# Electronic Banking Group Initiatives and White Papers

**Basel Committee for Banking Supervision**

Basel
October 2000

# Electronic Banking Group
# of the Basel Committee on Banking Supervision

**Chairman:**
**Mr John D. Hawke, Jr. – Comptroller of the Currency, Washington, D.C.**

| | |
|---|---|
| Commission Bancaire et Financière, Brussels | Mr Koen Algoet<br>Mr Jos Meuleman |
| Office of the Superintendent of Financial Institutions, Ottawa | Ms Judy Cameron<br>Mr Brad Sullivan |
| Commission Bancaire, Paris | Mr Alain Duchâteau<br>Mr Jerôme Deslandes |
| Deutsche Bundesbank, Frankfurt am Main | Ms Magdalene Heid<br>Mr Andi Kloefer |
| Bundesaufsichtsamt für das Kreditwesen, Berlin | Mr Uwe Neumann |
| Banca d'Italia, Rome | Mr Filippo Siracusano |
| Bank of Japan, Tokyo | Mr Toshihiko Mori<br>Mr Hiroaki Kuwahara<br>Ms Tomoko Suzuki |
| Financial Services Agency, Tokyo | Mr Kazuo Kojima |
| Commission de Surveillance du Secteur Financier, Luxembourg | Mr David Hagen |
| De Nederlandsche Bank, Amsterdam | Mr Erik Smid |
| Eidgenössische Bankenkommission, Bern | Mr Michael Kunz |
| Financial Services Authority, London | Mr Jeremy Quick<br>Ms Katy Martin |
| Federal Deposit Insurance Corporation, Washington, D.C. | Mr Michael Zamorski<br>Mr John Carter |
| Federal Reserve Bank of New York | Mr George Juncker<br>Mr Christopher Calabia<br>Ms Barbara Yelcich |
| Federal Reserve Board, Washington, D.C. | Ms Heidi Richards<br>Mr Jeff Marquardt |
| Office of the Comptroller of the Currency, Washington, D.C. | Mr Hugh Kelly<br>Mr Clifford Wilke |
| Secretariat of the Basel Committee on Banking Supervision, Bank for International Settlements | Mr Jean-Philippe Svoronos |

**Observers:**

| | |
|---|---|
| European Central Bank, Frankfurt am Main | Mr Michael Olsen |
| European Commission, Brussels | Mr Patrick Brady |

# Summary of Initiatives - Electronic Banking Group of the Basel Committee for Banking Supervision

## October 2000

The Electronic Banking Group's (EBG) workplan reflects the consensus view that bank supervisors should collaborate actively to determine and share sound supervisory guidance and principles regarding e-banking activities. Such efforts would provide the foundation for a harmonised approach to the supervision of e-banking within the global bank supervisory community. This would also, in turn, help to reduce impediments to the development of an efficient market for the electronic delivery of banking services.

Given that e-banking is still in its early stages, the EBG does not believe it appropriate to provide prescriptive advice or normative standards that would potentially restrict technological innovation. Accordingly, the group's work plan at this stage is focused on facilitating analyses and dialogue among supervisors that will lead to the development of a prudential supervisory framework for e-banking activities. Reasonable prudential standards should provide for safe and sound conduct of activities without inhibiting innovation and competition that will benefit the banking industry as well as the customers it serves.

In this regard, the EBG will focus on the following action items:

## 1. Building upon work conducted to date and in process, the EBG will develop guiding principles for the prudent risk management of e-banking activities

This guidance will be an extension of existing Basel Committee risk management principles. Such guidance will specifically outline appropriate supervisory expectations regarding the approaches banks should take in *identifying*, *assessing*, *managing* and *controlling* the risks associated with e-banking.

As part of this effort, the EBG will:

- Collaborate with the banking community to identify and promote the implementation of sound risk management practices for technology outsourcing, network and data security and other fast developing areas.

- Continue to study the potential implications of new technology and emerging e-banking business models on the banking industry. These developments, together with the increased entry from information services and technology firms into the financial sector, may lead to further globalisation and commoditisation of banking products and services, which would have significant consequences for the industry and for commerce more generally.

While there is general agreement among banks and bank supervisors that e-banking activities should be approached similarly to traditional banking practices, its unique characteristics warrant further study and follow-up. The dynamics of rapidly changing technology and the propensity of banks to outsource or partner with service providers can redefine or magnify certain traditional risks.

The supervisory processes for e-banking must be sufficiently dynamic to incorporate modifications in light of continuing developments. Key e-banking issues such as technology outsourcing management and due diligence, security management, "web-linking" of financial services and non-financial services, and "aggregation"[1] are good examples of evolving issues that would benefit from co-operative discussion between bank supervisors and banking industry participants.

## 2. The EBG will identify if and where existing Basel Committee guidance needs to be adapted to facilitate the sound supervision of cross-border e-banking activities

As part of this effort, the EBG will consider the practical implications of the various approaches supervisors may take to determine which cross-border banking activities trigger host country authorisation and regulatory requirements.

In light of the prospect that e-banking operations, including web-servers, back-office processing and other technological support, may emanate from a location outside the local (or home) jurisdiction, it is increasingly important that home and host country supervisors' work together to ensure effective and proactive oversight of cross-border activities conducted electronically.

## 3. The EBG will promote co-operative international efforts within the banking industry and between the public and private sectors to identify e-banking risk issues and sound practices to deal with them. Specifically:

- The EBG will work with regional groups of banking supervisors to share information on e-banking developments and promote the development of sound supervisory risk practices and cross-border co-ordination.

- The EBG will continue to gather information from banking institutions and service providers to assess the changing landscape of e-banking and associated risks.

---

[1] An aggregator can be a bank or a non-bank and acts as agent for customers to provide consolidated information on customers' accounts across several financial institutions. Customers provide the aggregator with the necessary security password or personal identification number to access and consolidate account information primarily through screen scraping, a process that involves culling data from the other institutions' web sites, often without their knowledge.

- The EBG intends to co-ordinate with other international financial market supervisory bodies such as IOSCO, CPSS and IAIS to develop consistent supervisory guidance related to e-commerce issues that are common to banking, securities and insurance activities and markets (e.g. risk management, legal, operational, and security issues).

The inherent borderless nature of the rapidly developing e-banking delivery channel requires active co-operation on the part of the financial markets supervisors around the globe to share information on common risks and facilitate the development of sound risk management practices. In addition, EBG members will continue their discussions with banks and Internet service providers in their jurisdictions in order to assess changing conditions, risks and associated risk management developments.

