improvement initiatives	➢ Capture, share and apply best practices and lessons learned in managing risk ➢ Identify new or changed risks and opportunities in relation to our key risks	➢ Risk Management Framework ➢ Risk Register

Quality Assurance and Control

The Risk Management Framework guidance, tools and training will be continuously improved through feedback from stakeholders, in an effort to ensure the risk management approach is helpful, valuable, and effective.

Continual learning and improvement is a key means of attaining excellence in our business processes and renewal. As our organization and workforce continues to change, risk management capacity will advance along the risk management maturity continuum.

Both formal and informal mechanisms will be used to identify, capture and share better practices in managing risk across the institution.

Risk Management Monitoring and Reporting

Reporting on risk management will be integrated into existing college performance, communication and governance systems.

Stakeholder Group	Risk Information	Timing	Type
Finance, Audit and Risk Committee (FAR)	High level risk report – actions planned/ taken and quantifiable change	As determined by the FAR Committee	Report
	Risk Policy and Framework – annual review (ongoing effectiveness – KPI's)	Annual	Report
	Strategic risk assessment	Annual	Comprehensive Institutional Plan (CIP) Annual Report
College Leadership Council	High level risk report – key risks and opportunities – actions planned/taken	Quarterly	As part of quarterly reporting
	Risk Policy and Framework – annual review (ongoing effectiveness – KPI's)	Annual	Report
	Risk assessment of key decision-making	As required	Proposals, business cases, RFDs ,etc.

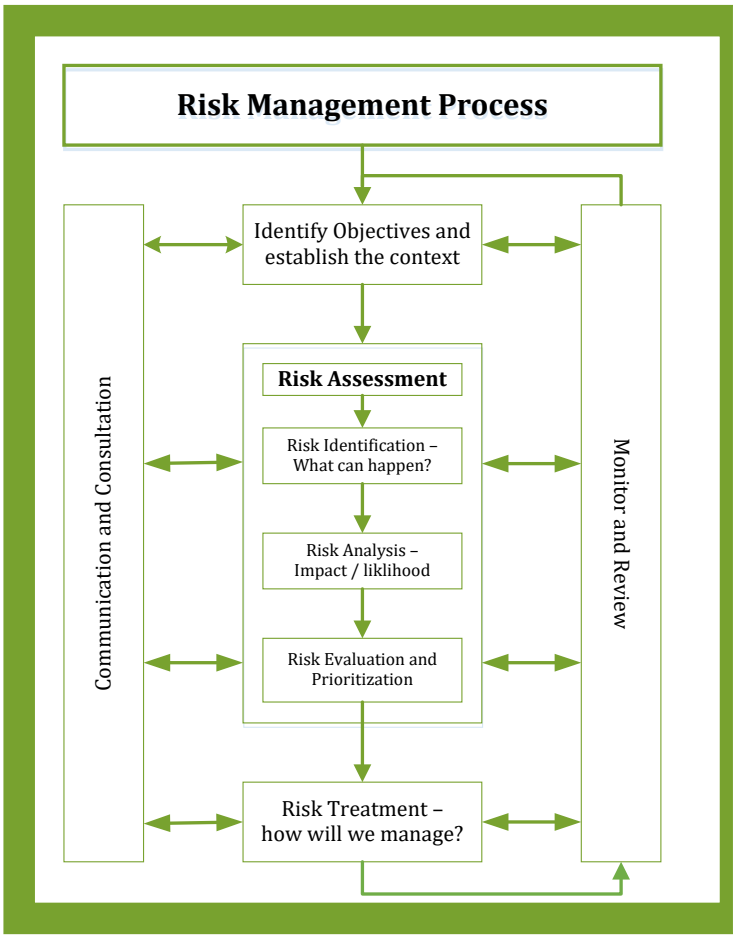
The effectiveness of the Risk Management Framework will be tracked and reported on annually. The key performance measures used to track performance are:

1. The Board (FAR Committee) and the College Leadership Council level of confidence and understanding regarding risk have been elevated.
2. Improvement in the severity of risks in the Risk Register.

Schedule 1 - Risk Management Process and Tools

Risk Management Process

Risk management will be integrated into and/or enhanced in the college's key processes. Most existing processes will have some degree of risk management. The college's approach to risk management will build on existing key processes, evaluating each process to identify risk management strengths and opportunities for enhancement. The following common Risk Process forms the basis for evaluating and enhancing risk management with college processes.



Risk Assessment Metrics Tools

Once risks are identified, they are evaluated on a two dimensional Risk Profile matrix using a qualitative rating of the likelihood of the event occurring and the scale of the possible consequences. When risks have been identified, they are analyzed by combining the consequences and likelihood to produce a level of risk. This form of evaluation provides a good graphical representation of how serious the risk is or where it lies within a group of risks. The risk analysis provides information critical to determining what risks need to be treated and what risks are accepted. Scores are linked to the college's risk tolerance/appetite – very high, high, moderate, low and zero. The Risk Profile matrix should be used as a guide for setting priorities in managing risk.

