A Comparative Survey for Evaluating Information Security Risk Assessment Methods

Dr. Edward Wadid Morcos

Assistant Lecturer at Sadat Academy
for Management Sciences
Computer and Information System Department
edward.wadid@sadatacademy.edu.eg

ABSTRACT

Information is a key asset for organizations, and reducing the risk of information compromise is a high priority. There are already many models of risk assessment and more are emerging every day. They all have the same fundamental target, but most attempts to hit the target from very different approaches. Some approaches can be applied to all types of risk; while others are specific to particular risks. There are two common approaches used in risk assessment: a quantitative approach and a qualitative approach. They all have the same fundamental target to estimate the overall value of risk, but most attempts to hit the target from very different approaches. Some approaches can be applied to all types of risk, while others are specific to particular risks. The main purpose of the study is addresses some of the methodologies used currently to analyze information security risks. The main task for an organization is to determine which one to use according to the selecting criteria . Since the organization will spend money on whichever method they choose, it is vital that the chosen methodology meet the requirements. The purpose of the study is to compare and clarify the different model of information security risk assessment and the analysis that effectively addresses the risks of information security.

1. Introduction

Information security has increasingly become an important topic for small and bigorganizations alike. Although awareness and efforts towards security have increased,unfortunately, this increase does not appear to be mitigating the number or cost ofincidents from either internal or external sources. One reason for the problem is that thetechnology is changing faster than what financially-strapped businesses and informationtechnology (IT) departments can handle.

Information security risk management is a recurrent process of identification, assessment and prioritization of risks, where risk could be defined as a possibility that a threat exploits aparticular vulnerability in an asset and causes damage or loss to the asset. Risk management has two primary activities, risk assessment and risk control. Risk assessment is a very important decision mechanism which identifies the information security assets that are vulnerable to threats, calculates the quantitative or qualitative value of risk (or expected loss), and prioritizes risk incidents. In an organization, in the past, a single manager was used to be the responsible sta to protect information systems where, nowadays, a group of managers could take the responsibility of this task or participate in the risk analysis process. As risk analysis becomes a cross-functional decision making process, researchers seek ways to develop new risk analysis methods which allow a group of people to participate.

There is not a single risk evaluation method which is best under all circumstances and for all purposes. Some researchers claimed that neither of the quantitative and qualitative approaches could properly model the assessment process alone. Alternatively, some of them developed comprehensive approaches combining both the quantitative and the qualitative approaches

There are numerous risk assessment models nowa-

days and many more emerging every day.They all have the same basic goal but try to achieve it trough very different perspectives andaddressing problems differently. Some of them can be applied to all kinds of risk, other arespecific for particular risks. A particularly hazardous risk in today's global economy isInformation Security. Information is a critical asset for organizations making information securityrisk very important.

The main information security risk assessment problem is that information security risk isdifferent from traditional risks. Information is one of the most challenging categories of criticalassets for an organization to understand and define. Therefore, identifying information securityrisk can be a quite difficult task, since few organizations have a comprehensive understandingof their information assets, threat vectors and security capabilities.

Additionally, traditional risk assessment does not provide a method to accurately assessinformation security risks facing an ever changing, dynamic environment; it can only provide asnapshot of those risks. Current risk assessment practices were inherited from other fields suchas insurance, medicine and finance but traditional risks are far easier to comprehend thaninformation security risk.

Information security is an organization's approach tomaintaining confidentiality, availability, integrity, nonrepudiation,accountability, authenticity and reliability ofits IT systems. Information security is requiredbecause the technology applied to information createsrisks. Commonly, information might be improperlydisclosed because its confidentiality could be exposed,modified in an inappropriate way because its integritycould be jeopardized, and destroyed or lost because itsavailability could be threatened

Information Security Risk Management ApproachesInformation security risk management methodologiesand analysis approaches available where some of whichare qualitative while others are more quantitative innature. However, these methodologies have a commongoal of estimating the overall risk value.

