Enterprise Risk Committee Charter

RigNet

Purpose

The purpose of the Enterprise Risk Committee (ERC) is to assist the CEO and CFO in fulfilling their responsibilities to oversee the Company's enterprise-wide risk management. The Enterprise Risk Committee (the "committee") is established by RigNet to oversee management activities related to risk oversight and risk management.

Authority

The Enterprise Risk Committee will report to CEO and CFO. In carrying out its duties and responsibilities, the committee shall have the authority to meet with and seek any information it requires from employees, officers, directors, or external parties.

The committee may request any advice/assistance from other departments for any matters and projects within its scope of responsibility and obtain advice and assistance from outside legal, accounting, or other advisors, as necessary, to perform its duties and responsibilities.

The committee will have the following authority;

- Review and approve the Enterprise Risk Committee Charter.
- Overseeing that the executive team has identified and assessed the major risks that the organization faces and has established a risk management infrastructure capable of addressing those risks categorized in the following six

categories;

1. Strategic Risk
2. Financial Risk
3. Operational Risk
4. Legal & Compliance Risk
5. Corporate IT/Systems Risk
6. Service Provider IT/Systems Risk

- Review the company's enterprise-wide risk management framework.
- Review Enterprise Risk Management Plan
- Overseeing the division of risk-related responsibilities to applicable committee members, or other designees, as clearly as possible and performing a gap analysis to determine that the oversight of any significant risks does not occur.

Composition and Meetings

The committee will be comprised of six or more members of the management team as determined by, and reporting to,the CEO and CFO. The membership will include a combination of management team members from various business functions to ensure good knowledge of risks across the business. Each member will have an understanding of risk management expertise commensurate with the company's size, complexity, and capital structure.

The committee will provide its members with continuing education opportunities and customized training focusing on topics such as leading practices about risk governance, oversight, and risk management.

The CEO and CFO will appoint the initial committee members. The members of the committee may designate a chairperson and a facilitator by majority vote. Additionally, the committee, in conjunction with CEO and CFO, may consider and plan for succession of risk committee members.

The committee will meet at least eight times per year, or more frequently as circumstances dictate. The committee will review the agenda for the committee's meetings, and any member may suggest items for consideration. Briefing materials will be provided to the committee as far in advance of meetings as practicable.

The Enterprise Risk Committee has the responsibilities to:

1. Review the risk management framework.
2. Set the tone and develop a culture of the enterprise vis-à-vis risk, promote open discussion regarding risk, integrate risk management into the organization's goals, policies, and procedures to create a corporate culture such that people at all levels manage risks rather than

reflexively avoid or heedlessly take them.

3. Monitor the organization's risk profile - its on-going and potential exposure to risks of various types (operational
   a. risk, compliance, financial crimes, information security (including cyber), and technology programs (including the Company's business continuity program, compliance risk management program, data management strategy and
   b. program, financial crimes program, and third-party risk management)
4. Monitor various enterprise risks; in doing so, the committee recognizes the responsibilities delegated to other management team members and understands that the other committees or departments may emphasize specific risk monitoring through their respective activities.
5. Conduct an annual risk assessment survey with the executive management. Integrate survey findings into risk assessment and the Risk Management Plan.
6. Develop, review, maintain the Risk Management Plan and provide an update to the CEO and CFO.
7. The Risk Management Plan should consider the maturity of the risk management of the company and should be tailored to the specific circumstances of the company. The risk management plan should include:
   i. Company's definition of risk and risk management. Refer to Appendix A: Definitions & B: Risk Rating
   ii. Company's risk, risk appetite, risk tolerance, risk mitigation plan, and risk acceptance.
   iii. Indicate how risk management will support the company's strategy and ownership for risk management within the company.
   iv. Define the company's risk management structure such as defining risk roles and responsibilities across the Company's three lines of defense for establishing protocols and processes for issue escalation and reporting.