## 4. The EBG will encourage and facilitate the exchange of supervisor e-banking training programmes and materials that are being developed by bank supervisors

In light of the technologically complex and rapidly evolving nature of the e-banking delivery channel, bank supervisors are significantly challenged to keep pace. Therefore, active exchange of examiner training materials and guidance developed by EBG members and other bank supervisors around the world would be extremely valuable.

It would also serve to enhance the ability of the international bank supervisory community to develop and maintain a "level playing field" with respect to supervision of e-banking activities while promoting the safety and soundness of banking systems.

# Electronic Banking Group White Paper
# September 2000

## Cross-Border Electronic Banking Issues for Bank Supervisors

## I. Introduction

This discussion note explores the cross-border supervisory issues and challenges related to electronic banking (e-banking) activities and points out the need for international co-operation among supervisors to address these issues. It concludes by identifying four action items, which the Electronic Banking Group (EBG) believes will promote international co-operation and exchange of information among supervisors regarding e-banking risks and supervisory issues.

## II. Background

The Basel Committee has issued a number of papers addressing sound supervisory practices for "home" and "host" country banking supervisors including guidance on effective cross-border communication and coordination.[2] These papers serve as a basic reference for bank supervisory and other financial market authorities in all countries. They establish several key cross-border principles pertaining to (i) global consolidated supervision; (ii) contact and information exchange with host country supervisory authorities; (iii) and supervision of local operations of foreign banks.

The Basel Committee guidance has provided comfort to host-country supervisors that cross-border branches and subsidiaries *licensed and supervised*[3] within their borders are capably supervised by the parent bank's home-country supervisor. However, many cross-border issues arise from the rapid expansion of e-banking activities that were not contemplated when the Basel Committee's existing guidance was developed.

E-banking is based on technology that by its very nature is designed to expand the "virtual" geographic reach of banks and customers without necessarily requiring a similar "physical"

---

[2] Key Basel Committee guidance includes: "Principles for the Supervision of Banks' Foreign Establishments" (the Concordat), May 1983; "Minimum Standards for the Supervision of International Banking Groups and Their Cross-border Establishments", July 1992; and "The Supervision of Cross-border Banking" October 1996; and the "Core Principles for Effective Banking Supervision", September 1997. This guidance introduced the "home" and "host" supervisor cooperative concepts that are included in many bilateral Memoranda of Understanding (MOU) between national supervisors.

[3] Within Europe, the Second Banking Co-ordination Directive makes it possible for banks licensed in the European Economic Area to provide services in other EEA countries under their home state authorisation (i.e. without being authorised or subject to prudential supervision in the host state).

expansion. Such market expansion can extend beyond national borders, which significantly increases cross-border cooperation challenges for bank supervisors due to:

(i) The potential ease and speed with which banks located anywhere in the world can conduct activities with customers over interconnected electronic networks[4] into countries where a bank is not licensed or supervised.

(ii) The potential ability of a bank or non-bank to use the Internet to cross borders and to seamlessly link banking activities that have typically been subject to supervision[5] with non-banking activities that might be unsupervised by any financial market authority.

(iii) The practical difficulties faced by national authorities wishing to monitor or control local access to e-banking sites originating in other jurisdictions without the cooperation of home country authorities.

Adapting Basel Committee guidance as necessary to address e-banking issues is therefore a principal goal of the EBG.

## III. The Current Situation

Recent surveys of bank supervisors conducted by the EBG indicate that supervisors generally believe that their existing laws, prudential bank regulations, and supervisory policies apply to e-banking activities. However, most respondents note the need for additional, specialised supervisory guidance to address the issues and risks specifically posed by e-banking. The EBG has determined that almost all banks are currently taking a conservative approach to entering new cross-border markets – essentially following the existing procedures that they have used when entering a new foreign market that requires formal regulatory approval.[6] To date, banks have generally refrained from conducting e-banking services in foreign markets where they do not already transact such services through traditional "brick and mortar" distribution channels (e.g. licensed branches, agencies or subsidiaries). Banks that currently conduct cross-border e-banking activities have limited such activities to either their home country currency or the currency of a country in which they are already licensed and have access to the local currency settlement systems either directly or indirectly through a licensed physical presence in the country.

In addition, supervisors have attained heightened sensitivity to choice of law and regulation issues that already exist in a cross-border context. The EBG notes that some countries have

---

4 Including the Internet, wireless and other web enabling technologies (hereafter, referred to as the Internet).

5 In addition to banking supervisors, different financial market authorities may exercise oversight.

6 Cross-border entry in the traditional banking environment generally requires getting a license and an agreement entered into between foreign banking organisation and the local (host) authorities, plus appropriate input from the home supervisor. The Committee's October 1996 paper on "The Supervision of Cross-Border Banking" identifies the roles of the host and home supervisors in the application process.

more restrictive laws or regulations regarding permissible banking activities than others. Over the years, any regulatory conflicts that have arisen have generally been addressed by the home and host supervisor on a cooperative and case-by-case basis as the bank entered the host's jurisdiction. Similarly, the EBG expects that any legal or regulatory issues that may arise as a result of cross-border e-banking will have to be addressed bilaterally between supervisors.

The Internet gives both new "virtual-only" banks and existing geographically-limited banks the opportunity to expand their reach into foreign markets without necessarily incurring the expense and analysis that is typically needed for the establishment of a foreign branch, agency or subsidiary. This situation could result in banks conducting cross-border e-banking without the benefit of a sound understanding of local customs, market conventions, regulations and legal requirements.

In addition, unlicensed and/or unsupervised financial institutions[7] may not exercise the same degree of prudential restraint and control as supervised banks when rolling out cross-border activities. This situation could result in unlicensed institutions providing, via the Internet, banking-like services into jurisdictions where banks are not permitted to provide the same service(s).

A threefold challenge results for banking supervisors:

(i) supervisors need to recognise that the Internet allows for the provision of e-banking services that can span geographic borders and potentially call into question existing jurisdictional authorisation requirements and the regulatory processes;

(ii) supervisors need to recognise the implications of taking a restrictive approach toward currently regulated banks without an even-handed treatment of foreign organisations that may conduct identical or nearly identical activities via the Internet in the local jurisdiction;

(iii) supervisors should ensure that banks appropriately manage the legal uncertainty during the period while the legal infrastructure for cross-border e-banking remains under construction.

## IV. Cross-Border E-Banking Supervisory Issues and Concerns

Several cross-border issues take on added significance for bank supervisors as a result of e-banking developments. While these issues are not necessarily new, complexity is added due to the inherent borderless nature of e-banking and the rapidly evolving underlying technologies.

[7] Or banks subject to less stringent supervisory oversight regimes.

