Chapter – 4

E-SECURITY AND SECURITY STANDARDS
4.1 Introduction to E-Security

Information is an asset that, like any other important business assets, is essential to an organization’s business and consequently business needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to an increase in number of frauds and a wider variety of threats and vulnerabilities.

Information can exist in different forms. It can be printed or written on paper, stored electronically, transmitted by post or electronic means, shown on films, or spoken in conversation. In whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security or E-security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, wherever necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes. To have better control in the information superhighway, a good number of security standards were developed over the last decade. These security standards which are comprehensively developed to protect data can control and maintain the data inflow/outflow without any interruption in this information technology superhighway.
4.2 What is a Standard and why it is required

Standards are means to share ideas and to establish a common understanding on a given subject for all stakeholders, which eventually helps in minimizing communication gaps and building low cost solutions. By following standards one can ensure quality, efficiency, reliability and interchangeability at an economical cost. The standards framework provides structure that one can follow and which helps everyone be on the same line because they can see what is expected. It becomes easier for all stakeholders to effectively use and implement any process/activity. According to their adoptability and its nature, classifications have been evolved.

4.3 Classification of Standards

Standards are classified in three categories namely mandatory, recommended and emerging.

**Mandatory:** Standards which are tried and tested and represent preferred solution. For example TCP/IP.

**Recommended:** Standards which are tried and tested, but are not mandatory and/or do not represent the preferred solution. For example ISO 9001, ISO/IEC 17799.

**Emerging:** Standards which are in line with the intended development trend, but they have not achieved mature level. For example PCI-DSS.

Standards which are being considered for incorporation are said to be under evaluation such as Mobile Banking Data Security Standard (MBDSS).

4.4 Information Security Standard

4.4.1 ISO/IEC 17799:2005\(^{17}\)

This standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security
management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:

- Security policy;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management;
- Compliance.

The control objectives and controls in ISO/IEC 17799:2005 are intended to be implemented to meet the requirements identified by a risk assessment. It is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

This recognizes that the level of security that can be achieved purely through technical means is limited. The required level of security established through assessing the levels of risk and associated costs through breaches of security, against the costs of implementing security should always be driven by appropriate management controls and procedures. Information security management requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties and customers. The standard identifies the controls that form the starting point for information security. It covers the critical success factors, the organization of information security, asset management, human resources, physical and environmental security, communications and operations management, information systems acquisition, development and
maintenance, incident management, business continuity management and compliance. It is destined to become an essential tool for organizations of every type and size, whether public or private.

4.4.2 ISO/IEC 27003: 2010

This standard focuses on Information technology security techniques, information security management system implementation guidance and suggestions that will be useful for all types of security-conscious organizations, regardless of their size, complexity and risks.

Today, information security is constantly in the news with identity theft, breaches in corporate financial records and threats of cyber terrorism. An information security management system (ISMS) is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems.

The successful design and implementation of an ISMS (ISO/IEC 27001:2005) will reassure customers and suppliers that information security is taken seriously within the organizations they deal with because they have in place state-of-the-art processes to deal with information security threats and issues. Since last two decades to meet the increasing customer requirements the banks and financial institutions started issuing credit/debit cards. This has led to the importance of maintaining the security of customer data. To ensure online data security the standard called PCI DSS was evolved by five companies in September 2005.

4.5 Payment Card Industry – Data Security Standard – PCI-DSS 

Any business that processes, stores or transmits cardholder data must comply with the PCI standard, a set of 12 requirements developed by five companies i.e. VISA, American Express, JCB, Discover Financial services and Master. The standard includes requirements for strictly controlling access to customer data, authenticating business users, monitoring access, maintaining secure network and auditing system resources. Failure to comply can result in the revocation of the privileges to collect credit card payments. The PCIDSS origin and its progress can be seen from the Figure 4.5.1
The detailed requirement of PCI-DSS is given in the Appendix-VIII. The PCI DSS requirements apply to businesses that store, process, or transmit a customer’s Primary Account Number, or PAN. If a PAN is not stored, processed, or transmitted, the PCI DSS requirements do not apply. These payment brands have established their own requirements and timeframes for businesses and merchants to comply with the current version of the standard as well as penalties for noncompliance. The payment brands can levy hefty fines on businesses that fail to comply or suspend their payment card processing privileges.