- 1st Line of Defense: Operations Managers and Department Heads, Executive Leadership Team, Policy Committee, Internal Controls Committee, Global Expansion Team, 401K & Compensation Committee.
- 2nd Line of Defense: Enterprise Risk Committee, Disclosure Committee, Legal and Compliance Committee, ELT Meetings, RigNet Connect.
- 3rd Line of Defense: Blackline SOX Controls Review and Internal Audit

   v. Define the standards and methodology adopted – this refers to the measurable milestones such as tolerances, intervals, frequencies, frequency rates, etc.;
   vi. Risk management guidelines; Continually, as well as at specific intervals, monitor risks, and risk management capabilities within the organization, including communication about escalating risk and crisis preparedness and recovery plans
   vii. Continually obtain reasonable assurance from management that all known and emerging risks have been identified and mitigated or managed. Update the risk management plan accordingly.
   viii. Provide training and awareness programs

8. The committee should review the risk management plan at least once a year.
9. Review and approve minutes of the previous Enterprise Risk Committee Meeting.
10. Define the agenda for the next Enterprise Risk Committee Meeting based on the current environment within the company, risk assessment, risk mitigation plan and action item due dates.
11. Understand how the company's internal audit work plan is aligned with the risks that have been identified and with risk governance (and risk management) information needs
12. The Committee shall review and assess the adequacy of this Charter annually. The Committee may

recommend amendments to this Charter at any time and submit amendments for approval.

13. The Committee shall annually review its own performance.

Reporting

The committee will be responsible for the following reporting duties.

- Communicate formally (on a quarterly basis) and informally (as needed) provide an update to the executive team, CEO, CFO, and the Corporate Governance Nomination Committee of the Company's Board of Directors about company's risk management plan regarding risk governance and oversight.
- Understand and review management's definition of the risk-related reports that the committee could receive regarding the full range of risks the organization faces, as well as their form and frequency.
- Respond to reports from management so that management understands the importance placed on such reports by the committee and how the committee views their content.
- Discuss with the CEO and management the company's major risk exposures and review the steps management has taken to monitor and control such exposures, including the company's risk assessment and risk management plan.

Finalized in the Enterprise Risk Committee Meeting on 7/24/2018.

APPENDIX A: Definitions

- Risk: "A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action."
- Risk appetite: "Risk appetite can be defined as 'the amount and type of risk that an organization is willing to take in order to meet their strategic objectives." A range of appetites exist for different risks, and these may change over time.
- Risk tolerance: "A realistic understanding of the company's ability and willingness to accept or avoid risk." In any group of people, there are gamblers or risk takers, and there are nongamblers or risk avoiders.
- Inherent Risk: "Inherent risk is the threat a certain risk poses to the organization before mitigation activities are taken into account."
- Residual Risk: "Residual risk is the threat a certain risk poses to the organization after the appropriate mitigation activities are taken into account."

APPENDIX B: Risk Rating

Risk Rating		
High	1	Financial Loss > $1 MM
	2	Stakeholder faith impacted and lasts >12 months.
	3	International Negative Media coverage, game-changing loss of market share
	4	Significant Injuries or fatalities to employees or third parties, such as customers or vendors.
	5	Multiple events of fine, fraud or legal action
	6	Complete system crash with loss of critical data
	7	Inability to recruit and/or retain staff to operate
	8	Multiple senior leaders leave
Medium	1	Financial Loss < $1 MM
	2	Stakeholder faith impacted and lasts >6-12 months. Negative Media coverage, game-changing loss of market share
	3	National short term media coverage.
	4	Out-patient medical treatment required for employees or third parties, such as customers and vendors.
	5	Isolate incident of fine, fraud, or legal action
	6	System crash during a peak period
	7	Difficulties in recruiting and retaining staff
	8	Labor disruptions that impacts operations of any duration
Low	1	Financial Loss < $500,000
	2	Stakeholder faith impacted and lasts < 6 months.
	3	Local Media attention quickly remediated
	3	No injuries to employees or third parties, such as customers or vendors
	4	Civil or criminal action threatened.
	5	Insignificant or not reportable to regulators. Immaterial minimal fines or penalties.
	6	System off-line periodically during non-peak periods
	7	Isolated staff dissatisfaction
	8	No labor disruptions that impacts operations of any duration
Each risk identified for RigNet needs to be categorized within above 3 buckets