The Study of Appropriate Potential Information Security Standards for Defending from Dark Cloud and Ensuring IT Security Assurance

Dr. Sunil Khilari Dr.Sachin Kadam

Abstract: *Information Security (IS) is a real-worldissue, not a theoretical build. Terrible need of practicing good and emerging IS standards and their efficient and effective management of has no any alternate option and has unique key concern for all organization. There are numerous ways a program can fail and countless ways to turn the underlying faults into security issues which may because of non-practicing required security code standards. It is of course better to focus on prevention than cure. Need to understand useof IS standards during software development to till the deployment of final system. In this paper, researcher provides an overview of several standards that can prove usefulness in finding and fixing security flaws. Since adequate standards cannot be provided by technology alone, it is necessary to rely on a combination of hardware, software, and procedural experts.The main goals of this paper areto identify some key IS standards and their usage in everyday life of digital generation and digital economy. The paper is mainly focused on the activities of control management as well as on the roles and responsibilities of the individuals andgroups involved in practicing the good IS standards.*

Keywords:*Information security standards, Information security assurance, dark cloud.*

1. INTRODUCTION

The IT security standards are compulsory actions or rules that give formal policies support and direction. Its good practice to avoid past mistakes related to information security. One of the more difficult parts of developing or writing standards for an information security program is getting a company-wide consensus on what standards need to be in place.

Figure-1: ISMS in business

Regardless of how the standards are established, by setting standards, policies that are difficult to implement and that affect the entire organization are guaranteed to work in safe environment. Even for small organizations, if the access policies require one-time-use passwords, the standard for using a particular token device can make interoperability a relative certainty

2. PURPOSE OF INFORMATION SECURITY STANDARDS

Maintaining the confidentiality, integrity and availability ofinformation. The IS standards can play vital role. AIS security standard is like any other standard within any other industry. A standard is "a published specification that establishes a common language, and contains a technical specification or other precise criteria and is designed to be used consistently, as a rule, a guideline, or a definition". Further, according to ISO, standards "contribute to making life simpler, and to increasing the reliability and effectiveness of the goods and services we use".

In essence a IS standard is a common set of rules, good practices, definitions and agreed regulations that all concerns can refer to for common reference. A standard would be a set of minimum requirements that an organization must meet in order to claim to be compliant with the standard.

Generally speaking a standard, whether it is an accountability standard, a technical standard or an information security standard, it represents a set of requirements that a product or a system must achieve. Assuming the conformity of a product or system with a certain standard demonstrates that it fulfills all the standard's specifications to reduce the risk.

There are currently some primary standards in place governing information security. First of them is the ISO/IEC 27000 series of standards. It is the most recognizable standard as it bears the internationally prominent name of the International Organization for Standardization and the International Electro technical Commission.

It was initiated by British Standard Institute in 1995 through BS7799 (Information Security Management System), and later was taken over by the ISO (International Organization for Standardization) and released under the name of ISO/IEC 27000 series (ISMS Family of Standards) and ISO/IEC 17799:2005 "Information Technology – Code of practice for information security management".

Another information security standard is the Information Security Forum's Standard of Good Practice for Information Security. This document also includes a description of COBIT and BSI Standards 100 series. Due to the lack of space other international security standards like ITIL could not be presented.

3. NEED OF INFORMATION SECURITY STANDARDS

Standards provide us with a common set of reference points to enable us to evaluate whether an organization has processes, procedures and other controls in place that meet an agreed minimum requirement. If an organization is compliant/meets a certain standard then it gives third parties such as

customers, suppliers and partners confidence in that organization's ability to deliver to that standard. It can also provide an organization with a competitive advantage over other organizations. For example an organization that is compliant with a security standard may have an advantage over a competitor who does not when customers are evaluating their products or services. In other cases certain regulatory and legal requirements may specify certain standards that must be met.

The use of standards is unanimously accepted and gives the possibility of comparing a personal security system with a given frame of reference adopted at an international level. A good example is the ISO 9000 set of standards regarding the quality management system, which is a common reference regardless of the industry in which a certain company activates.Standards ensure desirable characteristics of products and services such as quality, safety, reliability, efficiency.

