# ISG Framework for Online Banking Systems

**Dr. Tejinder Pal Singh Brar**
Associate Professor,
Department of Computer Applications,
CGC Landran.

## Abstract

E-banking primarily relies on Internet and communication technologies in order to operate their businesses and interacting with customers. On the other hand threats and security breaches have increased dramatically in recent years. Online attacks have caused loss of global businesses and customer's trust on banking systems. Thus, there is a need for an apposite framework to govern the information security in online banking systems. This paper tries to emphasize on the information assets and prospective threats for E-banking. It further scrutinizes and evaluates the elements from the universally used information security governance frameworks, standards and practices. This paper proposes the preliminary framework for governing the information security in online banking systems. This proposed framework will be implemented in online banking environment.

**Keywords:** Information Security Governance, E-Banking, Corporate Governance, Trust

## Introduction

With the introduction of enhanced communication technologies number of electronic services for both corporate and retail customers' have evolved and spread widely. On the other hand the need for security has also increased because attackers have developed more complicated methods to compromise authentication mechanisms and gain unauthorized access to customers' sensitive information. As a result of this, not only user's trust has been decreased but also the spread of Internet banking applications in the market. Malhotra and Singh (2009) found that slowly but steadily, the Indian customer is moving towards internet banking. But they are concerned about issues such as security and privacy. Mukti (2000) found that security is main barrier to e-commerce expansion in Malaysia. According to him, security is the most feared problem on the internet. Banks and customers take a very high risk by dealing electronically. The survey conducted by White and Nteli (2004) found that UK consumers ranked the security of bank's website as the most important attribute of internet banking service quality. This situation is further illustrated by Sathye (1999), investigate the adoption of internet banking found that security concerns and lack of awareness about the internet banking were the two main obstacles for the non-adoption.

Security affects trust and satisfaction of the customer. There are number of factors which affect the customers thinking about online banking security. Fitzergerald (2004) argued that lack of awareness of online banking and the security concerns are the major 'non-adoption' areas of E-banking. Kalakota and Whinston, (1997) defines Perceived security as a threat that creates a circumstance or condition, with the potential to cause economic hardship to data or network resources in the form of destruction, disclosures, and modification of data, denial of service, and/or fraud, waste and abuse. According to Aladwani (2001), future challenges for the adoption of E-banking are internet security, consumers' privacy, bank's reputation and online banking regulations. Author further found that customers ranked privacy and internet security as the most important future challenges.

According to the white paper published by Symantec co. malicious applications that steal financial account information have increased dramatically over the last few years, resulting in a direct loss of hard currency as well as loss of trust. Dixit and Dutta (2010) insist that banks needs to increase the level of trust between banks' website and customers. According to Alnsour and Hyari (2011) trust has a significant and positive effect on ease of use. The more a user trusted the bank and its website, the higher their belief that online banking is easy. Higher levels of security may make online banking more useful. Bala et al. (2011); Viega and McGraw (2001) suggests developers have to incorporate security during the development process itself in order to produce software assurance systems, since the existence of flaws at the design or coding stage of the development process can open web applications to a wide range of attacks. Lin and Vardharajan (2006) and Tat et al. (2008) confirmed the influence of trust on risk perception and consumer attitudes towards internet banking. Tendency to trust is a determinant not only for interpersonal relationships but also for trust in technological systems.

Karimi (2014) describes a security lapse related to credit and debit card transactions; about 105,000 credit card and debit card transactions were compromised in data breach. Finkle and Henry (2013) found that Target Corp (TGT.N) which is one of the biggest retailers in U.S. attacked by hackers in November 2013 which lasts for 19 days. This attack compromised up to 40 million credit cards and debit cards also managed to steal encrypted personal identification numbers (PINs) that makes it the second-largest data breach in U.S. retail history. The online fraud/attacks that have been reported around the globe over the last 2 years are related to poor or simplistic authentication practices. In spite of innovation in security technologies, fraudsters still manage to breach banks' resistance from time to time.

Nearly 80% of U.S. banks think that malware on their customers' PC is a top security risk. Indeed this seems justified because U.S. consumers lost over US$ 2 billion and 1.3 million PCs to malware in 2010, Dinesh (2011). The top spot of weak authentication is taken by password which is the most prevalent and weak form of authentication because it is very easy to steal, Kitten (2014). While analyzing Indian scenario of cyber attacks, Bipindra (2014) in his report highlight the incident when Defense Research and Development Organization's (DRDO) computers were hacked by Chinese hackers. Kumar (2014), also states that 3,000 internet connections of the defense ministry and the air force communication centre have been compromised and also vulnerable to Domain Name System (DNS) exploitation attacks. While taking note on state-wise scenario, NCRB (2013) reported 4,356 cases were registered under IT Act during the year 2013 as compared to 2,876 cases during 2012, thus showing an increase of 51.5% in 2013 over 2012.