The college will use the following measurement tools (metrics) in evaluating risk. Examples in the consequence /impact considerations should be used as a guide in evaluating the level.

Threats Consequence/Impact Considerations					
Impact Category **Impact Level**	**Academic/Ancillary and Business Development**	**Financial** **Legal Exposure**	**Brand**	**People**	**Operational**
Catastrophic 5	Total cessation affecting any 1 key or several educational/ancillary activities over 4 weeks; with continued disruptions over several weeks; Major and/or long term effect on program quality ; Major long term threat from competition; Major shift in strategy	Extreme environmental damage and/or clean-up costs; Loss of assets/ costs/ litigation >$10M; funding/ revenues >$10M Legitimate litigation <$2M	Long lasting damage to reputation; Ongoing negative nation-wide news coverage; Major long-term and/or widespread impact on external stakeholder relationships; Significant inconsistencies with mandate; Extreme breach in information management and/or privacy.	Multiple fatalities and/or injuries resulting in permanent impairment or disability of student(s), employee(s), or third parties; Loss of (2+) key (defined) Senior Leaders, faculty, operational personnel; Significant impact on staff or student welfare.	Extreme and widespread service disruption as a result of one or more major system failures (over 4 weeks with continued disruptions over several weeks); Major failure in project delivery expectations.
Major 4	Total cessation affecting any 1 or more key activities between 14-28 days; with continued disruptions over several weeks; Major long term effect on program quality or access; Significant and/or long term threat from competition; Some shift in strategy	Loss of assets/ replacement costs $2.5M and <$10M; funding/ revenues $2.5M and <$10M; Legitimate litigation against LC $500,000 and <$2M; Major environmental damage and/or clean-up costs.	Measurable damage to reputation; Negative front-page "Globe and Mail" type coverage. Negative audit or student outcome rating. Some inconsistencies with mandate; Significant and long-term impact on external stakeholder relationships; Major breach in information management and/or privacy.	Single fatality and/or injury resulting in long-term care of student(s), employee(s),or third parties; Long-term, unscheduled, absence of key employee(s); Serious impact on staff or student welfare.	Major service disruptions affecting any 1 or more key activities between 14-28 days; with continued disruptions over several weeks.
Significant 3	Total cessation affecting any 1(or key, identified) activity between 5-14 days; with continued disruptions over several days; Minimal impact on program quality; Some impact from competitors	Loss of assets/costs/ $100,000 and <$2.5M; funding or revenues $100,000 and <$2.5M; Legitimate litigation against LC $100,000 and <500,000	Measurable damage to reputation (localized); Negative national news-media coverage; Negative audit or student outcome rating; Minimal impact on stakeholder relationships; Significant breach in information management and/or privacy.	Major injury resulting in prolonged off-site medical attentions to student(s), employee(s),or third parties; Undefined (longer) absence(s) of any key employee(s); Moderate impact on staff or student welfare	Major service disruptions affecting any 1or more key activities between 5-14 days; with continued disruptions over several weeks
Moderate 2	Minimal impact on quality or access; Some impact to efficiency or effectiveness of programs	Loss of assets/replacement costs $5,000 and <$100,000; funding or revenues $25,000 and <$100,000; Legitimate litigation against LC $5,000 and <$100,000; Minor cost overruns	Minor setback in trust (internal); Some negative regional or provincial news-media coverage; Minimal impact on student and/or community satisfaction; Minimal breach in information management and/or privacy.	Minor injury requiring off-site medical attention to students, employee(s),or third parties; Short-term absence(s) of vital staff	Normal administrative difficulty; Minor unscheduled activity or service disruption (3-5 days) and continued disruptions over several days
Minor 1	Little or no impact to program quality or access	Loss of assets/replacement costs <$5,000; funding or revenues <$25,000); Legitimate litigation against LC <$5,000	No/minor impact on trust (internal); No/minor external or media attention (local news media coverage); Little or no impact on student and/or community satisfaction	Minor injury requiring on-site medical attention to students, employee(s),or third parties	Very low effects; Minor unscheduled activity or service disruption (<3 days); Very minor overruns; Minor delays in replacing staff; Very minor loss of data

