**Overview**

(COMPANY B) is one of Canada's leading producers of natural gas and oil, founded on November 7, 1973, in Calgary, Alberta. Its operations are also spread in Western Canada, the North Sea, and offshore West Africa. The company acquires, explores, develops, produces, and markets crude oil, natural gas, and natural gas liquids (NGLs). Its product portfolio includes light and medium crude oil, heavy crude oil, bitumen (thermal oil), synthetic crude oil (SCO), and natural gas. Its strategic marketing approach, skilled workforce, and aim for net-zero greenhouse gas emissions underline its commitment to sustainable growth and value creation for shareholders.

**Competitive Analysis**

**1.SWOT Analysis:**A diagram of a diagram

Description automatically generated with medium confidence

**2. PESTEL Analysis**

A diagram of a company's company

Description automatically generated with medium confidence

**3.Balanced Scorecard**



**PROBLEM STATEMENT**

The business model for COMPANY B is to explore, develop and produce natural gas and crude oil in its capacity as an upstream company. The main problem is that Canadian Natural Resources Ltd (COMPANY B) revenue greatly depends upon the market price of the oil and the natural gas that it produces, thus making it relatively more vulnerable to fluctuations in commodity prices.

However, other companies’ integrated model, which includes operations for upstream production as well as downstream refining and marketing, offers some protection against fluctuations in commodity prices. While they may reduce the profit earned through the exploration and production of crude oil, the downstream operations act as a buffer since the lower price of crude oil positively impacts the company's refining segment.

**Business Requirements**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| BUSINESS REQUIREMENTS  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO | | | | |
| **ID** | **REQUIREMENT DESCRIPTION** | **REQUIREMENT PRIORITIZATION (H, M, L)** | **TRACEABILITY** | **REQUIREMENT NOTES** |
| BR-01 | Conduct a thorough market study to support strategic decision-making. | H | Market Analysis Process | This includes developing goals, collecting data, assessing trends, and creating reports. |
| BR-02 | Implement and maintain strong cybersecurity protocols for SCADA systems. | H | Cybersecurity for SCADA Systems | This includes risk assessments, security audits, authentication procedures, and continuous monitoring. |
| BR-03 | Ensure that all applicable requirements are followed, and that employees receive regular cybersecurity best practices training. | H | Cybersecurity for SCADA Systems | Maintains legal adherence and increases cybersecurity awareness. |
| BR-04 | Create and optimize a systematic supply chain management procedure. | H | Supply Chain Management | This includes supplier selection, procurement, logistics, inventory management, and quality control. |
| BR-05 | To improve operational efficiency, we planned and executed downstream integration procedures using integrated technology. | H | Downstream Integration | This includes site acquisition, engineering, building, startup, and operation monitoring. |
| BR-06 | Ensure that all systems are highly available, scalable, and have user-friendly interfaces. | H | All processes | Supports company continuity and future expansion while improving user experience. |

**Solution 1: Downstream Integration with SCADA and Cybersecurity**

High-Level Design

**Integration of Downstream Activities:**

Objective: Construct facilities for the production of petroleum products, ensuring efficient processing of crude oil both locally and internationally. Align downstream operations with existing upstream activities to enhance capacity utilization and hedge against market fluctuations.

Rationale: This strategic move will solidify COMPANY B's market position while diversifying and stabilizing its revenue streams.

**SCADA System Implementation:**

Objective: Integrate Supervisory Control and Data Acquisition (SCADA) systems for refined downstream operations, interfacing them with current upstream systems to enable unified data management and process oversight.

Tasks: Implement redundancy and failover capabilities to prevent operational disruptions.

**Cybersecurity Measures:**

Objective: Protect SCADA systems from cyber threats.

**Measures:**

* Deploy firewalls, intrusion detection/prevention systems, and secure communication protocols.
* Segment the SCADA network from other enterprise networks.
* Regularly patch and update SCADA systems.
* Establish a Security Operations Center (SOC) for monitoring and managing security incidents.

**Impact Analysis**

Operational Efficiency: Enhanced process effectiveness will reduce downtime and improve product quality.

Revenue Stability: Downstream operations provide a buffer against fluctuations in commodity prices.

Market Position: Expanded operations and technological advancements will strengthen COMPANY B's competitive position.

Innovation and Technology: SCADA system enhancements and robust cybersecurity measures will improve operational resilience and reduce vulnerability to cyber threats.

**Out of Scope**

Upstream production and exploration activities.