Information security risk assessment is an on-going process of discovering, correcting and preventing security problems. The risk assessment is an integral part of a risk management process designed to provide appropriate levels of security for information systems. Information security risk assessments are part of sound security practices and are required by the Commonwealth Enterprise Information Security Policy.

The risk assessment will help each organization determine the acceptable level of risk and the resulting security requirements for each system. The organization must then devise, implement and monitor a set of security measures to address the level of identified risk. For a new system the risk assessment is typically conducted at the beginning of the System Development Life Cycle (SDLC). For an existing system, risk assessments may be conducted on a regular basis throughout the SDLC and/or on an ad-hoc basis in response to specific events such as when major modifications are made to the system's environment or in response to a security incident or audit.

2. Motivation and research objectives

Information System Security Risk Assessment (ISSRA) is paramount because it helps companies to adopt cost effective security measures. Indeed, security threats are so numerous that it is impossibleto act on all of them because:

(1) Every technological security solution has a cost,

(2) Companies have limited resources. Hence, companies want to make sure thatthey adopt only positive solutions.

This is done by comparingthe cost of a solution with the risk of not using it, e.g., the cost of a business disruptiondue to a successful security attack. In this sense, ISSRA plays an important role inthe alignment of a company›s business with its IT strategy.

3. Information Security

Federal Standard 1037C (1997) defines information security as: "The protection of information against unauthorized disclosure, transfer, modification, or destruction whether accidental or intentional". Information security is an area in which interest is mounting rapidly. It is becoming widely recognized that security is a fundamental aspect of any information system and warrants high attention beginning with system design and continuing throughout the product lifecycle. Failure to properly address secu-

rity requirements leads not only to operational risks but also to prospects of outright product rejection by customers. Currently, organizations are struggling to understand what the threats to their information assets are and how to obtain the necessary resources to combat these threats.

Acquiring the appropriate human and financial resources to offset the growing threats to information security continues to pose a challenge to many organizations. Information security includes many subjects, from high level principles and policy right down to the very detailed calculations in encryption algorithms.

4. The Nature of Security Threats

One useful model of the information security problem is to define three classes of objects. First, firms have intellectual property that represents value and therefore brings risk of several forms to the firm. Second, that intellectual property is embodied in a technology environment that is imperfect which exhibits design flaws, trade-offs, defects and obscure documentation. Third, there is an individual, inside or outside the firm; who for some reason or another, wishes to exploit those technological or procedural weaknesses with the goal of damaging or transferring the value of that intellectual property. What kinds of individuals might do this? At a high level, there are two traits of some relevance.

5. Information Security Risk

In information security, a risk can be defined as the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information security vulnerability and the resulting impact.

It's quite hard to insert information security risk into one risk category. Most consider it as an information systems risk, but information security implies more than information technology and consequently it goes beyond the range of information systems risk.

Despite implying more than technology, the focus of information security had always been, until recently, on protecting the IT (Information Technology) systems that process and store the vast majority of information, rather than on the information itself. Yet, information security is not synonymous of computer security. Information security is concerned with the confidentiality, integrity and availability of information regardless of the form it may take. Information can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. So technology is only one concern of information security, people and processes are other aspects that have to be taken into consideration.

5.1. Information Security Risk Assessment

Information security risk assessment is the process (part of Risk Management) that identifies and valuates the risks to information security by determining the probability of occurrence and the resulting impact. It identifies threats, classifies assets and rates system vulnerabilities as it provides key information and guidelines to implement effective controls.

6. Information Security Risk Assessment Models

There are several models and methods with different approaches that help in the risk assessment process.

This paper will address some of the methods that support the risk assessment process and those which can be applied to information security. Risk assessment models can be separated into quantitative and qualitative.

