Incident Management Practice

Program	Incident Management		
H&S Discipline	Occupational Health and Safety		
Content Owner	Manager, Central Health & Safety		
Custodian	H&S Programs & Projects		
Document Number	CEN-EHS101		
COMS Standard	COMS Incident Management Standard		
Version	3.1	**Review Cycle**	3 years
Revised Date	October 1, 2014	**Issued date**	June 5, 2006

Version	Description	Date	Approvals		
			Originator	Reviewer(s)	Approver(s)
3.0	Program update to align with COMS Incident Management Standard	Oct. 1/14			
3.1	Updated 4.2.1.2 EIN is required for H&S impact including process safety Tier 1 & 2 Incidents Removed 24 Hour Update concept 4.2.1.3 Removed requirements for recordable injury/illness EIN				

Table of Contents

List of Tables

1.0 Purpose

The purpose of the Incident Management Practice is to provide supplementary direction and guidance on how to achieve the requirements outlined in the COMS Incident Management Standard.

2.0 Scope

This standard applies across Cenovus Operations, including Cenovus staff, contractors and service providers.

3.0 Principles of incident management

Cenovus has developed a series of principles to guide incident management:

- Cenovus's goal is to conduct our work in a manner that prevents zero harm and loss to people, the environment, assets/property, and the community.

- Our intention is to minimize the need to apply the Incident Management Standard and Practice by implementing leading activities (e.g. proactive risk and hazard reduction measures such as hazard/risk analysis, work planning, workplace inspections, behaviour based observations, training, focus assessments, active management participation) that prevent incidents and near miss incidents.

- Cenovus expects that all incidents or near miss incidents, no matter the size or impact, be openly and honestly reported. Every individual is responsible to report an incident or near miss to their immediate supervisor. If the incident is an emergency, personnel are expected to report the occurrence by activating the emergency response plan (ERP).

- We recognize that reporting and quality investigating are not fault finding, but learning and improving to maximize opportunities and minimize or prevent harm and loss.

- We recognize that the quality of data collected in the Incident Management System (IMS) database impacts the interpretation of safety performance and the quality of strategic incident prevention planning.

- We will comply with regulatory reporting requirements.

- We will maintain a constructive working dialogue with all contractors and consultants with respect to incident management.

- We recognize that behaviours, equipment, processes and systems can cause incidents and we will pursue preventative measures for each of these causes.

- We recognize that incident management is a stewardship tool designed to maximize learning opportunities arising from incidents and to achieve best performance.

We recognize that incident management requires a high level of diligence in the way we manage our business.

4.0 Process Requirements

The Cenovus Incident Management Practice includes specific elements that are stewarded through an overarching Incident Management Process that provides logical guidance on the application of incident management practices. Can be found in the Incident Management Supplementary Tools Package, CEN-EHS8370.

The 10 elements of the process are:

1. Initial Report and Response

2. Internal and External Notifications

3. Investigate Incidents

4. Incident Analysis

5. Corrective Actions

6. Documentation and Records

7. Incident Review and Closure

8. Knowledge Sharing

9. Trending and Performance Reporting

10. Continuous Improvement

This process is supplemented by the Incident Reporting and Investigation Timeline located in the Incident Management Supplementary Tools Package, CEN-EHS8370.

4.1 Initial Reporting and Response

4.1.1 Initial Reporting

All incidents must be reported immediately (verbally) to your direct supervisor.

Emergencies must be reported using the protocol outlined at the worksite or facility, or in the work team Emergency Response Plan (ERP). Workers are also expected to report emergencies to their direct supervisors.

4.1.2 Response

The initial response begins with recognition and report of an incident. A rapid and accurate assessment of a situation is critical to establish the appropriate response. Any person can conduct this assessment and the purpose of the assessment is to determine if a situation is an emergency or an incident. It is important to recognize in this assessment that all emergency scenarios are considered incidents, but not all incidents are emergencies. In either case, work associated with the incident shall cease

until otherwise directed by a supervisor. If working under the authority of a safe work permit, the permit will also become void.

Once an emergency is terminated or reaches a stand-down state the investigation and subsequent actions shall follow the requirements of this practice.

For an incident that is not considered an emergency, the investigation process will be initiated by the frontline supervision responsible for the area or work as soon as the incident is reported. Supervisors are responsible to:

- Stop work and secure the incident scene to protect people and preserve evidence

- Identify and secure workers involved with the incident and witnesses

- Establish safeguards to protect personnel, the environment and/or equipment and assets and, if possible, ensure these actions do not alter potential evidence

- Follow the requirements outlined in the *Alcohol and Drug Testing Guideline* and complete the *Alcohol and Drug Testing Rationale Form* for incidents where workers are involved

- Determine the impact using the Incident Impact Tool and respond appropriately located in the Incident Management Supplementary Tools Package, CEN-EHS8370

4.2 Internal and External Notifications

4.2.1 Internal Cenovus Notifications Requirements

The responsible supervisor must notify and engage the appropriate business support teams and business leaders for reporting requirements and investigation support. Notification requirements are outlined in the Incident Notification Matrix, Incident Notification Flowchart see the Incident Management Supplementary Tools Package, CEN-EHS8370 and the Business Support Team Notification and Reference Guides (Appendix A).

Internal notification requirements are based on the incident impact and type. There are two impact scales that define notification requirements and drive the requirements for investigation rigour and knowledge sharing.

4.2.1.1 Low Impact Incidents

Low Impact Incidents are incidents with an actual or potential impact level of 1 – Minor [I1], or 2 – Moderate [I2].

For low-impact incident notifications, the responsible supervisor must enter the Incident into the IMS database within 48 hours. The Daily Summary of Incidents email shall serve as the minimum internal notification mechanism for low-impact incidents.

4.2.1.2   Significant Incident

Significant Incidents are incidents with an actual or potential impact level of 3 – Major [I3], 4 – Critical [I4], or 5 – Catastrophic [I5].

