Accepted Manuscript

ISCP: In-Depth Model for Selecting Critical Security Controls

Nadher Al-Safwani , Yousef Fazea , Huda Ibrahim

PII: S0167-4048(18)30553-4
DOI: 10.1016/j.cose.2018.05.009
Reference: COSE 1346

To appear in: *Computers & Security*

Received date: 24 January 2018
Revised date: 15 April 2018
Accepted date: 14 May 2018

Please cite this article as: Nadher Al-Safwani , Yousef Fazea , Huda Ibrahim , ISCP: In-Depth Model for Selecting Critical Security Controls, *Computers & Security* (2018), doi: 10.1016/j.cose.2018.05.009

ISCP: In-Depth Model for Selecting Critical Security Controls

Nadher Al-Safwani[a], Yousef Fazea*[b], Huda Ibrahim[c]

[a]CyberSecurity Consultant, International Telecommunication Union Regional Cybersecurity Centre, Oman
[b,c]InterNetWorks Research Laboratory, School of Computing, Universiti Utara Malaysia, 06010 Sintok Kedah, Malaysia

Abstract: The primary goal of all organizations worldwide is to reduce potential threats and vulnerabilities. An information security control assessment is a far-reaching way to deal with control analysis that can help organizations to measure the adequacy and effectiveness of their present and planned security controls. Availability of adequate resources and proper risk analysis practices should be considered in preventing security breaches in order to achieve returns on security investments. Nonetheless, and despite the necessity for a competent security analysis framework, present frameworks and methodologies for security control analysis lack practical guidelines and mostly depend on subjective judgment and qualitative approaches. This paper proposes an information security control prioritization (ISCP) model that can determine the critical vulnerable controls based on a number of assessment criteria. The model uses techniques from the Order Performance by Similarity to Ideal Solution (TOPSIS) method, which is a sub-method of multiple attribute decision making. The proposed model provides clear guidelines on how to accomplish control analysis in a structured, self-organizing and constituent manner, with minimal overlap. Evaluation of information security controls using TOPSIS as the prioritization method involves a cost-effectiveness analysis, an effective and efficient assessment in terms of testing and selecting information security controls in organizations.

Keywords: Information Security, Security Controls Assessment, Attribute Decision Making, Prioritization Model, TOPSIS, Critical Vulnerable Controls

1. Introduction

With the emergence of technology for conducting electronic business, organizations are increasingly relying on information systems and Information Technology (IT) assets to create new opportunities and enhance their current business. According to [3], when IT and technology play substantial roles in businesses and organizations, they should focus on information security. Aside from protecting organizations and their IT assets from loss and destruction, information security also ensures the Confidentiality, Integrity, Availability and Accountability (CIAA) of their resources [3]. Information security experts encourage organizations to conduct an Information Security Risk Assessment (ISRA) to protect the CIAA of business resources and their assets. Such precautions would help organizations to preserve their assets and achieve their business objectives [4].

In performing risk assessment, Singh in [5] proposed four steps: (1) identify the controls to be tested; (2) test the efficacy of these controls; (3) analyze the test results; and (4) recommend security enhancements based on the analysis. Research on risk assessment is gaining increasing attention from academic and business sectors. However, the crucial part of IT risk assessment has not received sufficient attention [6]. In fact, implementation of control risk management has been an ambiguous issue over the past few years [7]. Many risk analysis methodologies and models have proposed various approaches to solve these issues. Previous studies attempted to enhance security decisions by using either quantitative or qualitative modelling techniques [8]. Unfortunately, these risk assessment models remain inadequate, because previous research did not consider decision-making criteria and the cost effectiveness of the analysis. Information Security Controls (ISC), such as firewalls, routers, operating systems and databases, are technology solutions that mitigate risks to an acceptable level.

As the risk assessment process is important, several models have been proposed to improve the methodology. Although these methods help to provide a business process and general approach, they do not offer clear practical guidelines, and their selection is based on expert opinion and subjective judgment. This lack of objective quantitative practical guidelines affects the prioritization and analysis of vulnerable assets and controls. This paper contributes the successful design of an ISCP model. The design closed the literature identified gaps of existing ISRA methods. The model helps decision makers to select and prioritize the most vulnerable and most effective controls.

