THE PHILODRILL CORPORATION
Enterprise Risk Management Framework

Enterprise Risk Management (ERM) is a process, affected by Philodrill's Board of Directors, Management, and other personnel. This process is applied in strategy setting and across the Company, designed to identify potential events that may affect the company, and manage risks to be within its appetite.

ERM provides reasonable assurance regarding the achievement of the Company's objectives. Philodrill can identify, assess, respond and monitor the outcomes of the industry's leading risk factors with an Enterprise Risk Management system in place.

Risk management is an integral part of day-to-day business activities in the energy industry. Oil and gas companies face risks ranging from volatile commodity prices, which are less linked to basic supply and demand but more to global socioeconomic factors, to increased health, safety, and environmental pressures resulting from past and recent major accidents negatively impacting the environment, industry image, and its social lease.

However, risks related to asset damage, business interruption, pollution, injuries to people, and damage to properties are intrinsic in normal oil and gas activities. Then there are the additional risks of non-compliance and of major cost overruns for large construction projects so common in today's industry. Consider also some cyber threats targeting oil and gas companies in the Middle East. These are just a few examples of the serious risks and threats that can impact oil and gas companies. Technology can help mitigate these risks.

Philodrill explores the operational risks faced by oil and gas companies in today's business and regulatory environment, and how the right information technology can help mitigate those risks. Operational risk is experienced at the corporate level, but the framework also focuses on what impacts everyday well, pipeline, and plant operations.

According to the IEA's World Energy Outlook, global energy demand will grow by more than a third over the period to 2035, driven largely by rising living standards in China, India, and the Middle East, which together will account for 60% of that increase. At the same time, unconventional resources are changing the global energy map: the IEA forecast that the United States will overtake Saudi Arabia and Russia as the world's top oil producer.

OPERATIONAL RISKS

More Projects, More Complex and More Risks to Manage

In the oil and gas industry, managing capital projects, in particular large capital projects, in a global environment is becoming increasingly complex. This is especially the case as large reserves are being depleted and the industry copes by drilling multiple smaller wells to

compensate. Oil and gas companies need to make strategic decisions about which projects should be developed first to ensure their company's best performance.

The Company and its Management has to make decisions about equipment resources: When is the best time to reserve a rig? Should the decision be based on getting the best rate even if the rig will not be needed at that exact moment? Or should the Company wait until the exact date for a drilling project is known and risk the equipment not being available, or the threat of higher rental rates?

How does an equipment shortage impact planned revenues? Do key decision makers have the ability to review this information and prioritize projects based on equipment resources? The same resource issues are faced for human capital tied to exploration and production (E&P) projects. Are the appropriate teams in place for a project, or has an unexpected failure at another location impacted the project? As a result, the project portfolio needs to be dynamically managed as a process, in which the list of projects can be constantly revised, and new projects evaluated, selected, and prioritized based on parameters of importance to the company such as level of risk, expected return on investment, EHS considerations, etc.

Existing projects can be accelerated, stopped, or reprioritized, and resources can be allocated and reallocated to the most appropriate active projects as needed.

Operational Complexity

The oil and gas industry is operating in increasingly remote geographical locations and harsher environmental conditions, with unconventional processes to extract hydrocarbons. Joint collaboration between large producers on risky international exploration and production (E&P) projects is common. Articulated E&P sharing agreements with multiple stakeholders need to be managed. High rates of non-productive time require action, and overall equipment efficiency needs to grow. Ultimately, companies share the same primary goal of needing to produce hydrocarbon as efficiently and cost effectively as possible. One strategy for achieving this has been the adoption of a "digital oilfield" or "integrated operations" to enhance reservoir recoverability, optimize production, and reduce economic, environment, health, and safety risks. This strategy is focused on accessing and managing key asset-related data to improve decision making across the entire industry.

Shortage of Experts

A shortage of expert resources is not new to the industry. This problem has existed for several years. Shortages are mainly in the highly technical areas such as geology and geophysics and petroleum engineering. In some geographies there is also a shortage of IT personnel with expertise in some of the more complex information technologies, such as high-performance computing (HPC), used to support analysis of large volumes of scientific and engineering data in exploration and production.