Phone Reporting

Immediate phone notification is required for significant incidents. A phone reporting process must be initiated by the asset or business support team. Supervision and business leaders must report upward through the business management stream of the organizational chart with incident information. Depending on the seriousness and significance of the incident or situation, communications may possibly reach the President and Chief Executive Officer. Leaders must use discretion when determining the level of escalation required to inform the right parties.

Notification must be made to a person within 30 minutes of the incident. If the person does not answer, leave a voicemail and send a text message. For significant incidents, if you are unable to reach your direct leader the phone call should escalate to the next person in the organization.

The asset health and safety (H&S) team will also report upward through the H&S stream with final communication reaching the H&S Operations Vice-president (VP) for significant incidents.

Each asset or business support team must develop and manage an appropriate call-out or phone reporting process.

Early Incident Notification

For significant incidents with a health and safety impact, including process safety incidents with an impact potential of 3 or greater (e.g. Tier 1 and 2 process safety incidents), an Early Incident Notification (EIN) (see the H&S Communication Practice) must be developed and communicated. An EIN is used to report known facts and the next steps of the investigation process to Cenovus business leaders and applicable business support teams. The Lead Investigator distributes the EIN via email within four hours of the incident occurrence.

Asset or operations support leaders are responsible to maintain an accurate EIN notification distribution list for their respective areas that includes both senior leaders accountable for the area, site or work team, and H&S personnel who support the area, site or work team.

4.2.2   External Notification Requirements

Regulatory, jurisdictional government agency or stakeholder notifications/reports may be required depending on the type and outcome of the incident. Regulations, licensing agreements, permits, contracts and

government orders are items that govern external reporting. Such reporting will only occur after consultation and authorization from the responsible business leader.

Business support teams, who provide subject matter expertise on specific external requirements, shall be contacted by the responsible area supervisor. Incidents with potential regulatory or other legal liabilities must also be reported to Cenovus legal counsel.

Regulatory notifications must be made in accordance with the timeframes outlined by the respectful regulatory governing body or licensor.

External notifications to joint venture partners shall be conducted in accordance with the mutual agreement between Cenovus and the joint venture partner.

Communications with a regulatory body or external stakeholder shall be conducted in accordance with the External Communications COMS Standard.

4.2.3 Incident Naming Convention

All internal notifications or communications (e.g. EINs,

Email Notifications) must conform to the internal Cenovus Incident Naming Convention.

H&S incident notifications or incident communications/documentation must be labelled as **confidential** and must quote the incident name as per the naming convention in subject lines for email, supporting attachments and file names.

Incident Naming Convention Structure

CONFIDENTIAL: EIN/date or IMS#/asset/activity/company/preliminary classification/potential impact

Examples

Contractor incident with no IMS# generated:

CONFIDENTIAL: EIN/2013-01-18/Christina Lake/Operations/Company X/LTI/I3

Cenovus incident with IMS# generated:

CONFIDENTIAL: EIN/IN2013-01-18-0000/Christina Lake/Operations/Cenovus/LTI/I3

Table 1: Incident Naming Convention Requirements

Value	Requirement
Incident notification type	Early Incident Notification (EIN)
Date or IMS# if available	Showing as Year-Month-Day or IMS#, if available
Location	Asset or area
Activity	Operations, CMT, drilling, camps, earthworks, etc.
Company name	For a contractor incident, provide the contractor company name. For a Cenovus incident, insert 'Cenovus'. **Do not** use personal names.
Preliminary classification	LTI/MA/FA/RW/NM
Potential impact	1–5 based on Cenovus Risk Matrix

4.2.4 Investigate Incidents

All incidents are to be investigated. The investigation is intended to uncover all applicable facts and root cause(s). The level of detail required for an investigation is based upon:

The actual or potential impact (Impacting Rating Tool see the Incident Management Supplementary Tools Package, CEN-EHS8370)

- Regulatory expectations for the incident type

- The opportunity to gain value added lessons learned

Uncovering deficiencies and system failures is critical in driving continuous improvement. It is important that a robust investigation team is assembled and that significant effort is exerted to collect evidence and the facts surrounding an incident.

It is expected that the responsible business shall drive the investigation process and leverage from the expertise and experiences of business support teams.

4.2.5 Post-Incident Drug and Alcohol Testing

Cenovus supports workplace health and safety through a comprehensive investigation process that incorporates post-incident alcohol and drug testing. Post-incident testing may be conducted as part of a full investigation into a work-related incident, where it has been determined that the individual's actions or omissions contributed to the incident.

Supervisors shall follow the requirements outlined in the *Alcohol and Drug Testing Guideline* and complete the *Alcohol and Drug Testing Rationale Form* for incidents where workers are involved.

All applicable alcohol and drug related fields within IMS are to be completed and the *Alcohol and Drug Testing Rationale Form* must be attached to the incident report and uploaded to the IMS database.

For additional support on post-incident alcohol and drug testing see the following documents:

- Alcohol and Drug Policy

- Alcohol and Drug Practice

- CEN-EHS1194, Alcohol and Drug Testing Guidelines

- CEN726 Alcohol and Drug Testing Rational Form

4.2.6 Investigation Team

Investigations shall commence immediately upon report of an incident. Business leaders shall consult with business support teams to:

- Determine the lead investigator

- Form the investigation team

- Establish the scope of the investigation

- Engage the appropriate subject matter experts

Incident investigations are intended to be carried out with the appropriate personnel on the investigation team, as required. This may include contractors or service providers. Lead investigators are expected to delegate actions to investigation team members and ensure that the process outlined in this Incident Management practice is applied.

For significant or complex incidents (e.g. fires, explosions, significant equipment damage, major environmental spills/leaks or fatal injuries/illnesses) it is critical that the necessary investigating resources and personnel are made readily available. In some cases internal unbiased investigators may be acquired from other assets or business support teams to assist or lead an investigation. In other circumstances, an expert third-party investigator may be required.

4.2.7 Evidence Collection and Processing

It is critical that all facts and information related to **people, position, parts,** and **paper** evidence (the **4 Ps**) are attained through the investigation process. This information is critical in determining the root cause of an incident.