A prioritization model is proposed to evaluate and select critical vulnerable information security controls for ISRA, providing clear guidelines on how a structured, self-organizing and adaptive risk assessment can be accomplished. The aim of the model is to reduce the extensive use of resources in terms of cost and time, and to optimize control assessment. The model uses Multiple Attribute Decision Making (MADM) to prioritize critical control criteria, such as threats, severity and cost impact. It provides organizations with the best possible option by allowing them to select and implement critical controls based on their own constraints and budget. The remainder of the paper is organized as follows: the related work on ISC assessment is presented first, followed by a description of the information security control prioritization (ISCP) model and its results. The proposed model is then discussed in detail. Finally, the conclusion of the study and directions for future work are provided.

2. Related Work

This section reviews the literature on ISC in organizations. A great body of work on risk management process is available, including studies by standards organizations, academic institutions and industry bodies, such as [1], National Institute of Standard and Technology (NIST SP 800-30) [2], Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) [9], Information Risk Analysis Methodology (IRAM) [10], Expression of Needs, CCTA Risk Analysis and Management Method (CRAMM) [11] and Identification of Security Objectives (EBIOS) [12]. Although these models assist organizations in performing risk management, most of them focus on defining risk management processes rather than identifying optimal controls for organizations' resources.

Traditional risk management models did not endorse any effective assessment, control prioritization or implementation of the most effective controls that are suitable to a particular organization. Lv *et al.* [13] proposed multi-criteria selection models based on a number of dataset requirements. However, these models do not pay attention to the fact that the problem of control ranking is a group decision problem in which subjective and objective judgments of the results must be available to provide better ranking of security controls.

Controls should be evaluated according to weighted selected criteria and not only on control weighting., but no results of the security control ranking of these models has been reported. As these models are still at the proposal stage, further study is required to prove and validate this approach. Existing ISC frameworks can be used as a basis for risk evaluation in organizations.

Frameworks such as NIST SP 8-30, OCTAVE, IRAM, CRAMM and EBIOS provide information on how to reduce risk by implementing liability security controls, such as Control Objectives for IT and Available Technology (COBIT 4.1) [14], Sys Admin and Network Security (SANS) (SANS, 201), ISO 27001 and Information Technology Infrastructure Library (ITIL) [15]. Many studies focus on risk management processes from standards organizations, academic groups and industry bodies. The frameworks and models listed above define the risk management process and serve as effective references. However, they reduce the risk management programme to a mere checklist. Although these frameworks seem excellent in theory, most do not provide clear guidelines on how to accomplish control security assessment. The following subsections summarize the existing ISC frameworks and models.

2.1 ISO/IEC 27005

ISO/IEC [1] (see Fig. 1) provides guidelines for Information Security Risk Management (ISMS) in an organization. These guidelines give particular support to the requirements specified in ISO/IEC 27001, designed to assist the implementation of risk management. In this process, the background is first established. Then, the risks are assessed through a risk treatment plan in order to effectively implement recommended control and decisions. The standard attempts to identify the actual sources of particular risks before deciding what can be done, and when. The main objective of this standard is to reduce risks to an acceptable level. Despite being a generic guideline for managing risks, ISO 27005 does not obviously outline a proper analysis of current controls [5]. It fails to give granular guidance on the key steps of critical control identification, and qualitative data are used for analysis. In addition, selecting ISC from common practices is difficult and organizations are left to choose the best controls that fit their conditions [15].

