**Saudi Arabian Monetary Agency**

**e-Banking Rules**

**Banking Technology Department**

 **APRIL 2010**

**Table of Contents**

[1 Introduction: 4](#_Toc257621981)

[1.1 Electronic Banking Definition: 4](#_Toc257621982)

[1.2 E-banking Evolution: 5](#_Toc257621983)

[1.3 E-Banking Rules: 5](#_Toc257621984)

[1.4 Objective of the Rules: 6](#_Toc257621985)

[1.5 Scope of Application: 6](#_Toc257621986)

[1.6 Effective Date: 6](#_Toc257621987)

[2 Supervision of E-Banking: 7](#_Toc257621988)

[2.1 Supervisory Approach: 7](#_Toc257621989)

[2.2 New E-banking Products: 7](#_Toc257621990)

[2.3 Legal and Regulatory Requirements: 7](#_Toc257621991)

[2.4 Enforcement Mechanism: 8](#_Toc257621992)

[2.5 Reporting Requirements: 8](#_Toc257621993)

[3 Customer Protection and Education: 9](#_Toc257621994)

[3.1 Rights and Liabilities of Banks and Customers: 9](#_Toc257621995)

[3.2 Customer Security and Education: 9](#_Toc257621996)

[3.3 Banks’ Obligations: 10](#_Toc257621997)

[4 E-Banking Risks: 12](#_Toc257621998)

[4.1 Types of Services: 12](#_Toc257621999)

[4.2 Risk Profiles 12](#_Toc257622000)

[4.3 Associated Risks: 13](#_Toc257622001)

[4.4 Risk Management Approach: 15](#_Toc257622002)

[4.4.1 Risk Identification 15](#_Toc257622003)

[4.4.2 Risk Analysis and quantification 16](#_Toc257622004)

[4.4.3 Risk treatment 16](#_Toc257622005)

[4.4.4 Risk monitoring and review 16](#_Toc257622006)

[4.4.5 Summary 17](#_Toc257622007)

[5 Risk Management Principles for E-Banking: 18](#_Toc257622008)

[5.1 Principles 1-3: Board and Management Oversight: 18](#_Toc257622009)

[5.2 Principles 4-10: Security Controls: 20](#_Toc257622010)

[5.3 Principles 11-14: Legal and Reputational Risk Management: 23](#_Toc257622011)

[Appendix 1 26](#_Toc257622012)

[Glossary 26](#_Toc257622013)

[Appendix 2 32](#_Toc257622014)

[Security Controls Requirements 32](#_Toc257622015)

[Appendix 3 36](#_Toc257622016)

[Incident Reporting 36](#_Toc257622017)

# Introduction:

## Electronic Banking Definition:

The term “Electronic Banking” or “e-banking” is defined as remote banking services provided by authorized banks, or their representatives through devices operated either under the bank's direct control and management or under the outsourcing agreement. In other words, e-banking is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a branch and includes the systems that enable customers of banks, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet.

A “remote banking service” is defined as a:

* Dedicated banking service for which the Customer has explicitly registered and authorized.
* Service supplied using devices that are not under the control of the Provider;
* Service which demands the authentication of the Customer.

Cross-border e-banking is defined as the provision of transactional on-line banking products or services by a bank in one country to authorized customer in other countries. This definition would include situations where a foreign bank provides e-banking products or services to residents in a foreign country from (i) a location in the bank’s home country, or (ii) an “onshore” physical establishment in another foreign country.

The following terms used to describe the various forms of e-banking are often used interchangeably: personal computer (PC) banking; Internet banking; virtual banking; online banking; home banking and remote electronic-banking.

**Services Exclusions**

Usually, e-banking also involves phone banking and the use of automated teller machines (ATMs) but these are not covered under the above e-banking definition for the purpose of these Rules.

Furthermore, individual communications such as e-mail (digitally signed or otherwise) received by the Provider from a Customer outside the context of a remote banking service, are also not covered under this definition.

Various other related terms are defined in the Glossary at Appendix 1 to these Rules.

## E-banking Evolution:

Technology developments and innovations are having a significant impact on the banking business. Banks face the challenge of adapting, innovating and responding to the opportunities provided by the technological advancements. The growth of e-banking has benefited enormously to banks and their customers. It has allowed banks to expand outreach, reduce transaction costs, improve efficiency, and provide virtual banking services. On the other hand, customers have benefited from efficient banking services at relatively lower costs and having the option to choose from alternate delivery channels. The e-banking has also facilitated swift movement of funds domestically and across borders.

This changing financial landscape has posed new challenges for banks and policymakers/supervisors. Banks now have increased reliance on technology to compete in an increasingly competitive business environment and thus need to effectively manage the IT security and other related risks. Central Banks and supervisory authorities are facing new challenges in banking supervision as well as in designing and implementing monetary policy. The growing scope of e-banking and increasing complexity of banking products and services demands continuous adaptation of regulatory framework and effective supervisory oversight.

## E-Banking Rules:

In order to enable banks to protect customers’ information, reduce fraud incidents, and manage e-banking related risks as also to minimize the number of complaints from e-banking users, SAMA has decided to issue new “E-Banking Rules”. These Rules will replace the “Internet Banking Security Guidelines” issued in 2001.

The new E-Banking Rules are risk-based and set out SAMA’s prudential regulatory approach to the supervision of e-banking services. They provide guidance to banks on risk management in electronic banking and emphasize on:

* Board of Directors and Senior Management accountability;
* Customer protection and education;
* Customer privacy;
* Minimum security standards consistent with best international standard;
* Proper incident management and reporting to SAMA;
* Proper Availability Management
* Capacity building and business continuity planning.

Banks are expected to review and, if required, to modify their existing risk management policies and processes to bring their e-banking activities in line with these Rules.

## Objective of the Rules:

The main objective of the “E-Banking Rules” is to provide guidance to banks on implementation of security controls in their e-banking products and services and effective management of risks associated therewith. The Rules are not aimed at discouraging banks from innovation and creativity in e-banking provided they remain within the regulatory framework and ensure customers’ facilitation.

## Scope of Application:

The “E-Banking Rules” shall be applicable to all forms of e-banking as defined under Section 1.1 of these Rules. However, the e-banking services provided through Automated Teller Machines(ATMs), Points of Sale(POS) and Phone Banking are not covered under these Rules.