The Lead Investigator shall lead the investigation team in collection of all applicable evidence. The Lead Investigator must also upload/include all applicable evidence collected in the investigation process in the **Links** tab of the IMS database.

It is expected that investigation team members shall maintain, at all times, the integrity and security of all the evidence that is collected.

The Cenovus Incident Investigation Checklist provides guidance on what information should be collected. This checklist is not exhaustive and there may be other incident-specific actions required to deliver a rigorous investigation. The Incident Investigation Checklist must be completed for each incident investigation and uploaded to the IMS attachments section.

For further investigation information see:

- CEN-EHS374, Incident Investigation Guideline

- CEN715 – Incident Investigation Checklist

4.3 Incident Analysis

Understanding what caused or contributed to an incident is of great importance to Cenovus. The endeavour to understand gaps and deficiencies is the first step in the continuous improvement spectrum.

All incident investigations will be conducted in manner whereby the evidence collected can be used for root cause analysis.

4.3.1 Root Cause Analysis

The purpose of root cause analysis (RCA) is to systematically review the facts that contribute to an incident in order to move focus from the symptom or immediate cause(s) to the underlying or root cause. A root cause analysis tool provides a common problem solving structure for understanding the interdependent relationships of facts contributing to an incident.

All incidents require the identification of root cause(s). The effort required or the selection of a RCA tool is based on the impact rating of the incident.

4.3.1.1 Low-Impact Incident Root Cause Analysis

Multiple options exist for low-impact RCA such TapRooT®, 5 Whys, fault tree analysis and failure mode and effect analysis. The Lead Investigator shall determine the RCA method or tool used for low-impact incident analysis. The Lead Investigator must also demonstrate what RCA process was used for low-impact incident analysis and how the root cause was determined.

4.3.1.2 Significant Incident Root Cause Analysis

The TapRooT® RCA method shall be used by Cenovus to determine root cause(s) of significant incidents. The Lead Investigator is responsible to coordinate a TapRooT® RCA for significant incidents.

All TapRooT® RCAs must be facilitated by a trained and competent person who has successfully completed the required TapRooT® training.

The RCA will be scheduled upon completion of the evidence collection phase with the goal of being completed within seven days of the incident occurrence.

Alternate formalized RCA methods shall only be used for significant incidents once approved by the asset and business support team leaders.

An RCA exemption may be granted by asset and business support team leaders when:

➢ There is clear evidence limited learning value will be obtained

➢ The circumstances of the incident clearly indicate a root cause

➢ The injury or illness incidents are not related Cenovus work (non-occupational)

The reasoning for a root cause analysis exemption must be documented and added in the attachments section of the IMS database with the appropriate approvals.

4.4 Corrective Actions

Upon completion of the incident investigation and the root cause analysis (RCA), all incidents require the development of corrective actions. Each identified root cause shall be evaluated to determine the appropriate recommendations and the development of corrective actions. Corrective actions must focus on ways to prevent a recurrence of the incident, or another similar incident.

All identified root causes must have corrective actions assigned. Business leaders shall determine the best corrective actions with consultation from business support teams. Business leaders shall also review and approve implementation of corrective actions. All corrective actions must be entered into the IMS database and assigned accordingly.

Good quality and effective corrective actions must adhere to the principles of the hierarchy of hazard controls. The focus of an action must be on eliminating the hazards. If elimination is not reasonable, hazards must be controlled by first using engineering controls, then administrative controls and finally personal protective equipment.

Corrective actions must be framed using the SMARTER definition, see the Incident Management Supplementary Tools Package, CEN-EHS8370. Corrective actions following the SMARTER concept are intended to be of a high quality nature and provide the greatest influence on correcting a problem and preventing recurrence.

The lead investigator must enter corrective actions into the IMS database and assign accountability to a business leader with the authority and resources to complete the action.

The business leader accountable for the incident must define the process of monitoring the implementation and closure of corrective actions. Follow-up on the status of corrective actions is essential in order to:

- Confirm adequate resources are available to achieve the action

- Confirm the person responsible to complete the action is on track for completion

- Understand if there are any challenges that may have affected proper implementation

Once a corrective action has been implemented, the person responsible to complete the action can close the action in IMS. To satisfy closure evidence and back-up documentation (e.g. records, administrative controls, pictures, invoices, inspection reports, work orders) must be uploaded to IMS. In rare cases, documentation may not be available to demonstrate action has been taken. In such cases it is acceptable for the responsible party to write a brief narrative explaining what was done.

Implementation is successful if:

- The recommendations were implemented and the specified corrective actions are taken

- Follow-up indicated that the corrective actions have corrected the root cause and/or prevented similar incidents from occurring

- The corrective actions did not introduce new hazards or unmanaged, residual risks

- Evidence of completion was uploaded to IMS

An assessment of the effectiveness of a corrective action must be completed for all high priority corrective actions. Business leaders must implement a process that verifies the effectiveness of corrective actions.

4.5 Documentation and Records

4.5.1 Incident Report and Supporting Documentation

The results of an incident investigation and root cause must be documented. Both the impact of the incident and regulatory requirements will determine the level of detail needed for the investigation report.

For low-impact incidents, the frontline supervisor must complete the Initial Incident Report using the IMS database within 48 hours of the incident's occurrence. The front line supervisor or Lead Investigator shall enter significant incidents into IMS within 24 hours of occurrence.

As evidence and information is gathered, the IMS database must be updated. The Investigation and Link tabs in the IMS incident shall include all supporting evidence and analytical data and decisions. The Lead Investigator or designate must document, in the IMS incident entry, the results of an incident investigation and of the root cause analysis.

For certain significant incidents, or as required by external parties, a formal written incident report may be required. If a written report is required it shall be attached to the IMS entry to supplement the electronic IMS investigation report.

4.5.2 Report Distribution

Business leaders and other applicable business support teams (e.g. Environment, H&S, Engineering, Process Safety Management) must review and approve an incident report prior to its distribution to internal parties.