Opportunity Consequence/Impact Considerations			
Impact Category **Impact Level**	**Financial**	**Operational**	Brand
Major **5**	Model workplace and target employer of choice; Sustainable strategic targets met; Legally aware and compliant employee decisions ; Budget optimized; Effective asset management strategy	Ongoing and effective knowledge management; Reliable, continuously available, high quality services; Sustained achievement of operational objectives; Key projects completed successfully	Significant, sustained trust from stakeholders; Significant employee trust and credibility; Significant and consistently positive media reports
Significant 3	Productive, motivated and healthy workplace; Disclosure of confidential information does not occur; Some sustainable strategic targets met; Budget met	Some operational objectives exceeded; Significant improvement in projects: 1-2 months; or important functionality; Key institutional knowledge in most areas of the college	Clear evidence of trust from stakeholders; Clear evidence of employee trust; Regarded as an employer of choice; Rare criticism by stakeholders
Minor 1	Improving productive, motivated and healthy workplace; Comply with policy and procedures	Students and community members are aware of and can access many of our programs/services; Changes to minor projects	Some favourable media or public attention; Some favourable observations by stakeholders

Likelihood Measure The probability of the risk event occurring.			
Score	**Likelihood**	**Description**	**Frequency**
5	Almost Certain	**The event is expected to occur in most circumstances** High Frequency. Necessary factors that could cause loss are always present. Controls are needed at all times.	>95% chance of occurrence
4	Likely	**The event will probably occur in most circumstances** Medium – High Frequency. Necessary factors that could cause loss are always present. Controls and procedures are generally in place.	60% to 95% chance of occurrence
3	Possible	**The event should occur at some time** Necessary factors that could cause loss are present. Event is likely to occur at some point in the operational lifespan. Controls are in place; however, a single control failure would result in the loss.	30% to 59% chance of occurrence
2	Unlikely	**The event could occur at some time** Necessary factors may be present but the event is unlikely to occur. Controls are in place; however, multiple control failures would result in the loss.	5% to 29% chance of occurrence
1	Rare	**May occur in exceptional circumstances** Necessary factors not normally present. Event is so unlikely that it can be assumed the occurrence may never occur.	>5% chance of occurrence

Risk Clockspeed	
Assessment	**Description -** The rate at which the information necessary to understand and manage a risk becomes available. It is the time available to anticipate and react to an occurrence.
Very Fast	Information necessary to manage the risk will emerge in real time leaving insufficient time for rational cognitive consideration.
Fast	Information necessary to manage the risk will emerge in, or close to real time leaving little time for rational cognitive consideration.
Moderate	Information necessary to manage the risk will emerge in real time. This information will be available allowing the use of rational cognitive thought to forward manage the risk.
Slow	Information is available currently allowing the use of rational cognitive thought to forward manage the risk.
Very Slow	Good quality risk mitigation information is available currently allowing the use of rational cognitive thought to forward manage the risk.

Inability to Mitigate	
Assessment	**Description** - Inadequacy or lack of capability/tools available to fully or partially mitigate risks
High	Capability/tools do not exist to mitigate risks.
Moderate	Capability/tools exist to partially mitigate risks.
Low	Capability/tools exist to adequately mitigate risks.

Control Evaluation (controls in place)				
Uncontrollable	**Weak**	**Moderate**	**Strong**	**Very Strong**
- Outside the control of LC in respect of likelihood - LC has the ability to manage the impact, if appropriate weighting relating to the severity is applied	-While controls are in place, they are insufficient to prevent or mitigate this scenario - Any singular impact may also affect other activities and/or operations within LC - Near misses or actual losses may be recorded; however, they are not aggregated or reviewed for trending purposes	- Controls in place provide LC a reasonable certainty of control, although they may not afford management knowledge of all potential exposures or scenarios - Scenarios are being identified and disseminated across the organization but not to all levels of management	- Critical, but not all key risks, are known to LC - Controls in place provide LC a higher level of control, although not to all or every potential exposures or risk scenario. - LC's critical, known risks are disseminated across the organization but not to all levels of management	- Significant attention is paid to the identified scenarios - LC has undertaken all feasible economic investment to mitigate the scenario - LC maintains an ongoing monitoring system, which is actively reviewed and linked with overall goals, objectives and individual and/or activity performance

Risk Profile Matrix (Threats) – Linked to Risk Tolerance/Appetite

Catastrophic (5)	**5** **Moderate 3** Manage and monitor	**10** **High 4** Considerable management required	**15** **Very High 5** Must manage and monitor	**20** **Very High 5** Extensive management required	**25** **Very High 5** Extensive management required
Major (4)	**4** **Low 2** Accept but monitor	**8** **Moderate 3** Manage and monitor	**12** **High 4** Considerable management required	**16** **Very High 5** Must manage and monitor	**20** **Very High 5** Extensive management required
Significant (3)	**3** **Very low 1** Accept but monitor	**6** **Low 2** Accept but monitor	**9** **Moderate 3** Manage and monitor	**12** **High 4** Considerable management required	**15** **Very High 5** Must manage and monitor
Moderate (2)	**2** **Very low 1** Accept risks	**4** **Very low 1** Accept risks	**6** **Low 2** Accept but monitor	**8** **Moderate 3** Manage and monitor	**10** **High 4** Considerable management and monitor
Minor (1)	**1** **Very low 1** Accept **risks**	**2** **Very low 1** Accept Risks	**3** **Very low 1** Accept risks	**4** **Low 2** Accept but monitor	**5** **Moderate 3** Manage and monitor
	Rare (1)	**Unlikely (2)**	**Possible (3)**	**Likely (4)**	**Almost Certain (5)**