All banks licensed by SAMA and authorized to provide e-banking services whether locally or abroad through their branches/subsidiaries, are required to ensure compliance of these Rules.

The provision of cross-border e-banking services would be subject to proper authorization and compliance of home and host jurisdictions’ laws and rules/regulations. Foreign banks not licensed by SAMA to operate in Saudi Arabia are not allowed to engage in cross-border e-banking activities in Saudi market.

## Effective Date:

These Rules shall come into force with immediate effect. All banks are required to take necessary measures to ensure compliance of the Rules.

# Supervision of E-Banking:

## Supervisory Approach:

SAMA’s supervisory approach is to establish and maintain a prudent regulatory framework for the growth of e-banking services in Saudi Arabia. Banks are expected to implement the risk management controls that are commensurate with the risks associated with the types, complexity and volume of transactions carried out and the electronic delivery channels adopted. They should adopt robust risk management processes and IT security measures consistent with their e-banking business strategy and the established risk tolerance level. The risk management controls established for e-banking should be fully integrated into the overall risk management systems. Banks are also expected to introduce elaborate processes to ensure timely resolution of security related issues.

In order to ensure compliance with the best international standards, SAMA has endorsed the principles and recommendations for e-banking outlined by the Basel Committee on Banking Supervision’s paper - “Risk Management Principles for Electronic Banking” (<http://www.bis.org/publ/bcbs98.htm>).

Given the dynamic nature of e-banking and related technology, SAMA recognizes that the issues to be addressed may vary over time and from one bank to another. For this reason, these Rules distinguish between minimum requirements and additional recommended controls.

## New E-banking Products:

Banks shall seek prior no objection from SAMA before launching any new e-banking product or significantly modifying the existing product and/or launching a new product with same name. For this purpose, they will approach the Agency along-with the relevant information including salient features of the product, target market, related systems and controls and a confirmation to the effect that the proposed product comply with all the relevant laws and rules/regulations. The Agency may grant or withhold its no objection or grant it subject to such conditions as it may deem fit.

## Legal and Regulatory Requirements:

In addition to these Rules, banks are required to ensure compliance of other related laws and regulatory requirements. For outsourcing of e-banking related operations and activities, banks should follow “ SAMA’s Rules on Outsourcing” as amended from time to time.

Other related laws and guidelines include, inter-alia, the following:

* Banking Control Law;
* Anti-Money laundering Law;
* Rules Governing Anti-Money Laundering & Combating Terrorist Financing;
* Combating Embezzlement & Financial Fraud & Control Guidelines;
* Compliance Manuel for Banks;
* SARIE operating rules and regulations;
* Other relevant SAMA Rules, Guidelines and Circulars.

SAMA continuously updates its regulatory framework in line with international standards and changing market conditions. Banks are expected to keep track of such changes and ensure compliance of the latest regulatory requirements.

## Enforcement Mechanism:

1. Internal Audit:

Banks should define an adequate compliance audit program to ensure that e-banking business is carried out in accordance with these Rules and the bank’s policy and strategy. The scope of such audit should, inter-alia, include evaluation of related internal controls including segregation of duties, dual controls, information security controls and reconciliation.

Banks should also define the process of conducting compliance audit of their e-banking business. The audit process should include Vulnerability assessment and Ethical Hacking on all networks, systems and applications associated with e-banking. Furthermore they should define the level of involvement of the audit department in case of an e-banking related fraud incident. The audit process should also include a review of the introduction/setting up of New User A/c, subsequent changes to the User A/c, e-banking contracts, and customer education about authentication.

1. Supervisory Review:

SAMA will review the adequacy of IT security measures and risk management processes adopted by banks for conducting e-banking business. This will be done as a part of the Supervisory Review Process. Furthermore, the compliance of these Rules will be verified during on-site examination of a bank.

## Reporting Requirements:

Banks shall monitor and report to SAMA every security incident classified by the business owner as medium or high risk and the steps taken by them for its resolution on a timely basis, it should also mention the steps the bank has taken to avoid similar incident in the future. The details of incidents to be reported and the timeline of their reporting are given in Appendix 3 (Incident Reporting) to these Rules. All such reports should be submitted through e-mail to the Director, Banking Technology Department of SAMA.

# Customer Protection and Education:

## Rights and Liabilities of Banks and Customers:

Banks are expected to review customer contracts regarding rights and obligations of each contractual partner. Banks have to develop contracts which are:

* Easy to understand; written in a clear and concise language (in Arabic and English) that any customer will understand. It should avoid the ambiguous words or phrases; which may give rise to dual-meaning.
* Based on clear terms and conditions that should:
	+ Ensure around the clock (24x7x365) availability. If there is any schedule maintenance downtime, customers should be informed well in advance.
	+ Articulate the Service Level Agreement (SLA) between the bank and customer with a compensation program in case of failure to deliver e-banking service due to bank's mistakes or systems failure.
	+ Explain and educate customers on how to use strong authentication mechanism (strong passwords for instance).
	+ Use a secure messaging system when communicating with customers.
	+ Clearly articulate the level of customer privacy and at what extent his/her information will be exposed internally within the bank.
	+ Prohibit the bank from exposing customers' information to third parties.
	+ Explain the process for handling customer complaints or objections with reasonable time frame to file a complaint or an objection.
	+ Clearly explain the process of e-banking account activation and deactivation to protect customers when their accounts have been inactive for a long period of time.
	+ Clearly explain the danger of customers using public networks/computers or international networks when they are abroad.
	+ Explain in plain Arabic and English, the level of security the bank has undertaken to protect their assets and thus customers' information.
	+ Provide customers with a process on how they can automatically block their own accounts (e.g. 5 successive attempts are made to gain access with an incorrect password). The bank is prohibited from blocking customers' accounts or service without assigning valid reasons and without prior notice to customer.
* Based on clear statements on the liabilities of bank and customer in case of failure to meet their respective obligations.

## Customer Security and Education:

Banks should develop and execute appropriate awareness/education programs about their e-banking products and services to ensure that a customer is properly identified and authenticated before access to online banking functions is permitted. For this purpose, they can use multiple channels such as websites, messages printed on customer statements, promotional leaflets, or direct staff communication through call-centres and in branches.

