A Novel Approach to Design Quantitative Method for ICT Security Assessment

Eng. Wassim Ahmad[*]

Prof. Dr. Ghassan Fallouh[**] **Prof. Dr. Norbik Bashah Idris**[***]

Abstract

The intent of this paper is to present a novel quantitative equation to assess information security level for enterprises, establishments and corporate generally, and financial institutions specifically in public and private sectors in Syria. This method is the result of statistical study[1] which has been applied to a set of financial institutions in Syria as a sample of study to assess the gap between existing information security level and ISO 27K directives for Information and Communication Technology (ICT) security, benefiting from other international approaches and models designed for this purpose.

This study aims to highlight the special requirements and the modified framework required to develop ICT security in financial institutions taking into consideration the culture and the special conditions in Syria; Statistics and surveys were applied during four years (2006-2010) on four main Syrian financial institutions including two important Banks.

Keywords: Information security- Computer network

[*] PhD Student, Department of Computer Engineering and Automation, Faculty of Electrical and Mechanical engineering, Damascus University, Syria.

[**] Department of Computer Engineering and Automation, Faculty of Mechanical and Electrical Engineering, Damascus University, Syria.

[***] Centre for Advanced Software Engineering, University Technology Malaysia, Kuala-Lampur, Malaysia.

1. Introduction and motivations

"*When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind: it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to a stage of science.*" (Thomson, 1894).

Information technology is not limited to a group of people or a group of companies only; it is applied in all sectors of life that is why ICT (Information and Communication Technology) information security becomes increasingly important.

While some ideas for quantifiable ICT security measurements have been suggested recently (Bond[2], 2004), they are far from the unambiguous framework and definitions sought especially in Syria. The ambition of this work is to bring the research in the field closer to that goal especially in financial institutions in Syria which have the highest concerns about ICT security.

Simply, this research is going to find answers to the following questions:

- How can ICT security level be measured or evaluated?
- What is the best way to modify international prototype to fit Syrian financial institutions requirements?
- How can we produce a quantitative equation representing the real situation and the gap between this situation and ISO 27K[3]?
- What are the difficulties and restrictions preventing financial institutions from improving their information security level and reaching internationally acceptable level by applying international quantitative approaches?

2. Theoretical analysis

There are many definitions for ICT security, we can define it as: "*a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable*" (ECCouncil, 2006).

ISO 27K defines it as "*the preservation of Confidentiality, Integrity, and Availability. In addition other prosperities such as Authenticity, Accountability, Non-repudiation, and Reliability can be involved*".

Reaching a secure environment in which companies can operate and provide services is the main goal for everyone since we are in the Internet and electronic services era. Therefore all governments and research centers have been developing rules, regulations, guides, policies and controls to support their companies and organizations to achieve that goal.

ISO 27K is an example of the result of that effort which helps facilitating and controlling the management of ICT security system.

National Institute of Standards and Technology NIST has well defined the benefit of measuring ICT security level in public and private sector (Performance Measurement Guide for Information Security, NIST Special Publication 800-55) which includes:

- **Increase Accountability:** Information security measures can increase accountability for information security by helping to identify specific security controls that are implemented incorrectly.
- **Improve Information Security Effectiveness:** An information security measurement program will enable organizations to quantify improvements in securing information systems and demonstrate quantifiable progress in accomplishing agency strategic goals and objectives.
- **Demonstrate Compliance:**
- Organizations can demonstrate compliance with applicable laws, rules,

[2] Andres Bond has suggested a quantitative model with an output [0-1], which represents a framework for evaluating security for software working as Distributed Information System. We benefitted from it in the way he built the equation.

[3] A family of Information Security Management System (ISMS) International Standards is being developed within ISO/IEC. The family includes International Standards on information security management system requirements, risk management, metrics and measurement, and implementation guidance. This family will adopt a numbering scheme using the series of numbers 27000 et seq.

and regulations by implementing and maintaining an information security measurement program.

