5. **RISKS IN BANKING**

Risk-taking is an inherent element of banking and, indeed, profits are in part the reward for successful risk taking in business. Risks are considered warranted when they are understandable, measurable, controllable and within a banking institution’s capacity to readily withstand adverse results.

Risk in a banking organization refers to the possibility that the outcome of an action or event could bring adverse impacts on the institution’s capital, earnings or its viability. Banking institutions should attach considerable importance to improve the ability to identify, measure, monitor and control the overall risks assumed.

In order to properly manage risks, an institution must recognize and understand risks that may arise from both existing and new business initiatives.

5.1 **Financial Risk**

**Introduction**

The etymology of the word “Risk” can be traced to the Latin word “Rescum” meaning *Risk at Sea* or that *which cuts*. Risk is associated with uncertainty and reflected by way of charge on the fundamental/basic i.e. in the case of business it is the Capital, which is the cushion that protects the liability holders of an institution.

Risk is inherent in any walk of life in general and in financial sectors in particular. Business grows mainly by taking risk. Greater the risk, higher the profit and hence the business unit must strike a trade-off between the two. The essential functions of risk management are to identify measure and more importantly monitor the profile of the bank. Risk Management system is the pro-active action in the present for the future. Managing risk is nothing but managing the change before the risk manages. While new avenues for the
bank has opened up they have brought with them new risks as well, which the banks will have to handle and overcome.

When we use the term “Risk”, we all mean financial risk or uncertainty of financial loss. If we consider risk in terms of probability of occurrence frequently, we measure risk on a scale, with certainty of occurrence at one end and certainty of non occurrence at the other end. \textit{Risk is the greatest where the probability of occurrence or non-occurrence is equal.}

Banks are exposed to competition and hence are to encounter various types of financial and non-financial risks. Risks and uncertain ties form an integral part of banking which by nature entails taking risks. Till recently all the activities of banks were regulated and hence operational and environment risks were minimal.

Risks have adverse impact on the bank’s capital or earnings. The expected loss is to be borne by the borrower and depositors hence are to be taken care of by adequately pricing the products through risk premium and reserves created out of the earnings. It is the amount expected to be lost due to changes in credit quality resulting in default. Whereas, the unexpected loss on account of the individual exposure and the whole portfolio in entirety is to be borne by the bank itself and hence is to be taken care of by the capital. Thus, the expected losses are covered by reserves/provisions and the unexpected losses require capital allocation. Hence the need for sufficient Capital Adequacy Ratio is felt. Each type of risks is measured to determine both the expected and unexpected losses using VaR (Value at Risk) or worst-case type analytical model.
5.2 Theoretical Framework

Risks involved in Banking Portfolios: These risks can be classified in the following four heads namely.

1. Liquidity risk;
2. Interest rate risk;
3. Credit risk;
4. Capital risk

5.2.1. Liquidity Risk

It is the risk of meeting the Liquidity requirement of the banks as and when it arises without incurring unacceptable losses’. Liquidity risk includes the inability to manage unplanned decreases or changes in funding sources.

Quantity of Liquidity Risk Indicators

The following indicators, as appropriate, should be used when assessing the quantity of liquidity risk.

A. Low

1. Funding sources are abundant and provide a competitive cost advantage.
2. Funding is widely diversified. There is little or no reliance on wholesale funding sources or other credit-sensitive funds providers.
3. Market alternatives exceed demand for liquidity, with no adverse changes expected.
4. Capacity to augment liquidity through asset sales and/or securitization is strong and the Bank has an established record in accessing these markets.
5. The volume of wholesale liabilities with embedded options is low.
6. The Bank is not vulnerable to funding difficulties should a material adverse change occur in market perception.
7. Support provided by the parent company is strong.
8. Earnings and capital exposure from the liquidity risk profile is negligible.

B. Moderate
1. Sufficient funding sources are available which provide cost-effective liquidity.
2. Funding is generally diversified, with a few providers that may share common objectives and economic influences, but no significant concentrations. A modest reliance on wholesale funding may be evident.
3. Market alternatives are available to meet demand for liquidity at reasonable terms, costs, and tenors. The liquidity position is not expected to deteriorate in the near term.
4. The Bank has the potential capacity to augment liquidity through asset sales and/or securitization, but has little experience in accessing these markets.
5. Some wholesale funds contain embedded options, but potential impact is not significant.
6. The Bank is not excessively vulnerable to funding difficulties should a material adverse change occur in market perception.
7. The parent company provides adequate support.
8. Earnings or capital exposure from the liquidity risk profile is manageable.

C. High
1. Funding sources and liability structures suggest current or potential difficulty in maintaining log-term and cost-effective liquidity.
2. Borrowing sources may be concentrated in a few providers or providers with common investment objectives or economic influences. A significant reliance on wholesale funds is evident.
3. Liquidity needs are increasing, but sources of market alternatives at reasonable terms, costs, and tenors are declining.

4. The Bank exhibits little capacity or potential to augment liquidity through asset sales or securitization. A lack of experience accessing these markets or unfavorable reputation may make this option questionable.

5. Material volumes of wholesale funds contain embedded options. The potential impact is significant.

6. The Bank’s liquidity profile makes it vulnerable to funding difficulties should a material adverse change occur.

7. There is little or unknown support provided by the parent company.

8. Potential exposures to loss of earnings or capital due to high liability costs or unplanned asset reduction may be substantial.

It is measured with the ratio between liquidity out flow (withdrawal of deposits, repayment of bank borrowings) to liquid inflow (Maturing assets, fresh deposits etc.) A rough measurement of Liquidity risk will be (short term securities – Short term borrowing)/ Total Deposits. By increasing the proportion of liquid assets, bank can minimize the liquidity risk, but on this account its earning capacity will be adversely affected. The low interest bearing liquid investments affects both interest margin and profit margin.

The problem of liquidity for commercial banks is essentially of making available, at all the times, sufficient funds to meet the demand for money made from time to time. Liquidity is the protection against the risk that may develop in banks on account of forced sale or liquidate credit worthy assets in an adverse market causing unexpected losses. As explained by Howard D. Coosse, “In a more positive sense, liquidity can be defined as a bank’s (or the banking System’s) ability to meet not only possible withdrawal of deposits, but to provide for the legitimate credit needs of the community (or the
Risk in Banking

(116) economy) as well. It is in the latter sense that bank liquidity has been most sharply questioned in the recent years. To care for liquidity risk there should be appropriate liquidity reserves. These reserves should earn interest income and under all foreseeable circumstances be able to generate cash with little or no loss when the need arise”

5.2.2. Interest Rate Risk

It is the risk arising out of changes in interest rates and their impact on the income of the bank and the values of its assets and liabilities. *The assets or liabilities which are sensitive to interest rate changes are called Interest sensitive. Interest rate risk can be measured as the ratio of interest sensitive assets to interest sensitive liabilities.* An ideal ratio is considered one which safeguards safety with the interest rate fluctuations. The bank with interest rate risk of 1 will have equal variation in interest income or interest cost and therefore net-impact on the profit will be zero. If the ratio is below or above 1, the bank-profits will fluctuate depending upon how fast the interest rate on advances increases in comparison to the cost of deposits. A bank portfolio manager should monitor the interest rate moments or adjust the portfolio accordingly.

Interest Rate Risk Ratio = 1 (0 impact on profit)
Interest Rate Risk Ratio < 1 (profit will fluctuate)
Interest Rate Risk Ratio > 1 (profit will fluctuate)

It is a common knowledge that when market interest rate rises, the prices of existing bonds depreciates and when interest rates decline the prices of bond appreciates. The changes in bond values depends upon changes in market interest rates popularly known as yield and endogenous relations to the security like coupon rate frequency of payment of coupons and the remaining term to maturity of bonds. The changes in *A Comparative Study of Risk Parameters of Banks in India* 144 IJMT, Volume 19, Number 2, July - December 2011 interest rates affect the values of assets and liabilities items to
a great extent. Its impact calculation is a difficult task. The concept of duration is helpful to get over the above problem. Duration of a coupon bearing bond is the weighted average maturity of its cash-flow in present value items. The value impact on the market-value of equity change is calculated by multiplying the modified duration of the equity with the expected change in the interest rate. The duration gap is the difference between the duration of assets and the effective duration of liabilities. This can be zero, positive or negative. If duration gap is 0 (zero) the net worth of the bank is immunized against the interest-rate risk. If duration gap is positive value of net worth decreases when interest rate rises and value of net-worth increases when interest rate declines. If duration gap is negative value of net-worth increases when interest rate rises and vice-versa. Risk - Adverse banks try to reduce duration-gaps.