6.1. Qualitative Risk Analysis

The qualitative method rates the magnitude of the potential impact of a threat as high, medium, or low. Qualitative methods are the most common measures of the impact of risks. This method allows covered entities to assess all potential impacts, whether they are touchable or untouchable. The qualitative risk analysis methodology uses several elements such as threats, vulnerabilities and controls that are all interconnected.

Risk analysis includes processes such as the identification of activities, threat analysis, vulnerability analysis and guarantees. Risk analysis processes such as BS7799, GMIT, and CSE and explain the procedure to define the modalities for implementation.

There are several methods used for analysis: a matched comparison of dependency diagrams, asset-function assignment tables, and activities. Other models for the design of information security focus on the identification and assessment of the vulner-

ability of the system and the specification of counters to those vulnerabilities [7].

6.2. Quantitative Risk Analysis

This approach uses two basic elements: the probability of an event occurring and the losses that may be incurred.

Quantitative risk analysis uses one number produced from these elements. This is called the Expected Annual Loss (ALE) or Estimated Annual Cost (EAC). This is calculated for an event by simply multiplying by the probability of potential losses. Therefore, in theory, one may rank events in order of risk (ALE) and make decisions based on that risk.

7. Building a Risk Assessment Methodology

When developing their own risk assessment methodology, organizations may consider adapting an industry-standard methodology that is most appropriate for their particular culture and business climate, to ensure their particular risk objectives are met. Figure (1) illustrates typical risk assessment components.

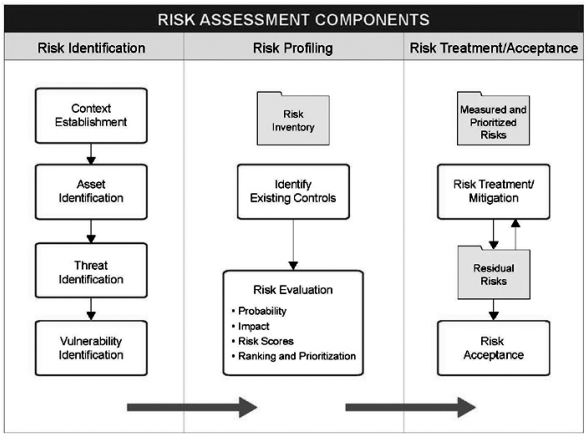

Figure (1) Risk assessment components

1.1. Risk Identification

Before an organization can assess its risks, it should understand its business processes, assets,threats, and vulnerabilities.

• Context Establishment – The risk assessment team needs to understand the internal and external parameters when defining the scope of the risk assessment and/or have access to the persons in the organization who can provide this information.

• Asset identification – Generally, assets could be anything of value to an organization. In the context of PCI DSS, assets include the people, processes, and technologies that are involved in the processing, storage, transmission, and protection of CHD.

• Threat identification – Threats may include people, the systems they use, and conditions that could cause harm to an organization. Talking to staff across all areas of an organization will help the risk assessor understand where they see the potential for threats to emerge.

• Vulnerability identification – vulnerability is a weakness that can be exploited by a threat and may originate from technology, the organization, the environment, or a business process. In a risk assessment, all vulnerabilities should be considered. For example, vulnerabilities can occur as a result of design, development, and/or deployment deficiencies of systems or software. Organizational and business-process vulnerabilities may exist because of non-existent or ineffective policies and procedures.

1.2. Risk Profiling

Risk profiling is the presentation of all risks to an asset, together with threats and vulnerabilitiesand their respective risk scores. Risk profiling enables asset owners to evaluate risks and takenecessary risk-mitigation measures.

Risk profiling generally includes the following:

• Existing controls

• Existing controls are those that are already present in an organization to protect against the identified threats and vulnerabilities. The identification of existing controls is necessary to determine their adequacy. The effectiveness of existing controls can be identified by reviewing existing policies/procedures, interviewing people, observing processes, and reviewing previous audit reports and incident logs.