- **Provide Quantifiable Inputs for Resource Allocation Decisions:** Fiscal constraints and market conditions compel government and industry to operate on reduced budgets.

On the other hand neither NIST nor other institutions of research and standards has placed a quantitative method to measure ICT security level, in simple words, NIST has defined the importance of the target without showing how institutions can reach this target.

Table 1 explains briefly some researches that have been conducted for measuring security and their limitations.

Research	Brief	Limitations
Scarfone,2008	It is one of the main models which was placed to assess ICT security level in institutions	No cultural factors were taken in consideration, moreover, it keeps the door open to modify the parameters of the resulted model to conclude quantitative model
Murdoch,2005	Measurement model of ICT security (without concluding any quantitative equation)	No resulted equation was concluded, only a measurement model (measures do not comply with conditions and culture in Syria)
Sadimies,2004	Quantitative model to measure ICT security level according to few directives of ISO 27K	Limited to few directives of ICT security, and it was applied in Finland
Bond,2004	Quantitative model to measure ICT security level for Distributed Information Systems	Evaluating only software working as Distributed Information System.
NIST Papers	They covered the necessity of using quantitative method to measure ICT security level	No equation or definite model was included in these papers

TABLE 1: Some Researches and their Limitations

3. Statistical Study and Research Steps

In Syria, measuring ICT security level (including ISO 27K compliance measurement) through applying international researches or standards like: (Scarfone, 2008), (Gutierrez, 2008), (Sadimies, 2004), (Bond, 2004), and (NIST papers) is not an easy task due to the following reasons (Concluded from multiple surveys and questionnaires we have done to a number of financial institutions and IT staff in Syria, and accepted for publication as research paper titled "*Gap analysis between ISO 27K standards and current situation of Information Security in financial institutions in Syria* " submitted to Tishreen University:

1. There are no laws or regulations to govern and control electronic services till now, for example: digital documents – even with digital signature- is not accepted as valid documents in courts.
2. The lack of qualified local staff in the field of information security.
3. Decision makers may face difficulties to understand the necessity of equipments, services, and procedures which are recommended by ICT security experts.
4. The culture factor, where the leader controls the law, not the law is the one which controls the leader; That means both of General Manager and IT managers must be aware of the importance and the necessity of ICT security in their organizations to be able to apply ICT security standards according to their understanding and approach not to the standards and regulations.
5. The lack of good training and awareness programmes related to information security in both public and private sectors.
6. The fact that more than 65% of employees in IT staff are females[4], and 90% of them lost their well and ability

[4] This percentage was concluded from our survey which we applied to a number of IT staff (Appendix 2).

to learn and develop their knowledge after having children[5]. Although if they are not married, it is not possible for them to work in evening or night shifts, because of traditions and local culture; in our research we asked for the ability to work in special conditions like outside the staff's own city, or travel for training outside the country, we found that most of female IT staff find that difficult or not possible. Appendix 2 shows a sample of the survey done for IT employees.

7. The average salaries of government organizations are very low, which results in losing the young and qualified employees who move to work in foreign countries or even in the private sector.
8. The complexity of the existing guides –like ISO 27K – to be understood and applied by IT staff where 80% of them are not aware of security requirements, according to our survey.

For those reasons in addition to the necessity of assessing information security level of companies in Syria, this research was launched by studying the conditions of four main financial institutions[6] including the largest bank which is The Commercial Bank of Syria as it has 100 branches, over 5000 employees, and more than 70% of market share in Syria[7].