Business leaders, legal counsel and other applicable business support teams (e.g. Environment, H&S, Engineering, Communications) must review and approve an incident report prior to its distribution to external parties. It is critical that the contents of incident report meet the requirements outlined by external agencies.

4.5.3 Safety, Environment and Regulatory Committee

Significant incident reports are required for the Safety, Environment and Regulatory (SER) Committee meetings. Business Leaders shall generate a Significant Incident Analysis Summary (SIAS) as per the H&S Communications Practice.

4.5.4   Investigation Documentation Storage

Any and all material generated during an incident investigation, including TapRooT® reports, must be attached to the IMS incident entry in the Links tab. Items that should be stored within IMS are:

- Witness statements

- Interview notes

- Investigation field notes/drawings

- Photographs

- Inspection records

- Hazard and risk assessments

- Third-party incident investigation or failure analysis reports

- Email communications

- Phone call logs

- Site safety documentation

- Alcohol and drug testing rationale form

- TapRooT® RCA documentation

- Physicians First Report (C-050) if personal information is removed or redacted (for Cenovus employees stored with Health & Wellness)

- And any other evidence recovered during the investigation

All evidence or correspondence that is considered confidential must be stored in a secure location that meets the requirements of the Cenovus Privacy Policy, Employee Privacy Practice, Commercial Privacy Practice and the Personal Information Protection Commitment.

Please see Cenovus Retention Guidelines and Practices for more information.

4.5.5   Injury Illness Recording and Reporting

Employee, contractor and service provider injuries and illnesses shall be classified and reported in accordance with the CAPP Health and Safety Performance Metrics Reporting Guide.

4.6   Incident Review and Closure

All incidents require a review and closure process whereby the proper individuals provide input and authorization to finalize an incident investigation.

4.6.1 Low-Impact Incident Review and Closure Process

1. Frontline supervisors (e.g. consultants, supervisors, or coordinators) and the appropriate business support teams shall review low-impact incident investigations and analyses before these receive final approval and closure by the responsible business leader.

2. The review process shall verify:

   ➤ appropriate root causes are assigned

   ➤ that corrective actions are complete

   ➤ that the IMS incident entry is complete

   ➤ that no issues or problems related to the incident are outstanding

3. Business leaders (e.g. group leads, superintendents, managers or directors) shall approve the closure of low-impact incidents.

4.6.2 Significant Incident Review and Closure Process

1. Business leaders (e.g. group leads, superintendents, managers or directors) and the appropriate business support teams shall review all significant incident investigations and analyses before these receive final approval and closure by a senior business leaders.

2. The review process shall verify that:

   ➤ a post-incident review meeting was conducted

   ➤ the RCA process is complete

   ➤ appropriate root causes are assigned

   ➤ corrective actions are complete

   ➤ the IMS incident entry is complete

   ➤ no issues or problems related to the incident are outstanding

3. Senior business leaders (e.g. Vice-Presidents, Senior Vice-Presidents, the Chief Operating Officer or Executive Vice-Presidents) shall approve the closure of significant incidents.

4.6.3 Post-Incident Review Meeting

Business leaders, with assistance from business support teams, shall plan and coordinate an incident review meeting for significant incidents. Business leaders shall also facilitate the meeting.

An incident review meeting must include the following participants:

- The lead investigator and the investigation team

- Business leaders responsible for the area, activity and/or people involved with the incident

- Applicable contractors/service providers

- Appropriate business support team based on the type of incident

- Personnel involved in the incident (if required)

The post-incident review meeting must cover the following agenda at a minimum:

- Summary of findings and lessons learned

- Corrective actions and implementation status

- Determination of which lessons learned shall be shared and who is the audience for the lessons learned

- A review of the effectiveness of the initial incident reporting and notifications:

  - ➢ incident response

  - ➢ investigation (what good looks like)

  - ➢ the incident analysis

Minutes from the post-incident review meetings must be documented by the meeting facilitator and added to the IMS incident entry.

4.7 Knowledge Sharing

Lessons learned from an incident analysis must be appropriately shared across Cenovus operations. Lessons learned refer to information identified and documented through incident investigations and root cause analyses that may assist others (internal and external) in preventing similar incidents from occurring.

Shared lessons learned are critical for organizational risk mitigation and incident management system improvements. Cenovus gains a direct and immediate benefit from timely and successfully implemented incident-specific corrective measures.

We share lessons learned within the company using:

- Post-incident review meetings

- Toolbox talks

- Topical meetings or presentations

- Alerts and advisories

- ▪ Training

- ▪ Formal reports

4.7.1 General Communication Methods

There are multiple communications tools and methods available to Cenovus when communicating incident occurrences and lessons learned to the entire company, a specific site, joint venture partners, industry peers or to contractors. The *Cenovus H&S Communications Practice* (CEN-EHS027) details the communication requirements and expectations related to incident management.

A Significant Incident Analysis Summary (SIAS) must be generated for all significant incidents. In turn, the information in the SIAS will be used to develop an alert or an advisory. The Director of Operations H&S, or a delegate, will determine if a significant incident alert or advisory will be required. All alerts are approved by the Vice-President of H&S or designate. All significant incidents communications must be shared across Cenovus operations.

For low-impact incidents each asset or business support team must decide what communication tools and processes will satisfy site-specific requirements.

4.8 Trending and Performance Reporting

Analysing trends serves to identify patterns in incidents and common system deficiencies that can be addressed to prevent recurrence and to facilitate continuous improvement. Trend analysis also assists in setting priorities for the business and allocating the appropriate resources in order to improve systems and processes.

Incident statistics are an important way of determining incident and near miss trends and of benchmarking safety performance. For statistics to be relevant, all incidents must be entered into IMS correctly and completely. Therefore investigations must be accurate and comprehensive to ensure the correct details are captured in the IMS database.

