13

Regulation of E-finance Institutions

The question of regulating the financial institutions assumes a totally new context particularly after the recent financial debacle. The chapter on 'Risk Management' dealt with recommendations made by Lord Turner in his report to the Chancellor of the Exchequer. Until now one was groping in the dark as to the likely shape of events to come. After the G20 summit (April 2009), the lines are more clearly drawn and the approaches likely to be adopted are also quite clear. One thing is certain, the regulators would not be mere passive observers. The expectation that the market would take care of such deviant behaviour is no longer the mantra; it would be a regulator with a heavy hand. The taxpayers expect deviant behaviour to be severely dealt with. In fact, there would be stringent rules and the scope of regulation would be much wider.

Before elaborating on these topics, two important terms have to be distinguished viz. regulation and supervision. Regulation generally deals with the formation of rules that are on the one side part of the legislation and, thus, approved by national parliaments, and on the other side, rules that are implemented by administrative bodies. Contrary to this, supervision deals with the enforcement of such rules, either *ex ante* in the form of control or *ex post* in the form of sanctions.

During the last two years it has become quite clear that regulating today's super markets in financial services is much more complex a task than is apparent. It is, therefore, necessary for the various authorities, whether working under the same roof like the Financial Services Authority in UK or different bodies working independently, to coordinate their activities and work in close cooperation with each other. It would perhaps be useful if the supervision by objectives approach was adopted and the desired

coordination achieved. However, this section does not detail the broader aspects of regulation; it is restricted to the narrower distribution channel issues.

It has been suggested that the safety and soundness of the Indian banking system, and the part played by the regulators in this behalf, must be highlighted and that the regulators should take steps to actively promote the financial system and ensure that Asian customers as also European and American institutional investors, feel confident about these aspects. Perhaps the RBI could, as in the past, take a lead in promoting investments in advanced technology, ensure adoption of security measures and also make it a point to evaluate the quality of staff deployed. This may be frowned on, but in today's context it is necessary. After all content control could be exercised only under direct supervision. Merely dubbing them as devils on Wall Street would not help.

The 'supervision by objectives' approach is based on the idea that all financial intermediaries and markets are subject to the control of more than one authority. In this regard, each authority is responsible for one objective of regulation regardless of both, the legal form of the intermediaries as well as the functions or activities they perform. The advantage of this approach, which was chosen for example in Australia, is that it is particularly effective in a highly-integrated market context. Therefore, this approach does not require an excessive proliferation of control units. Nevertheless, a regulatory framework organized by objectives has the side effect of a certain degree of multiplication of controls and can, therefore, lead to a lack of controls. Additionally, each intermediary is subject to the control of more than one authority, which might be more costly and moreover the administrative burden for financial intermediaries is significantly increased. However, costs need not deter us at this stage. It is a price to pay for demonstrating the superiority of our systems.

The functional supervisory model postulates a given financial system considered to perform the following basic functions: *(a)* provision of ways of clearing and settling payments in order to facilitate trade; *(b)* provision of a mechanism for the pooling of resources and for portfolio diversification; *(c)* provision of ways of transferring economic resources through time, across boarders and among industries; *(d)* provision of ways of managing risks; *(e)* provision of price information in order to help the coordination of decentralized decision making in the various sectors of the economy and *(f)* provision of ways of dealing with the incentive problems created when one party in transaction has information that the other party does not have or when one party acts as agent for another. This reflects on market

efficiencies and arises on account of information asymmetry. However, each type of financial services is regulated by a given authority independent of the operator who offers the services. Therefore, the advantage of this approach is the requirement of the same rules being applied to intermediaries performing the same activities of financial intermediation despite the fact that the operators may fall into different categories from a legal point of view. Moreover, this approach fosters economies of specialization within supervisory authorities and represents an attractive solution for the regulation of integrated and advanced financial markets. Nevertheless, it includes the risk of excessive division of competencies among regulatory agencies.