This research was developed by following these steps:

1. Statistical study (survey) of the current security status of these four financial institutions through formal questionnaire forwarded to IT managers in these institutions taking both ISO 27001and ISO 27002 directives in consideration (Appendix 1 shows samples of the survey).
2. Analysing the results obtained from the four institutions, focusing on the gap between current situation and required standards.
3. Weighting each directive and control of ISO 27K according to their importance in the current environment.
4. Developing an equation reflects the real situation of the ICT security level of the financial institutions in Syria.
5. Developing an automated system that can be easily used by IT managers, security offices, and auditors to automatically evaluate the institution ICT security level in those institutions.
6. Implementing the resulted equation on one of financial institutions in Syria (the bank was not included in our set of survey samples)

3.1 Weighting ISO 27001-27002 directives and controls

Based on statistics and surveys which have been applied to our set of samples, we managed to approximate the weight of each ICT security control and directive according to its importance and to which limit it may affect the ICT security level in these institutions, for this goal we followed below mentioned methodology:

1. Combining the two domains of ISO 27001, with the 11 domains of ISO 27002, as shown in Table 2 :

	Domain
ISO 27001 ISO 27002	1-ISMS (information Security Management System)
	2-Risk Assessment
	3-Security Policy
	4-Organization of Information Security
	5-Asset Management
	6-Human resources security
	7-Physical and Environmental security
	8-Communication and Operations Management
	9-Access Control
	10-Information system acquisition, development and maintenance
	11-Information security incident management
	12-Business Continuity Management
	13-Compliance

TABLE 2 Combining ISO 27001, 27002

[5] In our Arabic culture, we give a special priority to family in which the female is the most important player. Therefore female duties in their houses are much more than the male role which may affect their job capabilities, this result obtained from the survey.

[6] Institutions names are not mentioned according to their request.

[7] Source: Commercial Bank of Syria web site: http://cbs-bank.sy. Arabic version, Page: about CBS.

The resulted 13 domains can build comprehensive approach to ICT security.

2. Weighting each directive and control from these 13 domains according to the following:
    a) Its importance in the whole security environment.
    b) Ability to apply it. For example the control "there is a senior management forum to discuss ISM policies, risks and issues" (domain: information security policy), cannot be applied, simply because senior managers do not have time for this task, according to the survey.
    c) The existence of the service related to the control.
3. Concluding linear equation which gives the final score of ICT security level, taking in consideration that we chose a linear format for simplicity and we considered reformatting this equation using non-linear format as future work.
4. the final score will be compared to five levels of security status, which is produced automatically by the program. Table 3 shows the resulted security level and the equivalent score.

Security Level	Score
POOR	UP TO 40
LOW	40-60
MEDIUM	60-80
HIGH	80-90
FULL	90-100

TABLE 3: Security Levels and Scores

5. The output of the program will include in-depth gap analysis between the current status of the target of evaluation, and ISO 27K, along with recommendations to correct the situation, **section 5.1** displays a sample of the output .

4. Designing and Implementing

Here we need to have a detailed version of a prototype model to assess security level in Syrian financial institutions according to ISO 27K, taking in consideration that the design must be presented in details benefiting from all presented models and prototypes.

In this part, we are going to conclude and place a design for ICT assessment of ISO 27K compliance, so we can assess its directives weight in the resulting equation.

Expected results, limitations, and theoretical analysis must be presented in this part.

Finally automatic measurements of data will be developed as program which gives as an output the final equation and automatic analysis of the measures obtained.

4.1 Measurements and the equation

The following factors have been considered during development and implementation of this information security measurement research that yields the quantitative equation:

- Measures must yield quantifiable information (percentages, averages, and numbers).
- Data that support the measures need to be readily obtainable.
- Only information security processes which might be applied to all financial institutions should be considered for measurement.
- Measures must be useful for tracking performance and directing resources.
- Rules and regulations in Syria related to information security especially for financial institutions should be taken into consideration.
- Country culture, social barriers, traditions, and realistic approaches to reach a secure environment for financial institutions to operate are also considered in these measurements.