**Authorisation and Regulatory Issues**

Although banks are already providing services cross-border in the physical world (through mail for instance), Internet related technologies significantly increase the potential for jurisdictional ambiguities with respect to the supervisory responsibilities of different national authorities. Such situations could lead to insufficient supervision of cross-border e-banking activities.

Additionally, non-banks may offer with greater facility bank-like services without any type of supervisory approval or oversight due to definitional ambiguities that may exist with regard to what constitutes a bank (or banking services).

Furthermore, banks may inadvertently engage in cross-border activities without knowledge of local limitations. Such situations may expose banks to heightened legal risk associated with non-compliance with different national laws and regulations, including those pertaining to authorisation, consumer protection, record-keeping and reporting requirements, and anti-money laundering.

**Prudential Supervision**

While existing solvency requirements and prudential supervision rules apply equally to e-banking and traditional banking activities, alternative electronic delivery channels raise prudential issues that must be viewed in a new light by supervisors. These include the oversight of outsourcing and partnership arrangements, and the oversight of security and data integrity controls and safeguards, especially when the supporting operations are located in another jurisdiction.

Similar to the situation regarding e-banking authorisation and regulatory issues, additional complexities and ambiguities exist with respect to cross-border home and host supervisory relationships. The existing Basel Committee guidance provides a firm foundation for supervising cross-border banking activities but the EBG recognises that it needs to be reviewed to assure that it is sufficiently robust for the e-banking world.

## V. A Framework for Addressing Cross-Border E-Banking Issues

A framework to deal with e-banking issues among supervisors is essential to effective cross-border supervision, although the specifics may differ between jurisdictions depending upon a variety of local factors. Supervisors will have different perspectives in developing such a framework depending on whether they are a home country supervisor, a host country supervisor, or as is frequently seen, both. Two cross-border scenarios reflect the differences in perspective that need to be examined:

1. In-country institutions providing banking services to customers outside the home country (*the in-out scenario*).

2. Institutions based outside the home country providing banking services to parties within the home country (*the out-in scenario*). This scenario has two subsets: one where the banking institution has a physical presence and licensed operations within

the host country (*physical out-in*); and one where the banking institution has no physical presence and/or license and the banking services are solely provided in a "virtual" manner (*virtual out-in*).[8]

## The In-Out Scenario

When banking organisations provide e-banking services in foreign countries, mutual understanding of the oversight process by both the home and host supervisors is required. Existing Basel Committee guidance clearly establishes the principle that the home country supervisor is responsible for oversight of the banking organisation on a consolidated basis and the host supervisor's oversight is limited to the organisation's activities conducted within its local market.

Home country supervisors should have consolidated views and oversight approaches for e-banking activities. They would normally want e-banking activities outside the local jurisdiction to be subject to the same regulations and controls as within their home country. To the extent that a host country has more restrictive regulations and required controls, the host supervisor would want the banking institution to abide by the host's rules.[9]

Consistent with existing Basel Committee guidance, home supervisors should provide host supervisors with clear information on how they oversee an institution's e-banking activities on a consolidated level. Host country supervisors would generally rely on the home supervisor to effectively carry out its supervisory programme. Where there are concerns about the effectiveness of a home country supervisor's oversight programme, the host would approach the home supervisor on a bilateral basis. As warranted, cooperative supervisory arrangements by both the home and host supervisor would be undertaken.

## The Out-In Scenario

In the "physical out-in" scenario, the foreign institution typically has both (i) some type of licensed physical presence[10] in the host's jurisdiction that is overseen by the host banking supervisor and (ii) access to the local payments system. In this scenario, the host supervisor will apply its normal supervisory oversight processes to the local institution with a focus on activities within its local market. To the extent that e-banking regulatory issues are

---

8 In addition to the clear cross-border cases, supervisors should not lose sight that policies designed for only their own market (the *in-in scenario*) may have cross-border implications requiring international cooperation because of the borderless nature of the Internet. Specifically, the definition of what constitutes "banking services" will affect what institutions are "banks" and subject to licensing and supervision.

9 It is probably unrealistic for home country supervisors to be expected to know the laws and regulations of every possible jurisdiction and monitor compliance outside its own jurisdiction. However, home country supervisors should make certain that banks providing e-banking services under their supervision have reasonable expertise as well as policies and procedures in place to avoid violations of law or imprudent activities in foreign jurisdictions.

10 The presence might be in the form of a subsidiary institution such as a locally chartered bank, a branch or agency licensed by the host supervisor, or another type of regulated financial entity.

identified,[11] they would be addressed locally with the licensed entity and communicated to the home country supervisor as warranted. Where necessary, cooperative supervisory action involving both the host and home supervisors would be undertaken.

For the "virtual out-in" scenario, the foreign bank is providing e-banking services to customers in a country where it does not have a locally licensed entity or direct access to the payments system. In this scenario, the "potential" host supervisor will want to consider a number of issues pertaining to the nature and scope of the virtual bank's activities and determine whether they trigger a need for a license and local regulatory oversight.[12]

The objectives of both the host and home supervisors should be to avoid or minimise legal risks stemming from jurisdictional ambiguities, and to ensure that e-banking activities are adequately supervised with clearly defined supervisory responsibilities. If the virtual bank's activities originate in a jurisdiction lacking a competent and cooperative bank supervisor, the host country supervisor will need to consider what actions may be appropriate to protect local residents and their banking system.

## VI. The Opportunities for Cooperative Supervision on Cross-Border E-Banking Issues

E-banking developments outside a supervisor's home market may move at a pace very different than in the local market - either faster or slower. Nonetheless, the borderless nature of the Internet means external developments can - and in many cases will - affect the local market. Also, while, to date, e-banking transactional activities have been accepted by bank customers on a fairly modest scale and have arguably posed limited risks, this is likely to change.

Understanding and addressing the implications of the rapid pace of development of e-banking and the associated risks will require supervisory agility, resources and, in the cross-border context, cooperation between home and host supervisors. Cooperation among supervisors at the international level is also important with respect to the development of supervisory expectations and guidance for e-banking activities. Such cooperation will strengthen supervision in all jurisdictions as well as promote a level playing field globally.[13] Indeed, cross-border cooperation on the extension of existing supervisory programmes and sound surveillance practices and the development of supervisory guidance on the management of

---

[11] In addition to prudential issues, home-host supervisor communication may also be needed for matters such as choice of law between the different jurisdictions.

[12] Currently, bank supervisors approach this issue in different ways based on the way they would handle traditional "physical out-in" activities.