Security advice should, at a minimum cover the following issues:

* Awareness and avoidance techniques of possible online fraud attempts, including:
	+ Phishing attacks and the use of the Bank's identity on a fake website.
	+ Customers should be alerted not to access the bank's online resources from other websites, portals or emails.
	+ Customers should be advised not trust any online resource simply because it holds the Bank's Identity.
* Confidential use of Username and Password
	+ Customers should not share their passwords.
	+ Under no circumstances customer need to disclose their PIN or password to any bank staff.
	+ Necessity to periodically change the password.
* Careful password selection to avoid password guessing
	+ Advise customers on how to select or create robust passwords or personal identification numbers that cannot easily be guessed or predicted.
* Appropriate storage of passwords.
* Adopt two factor authentication based on SAMA circular no:40690 issued on 6th August 2009.
* Non-disclosure of personal information to unauthorised persons or to doubtful websites/emails.
* Reminders not to access e-banking services through public or shared computers.
* Advise customers on how to identify the bank’s dealing official in case of “somebody” claims to be it.
* Advise to use latest version of personal firewall and anti-virus.

## Banks’ Obligations:

Banks are directly responsible for the safety and soundness of the services and systems they provide to their customers. Their obligations in this regard include the following:

* Potential liability and damages to customers due to inaccurate or incomplete information about products, services, and pricing presented on the website.
* Potential access and threat to confidential Bank or customer information if the website is not properly isolated from the Bank’s internal network.

* Potential liability for spreading viruses and other malicious code to computers communicating with the institution’s website.
* Authentication processes necessary to initially verify the identity of new customers. Banks have to ensure that the identity of the customer is verified and proven correct before they start any kind of relationship. This process is especially important with new customers located outside the area of bank’s physically location.
* Authentication processes to identify existing customers who access e-banking services, for any usage of the e-banking offerings, at different levels: log in, transaction, orders, confirmations, and log off.
* Losses from fraud if the institution fails to verify the identity of individuals or businesses applying for new accounts or on-line credit. Banks have to know their customers and define ways for the explicit identification.
* Protection of the Bank's customers from online fraud attempt (Phishing and Pharming Attacks) using a reliable professional process or service that enables prevention, detection and response to these attacks.
* Protection of the Bank's identity online from illegitimate use or misrepresentation using a reliable professional process or service to prevent, detect and respond to such abuse.
* Taking action against any illegitimate representation of the Bank or any illegitimate use of the Bank's identity online regardless of the purpose.
* Education of the Bank's clients not to surrender their personal information to any entity that claims to be the Bank.
* Education of the Bank's clients not to trust any website simply because it holds the logo of the Bank.
* Possible violations of laws or regulations pertaining to consumer privacy, anti-money laundering, anti-terrorism, or the content, timing, or delivery of required consumer disclosures.
* Failure to process third-party payments as directed or within specified time frames, lack of availability of on-line services, or unauthorized access to confidential customer information during transmission or storage, and
* Assurance of a customer-friendly service by establishing appropriate processes to answer their claims within three (3) business days.

However, Banks cannot be made liable for customers’ failure in protecting their personal information such as giving away confidential details (i.e. PIN, or password).

# E-Banking Risks:

## Types of Services:

1. **Information-only websites**

Information-only websites are defined as those allowing access to general-purpose marketing and other publicly available information, or the transmission of non-sensitive electronic mail. Banks should ensure that consumers are alerted to the potential risks associated with unencrypted electronic mail sent over such a medium.

1. **Information transfer websites**

Information transfer websites are interactive in that they provide the ability to transmit sensitive messages, documents, or files among a group of users, for example, a Bank’s website that allows a customer to submit online loan or deposit account applications. Since communication and system security risks include data privacy and confidentiality, data integrity, authentication, non-repudiation, and access system design, some risk mitigation methods are therefore necessary.

1. **Fully transactional websites**

Fully transactional websites represent the highest degree of functionality and also involve high levels of potential risks. These systems provide the capabilities for information-only applications, electronic information transfer systems, as well as online, transactional banking services. These capabilities are provided by interactive connectivity between customer devices and the bank's internal systems. However, many systems will involve a combination of these capabilities.

##  Risk Profiles

These Rules classify e-banking services and products according to the level of security required to perform the service, and according to the contractual requirement associated with that service, as under:

1. General Information (e.g. brochures; advertising, etc.)

This profile presents the lowest risk. It is concerned with the provision of data which is not related to any account or individual. Descriptions, exchange rates, interest rates and contact details for the bank require only that the information is not corrupted.

1. Customer Related Information (e.g. statements)

This profile deals with information related to customers or their accounts. Examples include statements and account balances. Within this profile, no transactions which transmit funds or change data are allowed, so the risk is limited to exposure of existing confidential data.

1. Customer Pre-Mandated Instructions (sign once)

This profile relates to the lowest risk financial transactions: those which have been previously authorised using other (non e-banking) channels. Typically, these transactions only allow the customer to vary the amount to be paid, or the date to perform the transaction.

1. Customer Originated Transactions (individual transactions)

This profile relates to the provision of transactions, where the customer can specify the beneficiary, the amount and the date without prior arrangement or subsequent additional authorisation. It is this profile which is the main focus of this document. Banks may decide to sub-divide this profile depending on the transaction amount, or other parameters of the transaction.

1. Customer Recruitment and Registration (sign on)

This is the highest risk profile. Customer recruitment and registration form the basis upon which all future security rests and so must be treated with the greatest care. This profile includes the ability to alter the customer's name, address or authentication data.

## Associated Risks:

Electronic banking creates new risk management challenges for Banks. Typically, all risks associated with traditional banking and products may be impacted with the introduction of e-banking services. However, there are Seven major categories of risk specifically associated with e-banking. The associated risks are strategic, operational/transaction, technology, business, online fraud, reputation and legal.