The Health & Safety Intelligence Reporting (HSIR) tool provides the opportunity for routine and user-defined statistical analyses. Routine analyses are available to assess:

- ▪ Higher frequency incident types, locations, times

- ▪ Low-frequency — high-consequence actual or potential losses

- ▪ Inadequate or outdated tools and procedures

- ▪ Recurring root causes

- ▪ Management of change deficiencies

- ▪ Contractor management deficiencies

These deficiencies or issues can be mitigated through performance improvement plans using such tactics as:

- Targeting specific tasks through campaigns

- Improving central or asset specific practices and standards

- Implementing new policy

- Changing or refining work planning processes

- Re-evaluating project risk/hazard assessment or hazards

- Re-evaluating project specific H&S execution/management plans

- Improving contractor management processes

- Improving training and awareness courses

It is expected that business leaders will use incident management performance reports and data to identify and strategically attack high-risk areas and trends. Business leaders shall also implement performance improvement plans that focus on systemic deficiencies identified from performance reports and trends.

4.9 Continuous Improvement

Continuous improvement is a critical component of the Cenovus Operations Management System (COMS). Setting clear and attainable objectives and implementing verification tools to evaluate success are essential in the overall incident management process.

4.9.1 Metrics and Measurement

Cenovus business leaders shall establish annual key performance indicators (KPIs) related to incident management at the operations level, asset level, business support team level and site level. Incident Management KPIs must be generated as annual operating objectives and can also be produced to drive specific aspects of performance. KPIs will address both leading and lagging metrics.

4.9.2 Quality Assurance and Verification

Business leaders and business support teams shall participate in quality assurance activities related to incident management. Quality assurance activities include:

- Assessing the timely reporting of incidents

- Verifying incident classifications

- Verifying incident impact ranking is accurate and realistic

- Reviewing the incident data/information entered into IMS and ensure it is of a quality nature

- Evaluating if appropriate root causes were chosen based on the RCA method

- Evaluating if root causes are aligned with the action plans for prevention at system, equipment and behavioural levels

- Verifying that action items are achieved and closed as planned

- Reviewing and assess documented incident reports

- Verifying the quality of a TapRooT® analysis

5.0 Incident Management Expectations for Contractors and Service Providers

- Immediately report all incidents that occur within their company or a sub-contractor's company while performing work for Cenovus. A representative of the contractor or service provider's leadership team is expected to verbally contact the appropriate Cenovus representative to inform them of an incident occurrence.

- Provide an email or other form of appropriate electronic correspondence that documents known facts, immediate actions and the investigation plan within four hours of the incident. This communication must meet the intent of the Cenovus EIN.

- Investigate all incidents using the contractor or service provider's incident management processes and procedures provided they meet or exceed Cenovus's standards.

- Determine the root cause(s) of all incidents and demonstrate how this conclusion was made.

- Implement a process whereby the senior representative for the contractor or service provider company participates in all investigations related to recordable injuries or illnesses, and significant incidents.

- Certify their employees participating in incident management and investigation activities have adequate training and competencies that meet or exceed Cenovus's standards.

- Provide Cenovus an initial incident report within 24 hours that satisfies the requirements set forth in the Cenovus Initial Incident Report Form.

- Provide Cenovus a final written incident report within 72 hours for all low-impact incidents.

- For significant incidents, agree with Cenovus upon an adequate timeframe for the delivery of a final formal report including root cause analysis and corrective actions.

- Demonstrate what formalized RCA method was used to determine the root cause of an incident.

- In the final written report, include quality investigation results, corrective actions and plans to verify corrective action effectiveness.

- Provide Cenovus with any additional evidence or documentation related to an incident or an incident investigation that occurs at a Cenovus worksite.

- Participate in and present incident lessons learned at Cenovus sponsored incident review meetings.

- Allow Cenovus personnel to participate in the contractor or service provider's investigation if deemed necessary by Cenovus.

- Classify incidents as per the CAPP Health & Safety Performance Metrics Reporting of Occupational Injuries and Illnesses Guide.

- Contractors are accountable for all sub-contractor incidents.

6.0 Roles and Responsibilities

The following responsibilities apply to this practice:

Table 2: Roles and Responsibilities

Role	Description
Central Health & Safety	- Incident management program development and guidance - Owns the Incident Management System - Monitors performance and adherence to the practice
COMS Audit	Monitors compliance of Incident Management Standard and adherence to the standard
EHSR Audit	Monitors compliance of H&S Programs and adherence to the practice
Business Leaders (including Senior Business Leaders)	- Take ownership and responsibility for incidents at their operations or within their business support team. - Communicate and implement the incident management standards and practices at their operations or functional areas of authority. - Allocate and make available the necessary financial and human resources that are required to functionally implement the Incident Management Practice. - Confirm contractor or service provider Incident Management Programs are reviewed and approved prior to mobilization to Cenovus worksites. - Confirm that a contractor or service provider Incident Management Programs meets the requirement outlined in this Incident Management Practice.

	• Confirm that personnel who are involved in the incident management process are trained, knowledgeable, experienced and competent. • Correct workers who do not follow the incident management notification and reporting requirements. • Provide feedback to the Incident Management Process owner or representative concerning proposed changes or improvements to the incident management processes. • Review significant incidents and related corrective actions to prevent recurrence. • Confirm corrective actions are successfully completed on time and verify that the actions have corrected any deficiencies. • Provide authority to finalize and close incident investigations. • Assign a Lead Investigator for significant incidents.
Frontline Supervisors	• Make direct reports and contractors (including subcontractors) aware of their responsibility to report incidents in which they are involved or observe. • Provide prompt and immediate care of an injured party or persons following established response plans. • Promptly notify appropriate levels of management and business support teams of an incident in accordance with the incident notification matrix. • Facilitate and support reporting and investigation of incidents within their area(s) of responsibility. • Assist and participate in incident investigations and root cause analyses. • Communicate incident related reports to direct reports, contractors and sub-contractors in their area of responsibility. • Review and implement appropriate and timely corrective actions. • Assist in assigning a Lead Investigator and Investigation Team members.
Business Support Teams	• Provide subject matter expertise when requested by business leaders or a Lead Investigator.