Risk Profile Matrix (Opportunities)

Major (5)	**25** **Optimize** **Opportunity**	**20** **Optimize** **Opportunity**	**15** **Maybe worth considering**	**10**	**5**
Moderate (3)	**15** **Optimize** **Opportunity**	**12** **Consider versus effort**	**9**	**6**	**3**
Minor (1)	**5** **Consider versus effort**	**4**	**3**	**2**	**1**
	Almost Certain (5)	**Likely (4)**	**Possible (3)**	**Unlikely (2)**	**Rare(1)**

Risk Management Forms:

- Risk Register
- Risk Reports

Parent Policy:	**Risk Management**
Effective Date:	**October 8, 2014**
Last Reviewed Date:	**February 17, 2017**
Policy Sponsor:	**Vice President Corporate Services and Chief Financial Officer**
Administrative Responsibility:	**Vice President People and Planning**
Appendix B	

Risk Management Advisory Committee
Terms of Reference

Committee Purpose/Mandate:
The Risk Management Committee (RMAC) is an operational committee set up by the College Leadership Council (CLC) to oversee and provide direction on matters of risk management at the college. The committee reports to CLC.

The purpose of college-wide risk management, which includes a Risk Management Policy and supporting framework, is to integrate the process for managing risk into the overall governance, strategy and planning, management and reporting processes of the college.

Committee Responsibilities:
- Oversee the college-wide risk management process on behalf of CLC
    - Recommend Risk Management Policy and approve the Framework.
    - Recommend an appropriate risk appetite /tolerance for the college.
    - Assist in the identification and quantification of fundamental risks affecting the college, and ensure that follow-up arrangements are in place to mitigate those risks.
    - At least annually do a full review of the Risk Register.
    - Inform CLC on risks and controls that need further assessment.
    - Ensure that risks associated with emergency preparedness and business continuity are addressed in appropriate plans.
    - Help embed a risk management culture into major decisions through risk education, high level controls and procedures.
    - Consider major decisions affecting the college's risk profile or exposure.
    - Identify risks and controls that should be included in the reporting and communication.
- The committee will report as necessary to CLC and any other committees or bodies as deemed appropriate.

Membership:
Membership should be cross functional and include the following:
- Vice President Corporate Services and Chief Financial Officer
- Vice President People and Planning
- Director Financial Services
- Director Information Technology Services
- Director Facilities Management
- Dean Student Affairs
- Registrar

- Associate Vice President Research, Innovation and Entrepreneurship
- Deans (2) rotate annually
- Security Team Lead
- Occupational Health and Safety Team Lead
- Manager Institutional Compliance

In addition, the following will be resources to the committee and will be non-voting:

- Other Senior Administrators (as required)

Members will be appointed by CLC.

Meetings:

- The committee shall meet quarterly.
- Ad-hoc meetings shall be held as required.

Decision-making:

1. Full consensus (everyone is on board with the decision).
2. Consensus (everyone is on board or can live with the decision).
   Decision Moves Forward.
3. Conscientious objection (one or more members object and cannot live with the decision).
   Chair and relevant member(s) meet offline and return to the committee with a workable solution.

Responsibilities:

Chair:

- Committee will be chaired by the Vice President Corporate Services and Chief Financial Officer or designate.
- Agenda will be coordinated by the chair with input from members.
- Agendas and handouts will be distributed electronically before the meeting.
- Action items will be recorded and distributed in the next meeting package.

Communications Responsibility:

- The committee will be responsible for disseminating information as required to the Executive Leadership Team (ELT), CLC and the operations team.

Parent Policy:	**Risk Management**
Effective Date:	**June 28, 2011**
Last Reviewed Date:	**February 17, 2017**
Policy Sponsor:	**Vice President Corporate Services and Chief Financial Officer**
Administrative Responsibility:	**Vice President People and Planning**
Appendix C	

Emergency Management Plan Procedure

Purpose

Lethbridge College is potentially subject to natural and man-made incidents that could threaten the members of the college community, its resources and the achievement of goals and objectives. Emergency planning sets forth the basic information required to respond to the occurrence of a natural or human induced emergency or disaster. The following procedure highlights the main aspects of the Lethbridge College Emergency Management Plan (EMP).