5.2.3. Credit Risk

This is the risk resulting on account of default of repayment of principal and interest payment. It is true that first the default starts from payment of interest. In interest is regularly paid in time, loan is considered safe. It is therefore, investment risk is considered in terms of variability in the interest rates. Credit risk is defined by the losses on the part of borrower to repay his obligation in the form of interest and instalments or in the events of a deterioration of the client’s credit worthiness. In the credit risk rating, both, dimensions default and irrecoverable positions are taken into consideration. Here exposure risk should also be taken into consideration. Exposure risk is generated by uncertainty associated with future amount at risk. On some of the financing facilities like Amortized Credit and the credits for which there is a credit schedule, exposure risk is very small. But, other lines of credit like cash credit facility, overdraft balancing, this risk is relatively high. Exposure risk may also arise with derivative trading, on account of changed market behaviour and movements. The liquidation value of derivatives depends upon movements and changes constantly.
Whenever the liquidation value is positive, there is credit risk for the bank, since bank may lose money if the counter party defaults. In credit risk recovery risk is also calculated which arises in the event of unpredictable recoveries. This is on account of many factors such as whether guarantees have been received from the borrower, the types of such guarantees – collateral or third party guarantee and circumstances surrounding the default. In credit risk, collateral risk is also inherited. The existence of collateral minimizes the risk, provided, collateral can easily be taken in position and disposed off at significant value. The value of the collateral depends upon its nature and market conditions. Fixed equipment generally has a lower resale value whereas cash collateral value is 100%. There is also third party guarantor risk. A third party provides guarantee to the bank at the request of the borrower. This transforms the default risk of the borrower into a joint default risk of the borrower plus the guarantor. There also emerges the legal risk of not being able to enforce the guarantee. In this channel of credit risk the last aspect is the legal risk. A banking company resorts to legal action after due notices and negotiations efforts. In such a case, all commitments given to the borrower is suspended until some legal conclusion is reached. In this process, recoveries will be suspended. In the worst situation, there may also arise situation of no recovery because the company is resold or liquidated and fund available for repayment remains very insufficient.

The Reserve Bank of India as an apex bank and controller of the Banking System has issued guidelines for monetary credit risk in the Indian Banking Sector. A broad framework of guidelines is summarized below:-

1. Bank should frame broad policy spectrum while explaining target markets, risk acceptance criteria, credit approval authority, credit authorization, maintenance procedure and guidelines for portfolio management and risk management.
2. Banks should establish credit risk management practices like annual or half yearly industry studies and reviews, period planned visits and review of weak credits.

3. Business managers should be made accountable for risk management. Banks should define risk limits and lay down procedures for risk management.

4. Bank should have a system of check and balances in the place around the extension of credit.

5. The credit approving authority should be granted to only those officers having adequate experience and risk judging ability. The level of authority should increase with the increase in amount and worsening risk ratings. There should be consistency in credit standards and evaluation of credit risk.

5.2.4. Capital Risk

It is the risk that arises on account of reduction in capital due to losses. It measures how much the asset values may decline before the position of creditors and depositors becomes critical. Keeping adequate capacity is the hedge against capital risk. Higher the capital to assets ratio, lower will be the capital risk and vice-versa. But, this is a double edged sword. On the one hand, risk is reduced, but, on the other hand also reduces return on equity. Therefore, there is need for a proper balance between the risk reduction and earning enhancement objectives and in that line, the equity capital should be designed. Capital risk can be calculated by calculating the ratio between capital and risk assets.

The following factors are generally taken into consideration to affect the adequacy of capital –

1. The level of capital which is considered appropriate by the bank management for the operation of the banking business.
2. The minimum level of capital prescribed by the regulatory authority. The level of such capital changes from time to time and situation to situation. The Reserve Bank of India issued capital adequacy norms 1988 which was amended in 1996. As per these guidelines, banks were required to maintain a minimum capital to risk weighted Assets Ratio (CRAR) of 8%. With effect from 1st April, 2000, banks are required to maintain this ratio at 9% on an ongoing basis. The capital to Risk Weighted Assets Ratio is calculated as under –

\[
\text{CRAR} = \frac{\text{Capital}}{\text{Risk Weighted Assets}} \times 100
\]

The definition of capital and its various components as per the Basel Committee Recommendations weight prescribed by RBI for different categories of funded risk assets are summarized below:

<table>
<thead>
<tr>
<th>Types of funded Risk Assets</th>
<th>Risk Weight (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Cash and balance with RBI, loans &amp; Advances guaranteed by Centre and State Governments, SSI advances Guaranteed by (CGTSI), advances Against term deposits, LIC policies, etc. where adequate margin is available Equity investment in subsidiaries etc.</td>
<td>0%</td>
</tr>
<tr>
<td>2. Investment in Government Securities, investment in other approved securities guaranteed by Govt.</td>
<td>2.50%</td>
</tr>
<tr>
<td>3. Balance in current account with other banks. Claims on banks &amp; public finance institutions, loans and advances granted to staff of banks fully covered by super-annuation benefits etc.</td>
<td>20%</td>
</tr>
<tr>
<td>4. Investment in Government guaranteed securities of Government undertakings which do not form part of the approved market borrowing programmes</td>
<td>22.5%</td>
</tr>
<tr>
<td>5. Advances covered by DICGC / ECGC, housing loan to individuals against the mortgage of residential housing properties.</td>
<td>52.5%</td>
</tr>
<tr>
<td>6. Investment in mortgage backed securities</td>
<td>52.5%</td>
</tr>
<tr>
<td>7. Loans guaranteed to public sector undertakings to Government of India and State Governments, Loans and leased assets, takeovers, foreign exchange, open positions in gold, premises, furniture and fixers and all other assets.</td>
<td>100%</td>
</tr>
<tr>
<td>8. Investments in subordinated debt instruments and bonds issued by other banks or public financial institutions for the tiered second capital, Deposits placed with SIDBI / NABARD in lieu of shortfall in lending to priority sector</td>
<td>102.5%</td>
</tr>
</tbody>
</table>
III. Comparison of Risk Parameter of different groups of Banks in India

1. Comparison of Liquidity Risk

Table No 5.1
Liquidity Risk (Short Term Securities / Deposits)

<table>
<thead>
<tr>
<th>Category of Banks</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>Mean</th>
<th>St.Dev.</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Scheduled Banks</td>
<td>5.19</td>
<td>5.38</td>
<td>5.70</td>
<td>5.72</td>
<td>5.39</td>
<td>5.58</td>
<td>5.4933</td>
<td>.2084</td>
</tr>
<tr>
<td>SBI &amp; Groups</td>
<td>5.55</td>
<td>5.20</td>
<td>9.22</td>
<td>6.51</td>
<td>5.75</td>
<td>5.40</td>
<td>6.2717</td>
<td>1.5133</td>
</tr>
<tr>
<td>Nationalized Banks</td>
<td>4.00</td>
<td>4.28</td>
<td>3.38</td>
<td>3.99</td>
<td>4.20</td>
<td>4.48</td>
<td>4.0550</td>
<td>.3782</td>
</tr>
<tr>
<td>Other Scheduled Bank</td>
<td>5.93</td>
<td>5.43</td>
<td>5.53</td>
<td>5.82</td>
<td>6.13</td>
<td>5.63</td>
<td>5.7450</td>
<td>.2633</td>
</tr>
</tbody>
</table>

Source: Various issues of R.B.I. bulletins and statistical Tables Relating to Banks in India and Reports On Trends and Progress of banking in India.

The above Table reveals that Liquidity Risk has been ranging between 9.35 to 16.45 in Foreign Banks. It has ranged between 5.43 to 6.13 in Other Scheduled Banks. In SBI and Groups it has been between 5.20 to 9.22. In Nationalized Banks it has been between 3.38 to 4.28. If we look at the Mean Value of Liquidity Risk we find that it is very high in Foreign Banks which is 13.53 and very low in Nationalized Banks which is 4.05. The degree of variation (Standard Deviation) is very high in Foreign Banks which is 2.68 and very low in Other Scheduled Bank which is .26.

Source Various issues of R.B.I. bulletins and statistical Tables Relating to Banks in India and Reports on Trends and Progress of banking in India.
2. **Comparison of Interest Rate Risk**

**Table No 5.2**

*Interest Rate Risk (Interest Sensitive Assets / Interest Sensitive Liability)*

<table>
<thead>
<tr>
<th>Category of Banks</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>Mean</th>
<th>St. Dev.</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Scheduled Banks</td>
<td>1.65</td>
<td>1.48</td>
<td>2.04</td>
<td>1.90</td>
<td>1.70</td>
<td>1.53</td>
<td>1.7167</td>
<td>.2162</td>
</tr>
<tr>
<td>SBI &amp; Groups</td>
<td>1.80</td>
<td>1.45</td>
<td>2.22</td>
<td>1.99</td>
<td>1.85</td>
<td>1.50</td>
<td>1.8017</td>
<td>.2924</td>
</tr>
<tr>
<td>Nationalized Banks</td>
<td>1.70</td>
<td>1.55</td>
<td>2.13</td>
<td>2.03</td>
<td>1.75</td>
<td>2.60</td>
<td>1.9600</td>
<td>.3803</td>
</tr>
<tr>
<td>Other Scheduled Bank</td>
<td>1.54</td>
<td>1.55</td>
<td>1.77</td>
<td>1.66</td>
<td>1.59</td>
<td>1.60</td>
<td>1.6183</td>
<td>.565</td>
</tr>
<tr>
<td>Foreign Bank</td>
<td>1.12</td>
<td>1.05</td>
<td>1.52</td>
<td>1.30</td>
<td>1.17</td>
<td>1.10</td>
<td>1.2100</td>
<td>.1741</td>
</tr>
</tbody>
</table>

The above Table reveals that Interest Rate Risk in Foreign Banks has been between 1.05 to 1.52; in other Scheduled Banks it has been between 1.54 to 1.77; in Nationalized Banks it has been between 1.55 to 2.26 and in SBI & Groups it has been between 1.45 to 2.22. If we look at the Mean Value of Interest Risk we find that it is very high in Nationalized Banks which is 1.96 and very low in Foreign Banks which is 1.21. The degree of variation (Standard Deviation) is very high in Other Scheduled Banks which is .56 and very low in Foreign Banks which is 0.17. Thus the interest rate risk has been very high in public Sector Banks as compared to Private Sector and Foreign Banks.
3. Credit Risk