One perhaps would need a supranational authority both for supervising cross-border transactions and for avoiding regulatory arbitrage advantages/disadvantages. It is true that with coming up of the supermarkets in financial services sector, there is a need for a single authority like the Financial Services Authority (FSA) in UK/Scandinavian countries to overview the myriad functions undertaken by these financial entities. Today, after seeing the AIG debacle, the need for such a body is keenly felt. However, the creation of such a body will have to be viewed from an efficiency perspective also. Additionally, the creation of such a centralized authority at the supranational level has to be critically seen not only on the grounds of excessive concentration of power, but also on a lack of accountability. Moreover, there does not seem to be empirical evidence that justifies the superior wisdom of any given model of organizing financial supervision.

The Regulatory Content

The suitability of structures has been dealt with so far. The most important question, however, pertains to the methods which the regulator should adopt to ensure the stability of the system. Equally important is the need to save ourselves from the rogue traders ruining us. How could we let greed and avarice overtake sound business practices? Notwithstanding costs, the regulatory net will have to be cast wider. In the first place, the regulatory systems must be strengthened by bringing in auditors, company secretaries, by publishing risk-based audit reports with management outlook on the future developments and board perception of risk appetite, and so on, every quarter. Further stringent penalties under star chamber systems should also be permissible for gross negligence of systemic security and/or false reporting. Crying hoarse against regulatory costs is easy. Adhering to

strict financial discipline should not be ignored. It is only with a judicious combination of severe penal actions and rigid review that one could break the present unhealthy nexus between rogue traders and bonus dispensers.

Some of the wider questions that need to be handled have been discussed in the following paragraphs. One needs to pay attention to the questions of internet security systems and adhere to guidelines issued by regulators like SEBI. At this stage, we are concerned with the limited question of handling internet security and assume that the wider question of judicious balance between the market freedom and regulatory requirements would be resolved soon.

E-BROKING

Currently, the entire focus of the regulators is on evolving suitable strategies for salvaging the financial institutions and to ensure that the systemic risks are kept within reasonable limits so that the boat does not get rocked by such tremors. These are very genuine concerns, but it is precisely at such times that organizational vigilance has to be in a high state of alert so that fraudsters within and without do not take advantage of the fact that management's attention is focused on much wider issues than on rigid adherence to internal controls. Large scale retrenchment might have created gaping holes in the hierarchical structure and that deciding on lines of control might have been put on the backburner.

The main area of concern for the regulators and senior managements would be to ensure that dealers and others do not resort to excessive risk taking and that the bonuses likely to be paid out do not decide the fate of the organization. The Societe Generale fraud case is a classic example of the laxity of controls. Equally significant, is the case of AIG's credit swap trades, which brought down the entire edifice. It is true that some of these activities were carried on because regulators pleaded inability to control the hedge funds or as in the case of derivative trade did not want to regulate them. The dogmatic belief in market mechanisms could also come in for a great degree of blame in these cases.

Regulation of Broking Services offered through the internet comes under the jurisdiction of SEBI. In 2000 SEBI had issued guidelines for listing of brokers on the stock exchanges. But the circular is not readily available and one has to go to SEBI's website to get the original circular. Since these guidelines are applicable even now, some of the important ones are listed in the following pages for the benefit of the readers.

Operational and System Requirements

Operational Integrity: The stock exchange must ensure that the system used by the broker has provision for security, reliability and confidentiality of data through use of encryption technology. (Basic minimum security standards are specified in following paragraphs.) The stock exchange must also ensure that records maintained in electronic form by the broker are not susceptible to manipulation.

System Capacity: The stock exchange must ensure that the brokers maintain adequate backup systems and data storage capacity. The stock exchange must also ensure that the brokers have adequate system capacity for handling data transfer and must arrange for alternative means of communications in case of internet link failure.

Qualified Personnel: The stock exchange must lay down the minimum qualification for personnel intending to work as assistants to the brokers. This is to ensure that the broker has suitably qualified and adequate personnel to handle communication, including trading instructions as well as other back office work which is likely to increase in future.

Written Procedures: Stock exchange must develop uniform written procedures to handle contingency situations and for review of incoming and outgoing electronic correspondence.

Signature Verification/Authentication: It is desirable that participants use authentication technologies. For this purpose, it should be mandatory for participants to use certification agencies as and when notified by the government/SEBI. They should also clearly specify when manual signatures would be required.

