Financial Privacy Financial privacy involves the protection of consumers from unlawful access to financial accounts by private and public bodies, and the unlawful disclosure, sharing, or commercial use of financial information. Just as in the case of medical privacy, Indian law does cast a duty on bankers to protect the privacy of their customers. This duty of confidentiality is an extra layer of protection when it comes to financial information of individuals in addition to their right to privacy. Both these principles were used by the banks in one of the most important cases in the field of financial privacy, i.e. District Registrar and Collector, Hyderabad v. Canara Bank and others, 23 where a provision of law which allowed the person inspecting the documents to also seize and impound the documents was challenged by the banks. The provision also extended this power of inspection to include not only public officers but also to citizens and banks. It was challenged inter alia, on the ground that it intruded into the privacy and property of individuals. Considering the issue of allowing such inspections at banks which held the private documents of their customers or copies of such private documents, the question before the Court was whether disclosure of the contents of the documents by the banks would amount to a breach of confidentiality and would, therefore, be violative of privacy rights of their customers? Discussing this issue the Court held as follows: "It cannot be denied that there is an element of confidentiality between a Bank and its customers in relation to the latter's banking transactions…… …Once we have accepted in Govind and in latter cases that the right to privacy deals with 'persons and not places', the documents or copies of documents of the customer which are in Bank, must continue to remain confidential vis-a`-vis the person, even if they are no longer at the customer's house and have been voluntarily sent to a Bank. If that be the correct view of the law, we cannot accept the line of Miller in which the Court proceeded on the basis that the right to privacy is referable to the right of 'property' theory. Once that is so, then unless there is some probable or reasonable cause or reasonable basis or material before the Collector for reaching an opinion that the documents in the possession of the Bank tend, to secure any duty or to prove or to lead to the discovery of any fraud or omission in relation to any duty, the search or taking notes or extracts therefore, cannot be valid. The above safeguards must necessarily be read into the provision relating to search and inspection and seizure so as to save it from any unconstitutionality." Secondly, the provision was also struck down because it enabled the Collector to authorize 'any person' whatsoever to inspect, to take notes or extracts from the papers in the public office since this was considered by the Court to be excessive delegation as there were no guidelines regulating this and the it allowed the facts relating to the customer's privacy to reach non-governmental persons and would, on that basis, be an unreasonable encroachment into the customer's rights. Therefore, the Court held this provision to be unconstitutional and struck it down. Although banks are required to maintain confidentiality and thereby protect the privacy of their customers in their ordinary course of business, however sometime the duty to protect the right to privacy of their customers can come in direct conflict with the discharge of their functions. This situation has arisen a number of times when banks have sought to publish the photographs and information of wilful defaulters in newspapers, this practice has sometimes been objected to by the defaulters whose information is sought to be published on the ground that such publication would violate their right to privacy. There is currently a difference of opinion between various courts of law (i.e. High Courts in different States (provinces) have given different and opposing opinions on this issue). Some Courts have held that Banks are allowed to publish photographs of the defaulters even though it may violate the right to privacy of the defaulters since it would serve the interest of the bank and the economy as a whole by ensuring better recovery of bad loans.24 On the other hand it has also been held by other Courts that (government owned) banks have the power to realize their dues only in a manner authorized by law and there is no provision in law which allows the bank to publish the photographs of defaulters in newspapers. It further held that such an action by the banks would violate the right to privacy of the individuals.25 Apart from the general duty of bankers to maintain confidentiality, there are certain legislations which

also touch upon the need to maintain secrecy in financial transactions. The Credit Information Companies (Regulation) Act, 2005 and the Regulations thereunder which provide that specific instances under which credit information of individuals may be released by the credit information companies. Further, as far as financial institutions owned by the government are concerned the Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 198326 as well as the State Bank of India Act, 195527 provide that these institutions are prohibited from divulging any information relating to the affairs of its clients except in accordance with laws of practice and usage. To enforce this all their employees must take an oath of secrecy before carrying out their duties. Other than in the sectors discussed above, there exists some jurisprudence and legislation in relation to privacy in the fields of telecommunications, transparency as well as law enforcement which we shall discuss below under separate headings.

Introduction:

Information and the knowledge based on it have increasingly become recognized as 'information assets', which are vital enablers of business operations. Hence, they require organizations to provide adequate levels of protection. For banks, as purveyors of money in physical form or in bits and bytes, reliable information is even more critical and hence information security is a vital area of concern.