Cyber Security: Expanded Boundaries of Vulnerability

The industry has always been involved in efforts related to critical infrastructure protection. However, with the progressive digital evolution toward smart oilfields and refineries of the future, IT and OT security has been receiving greater attention. Concerns were originally raised about the security of process systems with the revelation that the highly sophisticated virus is capable of invading process control systems, and potentially disrupting processes by invading control systems on drilling rigs and in the refinery. The cyber attacks on Saudi Aramco and RasGas were a huge shock for many oil and gas organizations in the Middle East region. The world's largest oil-producing company, Saudi Aramco, was the victim of a significant cyber attack on August 15, 2012. The oil giant announced that 30,000 of its workstations had been infected by a virus. Moreover, on August 27, Qatar's natural gas pumper, RasGas, was hit by a similar attack, resulting in the company being taken offline for a few days. A group of hackers calling themselves the Cutting Sword of Justice claimed responsibility for the attack on Saudi Aramco. They allegedly infected the organization's systems with replicating malicious software (malware) for political reasons. Some IT analysts credit a virus called Shamoon for both attacks. Both Saudi Aramco and RasGas managed to limit the damage, as the attacks did not affect extraction or processing, but such a bold attack had important repercussions on the IT strategies of oil and gas organizations operating in the Middle East, demanding new projects on risk assessments, new IT security policies, and the adoption of additional security solutions.

WHAT TO DO TO HANDLE OPERATIONAL RISKS

Access and Visibility: Right Information at the Right Time

Most oil and gas companies would agree that the most significant challenge for their enterprise is management of information. Oil and gas companies continue to work to be able to create intelligence from the massive amount of technical and business data, both structured and unstructured, that they have collected. The ultimate goal in collecting all this information is to speed time to first oil, reduce risks, and meet compliance requirements with information life-cycle management. Some companies are establishing new information governance structures to harness Operational Technology and Information Technology data sources. At the same time, information needs to be shared in a secure manner with multiple partners to speed time to oil and lower EHS and economic risks.

Timely access to all relevant information is critical in case action is needed following catastrophic events. In order to reduce response time, oil and gas companies need to ensure immediate distribution of all relevant materials to all interested parties. Moreover, timely, contextualized, and consistent information is the basis for effectively implementing standard operating procedures, essential to cope with continuous changes in people and teams working on the assets.

When it comes to information related to assets the issue of data quality hits oil and gas companies. These are typical issues:

- Asset databases are incomplete
- Documents (including drawings) are not updated
- Information stored in the different company systems are not consistent or integrated
- Information is not available or not properly synchronized on mobile devices
- Data quality is not systematically audited. Poor data quality heavily impacts the decision-making process, increasing the risks of operational mistakes. Oil and gas companies need to carefully tackle this issue to avoid reducing effectiveness of operations. Additionally inconsistent data across systems increases the risk of fines from regulators.

Prevention of Non-Compliance

With the increasing regulatory pressure, oil and gas companies cannot afford the risk of being non-compliant. More stringent requirements for timely reporting on operations and accidents might be required, as well as risk mitigation plans for critical operations such as drilling. Philodrill ensures that vital documents, including approvals for drilling, building, and maintaining wells, are available throughout the enterprise and across enterprise boundaries to minimize risk and ensure regulatory compliance.

Environmental, Health and Safety (EHS) systems include a broad set of applications and technologies that cater to the EHS business needs of the oil and gas industry. Primarily, these systems automate the management of structured and unstructured EHS data and facilitate the necessary flow of EHS-related compliance actions, such as inspections and reporting. More sophisticated systems include enterprise operations risk management applications that aid with asset and worker safety. EHS technologies also refer to instrumentation and supporting software that aid with measurement and remediation activities related to ground, water, and atmospheric leaks. GIS and GPS systems, as well as preventive asset management, play an important role in promoting EHS initiatives.

Holistic Approach to Operational and Enterprise Risks

Operational risks are a key component of overall enterprise risk management, and information plays a key role in reducing them. Oil and gas companies, like any other capital-intensive business, need to take strategic, operational, and tactical decisions about their assets, whether they are resources, reserves, wells, plants, or facilities. Often there exists a disconnect between the tactical and the strategic levels.

The strategists do not have visibility into costs and efficiencies across the portfolio of assets. Also, well/plant-level decisions are made based on the perspective of the individual plant or asset and these decisions may not support the profitability goals set at the corporate level. This disconnect negatively affects the company's ability to handle risks. Technology can help reduce disconnect with analytics and governance, risk, and compliance (GRC) applications, which automate and document processes pertaining to the definition, assessment, and verification of business controls and operational risk at the corporate level. Enterprise GRC software includes

financial compliance management, audit management, corporate policy and procedure management, risk management, and continuous enterprise controls monitoring.