IT expenditures unrelated to SCADA or cybersecurity.

Non-manufacturing or refining-related systems or processes.

Risk and Mitigation

Market Volatility:

**Solution 2: Renewable Energy Implementation**

**High-Level Design**

**Develop Renewable Energy Infrastructure:**

Objective: Transition to renewable energy sources for power generation.

Components: Invest in hydroelectric, wind, and solar power plants.

Dependencies: Collaborate with renewable energy companies and secure government approval.

**Energy Storage Systems:**

Objective: Store surplus energy for later use.

Components: Install battery storage systems.

Dependencies: Partner with energy storage suppliers.

**Grid Integration:**

Objective: Integrate renewable energy sources with the existing electricity grid.

Components: Upgrade grid infrastructure to accommodate renewable energy.

Dependencies: Collaborate with grid management specialists.

**Monitoring of Renewable Energy:**

Objective: Track and manage renewable energy generation.

Components: Implement AI and SCADA systems for real-time monitoring and maintenance.

Dependencies: Train personnel to operate new systems.

**Regulatory Compliance:**

Objective: Ensure adherence to all relevant regulations and secure incentives.

Components: Apply for permits and comply with environmental regulations.

Dependencies: Consult with legal and regulatory experts.

**Social Acceptance:**

Objective: Engage with stakeholders and communities to gain support.

Components: Conduct community outreach and awareness campaigns.

Dependencies: Partner with local associations and stakeholders.

**Low-Level Design**

Solar Power Plant: Site selection, panel installation, and grid connection.

Wind Turbines: Site selection, turbine installation, and grid integration.

Hydroelectric Infrastructure: Develop small-scale, environmentally friendly hydro projects.

Energy Storage: Install and integrate battery storage systems with renewable energy sources.

Grid Modernization: Implement smart grid technology and enhance grid capacity.

SCADA Systems: Install real-time monitoring and predictive maintenance systems.

Impact Analysis

Environmental Impact: Reduced carbon footprint and support for sustainable energy.

Energy Security: Increased energy independence and resilience against market fluctuations.

Regulatory Compliance: Access to government incentives and avoidance of penalties.

Community Engagement: Improved public perception and stakeholder support.

**Out of Scope**

Non-renewable energy sources.

Infrastructure unrelated to renewable energy.

Existing SCADA systems and processes.

Risk and Mitigation

High Initial Costs

**Solution 3: DO - NOTHING with Existing SCADA Systems**

**High-Level Objective**

Objective: Maintain the current Supervisory Control and Data Acquisition (SCADA) systems and processes without implementing any significant changes or upgrades.

Existing Hardware: Continue using all current hardware devices, including servers, end-user devices, data storage, and networking equipment.

Existing Software: Maintain existing software applications without upgrades or new cybersecurity and AI updates.

Data Management Practices: Continue with the current data management, backup, and recovery processes.

**Impact Analysis**

Positive Impacts:

Cost Savings: Avoid immediate capital investments in new hardware, software, or training.

Operational Stability: Maintain current operational stability without disruptions from new implementations.

Resource Focus: IT and operational staff can concentrate on maintaining existing systems.

Negative Impacts:

Unresolved Inefficiencies: Persisting inefficiencies may impact productivity.

Scalability Issues: Inability to scale operations effectively, leading to potential bottlenecks.

Competitive Disadvantage: Risk of falling behind competitors who invest in advanced technologies.

Increased Maintenance Costs: Aging hardware and software may increase maintenance costs and risk of failures.

Data Security Risks: Older systems may lack the latest security patches, increasing vulnerability to cyber threats.

**RECOMMENED SOLUTION : Downstream Integration with SCADA and Cybersecurity**

**1. Comprehensive Approach to Business Expansion:**

Solution gives a solid foundation to move COMPANY B to downstream activities that straight answer the company’s current strategic direction of diversifying revenue sources and lessening fluctuating income. Through the establishment of manufacturing structures of petroleum products and incorporating them with the upstream ones, COMPANY B can efficiently address the challenge of resource usage and break the market risks hence strengthening its position in the market.

**2. Technological Integration with SCADA Systems:**

The new downstream processes require the integration of SCADA systems in their control and management. This solution is not only useful for the real-time control of processes but also develops a coordinated system that encompass both the upstream and downstream process. The extra layer of redundancy and failover capabilities guarantee that COMPANY B’s operations are effective and continuous with little risks of disturbances to its operation.