The standard comprises 12 high-level requirements grouped into 6 categories. These requirements apply to all system components, any network component, server, or application that is connected to that part of the network that contains cardholder data or sensitive authentication data. The excerpt from PCI DSS are given in the Appendix-IX.
4.5.1 PCI DSS compliance requirements\textsuperscript{43}

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized. 

*Build and Maintain a Secure Network.*

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

*Protect Cardholder Data.*

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

*Maintain a Vulnerability Management Program*

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

*Implement Strong Access Control Measures*

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

*Regularly Monitor and Test Networks*

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

*Maintain an Information Security Policy*

Requirement 12: Maintain a policy that addresses information security
4.5.2 Mapping out PCI DSS compliance for organization

PCI DSS compliance is not an overnight process; rather, it's the collaboration of numerous initiatives undertaken by various personnel within the organization, all working towards a common goal. In short, it can sometimes be a monumental effort needed by all for ensuring PCI DSS compliance is ultimately successful.Outlined are key activities, deliverables, and milestones for ensuring the organization is on the right path for PCI DSS compliance.

Phase I: Readiness Assessment
Phase II: Remediation & Implementation
Phase III: Assessment & Reporting

4.5.3 Phase I: Readiness Assessment

If the organization is new to PCI DSS compliance, then it's wise to begin the process with a Readiness Assessment which helps pave the way toward successful compliance by undertaking the following activities:

- In-depth scoping analysis as it related to the PCI DSS criteria and its 12 core areas.
- Review and analysis of current policies, procedures, and initiatives throughout the organization for meeting PCI DSS compliance.
- Analysis of debit/credit (i.e., payment) Card "Transaction Environment" Analysis of hardware/software systems, components and all other related application and network layer devices.
- Identifying and analyzing all significant third party outsourcers and managed service providers used by your organization. Internal assessment of available personnel within the organization.
- Cursory, initial walk-through of all 12 core PCI DSS standards necessary for meeting compliance.

4.5.4 Phase II: Remediation & Implementation

Immediately after the completion of a PCI DSS Readiness Assessment, it's critical that organizations take corrective action on any
deficiencies or weaknesses found that may serve as a roadblock for successful PCI DSS compliance. Generally, one of the areas of concern is that of documented policies and procedures. While most organizations are very good at what they do, they simply lacking many of these much needed policies and procedures that are so vital to PCI DSS compliance. Thus, the development of a companywide "Corporate Security Policy & Procedure" Handbook for helping meet the demands as set forth for PCI DSS compliance is essential. NDB Advisory can assist in helping developing these documents, creating highly customized policies and procedures for your company.

In addition to the policies and procedures, additional recommendations may be given on any number of topics or issues regarding PCI DSS compliance, such as adding, removing and modifying application and network layer devices, enforcing additional security procedures, or a host of other requirements. And because each entity has different needs and requirements that are based on a number of parameters, it's more proof of why a Phase I PCI DSS Readiness Assessment is considered crucial.

In short, the remediation and implementation phase is a vital element for ensuring your organization meets the rigorous demands set forth for PCI DSS compliance.