**Table No 5.3**

Credit Risk (Medium Quality Loan/Assets)

<table>
<thead>
<tr>
<th>Category of Banks</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>Mean</th>
<th>St. Dev</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Scheduled Banks</td>
<td>18.55</td>
<td>20.41</td>
<td>21.22</td>
<td>19.33</td>
<td>19.05</td>
<td>20.01</td>
<td>19.9117</td>
<td>1.0855</td>
</tr>
<tr>
<td>SBI &amp; Groups</td>
<td>17.40</td>
<td>20.22</td>
<td>20.23</td>
<td>18.69</td>
<td>17.94</td>
<td>20.72</td>
<td>19.2000</td>
<td>1.3784</td>
</tr>
<tr>
<td>Nationalized Banks</td>
<td>20.94</td>
<td>23.35</td>
<td>25.05</td>
<td>22.16</td>
<td>21.44</td>
<td>23.85</td>
<td>22.7983</td>
<td>1.5612</td>
</tr>
<tr>
<td>Other Scheduled Bank</td>
<td>13.31</td>
<td>14.07</td>
<td>13.52</td>
<td>12.86</td>
<td>13.81</td>
<td>14.57</td>
<td>13.6900</td>
<td>0.5992</td>
</tr>
</tbody>
</table>

Source: Various issues of R.B.I. bulletins and statistical Tables Relating to Banks in India and Reports On Trends and Progress of banking in India.

The above Table reveals that Credit Risk in Foreign Banks has been between 13.89 to 20.54; in other Scheduled Banks it has been between 12.86 to 14.87; in Nationalized Banks it has been between 20.94 to 25.05; and in SBI & Groups it has been between 17.4 to 20.72. If we look at the Mean Value of Credit Risk we find that it is very high in Nationalized Banks (Public Sector Banks) which is 2.79 and very low in Other Scheduled Banks which is 13.69. The degree of variation (Standard Deviation) is very high in Foreign Banks which is 2.56 and very low in Other Scheduled Banks which is 1.59. Thus it is clear that the Credit Risk is very high in Foreign Banks and low in Private Sector Banks.
4. Capital Risk

Table No 5.4
Capital Risk (Capital/Risk Assets)

<table>
<thead>
<tr>
<th>Category of Banks</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>Mean</th>
<th>St. Dev.</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Scheduled Banks</td>
<td>7.40</td>
<td>7.68</td>
<td>6.30</td>
<td>6.50</td>
<td>6.90</td>
<td>7.18</td>
<td>6.9933</td>
<td>.5300</td>
</tr>
<tr>
<td>SBI &amp; Groups</td>
<td>6.01</td>
<td>6.31</td>
<td>5.11</td>
<td>5.43</td>
<td>5.51</td>
<td>5.81</td>
<td>5.6967</td>
<td>.4330</td>
</tr>
<tr>
<td>Nationalized Banks</td>
<td>5.75</td>
<td>6.77</td>
<td>5.72</td>
<td>6.01</td>
<td>5.25</td>
<td>6.27</td>
<td>5.9617</td>
<td>.5216</td>
</tr>
<tr>
<td>Other Scheduled Bank</td>
<td>8.40</td>
<td>8.88</td>
<td>7.01</td>
<td>6.36</td>
<td>7.90</td>
<td>8.38</td>
<td>7.8217</td>
<td>.9558</td>
</tr>
<tr>
<td>Foreign Bank</td>
<td>16.03</td>
<td>16.07</td>
<td>13.90</td>
<td>14.07</td>
<td>15.53</td>
<td>15.07</td>
<td>15.1067</td>
<td>.9545</td>
</tr>
</tbody>
</table>

Source: Various issues of R.B.I. bulletins and statistical Tables Relating to Banks In India and Reports On Trends and Progress of banking in India.

Capital Risk is very high in Foreign Banks and Private Sector Banks and very low in Public Sector Banks as it is clear from the Table No.10 given below:-

The Table reveals that capital risk has been ranging between 13.9 to 16.07 in Foreign Bank. In Other Scheduled Banks it has been between 6.36 to 8.88. In Nationalized Banks it has been between 5.25 to 6.77. In SBI and Groups it has been between 5.11 to 6.31.

If we look at the Mean Value of Capital Risk we find that it is very high in Foreign Banks which is 15.10 and very low in SBI and Groups which is 5.69. The degree of variation (Standard Deviation) is also very high in Foreign Banks which is .96 and very low in SBI and Groups which is 0.43. This indicates that Capital is adequate in Public Sector Banks and less adequate in Private Sector Banks and Foreign Banks. The comparison of various risk parameters of different categories of Scheduled Commercial Banks reveals that degrees of risks faced by different categories of Scheduled
Commercial Banks are different. Degree of Risk has been very high in Foreign Bank and Other Scheduled Banks and low in Public Sector Banks.

5.3 Other Risks Involves in Public Sector Banks

5.3.1. Operational Risks

Banking is a business with full of risks. The risks can be classified into Credit Risk, Market Risk and Operational Risk. The banks give lot of attention to mitigate credit and market risks, but generally ignore the operational risks presuming that everything will be fine.

The types of controls required to manage the risks for computerized system are different than those for manual systems. It is therefore necessary for the banks to identify the key risks arising from the increased use of computerization and automation in their processes, and implement adequate controls to mitigate those risks. In brief operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Globalization, together with increased financial innovation, are making the activities of banking institutions and thus their risk profiles (i.e. the level of risk across an institution’s activities and/or risk categories) more complex. Due to these developments, operational risk is becoming more pronounced. Examples of these developments include:

- The greater use of more highly automated technology which has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on globally integrated systems;
- Growth of e-commerce brings with it potential risks (e.g., internal and external fraud and system security issues) that are not yet fully understood;
• The emergence of banking institutions acting as large-volume service providers creates the need for continual maintenance of high-grade internal controls and back-up systems;
• Growing use of outsourcing arrangements and the participation in clearing and settlement systems which can mitigate some risks but can also present significant other risks to banking institutions.

Operational risk is associated with the problems of accurately processing, settling, and taking or making delivery on trades in exchange for cash. It also arises in record keeping, processing system failures and compliance with various regulations. As such, individual operating problems are small probability events for well-run organizations but they expose a firm to outcomes that may be quite costly.

The operational risk is generally related to the risk of failure of man, machine or the systems to operate as expected. With more and more implementation of Information Technology based systems and procedures, the chances of IT related operational risks have increased unless proper safeguards are not implemented.

5.3.2 IT Application Risks
The IT risks can be classified in three categories

- IT environment risks
- IT operations risks
- Product and service risks

5.3.3. IT Environment Risk

This category represents the inherent risks that arise due to the commercial and business environment within which the computer and telecommunication systems are operating viz. Regulatory Risk, Strategic Risk, Organization Risk, Location Risk and Outsourcing Risk.
5.3.4. Regulatory Risk

The banks operate within a set of regulatory framework. The design and operation of computer systems must comply with the regulatory framework in place. Regulatory breaches can result in diminishing reputation, increased cost of capital, limited business opportunities and punitive action, which may ultimately result into loss of banking operations. The lack of or inadequacy of legal framework covering electronic transactions can increase the likelihood of disputes arising relating to banking transactions.

5.3.5. Strategic Risk

IT in banks is implemented to meet business needs. Thus, selection of right type of technology for the right type activity to achieve strategic business needs. When a bank adopts inappropriate IT strategy strategies, the bank may not be able to achieve its effectiveness and loose competitive edge and may place undue pressure on the banks IT resources and systems to adapt to new business environment, as new products and services come on-line. A risk exists that short term fixes may be made to the detriment of long term objectives and projects. The failure of IT strategies to take into account the changing needs of the bank may lead to the current systems becoming obsolete in short time.

5.3.6. Organization Risk

The organizational structure of a bank can determine the effectiveness of the bank’s use of IT. When the organizational structure fails to provide and define reporting lines and responsibilities for the IT functions, this can lead to misunderstanding of responsibility and a poor distribution of human and financial resources. In addition, poor segregation of duties can increase the risk of error and fraud within a computerized environment.
5.3.7. Location Risk

The technology resources are susceptible to the risks of unforeseen and sometimes naturally occurring events. Depending on the location of a bank's data processing activities, it can be susceptible to natural events such as floods, earthquakes, storms and other events like riots or sabotage.

5.3.8. Outsourcing Risk

It is increasingly common for banks to outsource some or all of their data processing activities. When outsourcing takes place there are some additional risks which need to be considered. Without proper management control and documentation, the responsibilities and liabilities of vendor and client may not be clear. Over reliance on single vendor/supplier increases the risks from their failure and may lead to unacceptably high costs. There is also risk of disclosure of some strategic business information and strategy.

5.3.9. IT Operations Risk

Operations risk relates to those risks arising from day to day transaction processing on computer systems. The operations risks cover Error Risk, Computer Fraud Risk, Disclosure Risk and Interruption Risk.

5.3.9.1 Error Risk

Errors in a computerized environment may arise from a number of sources, including errors made during the development and modification of computer programmes simple error in data entry or misuse of some tools and sensitive facilities. These errors may affect the completeness and accuracy of transactions and may result into loss to the bank. The bugs in the application programme may also result into errors.