Client–Broker Relationship

Know Your Client: The stock exchange must ensure that brokers comply with all requirements of 'Know Your Client' and have sufficient, verifiable information about clients, which would facilitate risk evaluation of clients.

Broker–Client Agreement: Brokers must enter into an agreement with clients spelling out all obligations and rights. This agreement should also include *inter alia*, the minimum service standards to be maintained by the broker for such services specified by SEBI/Exchanges for the internet-based trading from time to time.

Exchanges will prepare a model agreement for this purpose. The broker agreement with clients should not have any clause that is less stringent/contrary to the conditions stipulated in the model agreement.

Investor Information: The broker website providing the internet-based trading facility should contain information meant for investor protection such as rules and regulations affecting client–broker relationship, arbitration rules, investor protection rules, and so on. The broker website providing the internet-based trading facility should also provide and display prominently, hyperlink to the website or page on the website of the relevant stock exchange(s) displaying rules/regulations/circulars. Ticker/quote/order book displayed on the website of the broker should display the time stamp as well as the source of such information against the given information.

Order/Trade Confirmation: In addition to display of order/trade confirmations on real-time basis on the broker website, such confirmation should also be sent to the investor through email at client's discretion within the time period specified by the client. The investor should be allowed to specify the time interval on the website itself within which he would like to receive this information through email. Facility for reconfirmation of orders which are larger than that specified by the member's risk management system should be provided on the internet-based system.

Handling Complaints by Investors: Exchanges should monitor complaints from investors regarding service provided by brokers to ensure a minimum level of service. Exchanges should have separate cell specifically to handle internet trading related complaints. It is desirable that exchanges should also have facility for online registration of complaints on their website.

Risk Management

Exchanges must ensure that brokers have a system-based control on the trading limits of clients and exposures taken by clients. Brokers must set pre-defined limits on the exposure and turnover of each client.

The broker systems should be capable of assessing the risk of the client as soon as the order comes in. The client should be informed of acceptance/rejection of the order within a reasonable period. In case system-based control rejects an order because of client having exceeded limits, the broker system may have a review and release facility to allow the order to pass through.

Reports on margin requirements, payment and delivery obligations, and so on, should be informed to the client through the system.

Contract Notes

Contract notes must be issued to clients as per existing regulations, within 24 hours of the trade execution.

Cross Trades

As in the case of existing system, brokers using internet-based systems for routing client orders will not be allowed to cross trades of their clients with each other. All orders must be offered to the market for matching.

It needs to be emphasized that in addition to the requirements mentioned previously, all existing obligations of the broker as per current regulation will continue without changes. Exchanges should specify more stringent standards as they may deem fit for allowing internet-based trading facilities to their brokers.

Similar guidelines are also issued by SEBI for brokers offering securities trading through wireless medium on WAP platform. These guidelines are readily available in handbooks issued by publishers like Taxman and could be referred to by the readers. The same could also be seen on SEBI website (www.sebi.gov.in).

For ready reference a brief summary of the mandatory system is provided.

Brief Summary

The system flow of the STP framework would be as follows:

- An STP user intending to send an instruction would send the message to his STP service provider after digitally signing the same.
- The STP service provider would verify the signature of the STP user and forward it to the:
    - recipient STP user, if the recipient STP user is availing services of the same STP service provider; or the
    - STP centralized hub if the recipient STP user is not with the same STP service provider. In such a case, the STP service

provider would be required to prepare a message as per the STP centralized hub prescribed message format, enclose the user's message, digitally sign the message and then send it to the STP centralized hub.

- On receipt of the message by the STP centralized hub, the STP centralized hub would:
  - verify the signature of the sending STP service provider only;
  - send an acknowledgment to the sending STP service provider.
- The STP centralized hub would forward the message to the recipient STP service provider after digitally signing on the message.
- The recipient STP service provider on receipt of the message from the STP centralized hub shall verify the signature of the STP centralized hub, verify if the recipient STP user is associated with it and send an appropriate acknowledgment with digital signature to the STP centralized hub. The STP centralized hub would in turn forward the acknowledgment (received from the recipient STP service provider) duly signed to the sending STP service provider.
- The recipient STP service provider shall forward the message to the recipient STP user. The recipient STP user would receive the message and verify the signature of the recipient STP service provider and sending STP user.
- To enable inter-operation, the STP centralized hub would provide a utility/client software to the STP service provider. The STP service provider's point of interface with the STP centralized hub would be through this utility/client software. The PKI (public key infrastructure) system for the interface shall be implemented at a later stage.

