**Bulletin of Environment, Pharmacology and Life Sciences**
Bull. Env. Pharmacol. Life Sci., Vol 3 [6] May 2014: 63-70

Online ISSN 2277-1808
Journal's URL:http://www.bepls.com
CODEN: BEPLAD
Global Impact Factor 0.533
Universal Impact Factor 0.9804


**ORIGINAL ARTICLE**

# Evaluation of the Information Security Management System in Tehran Water and Sewage Company and Identification of Vulnerabilities according to ISO 17799

**Seyed Mojtaba Hosseini[1], Alireza Aghighi[2], Reza Shahhoseini[3]**
[1]Department of Accounting and Management, Faculty of Humanities, Hamedan Science and Research Branch, Islamic Azad University, Hamedan, Iran.
[2]Department of Management, Faculty of Economics and Management, Payame Noor University of Hamedan, Iran.
[3]Department of Health Care Management,Faculty of Health, Baqiyatallah University of Medical Science, Tehran, Iran.

**ABSTRACT**
*Current work aims at evaluating information security system of Tehran Water and Sewage Company as an organization with clear goals, strategies, and functions according to ISO 17799. Statistical society includes experts in Information Technology. The 83 persons were selected as sample by snowball sampling. Following investigation of different factors and models, binominal test was used for comparing current status and optimal status of the aspects. Friedman test was used for determining importance (ranking) of information security system's aspects in current and optimal status in the view of respondents. Descriptions and statistical analysis were done using SPSS Software. On the other hand, by ranking factors of information security in terms of their importance in this organization, some strategies are provided for promoting information security in Tehran Water and Sewage Co.*
***Keywords***: *Information security, information security management system, critical points, comprehensive evaluation system*

Received 10.02.2014 Revised 04.04.2014 Accepted 25.04. 2014

## INTRODUCTION

Information security is responsible for protecting information against a wide range of threats, risks, and vulnerabilities, aim of which is ensuring availability, integrity and confidentiality of information in order to reduce the threats and preserve organization activity's continuity [1].
Information security is obtained by applying an appropriate collection of controls including policies, processes, procedures, organizational structures, and software and hardware [2]. After 2000, each year more than a million attacks are done against governmental and private institutes and organizations, financial and credit institutions, service companies and e-commerce services is reported. It is just figure for those attacks which were reported formally, while most sabotageis not recorded [3].
Computer scientists often interpret "uncomfortable and dangerous occurrences" as in the category of "unauthorized access to data", "leaking confidential information", "tribute available from a service provider", "secretly change in data", "data theft"," wiping data", "data falsification", "interfere with the proper function of the user's machine" and "machine data privacy violations" (ibid, p.19).
In a study by Computer Emergency Readiness Team (CERT) in 2005 indicated most national organization concentrated on security threats and stated 35 percent of 918 companies reported increased electronic crimes in 2005 compared to 2003. 30 percent stated no change, and 22 percent stated they are not sure or aware about it. In other words, 65 percent of the companies have had experience of electronic threats and electronic crimes [4].
Various standards and models have been provided for achieving data security (such as GMITS, COBIT, NIST, etc.), however, ISO 17799 Standard is widely accepted and recognized. On the other hand, standards and models of data achievement are often developed by industries and there is rare academic theoretical literature. ISO 17799 Standard provides security controls and criteria for measurement of

criteria (ibid). ISO 17799 Standard was originally provided by British Standard Institution (BS) and then it was extended by International Organization for Standardization (ISO) and The International Electro technical Commission (IEC). ISO 17799 Standard is essentially interested in providing a model for managers and their staffs for planning and management of an efficient system of information security management. ISO 17799 Standard includes 11 articles of security control. It also is consisted of 39 security categories. Every main category should result in a control goal and it provides one or more controls whichshould be applied for achieving control goal [5].

11 main articles of ISO 17799 security control are as follows:

1. Information Security Policy 2. Organization of information security 3. Asset Management 4. Human Resources security 5. Physical and Environmental Security 6. Communications and Operations Management 7. Access Control 8. Acquisition, development and maintenance of information system 9. Information Security Incident Management 10. Business continuity management 11. Compliance.