5.3.9.2 Computer Fraud Risk

A computerized environment provides a number of new opportunities for fraudsters. This is primarily due to the ease with which fraudsters can hide
their actions on computer systems and the speed with which fraudulent activity can take place. It is imperative that the banks are aware of the vulnerable points within its system and guards against new opportunities for fraud which may materialize, especially during times of business and system change. Such risks are more likely when the security and control systems are weak or not properly implemented.

5.3.9.3 Disclosure Risk

Information held on a banks computer and passed around its communication network includes very sensitive financial and other data about the banks customers. Accidental or intentional disclosure of this information can have a negative impact on banks reputation and may result into loss to its customers and legal litigation.

5.3.9.4 Interruption Risk

The failure of computer and/or communication systems may result into interruption of banks operations and business. The impact of discontinuity of computer operations can be dramatic which may lead to customers dissatisfaction, loss of business, etc. If computer facilities and related infrastructures are not adequately protected and secured the result may be a major impact upon the business continuity.

5.3.9.5 Product and Service Risk

Banks may implement technology-based products to improve operational efficiency and effectiveness. Whilst the operational risks associated with these products remain fundamentally unchanged, the way in which management design and implement a control framework to mitigate against those risks is different. The services like ATMs, Electronic Funds Transfer (EFT), and Computer based dealing services, etc. required to be available without any disruption. It is clear that operational risk differs from other banking risks in that it is typically not directly taken in return for an
expected reward, but exists in the natural course of corporate activity, and that this affects the risk management process. At the same time, failure to properly manage operational risk can result in a misstatement of an institution’s risk profile and expose the institution to significant losses.

Banks have adopted IT in a big way in order to provide better service to the large customer base of the individual banks. The general awareness on the IT risks and its effects are yet to catch up the importance in banking industry and hence, the perils due to IT risk management, exist.

The focus of IT Security programme is to enlighten the nature of IT risks associated in every face of IT deployment and its safeguarding methodologies. Its further emphasis is on IT act, security policy issues, Disaster recovery and BCP and to protect the electronic form of exchanges and processing. Its ultimate objective is to make people aware about possible threats of IT and its protective measures.

5.4 Overview of Financial System

India’s financial sector is diversified and expanding rapidly. It comprises commercial banks, other credit institutions, insurance companies, pension funds, and mutual funds, with overall assets of 140 percent of GDP as of end-March 2010 (Figure 2, Appendix Table 3). Commercial banks are the largest group, comprising 55 percent of total financial assets, followed by insurance.6 other bank intermediaries include regional rural banks and cooperative banks that target under-serviced rural and urban populations. Many NBFCs operate in specialized segments (leasing factoring, microfinance, infrastructure finance), though some can accept deposits. Pension provision covers 12 percent of the working population and consists of civil service arrangements, a compulsory scheme for formal private sector employees, and private schemes offered through insurance companies.
5.4.1. Public ownership is a defining feature of the financial system

Majority publicly owned banks account for three quarters of banking system assets (Figure 3). About 69 percent of insurance premiums and 80 percent of insurance assets are accounted for by public insurers. Most of the pension system is in public hands. The public life insurance company and public provident fund are the two largest providers of funds to the Indian capital market, with US$200 billion and US$70 billion, respectively, in assets under management.

5.4.2. Another structural feature is limited foreign penetration

Foreign banks account for 7 percent of banking system assets, and their expansion is restricted. A change in the current entry norms for foreign banks (which permit only a branch presence in India, albeit with locally assigned capital requirements) is under discussion, which would provide incentives for foreign banks to incorporate as subsidiaries. In the insurance sector, foreign joint ventures are limited to a maximum of 26 percent of equity.
5.4.3. **Interconnectedness and complexity are increasing**

Banks’ connections through the interbank market reveal a tiered structure whereby large banks at the core deal mostly with each other, and banks at the periphery (foreign and old private banks) have minimal exposure to each other (Figure 4a). Banks, NBFCs, and mutual funds are linked through the wholesale funding market (Figure 4b). Financial conglomerations have also taken a foothold with major banks owning insurance, fund management companies, and securities firms. Currently, there are 12 financial conglomerations, of which 6 are bank-led, 3 are insurance-led, 1 is a mutual fund group, and 2 are led by NBFCs. Bank financial conglomerates comprise over 20 percent of financial system assets and 35 percent of commercial banks’ assets.

**Figure 5.2**

**India: Financial System Interlinkages, June 2011**

a. **Interbank**
b. Intra-financial Sector

Legend: Blue shapes are net lenders and red shapes are net borrowers. Thickness of lines indicates relative size of exposures.
Source: RBI staff calculations.

5.4.4 Commercial banks are required to hold substantial precautionary buffers of government securities

RBI uses the CRR (set at 5.5 percent) and SLR (set at 24 percent) to provide banks with sizeable buffers of low-risk assets while also supporting the government's financing needs. RBI’s flexible use of SLR and CRR, together with a range of other measures, enabled banks to cope well with liquidity pressures during the global crisis. Most holdings of government securities, however, are not available to meet liquid needs in normal times as they have to be held on a continuous basis to meet SLR requirements.
Stress tests confirm that commercial banks are well positioned to withstand a range of severe shocks. Stress tests were undertaken jointly with RBI and provide important insights into the resilience of Indian banks:

*Macro credit risk tests* indicate that the system overall is resilient to aggregate increases in credit risk. Under various risk scenarios, the banking system remains adequately capitalized—-with a sharp initial NPA increase declining gradually with the recovery of GDP (Figure 6).

*Liquidity stress tests* indicate that the banking system could withstand severe funding and market liquidity shocks, for instance coming from a reversal of capital flows, under the assumption that the SLR is used in repos with RBI with a 5 percent haircut. Tests included a sudden, substantial withdrawal of funds over a five-day and 30-day period, as well as tests on maturity mismatch and roll-over risk. Most banks pass several liquidity stress tests, with maturity mismatch presenting the highest risk.

*Single-factor sensitivity analyses* suggest that the system could withstand a range of shocks. Credit risk—including exposures to agriculture, power, telecommunications, and real estate—is the main source of vulnerability but appears to be manageable given high initial levels of capital and good profitability; only a few small banks would appear in need of recapitalization. Shocks to market risks (interest rate, foreign exchange, equity price risks) have low impact largely due to strict regulations that limit maturity gaps, net foreign currency exposures, and equity market exposures.

### 5.5 Stress Test Scenarios and Shocks

The macro stress tests used a *baseline* and two *adverse macroeconomic scenarios*, with projections based on end FY2010/11. The scenarios are based on the April 2011 *World Economic Outlook*; due to
downward adjustments in GDP projections since then, the medium-risk scenario has now effectively became closer to the baseline.

Two adverse macroeconomic scenarios were used: medium and severe. These broadly correspond to two and two and a half standard deviations in GDP growth over the last 15 years, respectively, with shocks occurring in FY2011/12, with the growth path improving over the following four years. Other macroeconomic variables were derived based on IMF staff calculations based on a partial equilibrium macroeconomic models for the Indian economy. An adverse shock to the Indian GDP could be fuelled by either domestic or external shock, such as a deepening of the global economic slowdown.

Table : 5.5

Macroeconomic Scenario Assumptions

(Changes in percent, unless indicated otherwise)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GDP growth Baseline-September</td>
<td>9.9</td>
<td>7.5</td>
<td>7.9</td>
<td>8.1</td>
<td>8.1</td>
<td>8.1</td>
</tr>
<tr>
<td>Medium Risk</td>
<td>9.9</td>
<td>5.1</td>
<td>5.5</td>
<td>6.5</td>
<td>7.0</td>
<td>7.5</td>
</tr>
<tr>
<td>Severe Risk</td>
<td>9.9</td>
<td>3.8</td>
<td>4.7</td>
<td>5.8</td>
<td>6.5</td>
<td>7.5</td>
</tr>
<tr>
<td>WPI Inflation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Baseline-September</td>
<td>9.0</td>
<td>7.9</td>
<td>6.6</td>
<td>5.8</td>
<td>5.4</td>
<td>5.4</td>
</tr>
<tr>
<td>Medium Risk</td>
<td>9.0</td>
<td>7.7</td>
<td>6.4</td>
<td>6.0</td>
<td>6.0</td>
<td>6.3</td>
</tr>
<tr>
<td>Severe Risk</td>
<td>9.0</td>
<td>7.6</td>
<td>6.1</td>
<td>5.9</td>
<td>6.1</td>
<td>6.5</td>
</tr>
<tr>
<td>Short term(call) interest rate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Baseline-September</td>
<td>6.2</td>
<td>7.2</td>
<td>6.3</td>
<td>6.3</td>
<td>6.3</td>
<td>6.3</td>
</tr>
<tr>
<td>Medium Risk</td>
<td>6.2</td>
<td>7.7</td>
<td>6.3</td>
<td>6.3</td>
<td>6.3</td>
<td>6.3</td>
</tr>
<tr>
<td>Severe Risk</td>
<td>6.2</td>
<td>8.2</td>
<td>6.3</td>
<td>6.3</td>
<td>6.3</td>
<td>6.3</td>
</tr>
<tr>
<td>Export/GDP ratio</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Baseline-September</td>
<td>20.2</td>
<td>19.9</td>
<td>20.7</td>
<td>21.4</td>
<td>22.0</td>
<td>22.6</td>
</tr>
<tr>
<td>Medium Risk</td>
<td>20.2</td>
<td>19.9</td>
<td>21.7</td>
<td>22.8</td>
<td>23.6</td>
<td>24.4</td>
</tr>
<tr>
<td>Severe Risk</td>
<td>20.2</td>
<td>20.1</td>
<td>22.1</td>
<td>23.4</td>
<td>24.4</td>
<td>25.1</td>
</tr>
</tbody>
</table>
A range of single factor shocks were also tested, both top-down and bottom up. Calibrations were based on Indian historical data for the last 15 years, as well as the experience from other countries:

- **Credit risk** was tested through several shocks, including increases in NPAs by up to 150 percent; reclassification of 15 percent of restructured loans; a uniform downgrade of all corporate borrowers by one notch; and an increase in probabilities of default by 25 percent.