1. **Strategic Risk** is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. Ideally, an e-banking service should be consistent with the bank’s overall financial strategy. The planning and decision making process should focus on how specific business needs are met or enhanced by e-banking, rather than focusing on the product as an independent business objective. Strategic vision should determine how e-banking is designed, implemented, and monitored.
2. **Operational/Transaction Risk** arises from fraud, processing errors, system disruptions, and the inability to deliver products or services, maintain a competitive position, and manage information. In the provision of e-banking services, banks may rely on outsourced software companies. They require the proper management of information systems and the right capacity to service their customers. Contingency and business resumption planning is necessary for Banks to ensure that they can deliver products and services in the event of adverse circumstances.
3. **Technology Risks** are risks related to any adverse outcome, damage, loss, disruption, violation, irregularity or failure arising from the use of or reliance on computer hardware, software, electronic devices, online networks, and telecommunications systems. These risks can also be associated with systems failures, processing errors, software defects, operating mistakes, hardware breakdowns, capacity inadequacies, network vulnerabilities, control weaknesses, security shortcomings, malicious attacks, hacking incidents, fraudulent actions and inadequate recovery capabilities. Banks have to control every single component and process related of their e-banking systems. Each component represents a control point to consider. This is also valid for potential components; they have to be assessed in appropriate ways before being implemented in the e-banking environment. The level of transaction risk is affected by the structure of the institution’s processing environment, including the types of services offered and the complexity of the processes and supporting technology.
4. **Business Risk**: In some circumstances, due to the more savvy nature of the e-banking consumer who is more focused on costs and rates, traditional banking risks, such as credit risks, interest rate risk, liquidity risk, and foreign exchange risk are elevated.
5. **Online Fraud Risk**: With online trade, it is essential to take online fraud risks into consideration. Scams such as Phishing and Pharming attacks, Identity theft and faulty corporate representation pose a serious risk to the bank itself and to the banks customers. The bank must take the appropriate measures to prevent the occurrence of losses due to online fraud and take the appropriate action to protect the bank's clients globally once an incident occurs.
6. **Reputation Risk** arises from negative public opinion. A bank’s reputation can be damaged by e-banking services that are poorly executed or otherwise alienate customers and the public. It is important that customers understand what they can reasonably expect from a product or service and what special risks and benefits they incur when using them. Customer education along with formal incident response and management procedures can help lessen a bank’s reputational risk. Banks are required to communicate in a transparent and clear way and to meet their obligations in this regard. The Board of Directors or the management has to agree on the communication strategy and content.
7. **Legal Risk** is the risk to earnings or capital arising from violations of, or non- conformance with, laws, rules, regulations, or ethic standards. The need to ensure consistency between paper and electronic advertisements, disclosures, and notices increases the potential for legal violations. Regular monitoring of the bank’s websites will help ensure compliance with applicable laws, rules, and regulations.

The Board of Directors and senior management are responsible for managing the above risks and must ensure that the risk management of e-banking is an integral part of the bank’s overall risk management. As a result, the applicable risk management policies and processes, and the relevant internal controls and audits as required in the institution’s risk management system should be enforced and carried out as appropriate for the e-banking services.

In addition, the Board or its designated committee should ensure that the bank’s risk management controls and systems are modified and enhanced as necessary to cope with the risk management issues associated with e-banking.

## Risk Management Approach:

The open and complex nature of IT infrastructures especially used by the Internet (e.g. the risks associated with using it, the risks related to partners in the delivery chain as telecommunication providers, system vendors and suppliers, product and service providers), are the key reasons why banks have to establish a sound risk management framework.

All relevant business, operational and support areas having technology risk management responsibilities at line or functional levels should be covered.

The board and all levels of management are responsible and accountable for managing and controlling technology risks (actual and future ones).

Since senior management has to oversee all risk management functions, they should establish risk management processes.

This responsibility calls for banks to perform risk identification and assessment by going through the spectrum of relevant risks and analyse the impact of the various risks on their business operations and systems.

Risks that are deemed material to the organisation should be thoroughly evaluated and prioritised to enable a strategy to be developed for addressing and mitigating these risks.

###  Risk Identification

Typical risks associated with e-banking services are in fact not new, however, the different ways in which some of the risks arise and their magnitude and possible consequences take on new dimensions. On the other hand, security risks such as those manifested in denial of service attacks have no precedents or equivalents in the traditional way of conducting business, but could cause severe disruption to the operations of a bank with consequential losses for all parties affected.

Risk identification should cover the determination of all kinds of threats, vulnerabilities and exposures present in the configuration of e-banking and all kind of components such as internal and external networks, hardware, software, applications, and operations and human elements, especially the impact of human misbehaviour. Further, it should cover direct e-banking environment as well as all support systems and functions and the respective interdependencies to obtain an adequate risk profile.

Risks related to the launch of new e-banking products or services or major modification to the existing product and services should be assessed and resolved during the conceptualisation and developmental stages. Risk control procedures and security measures should be put in place prior to or during the implementation phase.

The management has to identify, classify and assess risks that are relevant to the Bank's operations, as under:

1. Establish a risk classification model.
2. Define a plan containing policies, practices and procedures that address and control these risks.
3. Implement the plan.
4. Monitor risks and the effectiveness of the plan on an ongoing basis.
5. Define processes for regularly testing and updating the plan to take account of changes in technology, legal development and business environment (including external and internal threats to information security).

### Risk Analysis and quantification

This phase is about the analysis, understanding and quantification of the potential impact and consequences of identified risks on the overall business and operations: prioritise the risks, perform cost-benefit analysis and take risk mitigation decisions.

### Risk treatment

Management must also assess how much damages and losses the bank can withstand in the event that a given risk-related event materialises. Banks have to absorb any related losses that may eventuate without jeopardising their financial soundness and stability.

The costs of risk control and mitigation should be balanced against the benefits to be derived. Management has to take the decision regarding the resources to be allocated in control function and the expected reduction of incident, e.g. the reduction of the probability of occurrence.

The effectiveness of internal controls including segregation of duties, dual controls, and reconciliation is important. Information security controls, in particular, become more significant requiring additional processes, tools, expertise, and testing. Institutions should determine the appropriate level of security controls based on their assessment of the service they provide, on the sensitivity of the information to the customer and to the institution and on the institution’s established risk tolerance level.

Banks should not offer an e-banking product or service if the necessary controls and security measures cannot be adequately implemented.

### Risk monitoring and review

Facing the constant changes occurring in the e-banking environment, management should institute a risk monitoring and compliance framework on an ongoing basis to ascertain the performance and effectiveness of the risk management process.

Any time risk parameters change, the risk process needs to be updated and enhanced accordingly. Routine testing and regular auditing of the adequacy and effectiveness of the risk management process and the attendant controls and security measures taken should be conducted.

It is highly recommended that bank shall perform a third party comprehensive Risk Assessment exercise every year.

### Summary

The impact of e-banking on risk management is complex and dynamic. Management should constantly reassess and update its risk control and mitigation approaches to take into account varying circumstances and changes to its risk profile in the internet environment.

