Corporate Risk Management

Policies and Procedures

Last Updated : Dec 2013

Document History and Version Control Table			
Version No	**Author**	**Effective Date**	**Change Summary**
5.00	HR Team	Dec 2013	Risk Committee
4.00	HR Team	Jun 2012	Policy Authority
3.00	HR Team	Jan 2012	Staff
2.00	HR Team	Jun 2011	Risk Management Expectation
1.00	HR Team	Jan 2010	Initial Version

Contents

1. Policy Purpose and Scope

This policy describes NeoBytes' risk management principles and expectations applicable to all types of risk in all activities undertaken by or on behalf of NeoBytes. It also outlines roles and responsibilities for the Board of Directors, the President, the Chief Risk Officer and the Divisional Vice-Presidents of Corporate Groups across all geographies where NeoBytes operates, and all staff.

2. Risk Management Principles

2.1 Definition of Risk

Risk is often defined as the chance of something happening, measured in terms of probability and impact. At NeoBytes, a principal risk is defined as the chance of something happening, measured in terms of probability and impact, that may adversely affect the achievement of NeoBytes' strategic or major business objectives. For example, project standards are based on expected numbers of defects. If more defects are received for a particular project work, overall project delivery will fall unless resources are augmented to assist. Conversely, if the defect counts are lower than expectation, there is an opportunity to improve customer service and relations. Hence risks represent opportunities as well as threats.

2.2 Risk Management

Risk management is a structured and disciplined approach to assessing and managing the uncertainties that NeoBytes faces as it creates value and preserves value.

NeoBytes believes risk taking is a necessary and accepted part of our business. Effectively managing risk is a competitive necessity and an integral part of creating value through good business practices designed to ensure that NeoBytes achieves its strategic, business and governance objectives, and protects its corporate reputation, values and integrity. In the context of realizing strategic objectives, some amount of failure is an accepted outcome of risk taking as long as risks have been properly assessed and managed.

NeoBytes acknowledges that all activity has an element of risk and that not all risks can or should be transferred. NeoBytes is committed to managing risks including strategic risks, at all

levels in the organization and summarizes these risks into three broad categories:

- Operational risk
- Financial risk
- Safety, Environmental and Regulatory risk

Since many risks can impact our reputation, all risks must be evaluated in terms of the potential impact on our reputation.

NeoBytes does not engage in speculative activity which is defined as a profit-seeking activity unrelated to NeoBytes' primary business.

3. Risk Management Expectations

Risk management applies to and will be practiced in accordance with NeoBytes' Risk Management Principles as a part of all of NeoBytes' activities including developing strategic plans, preparing operational plans and capital budgets, completing detailed project approval requests, designing and managing project plans, operating NeoBytes' facilities across all geographies, as a part of other management systems and generally, in all decision making processes. NeoBytes' overall risk appetite and risk tolerance will be determined by the President in conjunction with the Senior Management and reported on by the Chief Risk Officer to the Board of Directors.

Risk will be evaluated, managed and documented consistent with guidelines, tools and framework advocated by this Corporate Risk Management Policy and other NeoBytes risk management policies, guidelines or practices such as the Information Security Policy. In all cases, risk will be evaluated in terms of the impact on the following areas:

- People
- Environment
- Assets
- financial/business objectives
- Reputation

The risk will be assigned a probability of occurrence, with a resulting risk level ranging from very low to very high.

Risks identified as very high, high or medium will require implementation of a risk transfer, reduction, elimination, or exploitation strategy to reduce the residual risk level to as low as reasonably practicable. Risks identified as very high or high with an impact above a specified threshold will be reported to the President or appropriate Vice-President of Corporate Groups, and the Chief Risk Officer.

The NeoBytes Risk Matrix is a tool that will be used to assess, measure and report risks. The NeoBytes Risk Matrix may not be readily applied to all risk areas but the concepts of impact and probability must be addressed in all cases. For example, emerging risks are those circumstances or factors which may be new to NeoBytes and may lack quantifiable impact or probability at a particular time. Emerging risks should be separately identified, and qualitative assessments of their impacts and probabilities should be provided.

The NeoBytes Risk Matrix will be the foundation for developing any risk sub-matrices in the Corporation. Sub-matrices will align with the NeoBytes Risk Matrix and will require the approval of the Chief Risk Officer.

Risk management reports will be maintained by Divisions and Corporate Groups and provided to the Chief Risk Officer at least quarterly for consolidation.

4. Risk Management Roles and Responsibilities

4.1 The Board of Directors

- Approving and authorizing the Policy.

- Ensuring that a system is in place to identify the principal risks to the Corporation and that the best practical procedures are in place to monitor and mitigate the risks.
- Reviewing the Chief Risk Officer's consolidated quarterly and annual risk reports that identify the principal risks to the Corporation and the mitigation strategies in place.

4.2 The President

- Identifying all significant risks to the Corporation's businesses and ensuring that procedures are established to mitigate the impact of the risks in the best interest of the company.
- Appointing or recommending the appointment of the Chief Risk Officer, as applicable.