4. INFORMATION SECURITY CHALLENGES

Information or Cyber security is major national, international and economic security issue of all concerns. Protecting assets and managing access to IT resources has more important. Dark cloud is expanding the attack surface and breaking traditional network boundaries. Need to check whether our current security architectures mitigate the threats and vulnerabilities. Many organizations are spending large amount of money on IT system because they recognize the tremendous benefits that IT can bring to their business operation and services. However they need to ensure that their IT systems are reliable, secure and not vulnerable to any attack or threat.

5. INFORMATION ASSURANCE VS. SOFTWARE SECURITY ASSURANCE

When management choose to beat competition by giving their employees increased access to business critical resources, it also felt the need to conduct a security audit to get a closer look at the strength and weakness of the current infrastructure along with advice on strategies and polices required to stay competitive. In this scenario Information assurance and software security assurance plays vital role.

Table No.1 : IA Vs SSA

Information assurance (IA)	Software Security Assurance (SSA)
The practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes	The process of ensuring that software is designed to operate at a level of security that is consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability, or misuse of the data and resources that it uses, controls, and protects

6. DARK CLOUD

"Dark Cloud" computing networks, known as botnets. Can run millions of infected computers, called bots which spread malware. Its take-up is still being held back by much fear, uncertainty and doubt among not just potential cloud users, but also some policymakers and regulators. It's been a few years since cloud computing hit the IT scene like rolling thunder, but many businesses still struggle with making the move to the cloud. A server that is not in-house is less secure. The cloud is very expensive. If someone else is managing the data, you don't need an in-house IT staff.

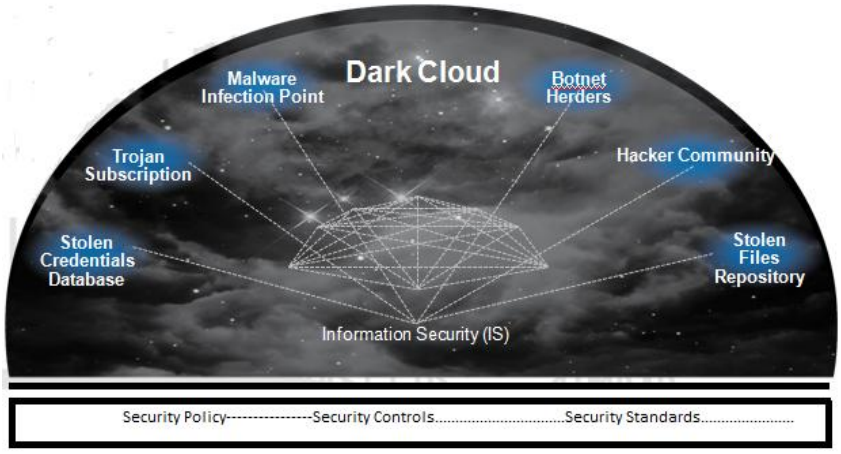

Figure-2: Dark cloud in IS

7. TYPES OF INFORMATION SECURITY STANDARDS

There are numerous standards available. These can be broken down into three main sections;

- Business Standards
- Product Standards
- Individual Standards

You can be assessed and certified against any of the above to demonstrate that you meet the minimum requirements to satisfy the standard. If you meet those requirements then you can be certified against that standard.

So a business standard would apply to an organization and state they meet the requirements for the organization to satisfy the standard. Product standards mean when you purchase a product you know it has been independently accessed as being secure according to predefined criteria. If you are hiring someone as a member of staff or as a consultant you can determine if they have the minimum knowledge that you require for that role by looking at the standards they have earned.