# Risk Management Principles for E-Banking:

SAMA endorses the “Risk Management Principles for Electronic Banking” (http://www.bis.org/publ/bcbs98.htm) issued by the Basel Committee on Banking Supervision(BCBS). Banks should take into account the requirements of these Principles in establishing their policies and processes for e-banking..

The Principles outlined below are mainly based on the BCBS’ Principles, contain some purposeful redundancies and set the minimum requirements to be complied by the banks.

## Principles 1-3: Board and Management Oversight:

***Principle 1:***

*The Board of Directors and senior management should establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.*

Senior Management and the Board of Directors of each bank should set clear direction and provide necessary management support to security initiatives for e-banking.

This encompasses:

* Promotion of safe and sound security within the organization through appropriate commitment and allocation of adequate resources.
* Approval of all policies and processes related to managing risks of e-banking activities.
* Review and monitor information about security incidents.
* Establishment of a separate unit within the Risk Management Department dedicated to risk management of e-banking which should report directly to Chief risk Officer/Head of Risk Management.
* Development of an internal and external communication plan to improve the e-banking security culture.
* Have the ability to prevent and respond to online fraud and corporate identity abuse.
* Promotion of a comprehensive customer awareness and education program.

***Principle 2:***

*The Board of Directors and senior management should review and approve the key aspects of the bank's security control process.*

Senior Management is responsible for matching security controls to the overall needs of the business. Senior Management therefore has to regularly review and approve security policies, processes and new initiatives including the following:

* Information security policy.
* Major initiatives to enhance information security.
* Efficiency of the security control processes.
* Reliability and consistency of e-banking systems in use.
* Customer awareness and education programs.
* Response methodology to online fraud and brand misuse incidents.
* Major changes in technology as well as new services and product launches.
* Evaluating efficiency of the security control processes implemented for e-banking activities.
* Incident management process and communication plan for employees, customers and SAMA.

***Principle 3:***

*The Board of Directors and senior management should establish a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.*

If banks rely on third party providers for e-banking services, management must generally understand the provider’s information security program to effectively evaluate the security systems’ ability to protect the bank and its customer data. Banks are still responsible for the weaknesses of their systems; this applies especially for outsourced solutions.

The following risks are related to outsourcing (non-exhaustive and non-prioritized list) and should be analysed before engaging the bank into such a contract:

* Loss of control
* Higher exit barriers
* Exposure to vendor risks, including:
	+ Financial strength
	+ Loss of commitment to outsourcing
	+ Slow implementation
	+ Promised features not available
	+ Lack of responsiveness
	+ Poor daily quality
* Become hostage to “extra usage” charge
* Difficulties in quantifying economies
* Costs of conversion.
* Attention required by senior management.
* Supply restrictions.
* Possibility of being tied to defective technology.
* Concerns with long-term flexibility and meeting the changing business requirements on a timely basis.
* Concerns regarding the continuing cost-benefit of outsourcing.
* Damage to corporate image.
* Potential liability claims.
* Lack of clarity of ownership, reporting and control.
* Concerns regarding industry acceptance.
* Inadequate technical service quality.

## Principles 4-10: Security Controls:

***Principle 4****:*

*Banks should take appropriate measures to authenticate the identity and authorisation of customers with whom it conducts business over the Internet.*

For the purpose of safe and sound banking, it is essential to confirm that a particular transaction or access request is legitimate. Banks therefore have to use reliable methods for verifying the identity and authorisation of new and existing customers. In this regard, some methods have been introduced to banks in a separate circular ( No 40690 Date. 6-08-09).

Banks in their communication to customers should not give the impression that e-banking services and products are completely secure. They should make customers aware of the threats to online banking.

***Principle 5:***

*Banks should use transaction authentication methods that promote non- repudiation and establish accountability for e-banking transactions.*

Technical non-repudiation involves creating proof of origin or delivery of electronic information to protect both:

* The sender against false denial by the recipient that the data has been received.
* The recipient against false denial by the sender that the data has been sent.

Banks should apply methods which involve secure trusted registration and a timestamp.

***Principle 6:***

*Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.*

Segregation of duties is critical for safe and sound e-banking. Banks are thus required to set up internal control measures designed to reduce fraud risk in operational processes and systems and to ensure that transactions and equipment are properly authorised, recorded and safeguarded:

* Develop and document procedures to define duties which should be segregated.
* Monitor procedures to ensure that segregation rules are followed.
* Three categories of duties should be defined:
	+ Authorisation: Responsibility to assign a duty to a person / persons.
	+ Custody: Responsibility to authorise a person to store data.
	+ Record keeping and reconciliation: responsibility to authorise a person to maintain records and reconcile them.

***Principle 7:***

*Banks should ensure that proper authorisation controls and access privileges are in place for e-banking systems, databases and applications.*

Non-privileged access to e-banking system (databases/applications) can lead to high impact incidents. Thus banks must have appropriate access controls in place, including the following:

* Only persons who need access to a particular system should be given access privileges.
* Auditors should be permitted to perform only those tasks that both general users and auditors are authorized to perform, not those permitted for operators.
* Banks should have a well documented and approved procedure which describes the certification process. A re-certification process should be conducted on a regular basis, with the line management verifying each individual’s need to retain privileges.
* In case principals are unable to perform their duties, and their authority needs to be transferred to other people, an emergency procedure should produce sufficient logs and notification to Senior Management about the substitution. Management must be able to control or revoke the substitution.
* All activities of privileged persons should be reported on audit records.
* All records, logs and notifications should be reviewed periodically, and any misuse should be fully investigated.

***Principle 8****:*

*Banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.*

Data integrity of transactions, records and information is essential for safe and sound e-banking. Failure to maintain data integrity can expose banks to financial losses as well as legal and reputation risk. With respect to the high risk exposure, banks should plan and introduce appropriate organisational, procedural and technical methods which ensure that the integrity of financial and transactional data is assured and maintained:

* Mechanisms should be in place to detect discrepancies and to ensure that corrective actions are planned and will be taken.
* Financial data recording should:
	+ reflect the actual values involved
	+ be posted on a timely basis
	+ be stored securely
	+ be readily retrievable for inquiry or reporting
	+ be safeguarded against improper alteration

***Principle 9****:*

*Banks should ensure that clear audit trails exist for all e-banking transactions.*

Delivery of financial services over the Internet can increase the difficulty to apply and enforce internal controls. Banks should thus ensure that the internal control system is adapted to e-banking services and products and that clear audit trails are maintained.