	• Provide guidance on regulations, incident investigation techniques and root cause analyses. • Participate in investigations as subject matter experts. • Participate in root cause analyses or facilitate as required. • Participate in incident management assurance activities.
Business Sponsor/ Contract Proponent	• Communicate the requirements of this Incident Management Practice to contractors and service providers. • Verify that a contractor or service provider's Incident Management Program aligns with the expectations described in this practice. • Include terms and conditions in a contractor or service provider's contract that align with the expectations described in this practice. • Consult with the appropriate business support team to review and approve a contractor's or service provider's Incident Management Program prior to mobilization to a Cenovus worksite.
Operations H&S	• Account for the development and governance of this practice. • Develop and maintain the Incident Management Practice in accordance with company policy, industry best practices and regulatory requirements. • Review the incident management documents every three years, or more frequently as required by regulatory changes or identified deficiencies, to confirm currency and applicability for the company.
Lead Investigator	• Plan, coordinate and conduct an impartial incident investigation from start to finish. • Maintain the continuity of the incident management process throughout the investigation, root cause analysis and the development of corrective actions. • Lead the investigation team in collection of all applicable evidence in the form of people, parts, positions and papers (4 Ps). • Confirm that the investigation report is completed in IMS. • Identify and assign Investigation Team members.

Investigation Team	• Assist the Lead Investigator in completing investigation from start to finish. • Complete tasks such as collecting evidence, communicating with management members, participating in the root cause analysis and developing corrective actions.
Workers	• Plan and perform work in a manner that prevents incidents. • Report all incidents to their immediate supervisor regardless of the size or perceived impact of the incident.

7.0 Training and Competency

Competency describes the knowledge and skills required to successfully perform the technical aspects of a job. A worker must be able to demonstrate competency in safely performing work tasks or using equipment.

7.1 Training

It is expected that all personnel involved in the incident management process will have training and the appropriate competency to perform their role. Cenovus incident investigation training expectations are outlined in the Incident Management Awareness and Training Matrix (Appendix B).

7.2 Competency Verification

Competency will be validated through formal, theory-based evaluations and practical skill demonstration. All theory-based training requires a written knowledge check (e.g. test, quiz, exam) that will be reviewed and assessed by a competent instructor. Practical skill assessments of task completion and equipment use must be conducted by a competent supervisor or mentor.

Workers may be required to attended additional training sessions or complete further on-the-job training if performance deficiencies are identified through formal assessments.

All written evaluations and practical skill assessments must be documented and retained in the worker's personnel file. Records may be maintained in hard copy or electronically.

8.0 Quality Assurance

8.1 Performance Measurement

Compliance with this practice and program effectiveness shall be assessed through program assessments and internal audits, or other measurement criteria as specified in the COMS Assurance Standard. Measurement can also be accomplished through the tracking of appropriate Key Performance Indicators (KPI).

Business functions or departments impacted by this practice must include compliance and program effectiveness verifications in their business assurance program. Performance will be monitored and reported within the responsible departments at least every three years.

Central Health and Safety Services will review Cenovus-wide program KPIs at a minimum every three years in conjunction with program review and update activities.

8.2 Management of Change

Proposed changes to this practice can be directed to H&S Programs and Projects.

8.3 Practice Verification

The document owner will complete and document reviews of this practice as follows:

- At minimum once every three years

- If there is a significant regulation or industry best practice change that indicates the need for review

- If an incident investigation indicates the causes were related to unclear or inadequate written instructions described within this practice

If frequent and multiple variances are required due to operational needs, the reason(s) will be investigated and the document owner will determine if there is a business need to update the practice.

If submitted MOC requests indicate gaps or significant improvement opportunities, the document owner will determine if there is a business need to update the practice.

9.0 Glossary

Definitions and acronyms for safety documents are described in H&S Definitions and Acronyms. The following definitions and acronyms are specific to this document.

Table 3: Terms and Definitions

Term	Definition
Business Leaders	Business representatives (e.g. group leads, superintendents, managers or directors) are line mangers that have authority and administrative control of work activities at Cenovus worksites.
Business Sponsor/Contract Proponent	The Cenovus representative accountable for a contractor's or service provider's contract or service agreement.
Business Support Teams	Functional support teams such as Health & Safety, Environment, Process Safety, Electrical, Security, Regulatory, Maintenance and Reliability, Transportation, Legal, etc.
Corrective Actions	Actions primarily focused on improving our organization processes or systems and addressing causal factors and root causes identified through the root cause analysis process.
Early Incident Notification (EIN)	An EIN is an initial communication distributed to a specific audience notifying them of the significant incident. The EIN includes pertinent details of the incident. An EIN is developed and distributed in accordance with the H&S Communications Practice.
Electrical Incident	An incident that involves electrical equipment and/or originates from electricity.
Emergency	Any present or imminent unplanned incident outside the scope of normal operations that requires prompt coordination of actions to protect against: • life-threatening injury or illness • a fatality • prolonged process disruption • significant property damage • significant environmental impact At Cenovus an Activation of an ERP occurs when an Incident Commander has been engaged and the incident has been classified as a "Level 1 Emergency" on AER's Assessment Matrix for Classifying Incidents.
Equipment Failure Incident	A mechanical or equipment/process failure that results in, or has the potential to, cause injury, illness, production impact, process upset, or other significant loss.
Fire/Explosion Incident	An incident that is caused by, or involves, a fire or explosion.