**3. Robust Cybersecurity Framework:**

Considering that threat to industrial control systems is on the rise, the focus on cybersecurity in Solution is essential. With firewalls, IDS, secure communication protocols and with the separation of the SCADA network, the COMPANY B will be secure from cyber threats. The creation of an SOC enhances the organisation’s capacity to identify and contain security threats as promptly as possible to protect operations and maintain compliance with the industry.

**4. Impact on Operational Efficiency, Revenue Stability, and Market Position:**

The integration proposal is expected to improve operational efficiency since the need for spare parts will be eliminated, raw materials will be of high quality, and finished goods will take lesser time in the market. The downstream operations will serve as a hedge to COMPANY B in that it will be able to receive regular and predictable cash inflows from the sale of its commodities. Also, the implementation of new SCADA systems as well as the use of strong cybersecurity measures will ensure that COMPANY B ranks among the most technological companies within the industry.

**5. Alignment with Long-Term Strategic Goals:**

Solution is well-aligned with COMPANY B’s long-term strategic goals of expanding its operations, increasing technological capabilities, and ensuring market leadership. The holistic approach of this solution addresses multiple facets of the business—operational efficiency, technological advancement, cybersecurity, and market positioning—making it a comprehensive and future-proof strategy.

This solution offers a balanced approach to addressing COMPANY B's needs for growth, efficiency, and security. It provides a clear path to achieving downstream integration while leveraging advanced technologies like SCADA and robust cybersecurity measures. The combination of these factors makes Solution the most viable and strategic choice for COMPANY B’s future development.

# Transition Requirements

### Current State Assessment

The first of them entails a rigorous making of an assessment of the current status of downstream refining, processing and distribution network. This assessment will also carry out a status check of the existing IT systems with special emphasis on the integration of the upstream and downstream activities. Also, a gap analysis on the current cybersecurity assessment will be done especially concerning OT since the recommendation looks at enhancing the existing architecture.

### Stakeholder Engagement

This means that it is important to engage stakeholders in the right manner so as to ensure that the process of transition that is to be implemented will be successful. Main interested parties which include operational managers, IT personnel, cybersecurity personnel, and SCADA vendors will be determined. Seminars and conferences will be conducted with the purpose of taking requirement information, responding to concerns, and adjusting stakeholders to the project. Stakeholders will always be in touch through proper communication structures so that they are able to keep on giving feedback as the transition progresses.

### Infrastructure Development

There will be a proper course of action when talking about downstream development that will require enhancement of refining units, pipelines as well as other crucial equipment. The construction and installation will be done in phases due to the functionality of the complex as construction is going on there will be limited interruptions to the working of the complex. Another peculiarities include the fact that all the developments in infrastructure should be designed to be acceptable for integration with SCADA systems.

### SCADA System Integration

In regards to downstream operations, the incorporation of SCADA systems will be done systematically. To monitor and control refining, processing and distribution business activities, SCADA systems will be employed. Also to enhance good flow of data from the upstream operations to downstream operations efficient data management system will be developed. The integration will first undergo some test in realism to prove the compatibility and functionality before going for broad deployment.

### 

### Cybersecurity Enhancements

Improving matters of security is one approach that needs to be adopted in the transition. The cybersecurity strategy will be improved as to provide high levels of protection for SCADA systems and critical infrastructures. Software that enables monitoring in real time and intrusion detection systems will be adopted, together with incident handling plans. Vulnerabilities and risks review and penetration testing shall be done on regular basis in order to reduce the threats. Furthermore, measures in regard to the staff shall include conducting of seminars aimed at the promotion of cybersecurity measures in relation to SCADA systems as well as other important operational data.

### 

### Training and Change Management

A set of organisational SCADA and Cybersecurity training modules that will be implemented to train operating staff is as follows: Stakeholder management support will be given in terms of creating awareness to the staff to embrace new system and processes that are to be put in place. A helpdesk or a support team will be made available to supply help in case of difficulties during the changeover process.

### Testing and Validation

Prior to rolling out the full application, extensive trials of the new infrastructure, SCADA systems and protective layers to cyber threats shall be made. It will check the compatibility between SCADA and the upstream and downstream processes which will be integrated with it. The reliability of the SCADA systems with regard to redundancy and failover will also be proven to ensure that the SCADA system will keep on operating in the event of such a failure.