Definitions

Alberta Emergency Management Agency (AEMA): An agency that leads the co-ordination, collaboration and co-operation of all organizations in Alberta involved in the prevention, preparedness and response to disasters and emergencies. This ensures the delivery of vital services during a crisis. These organizations include government, industry, municipalities, and first responders. See www.aema.alberta.ca for more information.

Disaster: An event resulting in serious harm to the safety, health, or welfare of people or in widespread damage to property (AEMA).

Emergency: a present or imminent event that requires prompt coordination of action or special regulation of persons or property to protect the health, safety or welfare of people or to limit damage to property (AEMA).

Emergency Preparedness: The planning, exercising, and education necessary to achieve a state of readiness for disasters and emergencies (AEMA).

Incident: An occurrence, either caused by humans or by natural phenomena that requires a response to prevent or minimize loss of life or damage to property and/or the environment (AEMA).

Plan Overview

The Emergency Management Plan (EMP) is:

- a comprehensive plan and can be used for all hazards
- a basic framework for emergency preparedness and incident management

- in alignment with external agencies including the City of Lethbridge Emergency Services and the Alberta Emergency Management Agency (AEMA)

The EMP does not address the specific needs of a department in an extended emergency. Departments and centres are required to develop their own Business Continuity Plans (BCP).

The EMP objectives are to:

- be prepared for emergencies
- minimize the effect on student learning
- protect people from further injury
- protect assets and informational resources from further damage
- provide for the continuation of critical functions and return to normal operations

Authority and Succession

The President and CEO has ultimate authority. If the President/CEO or designate is not available, the line of succession is:

- senior responsible person (next most senior level i.e. ELT, CLC, Management.)

The Emergency Management Plan delegates authority to the Incident Command Team (ICT) led by the Incident Commander to declare an emergency and respond to, manage and control all aspects of that emergency situation in conjunction with emergency response agencies.

Concept of Operations

The Emergency Management Plan operates under the following concepts and assumptions.

- It is structured using the nationally recognized Incident Command System (ICS).
- It utilizes a Management by Objectives (MBO) approach.
- Resources are assigned on a ramp-up, ramp-down basis as required.
- Emergency service organizations may take a lead role depending on the nature of the incident.
- Operations progress through the following priority responses:
  1. protection of life safety
  2. crisis management and mitigation of damages
  3. property preservation and restoration of college operations.
- The Crisis Communications Plan forms part of this plan and includes emergency notifications.

Organizational Structure

The plan is managed using the following two teams:

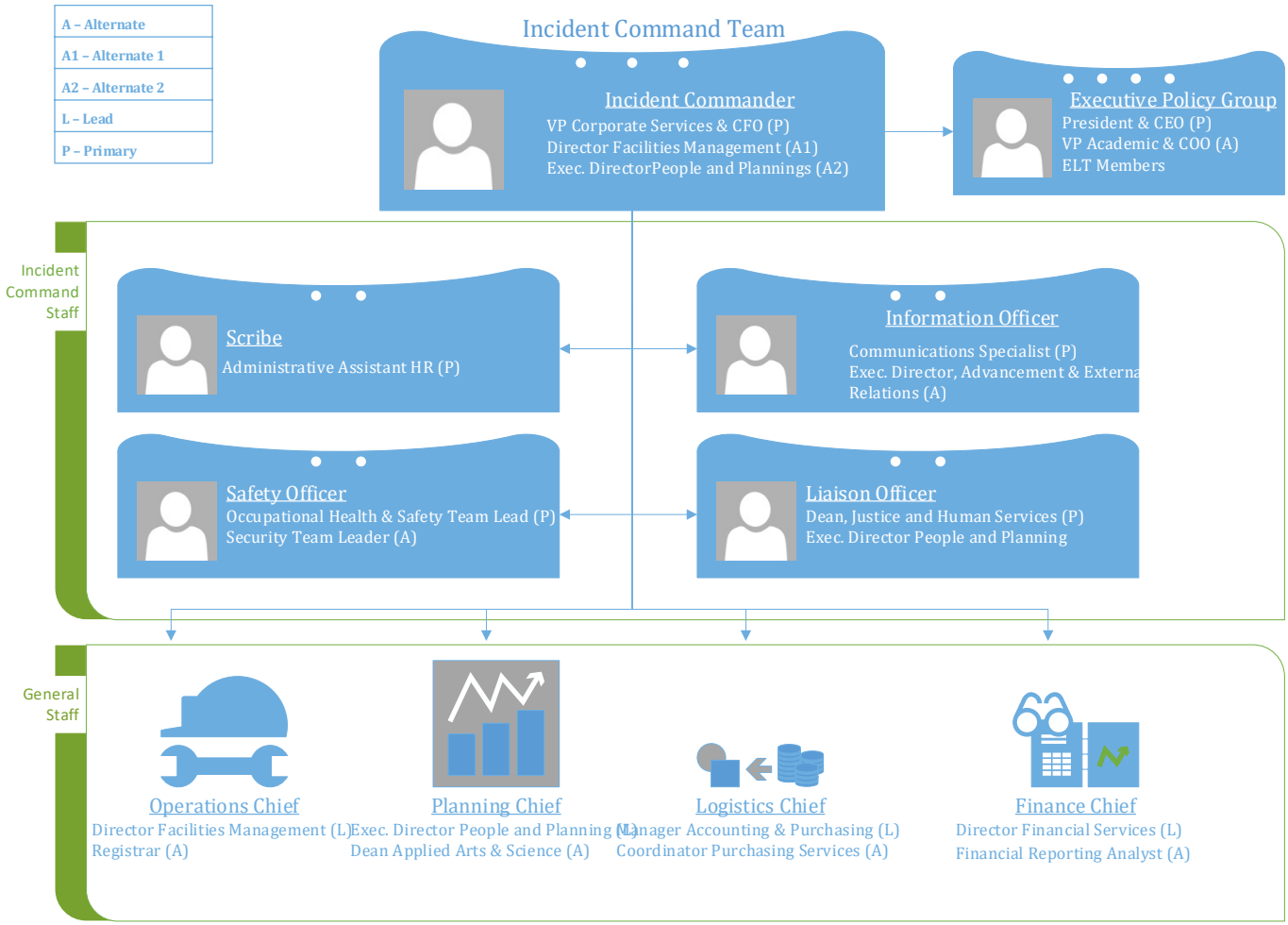
The Executive Policy Group (EPG):