Robust information is at the heart of risk management processes in a bank. Inadequate data quality is likely to induce errors in decision making. Data quality requires building processes, procedures and disciplines for managing information and ensuring its integrity, accuracy, completeness and timeliness. The fundamental attributes supporting data quality should include accuracy, integrity, consistency, completeness, validity, timeliness, accessibility, usability and auditability. The data quality provided by various applications depends on the quality and integrity of the data upon which that information is built. Entities that treat information as a critical organizational asset are in a better position to manage it proactively. Information security not only deals with information in various channels like spoken, written, printed, electronic or any other medium but also information handling in terms of creation, viewing, transportation, storage or destruction .This is in contrast to IT security which is mainly concerned with security of information within the boundaries of the network infrastructure technology domain. From an information security perspective, the nature and type of compromise is not as material as the fact that security has been breached.

To achieve effective information security governance, bank management must establish and maintain a framework to guide the development and maintenance of a comprehensive information security programme.

Basic Principles of Information Security:

For over twenty years, information security has held confidentiality, integrity and availability (known as the CIA triad) to be the core principles. There is continuous debate about extending this classic trio. Other principles such as Authenticity, Non-repudiation and accountability are also now becoming key considerations for practical security installations.

* Confidentiality: Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Breaches of confidentiality take many forms like Hacking, Phishing, Vishing, Email-spoofing, SMS spoofing, and sending malicious code through email or Bot Networks, as discussed earlier.

* Integrity: In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases.

Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when he/she is able to modify his own salary in a payroll database, when an employee uses programmes and deducts small amounts of money from all customer accounts and adds it to his/her own account (also called salami technique), when an unauthorized user vandalizes a web site, and so on. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

* Availability: For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the

communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service (DoS) and distributed denial-of service (DDoS) attacks.

* Authenticity: In computing, e-business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

* Non-repudiation: In law, non-repudiation implies one's intention to fulfill one’s obligations under a contract / transaction. It also implies that a party to a transaction cannot deny having received or having sent an electronic record. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

In addition to the above, there are other security-related concepts and principles when designing a security policy and deploying a security solution. They include identification, authorization, accountability, and auditing.

* Identification: Identification is the process by which a subject professes an identity and accountability is initiated. A subject must provide an identity to a system to start the process of authentication, authorization and accountability. Providing an identity can be typing in a username, swiping a smart card, waving a proximity device, speaking a phrase, or positioning face, hand, or finger for a camera or scanning device. Proving a process ID number also represents the identification process. Without an identity, a system has no way to correlate an authentication factor with the subject.

* Authorization: Once a subject is authenticated, access must be authorized. The process of authorization ensures that the requested activity or access to an object is possible given the rights and privileges assigned to the authenticated identity. In most cases, the system evaluates an access control matrix that compares the subject, the object, and the intended activity. If the specific action is allowed, the subject is authorized. Else, the subject is not authorized.

* Accountability and auditability: An organization's security policy can be properly enforced only if accountability is maintained, i.e., security can be maintained only if subjects are held accountable for their actions. Effective accountability relies upon the capability to prove a subject's identity and track their activities. Accountability is established by linking a human to the activities of an online identity through the

security services and mechanisms of auditing, authorization, authentication, and identification. Thus, human accountability is ultimately dependent on the strength of the authentication process. Without a reasonably strong authentication process, there is doubt that the correct human associated with a specific user account was the actual entity controlling that user account when an undesired action took place.

Information Security Governance

Information security governance consists of the leadership, organizational structures and processes that protect information and mitigation of growing information security threats like the ones detailed above.

Critical outcomes of information security governance include:

* Alignment of information security with business strategy to support organizational objectives
* Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level
* Management of performance of information security by measuring, monitoring and reporting information security governance metrics to ensure that organizational objectives are achieved
* Optimisation of information security investments in support of organizational objectives

It is important to consider the organisational necessity and benefits of information security governance. They include increased predictability and the reduction of uncertainty in business operations, a level of assurance that critical decisions are not based on faulty information, enabling efficient and effective risk management, protection from the increasing potential for legal liability, process improvement, reduced losses from security-related events and prevention of catastrophic consequences and improved reputation in the market and

among customers.

A comprehensive security programme needs to include the following main activities:

* Development and ongoing maintenance of security policies
* Assignment of roles, responsibilities and accountability for information security
* Development/maintenance of a security and control framework that consists of standards, measures, practices and procedures
* Classification and assignment of ownership of information assets
* Periodic risk assessments and ensuring adequate, effective and tested controls for people, processes and technology to enhance information security
* Ensuring security is integral to all organizational processes
* Processes to monitor security incidents
* Effective identity and access management processes
* Generation of meaningful metrics of security performance
* Information security related awareness sessions to users/officials including senior officials and board members