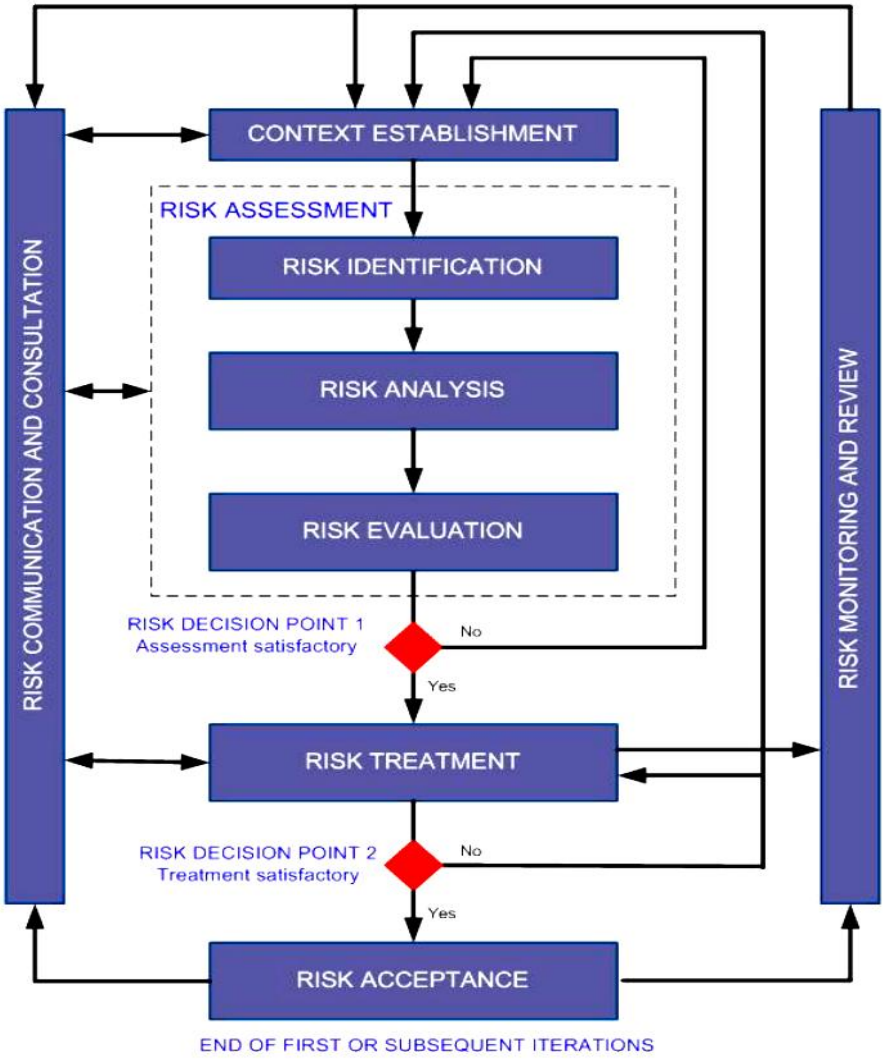

Fig. 1. ISO/IEC 27005 risk management [1]

2.2 Risk Management Guide for Information Technology Systems (NIST SP 800-30)

NIST SP 800-30 is a guide issued by NIST for the development of a risk management programme, primarily for US government sectors [2, 16]. It contains practical guidelines and definitions necessary for developing effective risk management programmes within existing IT systems. Its main goal is to help organizations manage risks more effectively within their IT resources.

The NIST risk management guide assists IT managers to reduce operational costs and achieve revenue by minimizing loss that results from IT failure. The risk assessment framework consists of nine primary steps or activities, as illustrated in Fig. 2.

The NIST guideline highlights risk assessment and risk mitigation as two critical components. In the risk assessment process, control analysis (step four) does not provide granular guidance on how control analysis should be conducted, unlike ISO 27005 [5]. Its risk assessment process is based on the organization's subjective judgment [17] rather than objective evaluation. No further guidance, particularly on how controls should be selected for testing purposes, is provided [18, 19].
Nor does it consider the specific constraints, such as costs, scheduling and resources, experienced by each organization [3], which suggests that expertise is necessary in selecting the best and critical controls. The key risk assessment steps

are conducted qualitatively, although many organizations do not use qualitative analysis, preferring the quantitative approach, particularly through intelligent decision support systems.