In addition, the internal controls should be independently auditable by external agencies.

Audit trails should:

* Provide sufficient evidence to demonstrate the transaction flow, from beginning to end, and any accompanying control / procedural performance.
* Be adequate to satisfy the rules of the courts under which they could be used.

Technical measures such as encryption, digital signatures and message authentication codes should be used to protect the integrity of audit trail records. In addition, a tamper proof electronic copy should be maintained for audit trails.

***Principle 10:***

*Banks should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in databases.*

The advent of e-banking presents additional security challenges for banks because it increases the exposure that information transmitted over the public network or stored in databases may be accessible by unauthorised or inappropriate parties, or used in ways the customer providing the information did not intend. Additionally, increased use of service providers may expose essential data of banks to other parties.

Thus key data of a bank must remain private to the bank. Any misuse exposes banks to high impact reputation and legal risk.

The protection of confidentiality should be commensurate with the impact of the risk of unauthorised exposure:

* Confidentiality should be maintained by use of access controls and encryption.
* Cryptographic techniques should be based on recognized algorithms that have not been disputed in their strength or use.
* Access should only be permitted based on the “need to know” principle.

## Principles 11-14: Legal and Reputational Risk Management:

***Principle 11****:*

*Banks should ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status prior to entering into e-banking transactions.*

SAMA requires all banks to protect customers against fraudulent websites:

* Entity authentication procedures should be implemented to avoid the capture of customer's authentication data and financial information.
* Controls should be implemented to protect essential records and information from loss, destruction and falsification.

Banks should raise customer awareness on the risk of fraudulent websites. It is key in educating the customer. In this regard, the usage of recognisable SSL certificates and a URL with recognisable link to the bank (i.e. in published bank literature) is encouraged.

***Principle 12:***

*Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services.*

Banks should ensure that the provision of services in any particular jurisdiction takes into account any additional safeguards necessary to protect the customer's (and the bank's) privacy in that jurisdiction. Data privacy laws may not be consistent across the world, but the laws under which the bank and their customers operate still demand equivalent protection. The remote legislation might also impose controls which are not required by the local legislation.

Banks desirous of engaging in cross-border e-banking activities should understand the challenges and risks associated with such business and take adequate measures to effectively manage these risks.

***Principle 13:***

*Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.*

Banks are expected to develop plans for maintaining or restoring business operations in appropriate time scales following interruption to, or failure of, critical business processes.

All contingency plans should be part of a consistent business continuity framework.

Each plan should:

* Identify priorities for testing and maintenance.
* Clearly specify the conditions for its activation, as well as the individuals responsible for executing each component of the plan.
* Identify and agree responsibilities and emergency procedures.
* Include the regular tests and updates of the plan.

In addition, Banks should build up an appropriate disaster recovery plan, including at a minimum:

* An offsite backup infrastructure.
* A documented and tested recovery procedure.
* Regular tests to ensure that recovery is within the maximum allowable outage (defined by the bank).

SAMA requires banks to develop capacity plans (scalability) to ensure the accommodation of future growth in e-banking. Banks have to set up appropriate capacity planning in order to support the evolution of transaction with acceptable response times. The planning will be focused on the level of capacity to be provided at each stage of the production or service delivery. Capacity planning addresses the the issue of unpredictable workload/volume of traffic due to the future evolution of the e-business to produce a competitive and cost-effective architecture and system.

The capacity building plan of a bank should cover the following at a long, medium and short term horizon:

* the expected storage capacity of the system and the amount of data retrieved, created and stored within a given cycle.
* the number of on line processes and the estimated likely contention.
* the required performance and response required from both the system and the network i.e. the end to end performance.
* the level of resilience required and the planned cycle of usage - peaks, troughs and average.
* the impact of security measures e.g. encryption and decryption of all data.
* the need for continuous (24x7x365) operations and the acceptability of [downing the system](http://www.yourwindow.to/information-security/gl_down.htm) for maintenance and other remedial work.

Redundancy to be built in the system planning infrastructure.

Threshold mark for the system resource utilization should be defined while doing the capacity planning.

***Principle 14:***

*Banks should develop appropriate incident response plans to manage, contain and minimise problems arising from unexpected events, including internal and external attacks, which may hamper the provision of e-banking systems and services.*

SAMA believes that appropriate management of incidents is key for safe and sound e-banking in Saudi Arabia.

Banks should encourage Incident reporting from all parties especially from customers. They should introduce a special section on their websites for such purpose.

 Banks are strongly advised to develop incident response plans, including at a minimum:

* Mechanism to detect incidents as soon as they occur, assess their materiality, and control the risk associated with any disruption in service (special focus on reputation).
* Have the ability to protect their online customers from online fraud.
* Have the ability to protect their online identity from illegitimate use.
* Have the ability to prevent, detect and respond to online fraud attempts and brand misuse.
* Documented and tested procedures that enable a fast reaction to detected incidents and limit the probability of recurrence.
* A communication plan to ensure that all relevant external parties, including a bank’s customers, counterparties and the media, are informed in a timely and appropriate manner on material e-banking disruptions and business resumption developments without creating any panic in the minds of public.
* An employee training plan to ensure that staff is sufficiently trained in analyzing incident detection/response systems and interpreting the significance of the related output.

In addition, incident management responsibilities and procedures should be established to ensure a quick, effective and orderly response to security incidents. Furthermore, the exchange of information and sharing of experience between banks and other parties is encouraged. The banks are also encouraged to participate in the incident response initiative managed by the Banking Committee for Information Security (BCIS).

# Appendix 1

# Glossary

**Senior management**

Senior management is any personal occupying general manager position or above.

**Authentication**

A feature of Internet Security software that seeks to verify the identity of a person or process.

**Bandwidth**

The amount of data that can be transmitted in a fixed amount of time. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz). And for digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second.

**Bits per second (bps)**

The units at which the transmission speed of data is measured as the bits are transmitted over a communications medium.

**Broadband**

A type of data transmission in which a single medium (usually a wire) can carry several channels at once. Cable TV, for example, uses broadband transmission.

**Browser**

A program used to access and display documents from the Web and other Internet resources. Popular browsers include Netscape and Internet Explorer.