Information is available in various forms; on paper, electronically, sent by mail or electronic means, recorded on film or orally presented in conversation. Any way by which information is obtained or they are shared or stored, they require accurate and proper protection (Enrique et al., 2006). Tehran Water and Sewage Co. and its current and stored information are not exception and require ongoing protection and preservation and review.

This work attempts to measure and extract characteristics and indices of an information security system from ISO 17799 Model. They it is going to investigate and evaluate status of information security system on Tehran Water and Sewage Co. using these indices so that priorities are identified and necessary recommendations are made for promoting status of information security system of Tehran Water and Sewage Co.

## METHODOLOGY

Current work is applied research in terms of the purpose and it is survey study in terms of methodology.

### Statistical Society and Sample

Statistical society includes 128 experts and managers of Tehran Water and Sewage Co. who were active in the company within first six months of the year, 83 of whom were selected using snowball sampling method.

### Data Collection Methods

Necessary indices for evaluating information security system of Tehran Water and Sewage Co. were firstly measured by library review and they were collected through field study and questionnaire. An initial sample including 30 questionnaires for pre-test was prepared. Using data obtained from these questionnaires and using SPSS Software, reliability coefficient was calculated by Cronbach's alpha as 0.9653. It denotes reliability of the questionnaire. Contentvalidity of the questionnaire was supported by professors and practitioners.

In order to evaluate and measure information security, Reductionism process was used, so that information security concept was classified into its aspects (11 Articles of ISO 17799) and each aspect was classified into its components (categories of ISO 17799), and several indices will be defined for each component, all of which finally constitute questionnaire's items.

### Data Analysis Method

Due to unknown society distribution and limitation of the number of samples, non-parametric statistics techniques should be used. Binominal test is used for comparing current and optimal status, and Friedman test was used for determining importance (ranking) of information security system's aspects in current and optimal status in the view of respondents.

## RESULTS

For testing research hypotheses and ranking aspects of information security, binominal and Friedman tests were used.

Table 1 indicates results of binominal test for comparing current and optimal status of information security in Tehran Water and Sewage Co.

| Variable | | Sum of ranks | | Z statistics | Sig. level |
|---|---|---|---|---|---|
| | | **positive** | **negative** | | |
| Optimal status | **Current status** | **423** | **137** | **-2.69*** | **0.007** |
| *test is based on negative ranks | | | | | |

As it is observed in Table 1, the assumption for equality of means of optimal and current status variable is rejected ($p-value < 0.05$), thus there is difference between current status rank mean and optimal

status rank mean. Investigating positive and negative ranks indicates mean of optimal status rank is higher than mean of current status rank.

Following table presents results for binominal test for comparing current and optimal status regarding information security in security policy aspect in Tehran Water and Sewage Co.

Table 2.Results for binominal test for comparing current and optimal status regarding information security in security policy aspect

| Variable: security policy | | Sum of ranks | | Z statistics | Sig. level |
|---|---|---|---|---|---|
| | | **positive** | **positive** | | |
| Optimal status | **Current status** | **361** | **134** | **-2.34*** | **0.019** |
| *test is based on negative ranks | | | | | |

As it is observed in Table 2, the assumption for equality of means of optimal and current status variables is rejected ($p - value < 0.05$), thus there is difference between current status rank mean and optimal status rank mean in security policy aspect. Investigating positive and negative ranks indicates mean of optimal status rank is higher than mean of current status rank.

Table 3 presents results for binominal test for comparing current and optimal status regarding information security in organizing information security aspect in Tehran Water and Sewage Co.

Table 3. Results for binominal test for comparing current and optimal status regarding information security in organizing information security aspect

| Variable: organizing information security | | Sum of ranks | | Z statistics | Sig. level |
|---|---|---|---|---|---|
| | | **positive** | **positive** | | |
| Optimal status | **Current status** | **361** | **134** | **-2.34*** | **0.019** |
| *test is based on negative ranks | | | | | |

As it is observed in Table 3, the assumption for equality of means of optimal and current status variables in organizing information security aspect is rejected ($p - value < 0.05$), thus there is significant difference between current status rank mean and optimal status rank mean. Investigating positive and negative ranks indicates mean of optimal status rank is higher than mean of current status rank.