The Insurance Sector

This section discusses issues relating to regulation of insurance activities on the internet. The International Association of Insurance Supervisors has brought out a report dealing exclusively with the principles on the supervision of insurance activities on the internet. The recommendations and the rules made by Insurance Regulatory and Development Authority (IRDA) in India have been reviewed in the following pages. The internet creates a new environment in which insurance products can be advertised, sold and delivered, but it does not alter the fundamental

principles of insurance and insurance supervision. It is a new medium o transact business. The Association is rightly concerned about substantial risks to consumers. The opportunities for fraud, money laundering and the miss selling of insurance products, have, no doubt, been considerably enhanced. The supervisors, thus, have an added responsibility to protect the consumers in their jurisdiction. The questions of applicability of a given contract law and the means of redress in case of a dispute are important issues that need to be settled.

The Association suggests that that the supervisors must ensure that the sale, purchase and delivery of insurance are conducted in a secure environment.

Principle 1: Consistency of Approach

'The supervisory approach to insurance activities on the internet should be consistent with that applied to insurance activities through other media' (International Association of Insurance Supervisors 2002).

The Association indicates the areas where supervisors must assert their authority over internet activities.

- When an internet site is targeted at residents and/or risks within the supervisors' jurisdiction.
- When insurance activities are provided via the internet site to residents in the supervisors' jurisdiction.
- When information is presented to potential policyholders within the supervisor's jurisdiction through proactive means.

Principle 2: Transparency and Disclosure

'Insurance supervisors should require insurers and intermediaries over which they exercise jurisdiction to ensure that the principles of transparency and disclosure applied to internet insurance activities are equivalent to those applied to insurance activities through other media' (International Association of Insurance Supervisors 2002).

It is suggested that the insurer must disclose the address of the head office, the branch office and the jurisdiction in which the insurer can offer such services. It is also necessary that the procedure for the submission of claims and claim handling procedures be indicated.

Principle 3: Effective Supervision Based on Cooperation

'Supervisors should cooperate with one another, as necessary, in supervising insurance activities on the internet' (International Association of Insurance Supervisors 2002).

The regulation of internet activities based purely on actions capable of being taken in a single jurisdiction is often inadequate. Therefore, a greater degree of cooperation between supervisors is a must. The Association takes note of operational risks and suggests a close scrutiny of the control mechanism by the insurer.

A truly significant departure is the insistence on the need for the supervisors to observe transparency and their recommendations for disclosure of information through annual reports of the supervisory authority, links to other websites, relevant statistics, and so on. They are quite right in suggesting that the supervisors should publish texts of relevant legislation on their websites.

The approach is somewhat superficial. One gets a feeling that they are hesitating to tread into uncharted areas. The banking supervisors have gone into these matters in a much more detailed manner. Perhaps, the conceptual debate about intervention and leaving it to the market is still not sufficiently tilted in favour of one or the other and, hence, the hesitation. These are sensitive areas and need a greater clarity of approach. It cannot be left to evolve over a period of time.

Monetary Policy Implications

Certain aspects of monetary policy, which have not been discussed at length till now, like the growing body of credit card users with ever-increasing drawing limits, are now posing significant problems. Add to these, currencies like 'Beeze' or other similar ones and one can understand the woes when consumers start reacting to these newer modes of payment.

There are many who scoff at the idea of any relatively inconsequential device morphing into a major competitor for the US Dollar or the Pound Sterling. It would, in our view, not be at all correct to brush aside the whole subject as ridiculous. Non-banks such as universities and transit systems already issue smart cards backed by the ability of the sponsor to pay. Put these or similar cards in an open environment where they are accepted as vehicles and a 'new' currency is available. Together with e-purses, these could provide a formidable area needing control. A possible e-commerce

multi-currency worldview is given in Table 13.1 with details regarding 'New Ways of Paying On-line'.