4.5.5 Phase III: Assessment & Reporting

The actual PCI DSS assessment is not a standalone process that starts from scratch; rather, it is collection of efforts continued over from the Readiness Assessment and the implementation phases. All the time and effort put into Phases I and II have prepared the organization for the assessment and all testing and validation activities that accompany it. Upon completion of the PCI DSS assessment, there are a host of reporting and deliverable requirements necessary for final confirmation of successful PCI DSS compliance. Reporting and submittal of compliance can become complex, as there are a number of different protocols to follow. The PCI DSS Qualified Security Assessor (QSA) will help assist and guide organization on these administrative matters.
4.5.6 PCI-DSS 1.1, 1.2 – summary changes from 1.1 to 1.2

PCI DSS 1.2 is considered a minor update to the DSS version 1.1. PCI DSS 1.2 has the same 12 requirements as did 1.1 and no new requirements have been added. The intent of 1.2 is mainly to clarify the existing requirements and provide some flexibility in terms of interpretation of the standard.

Segmentation of network, although not a requirement, the council provided guidance around scope of PCI DSS and elaborated on segmentation of Card Holder Data Environment. Segmentation of network helps isolate cardholder data environments and provides better controls and thus reduces the scope of devices that come under the PCI DSS.

Segmentation of network, although not a requirement, the council provided guidance around scope of PCI DSS and elaborated on segmentation of Card Holder Data Environment. Segmentation of network helps isolate cardholder data environments and provides better controls and thus reduces the scope of devices that come under the PCI DSS.

Scope of PCI DSS and elaborated on segmentation of Card Holder Data Environment. Segmentation of network helps isolate cardholder data environments and provides better controls and thus reduces the scope of devices that come under the PCI DSS.

Scope of PCI DSS and elaborated on segmentation of Card Holder Data Environment. Segmentation of network helps isolate cardholder data environments and provides better controls and thus reduces the scope of devices that come under the PCI DSS.

The changes are made to counter the growing number of violations of PCI-DSS. These changes were made according to feedback from the merchants, service providers and banks. The main changes are as follows.

- Segmentation of network helps isolate cardholder data environments and provide better controls.
- Wireless networks should be implemented using industry best practices like IEE 801.11X.
- Web application security is mandatory
- Firewall audit for 6 months (90 days in 1.1)
• Annual visit to offsite storage and review and acceptance of security policy annually.
• Announcement of Quality Assurance(QA) program for assessors.
• Documentation of cardholder data environment.

PCI-DSS 1.2 is largely focused on securing the perimeter to stop cyber criminals from getting in. There is a desire to have more requirements to addressing the internal threat. (APPENDIX- XI-XIII)

4.5.7 PCI-DSS 2.0 summary changes

The latest version of the Payment Card Industry Data Security Standard (PCI DSS v2.0) came into effect on January 1, 2011. In this version, one year has been given to comply with the new standard. If a company started a Report on Compliance( RoC) assessment cycle in 2010 using v1.2.1, that cycle can be completed before the end of 2011 against v1.2.1. If an organization starting a new assessment in 2011, the RoC will be based on v2.0 but that doesn’t mean a significant change from previous assessments. The reason for this is that the overwhelming majority of changes between the previous and new version of the standard are clarifications.

The PCI Security Standards Council defines “Clarifications” to the PCI DSS as follows – “Clarifies intent of requirement. Ensure that concise wording in the standards portray the desired intent of requirements.” Of the 137 changes detailed in the Summary of Changes from PCI DSS Version 1.2.1 to 2.0, 119 of them are typed as clarifications. The purpose of the clarifications is to lower the points of contention during audit with better, more precise wording in the standard.

4.6 Evolving standards

Though not necessarily comprehensive, the following standards can help address many of the considerations like protecting privacy and securing transactions.
4.6.1 ISO/IEC JTC 1 SC 37

Subcommittee 37, Biometrics, develops generic biometric standards in the areas of vocabulary (WG 1), technical interfaces (WG 2), data interchange formats (WG 3), application profiles (WG 4), performance testing and reporting (WG 5), and cross-jurisdictional and societal aspects (WG 6) of biometrics. Some of these have developed standards that are used in biometric authentication and identity systems. For example, biometric data representations are specified in the ISO/IEC 19794 (Biometric Data Interchange Format) series of standards and data structures are defined in ISO/IEC 19785 (Common Biometric Exchange Formats Framework).