[13] It is unlikely that guidance will be identical in all markets because markets, like institutions, differ. However, the more similar the guidance is, the easier it will be for supervisors to deal with cross border issues.

e-banking risks may avoid the need for the promulgation of entirely new laws and regulations pertaining to e-banking.[14]

In developing such supervisory tools and guidance, supervisors should recognise that there are different levels of risk appetites and different ways of offsetting risks. Bank supervisory regimes in most countries recognise that "one size does not fit all" for the supervisor's expectations regarding its financial institutions. Expectations may vary depending upon the size, complexity and risk profile of the institution, the business(es) in which it engages, as well as the effectiveness of internal risk management processes.[15] Any supervisory guidance needs to recognise the various trade-offs that management will face. If guidance is too rigid and prescriptive, necessary management flexibility may be impeded.

Furthermore, bank supervisors should work in collaboration with private sector banking industry groups in identifying sound risk management guidance and industry standards that can facilitate the development of e-banking within prudent risk parameters without unduly constraining its innovation.

## VII. Next Steps for Addressing Cross-Border E-Banking Issues

The rapid growth of e-banking poses new cross-border supervisory issues and challenges for bank supervisors, particularly with respect to the allocation of home and host supervisor oversight responsibilities and international coordination. Accordingly, the EBG will focus on the following during Phase II (June-December 2000) of its Workplan:

1. *Reviewing and identifying if and where existing Basel Committee guidance needs to be modified to more specifically address cross-border e-banking issues.*

2. *Working cooperatively with regional groups of banking supervisors to share information on international e-banking developments and promote the development of sound supervisory practices and cross-border coordination.*

3. *Cooperating with other international fora that are establishing general rules and guidance for cross-border electronic commerce that may affect e-banking.*

4. *Promoting cooperative international efforts within the banking industry and between the public and private sectors to identify e-banking risk issues and sound practices to deal with them.*

---

[14] These are areas where the EBG will consider offering guidance on sound market practices beginning in Phase II of its workplan. See the accompanying EBG note on "E-Banking Risk Management Issues for Bank Supervisors".

[15] The recent experience with Year 2000 (Y2K) provides a clear example where supervisory expectations differed, especially in the areas of Y2K remediation and testing. In many countries, large financial organisations that are part of the financial infrastructure serving many others were expected to complete these phases at an earlier date than others in order to allow sufficient time for others to test with them.

# Electronic Banking Group White Paper
# October 2000

## Electronic Banking Risk Management Issues for Bank Supervisors

## I. Introduction

This discussion note assesses the current status of developments in electronic banking (e-banking) and explores how it differs from conventional banking. The note extends the discussion contained in the Basel Committee's March 1998 paper entitled "Risk Management For Electronic Banking And Electronic Money Activities". It identifies emerging trends and risk management issues related to rapid developments in the area of e-banking that raise challenges for both banks and bank supervisors. Four action items for the Electronic Banking Group (EBG) to extend the risk management framework to deal with these risk issues are identified.

## II. Background

Banking organisations have been delivering services to consumers and businesses remotely for years. Electronic funds transfer, including small payments and corporate cash management systems, as well as publicly accessible machines for currency withdrawal and retail account management are global fixtures. However, delivering financial services over public networks such as the Internet[16] is bringing about a fundamental shift in the financial services industry. The changes created, and some of the technical characteristics of Internet technology raise new concerns for both bankers and supervisors. Recent EBG surveys of supervisors and bankers in the G10 countries cite a number of emerging trends and issues that could impact bank risk profiles:

(i) A significant increase in competition in the electronic financial services industry as both banking and non-banking firms rapidly introduce new financial products and services.

(ii) Rapid technological improvements in telecommunications and computer hardware and software enabling greater speed in transactions processing.

(iii) Bank management and staff often lack expertise in technology and e-banking risk issues.

[16] The Internet is meant to include all web enabling technologies, that is, for the time being, the Internet, wireless and other networks (hereafter, the Internet).

(iv) Greater reliance on outsourcing to third party service providers, and a proliferation of new alliances and joint ventures with non-financial firms.

(v) Greater demand for global infrastructures for technology that are scalable, flexible and interoperable, both within and across enterprises and that can ensure the security, integrity and availability of information and services.

(vi) Increased potential for fraud, due to the absence of standard business practices for customer verification and authentication on open networks like the Internet.

(vii) Legal and regulatory ambiguity and uncertainty with respect to the application and jurisdiction of current laws and regulations to evolving e-banking activities.

(viii) The collection, storage and frequent sharing of significant quantities of customer data can lead to customer privacy issues that potentially create prudential risks for banks (e.g. legal and reputational).

(ix) Questions regarding the effectiveness and efficiency of online disclosures. Lengthy or complicated online disclosures may cause customers to simply "click through" or even quit a web site; moreover, extensive disclosure reduces the speed at which web sites and pages can be downloaded.

Banks and bank supervisors generally agree that the supervisory principles that apply to traditional banking are applicable to e-banking. However, the combination of rapid changes in technology and the degree of bank dependence on technology vendors and service providers modify and sometimes magnify traditional risks. Recent EBG surveys of supervisors and banks in Asia, Europe and North America indicate that there is a need for additional supervisory guidance in selected areas to enhance the overall risk management framework for e-banking activities.

Although e-banking activities raise cross-border issues that may require coordinated international efforts they are discussed only briefly in this paper. Cross-border issues are addressed comprehensively in a separate EBG white paper.

## III. The Current Situation

Banking organisations are focusing increasingly on their e-banking activities and are globally expanding Internet banking activities, exploring the use of wireless networks and venturing into some new areas of electronic commerce.

Banks offer e-banking services to defend or expand market share or as a cost saving strategy to reduce paperwork and personnel. The Internet also provides banks with substantial opportunity to extend their customer reach beyond existing boundaries. However, the nature of the open network and the evolution of electronic commerce exposes banks to significant competition from both banking and non-banking firms. In addition, electronic delivery channels operate in an uncertain legal and regulatory environment that differs by jurisdiction. All these factors present new challenges for financial institutions in managing security, integrity and availability of services provided while remaining sufficiently profitable.

In industry surveys, most banking organisations cited other banks and financial services companies as their primary competitors. Some of the larger banking organisations have also cited Internet portals and discount brokerage firms as significant competitors. These non-bank entities have begun to offer checking, electronic bill presentment and payment and other financial services under their own brand name through their web sites.[17]

Despite the emergence of a small number of "Internet only" banks, established banks (as opposed to new entrants not previously involved in banking) are offering e-banking largely as an extension of traditional "brick and mortar" business activities. While Internet-only organisations may benefit from lower initial cost structures, greater flexibility, and lower requirements for facilities, initial enthusiasm for this strategy is beginning to give way to a modified view of Internet-accessed financial services coupled with selected physical presence, a "clicks and mortar" approach. Banking organisations are generally integrating the Internet channel into their overall delivery strategy.[18] They recognise the value in their brand name and the potential to leverage their existing customer relationships by cross selling of products and services.