Table 4 presents results for binominal test for comparing current and optimal status regarding asset management aspect in Tehran Water and Sewage Co.

Table 4. Results for binominal test for comparing current and optimal status regarding information security

| Variable: assets management | | Sum of ranks | | Z statistics | Sig. level |
|---|---|---|---|---|---|
| | | **positive** | **negative** | | |
| Optimal status | **Current status** | **317.5** | **117.5** | **-2.24*** | **0.025** |
| *test is based on negative ranks | | | | | |

As it is observed in Table 4, the assumption for equality of means of optimal and current status variables in assets management aspect is rejected ($p - value < 0.05$), thus there is significant difference between current status rank mean and optimal status rank mean. Investigating positive and negative ranks indicates mean of optimal status rank is higher than mean of current status rank.

Table 5 presents results for binominal test for comparing current and optimal status regarding human resources security aspect in Tehran Water and Sewage Co.

Table 5. Results for binominal test for comparing current and optimal status regarding information security

| Variable: human resources management security | | Sum of ranks | | Z statistics | Sig. level |
|---|---|---|---|---|---|
| | | **positive** | **positive** | | |
| Optimal status | **Current status** | **166.5** | **361.5** | **-1.88** | **0.06** |
| *test is based on negative ranks | | | | | |

As it is observed in Table 5, the assumption for equality of means of optimal and current status variables in human resource security aspect is rejected ($p - value < 0.05$), thus there is significant difference between current status rank mean and optimal status rank mean. Investigating positive and negative ranks indicates mean of optimal status rank is higher than mean of current status rank.

Table 6 presents results for binominal test for comparing current and optimal status regarding physical and environmental security aspect in Tehran Water and Sewage Co.

Table 6. Results for binominal test for comparing current and optimal status regarding information security

| Variable: physical and environmental security | | Sum of ranks | | Z statistics | Sig. level |
|---|---|---|---|---|---|
| | | **positive** | **positive** | | |
| Optimal status | **Current status** | **176** | **352** | **-1.7** | **0.089** |
| *test is based on negative ranks | | | | | |

As it is observed in Table 6, the assumption for equality of means of optimal and current status variables in physical and environmental security aspect is supported ($p-value > 0.05$), thus there is no significant difference between current status rank mean and optimal status rank mean.

Table 7 presents results for binominal test for comparing current and optimal status regarding communications and operations management aspect in Tehran Water and Sewage Co.

Table 7. Results for binominal test for comparing current and optimal status regarding information security

| Variable: Communications and Operations Management | | Sum of ranks | | Z statistics | Sig. level |
|---|---|---|---|---|---|
| | | **positive** | **positive** | | |
| Optimal status | **Current status** | **317.5** | **117.5** | **-2.24*** | **0.025** |
| *test is based on negative ranks | | | | | |

As it is observed in Table 7, the assumption for equality of means of optimal and current status variables in communications and operations aspect is rejected ($p-value < 0.05$), thus there is significant difference between current status rank mean and optimal status rank mean. Investigating positive and negative ranks indicates mean of optimal status rank is higher than mean of current status rank.

Table 8 presents results for binominal test for comparing current and optimal status regarding access control aspect in Tehran Water and Sewage Co.

Table 8. Results for binominal test for comparing current and optimal status regarding information security

| Variable: access control | | Sum of ranks | | Z statistics | Sig. level |
|---|---|---|---|---|---|
| | | **positive** | **positive** | | |
| Optimal status | **Current status** | **331** | **75** | **-2.99*** | **0.003** |
| *test is based on negative ranks | | | | | |

As it is observed in Table 8, the assumption for equality of means of optimal and current status variables in access control aspect is rejected ($p-value < 0.05$), thus there is significant difference between current status rank mean and optimal status rank mean. Investigating positive and negative ranks indicates mean of optimal status rank is higher than mean of current status rank.