• Risk evaluation

• Risk evaluation allows an organization to determine the significance of risks in order to prioritize mitigation efforts. This helps organizations achieve the optimum usage of resources. Risk-measurement techniques used during the evaluation process can be quantitative, qualitative, or a combination of both:

• Quantitative risk assessment – A quantitative risk

assessment assigns numerical values to elements of the risk assessment (usually in monetary terms). This is accomplished by incorporating historical data, financial valuation of assets, and industry trends.

• Quantitative risk assessments can be regarded as more objective than qualitative risk assessments as they are based on statistical information. However, performing a purely quantitative assessment is often difficult since it may be difficult to determine a monetary value for some assets, such as an organization's "reputation."

• Qualitative risk assessment – Qualitative risk assessments categorize risk parameters according to the level of intensity or impact to an asset. The categorization of risk parameters is accomplished by evaluating the risk components using expert judgment, experience, and situational awareness. The scales are typically based on an escalating set of values—for example, low, moderate, and high.

		Consequence		
		Minor Impact	***Moderate Impact***	***Major Impact***
Likelihood	***Very likely***	Medium Risk	High Risk	High Risk
	Likely	Medium Risk	Medium Risk	High Risk
	Possible	Low Risk	Medium Risk	High Risk
	Unlikely	Low Risk	Low Risk	Medium Risk

Figure (۲)Example of a risk calculation matrix

Many organizations perform risk assessments using a combination of quantitative and qualitative methods.

1.1. Risk Treatment

Once risks have been identified and measured, it is important to define risk treatment strategies.

Because the elimination of all risk is usually impractical or close to impossible, it is important toimplement the most appropriate controls to decrease risk to an acceptable level. Risk treatmentstrategies include:

• Risk reduction - Taking the mitigation steps necessary to reduce the overall risk to an asset. Often this will include selecting countermeasures that will either reduce the likelihood of occurrence or reduce the severity of loss, or achieve both objectives at the same time. Countermeasures can include technical or operational controls or changes to the physical environment.

• Risk sharing/transference2 - The organization shares its risk with third parties through insurance and/or service providers. Insurance is a post-event compensatory mechanism used to reduce the burden of loss if the event were to occur. Transference is the shifting of risk from one party to another.

• Risk avoidance - The practice of eliminating the risk by withdrawing from or not becoming involved in the activity that allows the risk to be realized. For example, an organization decides to discontinue a business process in order to avoid a situation that exposes the organization to risk.

• Risk acceptance - An organization decides to accept a particular risk because it falls within its risk-tolerance parameters and therefore agrees to accept the cost when it occurs. Risk acceptance is a viable strategy where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are accepted by default.

1. Comparing Information Security Risk Analysis Methodologies

As stated earlier there are two fundamental types of risk assessment. Quantitative risk analysis applies mathematical and statistical tools to represent risk. Qualitative risk analysis methods perform risk analysis with the help of adjectives, not mathematics.

1.1. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation SM)

OCTAVE is asuite of tools, techniques, and methods for risk-based information security strategicassessment and planning. The OCTAVE method lists eight processes for a formal riskassessment. It leverages people's knowledge of their organization's security-relatedpractices and processes to capture the current state of security within the organization.

Risks to the most critical assets are used to prioritize areas of improvement and set thesecurity strategy for the organization. OCTAVE resources provide a useful source forguidance.

OCTAVE was developed at the CERT Coordination Center by Carnegie Mellon Software Engineering Institute. It is a technique for performing risk analysis. It considers both technological and organizational issues. Octave looks at the daily usage of organization's computing infrastructure [14]. This approach focuses on activities, threats, and vulnerabilities. One of the main concepts of OCTAVE is self-direction. This means that people within the organization must practice information security risk assessment.

The OCTAVE methodology uses an Expected Value Matrix to determine a risk's expected value. The impact values and probability values are subjective and are then applied mostly to the Expected Value Matrix to get an overall value. The main formula is:

Loss = Impact/consequence x Probability

OCTAVE implements no mathematical computations and thus it catches a value of 3 for simplicity and a value of 1 for precision. If an organization is concerned with simplicity rather than accuracy, OCTAVE is a good fit [5].