Real-Time Monitoring and Predictive Maintenance to Prevent Incident Failure or Non-Productive Time

The upstream industry has adopted many of the same techniques to improve capital asset management. The company use a variety of techniques to reduce maintenance costs, increase uptime, and increase availability. These techniques include:

● Condition-based monitoring. Placement of sensors to measure various conditions (temperature, vibration, etc.) to detect situations that may indicate potential equipment failure. The more sophisticated systems have alerting capabilities and are integrated with enterprise asset management applications that can automatically generate inspection or work orders.

● Predictive maintenance. Predictive maintenance goes beyond condition-based maintenance in applying advanced analytics to predict potential equipment failures, providing enough notice to procure complex non-commodity replacement equipment. The algorithms identify a departure from normal operating levels of a piece of equipment rather than comparing performance with expected performance levels for the equipment class.

● Criticality-based maintenance. This technique informs decisions on maintenance strategy by identifying which assets are critical to the process and what the process impacts would be if the asset were to fail. Criticality-based maintenance also informs procurement strategy so that inventories, and the costs associated with keeping them, are reduced but not at the expense of increased downtime.

● Performance center or center of excellence. The Company intends to adopt centers of excellence where engineering staff are able to bring together engineering knowledge for root cause analysis when potential problems are identified. Centers of excellence can also have a view of multiple assets to support decision making and maintenance planning and even suggest future equipment design modifications.

Collaborative Planning, Operations and Decision Making

To reduce non-productive time, enhance production, and reduce both economic and EHS risks, the Company is creating a stronger and more comprehensive connection between field operations staff and remote experts. This connection involves:

● Collaboration. The ability for multiple parties to visualize and analyze the same set of data and information from disparate locations.

● Workflow. Rationalizing data to make it automatically available to personnel and applications according to role-based need.

● Access to real-time data. Surface and subsurface to improve production, often involving sensors. This is often accomplished through collaboration rooms accessible from multiple locations, both on-rig and off-rig. Visualization can be 3D or 4D and, depending on the data, is most effective with a geospatial overlay.

Cyber Security Policy Design and Execution

One of the most basic elements to guarantee information security is to have an enterprise information security architecture applied to all the data, systems, processes, and people. It is imperative to be able to track from the business strategy to individual security technologies.

Information technology can help mitigate operational risks. Organizations that understand their risk profile and take concrete action to mitigate risks will be better positioned to be successful in the marketplace. It is therefore recommended that the following should be practiced:

● Consider developing a corporate wide approach to managing information in the plant. Best practices cover use of technology to support operations, business analytics, application integration, EHS compliance, and enterprise content management.

● Work to develop business processes for operations and identify document control workflow for approvals within the organization, including the transmittal and standard operating procedure (SOP) processes. Determine how often you wish to share documents with vendors, partners, regulators, and others. Work together to develop a coding standard for components/documents to ensure that there is consistent master data management.

● Participate in industry associations and user communities to help arrive at standards for sharing of content and supporting well and plant workflows.

● Look to areas of high vulnerability in your operation such as current processes that still rely on paper files that can potentially be difficult to find and update and may be misfiled or lost and ultimately expose your company to regulatory or internal audit failures.

● Focus on process improvements that will allow more effective creation and sharing of content both inside and outside the firewall. A good area to start would be the transmittal and SOP processes.

● In this time of increased regulatory pressure, look at solutions that optimize the way you manage, share, store, and archive content to comply with environmental, health, and safety regulations.

● Look at deploying information rights management tightly integrated with content management to ensure that only authorized recipients can view, copy, print, or edit confidential information.

● Reassess your customer communications capabilities to ensure timely and personalized correspondence tailored to the delivery requirements of the recipient, including customers and regulatory agencies.

● Take a more holistic approach of your asset information to ensure that drawings, records and other documentation are properly identified, stored, classified, accessible, accurate, and appropriately safeguarded.

● Familiarize yourself with emerging asset management standards such as PAS 55 and ensure that future asset management solutions that are deployed in your company operations adhere to such standards.

● Evaluate solution vendors that have the flexibility to support mobile access of project and plant information, which enables and optimizes access of information wherever it is accessed.

● Consider solutions that provide options to deploy cloud-based solutions and can support projects that require cloud deployments.