- is led by the President and CEO or designate
- provides executive level information and support and assumes overall coordination of the external community response

The Incident Command Team (ICT):

- is led by Incident Commander
- provides incident management and return to normal operations

Incident Command Team - Roles and Responsibilities



The Incident Commander:

- reports to the President/CEO or designate
- has delegated authority to provide overall leadership for the incident response
- delegates authority to others as the incident complexity dictates
- is the only position that is **always** staffed in ICS events and serves in all functional roles until they are delegated
- is responsible for:
  - incident safety
  - providing Information to internal and external stakeholders
  - establishing and maintaining liaison with public service agencies participating in the incident
  - establishing incident objectives
  - the development and implementation of the incident action plan

The Information Officer:

- develops and releases information regarding the incident to the public, incident personnel, internal stakeholders, and other appropriate agencies and personnel

The Safety Officer:

- helps prevent injuries from occurring – can override the Incident Commander if safety is compromised

The Liaison Officer:

- serves as the primary contact for responding agencies (law enforcement, fire, etc.)

The Operations Section Chief:

- directs the Operations Section Staff
- participates in the development of the Incident Action Plan (IAP)
- manages all tactical operations of the incident and directs the implementation of the IAP to accomplish objectives

The Logistics Section Chief:

- directs the Logistics Section Staff
- participates in the development of the IAP
- sources and supplies necessary resources and services required to support incident activities including any additional staffing

The Planning Section Chief:

- directs the Planning Section Staff
- collects, evaluates and disseminates information needed to measure size, scope and seriousness of the incident
- looks beyond the current and next operational period and anticipates potential problems or events
- anticipates and arranges for specialized staffing (technical experts etc.)

The Finance Section Chief:

- directs the Finance Section staff
- tracks incident costs including employee time records; files claims for loss and compensation

The Scribe:

- ensures documentation of all actions, decisions, critical communications and requests are recorded and preserved

All of the above positions report directly to the Incident Commander. All staff functions may have additional supporting members as required to meet the objectives and complexity of the incident.

Threat Severity Levels and Actions

Threat Severity Levels and Actions				
	Minor (Prov. Level 5)	**Moderate (Prov. Level 4)**	**Severe (Prov. Level 3)**	**Catastrophic (Prov. Level 2,1)**
Scope	Limited – is or may affect one or more customers/ employees; handled by appropriate administration	May impact one or more college facilities, students or employees. Potential to expand and requires additional resources	Employees and customers are in danger and/or facilities are at risk. Coordination with outside agencies may be required	Large disaster impacts well beyond the college. Multiple jurisdictions (i.e. Slave Lake); vast resources
Time Frame	Short (<4hrs)	May extend beyond an operational period (>4 hrs.)	May extend into multiple operational periods (days, weeks, months)	Multiple operational periods
Response	IC – notified and may take action to put teams on standby	EPG briefed; IC and ICT required functions activated, others may be on standby	Coordination with outside agencies may be required. EPG, IC, and ICT functions as required	Local, regional, provincial response; EPG, ICT – as required
Document-ation	Verbal Incident Action Plan (IAP); written Incident Briefing form (ICS201)	Verbal Incident Action Plan (IAP); written Incident Briefing form (ICS201)	Written IAP and Briefing Form for each operational period	Written IAP and Briefing Form for each operational period
Follow-up	Debrief – lessons learned	Debrief – lessons learned	Debrief – lessons learned	Debrief – lessons learned

Crisis Communications

Modes of Communication
Depending on the event, multiple modes of communication may be utilized. Some may be more successful than others.