1.2. CORAS

CORAS was developed using information society technologies (IST). One of the main objectives of CORAS is to develop a structure that uses the methods of risk analysis, semi-formal methods for object-oriented modeling, and computer tools for an accurate and unambiguous assessment of risk, and efficient critical safety systems [14]. The methodology is based on Unified Modeling Language (UML), a language that uses diagrams to illustrate relationships and dependencies between users and the environment in which they work. The framework has four main pillars, of which risk management is one. In CORAS, the decisions made can be based on UML class diagrams of each asset [17, 18, 25,].

Loss = Impact x Probability

CORAS applies no mathematical computations, consequently it obtains a value of 3 for simplicity and a value of 1 for precision. The CORAS method also employs the impact and probability method .

1.3. CRAMM (CCTA Risk Analysis and Management Methodology)

The CCTA Risk Analysis and Management Method (CRAMM) is a qualitative risk analysis and management tool developed by the UK Government Central Computer and Telecommunications Agency in 1985 to provide government departments with a method for revisions to the security of information systems. CRAMM can be used for all types of organizations.

CRAMM has been accepted as the governmental standard for risk analysis and management. The process of risk management according to this methodology consists of three stages; asset identification and valuation wherein the goal is to identify and value assets, threat and vulnerability assessment in order to assess the CIA risks to assets and countermeasure selection and recommendation which identifies the changes required to manage the CIA risks identified.

This methodology uses dedicated software as an integral element supporting the three stages. The concepts of CRAMM applied via formal methods ensure consistent identification of risks and countermeasures, and provides cost justification for the countermeasures proposed .

Demonstrating acquiescence with BS7799 (British standard for information management) during a certification process. It can also be regarded as a benchmark for organizational risk and emergency management considering input from a number of public and private sector experts in the security instrument.

The crucial essentials of data collection, analysis and output results that should be present in a programmed risk analysis tool are covered in the three stages of a CRAMM review:

• Recognizing and valuing assets.

• Recognizing threats and vulnerabilities, computing risks.

• Recognizing and prioritizing countermeasures.

CRAMM computes risk for each group of assets versus the threats to which it is vulnerable on a scale of 1 to 7 utilizing a risk matrix with the default values by comparing it with the activity level of threat and vulnerability. On this scale, 1 implies a fundamental requirement of safety and 7 shows a very high safety requirement [28].

1.4. ISRAM

ISRAM was improved in December 2003 at the CNR Institute of Electronics and Cryptology and Gebze Institute of Technology in Turkey. It was marketed as a quantitative approach to risk analysis, which allows the participation of the Director and staff of the organization. ISRAM is poll-based model. Two separate and independent investigations are established for the two attributes of risk, whose names are probability and consequence. ISRAM does not implement techniques such as single occurrence losses (SOL) or annual loss expectancy (ALE). However, the risk factor is a number between 1 and 25. This numerical value keeps in touch with a high, average or low qualitative assessment, and this quality value is based on risk management decisions. The ISRAM methodology has seven steps [6].

1.5. CORA

International Security Technology, Inc. (ICT) has developed Cora, a system for estimating and analyzing the cost of risk. Cora risks using data collected on the threat, functions, and assets, and weaknesses of the functions and assets to the threats to calculate the consequences. That is, the losses due to incidents of threats. It is a method in which the parameters specified in quantitative risks and where the loss is expressed in terms of quantitative finance. Cora uses a two-step process to support risk management. The parameters of the threat, the functions and assets, are verified and refined until the best values are determined. Cora then calculates SOL and ALE for each identified threat. The total losses to the organization are evaluated for each threat, and then this value is multiplied by the frequency of threats. [30].