### Deployment and Go-Live

Implementation of the new infrastructure and the SCADA systems shall therefore be done systematically with time lines, organized resources and backup options to be issued. The first phase of implementation will therefore be the selection of some pilot sites followed by implementation across all operations. Health care will carefully observe the performance of new systems, during the initial deployment period, and any problems encountered will be corrected to enhance successful implementation.

### Post-Implementation Support

The new infrastructure and SCADA systems to be implemented shall be followed by support and maintenance after the go-live phases. A constant surveillance of Cyber threats will be conducted to ensure security threats are apprehended and eradicated as early as possible, with upgrades to the security measures as and when new threats are identified. Stakeholders and the staff will be asked to provide their opinions on the operations in order to find out areas that need further enhancement and enhancements of the systems.

### Documentation and Reporting

Records of all the activities, setting and alterations that will have taken place through the change process will be documented. For stakeholders’ information, updates on the transition process, activities, and accomplishments and issues encountered along the way will be made available on a regular basis. These records will be on-going and readily retrievable after the transition for easy update and as per the audit then and there.

**Database Design**

A computer screen shot of a computer

Description automatically generated

This database schema is intended to manage and streamline the supply chain and production process in a manufacturing context. It includes suppliers, raw materials, refinement processes, products, SCADA sensor devices, distribution locations, and shipments. The schema ensures that raw materials are tracked and managed efficiently from suppliers to final product distribution, and it also incorporates SCADA technologies for real-time monitoring and security. Each entity is linked by well-defined relationships, allowing for seamless data flow and operational oversight across the full production and distribution network.

**PROCESS FLOW**



The above image shows a flow chart of the production process and supply chain of a petroleum refinery, starting with the procurement of inputs from suppliers. The previously mentioned raw materials are stored and treated in a way that produces the necessary quality for refining. However, the items acquired during the second phase are stored and maintained as completed goods. A shared database is used to collect and store data throughout refining, resulting in a continuous database with control settings that can be monitored and adjusted as needed. Quality control checks are done to make sure that items are created to standard because quality is a crucial component of product production. The distribution center gets ready for the final or refined items to be shipped to various locations before arranging for road transport or another method of delivery to the production sites. All of these products are then sent to the consumer market and purchased by customers. In this way, the entire petroleum product production and distribution process is made thorough, efficient, safe, and of the highest caliber.

**ROI Calculation**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Year 1**  **(in million)** | **Year 2**  **(in million)** | **Year 3**  **(in million)** | **Year 4**  **(in million)** | **Year 5**  **(in million)** |
| **Revenue Increase** | $30 | $33 | $36.30 | $39.93 | $43.92 |
| **Operational Costs** | $5 | $5.25 | $5.51 | $5.79 | $6.08 |
| **Net Revenue** | $25 | $ 27.75 | $30.79 | $34.14 | $37.85 |

**Total Net Revenue Increase:** $25 + $27.75 + $30.7875 + $34.14 + $ 37.85

= $ 155.52 million

**ROI: (Total Net Revenue Increase – Initial Investment) / Initial Investment \* 100**

= ($ 155.52 million - $ 80 million) /80 million \* 100

= 94.41%

**Summary:**

**Initial Investment**: $80 million

**Total Net Revenue Increase Over 5 Years:** $155.52 million

**ROI Over 5 Years: 94.41%**

**Assumptions:**

Initial Investment Costs:

Downstream Infrastructure: $50 million

SCADA System Deployment: $20 million

Cybersecurity Enhancements: $10 million

Total Initial Investment: $80 million

Expected Revenue Increase: Due to improved operational efficiency, increased refining capacity, and better data management and security, let's assume a conservative annual revenue increase of $30 million for the first year, with a 10% yearly growth in this increase due to scaling and optimization.

**Risks Log**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk ID** | **Risk Description** | **Severity/Impact** | **Probability of Occurrence** | **Mitigation Strategy** |
| R1 | Market price fluctuations affect profitability levels. | High | Medium | Utilize financial risk mitigation strategies, stress testing, and cautious budgeting. |
| R2 | Business risks associated with new refining schemes. | High | Medium | Enhance safety measures, enforce a strict safety code, ensure routine checkups, and train staff thoroughly. |
| R3 | Cyberattacks are disrupting SCADA system operations. | Very High | High | Implement robust cyber defences, conduct regular penetration tests, and have coordinated responses to security incidents. |
| R4 | Noncompliance with industrial and environmental standards. | High | Medium | Ensure ongoing compliance through regular analyses and implementation of required regulations. |

**Testing Strategy**

**STAGES OF TESTING:**  
**Unit Testing**: Verify each control system segment and security enhancements against other segments independently. Ensure that each of the pieces runs standalone.  
**Integration Testing:** Look at how the elements of the control system link with security procedures. Ensure that each one is optimizable when linked together for the whole system's efficiency.  
**System Testing:** The last activity requires the complete testing of the downstream system with control and security. Ensure the system provides all the necessary functions listed and must meet standard provisions.  
**User Acceptance Testing (UAT):** Use end-users in the tests to ensure that the developed system will suit their requirements and expectations. Gather their comments and, if necessary, make some modifications before the product is released.