4.2 Weighting controls and domains and the resulting equation

We follow below the proposed method:

1. Each control is assigned a specific weight (integer value).

2. The summation of each domain controls values will result in the domain value, which is 100 points as maximum.
3. Each domain can be powered to a positive integer number and/or multiplied by positive integer value; according to its importance.
4. Appendix 1 displays samples of the survey conducted, and weighting of controls.
5. The final equation will be of the form:

$$L = \frac{1}{m}\sum_{i=1}^{n} \alpha_i . V_i^{\beta_i}$$

Where:

- L : The final level of the organization security, which is an integer value from 1 to 100.
- n : The number of domains.
- Vi : The domain final value, which is the summation of all its control's value, V_i is from 1 to 100.
- α_i : Factors multiplied to each domain final value according to its importance[8].
- β_i : (for future development) The power of V_i according to domain importance, in case the linear α_i values do not reflect the domain importance- β_i could be 1,2,3…
- m : The sum of α_i . In order to have a final value of L out of 100, we need to divide the summation by m. m is related to how we decide to allocate controls –for example 13 domains, each is out of 100-, and the value of β_i and α_i .

4.3 Assumptions

For the sake of this paper and to reduce complexity, we will follow the following assumptions:

1. We will consider . β_i Could be for future development.
2. n = 13, the number of domains.
3. $\alpha_i = \sum_{i=1}^{13} \alpha_i$, where α_i is the values of α_i are the average values collected from the survey. Table 4 shows the average values of α_i and calculation of m.

I	Domain	α_i
1	ISMS (information Security Management System)	2
2	Risk Assessment	1
3	Security Policy	2
4	Organization of Information Security	2
5	Asset Management	2
6	Human resources security	5
7	Physical and Environmental security	4
8	Communication and Operations Management	2
9	Access Control	4
10	Information system acquisition, development and maintenance	3
11	Information security incident management	3
12	Business Continuity Management	2
13	Compliance	3

TABLE 4: Calculation of m

m = 35.

4. Important Note: all variables in the equation, the number of domains, controls in each domain, and weights can be modified automatically by the program developed for this purpose.
5. The equation will be of the form:

$$L = \frac{1}{35}\sum_{i=1}^{13} \alpha_i . V_i$$

[8] Some domains are more important than others, and this is related to IT manager perspective, company policies, and services provided. For example some companies need Physical Security much more than Risk Assessment.

5. Experimental results and discussion

Here we are going to apply our equation which has been automated as a program on a bank in Syria as a sample of Syrian financial institution and measure the level of Security in this bank, then we applied our survey and experts' measure to check and see how much our model is close to the right results.

The results of applying our quantitative method, were assembled in detailed report and submitted to this bank, this report consists of more than 40 pages, and as it is impossible to include the results in our research paper, we are going to spot a light on main weaknesses and ICT security limitations in the bank, in addition to the level of ICT security in the bank based on our quantitative model.

5.1 Sample of the study for Security Policy domain[9]

Table 5 and 6 shows a sample of the output of applying part of one domain - Security Policy - on the target institution (here it was a Bank).

Information Security Policy

Information security policy	Yes	No	Comments
Are the policies communicated, understood and accepted? • Standards for physical security of the computer and telecommunications installation and associated facilities; • HR procedures governing access to and use of IT services (usernames and passwords, disciplinary procedures); • End user guidelines covering PC software licensing and virus prevention, etc?	☒ ☒	☒	Needs to review
Are they reasonable and workable?	☒		
Do they incorporate suitable and sufficient controls?	☒		Partially
Do they cover all essential computing and telecommunication services?		☒	Only applied on technical level