- **Interest Rate Risk** was tested for both the banking and trading books, including parallel downward and upward shift of the INR yield curve (250 bps); a steepening of the curve (100 bps linearly spread between 15-day and over 25-year maturities; and an inversion of the curve (two-year rates up 250 bps and 10-year rates up 100 bps).

- **Foreign Exchange Risk** was tested, including a 10 percent and 15 percent depreciation of INR in 30 days (the former corresponding to the experience of 2008); a 10 percent and 15 percent appreciation of INR in 30 days; and a reverse test (how much depreciation of INR is necessary for Tier 1 capital to move down to 3 percent over 60 days).

- **Equity Price Risk**: a drop in the equity price index by 40 percent within a 30-day period, corresponding to the experience of 2008.

- **Liquidity Risk**: a 30-day deposit and, separately, wholesale funding withdrawal of 10 percent; and a 5-day deposit (wholesale funding) withdrawal of 5 (3) percent.

### 5.6 The Data Recovery Challenges in Banks

As the banking IT system improve and increase its services, they face challenges in reducing business risk due to IT outages. As banking applications grow there is a pressure on IT managers to reduce the time and resources for conducting regular ‘recovery drills’. Meeting RTO objectives can become tricky as it means organizing access to experience and scarce expertise.
It is mandatory for IT managers to gather a required documentation to demonstrate that adequate systems and process are in place to ensure regulatory compliance. Some of the key challenges that banks face are as follows:

- As banking services are available for 24 * 7, there is a little downtime for DR drills.
- Complete IT applications running on heterogeneous technologies require manual intervention and expertise to test recovery readiness.
- Managing and propagating changes done on primary site to DR site. While making these changes sometimes inconsistent application environments, causing recovery system at the DR site to fail.
- IT landscape in a bank usually consists of multiple IT applications that are interdependent and have to be accounted for when planning for recovery. Example: Internet banking and ATM needs core banking. These dependencies increase recovery complexity.
- IT managers have little visibility of how well their solutions are meeting recovery SLAs. They can find it out only at the time of drill.
- Coordinating the required information to submit to regulatory authorities is a time consuming task.

### 5.7 Disaster Recovery Planning (DRP)

DRP has become a very difficult task for Indian banks. We come across high profile natural and man-made disasters. DR Methodology of banks is a straightforward application which follows a project plan similar to System Development life cycle (SDLC).

- Networks are more complex than before. Multiple layers of devices (optical/physical, Ethernet, IP)
• Complexity of operating a network is directly proportional to Number of device Relationships in the network. The number of device relationships can reach up to square if the number of devices.

• Devices are more complex. Number of parameters requires to describe an interface are more than a decade ago. More interface per device.

• Services are more complicated as they have to coordinate behavior of more devices.

• Regular Software updating and management of computers is complex to manage, problem with troubleshooting, telecom network operations personnel have very less experience with new issues.

• Maintaining stable network operations under all possible operating conditions is difficult to achieve as number of standards with extensions and interpretations differ among vendors.

5.8 Disaster Recovery Risk assessment

IT disaster recovery focuses on the following risk scenarios. Loss of these scenarios has negative impact on banks:

- Loss of access to premises
- Loss of data
- Loss of IT functions
- Loss of skills

Risk assessment focuses on the risks that can lead to the above outcomes. According to Peter Barns, FBCI managing director of London based 2C consulting “The key activities from an IT perspective are to consider the impact on the business if delivery of critical applications and services were to be denied as a result of a fire or server failure. For example to access the risks that such a scenario might arise.”
Key Aspect is to know what services run on which parts of the infrastructure. It was suggested by Andrew Hiles, FBCI, managing director of Oxfordshire-based “Kingswell” International that:

“It sounds obvious, but one major insurance company had grown by acquisition and suddenly had several data centers. They did not have a clue of the risks associated with their new acquisitions.

5.9 **Disaster Recovery Risk Assessment (DDRS) and Business Impact Analysis (BIA)**

- DDRS and BIA both are crucial steps in building DRP. Before looking for DDRS and BIA bank has to locate disaster recovery risk assessment.
- IT disaster recovery process has a standard process flow
- Network Disaster Recovery Plan
- Network Disaster Recovery Plan document is prepared so that at the time of disaster banks can refer that document and bring network to normal state as soon as possible. Things which should be documented in network disaster recovery plan are:

**Hardware and Software**

- Configuration setting of every networking hardware of data centre(example ROUTERS)
- Ports which are open on firewall
- Firmware versions used on each of the hardware device

**Network Diagram**

Network Diagram of the data centre is must.

Example: Router of the data centre is stuck by lightening. At this time bank can refer to configuration document of old devices which will help to replace that old router with the new one. The new router is configured.
Problem: If the two routers are not identical then engineers have to find out which network cables will be plugged into each port.

**Solution:** Network Diagram helps to figure out the correct network cables and ports. LAN surveyor is a tool from Solar winds which helps produce network diagram. Network mapping applications can also be used some of which are available free of cost.

**Contact Information**

Contact Information of those employees who are useful at the time if emergency Employees in IT unit Vendors Technical support contact numbers (and your account number for the tech support lines) for the hardware and software manufacturers.

**Product Information**

Serial Number and Model Number of all the hardware

License Information of software (when software publisher is called for support). Operating System that software is running on.

**5.10 Steps to Create a Disaster Recovery Plan**

**5.10.1. Define Unacceptable loss**

Before developing a plan, the bank should decide how much it will lose when plan is not there. This will help us decide how much time, effort and money should be spent on the plan.

**5.10.2. Backup Everything**

Everything should be backup

- Data
- Metadata
- Instructions needed to get them back
Backup facilities includes
- Building
- Phones
- People

5.10.3. Organize Everything
Suppose bank has proper documentation of disaster recovery plan but at the time of disaster we cannot locate it. Then the hard work behind documentation is of no use. Therefore backup plans should be properly and safely kept in an organized manner so that backup facilities are the hardest part of the DR plan.

5.10.4. Protection against disaster
Disaster recovery plan should be planned to protect the bank against all types of disasters mainly technological because today’s banking industry is based on IT.

5.10.5. Documentation of Everything
The person who is documenting the plan should document in such a way that anyone can follow these steps after or during a disaster.

5.10.6. Test
Testing of documentation of disaster recovery plan is necessary as without testing plan is mere a proposal.

5.11 IT Hardware
IT hardware includes
- Servers and Storages like backup, input, output and monitoring devices
- Network devices like routers, switches and legacy devices like hubs.
- Passive devices like cables and stack
All the devices are used to ensure information security audit firewalls, threat prevention systems and antivirus gateways. Power Supply without fail should be available. Bank should regularly audit power efficiency, supply and chances of downtime. Cooling is also important since data centre equipment works 24*7. Data centre and Disaster Recovery site(s) should be on different seismic zones. All the laptops, desktops, smart phones and tablets belonging to the bank employees, customers, and vendors should be audit.

5.12 IT Software

Database and application should be audited regularly. Best practices of disaster recovery audit are as follows:

a. **Customize Disaster Recovery Templates**

Disaster Recovery audit should be done strategically as it contains confidential information about the bank. Confidential information is like bank functions profit centers, bank stress points. Template should be made and implemented according to bank’s need.

b. **Have a Mix of Internal and External Audits**

Bank should have internal and external auditors. The benefits of mixed auditors are that, internal auditors bring their expertise in representing bank functionalities and critical things of banks. The external auditors give unbiased person view of the bank’s risks, loopholes which got unnoticed by internal auditors. Before inviting external disaster recovery auditors, internal team should be done away with GAP analysis of the bank. Based on the trust in external auditor’s understanding of the banking business and involved risks, formulate a disaster recovery audit program.

c. **Conduct Regular audits and Certificate program**

Once a bank is complete with disaster recovery audit program and set of security policies, regular audits are necessary as technological up
gradations takes place and as a consequence employees have to trained new skills. Bank can certify them in the areas like:

- ISO 27001 (information security)
- ISO 9001 (Quality Management)
- ISO 14001 (Environment Management)

d. **Have Emergency Procedures and Drills**

At the time of earthquake offices are evacuated on priority.

- Ensure all processes are switched over to the DR site located at a different seismic zone.
- Resume activities in the primary site at the earliest.
- Regular tanning and DR drills are must. Unplanned audits by internal as well as external auditors to explore loopholes and non-compliance.
- Proper documentation of checks and drills is done to prepare users for unforeseen circumstances. Replication and policy based backup of other databases ensure safety and recovery of these documents.
- Regularly audit service level agreements (SLA) signed between various hardware and software vendors. This ensures good integration between banks SLA during disaster recovery audits to ensure unified uptime. Inlinked SLAs will ensure availability on all technological fronts.