**DEFECT HANDLING:**  
**Defect Logging:** The following is a checklist of all problems that can be identified during testing: Organize the issues in terms of severity and the time of their solving by urgency.  
**Defect Resolution:** Ensure people are put in a position to solve the problems by assigning them to personnel with the relevant skills to solve them. Check their performance and ensure they complete those cases on time.  
**Defect Retesting**: Once again, sit for the fixed problems to ensure they are well solved. Moreover, more tests should be performed to see if new issues interfere with the phone’s processes.  
  
**SIGNOFFS REQUIRED:**  
**Exit Criteria for Each Stage:** After defining each testing phase, determine when each testing phase is done. Ensure that all the critical issues with the current phase are addressed before proceeding to the next phase.  
**Final Signoff:** Obtain sign-off from crucial opinion leaders before the more extensive implementation. Ensure that every testing document has been written and adequately completed.

**Implementation Strategy**

**PHASE 1: PLANNING AND PREPARATION:**

**Evaluate the current infrastructure:** Pay particular attention to how current systems are employed for the organization and regulate company activities following the primary production line. This also implies inspecting the computer systems and supervising and regulating such operations remotely. Discover gaps in these systems and where something is lacking or going wrong. As a result, determine which elements require enhancement or substitution with superior technology.  
**Developing Project Plan:** This will then entail developing a schedule for the project, which will indicate when things should be done and what needs to be completed by then. Choose a team to manage the project and state the roles of each team member.  
**Allocating Resources:** Decide what is required for the project & get equipment, software, staff & other requirements related to the project. Seek the budget's approval and ensure all the necessary funds are available.

**Stakeholder Engagement:** Ensure that relevant people are involved in the project from the onset so that they all buy into it. Convey the objectives, updates, and any alterations that concern the project to the people involved frequently.

**PHASE 2: PILOT TESTING AND INITIAL ROLLOUT**

**Pilot Deployment:** You should test the improved control system and security upgrades on one device before implementing them on all the others. To use everything carefully, it is essential to do tests to ensure it is functioning well and safe.  
**Monitoring and Feedback:** Pay attention to whether the system operates as required and consolidate the testimonies of ordinary and influential people. Perform some corrections depending on what is obtained from the pilot test that is likely to be done.

**PHASE 3: STEADY GROWTH**  
**Incremental Rollout:** Gradually expand the system to the other stores by applying the lessons from the pilot. It is important to perform tests and check on the system at the various stages.  
**Training and Support:** Defend and increase the training frequency among the staff in each new location so they can fully utilize the latest systems effectively. Follow up with various types of assistance to solve operational issues that may arise.  
  
**PHASE 4: COMPLETE IMPLEMENTATION AND ENHANCEMENT**

**Complete Rollout:** Take full system commissioning at all places as planned earlier. Check that all components are properly functioning and that they are correctly linked.  
**Optimization:** Continue observing how the system is working and improve the operations. The process also needs to ensure that there are mechanisms for receiving feedback to facilitate constant improvement.  
  
**BACKOUT STRATEGY:**  
**Fallback Plan:** Some larger-scale countermeasures can be developed to switch back to previous instruments and techniques when critical issues occur. Ensure backup systems are available and functional if needed.  
**Continuous Monitoring** is crucial in all process stages to prevent adverse incidents. Minimize interruptions by identifying issues promptly and solving them as soon as possible.  
  
**REQUIREMENTS FOR RESOURCES:**  
**Client-Side Resources:** A team manages the project, and a project manager coordinates it. They are the individuals who understand how to establish and rectify the structures—cash to be used for purchasing equipment and computer software.  
**Training Effort and Timing**: Sensitization and capacity building of the Behavioral Centers’ staff at the beginning of Phase 1. A reinvention workshop for anyone who may have forgotten or has not been in contact with these skills during the duration of each of the rollout phases. Extra classes when needed and the opportunity to take more courses as a part of our education.