TABLE 5: Sample of Applying the proposed equation on Information Security Policy

Technical Security Policy

Technical Security Policies	Yes	No	Comments
Is a technical security policy in place?	☒		
Are unused services disabled?		☒	
Are unused interfaces disabled?		☒	
Do any applications use telnet to perform management activities such as backing up configuration?	☒		
Do passwords appear in encrypted form wherever they viewed or appeared?	☒		
Do the passwords meet with the required complexity as defined by the policy?		☒	
According to policy, Is there any enforcement to change passwords regularly?	☒		
Is authentication done through: Locally configured usernames and passwords TACACS+/ RADUIS/ Database server	☒		
Is there a documented procedure for creation of users?		☒	
Does each administrator have a unique account for himself/herself?		☒	
Is there a login and logout tracking/command history?		☒	
Are all user accounts assigned the lowest privilege level that allows them to perform their duties? (Principle of Least Privilege)	☒		
Are the default settings changed in all systems and equipments?	☒		
Is the NTP (Network Time Protocol) server service used to synchronize the clocks of all equipments?	☒		
Is configurations backed up done regularly?	☒		
Is the backup moved to an off-site/DR(Data Recovery) site?	☒		
On the system where the configuration files are stored, is the local operating system's security mechanisms used for restricting access to the files (i.e., the machine should be password enabled and prevent unauthorized individuals from accessing the machine.)?		☒	
Is the TFTP protocol used to transfer network configuration or image files? If yes, Is the TFTP process restricted to certain addresses only? Is the TFTP service disabled when not in use?	☒		Yes to all
Is there a documented procedure for backup of configuration files?	☒		
Are all changes and updates documented in a manner suitable for review according to a change management procedure?	☒		
Is there a redundant machine in cold standby or hot standby?	☒		

[9] This sample is part of a large research paper submitted to Tishreen University Journal for Research and Scientific Studies, Syria. Acceptance letter No. 230, Date 20 Feb. 2011.

Are disaster recovery procedures for the network documented and are they tested?	☒		
Are all attempts to any port, protocol, or service that is denied logged?		☒	
Are all CPUs /memories / storages monitored?		☒	
Is there a special logging server enabled and login restricted?	☒		
Are procedures for audit log review generated by different systems and machines documented and followed?		☒	
Are all logs (covering administrator access /access control) reviewed?		☒	
Are reports and analyses carried out based on system and log messages?		☒	
Is there any course of action to be followed if any malicious incident is noticed?		☒	
Are the network/ system /applications /services engineers aware of the latest vulnerabilities that could affect their domain of proficiency?		☒	

TABLE 6: Sample of Applying the proposed equation on Technical Security Policy

5.1.1 Gap Analysis

After collecting the information from Table 4 and 5, we will analyse the data obtained:

As long as Information Security Policy is not reflected on the bank strategy and business objectives, despite of general unawareness of necessity to be fully understood by staff, it makes policies too hard to be followed or applied.

The gap can be divided into four critical missing processes as below:

- Follow up process;
- Review process;
- Corrective actions; and
- Tracking /over sighting process.

5.1.2 Code of Practice[10]

Here and for the purpose of Security Policy as an example, we specify according to ISO 27K how practically we can close the gap found.

Objective

Information Security Policy (ISP) should provide management directions and support for data protection, in accordance with the norms of professional ethics, business requirements and all relevant laws, regulations and private certificatory requirements.

Scope

ISP, taken as a whole, should provide clear controls for all data collected, used or stored in the bank's data processing, communications, and storage systems, as well as for data collected, used or stored in the systems of external parties under contract with the organization.

Approval

ISP should be formally approved by appropriate organizational authorities.

Documentation

ISP should be fully documented in designated organizational document repositories. Policy documentation could include:

- overall objectives and scope, including statements of management intent, supporting goals and principles;
- listing of identified authorities (statutory, regulatory, private) and requirements that condition or control data protection activities, including an explanation or listing of policies, principles, standards and compliance requirements relevant to the organization;
- framework for setting policy objectives and components of the policies themselves, including a structure for risk assessment and risk management;
- definitions of general and specific responsibilities for the organization's data security management;
- references to additional documentation that supports or underpins the policies; and
- formal historical record of material changes to the policies and any accompanying approvals.

Communication, training and awareness

ISP should be communicated to all relevant affiliates of an organization, as well as relevant external parties, via an appropriate training and awareness program.

Periodic review

[10] SOURCES: ISO-27001/27002:2005, sects. 5.1.1 – 5.1.2.