Similarly, according to Gurung (2014) there is an increase in the cyber crime by 51%, the cases related to cyber crime that was filled in the year 2013 was 4356 and this year it is increased by 51 percent in comparison to previous year.

**Role of Information Security Governance (ISG) in Banking**

There are number of definitions on information security governance but there is lack of consensus in the definition of Information Security governance (Rastogi and Von Solms, 2006). Harris (2006) summarized that information security governance ensure security is carried out to meet an organization's specific needs. It requires organizational structure, roles and responsibilities, performance measurement, defined tasks and oversight mechanisms.

The identification of the information assets of the company is critical for success of information security in companies. Kurt and Tentra (2004) categorize the information assets to be protected in the banking industry into four items i.e. insider information, client information, client information and balance information and transaction information.

**Information Security Governance Framework**

Rastogi and von Solms (2006) describe that information security governance consists of structures, relationships and processes. There are various information security governance frameworks which have been widely used such as FFIEC, PCI, COBIT, ISO 27002, IISA, CGTF and CISWG. Holmquist (2008) suggests that there are several choices of information security governance frameworks applicable to banking industry such as FFIEC, COBIT, ISO 27002 and PCI data security standard. Based on this suggestion, we further look into the information security governance framework approach based on ISO 27002**,** COBIT and FFIEC. Table 1.1 shows brief description to each framework.

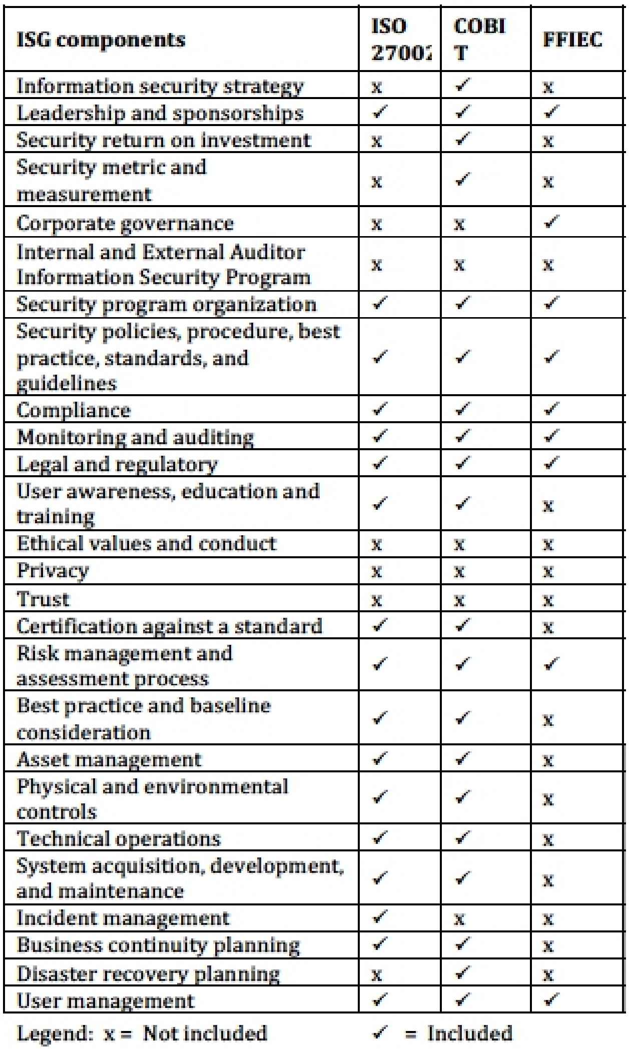
**Table 1.1: Description of different security governance frameworks**