CORA employs the following:

ALE = Consequence x Frequency

where the result equals Sn(individual SOLs) n the number of SOLs, and SOL = loss potential (worst case monetary value) x vulnerability. Cora utilizes some mathematical computations, but they are not extensive. It earns a value of 2 for both simplicity and accuracy.

1.6. IS Risk Analysis Based on a Business Model

Based on a business model, IS Risk Analysis has been developed at the Korea Advanced Institute of Science and Technology (KAIST) in 2002. They developed this model owing to some limitations of traditional risk analysis methodologies. An asset's value is taken by this model and then not only supports the analysis on its replacement cost, but also its tangible asset's value from the viewpoint of the operational continuity measured. The methodology is comprised of four stages. By this method, the significance of various business functions of the business model and the necessity of various IS assets are determined. Mathematical formulae are applied to compute ALE for a single threat occurrence of the organization. The end result is a quantitative monetary value [7].

A Framework forthe Comparison of Risk Analysis Methodologies

CRITERIA	QUALITATIVE			QUANTITATIVE		
	OCTAVE	CORAS	CRAMM	ISRAM	CORA	IS
Method/Tools	Method/Tools	Tools	Method/Tools	Method/Tools	Tools	Method/Tools
Method/Tool Name	OCTAVEv2.0 OCTAVE – S v1.0	CORAS Editor v.1.1	CCTA Risk Analysis and Management Method	ISRAM	CORA 5.0	IS Risk Analysis based on a Business Model
Vendor Name	Carnegie Mellon University, SEI(Software Engineering Institute)	European Commission	Insight Consulting	National Research Institute of Electronics and Cryptology and the Gebze Institute of Technology	International Security Technology, Inc.	Korea Advanced Institute of science and Technology
Country of Origin	USA	Intracom(Greece) Solinet(Germany) Telenor(Norway)	United Kingdom	Turkey	New York	Seoul, Korea
Date of First Release	Version 0.9 1999	January 2001	1985	December 2003	1978	2002
Languages	English	English	English, Dutch, Czech	English	English	English
Price	Free	Free	Unknown	Free	$ 7000-$85000	Free
Compliance to IT Standards	N/A	ISO 31000 ISO/IEC17799 AS/NZS 4360	ISO/IEC17799	NIST SP 800-30 ISO/IEC17799 ISO/IEC13335	N/A	N/a
Skills Needed	Standard	Standard	Specialist	Standard	Standard	Standard
Availability	Trial version available, registration required	Trial version available, registration required	Registration required	Open	Licensing organization without limit	Open
Tools Supporting the Method	Commercial Tools - Licensed materials - Trainings	An XML Mark-up for exchange of risk assessment data -A UML based specification language targeting security risk assessment	Commercial Tools -CRAMM Expert (Insight) -CRAMM Express(Insight)	Key Risk Management Tools for Information	N/A	N/A

Table 1 Comparison of Risk Analysis Methodologies

1. Critical success factors for information security risk assessment

• Identification

The correct identification of assets plays an important role in the risk assessment process. Therefore, organizations should gather input from all stakeholders (such as Human Resources, Information Security, business departments, etc.) that are involved in the processing, storage, and transmission of CHD.

To properly identify threats and vulnerabilities, assessors should have an open mind and factor inthe various conditions that could negatively impact the CDE. Historical events, audit reports, andsecurity incidents (within the organization or industry) can also provide additional insight.

• Proactive approach

The risk assessment process should be proactive instead of reactive. Thiswill allow the organization to proactively identify, analyze, and document their risks. Taking aproactive approach helps organizations avoid costly corrective measures. Therefore, there is aneed for the continuous monitoring of risks throughout the year.

• Keeping it simple

The risk assessment process can be kept simple by developing amethodology that best suits the needs of an organization. Published industry-standardmethodologies may assist in this process.