ISP should be reviewed at planned intervals, and when significant changes in the external environment occur, to ensure their continued suitability, adequacy and effectiveness. Review steps could include:

- solicitation and integration of feedback from all interested parties inside and outside the organization;
- independent contracted external reviews;
- checklists of recommendations and requirements of relevant authorities;
- consideration of trends in threat types and threat capabilities, system vulnerabilities, and available technologies for counter-measures and mitigation;
- consideration of trends in compliance requirements of domestic and private certificatory authorities;
- consideration of trends in and anticipated changes to the organizational environment, business circumstances, and resource availability;
- historical data on information security incidents at the organization itself and at peer institutions; and
- Formal historical record of the reviews undertaken as part of policy development and refinement, and their outcomes.

Coordination with other policies

Review of ISP should include consideration of other relevant organizational policies, to minimize inconsistencies and gaps. This could include:

- identification of all other relevant policies; and
- Inclusion of the representatives from the areas responsible for such policies in the periodic review of information security policy.

5.2 Evaluation of the Equation

In order to verify and evaluate the proposed equation, we need another party feedback, and compare it with the proposed equation results. After applying our model, we have submitted our report to the technical department of the bank –subject to the research –, and we asked about their feedback and evaluation of each directive regardless of our report. Then we compared our report with their report for each directive in the 13 domains, and present the final results as percentage between our proposed measurement compared to their evaluation, and we have the following results which reflect accuracy of our quantitative method.

Table 7 shows the Acceptance Results.

Domain	Bank feedback (%)
ISMS (information Security Management System)	85
Risk Assessment	90
Security Policy	83
Organization of Information Security	88
Asset Management	82
Human resources security	91
Physical and Environmental security	95
Communication and Operations Management	80
Access Control	87
Information system acquisition, development and maintenance	83
Information security incident management	88
Business Continuity Management	89
Compliance	90
Average Acceptance	87%

TABLE 7: Acceptance Results

The result shows that the Bank IT experts agree upon 87% with the results given by our equation.

This means that our equation can be considered as acceptable method for measuring ICT security level of financial institutions in Syria.

6. Conclusion

The few quantitative methods which were developed by international institutions and researchers to measure the level of ICT security in organizations, establishments, companies...etc

are limited to the culture and business sectors in the countries from which they came. Moreover, these approaches need to be fine tuned to comply with business requirements and needs in financial institutions in Syria.

We have developed new quantitative method based on ISO 27K standards benefiting from the knowledge base we assembled about business sector in Syria in general, and financial institutions in particular.

Based on the experimental results we could verify that our model reflects ICT security level in financial institutions in Syria including recommendations and countermeasures which can be a corner stone in recognising the level of security in these institutions and to solve all problems and vulnerabilities which may affect the whole process of business in these institutions.

7. Future work

We can summarize the future work in below mentioned points:

1- We have developed our quantitative method based on linear approach (as an approximation), as a future work we can compare our linear approach with none linear approaches which may result in better model and methods

2- Due to long time and big effort we need to spend on our samples while making our surveys and applying resulted models, it is strongly recommended –as a future work- to use more samples while performing surveys and concluding quantitative methods and models.

3- To foster our results and concluded methods, it is more convenient to use a third party consultants to measure the gap between ICT security level in financial institutions and the results calculated based on our quantitative method

8. Appendix 1 (Survey and Directives Weighting –Samples-)

Questions	Findings			Notes	Weight					Item No.
	YES	No	Partially Applied		Sample4	Sample3	Sample2	Sample1	Average	
1-Information security management system (ISMS)										
Is there any evidence that management genuinely understands and supports the ISMS?	☐	☐			22	23	20	15	20	1
Is there any exclusion from ISMS scope?	☐	☐			20	10	16	15	15	2
If yes; are there justified reasons for excluding any elements?	☐	☐			13	9	10	8	10	3
Does organization 's ISM Policy adequately reflect the organization 's general characteristics and its strategic risk management approach?	☐	☐			17	17	12	11	15	4
Does ISM incorporate the organization 's business requirements plus any legal or regulatory obligations for information security?	☐	☐			20	17	22	18	20	5