| Item | Description |
|---|---|
| ISO 27002 | The International Organization for Standarization (ISO) is "the world's largest developer and publisher of international standards in a wide area of subjects including information security management systems and practices. The ISO 27002 (2006) standard, formally The ISO 17799 (2005) standard, is an industry benchmark code of practice for information security practice”. IT outlines 11 control mechanisms and 130 security controls. The standard establishes guidelines and general principles for "initiating, implementing, maintaining, and improving information security management within an organization". |
| COBIT | Control Objectives for Information and related Technology (COBIT) is developed by The Information Systems Audit and Control Association & Foundation (ISACAF) to provide management and business process owners with an IT governance model to help understand and manage the risks associated with IT. COBIT consists of four main components namely, plan and organize, acquire and implement, deliver and support, and finally monitor and evaluate. |
| FFIEC | The Federal Financial Institutions Examination Council (FFIEC) was established in 1979. It was given the authority to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. The FFIEC publication: "Information Security ITExamination Handbook" is used by federal examiners auditing the operations of financial institutions for compliance with their obligations. FFIEC’s October 2005 "Authentication in an Internet Banking Environment" guidance will be part of that handbook. |

Source: Developed by the researchers

In order to define and construct a new information security governance framework for banking table 1.2 provides the different components and compares the commonly used approaches to information security governance frameworks. It is found that the design of business oriented information security can only originate from an information strategy that is in agreement with the business strategy. Table 1.2 shows that corporate governance, ethical conduct, trust, and auditor security program are not included in many other frameworks, although all four components are considered as important components number of researchers [Flowerday and Von Solms, (2006); Allen and Westby, (2007)] when governing information security in an organization. It is important to note that not one of the frameworks cover all information security governance components.

**Table 1.2: Information Security Governance Approach Comparison**



| ISG components | ISO<br>2700: | COBI<br>T | FFIEC |
|---|---|---|---|
| Information security strategy | x | ✓ | x |
| Leadership and sponsorships | ✓ | ✓ | ✓ |
| Security return on investment | x | ✓ | x |
| Security metric and measurement | x | ✓ | x |
| Corporate governance | x | x | ✓ |
| Internal and External Auditor Information Security Program | x | x | x |
| Security program organization | ✓ | ✓ | ✓ |
| Security policies, procedure, best practice, standards, and guidelines | ✓ | ✓ | ✓ |
| Compliance | ✓ | ✓ | ✓ |
| Monitoring and auditing | ✓ | ✓ | ✓ |
| Legal and regulatory | ✓ | ✓ | ✓ |
| User awareness, education and training | ✓ | ✓ | x |
| Ethical values and conduct | x | x | x |
| Privacy | x | x | x |
| Trust | x | x | x |
| Certification against a standard | ✓ | ✓ | x |
| Risk management and assessment process | ✓ | ✓ | ✓ |
| Best practice and baseline consideration | ✓ | ✓ | x |
| Asset management | ✓ | ✓ | x |
| Physical and environmental controls | ✓ | ✓ | x |
| Technical operations | ✓ | ✓ | x |
| System acquisition, development, and maintenance | ✓ | ✓ | x |
| Incident management | ✓ | x | x |
| Business continuity planning | ✓ | ✓ | x |
| Disaster recovery planning | x | ✓ | x |
| User management | ✓ | ✓ | ✓ |

Legend: x = Not included ✓ = Included

(Source: Developed by the researchers)

Corporate information security governance should have its own place within the framework of corporate governance, beside IT governance and risk management. ISO 27002 and COBIT included technical practice security standards, which have the character of basic configuration and operation of IT systems and only indirectly affect information security (Kurt and Tentra, 2004). There are some frameworks that have been developed and widely practiced in corporate governance, but each of them has its own strengths and weaknesses. Therefore, customization is pertinent to appropriately fit with the organization's environment.

**Proposed Information Security Governance Framework**

The initial design of the proposed ISG framework can be used as a starting point by banking sector to govern information security by developing guidelines and implementing controls to protect banking information assets from the threats identified in literature reviews. This framework is an integration of all available framework components discussed and derived from literature review. However, the suggested framework is still a general approach to information security governance program which needs to be reviewed by professionals and tested in the real banking environment. As each organization's environment is different and subject to different national and international legislation and regulations, additional components might be required, while others may not be relevant. Based on structure given by Rastogi and Von Solm (2006), the initial design of information security governance framework constructs by mapping information security components into corporate hierarchy which are strategic level, tactical and operational level and operational level. Each level of information security components and the composition thereof are discussed below.

**Strategic Level:** Strategic level refers to board of directors and senior executive management; at this level information security strategies are compiled to address a successful information security program. The information security strategy should be linked to the organizational and IT strategy to ensure that the organization's objectives are met both in the short and in the long term. This level requires executive sponsorship for information security program as well as commitment from the board and management to protect information assets, (Witty and Hallawell, 2003).