### 5.13 DR Plan includes the following

#### 5.13.1 Risk Analysis

It is the 1st step for DR and contingency planning. It takes a list of possible risks to operations. Risk Analysis involves

- Risk identification
- Assess of likelihood of the event to occur
- Define severity of events consequences
Risk can be anything from power outage, hardware failure to earthquake or flood.

5.13.2 BIA

BIA evaluates critical Banking functions. It identifies and quantifies the impact of those functions (Functions can be operational and functional) would have on the organization.

Figure 5.5

Keystone BCM Lifecycle

5.13.3 Building DR Plan

‘DR plan provides structured approach for how to respond to unplanned incidents’

Plan provides step-by-step procedures for recovering disrupted systems and Networks to resume normal operations.
Plan identifies critical IT systems and networks, prioritize recovery time Objectives and outlines the step needed to restart, reconfigure and recover.

**Figure 5.6 Know Your Business**

5.13.4 Business Continuity Management (BCM)

BCM is a function which consists of a complete set of processes. These processes identify potential threats which impact banking processes in the bank. It provides a framework for building resilience for an effective response which safeguards the interest of key stake holders, reputation, brand and value creating activities. It is inclusive of disaster recovery, crises management, contingency planning as well as alternative planning. BCM includes conducting.
BIA- Process of analyzing the affect of interruptions to business operations or processes on all banking functions.

BCP- Process of developing prior arrangements and procedures that enable banks to respond to an event in such a manner that critical banking functions can continue within planned levels of disruption.

5.13.5 Information Policy (IP)

IP classifies the available information based on sensitivity. It outlines the owners of the information to which it is end use of the information to which it is subjected. Therefore it is essential that clear, specific and Comprehensive Information Policy is framed so that timely and relevant information is available for banks development effectiveness.

The major rationale for forming an information policy is
- Importance of transparency in bank’s mission
- Commitment to foster ownership
- Build Dialogue
- Strengthen public oversight of development initiatives

Principles of access to information set path in the foundation of IP. There are standards for collection, compilation, storage, retrieval and dissemination of information on which framing and implementation of IP is based. IP should be reviewed and updated periodically.

5.13.5 Information Security Policy (ISP)

ISP is a documented banking business rule for protecting information and the systems which store and process this information. ISP provides high-level description of various controls of the bank will use to protect information. Information should be based on the principles of integrity, reliability and validity. Protecting confidential information of banks is the
priority. ISP should be reviewed and updated at periodical intervals. It may
mansion and gives details of principles for protecting information from
unauthorized access, use, disclosures, disruption, modification or destruction.
It inter-alia, relate to policies such as firewall, email, network security, and
password. It mansions prevention of cyber attacks by deploying technologies
such as two-factor authentication.

5.14 Audit of IT Process and Infrastructure

Audit of IT Process and Infrastructure are done to ensure
confidentiality, integrity, authenticity and timely availability of information.
To ensure this there are various types of audits

Organizational IT audit (Management control over it)

Technical IT audit (infrastructure, data centers, data communication)

Application IT audit (business/ financial/operational)

Development/Implementation IT audit
(specification/requirements, design, development and post- implementation
phases).

5.15 Compliance IT audit

These audits may be conducted at periodic intervals keeping in view
the requirements for the bank. Audits may conduct up to national /
international standards.

Interruptions can occur anywhere and at anytime. Like tsunami, power
outage, terrorist bombing were in headlines in the last decade.

In today’s 24 * 7 *365 world it has become very important to prepare
DR plans. Anything can happen anytime and banks should be prepared for it.
With the increasing dependence on banks for both electronic and traditional
banking services, it has become mandatory for banking sector to plan for
‘Business Continuity’.
Today almost all the activities are dependent on banks. They are tuned into business models to deliver service in the age of BOUNDRYLESS COMMERCE.

In 2005 flood in Mumbai since ATM terminals are located on ground floor with their backup power generator located in its basement, due to rain all ATMs were non-functional. In such situations lack of access to financial resources could have severe implications, without those resources other organizations and common man finds it difficult to recover from these interruptions.

5.16 Essential Ingredients of Successful BCM Implementation In Banks

The research highlighted several salient features of successful BCM Implementation. It was found that most banks address the issue with the organizational focus on strong technology and facility infrastructure. Most large banks have near world-class facility and technology infrastructure in place as well as the organizational structure and processes to ensure continuity in the event of disruptions. Banks are also factoring in their BCM implementation “softer” issues such as customer satisfaction (e.g., convenience, ease, feel-good, etc.), esteem (the image of the bank in the market and in the eyes of customers), and climate (motivation levels of employees and partners). The “harder” issues such as IT Infrastructure, facilities, procedures, etc. have already attained a high degree of maturity in most banks. These are taken as “given”. Therefore banks are now aspiring to attain a higher BCM maturity level by taking necessary actions to improve the softer aspects noted earlier.

The essential ingredients of successful BCM Implementation as culled out from the research findings are grouped in three clusters, - Strategic, Operational and Technological. They are discussed in turn in this section.
5.16.1 Strategic

The Strategic cluster encompasses the following factors that top management should consider while setting out policy to institute reliable BCM practices.

- **Multiple Delivery Options**

  “Banks delivering their products and services through a wide range of delivery channels: Branch Outlets, ATMs, Phone and Internet Banking, Kiosks and Mobile Devices provide the freedom of choice to customers to transact using the channel they are comfortable with or which is available to them at ease” [1]. Such banks are generally found to be at a higher level of continuity from the customers’ perspective.

- **Customer Focus**

  “The implementation of core banking and other IT solutions have made the huge workforce of SBI available to undertake more value-added tasks such as supporting and helping customers” remarked the Assistant GM, State Bank of India (SBI), the largest public sector bank in India [2]. With the IT-enabled self-service transaction handling systems becoming common place in the banking industry, differentiation in products and services can only be achieved through a personalized customer-centric approach. The goodwill of customers results in their showing a greater degree of tolerance and support when the bank goes through troubled times. “The business does not stop (apparently) from the customer’s perspective even if there is a discontinuity that is short-lived. In other words, the tolerance limit of customers to accept disruptions is more if they are satisfied with the bank’s delivery systems”

- **Concept of “Bank Customer”, Not “Branch Customer”**

  “HDFC pioneered the concept of customers belonging to the bank and not a branch, as was the case prevalent then. A customer can transact in any branch of HDFC anywhere in India (now also abroad)”. [4] Customers are
viewed as “Bank Customers” and not “Branch Customers” from a BCM perspective.

- **Trust of Society at Large**

  Banks that serve various levels of society in urban and rural areas as well as in the personal and business segments enjoy a higher level of trust of society. “SBI is present, that too very significantly, in personal banking, industrial banking, corporate banking, rural banking, international banking etc. Almost the entire nation and that too all levels know the bank by way of personal experiences” remarked a senior official from SBI [5]. The participants of economic activity in society, wherein there is interaction between small, medium and large businesses as also between the moneyed and not-so-moneyed people, channel their banking relationships with certain large banks. Such banks enjoy greater trust and faith about their strength in terms of continuity, particularly, from the financial perspective. The customer does not feel insecure in investing in banks with larger net worth. Such banks hence enjoy very high level of continuity in the perception of society at large.

- **Rich Collaboration**

  Certain banks, for example, HDFC, have successfully entered into profit-sharing arrangements with a wide range of businesses to implement e-transactions in online shopping malls, railways, online trading and online auction sites [4]. These arrangements provide more outlets to effect transactions. The probability of disruptions is reduced through increase in the number of banking “touchpoints”.

- **Trusted Partnership**

  “A large public sector bank has teamed up with Tata Consultancy Services (TCS), the total IT solutions company for software project implementation, maintenance and system administration. The hardware is supplied, supported and maintained by HP. The network services are
maintained and managed by Data Craft. The partnership with these companies is a comprehensive one and is built on mutual faith and trust”. The partnering organizations such as TCS and HP see synergistic arrangements for mutual growth and are hence “locked-in” with the bank. Such arrangements are comprehensive, rugged, robust and scalable, thus ensuring a high degree of continuity.

- **Centralized Processing**
  Most large banks resort to central processing of a large number of transactions. “The infrastructure at the central hubs has adequate alternate and failsafe systems to ensure high availability and continuity”, remarked the AGM, SBI. This allows their employees to devote more time to customer service, as they are relieved of the back office processing work, which is pushed to central hubs.

- **Range of Customer Segments**
  Larger banks service a vast range of customer segments. “Differentiated and higher levels of service are rendered to certain specialty groups (high-value, retired, etc), thereby ensuring customer lock-in”. This bondage with satisfied customers leads to greater tolerance on their part, which will support the recovery phase of the bank when it has a major disruption.

- **Leverage Internal Strengths**
  Banks that synchronize their operations with the internal organization culture exhibit a greater resilience for combating eventualities. For example, if employees are comfortable with Lotus Notes, it would be advisable to use that tool for the unstructured workflow processes which are not covered by the core banking solution.
5.17 Hybrid Approach of “Old Economy” Manual and IT-Based Systems

“SBI, whilst embracing technology for automation, has retained its culture of the old-economy days of running business in branches. There are multiple delivery channels to transact business. However, experience has shown that when disaster hits, you need people to manage the crisis, particularly as regards emotions that are most important to defuse the situation. No technology can substitute this”. Banks in India ought to have a judicious mix of “manual” and “IT-enabled” processes as there are limitations of infrastructure, capital for investment and slow-changing mindsets.