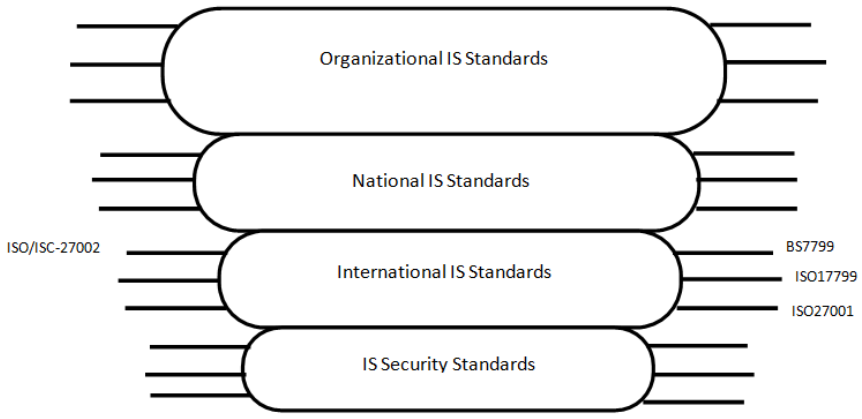

Figure-3: Types of IS standards

In order to obtain a standard I suggest you;

- Determine which one is suitable to you and/or your organization or product.
- Become familiar with that standard. You can obtain a copy of that standard from the organizationsthat develop the standard or it may be available from other third parties.
- Engage someone with knowledge of that standard, either in-house use an external consultant.
- Determine what gaps currently exist within your organization against the standard and develop a plan to address those gaps.
- Engage with a certification body to achieve the standard.

8. DEVELOPMENTS AND IMPLEMENTS OF IS STANDARDS

International, regional, national, industry, and government groups are involved in the development of cyber security standards. An *SDO* is an organization whose primary mission is the development of voluntary consensus standards on an international, regional, or on a national basis. Most SDOs cover a wide variety of technical areas, not just cyber security. *Consortia, industry alliances,* and *associations* are all groups of organizations or individuals with similar interests that promote standards development. A consortium is typically formed for a limited time to achieve a specific goal, such as the development of standards. *Industry alliances* and *associations* tend to be more loosely formed to foster common interests. Consortia and industry alliances comprise companies, and associations are made up of individuals. Finally, the US *government* and other national governments develop standards specifically intended for government audiences. Examples of organizations in each of these categories are provided below, along with brief discussions of some of the organizations' cyber security standards work.

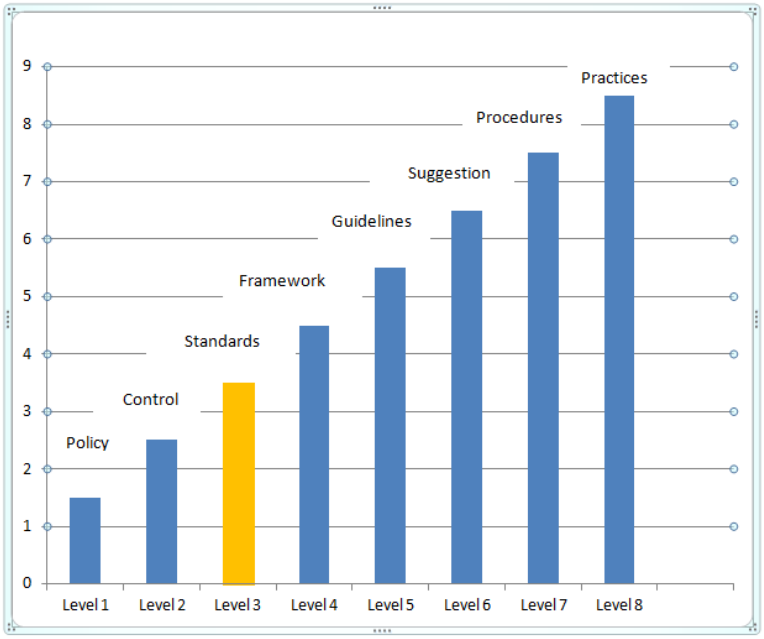

Figure No. 4: Levels of defense in IS

Cyber Security Standards Developers

International, regional, national, industry, and government groups are involved in the development of cyber security standards. An *SDO* is an organization whose primary mission is the development of voluntary consensus standards on an international, regional, or on a national basis. Most SDOs cover a wide variety of technical areas, not just cyber security. *Consortia*, *industry alliances*, and *associations* are all groups of organizations or individuals with similar interests that promote standards development. A consortium is typically formed for a limited time to achieve a specific goal, such as the development of standards. *Industry alliances* and *associations* tend to be more loosely formed to foster common interests. Consortia and industry alliances comprise companies, and associations are made up of individuals. Finally, the US *government* and other national governments develop standards specifically intended for government audiences. Examples of organizations in each of these categories are provided below, along with brief discussions of some of the organizations' cyber security standards work.