Table 9 presents results for binominal test for comparing current and optimal status regarding acquisition, development and maintenance of information system aspect in Tehran Water and Sewage Co.

Table 9. Results for binominal test for comparing current and optimal status regarding information security

| Variable: Acquisition, development and maintenance of information system | | Sum of ranks | | Z statistics | Sig. level |
|---|---|---|---|---|---|
| | | **positive** | **positive** | | |
| Optimal status | Current status | **331** | **75** | **-2.99*** | **0.003** |
| *test is based on negative ranks | | | | | |

As it is observed in Table 9, the assumption for equality of means of optimal and current status variables in acquisition, development and maintenance of information system aspect is rejected ($p-value < 0.05$), thus there is significant difference between current status rank mean and optimal status rank mean. Investigating positive and negative ranks indicates mean of optimal status rank is higher than mean of current status rank.

Table 10 presents results for binominal test for comparing current and optimal status regarding Information Security Incident Management aspect in Tehran Water and Sewage Co.

Table 10. Results for binominal test for comparing current and optimal status regarding information security

| Variable: Information Security Incident Management | | Sum of ranks | | Z statistics | Sig. level |
|---|---|---|---|---|---|
| | | **positive** | **positive** | | |
| Optimal status | Current status | **146.5** | **259.5** | **-1.34** | **0.18** |
| *test is based on negative ranks | | | | | |

As it is observed in Table 10, the assumption for equality of means of optimal and current status variables in Information Security Incident Management aspect is supported ($p-value > 0.05$), thus there is no significant difference between current status rank mean and optimal status rank mean.

Table 11 presents results for binominal test for comparing current and optimal status regarding business continuity management aspect in Tehran Water and Sewage Co.

Table 11. Results for binominal test for comparing current and optimal status regarding information security

| Variable: Business continuity management | | Sum of ranks | | Z statistics | Sig. level |
|---|---|---|---|---|---|
| | | **positive** | **positive** | | |
| Optimal status | Current status | **562** | **104** | **-3.7*** | **0.000** |
| *test is based on negative ranks | | | | | |

As it is observed in Table 11, the assumption for equality of means of optimal and current status variables in business continuity management aspect is rejected ($p-value < 0.05$), thus there is significant difference between current status rank mean and optimal status rank mean. Investigating positive and negative ranks indicates mean of optimal status rank is higher than mean of current status rank.

Table 12 presents results for binominal test for comparing current and optimal status regarding compliance aspect in Tehran Water and Sewage Co.

Table 12. Results for binominal test for comparing current and optimal status regarding information security

| Variable: Compliance | | Sum of ranks | | Z statistics | Sig. level |
|---|---|---|---|---|---|
| | | **positive** | **positive** | | |
| Optimal status | Current status | **51** | **384** | **-3.71** | **0.000** |
| *test is based on negative ranks | | | | | |

As it is observed in Table 12, the assumption for equality of means of optimal and current status variables in compliance aspect is rejected ($p-value < 0.05$), thus there is significant difference between current status rank mean and optimal status rank mean. Investigating positive and negative ranks indicates mean of optimal status rank is higher than mean of current status rank.

Ranking 11 major articles of security control

Table 13 indicates results for Friedman test for comparing rank mean of 11 major articles of security control.

Table 13. Results for Friedman test for comparing rank mean of 11 major articles of security control

| major articles of security control | rank mean | Median | chi-square | degree-of-freedom | significance level |
|---|---|---|---|---|---|
| Information Security Policy | 8.53 | 4 | 207.31 | 9 | 0.000 |
| Organization of information security | 6.29 | 3 | | | |
| Asset Management | 5.15 | 3 | | | |
| Human Resources security | 7.65 | 4 | | | |
| Physical and Environmental Security | 3.44 | 2 | | | |
| Communications and Operations Management | 3.35 | 2 | | | |
| Access Control | 4.94 | 3 | | | |
| Acquisition, development and maintenance of information system | 6.64 | 4 | | | |
| Information Security Incident Management | 6.41 | 5/3 | | | |
| Business continuity management | 2.61 | 1 | | | |
| Compliance | 3.57 | 2 | | | |