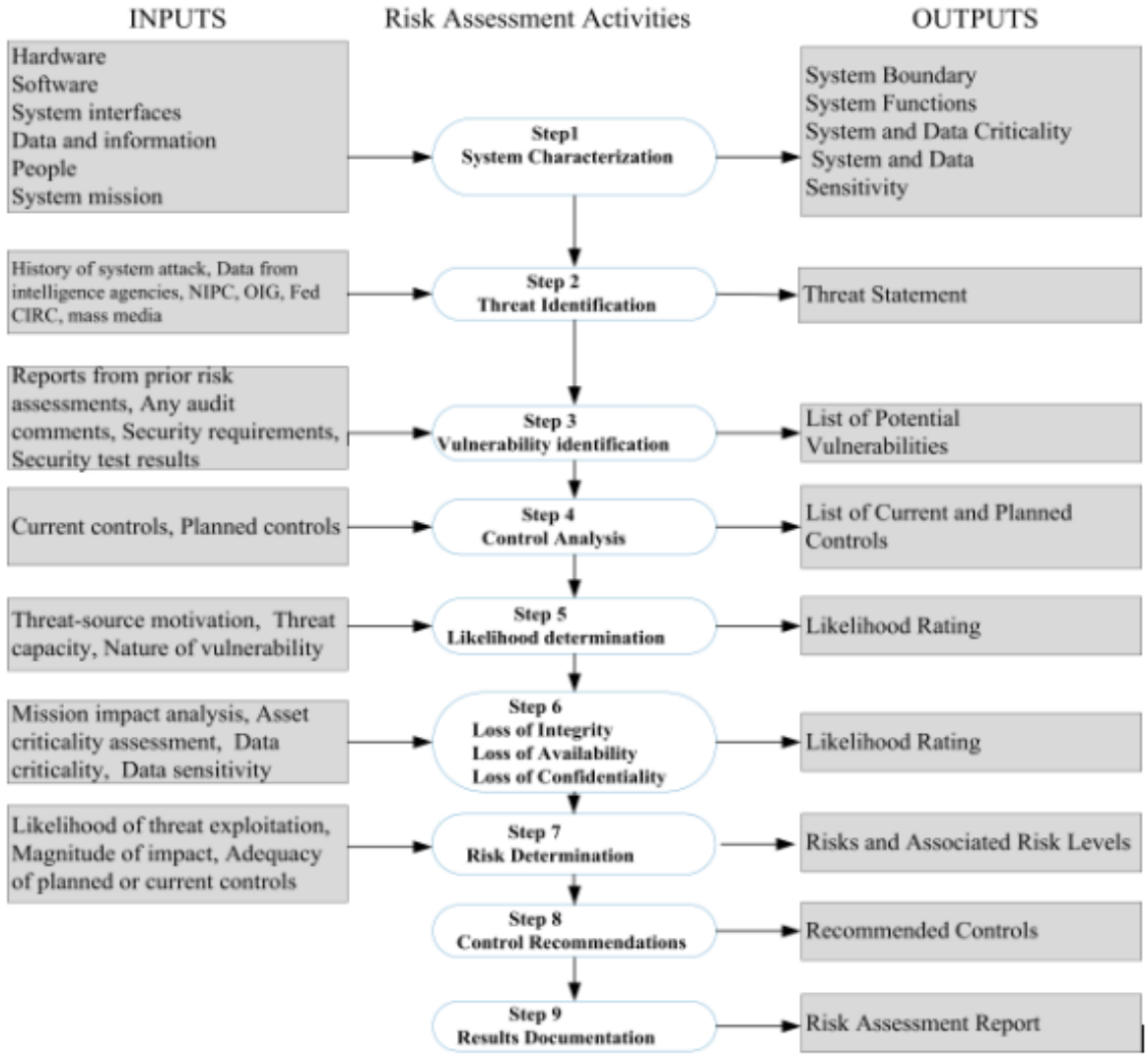

Fig. 2. NIST risk assessment activities [2]

2.3 OCTAVE

OCTAVE is a suite of tools, techniques and methods for risk-based information security strategic assessment and planning [20]. The OCTAVE concept was published by the Software Engineering Institute of Carnegie Mellon University in 1999 and was formalized into the OCTAVE criteria in [21]. The method and plan-development phase in risk management are covered in the OCTAVE strategy, which includes risks to critical assets, protection strategy, risk measures and risk mitigation plans. The basic requirements of the OCTAVE approach are materialized in a set of criteria. Several methods, such as OCTAVE methodology and OCTAVE-S, were developed specifically for these criteria. [11, 22].

OCTAVE is reportedly more effective than NIST and ISO 27005 in providing prescriptive guidance. It details risk management instead of only the process framework [5]. However, it focuses on qualitative risk determination. Risk assessment has obviously shifted towards the need for quantitative information, which would more accurately help in

the decision-making process of organization leaders [23]. OCTAVE is also known to depend on expert analysis in determining the critical controls and related risks. When more people are involved, analysis becomes more subjective [18, 24]. Qualitative data analysis and team-subjective factors may result in an inaccurate and ambiguous output [25].