Measurement scales should be limited to a small number of categories. Inclusion of numerouscategories will often introduce unnecessary complexity and reduce the likelihood that riskstakeholders will understand the results. Each value on a measurement scale should be explicitlydefined. Without clear definitions, stakeholders will often form differing opinions on the data. Oncethe measurements are defined, they should be validated by the individuals who participated in therisk assessment process to ensure that the results are interpreted consistently across theorganization.

• Training

It is also suggested that risk assessors are trained on formal risk assessmentprocesses to ensure they are better prepared to understand the threats and vulnerabilities thatcould negatively impact the security of cardholder data, and ultimately their organization.

2. Conclusion

Information security is an ongoing process to manage risks. One could say that risk management is essentially a decision making process. The risk assessment stage is the collection of information that is input into the decision. The risk mitigation stage is the actual decision making and imple-

mentation of the resulting strategy. The effectiveness evaluation is the continual feedback into the decision making.

There are numerous risk assessment methodologies available today, some qualitative and others more quantitative, and a major task for an organization is to determine which one to use. Since the organization will spend money on its risk analysis methodology, it is critical that a methodology be selected that will meet its needs. The best way to choose between methodologies is to compare them, using objective, quantifiable criteria. This is where a framework for comparison is needed. If the criteria that are used are applicable to all risk analysis methodologies, the organization can compare different methodologies objectively, and decide on the best one.

This paper covers some of the methodologies currently available to assess information security risks. This is done in order to investigate the criteria that can be used when selecting methodologies.

References:

1. Kiran Kumar Kommineni, Adimulam Yesu Babu , An Approach for the Assessment of the Information Security and Its Measures, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013 .

2. Anita and Les Labuschagne, A Framework Comparing Information Security Risk Analysis Methodology, 2005.

3. Nik Zulkarnaen Khidzir, Azlinah Mohamed, Noor Habibah Hj Arshad, Information Security Risk Management ,An Empirical Study on the Difficulties and Practices in ICT Outsourcing, Second International Conference on Network Applications, Protocols and Services,2010.

4. A Qualitative Risk Analysis and Management Tool - CRAMM: http://www.sans.org/reading_room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm_83

5. Neeta Shukla, Sachin Kumar, A Comparative Study on Information Security Risk Analysis Practices, Special Issue of International Journal of Computer Applications (0975 - 8887) on Issues and Challenges in Networking, Intelligence and Computing Technologies - ICNICT 2012, November 2012.

6. Information Supplement • PCI DSS Risk Assessment Guidelines • November 2012.

Global ICT Trends Emerging in 2013

Smart handheld devices are red hot.

Early in January each year, the Las Vegas Consumer Electronics Show (CES) is not just the world's largest consumer electronics exhibition: it's a strategic battleground for ICT heavyweights. Moreover, many regard CES as a leading indicator of electronics industry trends. After participating in CES, ITRI has identified 10 new trends in the global ICT industry.

In 2013, the tablet business is likely to continue strong growth.

Big Data Drives Cloud Opportunities

In recent years, an increasing number of enterprises have used big data as a basis for business intelligence analysis, and they plan to build intelligent systems frameworks through cloud computing. Chung predicts that in the next 10 years, this strategy will extend to manufacturing, health care, telecommunications, retail, energy, transportation, automotive, security and other industries, creating considerable opportunities.

It is worth mentioning that as companies have begun to actively develop emerging cloud applications and provide customers cloud services, business opportunities look attractive for the optimization of business processes and creation of large data centers.

In 2013, the tablet business is likely to continue strong growth with global shipments expected to reach 200 million units and an annual increase of approximately 38%. ITRI estimates that tablet's promotional activities to provide customers real-time spreadsheets, documents, and other business applications will reach an annual growth rate of approximately 46%. The tablet's supply of shopping, logistics, education, social media, entertainment, health counseling, and other service-oriented applications will achieve an even more dazzling growth rate of as much as 52%. These two segments will be major forces pulling the tablet business forward.