5.18 Operational

The factors that go into development of operational processes and structure to ensure higher levels of Business Continuity in banks are discussed below:

- **Automation**

“It reduces reliance on human knowledge of processes thereby reducing dependence on specifically trained personnel and giving greater flexibility to the bank in utilization of its human capital and also allowing the work force to address more value-added activities” remarked Munish Mittal, Assistant Vice President of Information Technology, HDFC Bank [9].

- **Technology for Competitiveness**

Banks that endeavor to remain a leader in adopting the latest technology to enhance efficiency in delivering services such as B-to-B EDI systems show greater resilience. [8]

- **Product Innovations**

The wider the range of product options, the higher is the probability of continued business. “HDFC innovated in bringing differentiated products like Private Banking and Smart Cards. Private banking provides specialized
banking, financial and investment services to high net worth individuals and institutions. Smart Cards have multi-application capability (insurance, e-purse, toll payments, etc.) and can run on multiple technology platforms” [4].

- **Integration of Diverse Products**

Integration of diverse products using enterprise applications improves employee productivity and increased customer satisfaction by providing a single view across applications [1].

- **Innovations in Delivery Channels**

The bank that innovates in coming up with a wider range of services and products delivered reliably through multiple channels provides greater accessibility and availability to their customers. “Internet based self service solutions earn confidence of customers and improves chances of enhanced cross-selling” [7].

- **Multi-Channel Integration**

A high degree of integration of all channels of delivery improves efficiency and ensures greater promise as regards continuity owing to regular availability of a medium for transactions through multiplicity of touch points [1].

- **Finger on the Pulse of Technology**

Banks, who embrace technology for automated service delivery, benefit from higher degree of operating efficiency and continuity. “SBI has teamed up with Reliance Infocomm to install CDMA based wireless ATMs at remote locations. The bank has excellent electronic fund transfer solutions using STEPS and SEFT. The bank has advanced MICR processing equipment. It has Internet-based facility for handling trade finance transactions for corporate and commercial network branches”, remarked a senior official of the bank [10].
• **Optimal Utilization of Disaster Recovery (DR) Site**

  “HDFC’s DR site at Chennai is designed to ensure near zero data loss and is manned 24X7. The DR site is online and data from the banking system is replicated every 15 minutes and is designed for a quick changeover”. [11]

  The load is optimally balanced between the main site and the DR site, which takes the operating load at pre-designated instances. Large numbers of ATMs connect to the DR site for normal operations with a facility to changeover to the central site when required. This also keeps the staff as also the systems at the DR site fully functional and attentive. “There have been some instances in installations of other banks wherein the changeover to DR sites during failure have been delayed making the arrangement questionable” [11].

• **Physical Security**

  The access permissions and rights must be defined at various levels - administrators, operators and trainees - and should be closely regulated for use as well as change of roles. “The entry to the data center and sensitive areas is highly regulated through use of ID cards, security strings and biometrics. Movement of personnel and assets is regulated and logs are kept for monitoring and analysis. All without exceptions are required to declare contents and purpose of media being carried while moving from anywhere to anywhere within the organization”, as noted by an official of UTI Bank. [12]

• **Customer Sensitivity Monitoring**

  Progressive banks proactively test their employees for customer sensitivity on a regular basis. “UTI engaged in an initiative called Mystery Customer Shopping, wherein the project team members simulate an exercise by visiting bank branches as pseudo customers to observe and measure their behavior. They also visit other banks and benchmark the observations with their own bank and suggest improvements / modifications”. [12]
Optimizing the IT Workforce

The IT departments of banks, who have experienced success in their BCM implementation, comprise a rich blend of functional and technical specialists to ensure smooth flow of operations related to transactions and customer service. The HDFC experience is a case in point: “The areas of technology operations related to application support and facilities management are outsourced. The distribution of work to the right groups, both internal and outsourced, provides better resilience to meet any eventuality”. [11]

Location of Assets

“A large bank has taken special care to locate sensitive assets such as server rooms, communication equipment, data centers and work places in a manner that they are not affected by small and large accidents such as fire, flooding, etc” [6]. This aspect is often neglected and most important assets are generally housed in basements or in places which could be easily spared, whereas these have to be carefully located to withstand any unforeseen eventuality. “It is commonplace to find captive power plants, UPSs and air-conditioning equipments in the basements, which are affected the most in the unlikely event of flood and earthquakes”[6]. The major disruptions caused by the Mumbai deluge of July 26, 2005 are a testimonial to this danger.

Incidence Reporting and Monitoring

The practice of timely reporting and monitoring “exceptions” instill the right culture and resilience in the organization to ensure prevention of incidences, rather than looking for cures. The UTI practice states: “Our bank, where Vigilance is the watchword, ensures that all personnel log security incidences regularly. These are picked up, acted upon and subsequently analyzed by the helpdesk staff. The security coordinator and a high level
committee periodically analyze these reports, identify loopholes, work out methods to counter them and promulgate them organization-wide”. [12]

- **Internet Discipline**
  Progressive banks enforce strict guidelines for operators who connect to the Internet for operations or monitoring to ensure that good practices are followed to prevent security breaches [13].

- **Business Continuity Planning (BCP)**
  BCP in banks aims at ensuring minimum downturn of business and speedy recovery of work area and data center sites. It has well-documented and communicated actions to be taken during a crisis. “The BCP at UTI, developed with the help of TCS and IBM, is complete and comprehensive, and caters for a large number of discontinuities: technological, man-made and natural disasters. The plan is reviewed periodically for corrections and upgrades”. [12]

- **Proprietary versus Open Systems**
  “UTI’s IT infrastructure is supported on server and storage solutions (IBM pSeries Power4 plus and SAN) at their central data centre in Mumbai. The bank has made efforts to also create facilities on open systems hardware and software. This is primarily to leverage the excellent skills in UNIX and Linux present amongst the IT staff”. [14] Open systems provide an alternative to proprietary systems, which makes the organization “highly vendor-dependent”. It also presents options of running parallel systems at a lower cost but almost as efficient, thus enhancing resilience for continuity.

- **Relationship with Government Machinery**
  “SBI manages banking requirements of governments at Centre, State and large cities (municipal councils). The bank has relationships with most large and medium-sized corporate” remarked the Deputy GM, SBI. [5] These
relationships provide good support in the event of disasters as was seen in the recovery of the bank from major disruptions caused by forces of nature and man-made reasons in the recent past.

5.19 **Technological**

The following practices are crucial when setting up and operating technological structures to ensure a high level of continuity in banks.

- **Efficient Data Sharing**
  
  Banks should share data across products: banking, loans, investments, etc. This results in better information systems for bank operations. In addition, customers can obtain an integrated view of their business with the bank, creating both “real” and “virtual” continuity [15].

- **Reliable Data Protection**
  
  IT-enabled operations of gigantic volumes, such as those experienced at the data center of a bank, can only be sustained by providing appropriate protection. The enterprise servers coupled with appropriate positioning of security infrastructure should provide data protection at various levels while transactions are in process [15].

- **Balanced Portfolio of Applications**
  
  “The bank using the right combination of standard core banking solution from quality software providers and in-house developed tools, which provide higher efficiency and are more comfortable for the workforce, is less dependent on a particular vendor. This ensures higher degree of Business Continuity”, remarked a senior official of ICICI Bank [16].

- **Best-In-Class IT Infrastructure**
  
  The IT infrastructure ought to be scalable and should deploy the latest technology. “The use of latest technology ensures faster response, higher
security, better accessibility, higher productivity and uninterrupted business. The infrastructure ought to be built using best-in-class servers, highest-level available security scheme and a rugged and reliable mesh network to support high-speed and secure data transmissions”, as noted by the ICICI bank official [16].

- **Data Centre Availability and Disaster Recovery**
  The dynamic requirements of progressive banks necessitate the establishment of quality and world class data centre(s) together with a Disaster Recovery site to provide a highly reliable and efficient IT setup that ensures availability and data protection. “The hardware, software and data communication setup needs to be maintained by partners who have the ability to solve a whole class of problems and not just the elements provided and supported by them” [8].

- **Disaster Recovery Setup**
  “SBI’s main data centre is at Belapur, which houses the central database in a hierarchical client server setup. The bank’s disaster recovery setup is at Chennai. The DR setup at Chennai is designed for a Recovery Time Objective (RTO) of five hours. The DR site is manned 24X7 and has adequate changeover facilities” [13]. The data centre was hit briefly during the Mumbai floods, which affected banking operations throughout the bank since most banking solutions are now Internet-based. “The problem was with the location of power supply units in the basement which got flooded and hampered process of recovery” according to the DGM, SBI [10].

- **Shared Storage Options**
  Banks have to handle humongous growth of data, particularly, when using a common database across products and services and multiple delivery channels. This necessitates deployment of fast but reliable data storage both for online operations and backups. The bank storage, therefore, has to be a
perfect blend of disk and tape-based online storage-cum-backup arrangements using heterogeneous platforms which are monitored by advanced tools [8].

- **Systems Administration**

  Banks ought to invest regularly in training the technical staff on key aspects of network and systems administration to ensure smoothness of operations [15].

- **Backup**

  Storage on Network Attached Storage (NAS) enhances recovery capabilities as the storage device can be located anywhere on a Local Area Network (LAN) and these devices have all the functionalities of a server. “A large bank that currently deploys SAN is also contemplating installation of NAS. The bank enforces strict policy of regular backups” [11].

- **Database Security**

  This is implemented by configuring and executing integrity checks at multiple levels: user level, application level and data administration level [12].