2.4 IRAM

IRAM [10] is a proprietary methodology available in the Information Security Forum. It uses business influence analysis approaches to risk analysis. It is geared towards assessing the influence of potential security breaches on business, assessing threats and vulnerabilities, determining information risks, identifying and analyzing control requirements and generating an action plan to address the identified control requirements. The IRAM control selection is conducted through qualitative interviews of all stakeholders and business owners. As mentioned earlier, human judgments are always subjective and vary among individuals, and may thus result in inaccurate risk assessment [23, 24]. However, the goal of risk analysis is to minimize the subjective factors; risk analysis based on quantitative measurements facilitates accurate decision making [23].

2.5 EBIOS

EBIOS [12] is a comprehensive set of guidelines for information system risk managers. It was originally launched by the French government but is now supported by a team of experts of diverse origins. It produces common practices and application documents targeted to end users in various contexts, and yields critical IT security standards [18]. Although EBIOS suggests common practices and identifies controls by formalizing security objectives, it does not have clear guidelines on how to accomplish these objectives in a structured manner [26]. Similar to IRAM, EBIOS depends on self-judgment or expert opinion. Several risk assessment methods rely on subjective inputs by human experts. As stressed in the preceding paragraphs, human judgment can be inconsistent, particularly in the contexts of uncertainty and risk [26].

2.6 CRAMM

CRAMM is a risk analysis method developed by the Central Communication and Telecommunication Agency, a British government organization. It requires the use of a special tool. The first release of CRAMM (method and tool) was based on the best practices of British government organizations. CRAMM is the risk analysis method currently preferred by large organizations, such as government bodies and industries, in the United Kingdom [11]. The risk management tool is compliant with ISO standards to provide guidance for ISMS. Unfortunately, CRAMM depends solely on qualitative risk evaluation, which suggests that the results may be subjective and inaccurate [27].

3. Statistical Design of Experimental Approach

As an alternative to the qualitative approach of the models described above, Stoneburner *et al*. in [19] proposed the statistical design of experiments based on the Plackett and Burman model [28], considering important aspects of risk assessment.

The proposed model identifies and ranks security controls that are specifically important to an organization. Only the selected controls are tested. The advantage of this approach is that security control recommendations are based only on the nature of the threat and the cost important to the organization. However, the sum of the ranks used in assessing the risk is not suitable for evaluating the complexity of different evaluation criteria and is insufficient for calculating the approximate cases of ISC. This approach can be further enhanced as a decision-support system for control selection by increasing the number of criteria to achieve better results Organizations should be provided with risk severity details and the cost of remediation effort, which are not considered in this model.

3.1 Multi-Criteria Evaluation Methods

Lv *et al.* [29] developed a multi-criteria evaluation method, which quantitatively ranks the available risk controls with the help of PROMETHEE methodology and Geometrical Analysis for Interactive Assistance (GAIA) plane. PROMETHEE is a multi-criteria analysis method based on pairwise comparisons and GAIA.

This model does not consider control ranking as a group decision problem in which the subjective and objective judgments must be available to achieve the accurate ranking of controls. The control weight and the preferred functions are identified by expert opinion prior to analysis. Cyber investment analysis methodology was proposed by Lianso [13]. A data-driven approach for selecting and prioritizing security controls was used as a framework in ranking the security controls, based on the dataset extracted from previous experiments and control effectiveness scoring. This methodology consists of multiple steps, prioritizing the controls based primarily on their effectiveness score. However, in setting the security controls, the weighting is computed according to expert opinion on security control capabilities, that is on expert observations on the effectiveness of controls. A clear classification of the dataset, which would indicate how the data are estimated and analyzed, is unavailable.