**Cookie**

A packet of information that is sent by a HTTP server to a client's browser and then sent back by that browser each time the client accesses the server. Typically they are used to identify, track a registered user of a website without requiring them to sign on each time they access that site.

**Domain name**

That part of the Internet name that specifies your computer location in the world, written as a series of names separated by full stops.

**Encryption**

Encoding of data travelling across the Internet to prevent it from being read by unauthorized recipients.

**FB’s**

Foreign Banks

**Firewall**

A security measure on the Internet, protecting information, preventing access, or ensuring that users cannot do any harm to the underlying computer systems. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall which examines each message and blocks those that do not meet the specified security criteria.

**FTP**

File Transfer Protocol, one of the protocols on the Internet, which allows for very efficient transfer of entire data files between computers.

**HTTP**

(Hyper Text Transport Protocol)

A set of rules that provide the means of communicating, moving hypertext files on the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. Requires an HTTP client program on one end, and an HTTP server program on the other end. HTTP is the most popular protocol used in the World. You can normally see the http at the beginning of each web address.

**HTML**

HyperText Markup Language is a convention for creating documents on the World Wide Web. HTML files usually have the extension .HTML or .htm.

**Hyperlink**

An element in an electronic document that links to another place in the same document or to an entirely different document. Typically, you click on the hyperlink to follow the link.

**Internet**

The worldwide organization of computer networks stretching across the world, linking computers of many different types and protocols. The Internet provides file transfer, remote login, electronic mail, news, and other services. No one organization has control of the Internet.

**Internet service provider**

An organization that offers a server computer and the software needed to access the Internet for a fee.

**Intranet**

A private Internet-like network internal to a particular organization, usually not accessible to the unauthorized public.

**Java**

A programming language used to create mini programs (known as applets), which are automatically downloaded when you come across a Java-enhanced WEB site. Sun Microsystems developed it, and it is now used in several online games and to animate some images.

**Junk or chain e-mail**

Unsolicited commercial email, also called "spam".

Chain e-mail messages have the same content as chain letters but are sent through e-mail networks rather than the Mail. A chain message, or chain e-mail, is defined as any message sent to one or more people that ask the recipient to forward it to multiple others and contains some promise of reward for forwarding it or threat of punishment for not doing so.

**Modem**

A piece of equipment that connects a computer to a data transmission line - typically a telephone line. Usually people use modems that transfer data at speeds ranging from 1200 bits per second (bps) to 19.2 kbps.

Wireless devices have limitations that increase the security risks of wireless-based transactions and that may adversely affect customer acceptance rates.

**PC banking**

A form of online banking that enables customers to execute bank transactions from a PC via a modem. In most PC banking ventures, the bank offers the customer a proprietary financial software program that allows the customer to perform financial transactions from his or her home computer. The customer then dials into the bank with his or her modem, downloads data, and runs the programs that are resident on the customer’s computer. Currently, many banks offer PC banking systems that allow customers to obtain account balances and credit card statements, pay bills, and transfer funds between accounts.

**Phishing**

The act of sending an [e-mail](http://www.webopedia.com/TERM/p/e_mail.html) to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for [identity theft](http://www.webopedia.com/TERM/p/phishing.html##). The [e-mail](http://www.webopedia.com/TERM/p/phishing.html##) directs the user to visit a [Web site](http://www.webopedia.com/TERM/p/Web_site.html) where they are asked to update personal information, such as [passwords](http://www.webopedia.com/TERM/p/phishing.html##) and credit card, social security, and bank account numbers, that the legitimate organization already has. The [Web site](http://www.webopedia.com/TERM/p/phishing.html##), however, is bogus and set up only to steal the user’s information.

Phishing, also referred to as brand spoofing or carding, is a variation of “phishing,” the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted to bite.

**Phone Banking**

To access a Bank's network(s) using cellular phones, pagers, and personal digital assistants (or any similar devices) through telecommunication companies’ wireless networks. Wireless banking services supplement e-banking (Internet banking) products and services.

**PIN**

Personal Identification Number. Some Banks may use PIN as a synonym for password.

**Protocol**

A set of rules for the exchange of data between a terminal and a computer or between two computers.

**Proxy**

A device used to access the Internet around a "fire wall" put up to ensure security in a large system/network.

**PKI**

Short for public key infrastructure*,* a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of the parties involved in an Internet transaction. PKIs are currently evolving and there is neither a single PKI nor even a single agreed-upon standard for setting up a PKI.

**Search engine**

A program that allows you to do keyword searches for information on the Internet.

**Security certificate**

An attachment to an electronic message that is used by the SSL protocol to establish a secure connection and to verify the identification of the individual/organization.

Senior management:

Senior management is any personal occupying general manager position or above.

**SET, Secure Electronic Transaction**

Secure electronic transaction (SET) is a standard protocol for securing credit card transactions over insecure networks, specifically, the Internet. SET was developed by VISA and MasterCard (involving other companies such as GTE, IBM, Microsoft and Netscape) starting in 1996.

SET makes use of cryptographic techniques such as digital certificates and public key cryptography to allow parties to identify themselves to each other and exchange information securely.

SET was heavily publicised in the late 1990’s as the credit card approved standard, but failed to win market share. Reasons for this include the need to install client software (an e-Wallet), its cost and complexity for merchants to offer support and the comparatively low cost and simplicity of the existing, adequate SSL based alternative.

**Sniffing, packet sniffing**

Packet sniffing is a form of wiretap applied to computer networks instead of phone networks. It came into vogue with Ethernet, which is known as a "shared medium" network. This means that traffic on a segment passes by all hosts attached to that segment. Ethernet cards have a filter that prevents the host machine from seeing traffic addressed to other stations. Sniffing programs turn off the filter, and thus see everyone’s traffic.

**Spoofing, Spoof Websites**

Also known as brand spoofing or carding, is a variation of “phishing,” a form of cyber crime. The idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted to bite.

**SSL**

Short for **S**ecure **S**ockets **L**ayer*,* a protocol developed by Netscape Communications to enable encrypted, authenticated communications across the Internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. In an SSL connection, each side of the connection must have a Security Certificate, which each side's software sends to the other. Each side then encrypts what it sends using information from both its own and the other side's Certificate, ensuring that only the intended recipient can de-crypt it, and that the other side can be sure the data came from the place it claims to have come from, and that the message has not been tampered with.