- **IT Security**

  IT security should be implemented at both the systems and user levels. The system level security is implemented at the network level by installing catalyst switches and Intrusion Detection System (IDS). Intra- and inter-application level security is implemented through access control using authentication at application ports and firewalls. This creates VLANs for applications running on various delivery channels. “UTI enforces access control using the model of PKI deploying “certifying authority servers” for administering “session keys” and “registration authority servers” for generating digital signatures” [14].
• **Speedy Server Rebuilding**
  The multiplicity of operations across diverse platforms makes server rebuilding an essential requirement. “The Net Backup Bare Metal Restore Option has enabled ICICI to reduce server rebuilding time by almost 50 percent”. [8]

• **Redundancy of Hardware and Network**
  Building appropriate redundancy improves continuity levels. “HDFC’s infrastructure has redundant hardware and systems to ensure a higher degree of continuity. Each branch connects to a regional hub as well as to a central data centre with a quick changeover option. There are multiple data links, both leased and private, to facilitate data transfer”

• **Network Management**
  Managing networks using remote control systems enables IT staff to install, manage, de-install and upgrade software from a central location thereby improving efficiency of Network Management and enhancing continuity. “HDFC deploys Unicentre remote control solution to manage its network which has resulted in high efficiency in managing the infrastructure and savings. The solution being network-based and with alternate pathways in it comes handy while recovering systems from failure remotely”. [11]

• **Internet Banking Software**
  Web-based banking solutions provide multi-exchange, multi-segment, multi-currency, single-window and intelligent decision support system for proactive client management. “The customizable and user-friendly environment provided by Internet-based banking solutions prevents blockages of transactions due to lack of information and thus enhances continuity” [17].

• **Server and Storage Consolidation**
  Currently most large banks are bringing in state-of-the-art infrastructure practices such as server virtualization and consolidation to
reduce the clutter of servers. This is effected by better utilization of servers located anywhere in the setup, not just the central data centre, which are made to work as central servers (virtually). “This provides greater degree of resilience, as all eggs are not in one basket, i.e., all servers in the central data centre”. [11]

5.20 Status of Bcm Essentials In Banks – A Snapshot

The essential ingredients “as they exist” and “as they should be” have been analyzed on the basis of the interviews conducted with 26 senior officials of the selected banks.

Each of the “essential ingredients” discussed in Section 4 under “Strategic”, “Operational”, and “Technological”, was evaluated in terms of the perceived Importance or Criticality (the “should be”) versus the existing Status (the “as is”) in the bank. The findings are summarized below for each of the three clusters.

Table: 5.6 Strategic

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Essential Ingredient</th>
<th>Importance/Criticality (% respondents)</th>
<th>Status in Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Multiple Delivery options</td>
<td>90</td>
<td>65</td>
</tr>
<tr>
<td>2.</td>
<td>Customer Focus</td>
<td>85</td>
<td>80</td>
</tr>
<tr>
<td>3.</td>
<td>Concept of “Bank Customers”</td>
<td>80</td>
<td>65</td>
</tr>
<tr>
<td>4.</td>
<td>Trust of Society at Large</td>
<td>80</td>
<td>50</td>
</tr>
<tr>
<td>5.</td>
<td>Rich Collaboration</td>
<td>75</td>
<td>55</td>
</tr>
<tr>
<td>6.</td>
<td>Trusted Partnership</td>
<td>75</td>
<td>55</td>
</tr>
<tr>
<td>7.</td>
<td>Centralized Processing</td>
<td></td>
<td>65</td>
</tr>
<tr>
<td>8.</td>
<td>Range of Customer Segments</td>
<td></td>
<td>50</td>
</tr>
<tr>
<td>9.</td>
<td>Leverage Internal Strengths</td>
<td>55</td>
<td>40</td>
</tr>
<tr>
<td>10.</td>
<td>Hybrid Approach of “Old Economy” Manual and IT-Based Systems</td>
<td>50</td>
<td>40</td>
</tr>
</tbody>
</table>
“Customer Focus” is the only essential ingredient where the current Status has matched the perceived Importance / Criticality. This is true to a slightly lesser extent with regard to “Centralized Processing”. Stark differences are seen for five other ingredients, #s 1, 3, 4, 5 and 6, where the Status is at a much lower level than the highly-rated Importance / Criticality of that ingredient. Three of the ingredients, #s 8, 9 and 10, were rated lower than the others in terms of Importance / Criticality; and, the current Status of these ingredients is also low.

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Essential Ingredient</th>
<th>Importance/Criticality (% respondents)</th>
<th>Status in Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Automation</td>
<td>90</td>
<td>80</td>
</tr>
<tr>
<td>2.</td>
<td>Technology for Competitiveness</td>
<td>90</td>
<td>75</td>
</tr>
<tr>
<td>3.</td>
<td>Product Innovations</td>
<td>80</td>
<td>70</td>
</tr>
<tr>
<td>4.</td>
<td>Integration of Diverse Products</td>
<td>85</td>
<td>65</td>
</tr>
<tr>
<td>5.</td>
<td>Innovations in Delivery Channels</td>
<td>85</td>
<td>65</td>
</tr>
<tr>
<td>6.</td>
<td>Multi-Channel Integration</td>
<td>90</td>
<td>70</td>
</tr>
<tr>
<td>7.</td>
<td>Finger on the Pulse of Technology</td>
<td>80</td>
<td>65</td>
</tr>
<tr>
<td>8.</td>
<td>Optimal Utilization of DR Site</td>
<td>70</td>
<td>70</td>
</tr>
<tr>
<td>9.</td>
<td>Physical Security</td>
<td>70</td>
<td>80</td>
</tr>
<tr>
<td>10.</td>
<td>Customer Sensitivity Monitoring</td>
<td>70</td>
<td>55</td>
</tr>
<tr>
<td>11.</td>
<td>Optimizing the IT Workforce</td>
<td>65</td>
<td>55</td>
</tr>
<tr>
<td>12.</td>
<td>Location of Assets</td>
<td>65</td>
<td>65</td>
</tr>
<tr>
<td>13.</td>
<td>Incidence Reporting and Monitoring</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>14.</td>
<td>Internet Discipline</td>
<td>55</td>
<td>50</td>
</tr>
<tr>
<td>15.</td>
<td>Business Continuity Planning</td>
<td>55</td>
<td>50</td>
</tr>
<tr>
<td>16.</td>
<td>Proprietary versus Open Systems</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>17.</td>
<td>Relationship with Government Machinery</td>
<td>50</td>
<td>40</td>
</tr>
</tbody>
</table>
Ingredients 1, 2, 3, 4, 5, 6 & 7 are all rated highly with regard to Importance / Criticality, whereas Status reasonably matches this requirement only for “Automation”. For the other 6 ingredients rated highly, the Status is only at a moderate level.

Interestingly, “Physical Security” is the only ingredient where the Status is rated higher than Importance / Criticality.

Four of the ingredients, #s 14, 15, 16 & 17, received a low Importance / Critical rating that is matched by the current Status in the bank.

Table : 5.8 Technological

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Essential Ingredient</th>
<th>Importance/Criticality (% respondents)</th>
<th>Status in Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Efficient Data Sharing</td>
<td>90</td>
<td>80</td>
</tr>
<tr>
<td>2.</td>
<td>Reliable Data Protection</td>
<td>90</td>
<td>85</td>
</tr>
<tr>
<td>3.</td>
<td>Balanced Portfolio of Applications</td>
<td>85</td>
<td>70</td>
</tr>
<tr>
<td>4.</td>
<td>Best-In-Class IT Infrastructure</td>
<td>80</td>
<td>65</td>
</tr>
<tr>
<td>5.</td>
<td>Data Centre Availability and DR</td>
<td>80</td>
<td>70</td>
</tr>
<tr>
<td>6.</td>
<td>Disaster Recovery Setup</td>
<td>80</td>
<td>70</td>
</tr>
<tr>
<td>7.</td>
<td>Shared Storage Options</td>
<td>75</td>
<td>65</td>
</tr>
<tr>
<td>8.</td>
<td>Systems Administration</td>
<td>75</td>
<td>75</td>
</tr>
<tr>
<td>9.</td>
<td>Backup</td>
<td>75</td>
<td>80</td>
</tr>
<tr>
<td>10.</td>
<td>Database Security</td>
<td>75</td>
<td>75</td>
</tr>
<tr>
<td>11.</td>
<td>IT Security</td>
<td>70</td>
<td>70</td>
</tr>
<tr>
<td>12.</td>
<td>Speedy Server Rebuilding</td>
<td>65</td>
<td>60</td>
</tr>
<tr>
<td>13.</td>
<td>Redundancy of Hardware and Network</td>
<td>65</td>
<td>55</td>
</tr>
<tr>
<td>14.</td>
<td>Network Management</td>
<td>65</td>
<td>55</td>
</tr>
<tr>
<td>15.</td>
<td>Internet Banking Software</td>
<td>55</td>
<td>50</td>
</tr>
<tr>
<td>16.</td>
<td>Server and Storage Consolidation</td>
<td>55</td>
<td>50</td>
</tr>
</tbody>
</table>
“Efficient Data Sharing” and “Reliable Data Protection” are two highly rated ingredients with regard to Importance / Criticality, which are also matched reasonably by the current Status in the selected banks. Four ingredients, “System Administration”, “Backup”, “Database Security” and “IT Security”, on the other hand, stood out since the Status is rated on par or even a little higher than Importance / Criticality for these ingredients.