8.1 International Standards Development

The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) develops standards in many areas, including information technology, telecommunications, and power generation. An example of IEEE-SA's security work is its 802 Local Area Network (LAN)/Metropolitan Area Network (MAN) Standards Committee.

ISO, whose membership consists of the national standards institutes of more than 150 countries, addresses all standards except those for electrical and electronic engineering, which are the responsibility

of the IEC. ISO and IEC formed the Joint Technical Committee 1 (JTC1) for IT standards development, including standards for the security of systems and information. JTC1 has a number of subcommittees (SC) and working groups that address specific technologies

8.2 Regional Standards Development

The European Telecommunications Standards Institute (ETSI) produces telecommunications standards within Europe. ETSI's cyber security standards activities include work on electronic signatures, smart cards, lawful interception, and 3GPP.

The CEN, whose members are the national standards organizations of 30 European countries, develops cyber security standards on its own and in conjunction with other international, national, and government standards developers.

8.3 National Standards Development

The International Committee for Information Technology Standards (INCITS) is an ANSI-accredited organization, which develops US standards for information and communications technologies. INCITS comprise technical committees (TCs) that create standards for different technology areas. The Information Systems Audit and Control Association (ISACA) is an organization for information assurance, governance, security, and audit professionals. It is best known for its information system auditing and control standards and related initiatives. For example, ISACA has developed Control Objectives for Information and related Technology (COBIT), which is a control framework that encompasses several aspects of IT governance, including risk assessment. COBIT is based on various international standards and can be used to identify appropriate standards references during audits.

The Instrumentation, Systems, and Automation Society (ISA) are a professional association that develops standards for automation technologies.

- ISO/IEC 27000 family of Information Security Management Systems - This document provides an overview of ISO/IEC 27000 family of Information Security Management Systems which consists of inter-related standards and guidelines, already published or under development, and contains a number of significant structural components.
- ISO 27001 - This document provides the ISO standards of the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.
- ISO 27002 - This document introduces the code of practice for information security controls.
- British Standard 7799 Part 3 - This set of guidelines is published by BSI Group for the information security risk management.

- COBIT - The Control Objectives for Information and related Technology (COBIT) is published by the Standards Board of Information Systems Audit and Control Association (ISACA) providing a control framework for the governance and management of enterprise IT.
- Common Criteria (also known as ISO/IEC 15408) - This set of evaluation criteria's is developed by and aligned with national security standards organizations of Australia, Canada, France, Germany, Japan, Netherlands, New Zealand, Spain, UK and US.
- ITIL (or ISO/IEC 20000 series) - This document introduces a collection of best practices in IT service management (ITSM), and focuses on the service processes of IT and considers the central role of the user.
- National Information Security Technology Standard Specification - This webpage introduces a collection of national information security standards formulated by the National Information Security Standards Technical Committee. These standards include information security management, information security evaluation, authentication and authorization, etc.

Present technology offers no way to absolutely protect information or the computer operating system itself from*all* security threats posed by the human beings around it. As a consequence, procedural and administrative safeguards must be applied in resource sharing computer centers to supplement the protection available in the hardware and software. .problems of security is admittedly most acute at. Present, must be designed to protect each user from interference by another user or by the system itself, and must provide some sort of "privacy" protection

To users who wish to preserve the integrity of their data and their programs. Thus, designers and manufacturers of resource-sharing systems are concerned with the fundamental problem of protecting information.