- **Primary** - Lethbridge College Website "News and Events page"
- **Secondary** – email, social media, radio/TV, college monitors, posters/ bulletins

The initial response to any level of security threat

- The Information Officer will issue a holding statement sent via **email** to internal stakeholders (employees, students and security) acknowledging the event.

- The message will convey that as details emerge more information will be forthcoming in a timely fashion.
- If immediate action is needed, direction will be sent via **email** to all staff and students.
- This information will then be posted to the **main college website** under the **News & Events** section which will then automatically transfer to the **portal**.
- After the immediate notification to internal stakeholders, the information will be dispersed to **external stakeholders** (media, board of governors, government) as seen fit by the Incident Command Team.

Ongoing information

- The Information Officer will send regular updates to stakeholders.
- Each message will be followed with an update of the same information to the web with a display of the time posted.
- The timeliness of these updates will be dependent on the situation and the speed at which it unfolds.

Social media

- Social media will be integrated into the dissemination of information based on the event itself.
  - The Information Officer and the communication team have the ability to take control of all college-related social media accounts. Depending on the severity of the event, all Facebook pages and Twitter accounts will be updated to display an emergency response graphic.
  - Ongoing updates and instructions will also be posted on these pages.
  - Accounts will be continuously monitored for questions and other communications.
- At any given time, stakeholders may also follow the college's Twitter feed for updates without having to have a Twitter account. Simply click the feed that is displayed on the News & Events page on the lethbridgecollege.ca website.

Emergency Operations Centre (EOC)

EOC – A centralized location in which emergency staff will gather, check in, and assume their emergency response roles. The location of the EOC is based on the size, scope, and seriousness of the incident. The main activities performed within the EOC may range from a centralized meeting place to prepare for and/or manage a minor incident to a 24/7 operation for managing severe incidents.

EOC Locations

- Primary 1– Executive Boardroom
- Alternate 2 – On-campus unaffected facility with emergency power
- Alternate 3 – **Off-campus** Facility

Command and Transfer of Command

All activities of the EOC are under the direction of the Incident Commander (IC). Formal transfer of command protocol must be followed when there is a change in the IC or a supervisory position. Protocol calls for a face-to-face meeting in which a complete incident briefing takes place using ICS Form 201- Incident Briefing Form.

Activities performed within an EOC

Incident Action Plans (IAPs) are developed for each operational period. As appropriate, plans should cover the following phases:

- Initial response (i.e. safety and security)
- Damage assessment and incident stabilization
- Business continuity
- Recovery to normal operations

Note: Business Continuity Plans are the responsibility of each college centre and/or department.

Incident Management

Initial Response Options

Depending on the incident assessment a decision by the Incident Commander (IC) to enact one of the following response options may be required.