3.2 ISCP Model

The limitations of the existing risk assessment models were discussed in the previous sections. In general, the major limitation is the qualitative approach, which is unpopular with decision makers. Therefore, a quantitative approach, namely, the prioritization model, is proposed to improve the overall risk assessment process. The proposed model and its components are described in the succeeding paragraphs. The model aims to improve ISC assessment by analyzing multiple evaluation criteria, such as vulnerability, weakness, attack severity and cost of remediation effort of the organization. The model consists of three main stages, namely, (1) control aggregation, (2) control assessment, and (3) control analysis. The output of the control aggregation stage is a list of the evaluation criteria used to determine the value of the information assets, potential consequences and scope of the risk assessment activity. Similarly, the output of the control assessment stage is a real experiment with raw data driven from risk exposure, consisting of valid threats attaching to the identified vulnerabilities. The purpose of the last stage, control analysis, is to correlate all the findings, filter all the inputs, and validate the data into a readable view by applying MADM. These three stages can help organizations in selecting and analyzing appropriate controls for their IT resources. This model helps decision makers to select the most effective and most vulnerable controls in resource-constrained environments. Fig. 3 describes the three stages and the related steps of the ISCP model. The phases are discussed in the succeeding subsections.

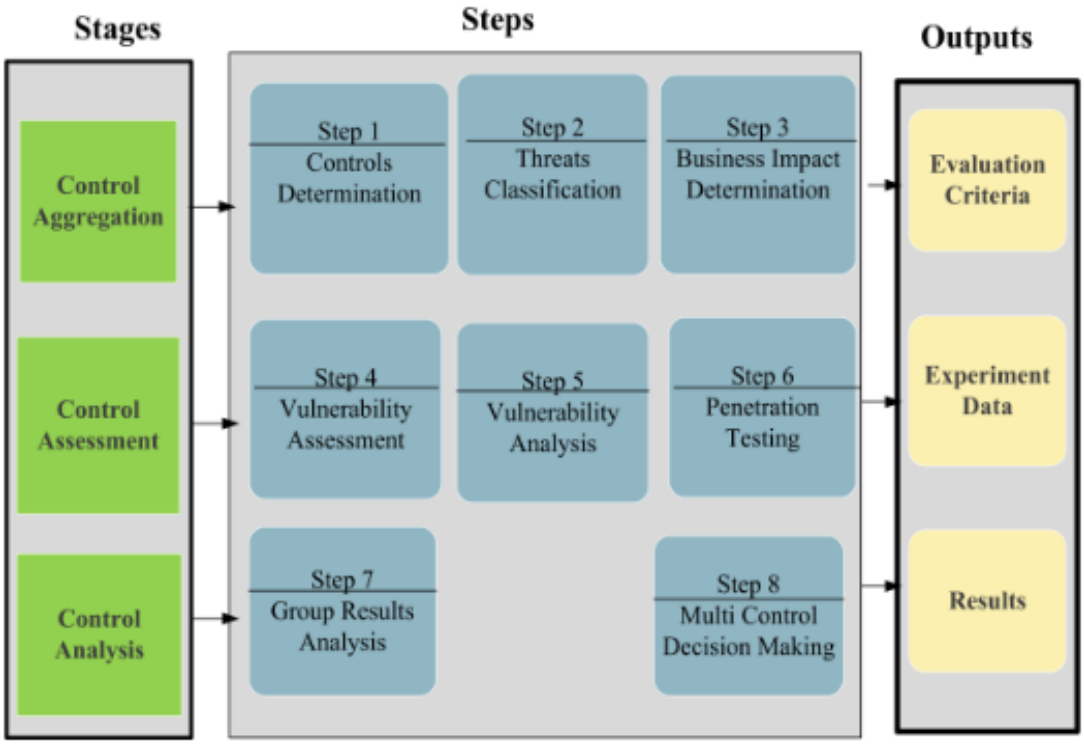

Fig. 3. ISCP model

A case study is used to demonstrate the ISCP model clearly. It was conducted in an SME in Kuala Lumpur, Malaysia, following the three stages of the prioritization model. This enterprise was an Internet security consulting company with fewer than 250 employees. A three-person internal audit team was responsible for risk assessment, and the organization complied with ISO 27001 and 27002 standards for conducting risk assessment.

3.2.1 Control Aggregation

This phase identified all the information regarding the security controls, such as test scope, threats aligned with controls and control evaluation criteria. Control aggregation consists of three steps, as follows:

A. Control Determination

The scope and infrastructure barriers of the security controls are determined, classified into technical and non-technical controls. Technical control is known as safeguards that are built into the hardware and software to mitigate risks. This model is primarily concerned with technical controls, such as routers, firewalls, wireless access points and servers.