Both CBEFF and BioAPI (ISO/IEC 19794) provide a biometric data structure (called a biometric information record, or BIR) that provides for the confidentiality and integrity of the biometric data through header elements and an optional security block (which could contain, for example, a digital signature or encryption parameters). In addition, other elements of the biometric header can also contribute to the protection of the data. These include payload and challenge-response elements as well as a “purpose” field. When signed, this can prevent enrolment data from being replayed as a captured biometric verification sample. BioAPI is currently being extended to support the exchange of certificates and security assertions.

The work of WG 5 in the 19795 (Biometric performance testing and reporting) series specifies the methodology for quantifying the performance of biometric systems and algorithms. This allows implementers to have more confidence in the error rates associated with biometric components used in their systems.

4.6.2 ISO/IEC JTC 1 SC 27

Subcommittee 27, IT Security Techniques, in addition to general IT security and cryptographic standards that would apply to biometric system security and data protection, has several standards and projects that relate directly to the area of biometric security or identity management. These include:

ACBio specifies a technique for securing remote biometric authentication over an open network. It includes methods for message integrity, component authentication, and an associated cryptographic syntax.


This standard addresses the basis of trust in the security of applied biometrics in the context of common criteria testing.

ISO/IEC 24745 - Information technology - Security techniques - Biometric template protection (Committee Draft)

This standard addresses methods for protecting biometric data, including the confidentiality, integrity, and availability thereof. It also addresses template binding techniques and biometric cryptosystems.

ISO/IEC 24760, Information technology - Security techniques – A Framework for Identity Management (Committee Draft)

This project provides an ontology and structure to facilitate common representations for the many diverse conceptualizations and implementations of Identity Management. In its draft form, it seeks to define identity and the concepts of managing identity information, including identity management capabilities:

- Provide principles for frameworks that may serve the management of identities and the respective applicable requirements (e.g., policy, law); and
- Provides rules for the secure and reliable processes of managing identity information, including the control of the lifecycle of identities and identity information as they are established, activated, suspended, terminated or archived.

4.6.3 ISO TC 68

TC 68, Financial Services, has developed a standard focused on the security of biometric systems - ISO 19092 1:2006, Financial Services - Biometrics - Part 1: Security Framework. This standard addresses core
security requirements related to the use and management of biometric data in financial systems and transactions, to include integrity, authenticity, and confidentiality. It also describes the architectures for implementation, specifies the minimum security requirements for effective management, and provides control objectives and recommendations suitable for use by a professional practitioner.

4.6.4 Mobile Banking Data Standard

The Draft was released for mobile security standard in Sept 2006. The specification is designed to protect data and prevent tampering. The Trusted Computing Group (TCG) has released a first draft of its Mobile Trusted Module (MTM) specification at the CTIA trade show in Los Angeles. The specification provides a standard for manufacturers and developers to store data securely on mobile phones. The project includes such manufacturers as Ericsson, Nokia, Motorola and Sony, along with Intel, IBM and VeriSign. The TCG first introduced its plans for the mobile security chip at CTIA in San Francisco in 2005.

The MTM would be stored within a protected area of the phone, and would require various "engines" within the device to report the state of their code, ensuring the integrity of the data on the handset.

While the MTM could allow manufacturers and operators to reduce the risk of virus attacks and identity theft, it also could be used to further limit consumers in what they can do with their mobile phones. This could include the regulation of downloadable applications and ring tones, as well as enforcing digital rights management (DRM) technology.

This researcher also written article on MBDSS\textsuperscript{45} framework in a research journal. The framework model for the mobile phones for financial transactions has been discussed in the article.

The Security standards followed by online banking service providers are mandatory and adhere PCI-DSS. The details of PCI-DSS version 1.0 &1.1 comparison is given in the APPENDIX-XII. The researcher has conducted a survey of selected banks in India that are issuing credit/debit cards to its customer and the study is presented in the next chapter.