4.3 The Chief Risk Officer

- Identifying the principal risks to the business and ensuring that the Corporation has implemented appropriate systems and effective risk management programs to manage these risks.
- Developing, implementing, monitoring overall compliance with and adhering to the Policy.
- Overseeing development, administration and annual review of this Policy for approval by the Board of Directors.
- Developing and implementing risk management practices, systems, controls and business continuity plans for the Corporation, which are aligned with and complementary to the Policy.
- Developing external risk reporting protocols and disclosures where required by regulation or good governance.
- Reporting to the Board of Directors and the Senior Management NeoBytes' principal consolidated risks and mitigation strategies on a quarterly and annual basis.

4.4 The Divisional Vice-Presidents

- Identifying risks and developing and implementing risk management practices, including mitigation strategies, systems, controls and business continuity plans specific to their respective Divisions or Corporate Groups, which are aligned with and complementary to the Policy.
- Maintaining risk management reports detailing the principal business risks for the Division or Corporate groups and which will be available for consolidation at the Corporate level.

4.5 Staff

- In alignment with the values and principles embodied in NeoBytes' Corporate policies and charter, this Corporate Risk Management Policy commits all staff to consistently apply risk assessment processes and to take professionally assessed risks based upon high-quality work.

5. Risk Committees

The Senior Management; comprised of the President, the Chief Risk Officer and the Divisional Vice-Presidents of Corporate Groups, are collectively responsible for developing the Corporation's risk management principles and risk management expectations as well as defining the Corporation's risk appetite and tolerances, in addition to those specific responsibilities as outlined in Risk Management Roles and Responsibilities referred to above.

Risk management committees may be established by the President from members of Senior

Management to address specific risk areas.

6. Policy Authority

Unless otherwise noted in this Policy, any significant exceptions to this Policy require the approval of Senior Management and these exceptions will be reported at the next regularly scheduled meeting of the Board of Directors.

Appendix A: Risk Identification Steps

Step	Action	Example
1	Identify specific Item of the project's ;,lms, objectives ;,nd t;,rgcts	Execute;, new project for ;,n lnsur;,ncc client, to Implement ;,n end to end policy processing system
2	Identify wh;,t mlaht stop the ;,lms or object ive ort;,rgct from being achieved and describe them In tc nns of ''cvcnt/c< usc'' and ''resu lt'".	l.;)c:k of avall;,blc resources to develop and Implement the project due to availabi lity or difficulties In rccrultin& resources with niche skllllsets
3	For each ''risk'' score Its lmp;,ct and likelihood and prlorltisc ;,ccordlnaly.	lmp;,ct ''medium'' If resources with experience on the system arc busy on another project ;,nd staffing other resources could result In Increased cost/schedule lmp;,ct to the project. Impact could rise to ''high'' If resource shortfall is In *a* niche area where resources arc un-av;,llablc to start on time but able to join at;, later d;,tc ;,nd still do not lmp;,ct the overnll project's cost/schedule. And Impact could rise to ''very hl&h'' If these st01ffina and recruitment problems were more severe with m;,jor lmp;,ct to cost/schedule.
4	Identify mltlaatina actions and Include these In business plans If appropriate. Mitigation should be specific and time limited.	1. Identify any shortfall in numbers of resources required by December. 2. Identify existing experienced resources who can be used on the project by Janu;,ry ;,nd ;,grec to tr;,nsfers ;,nd st;,rt dates with other Project Managers. 3. Initiate recruitment of new staff to fill any remalnlna shortfall by Fcbru;,ry ;,nd plan to h;,vc st01ff In pl;,ce by April. 4. Monitor cost/schedule diligently and *aarcc* on trlgaers that would need any notificat ion to Senior M;,nagcment or Client.
S	Acree risk status ;,fter mltlaatlna ;,ctlon.	Assuming reason;,bly successful staff lna of the project, the probability would fall to ''low''. However, Impact would remain ;,t ''medium'' ;,s this has not been addressed by mitigation.

Appendix B: Risk Probability and Impact settings and scoring

Risk Probability Settings

Probability	Points	Criteria
Very low		0-S"' – extremely unlikely or virtually impossible
low	2	6-20% - low but not impossible
Medium		2150% - fairly likely to occur
High	4	St-80% - more likely to occur than not
Very High		81100% - almost certainly will occur

Risk Impact Settings

Impact	Points	Criteria
Very low		Ukely to have minor impact in one or a few areas
low		Ukely to have minor impact in many areas
Medium		Ukely to have major Impact in one or a few areas
High	4	Ukely to have major impact In many areas
Very High		Ukely to have major impact on the whole company

Probability

Impact \ Probability	Very low (1)	low (2)	Medium (3)	High (4)	Very High (5)
Very ow (1)	Green (1)	Green (2)	Green (l)	Green (4)	Yellow (5)
ow (2)	Green (2)	Green (4)	Yellow	Yellow	Yellow
Medium (3)	Green (J)	(6)			Red (15)
High (4)	Green (4)	(8)		Red (16}	Red (20)
Very High (5)	Yellow (5)	(10}	Red (15}	Red (20}	Red (25}

Step 1: Risk		Step 2: Risk Assessment			Step 3: Risk Management				
No	list of Po:r.sible Risks	Probability VH/H/M/L/VL (5/4/3/2/1)	Impact VH/H/M/L/VL (5/4/3/2/1)	Risk Level Red/Yellow/Green (Probability • Impact)	Mitigating factor:r.	What more can we do about it?	Timescale	Person Responsible	Reviewed Level of Risk