Item No.	Questions	Findings			Notes	Weight				
		YES	No	Partially Applied		Average	Sample1	Sample2	Sample3	Sample4
6	Are responsible owners identified for all the information assets?	☐	☐			1	1	1	1	1
7	Is there an adequate analysis/evaluation of threats?	☐	☐			6	4	5	6	9
8	Is there an adequate analysis/evaluation of vulnerabilities and impacts?	☐	☐			6	7	8	4	5
9	Is there an adequate documentation of risk scenarios plus the prioritization or ranking of risks?	☐	☐			5	9	3	2	6
	2-1 Risk Treatment Plan									
10	Are appropriate "treatments" specified for all identified risks?	☐	☐			10	12	8	11	9
11	Are changes suitably fitted in the plan?	☐	☐			6	4	5	7	9
12	Is the Risk Treatment Plan being used and updated proactively as an information security management tool?	☐	☐			8	10	9	8	5

Item No.	Questions	Findings			Notes	Weight				
		YES	No	Partially Applied		Average	Sample1	Sample2	Sample3	Sample4
6	Has it been formally approved by management and set meaningful criteria for evaluating information security risks?	☐	☐			20	21	25	22	12
	2-Risk Assessment (14 Controls)									
1	Is there any systemic risk assessment method(s)?	☐	☐			10	13	10	9	8
2	Are the results of risk assessments comparable and reproducible ?	☐	☐			6	6	5	7	7
3	Is the risk assessment method updated as a result?	☐	☐			7	6	7	8	6
4	Is the definition of criteria sensible and practicable in relation to information security risks?	☐	☐			9	5	10	12	10
5	Are all relevant in-scope information assets included?	☐	☐			8	9	7	6	8

Item No.	Average	Sample1	Sample2	Sample3	Sample4	Notes	Partially Applied	No	YES	Questions
3	6	9	6	4	5			☐	☐	Do the top managers seriously commit to information security in their behaviour?
4	12	13	11	12	11			☐	☐	Are necessary competencies and training/awareness requirements for information security professionals and others with specific roles and responsibilities explicitly identified?
5	10	8	12	11	9			☐	☐	Is there a scheduled reviewing, at last once a year?
6	6	5	4	5	10			☐	☐	Does management play an active part and is fully engaged in the review/s?
										3-1 Internal ISMS audits
7	8	10	6	9	7			☐	☐	Is there any internal audits plan?
13	8	7	12	6	7			☐	☐	Are defined controls objectives and selected controls satisfied?
14	10	9	8	12	11			☐	☐	Is the organization effectively and proactively reviewing the implementation of the ISMS to ensure that the security controls identified in the Risk Treatment Plan, policies, etc. are actually implemented and are in fact in operation?
										3- Management responsibility
1	20	19	23	22	15			☐	☐	Are there enough resources allocated to the ISMS in terms of budget, manpower etc?
2	15	17	14	13	16			☐	☐	Are sufficient funds allocated by management to address information security issues in a reasonable timescale and to a suitable level of quality?

Item No.	Questions	Findings			Notes	Weight				
		YES	No	Partially Applied		Average	Sample1	Sample2	Sample3	Sample4
1	Are the policies communicated, understood and accepted? Standards for physical security of the computer and telecommunications installation and associated facilities; HR procedures governing access to and use of IT services (usernames and passwords, disciplinary procedures) End user guidelines covering PC software licensing and virus prevention, etc?	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐			15	11	12	19	18
2	Are they reasonable and workable?	☐	☐			8	8	10	6	7
3	Do they incorporate suitable and sufficient controls?	☐	☐			5	3	4	8	5
4	Do they cover all essential computing and telecommunication services?	☐	☐			8	7	10	6	5
8	If yes, are responsibilities for conducting ISMS internal audits formally assigned to competent, adequately trained IT auditors?	☐	☐			8	9	7	6	10
9	Does ISMS changes in response to the identification of significantly changed risks?	☐	☐			15	15	17	16	12
	4- Information security policy									