**Tactical and Operational Level:** Tactical and operational level refers to senior managers and operation managers. This level addresses user awareness; education and training as key component. But not many researchers suggest ethical conduct, trust and privacy to be included in this level. Ethical conduct, trust and privacy are key component at this level. As part of the information security governance framework, ethical conduct must be addressed by the organization to minimize the online risks. These ethical conducts preserve to employees as part of the security awareness program. The other key component proposed in this level is “trust”. When implementing the information security governance framework components, management must be able to trust employees to adhere to information security policies, while employees must be able to trust management in keeping the commitment for implementing information security program. And privacy as key component in this level also an essential issue of trust when it comes to good relationships with customers, suppliers and other business partners (Tipton and Krause, 2004).

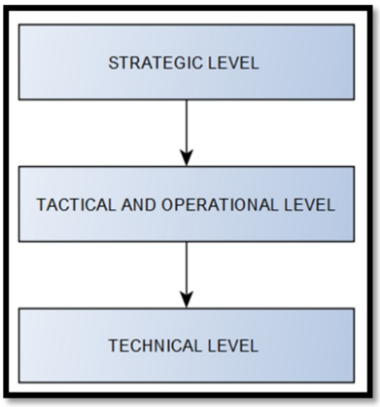


**Figure 1.1: Initial design of proposed ISG framework**

Source: Developed by the researchers

**Technical Level:** Technical level refers to all employees. It involves the technical and physical mechanisms implemented to secure an IT environment. When implementing the security governance framework, the technology controls applicable to the organization's environment and identified risks must be implemented. These include asset management, system development requirements, incident management, technical operations such as network security, and physical, environment, business continuity controls and user management. It is essential that the technology environment be monitored on a constant basis and that the risks of technology changes in the market are addressed.

## Conclusion

Threat landscape has been significantly changed because attackers have developed more complicated methods to compromise authentication mechanisms and gain unauthorized access to customers' information. Phishing attacks or malware can easily steal passwords, and attacker correctly answers the challenge questions on the basis of amount of information about customer that is available online. Challenge questions generally ask things like date of birth. These types of questions are easy to answer because large amount of information is available online about customer. When we talk about social networking websites, a large number of answers to challenge questions can be easily figured out from these online resources. In today's online environment, security is vital part of financial institution system. Having a reputation for safeguarding information and the environment within which it resides enhances an organization's ability to preserve and increase market share.

A comprehensive information security governance framework is highly needed for banking information system. Some general standards and best practices have been developed such as FFIEC, COBIT, ISO 27002 and PCI data security standard, but none of them can fulfill specific and unique needs of an organization. This in-progress research is to develop a specific information security governance framework with banking environment and IT information system in mind. To this end, the framework can be used as an initial effort for bank to govern their information security. This framework is an integration of all framework components available today. Essentially, this framework is still a general approach to information security governance program, it needs to be reviewed by professionals and comprehensively tested in the real banking environment. This study will proceed with a web-based survey to further examine the IT professional perception on information security governance framework in a newly developed country.

**References**

[1] Aladwani, M. (2001). Online banking: a field study of drivers, development challenges, and expectations. International Journal of Information Management, pp. 213-225.

[2] Allen, J. H. & Westby, J. R. (2007). Governing for Enterprise Security (GES), Implementation Guide: Characteristics of Effective Security Governance1. USA: Carnegie Mellon University. 5-7

[3] Alnsour, M. and AL-hyari, K. (2011). Internet banking and jordanian corporate customers: issues of security and trust. Journal of Internet Banking and Commerce, vol. 16, no.1. Retrieved from http://www.arraydev.com/commerce/jibc, November 2012.

[4] Bala, M.S. and Norita, M.N. (2011). Secure E-commerce web development framework. Information Technology Journal 10(4):769–779.

[5] Bipindra, N. C. (2013). Chinese 'hack' DRDO computers. Retrieved online at http://www.newindianexpress.com/nation/article1500336.ece, July 2014.

[6] Dinesh, T. C.(2011). What the future of online banking authentication could be. Retrieved from www.infosys.com/finacle, July 2014.

[7] Dixit, N. and Datta, S. K. (2010). Acceptance of E-banking among adult customers: an empirical investigation in India. Journal of Internet Banking and Commerce, August 2010, vol. 15, no.2. Retrieved from http://www.arraydev.com/commerce/jibc, November 2012.