As observed in Table 13, equality assumption for rank mean of 11 main articles of security control is not supported ($p - value < 0.05$); in other words, at least there is significant difference between rank mean of two major articles of security control (their ranks are not equal in the view of experts). Investigation of rank means indicates Security Policy article has the highest rank and Business Continuity Management article has the lowest rank among 11 major articles of security control.

## DISCUSSION AND CONCLUSION

Field studies of this research were collected through questionnaire distribution among managers, staffs, and experts of informatics, network, digital library, training, protection and other people who were involved in information security in the organization.

Main Hypothesis: there is significant difference between current and optimal status of information security in Tehran Water and Sewage Co. thus, there is significant difference between rank mean of current status and optimal status, and main hypothesis is supported.

Investigation of sum of positive and negative ranks shows rank mean of optimal status is higher than rank mean of current status.

Minor Hypothesis 1: There is significant difference between current and optimal status in information security in Tehran Water and Sewage Co. in terms of Security Policy aspect. Results indicated there is significant difference between rank mean of optimal status and rank mean of current status in terms of Security Policy aspect. Investigation of sum of positive and negative ranks shows rank mean of optimal status is higher than rank mean of current status. Findings in the current work are consistent with findings[6].

Minor Hypothesis 2: There is significant difference between current and optimal status in information security in Tehran Water and Sewage Co. in terms of Organization of information security aspect. Results indicated there is significant difference between rank mean of optimal status and rank mean of current status, supporting the hypothesis. Investigation of sum of positive and negative ranks shows rank mean of optimal status is higher than rank mean of current status.

Minor Hypothesis 3: There is significant difference between current and optimal status in information security in Tehran Water and Sewage Co. in terms of Asset Management aspect. Results indicated there is significant difference between rank mean of optimal status and rank mean of current status. Investigation of sum of positive and negative ranks shows rank mean of optimal status is higher than rank mean of current status. Findings in the current work are consistent with findings by Karimi and inconsistent with findings [6].

Minor Hypothesis 4: There is significant difference between current and optimal status in information security in Tehran Water and Sewage Co. in terms of Human Resources Security aspect. Results indicated there is significant difference between rank mean of optimal status and rank mean of current status. Investigation of sum of positive and negative ranks shows rank mean of optimal status is higher than rank mean of current status. Thus this hypothesis is supported. Findings in the current work are consistent with findings by all observed studies especially [6].

Minor Hypothesis 5: There is significant difference between current and optimal status in information security in Tehran Water and Sewage Co. in terms of Physical and Environmental Security aspect. Results indicated there is no significant difference between rank mean of optimal status and rank mean of current status. Considering lack of significant difference, Minror Hypothesis 5 is rejected. Findings in the current work are consistent with findings [6].

Minor Hypothesis 6: There is significant difference between current and optimal status in information security in Tehran Water and Sewage Co. in terms of Communications and Operations Management aspect. Results indicated there is significant difference between rank mean of optimal status and rank mean of current status. Investigation of sum of positive and negative ranks shows rank mean of optimal status is higher than rank mean of current status. Findings in the current work are consistent with findings [6].

Minor Hypothesis 7: There is significant difference between current and optimal status in information security in Tehran Water and Sewage Co. in terms of Access Control aspect. Results indicated there is significant difference between rank mean of optimal status and rank mean of current status. Investigation of sum of positive and negative ranks shows rank mean of optimal status is higher than rank mean of current status. Thus, it is supported.

Minor Hypothesis 8: There is significant difference between current and optimal status in information security in Tehran Water and Sewage Co. in terms of Acquisition, Development and Maintenance of Information System aspect. Results indicated there is significant difference between rank mean of optimal status and rank mean of current status. Investigation of sum of positive and negative ranks shows rank

mean of optimal status is higher than rank mean of current status. Findings in the current work are consistent with findings [6].