9. BENEFITS OF IS STANDARDS

There are many more benefits of information security standards .Some of them are as below-

- Provides an opportunity to systematically identify and manage risks
- Allows an independent review of information security practices
- It provides a holistic, risk-based approach to secure information
- Demonstrates credibility to stakeholders
- Demonstrates security status according to internationally accepted criteria
- Creates a market differentiation

Cyber security standards are proliferating. Governments and businesses increasingly mandate their implementation. More manufacturers and vendors are building and selling standards-compliant products and services. In addition, a growing number of organizations are becoming involved in standards

development. Cyber security standards are being embraced because they are useful. They provide tangible benefits that justify the time and financial resources required to produce and apply them.

Security technology has not kept pace with the rapid development of IT, leaving systems, data, and users vulnerable to both conventional and innovative security threats. Politically motivated adversaries, financially motivated criminals, mischievous attackers, and malicious or careless authorized users are among the threats to systems and technology that have the potential to cyber security.

Designing, building, and testing software. The Nature of Software Development Software development is often considered a solitary effort; a programmer sits with a specification or design and grinds out line after line of code. But in fact, software development is a collaborative effort, involving people with different skill sets who combine their expertise to produce a working product.

We can examine both product and process to see how each contributes to quality and in particular to security as an aspect of quality. Let us begin with the product, to get a sense of how we recognize high quality secure software

10.CONCLUSION

Organization must implement standards to reduce the risk as well as develop incident response plans and business continuity plans. The ISstandards should periodically be scrutinized and updated, and risk analysis performed on priority basis. Information security standards are needed in order to implement information security controls to meet an organizations requirements as well as a set of controls for business relationships with other organizations. The most effective way to do this is to have a common standard on best practice for information security management. By practicing these standards organizations can benefit from best practice at an international level, and can prove the protection of their business processes and activities in order to fulfill business needs. The only problem is to choose which of the standards is appropriate for an organization judging by the nature and field of activity. The success of information security can only be achieved by full cooperation at all levels of organization.

Improvements in cyber security can help manage security risks by making it harder for attacks to succeed and by reducing the effect of attacks that do occur. Cyber security standards enhance security and contribute to risk management in several important ways. Standards help establish common security requirements and the capabilities needed for secure solutions. Security standards facilitate sharing of knowledge and best practices by helping to ensure common understanding of concepts, terms, and definitions, which prevents errors.

11.REFERENCES

1. *Federal Office for Information Security (BSI), BSI Standard 100-1 Information Security Management System, http://www.bsi.de/english/publications/bsi_standards/index.htm 2008*
2. *An Overview of Information Security Standards, The Government of the Hong Kong Special Administrative Region, 2008, www.infosec.gov.hk/english/technical/files/overview.pdf*
3. *National Institute for Standards and Technology, An introduction to Computer Security – The NIST Handbook – SP 800-12, NIST 1995, http://csrc.nist.gov.*
4. *Baker, W. H., & Wallace, L. (2007). Is information security under control? Investigating quality in information*
5. *Security management. IEEE Security & Privacy, 5(1), 36-44.*
6. *Brykczynski, B. & Small, B. (2003). Securing your organization's information assets. The Journal of DefenseSoftware Engineering, 16(5), 12-16.*
7. *National Institute for Standards and Technology (2001). FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.*
8. *ITU Telecommunication Standardization Sector (2008). Security Compendium, Part 2—Approved ITU-T Security Definitions, http://www.itu.int/dmspub/itu-t/oth/0A/0D/T0A0D00000A0001MSWE.doc.*
9. *ISO/IEC 27001:2005 Information technology Security techniques - Information security managementsystems - Requirements, International Standards Organization, ISO/IEC 2005.*
10. *Thompson T. US Former secretary of Health and Human Services Keynote Speech at the 2007 CDHCExpo, Business Wire, Nov. 13, 2006*
11. *National Institute of Standards and Technology, "Minimum Security Requirements for Federal Information and Information Systems," FIPS PUB 200, March 2006.*
12. *National Institute of Standards and Technology, "Information Security Handbook: A Guide for Managers," NIST Special Publication 800-100, October 2006.*
13. *National Institute of Standards and Technology, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)," NIST Special Publication 800-27, June 2004.*