

Figure 1—NSE IT Risk Management Project

Project Step	Outcome
1. Define the risk management framework by considering available global standards.	IT risk framework, risk evaluation criteria and risk response policy
2. Implement the framework uniformly across the IT organization.	Identifying stakeholders and risk champions in each process area (e.g., applications, operations, network, databases, system administration)
3. Conduct risk identification workshops to confirm existing risk and identify new risk.	Risk register for each process area
4. Use framework to assess identified risk and develop risk response options.	Updated risk register and control catalog based on response
5. Build a risk register and link it with the control catalog.	Analyzing risk register and control catalog to identify control gaps
6. Develop a process for risk aggregation and developing the risk profile.	Risk register for the organization and the risk profile, showing inherent, current and residual risk
7. Establish communication channels to communicate the risk profile.	Identifying stakeholders and communicating the risk profile and results of the risk management process
8. Link IT risk management with governance process.	Definitions of key performance indicators (KPIs), key risk indicators (KRIs) and establishment of monitoring process