Minor Hypothesis 9: There is significant difference between current and optimal status in information security in Tehran Water and Sewage Co. in terms of Information Security Incident Management aspect. Results indicated there is no significant difference between rank mean of optimal status and rank mean of current status. Thus, Minor Hypothesis 9 is rejected. Findings in the current work are consistent with findings [6].

Minor Hypothesis 10: There is significant difference between current and optimal status in information security in Tehran Water and Sewage Co. in terms of Business Continuity Management aspect. Results indicated there is significant difference between rank mean of optimal status and rank mean of current status. Investigation of sum of positive and negative ranks shows rank mean of optimal status is higher than rank mean of current status. Findings in the current work are consistent with findings [6].

Minor Hypothesis 11: There is significant difference between current and optimal status in information security in Tehran Water and Sewage Co. in terms of Compliance aspect. Results indicated there is significant difference between rank mean of optimal status and rank mean of current status. Investigation of sum of positive and negative ranks shows rank mean of optimal status is higher than rank mean of current status. Findings in the current work are consistent with findings by Karimi, and they are inconsistent with findings [6].

Results of Friedman test shows equality assumption for rank mean of 11 main articles of security control is not supported ($p - value < 0.05$); in other words, at least there is significant difference between rank mean of two major articles of security control (their ranks are not equal in the view of experts). Investigation of rank means indicates Security Policy article has the highest rank and Business Continuity Management article has the lowest rank among 11 major articles of security control.

Considering supporting minor hypotheses 1-4, it is recommended reexamination is done regarding information security policy, its implementation and information security organization and it is attempted to institutionalize such policy as internally in all staffs of the organization so that confidential information leakage is prevented. It is especially important for Water and Sewage Company which is a semi-governmental organization.

In minor hypothesis 3, assets management is mentioned. Respective standard is considerably different from what is current in the organization, thus this standard should be implemented locally and in tangible manner for staff. If it is understood by staff, it will be implemented automatically by them. Regarding assets management, organization's assets should be considered as personal assets of the staff so that they attempt to preserve and use them efficiently and properly.

Minor hypothesis 4 addresses human resources security. It suggests the fact that organization can have staffs with high commitment toward organization by accurately selection of the staff and preserving safe working environment free from any stress.

Minor hypotheses 6 and 7 on communication and operations management and access control are in the same line. It these parts which are critical parts, it is recommended that organization uses specific network communicative software and information access level for individuals is clear and it is better that controllers of these parts are anonymous.

Considering minor hypothesis 8 organizations are recommended to use information systems with exclusive ownership and utilize limited reliable people of the preservation for development and preservation of the systems.

Considering hypothesis 10, the organization, which is able to preserve its internal information and receive external information and it can impose low information access level for its competitors, can think of its survival and progress.

Overall it is recommended organization's equipment and information system is inspected regularly and problems are reported and solved as soon as possible. In addition, organizations should update information and security system of the organization regularly and it continue ongoing staff training.

## REFERENCES

1. Solms, R. (1999), “Information security management: why standards are important”, Information Management & Computer Security, Vol. 7 No. 1, pp. 50-7.
2. Alaboodi, Saleh(2007), “Towards evaluating security implementations using the Information Security Maturity Model” , A thesis for the degree of Master of Applied Science in Electrical and Computer Engineering presented to the University of Waterloo, Canada.
3. Zaker-alhuseini, A. and Malekian, E. (2011), Data security, Nas Scientific - Cultural Institute: Tehran
4. Computer Emergency Response Team. (2006). *2005 E-crime watch survey shows significant increase in electronic crimes.* Retrieved September 13, 2005, from http://www.cert.org/about/ecrime.html

5. ISO (2005), International Organization for Standardization, ISO/IEC 17799, Information technology Security techniques - Code of practice for information security management.
6. Hajhusseini, M. (2009), Evaluation of information security network risk according to ISO 17799, Shahid Beheshty University, Faculty of Electrical