[8] Finkle, J. And Henry D. (2013). Target hackers stole encrypted bank PINs. Retrieved online at http://www.reuters.com/article/2013/12/24/us-target-databreach-idUSBRE9BN0L220131224, August 2014.

[9] Fitzergelad, K. (2004). An Investigation into people's perceptions of online banking. Retrieved from http://staffweb.itsligo.ie/staff/eward/ebus%200203/Discussion%20topics/Online%20Banking.ht, March 2011.

[10] Flowerday, S. & Solms, R. V. (2006). Trust an Element of Information Security Security and Privacy in Dynamic Environments. IFIP/SEC2005; Boston: Kluwer Academic Publishers, 87–97.

[11] Gurung, V. (2014). Latest Cyber Crime Reports of India. Retrieved online at http://www.cyberkendra.com/2014/07/latest-cyber-crime-reports-of india.html#.U_aF_8WSySo, July 2014.

[12] Harris, S. (2006). “Information Security Governance Guide”. Retrieved online at www.SearchSecurity.com, June 2013.

[13] Holmquist, E. (2008). "Which Security Governance Framework is The Best Fit?" TechTarget ANZ, Australia. Retrieved online at http://searchcio. techtarget.com. au/articles/24787-Which- securitygovernance- framework-is the-best-fit-.htm, May 2012.

[14] Kalakota, R. and Whinston, A.B. (1997). Elecronic commerce: A manager guide. Addoson Wesley, Reading, MA.

[15] Karimi, S. (2014). 6 Things You Must Do After Hackers Steal Your Credit Card Data. Retrieved online at http://money.usnews.com/money/blogs/my-money/2014/02/19/6-things-you-must-do-after-hackers-steal-your-credit-card-data, August 2014.

[16] Kitten (2014). How to Improve Threat Detection. Retrieved from http://www.bankinfosecurity.com/interviews/banks-how-to-improve-threat-detection-i-2328, August 2014.

[17] Kumar, V. (2014). Cyber snoops hack India's secrets: Report reveals how internet spies may have 'compromised' the nation's security. Retrieved online at http://www.dailymail.co.uk/indiahome/indianews/article-2586442/Cyber-snoops-hack-Indias-secrets-Report-reveals-internet-spies-compromised-nations-security.html#ixzz3B5sPlTfV, June 2014.

[18] Kurt, B .& Tentra, G.M. (2004). "Corporate Information Security Governance in Swiss Private Banking," Master's Thesis University of Zurich.

[19] Lin, C., Varadharajan, V. (2006). Trust enhanced security—a new philosophy for secure collaboration of mobile agents. In: Collaborative computing: networking, applications and worksharing (CollaborateCom'06), Atlanta, pp 1–8.

[20] Malhotra, P. and Singh, B. (2009). Analysis of internet banking offerings and its determinants in India. internet Research, 20 (1), 87-106.

[21] Mukti, N. (2000). Barriers to putting businesses on the internet in Malaysia. The Electronic Journal of Information Systems in Developing Countries, 2(6), 1–6.

[22] NCRB (2013). Cyber crimes. Retrieved from http://ncrb.gov.in/CD-CII2013/Home.asp, May 2014.

[23] Rastogi, R & Von Solms, R. (2006). Information Security Governance a Redefinition. IFIP International Federation for Information Processing, Volume 193/2006, Springer Boston.

[24] Sathye,M.(1999).Adoption of internet banking by Australian customer: An empirical investigation. International Journal of Bank. Vol. 17 (7), 324-334.

[25] Tat, H. H., Nor, K.M., Yang, T.E., Hney, K. J., Ming, L. Y. and Yong, T.L. (2008). Predictors of the intention to continue using Internet banking services: An empirical study of Current users. International Journal of Business Information, Volume 3, No.2.

[26] Tipton H. F. & Krause, M. (ED.) (2004). A Matter of Trust: Information Security Management Handbook fifth Edition. London: AUERBACH PUBLICATIONS

[27] Viega, J. and McGraw, G. (2001) Building secure software. Addison-Wesley, Boston.

[28] White, H. and Nteli, F. (2004). Internet banking in the UK: why are there not more customers? Journal of Financial Services Marketing, 9 (1), 49-56.

[29] Witty, R. J. & Hallawell, A. (2003). "Client Issues for Security Policies and Architecture," Gartner. ID number: K-20-7780.