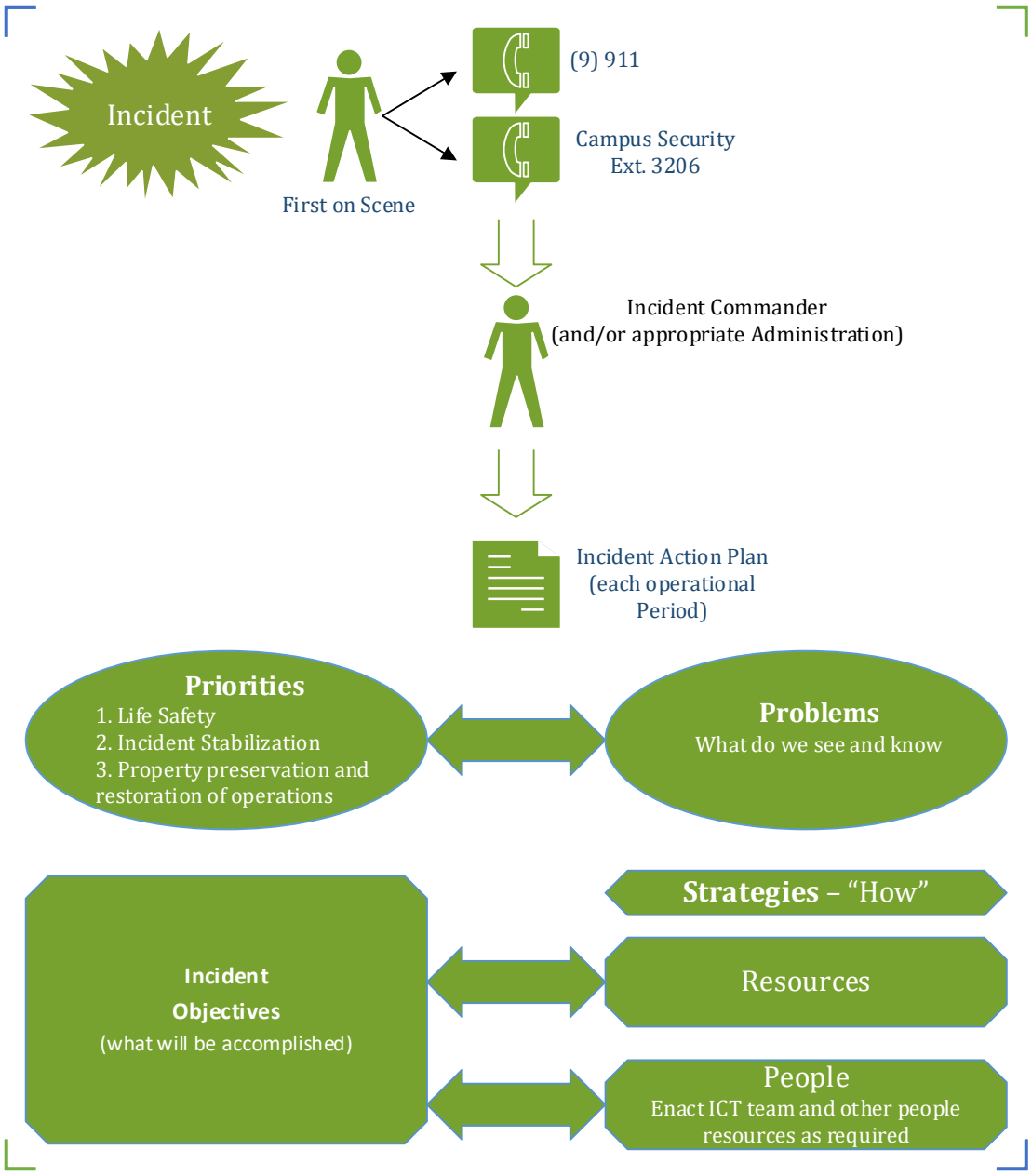
Primary resources to support the response will be the Incident Command Team (ICT) - primarily the Information Officer and members of the college's **Building Emergency Response Team (BERT).**

- cancel normal operations or modify services for the work day
- emergency dismissal – services suspended
- shelter-in-place (protection within grounds/facilities)
- lock-down – secure buildings and isolate the threat
- evacuation to a safe site
- relocation (for sheltering) in conjunction with evacuation

Forms and Documentation

For the majority of incidents, the ICS Form 201 - Incident Briefing Form will be all that is required. Check in sheets and other working documents are available for working groups. Other ICS forms are available for more severe incidents.

The following diagram provides an overview of the incident management process in a response to an incident that is *outside of normal operations AND requiring a response from a public service agency (i.e. fire, police)*


Incident
First on Scene
(9) 911
Campus Security
Ext. 3206
Incident Commander
(and/or appropriate Administration)
Incident Action Plan
(each operational
Period)
Priorities
1. Life Safety
2. Incident Stabilization
3. Property preservation and
restoration of operations
Problems
What do we see and know
Incident
Objectives
(what will be accomplished)
Strategies – "How"
Resources
People
Enact ICT team and other people
resources as required

Training and Plan Exercise

The Vice President People and Planning is responsible to coordinate training activities and regular opportunities for exercising the plan.

Training for members of the Incident Command Team and Executive Policy Group will consist of:

- knowledge of the college's Emergency Response Plan and implementation;
- a working knowledge of the Incident Command System;
  - All ICT members are required to take **ICS 100** (AEMA web-site)
  - other courses as required
- the skills necessary to increase their effectiveness to respond to and recover from emergencies of all types;
- at least annually conduct realistic exercises and drills to evaluate local capabilities and test the plan;
- lessons learned from actual or test incidents will be incorporated into the plan; and
- ensuring members of the BERT team receive appropriate training.

Plan Maintenance

The Vice President People and Planning or designate is responsible for maintaining the Emergency Management Plan. Plan maintenance shall include:

- an annual review and update of the plan based on stakeholder input and lessons learned
- regular maintenance of teams (ICT, EPG)
- centralization of all associated plans and documents.

The Vice President People and Planning or designate is responsible to assist departments and centres in the development of business continuity plans.

The Communications Manager is responsible to develop and maintain the Crisis Communication Plan.