Initially, most banking organisations focused their attention on developing *retail Business-to-Consumer (b2c)* e-banking services. However, recently, banks have begun to develop new products and services to support *Business-to-Business (b2b)* e-commerce. For example, some banking organisations have formed joint ventures to develop certification authority systems that ensure secure corporate communications.[19] Others are working to develop electronic bill presentment systems that can link with existing or improved electronic bill payment systems. In each instance, the banks are seeking to leverage their existing corporate relationships, set standards in these areas, carve out a meaningful role for themselves in b2b electronic commerce, and extend their reputation as a "trusted third party" in commercial transactions.

Some of the larger banking organisations have also formed strategic alliances with technology companies to develop full service b2b exchanges and marketplaces. The banks, in effect, are filling a significant void for these companies through their provision of foreign exchange, cash management and payments services.[20]

Other banking organisations have begun to build on their experiences of Internet-enabling their own internal purchasing operations and are now offering procurement services to customers as a natural extension of their cash management services. In some countries, banking institutions have looked to expand into new areas of e-commerce and serve small and

---

[17] While some of the larger banks have entered into partnership arrangements with these firms, branding may be an issue of contention between the two parties.

[18] A few banking institutions have, however, created Internet-only brands that are effectively operated as separate divisions within the organisation.

[19] Certification authority systems use digital signatures to authenticate participants within an established network. The certification authority issues credentials, called digital certificates, after verifying the identity and public/private key pair of the system participant. Each participant uses their encryption capability to digitally sign all communications, including financial transactions that flow through the network.

[20] In turn, some of the technology companies have agreed to develop their software to facilitate procurement services for the banks' corporate customer base.

medium-sized businesses by providing access to web site design services, web-hosting services and sometimes acting as an Internet Service Provider (ISP).

Although these activities can provide new sources of income, they clearly introduce new risks to banking organisations that the supervisor must contend with.

The banking industry recognises the need for adequate transparency to promote confidence and acceptance of electronic commerce, and to minimise misunderstandings that can lead to legal action on the part of customers. Industry representatives have expressed some disagreement, however, on the optimal nature and extent of online disclosure to customers in e-banking. These different views arise from concerns about, for example, the effectiveness and practicality of on-line disclosure, level playing field concerns and technological concerns.

New technologies facilitate the collection, storage and processing of significant quantities of customer data. Both existing banks and new entrants have high profit expectations from such activities. Customer data are perceived as a core strategic asset for both bank and non-bank industry participants. Some institutions, including new market entrants, aware of the value of such data in banking, are allocating significant resources to "data mining"[21] to increase their ability to capture and consolidate information from multiple systems or across product lines. Some non-banks are even considering the acquisition of an established bank for the sole purpose of accessing its customer database.

It should be recognised that the enhanced ability to collect and "mine" information on customers may in some cases help banks to understand their customers' needs better and to create or market new products and services that fit those needs and that reflect the underlying risks associated with the customer. However, increased collection, sharing and mining of data also raises potential legal and reputational risks for the banking industry.

The development of new technologies has also led to the emergence of "aggregation" and "screen scraping".[22] Aggregation and screen scraping, although largely centred today in the United States, are expected by many in the industry to become commonplace in a few years as both banks and non-banks introduce new e-commerce business models. These developments raise major strategic and competitive issues for the financial services industry, together with security, legal and reputational risks for financial institutions because they presently have no control over who is screen scraping customer information from their databases but they may be held liable if information is misused.

These developments in e-banking to date suggest that:

---

[21] Data mining refers to the practice of using algorithms to find patterns in customer transaction data to market specific products and services to customers.

[22] An aggregator, who can be a bank or a non-bank, acts as agent for customers to provide consolidated information on customers' accounts across several financial institutions. Customers provide the aggregator with the necessary security password or personal identification number to access and consolidate account information primarily through screen scraping, a process that involves culling data from the other institutions' web sites, often without their knowledge. Many industry participants believe that aggregation technology will become the basis for expanded financial services, including more extensive account sweeps, auctions and intelligent agents.

(i) The desire to benefit from the advantages of e-commerce in financial services has become widespread. The financial services industry is increasingly focused on providing technology-based financial services solutions directly to customers in order to help build and retain customer bases.

(ii) Speed-to-market has become a critical factor for success in e-banking. To reduce time to market, banking institutions are allying with non-banking firms to provide total financial services solutions.

(iii) The current trends in the formation of strategic alliances and technology outsourcing will grow.

These developments present challenges for both banks and bank supervisors. Bank management needs to re-evaluate the robustness of traditional risk management practices in light of the new risks posed by e-banking activities. Also, bank supervisors need to take a balanced approach to the introduction of new regulation and supervisory policy on e-banking, so as to ensure safe and sound operations of banks while at the same time not stifling innovation and the competitiveness of the banks relative to non-banks.

## IV. Implications for Banks' Risk Profiles and Management Practices

E-banking using the Internet as an added delivery channel may shift bank risk profiles to some degree and create new risk control challenges for banks. Accordingly, bank supervisors need to consider the implications of a bank's use of the e-banking delivery channel on its strategic risk, operational risk, reputational risk, legal risk, credit risk, liquidity risk, market risk and foreign exchange risk.

### 1. Strategic and Business Risk

Strategic risk is one of the most significant risks that e-banking activities present for banking organisations. Strategic risk differs from other risk categories in that it is more general and broad in nature. Strategic decisions to be taken by a bank's Board of Directors and executive management will have implications for all other risk categories.

Given growing customer acceptance and demand for e-banking, as well as the potential efficiencies afforded, most banks will need to develop a strategy to use the Internet delivery channel to provide informational content and/or transactional service to customers. The rapid changes in technology, the pace of competition with other banks and non-bank competitors and the nature of that strategy could expose banks to substantial risk if the planning and implementation of the strategy is flawed or otherwise not well thought through.

Some of the strategic risks involved with e-banking are directly linked with timing issues. There can be significant strategic risk associated with a management decision to be a technology pioneer, particularly if the institution becomes burdened with systems made redundant by rapid technological changes. Likewise, an overly cautious technology follower may find itself unable to adequately position itself in a saturated market or a market that is consolidating rapidly.