Frontline Supervision	A supervisor directly responsible for execution of work at the field level (e.g. consultants, supervisors, or coordinators).
Hazard Identification	A condition that, left unaddressed, has the potential to cause an incident or a Near Miss.
Hierarchy of Hazard Controls	A systematic approach used to minimize or eliminate exposure to hazards. The hierarchy in order of most effective to least effective controls is elimination, engineering, administrative, PPE.
Illness	Any abnormal health condition or disorder caused by repeated or prolonged exposure to activities or environmental factors associated with employment.
Incident	An incident or occurrence that results, or potentially results, in an injury, illness, spill or release from primary containment, operation beyond regulatory limits, a regulatory noncompliance, property damage production or financial loss and reputation impacts. Near Miss incidents are considered incidents.
Incident Impact	A rating used to describe the potential impact of an incident. The impact table of the risk matrix is used to determine actual and potential impact. To be included in the Incident Management Practice.
Incident Investigation	A post-occurrence process used to establish the facts of an incident in order to properly understand the circumstances that led to the incident and the facts surrounding the incident. An investigation is conducted with rigour and to the level of detail appropriate to support the requirements of a follow-up RCA for that incident.
Incident Management System (IMS) Application	The Incident Management System is a corporate software application used to capture incident details and data.
Incident Review Meetings	An incident specific meeting held to discuss incidents, the investigation process, findings and corrective actions. This meeting can be elevated to the Senior Business Leader level as necessary.
Injury	Any cut, fracture, sprain, amputation, loss of consciousness, etc., that results from an exposure involving a single incident in the work environment. For injury sub-classifications see to the IMS reporting standard.
Initial Notification Matrix	A matrix defining reporting requirements based on incident impact and type.
Lead Investigator	A Business Leader or other qualified person assigned to lead an investigation. This individual shall be one level removed from the execution of the work.

Low-Impact Incident	An incident that is described by an impact that poses no risk of life altering injury. Low-Impact Incidents are incidents with an actual or potential impact level of 1 – Minor [I1], or 2 – Moderate [I2].
Motor Vehicle Incident	An incident involving a motor vehicle that is licensed for highway use that is involved in any type of collision with an object, person, animal, or another motor vehicle while in use.
Near Miss	An incident that had the potential to result in an injury, illness, property damage or loss, but did not. Once a worker is exposed to a hazard, the hazard identification becomes a near miss.
Property Damage Incident	An incident that results in damage to property, including licensed motor vehicles that are in a stationary position (not in use), whether occupied or not.
Powered Mobile Equipment Incident	An incident involving any vehicle that is not designed to operate primarily on public streets or roadways. (e.g. zoom-boom, Quad, All-Terrain Vehicle, Argo, aerial work platform).
Process Safety Incident	A process safety incident is an actual unplanned or uncontrolled incident that leads to an overpressure or loss of primary containment. These incidents typically result from the failure of process equipment. Example incidents: • explosion or implosion • fire • exposure to hazardous material(s) • chemical release
Public Complaint Incident	An incident involving anyone outside of Cenovus's operational personnel or complaints received from non-Cenovus operational personnel that could impact the company reputation.
Recordable Injury/Illness	An injury or illness that is considered as 'recordable' within the Canadian Association of Petroleum Producers' Health and Safety Performance Metrics reporting Guide.
Release/Spill Incident	A release incident that includes a spill, discharge, dispose of, spray, inject, inoculate, abandon, deposit, leak, seep, pour, emit, empty, throw, dump, place, and exhaust (see the *Cenovus Spill Reporting Requirements* for regulatory reporting requirements in Alberta and Saskatchewan).
Reportable Incident	An incident that requires notification to external parties as per regulation, licensing/permit agreements or joint venture partnership arrangements (e.g. Alberta Energy Regulator, Provincial Occupational Health and Safety, Saskatchewan Ministry of Energy and Resources, Alberta Boilers Safety Authority, Department of National Defence).

Root Cause Analysis (RCA)	Is a problem solving method or analytical analysis process intended to uncover or identify the root cause (the most basic causes(s) that can reasonably be identified) that led to an incident.
Security Incident	An incident involving theft, civil unrest, threats, workplace violence, weapons, drug and alcohol violation, site/facility alarm, and/or break and enter on company property.
Senior Business Leaders	Business leaders responsible for corporate affairs and the development and execution of an asset or operations support teams' business strategy (e.g. Vice-Presidents, Senior Vice-Presidents, the Chief Operating Officer or Executive Vice-Presidents).
Significant Incident	A Significant Incident (SI) is an incident that, if not for luck, could have produced a more serious outcome, or potentially life-altering or fatality injuries. Incident described by an impact that that could produce a life-altering outcome. Significant Incidents (i.e. High Impact) are incidents with an actual or potential impact level of 3 – Major [I3], 4 – Critical [I4] or 5 – Catastrophic [I5].
SMARTER	Is a mnemonic acronym that guides a user through a process to generate functional objectives. SMARTER: • Specific • Measurable • Accountable • Reasonable • Timely • Effective • Reviewed
TapRooT®	Commercial RCA tool used under license to evaluate the root cause(s) of incidents with an actual or potential impact level of 3 – Moderate (I3), 4 – Major (I4) or 5 – Catastrophic (I5).
Witness	Any person with knowledge of an incident or who witnessed an incident occurrence.
Worker(s)	Individuals or work groups preforming tasks or activities as part of their occupation. This does not just apply to frontline field or office workers, but includes frontline supervisors or business leaders when active in the course of their occupations.

Table 4: Acronyms and Abbreviations

Term	In full
A&D	Alcohol and Drug (program and testing procedures)
EH&S	Previous department designator for the Health & Safety Department
EIN	Early Incident Notification
ERP	Emergency Response Plan
H&S	Health and Safety
IMS	Incident Management System Database (online reporting program)
RCA	Root Cause Analysis
SIAS	Significant Incident Analysis Summary

10.0 References

10.1 External Documents

The following external documents support this practice:

Table 5: External Document References

Document Type	Document Title
Regulatory	Alberta OHS Act, Regulation and Code
Regulatory	Saskatchewan OHS Regulation
Regulatory	Alberta Worker Compensation Act and Regulation
Regulatory	Saskatchewan Worker Compensation Act
Governance	Canadian Association of Petroleum Producers Health & Safety Performance Metrics Reporting

10.2 Internal Documents

The following Cenovus documents support this practice:

Table 6: Internal Document References

Document Type or Number	Document Title
Policy	Corporate Responsibility Policy
Framework	Cenovus Operations Management System (COMS) Framework
CEN-EHS243	H&S Definitions and Acronyms Standard
CEN-EHSReg787	Regulatory Definitions and Acronyms
Policy	Enterprise Risk Management Policy
Policy	Alcohol and Drug Policy
Corporate practice	Alcohol and Drug Practice

CEN-EHS110	Incident Management System Reporting Standard
CEN-346	Incident Management System Report Form
CEN-EHS374	Incident Investigation Guideline
CEN-EHS377	Incident Classifications and Definitions
CEN-715	Incident Investigation Checklist
CEN-726	Alcohol and Drug Testing Rationale
CEN-EHS817	Early Notification Form
CEN-EHS1194	Alcohol and Drug Testing Guideline
CEN-EHS2610	Incident Management System User Guide
CEN-EHS022	EH&S/Operations Risk Management
CEN-EHS2206	WCB Reporting Standard
CEN-EHS374	Incident Investigation Guideline
CEN-EHS037	Record and Retention Practice
CEN-EHS027	Alerts and Advisory Practice
CEN-EHS027	IMS User Reference Guide

Appendix A: Business Support Team Notification and Reference Guides

Table 7: Business Support Team Notification Guide

Incident Type	Support Team
Overpressure/Pressure Equipment Related	Facility Integrity
	Process Safety
	Health & Safety
Release/Spill (liquid, gas or chemical)	Environmental Services and Compliance
Equipment Failure	Maintenance and Reliability (M&R) Engineering
Control System	Process Control Engineering
Electrical (including electrical utility line strike)	Electrical
	Health & Safety
Production	Operations Coordinator
	Operations Superintendent
Motor Vehicle	Health & Safety
	Transportation/Fleet (if a CVE Vehicle or Bus)
	Range Control (Foster Creek and Suffield Only)
Injury	Health & Safety
Illness	Health & Safety
Significant Incident	Health & Safety
Underground Utility Piping/Pipeline Strike	Facility Integrity
	Health & Safety
Security (i.e. Alcohol and Drug, Theft, Violence, Vandalism)	Site Security
	Calgary Building Emergency Line (if in Calgary)

Table 8: Environmental Services and Compliance Reference Guide

Business Support Team: Environmental Services and Compliance
Business Support Team Objective: In support of Cenovus's long range business plans our team key driver is to design, execute, implement, review and report on compliance and monitoring activities with respect to environmental regulations, approval conditions and commitments across Cenovus. This includes operational regulatory compliance assurance activities to support continuous improvement. We seek to provide innovative means of meeting and assuring environmental compliance and monitoring requirements. In doing so we provide confidence to the business, regulators and stakeholders that Cenovus operates in a compliant responsible manner. This includes support to operations relating to spill response and remedial activities, regulatory reporting, and engagement in formal root cause analysis as required.
When to engage: Any incident that results in an adverse effect to the environment, regulator reportable release, and/or when a formal root cause analysis is being conducted Environment Services and Compliance should be consulted and engaged as required.

Table 9: Process Safety Engineering

Business Support Group: Process Safety Engineering
Business Support Group Objective: Process Safety Engineering exists to support the operations in preventing major accidents through both engineering and management. Process safety engineers have subject matter expertise in incident investigation and root cause analysis especially with engineering systems. Due to the complex nature of some incidents related to the process, it is critical to have this engagement. Lack of engagement could prevent correct determination of latent root causes and hamper the prevention of future incidents.
When to engage: Process safety incidents are well-defined within Cenovus. Process Safety Engineering should be engaged immediately whenever one such incident occurs.
Process safety flow chart link: https://contentserver.cenovus.com/otcs/cs.exe?header func=ll&objId=183429880&objAction=view

Table 10: Operations Shared Services Electrical Engineering Group

Business Support Team: Operations Shared Services Electrical Engineering Group
Business Support Team Objective: The Cenovus Operations Shared Services Electrical Engineering Group manages compliance to the obligations of Corporate Accreditation in the Electrical Discipline under the Alberta Safety Codes Act. The Electrical Regulatory Management Plan (ERMP) Manager is the Administrator of Record for Cenovus in the Electrical Discipline with Alberta Municipal Affairs. The ERMP Manager reviews and assesses all electrical incidents to determine reporting obligations. The ERMP Manager is obligated and accountable to appropriately report electrical incidents to Alberta Municipal Affairs.
When to engage: Within 24 hours of an electrical incident, at any voltage, that involves contact with electricity by a person, fatal contact with electricity by livestock, contact with a power line, unintended contact with energized or de-energized electrical power distribution and transmission facilities, unintended contact with energized electrical installation or equipment, a fire that is electrical in origin or of suspected electrical origin, the incident must be reported to the Cenovus Electrical Regulatory Management Plan Manager and the Cenovus Central Electrical Engineering Leadership Team.

Appendix B: Incident Management Awareness and Training Matrix

	Incident Mgmt. Awareness (eLearning)	Basic KMI IMS Software (eLearning)	Advanced KMI IMS Software (eLearning) TBD*	Incident Investigation (Facilitated 1 Day)	TapRooT® Awareness (Facilitated 2 Hours)	TapRooT® Refresher (Facilitated 4 Hours)	TapRooT® Process/ Theory (Facilitated 1 Day)	TapRooT® Software (Facilitated 1 Day)
Frontline Supervisor	X	X	X	X			X	
Business Leaders	X	X		X	X			
Senior Business Leader	X				X			
Business Support Team	X	X	X	X			X	
TapRooT® Facilitator	X	X		X			X	X
Lead Investigator	X	X	X	X			X	
Investigation Team Participant	X			X	X			
TapRooT® Software User					X			X

Note: The Central H&S Services training team offers a three day TapRoot® and Incident investigation training course. This three day session includes from the above training matrix the following courses: Incident Investigation (1day),TapRoot® Process/Theory (1 day) and TapRoot Software (1 day).