There are round the world rules against fictitious instruments. But they are not applied to the area of electronic currency. The general apprehension is that once instability sets in, it would be difficult and too late for any remedy. Some European countries have, in our view, rightly allowed only banks to issue such 'currencies'. Further, if and when banking functions get carried out by multiple uncoordinated financial and non-financial entities, who would strive to bring about the 'stability' which is the bedrock of the system. It would not be wrong to say that sound currency and monetary control is more difficult to maintain in this New World of fragmented financial players and multiple currencies. The computers and telecommunication devices have enabled non-bank companies to simulate banking services that customers cannot distinguish. The same forces will enable banks to simulate the functions of currency even though it is not 'legal tender'. The only conclusion is that forces that could destabilize need to be channeled appropriately.

This brings us to the next question. Are smart cards, e-purses covered by deposit insurance? Perhaps, the wider question of safety nets in the financial sector needs to be addressed. Should these instruments be treated separately from other economic agents? In today's world many substitutes for banks' deposit products have emerged and are emerging. Alternate payment mechanisms have also developed. E-finance allows non-deposit taking financial institutions and capital markets to reach far more depositors as well as borrowers. It would not be wrong to say that the whole gamut of 'safety net' is in a melting pot. One could even plead for such safety nets

Table 13.1 New Ways of Paying On-line

	A Guide to a New Generation of On-line Payment Systems	
Company	*Merchant/Content Partner*	
Cyber Gold	Earn and spend programme, Click on ads and spend in network	Animation Factory, Axis3d ZDNet, CD world
E-charge	Advance payment with on-line bank account	
Ipin	Charges digital content to ISP bill	E-music, AT&T music, Virgin Radio, BBC
Millicent	Digital wallets with Milicent 'scrip'inside	Asahi.com. Oxford University Press, and so on

Source: *Journal of Lending and Credit Risk Management*, December 1999–2000.

being extended to other non-deposit institutions. After this the questions relating to the structure and the wider question of currency guarantee need to be addressed. Obviously, the question is related to the consumer protection issue. How do we protect the investors/depositors? Should we lay down minimum standards for institutions and self-regulatory agencies? Equally important is the problem of enforcement. How are these policies to be implemented and by whom?

Smart/Debit Cards

Reserve Bank of India has issued specific guidelines (RBI circular FSC. BC.123/24.01.019/99-2000) to banks, which intend to issue these cards. The Boards of Banks are authorized to decide on issuing such cards and banks have been asked to shoulder responsibility for monitoring the operations. Banks are further advised to ensure safety of these cards. In fact, the losses incurred by customers on account of breach of security or its failure, would have to be borne by the banks. Banks also need to have in place an arrangement for 24-hour notification of loss, theft, and so on of the cards.

Competition Policy

There is an acute need for global coordination. A series of questions could be posed at this stage and the answers could well depend on certain value premises and the ground realities.

- Would free trade in financial services be the order of the day? It would logically be followed by an equally important question viz. should it be so?
- Should there be free entry? No longer would scale and scope economies be barriers to entry.
- Do we have to reanalyse concepts like markets/competition?

Perhaps, the question could be narrowed down to deciding which payment services should fall under regulatory oversight and which institutions should have access to the payment system? The other alternative is to define them narrowly and restrict it to deposit taking institutions chartered by the regulator. These are important issues and need to be debated and discussed at a time when they have not assumed serious proportions. It is necessary to be ready to meet the contingencies when they arise. The more urgent questions regarding regulation of existing institutions and the

ones coming on the scene remain and need to be addressed. But that does not justify leaving futuristic issues untouched.

A combination of prescriptive measures suggested by the BIS and examination techniques proposed by FDIC are a good starting point. There is considerable unanimity about the proposals made and one is on a safe wicket in adopting them.