Prior to the Internet, banking institutions used proprietary networks within their consolidated enterprise and connected in limited ways to other banks. These proprietary networks helped provide a strategic defence against new entrants and provided individual franchise protection. However, the Internet as an open network with open access allows both banks and non-banks freedom to create and leverage existing business without the need for expanded physical presence. Consequently, competition within the financial services industry has been significantly increased and is likely to increase further.

Most bankers believe that the e-banking delivery channel will enable them to reduce operational expenses. However, many bank customers wish to maintain a traditional banking relationship, which makes it difficult for banks to abandon the existing physical infrastructure. This means that banks will - at least for the foreseeable future - need to run multiple delivery channels for sometime and e-banking will be a net additional expense. Thus, operational expense savings may occur over the long run only.

The challenge the banking industry faces in maintaining market share is complicated by the entry of new firms that are providing individual financial services via the Internet to existing bank customers. The emergence of aggregation and screen scraping technologies poses both strategic opportunities and threats to banks. Depending on the evolving relationship between the aggregator, the banks affected and the consumer, banks may get further disintermediated as aggregators potentially disrupt the traditional relationship between the customer and the bank and "limit" the direct access that banks will have on-line to retail customers. In addition, aggressive aggregation by both banks and non-banks may lead to greater commoditisation of banking products and services, thereby reducing bank profit margins and adding new security and legal risks.

In essence, bank management needs to carefully consider how its Internet strategy will help maintain the competitiveness and profitability of the institution[23] yet not lead to unwarranted increases in its risk profile. Supervisors should expect banking institutions to carefully assess the pros and cons associated with their strategic options.

## 2. Operational Risk

Because of the reliance on technology for all facets of e-banking, operational risk is one of the more significant risks. To limit operational risk, banking organisations may want to consider implementing an integrated enterprise-wide architecture and technology infrastructure that can facilitate interoperability, ensure the security, integrity and availability of data and support the management of relationships with third-party service providers. Further, as technology is also dramatically changing business models and operating processes, banks need to ensure that they have appropriate control procedures (including change control) and audit processes.

[23] This would include provisions for avoiding or mitigating the risk of disintermediation.

### *(a) Technology Infrastructure*

E-banking has brought the issue of technological systems and applications integration to the forefront. Many large banks are now faced with the task of integrating systems for e-banking activities with their existing legacy systems and with the systems of multiple service providers and partners. These banks are exposed to significant operational risks from errors in transaction processing if the systems for e-banking are not properly integrated.

Accordingly, many large banks are making significant investments in technology infrastructure in order to create improved internal controls and enhanced risk management oversight processes. The banks are also hoping to improve flexibility, scalability and interoperability of their systems and operations both within their enterprises and across outside service providers.

While these general developments by large banks are positive, in general the banking industry has much further to go towards improving its systems and risk management infrastructure to effectively support e-banking. Small to medium-sized banking organisations are particularly challenged because of budget restrictions for acquiring hardware and software, as well as attracting and keeping technical staff. Many of these banks rely significantly on third party service providers to manage the necessary technological infrastructure to support the bank's e-banking operations. In this situation, the bank still retains ultimate responsibility for ensuring that these operations are well controlled and managed, and the bank supervisor will wish to assess the ongoing ability of bank management to do so adequately.

### *(b) Security*

The majority of bankers surveyed by EBG members identified security risk as a primary concern relating to e-banking. External threats such as "hacking"[24], "sniffing"[25], "spoofing"[26] and "denial of service"[27] attacks expose banks to new security risks. Open electronic delivery channels create new security issues for banks with respect to confidentiality and integrity of information, non-repudiation of transactions, authentication of users and access control.

Based on recent EBG surveys and discussions with industry practitioners, most banks appear to be sensitive to external security threats. Among the issues identified for immediate attention is the development of more robust tools to verify the identity and authenticity of larger value transaction requests.[28] In addition, the banking industry needs to continue to work

---

[24] Hacking refers to the practice of breaking into a computer without authorisation, for malicious reasons, just to prove it can be done, or for other personal reasons.

[25] Sniffing involves the use of a software program that is illicitly inserted somewhere on a network to capture ("sniff") user passwords as they pass through the system.

[26] Spoofing refers to an attempt to gain access to a system by posing as an authorised user.

[27] A denial of service attack represents an attempt to overwhelm a server with requests so that it cannot respond to legitimate traffic.

[28] Identification is concerned with positively establishing the identity of the person or organisation conducting the transaction. Passwords are a common approach although evolving approaches such as biometrics may become

towards international best practices for encryption requirements, including the legality of electronic signature and records. Moreover, since many banks' internal networks rely on security technology similar to that used to manage their external systems, it is important that bankers also be sensitive to managing the security risk arising from their internal networks. If not managed properly, internal security exposures can also compromise the integrity and confidentiality of bank records and customer data.[29]

Poor security may create reputational or legal risks for banks, as they may be deemed to have provided inappropriate protection for customers' personal data, with consequential legal and/or reputational damage.

At the international level, bank supervisors should encourage the development of a comprehensive approach to managing risk associated with both internal and external security exposures. Given the continuing evolution of industry standards, security risk management may be an area where bank supervisors can work collaboratively with the industry to promote the development of sound practices.

### *(c) Data Integrity*

Data integrity is an important component of system security. Banking organisations must improve interoperability within and across enterprises to effectively manage relationships with customers, other banks and external service providers. Until industry standards are identified for electronic data management, banking organisations will continue to be challenged to establish effective control processes to ensure the accuracy and integrity of data being transmitted and received. The processes should include, at a minimum, sound policies and practices related to project management, system development life cycle, change control and quality assurance. Bank supervisors should also encourage banks to review the integrity of the data used by their risk management systems.

Given the lower cost and ubiquitous nature of the Internet, organisations are increasingly using TCP/IP[30] as a standard communications protocol to achieve this. While there are significant benefits of communicating via TCP/IP, organisations must ensure that data transmitted between bank legacy systems and systems of other parties are translated and integrated accurately. Moreover, while the introduction of middleware[31] and languages such

---

increasingly prevalent. Authorisation is concerned with establishing the authority that an individual has to conduct a particular transaction.

29 Attacks on internal systems including those by employees are more frequent than external attacks in many organisations.

30 TCP/IP is a standardised communications protocol for transmitting data in packets via the Internet. TCP (Transfer Control Protocol) deals with the construction of the data packets, while IP (Internet Protocol) routes them from computer to computer.

31 Middleware is transaction-processing software that facilitates client/server communications over a network (e.g. TCP/IP) allowing client applications to access and update information from unlike platforms, databases and mainframes.

as XML[32] are helping to facilitate this effort, the development of industry standards to support these new technologies is still in its very early stages.