**Token**

In [computing](http://en.wikipedia.org/wiki/Computing), a [token](http://en.wikipedia.org/wiki/Token_ring) is a virtual object that is passed between computers or other devices on a network and similarly authorizes them to communicate. Only the device with the token may communicate, to avoid clashing with other devices.

In [computer security](http://en.wikipedia.org/wiki/Computer_security), token technology uses devices with embedded microchips containing information about the owner to determine security clearance. Tokens can be items such as key rings, buttons, jewelry and smart cards.

In the [Windows NT](http://en.wikipedia.org/wiki/Windows_NT) family of operating systems, a [token](http://en.wikipedia.org/wiki/Token_%28Windows_NT_architecture%29) is a system object representing the subject of access control operations.

**URL**

Universal Resource Locator is an address that completely defines a resource of the World Wide Web. A URL has four elements:

1. The service - HTTP or FTP or a few others
2. The host - the computer that handles the resource
3. The port number (often not necessary because it defaults according to the service requested).
4. The path and filename of the resource.

URL format is: service://hostport/path.

**WWW**

The World Wide Web, also called the Web or W3, is a system of Internet servers that support specially formatted documents. The documents are formatted in a language called HTML that supports links to other documents, as well as graphics, audio, and video files. This means you can jump from one document to another simply by clicking on hot spots. Not all Internet servers are part of the World Wide Web.

# Appendix 2

# Security Controls Requirements

Banks have to define the following independent security controls under the responsibility of senior management: In order to illustrate the topics that would be comprehensively addressed a non-exhaustive list of controls is included below which follows the new ISO27001 standard:

**Security Policy**

Those controls which provide management support and direction and included the following:

* Information security policy document;
* Review of the information security policy.

**Security Organization**

Those control relating to the management of information security within the organization. The controls cover the following areas:

* Management commitment to information security;
* Information security co-ordination;
* Allocation of information security responsibilities;
* Confidentiality agreements;
* Independent review of information security.

**Asset Management**

Those controls in place to account for, control and maintain all assets in order that all parts of the system are given a level of protection commensurate with their importance/value to the organization. The controls cover the following areas:

* Inventory of assets;
* Ownership of assets;
* Asset Classification;
* Information labeling and handling.

**Human Resources Security**

Those controls that cover all security aspects involved with the management of personnel covering the following areas:

* Roles and responsibilities;
* Screening;
* Terms and conditions of employment;
* Management responsibilities;
* Information security awareness, education and training;
* Disciplinary process;
* Termination responsibilities;
* Return of assets;
* Removal of access rights.

**Physical and Environmental Security**

Those controls that cover the direct physical protection of assets and the environments in which they are situated throughout their lifespan, including their maintenance and eventual disposal and cover the following areas:

* Physical security perimeters;
* Physical entry controls;
* Securing offices, rooms and facilities;
* Protecting against environmental threats;
* Working in secure areas;
* Public access, delivery and loading areas;
* Equipment security.

**Communications and Operations Management**

Covers the controls required to operate the system in a secure manner commensurate with its Protective Marking. It includes the following areas:

* Documented operating procedures;
* Change management;
* Segregation of duties;
* Separation of development, test and operational facilities;
* System planning and acceptance;
* Protection against malicious and mobile code;
* Network security management;
* Media handling;
* Exchange of information;
* Electronic commerce services;
* Monitoring.

**Access Control**

This covers the controls necessary to restrict and monitor access to all aspects of the system and include the following areas:

* Access control policy;
* User access management;
* User responsibilities;
* Network access control;
* Operating system access control;
* Application and information access control;
* Mobile computing and teleworking;

**Information Systems Acquisition, Development and Maintenance**

Those controls required ensuring that security implications are considered during all updates or changes to the system and cover the following areas:

* Security requirements of systems;
* Correct processing in applications;
* Cryptographic controls;
* Security of system files;
* Security in development and support processes;
* Technical vulnerability management.

**Information Security Incident Management**

Those controls required in order to ensure that information security incidents and weaknesses are reported in a controlled manner which enables any corrective actions to be carried out without delay and covers the following areas:

* Reporting information security events;
* Reporting security weaknesses;
* Collection of evidence;
* Learning from information security events.

**Brand Protection and Fraud Prevention**

These controls are required to protect the Bank's online customers from possible frauds (Including Phishing and Pharming Attacks) and misuse of the Bank's identity in illegitimate activities. These controls must provide the following:

* The ability to detect possible fraudulent sites on the internet.
* The ability to detect representation of the Bank or the use of its identity illegitimately on the internet.
* The ability to take action to protect the Bank's customers globally from becoming victims of a given fraudulent site.

**Business Continuity Management**

Even though this area will be covered by another project, we propose to address part of the controls also in this security Assessment. Those controls required to ensure that disruption to the system is kept to an agreed, acceptable level covering:

* Business continuity and risk assessment;
* Developing and implementing continuity plans;
* Testing, maintaining and re-assessing business continuity plans.

**Compliance**

Those controls that are required in order that the system complies with applicable legislation whilst maintaining the security of its assets and covering the following areas:

* Legal and regulatory compliance;
* Protection of organizational records;
* Prevention of misuse of information processing facilities;
* Auditing.

# Appendix 3

# Incident Reporting

The following list of incidents must be reported through e-mail to the Director, Banking Technology Department (BTD), SAMA.

| Incident | Time of report |
| --- | --- |
| Any cases of fraudulent attacks for compromising customer identity and credentials. (phishing, pharming, Trojans, malware etc) | Banks are requested to notify SAMA **immediately** after detection of incident.In addition, a detailed technical report has to be submitted within one week. |
| Unauthorised intrusion into Bank’s IT systems for compromising customer data relevant to E-banking. | Banks are requested to notify SAMA within **one day** after detection of incident. |
| Any corruption of data relevant to E-banking systems that is not recoverable.  | Banks are requested to notify SAMA **immediately** after detection of incident.Detailed technical report within one week. |
| Intentional or accidental disruption to e-banking services  | Banks are requested to notify SAMA within **one day** after detection of incident. |
| Any cases of internal fraud relevant to E-banking | Banks are requested to notify SAMA **immediately**. In addition banks should submit a detailed report on the nature and impact of fraud within one week. |

Note: The bank should also provide the root cause analysis of the security incident and measures taken by the bank to avoid similar incidents in future.