Questions	Findings			Notes	Weight					Item No.
	YES	No	Partially Applied		Sample4	Sample3	Sample2	Sample1	Average	
4-1 Internal Responsibilities and Communications										
Are the following positions well defined and activated: Senior manager responsible for IT and ISM; Information security professionals; Security administrators; Site/physical security manager and Facilities contacts; HR contact for HR matters such as disciplinary action and training; Systems and network managers, security architects and other IT professionals.	☐	☐			2	2	7	5	4	5
Is ISM given sufficient emphasis (is there a 'driving force'?) and management support?	☐	☐			6	5	4	5	5	6
Is there a senior management forum to discuss ISM policies, risks and issues?	☐	☐			2	3	2	1	2	7
Are roles and responsibilities clearly defined and assigned to skilled individuals?	☐	☐			5	10	6	9	8	8
Is there sufficient co-ordination within the BU (business unit), between BUs and with HQ?	☐	☐			5	3	2	2	3	9
Are the information flows (like incident reporting) operating effectively in practice?	☐	☐			3	5	7	6	5	10
4-2 External Parties										
Is there a risk analysis process in place for 3rd-party communications and connections?	☐	☐			8	9	11	12	10	11
Is there any individual who has responsibility for ensuring that all 3-party links are in fact identified and risk assessed?	☐	☐			3	9	6	3	5	12

Questions	Findings			Notes	Weight					Item No.
	YES	No	Partially Applied		Sample4	Sample3	Sample2	Sample1	Average	
Are ISM arrangements in operation on 3-party connections routinely reviewed against the requirements?	☐	☐			5	8	9	7	7	13
Are there formal contracts covering 3rd party links? Ownership and responsibility for ISM issues? Legal requirements? Protection of systems, networks and data via physical, logical and the right of audit by the organization? Procedural controls business assets, availability of services in the event of disasters, management notification for security incidents? Security clearance of staff?	☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐			14	12	10	12	12	14

9. Appendix 2 (Survey for IT employees-Sample page 1/3)

Name	Age	Gender	No. Of Children	Certification (s)

Please answer the following questions	
IT Training & Experience. Please specify course and certificate title and date	
Do you think your IT superiors are competent ?	
Are you able to manage and control the IT tasks assigned to you? Please explain	
Are you up-to-date with the latest developments and upgrades to the systems under your management? Please explain	
Can you work at night shifts? If not please write the reasons	
Are you able to continue improving your capabilities at home? Please specify how, for example using Internet, books, ...	
Can you travel outside you city (town) for training and/or work?	
Is there any social and culture difficulties affecting you job? Please explain	
Please define the following Security terms (please leave it blank in case of no answer)	
Confidentiality	
Integrity	
Availability	
Authentication	
Non-repudiation	
Password Policy	
Backup Policy	
Disaster Recovery	
Virus	
Denial Of Service	

References:

1- William Thompson, Lord Kelvin, Popular Lectures and Addresses [1891-1894], in Bartlett's Familiar Quotations, Fourteenth Edition, 1968, p. 723a.
2- ECCouncil, www.eccouncile.org, 2006.
3- ISO/IEC 27001:2005, Information technology-Security techniques-Information Security Management Systems (ISMS)-Requirements.
4- ISO/IEC 27002 or BS 17799:2005, Information technology-Security techniques-Code of practice for information security management.
5- Performance Measurement Guide for Information Security, *NIST Special Publication 800*-55, www.nist.gov.us.
6- Bond, A. (2004). *A quantitative evaluation framework for component security in distributed information systems.* Linkoping University: Institute of Technology.
7- Sademies A. and Savola R. Measuring the Information Security Level – A Survey of Practice in Finland. In: Proceedings of the 5th Annual International Systems Security Engineering Association (ISSEA) Conference, Arlington, Virginia, October 13-15, 2004. 10p
8- Murdoch, J. (2005, July). Security Measurement. York, United Kingdom.
9- Scarfone, K. (2008, September). Technical guide to information security testing and assessment. Gaithersburg, United States of America.

Received 18/5/2011