### *(d) System Availability*

In addition to ensuring a secure internal network for their e-banking activities, effective capacity planning is critical to ensuring the ongoing availability of e-banking products and services. Transaction volumes may become increasingly volatile due to price sensitivities and greater automation. Also, competitive pressures and increased reliance on having services available 24 hours a day and 7 days a week (24x7) have raised customer expectations considerably and in turn reduced the tolerance for error. To compete effectively and avoid potentially significant reputation risk that could arise from systems outages, banks offering e-banking services must deliver the right mix of products and services securely, accurately and consistently. These factors underscore the importance of effective business continuity, recovery and incident response plans. Moreover, trends in outsourcing make it necessary for bankers to ensure that similar plans are in place at their external service providers and are periodically tested for effectiveness.

Denials of service attacks can also reduce or eliminate a bank's ability to serve its customers while under attack. These attacks have become increasingly common against high profile e-commerce providers. An added challenge is posed by banks' inability to control the availability of the Internet network itself. Thus, a bank needs to consider, as part of its contingency plans, alternative means to deliver service in the event of a major disruption to the Internet network.

### *(e) Internal Controls/Audit*

The ability to detect and correct errors is a critical internal control component of any banking operation. Moreover, banking organisations must have sufficient controls in place to prevent fraud from both internal and external sources and safeguard the bank's information and assets.

Much of the efficiency and cost reduction in e-banking services stem from banks' ability to implement "straight-through processing"[33]. While the benefits of straight-through processing are many, the reality is that e-banking modifies how internal controls, proper segregation of duties and clear audit trails are applied over broad access channels. The challenges presented by these changes are compounded by a critical shortage of skills and expertise in the industry in both the operations and audit areas. Going forward, banks will be increasingly challenged to ensure that highly automated environments provide effective control and that the controls can be independently audited.

---

[32] XML (Extensible Mark-up Language) is a universal, flexible, text-based data format that facilitates structured data interchange on the Web.

[33] Straight-through processing refers to automatic transaction processing without any human intervention in the transaction process flow.

### *(f) Outsourcing*

Perhaps more than any other industry development relating to e-banking, banks' increased reliance on outsourcing is having a significant impact on the risk profiles of all banking organisations – both large and small. Large banks are outsourcing many activities as they are increasingly focusing on their core businesses and partnering with other organisations for solutions outside of their core competencies. Small banks usually must outsource because they often lack the necessary technical expertise and resources to build an e-banking delivery channel on their own. Additionally, a decline in the cost of "turnkey" solutions has made it more affordable for small banks to purchase e-banking applications from vendors. These developments are positive in that they increase efficiency, they allow smaller institutions to compete more effectively and they promote the introduction of "state of the art" applications within the industry. However, they can also substantially add to banks' challenges in managing operational risk.[34]

Preliminary indications from surveys tend to indicate that financial institutions rely upon a relatively small number of third-party providers. This seems to be especially the case for small to medium-sized institutions. In some cases, these third parties happen to be new firms with a relatively short track record. This apparent reliance on a concentrated number of third parties, which the EBG will investigate further, could have systemic implications if a major problem would arise with one of these service providers.

To properly manage the risks associated with outsourcing, banks must conduct appropriate due diligence and monitoring of the ongoing viability of third party service providers. The adequacy of terms under contract and service level agreements must also be carefully reviewed for legal risk. Operations processing and the management of security, integrity and availability risks are also more complicated. Furthermore, many technology providers and partners are newly established and may lack knowledge of the controls required within a banking environment. Minor disruptions on the part of third party service providers can expose banking organisations to potential financial loss and substantial legal and reputation risk. Complexity is also added by multiple vendor/service provider relationships that often support e-banking operations. Although to date such disruptions seem to have been controlled, in the future their potential impact could be quite considerable and raises significant concerns for supervisors and industry participants.

Outsourcing can lead to additional privacy related risk exposures. Banks may not always be aware of the exact collection and usage of customer data by vendors and other third parties, and/or may not be adequately managing such activities. Moreover, the legal rights and responsibilities of service providers and vendors may not always be clear. Banks should be encouraged to address privacy issues in their contractual and ongoing relations with vendors.

Various bank supervisors around the world have developed specific guidance related to technology outsourcing. The EBG plans to conduct a review of such guidance and to explore

[34] It is noteworthy that, as discussed throughout this paper, outsourcing management has implications for successful management of many of the other risks.

ways to coordinate the development of sound practices in this area for both the banking industry and its supervisors.

## 3. Reputational Risk

A bank's reputation can be impacted by any adverse development that precludes the availability of their e-banking delivery channel. Banks have long based their business on a reputation of trust. The ability to provide a trusted network to support e-banking is critical, and a bank's reputation can be damaged by Internet banking services that are poorly executed or otherwise alienate customers and the public.

A bank's reputation can suffer if it fails to deliver secure, accurate and timely e-banking services on a consistent basis. A bank's reputation can also be adversely impacted if it fails to respond to inquiries posted via e-mail, does not provide proper disclosure, or violates customer privacy.

Hypertext links from a bank to third party web sites or outsourced service providers may cause customer confusion about the provider of specific products and services offered, and whether they are insured or uninsured. Customers can also be confused about whether the links from the bank reflect an implied endorsement of the third party's products or services and may well look to the bank for recourse if problems are encountered.

Further, major security breaches in a bank or a non-bank competitor's web site could undermine overall consumer or market confidence in banks' ability to appropriately manage Internet-based transactions.

Any problems that a bank might experience with regard to data and privacy protection could threaten the reputation of that bank as well as the reputation of any other banks perceived to be involved in similar activities.

To protect against adverse situations that may cause damage to their reputation, banking organisations should develop and monitor performance standards for their e-banking activities. Regular review and testing of business continuity, recovery and incident response plans, and communications strategies are also critical to protecting banks' reputations.

## 4. Legal Risk

Legal risk arising from e-banking activities represents another area of increased concern. Currently, supervisors in every jurisdiction are examining how existing legal and regulatory frameworks originally designed to address issues affecting the "physical' world of banking interact with the developing e-banking delivery channel as well as examining potential ambiguities.

A bank that develops relationships via the Internet with customers in other jurisdictions may be unfamiliar with the banking and customer protection laws and regulations specific to those countries and may consequently incur heightened legal risks. Even banks that do not intend to solicit business from consumers in foreign jurisdictions may find that their offerings on-line are considered solicitations in some countries. For example, if a bank makes its web site available in another language, regulators in any country where that language is spoken may

determine that the bank is marketing services to its citizens and may find that the bank is therefore subject to its local laws and regulations.