The existing risk management principles must be tailored, adapted and in some cases, extended to address specific risk management challenges created by the peculiar characteristics of e-banking activities. 'The RBI could extend the policies enunciated in 1998 [RBI Circulars dealing with Asset/Liability Management and Risk Management: Nos. *(a)* DBOD No. BP.BC.94/21.04.098/98 and *(b)* DBOD.No. BP(sc.BC.98/21.04.103/99)] and make it mandatory for banks to adopt the suggestions made by BIS in its report on 'Risk Management Principles for Electronic banking' (as quoted from a report by Bank for International Settlement, Basel) in consultation with RBI. BIS is quite right in asserting that setting detailed risk management requirements must not be counter productive. Each bank's risk profile is different and requires a tailored approach for risk mitigation appropriate for the scale of e-banking operations, the materiality of risks present, and the institute's willingness and ability to manage the risks. This does imply that one-size fits all approach to e-banking risk management may not be universally suited.

Broadly the risk management efforts fall into three groups as discussed further.

Management Oversight

Effective management oversight of the risks associated with e-banking needs to be in place and risk management should be integrated with overall risk management. There must be an explicit, informed and documented strategic decision–covering specific accountabilities, policies and controls, to address risks. Key aspects of security control process must be covered.

Security Controls

These should include appropriate control processes such as *(a)* authorization measures, *(b)* authentication measures, *(c)* logical and physical controls, *(d)* adequate security to maintain appropriate boundaries, *(e)* restrictions on both internal and external user activities, *(f)* data integrity and *(g)* audit trails.

Due Diligence

This includes comprehensive due diligence and management oversight processes for outsourcing relations and third party dependencies.

Security Controls

- Authentication of e-banking customers.
- Non-repudiation and accountability for e-banking transactions.
- Appropriate measures for segregation of duties.
- Data integrity of e-banking transactions, records and information.
- Establishment of clear audit trails for e-banking transactions.
- Confidentiality of key banking transactions.
- Legal and reputational risk management principles.
- Appropriate disclosures for e-banking services.
- Privacy of customer information.
- Capacity, business continuity.
- Contingency planning to ensure availability of e-banking services.
- Indent response planning.

Against the backdrop of information given here the committee has developed the following 14 key risk management principles:

- Management oversight.
- Management of outsourcing and third party dependencies.
- Segregation of duties.
- Proper authorization measures and controls.
- Clear audit trails.
- Authentication of all entities, counterparts and data.
- Non-repudiation of e-banking transactions.
- Comprehensive security.
- Integrity of banking transactions, records and information.
- Appropriate disclosure for e-banking services.
- Confidentiality and privacy of customer information.
- Business continuity and contingency planning.
- Incident response planning.
- Role of supervisors.

The aforementioned suggestions, need to be supplemented with a report prepared by FDIC for bank examiners. The salient features of the suggestions have been listed in the following paragraphs. The summarized

version is in two parts. The standards represent performance objectives to ensure that the bank operates in a safe and sound manner and that the bank's objectives are carried out. Associated risks represent potential threats because of failure to adhere to such standards. The supervisors are advised to look into these areas to see that the banks operate in a safe environment and that the institution's objectives are carried out properly.

The examiners have to ensure that the systems are used with clear strategic direction and with a comprehensive risk management programme. They are apprehensive that critical units may have been excluded from the planning process and that a proper evaluation of costs may not have been made. Further, they are worried that the systems would be such that customer demands would not adequately met. It is noteworthy that the supervisors are keen on ensuring that policies and procedures adequately address the impact on bank activities, operations or security. It is recommended that adequate training of staff on proper controls and potential risks is undertaken. Therefore, the board must establish the standards for overall performance and systems operations. Further, internal and external auditors are advised to review alternate delivery systems. Security of information systems is bound to attract the attention of the supervisors. Outsourcing is the order of the day. Needless to add, such arrangements need to be critically examined by the regulators.

FDIC has recommended the review of following features at the time of examination.

- Planning and implementation.
- Operating procedures and policies.
- Audit.
- Legal and regulatory matters.
- Administration.
- Outsourcing arrangements.

A noteworthy feature is the recommendation that, whenever required, experts may be called in to assist the supervisors. One finds that the examination 'manual', if it could be so described, is a public document and institutions can use it to guide them through a very difficult transition phase.

To conclude, it can be said that in the emerging scenario it is essential for financial institutions, technology firms, auditors and regulators to work closely together in evolving appropriate solutions to safeguard the customer interests, and those of the institutions and of the system as a whole. The newer systems need to be nurtured carefully in the initial stages.