Unauthorised use or misuse of data collected over the Internet is another potential source of legal risk. Unauthorised individuals can attack and/or try to infiltrate the "data warehouses"[35] maintained about consumers by both banks and third party vendors. For example, hackers or others might break into banks' or vendors' databases or build their own databases and use the consumers' information to perpetrate fraud. Authorised staff may also deliberately misuse data. Surveys of banks and third party vendors conducted by the EBG have showed that such attacks on "data warehouses" have already occurred, although the impact of these attacks has been minimal to date.

The enforceability of certain emerging areas of law is also uncertain. Laws related to the enforceability of electronic contracts and digital signatures are still under development and vary from jurisdiction to jurisdiction. Effective "know your customer" (KYC) practices are also becoming more critical to bankers in their attempts to prevent fraud.

## 5. Other Traditional Banking Risks

The e-banking delivery channel also has implications for other traditional banking risks such as credit risk, liquidity risk, interest rate risk, and market risks. The impact of the introduction of e-banking does not necessarily result in an increase or decrease in the risk profile of the institution, but risks can be shifted, sometimes in complex ways.

### *(a) Credit Risk*

The credit risk of a banking institution can be affected by e-banking activities in a number of ways. The use of the Internet delivery channel may allow banks, especially small institutions, to expand very rapidly, which could lead to heightened asset quality and internal control risks. The use of the Internet also allows banks to expand their geographic reach out of their traditional area, which increases the challenge of understanding local market dynamics and risks, verifying collateral and perfecting security liens with out-of-area borrowers. In addition, the Internet also makes it more difficult to authenticate the identity and creditworthiness of a potential customer, which are essential elements to sound credit decisions.[36] Further, there has been a tendency for some Internet-only banks to pay higher rates on deposits opened over the Internet, which could lead to a higher level of sub-prime credits at these institutions in order to support these higher deposit rates. These factors underscore the importance of sound credit underwriting policies, credit monitoring and administration practices regardless of which product delivery channel is used.

---

[35] A data warehouse is a large database of customer transactions, updated regularly, which is used as a source of information for data mining.

[36] On the other hand, the use of the Internet delivery channel can potentially lead to a reduction in a bank's concentration of credit to a single local industry, market or geographic region.

### *(b) Liquidity Risk*

The speed with which information and misinformation moves over the Internet can have implications for the liquidity risk profile of a bank. Adverse information about a bank, whether it is true or not, can be easily disseminated over the Internet through bulletin boards and news groups. This could cause depositors to withdraw their funds in mass at any time of the day, any day of the week. Also, Internet banking can increase deposit volatility to the extent that new customers brought in through this channel maintain accounts solely on the basis of interest rate or terms. Accordingly, increased monitoring of liquidity and changes in deposits and loans may be warranted depending on the volume of activity created through e-banking.

### *(c) Market Risk*

The impact of recent growth in securities issuance and trading over the Internet on banks' market risk profiles is complex. From a market standpoint, the increased volume of securities, which are traded over the Internet, can on the one hand lead to increased volatility, but, on the other hand, it can lead to increased liquidity. From an individual bank's standpoint, banks may be exposed to increased market risk if they create or expand deposit brokering, loan sales, or securitisation programme as a result of Internet banking activities. As with liquidity risk, the effects of increased e-banking activities on market volatility need to be monitored by banks and supervisors.

### *(d) Foreign Exchange Risk*

A bank may be exposed to foreign exchange risk if it accepts deposits from foreign customers or create accounts denominated in currencies other than their local currency. Since the Internet allows banks the opportunity to expand their geographic range, even internationally, some banks may take on greater foreign exchange risk through e-banking activities than they have through their traditional delivery channels. Also, foreign exchange risk can be intensified by political, social or economic developments, which a bank inexperienced in cross-border banking may not appreciate fully. Supervisors should ensure that a bank initiating cross-border e-banking activities through the Internet has the appropriate risk management systems and expertise to manage these risks properly.

## V. Implications for Bank Supervisors

As the preceding discussion indicates, the basic types of risks associated with e-banking are not new. However, the specific ways in which these risks arise, as well as the potential magnitude and speed of impact on banks, may be new for bank management and supervisors alike. In addition, while assessing risk should already be dynamic, the rapid pace of technological innovation supporting e-banking, the increased degree of systems outsourcing and the reliance of some products/services on the use of open networks such as the Internet, intensifies the need for a rigorous and ongoing risk management process.

Bank supervisors should expect their banks to have comprehensive risk management processes in place that include the three basic elements of *assessing* risks, *controlling* risk

exposure, and *monitoring* risks associated with e-banking. This comprehensive risk management framework should be integrated into the bank's overall risk management framework.

It is also essential that this risk management process is supported by appropriate oversight by the board of directors and senior management and is carried out by staff with the necessary knowledge and skills to deal with the technical complexities of new e-banking developments.[37]

Similarly, bank supervisors must recognise their own critical need for supervisory staff with appropriate technology knowledge and skills to ensure that they understand the risks and challenges arising from the development of the e-banking delivery channel. Enhanced technical training of existing supervisory staff, complemented by appropriate recruitment of outside expertise, should be a high priority in order to ensure that the supervisor keeps abreast of increasingly complex technology and market developments.

## VI. Next Steps for Addressing E-Banking Risk Management Issues

The EBG recognises the benefits of ongoing international cooperation in identifying sound risk management practices and industry standards that will facilitate the evolution of e-banking within prudent risk parameters without unduly hampering its useful innovation and experimentation. Accordingly, the EBG will focus on the following action items during Phase II (June-December 2000) of its Workplan:

1. Building on the work conducted by EBG members to date, the EBG will develop supervisory guidance for the prudent risk management of e-banking activities. This guidance will be an extension of existing Basel Committee risk management principles and will specifically outline appropriate supervisory expectations regarding how the banks should *assess, control* and *monitor* the risks associated with e-banking.

2. In collaboration with the banking industry and technology providers, the EBG will identify and promote the implementation of sound industry risk management practices for critical or emerging areas, such as technology outsourcing, security issues, and aggregation activities.

3. The EBG will continue to study the potential implications of new technology and emerging e-banking business models (e.g. aggregation, business to business and business to customer exchanges) on the banking industry. These developments, coupled with the increased entry from information services and technology firms into the financial sector, currently point to further globalisation and commoditisation of banking products and services, which will have potentially significant strategic and competitive consequences for the industry.

---

[37] The Basel Committee's March 1998 paper on "Risk Management for Electronic Banking and Electronic Money Activities" outlines risk management considerations for banks engaging in e-banking.

4. The EBG will promote and facilitate an exchange of supervisor e-banking training programmes and materials that are being developed by bank supervisors.