B. Threat Classification

Table 1 shows the seven types of threat considered in the model [5]. These threats will be used for identifying the gaps of the current controls of the organization's infrastructure and for testing purposes. Each threat is described with the possible attacks. In this research, our test focused on the Web environment. The threat classification was adapted from the definition provided by the Web Application Security Consortium [30], which described threat classification as a cooperative effort to clarify and organize threats to website security.

C. Business Impact Determination

In this step, the degree of the threats for the affected controls were specified in terms of the following characteristics:

- Vulnerabilities: The total number of possible vulnerabilities that might damage the particular controls.
- Valid vulnerabilities: Vulnerabilities are not always weaknesses. Thus, the total number of weaknesses should be considered in evaluating the particular controls.
- Exploit attacks: The attack types and classification are the main factors considered in evaluating the particular controls (refer to Table 1 for more detail)
- Attack severity: Damage or consequences to the organization caused by the attacks are identified based on the DREAD criteria (damage potential, reproducibility, exploitability, affected users and discoverability) [31]. DREAD is a popular classification scheme for quantifying, comparing and prioritizing the attacks presented by each evaluated threat. Each category was divided into four levels to describe the level of attack: critical, high, medium and low. Each finding was assigned a composite severity score and the severity was calculated by adding each of the DREAD components, thereby producing a number between 1 and 50. Table 2 illustrates the severity scores
- Remediation effort level: The cost level of the remediation effort required to rectify the identified vulnerabilities was determined. The remediation levels were divided into three categories, namely, high, medium and low. Table 3 shows the cost remediation levels for the related threats.

3.2.2 Control Assessment

In this stage, a test was set up and data were collected for the particular controls. There are three steps, which are explained as follows:

A. Vulnerability Assessment

Vulnerability assessment is the process of identifying, quantifying and prioritizing known vulnerabilities to fix the threat, to prevent a compromise, or to apply a patch. Internal and external scans are performed to detect security vulnerabilities across the entire infrastructure before such vulnerabilities are exploited by an attacker. The entire completed assessment includes analysis of both internal and external threats and vulnerabilities.

B. Vulnerability Analysis

All redundant data from different vulnerability assessment tools are combined to create one formal result for all findings. The identified vulnerabilities were verified to minimize false positives, vulnerability duplication by different tools and errors during the test.

C. Penetration Testing

Penetration testing (also called pen testing) is the process of testing a computer system or network to find valid vulnerabilities that an attacker could exploit. Vulnerabilities are the greatest risks to the computing environment and penetration testing reveals risks that need priority fixing. The objectives depend on the type of pen test performed. Penetration testing has two types, namely, internal or external.

Table 1. Threat classification [5]

Class	Attacks
Authentication	"Brute Force, Insufficient Authentication, Weak Password Recovery, Validation Server Misconfiguration, Application Misconfiguration, Insufficient Password".
Authorization	"Credential/Session Prediction, Insufficient Authorization, Insufficient Session Expiration, Session Fixation, Eavesdropping, Command Authorization Bypass".
Client-side attacks	"Content Spoofing, Cross-site Scripting".
Command execution	"Buffer Overflow, Format String Attack, LDAP Injection, OS Command Injection, SQL Injection, SSI Injection, Xpath Injection, Improper Output Handling, Denial of Service".
Information disclosure	"Directory Indexing, Information Leakage, Path Traversal, Predictable Resource Location, Fingerprinting".
Logical attacks	"Abuse of Functionality, Insufficient Anti-automation, Insufficient Process Validation, Worms".
Insider attacks	"Transfer of Confidential Data, Access of Prohibited Content, Access to Isolated Sub-nets, Output Redirection".

Table 2. Severity score [31]

Severity rating	DREAD score	Risk description
Critical (7)	40 to 50	"A critical finding should be considered immediately for review and resolution. Exploitation of critical vulnerabilities is relatively easy and can lead directly to an attacker gaining privileged access (root or administrator) to the system. Findings with this risk rating pose risks that could negatively influence business operations or business continuity".
Severe (5)	25 to 39	"A severe finding should be considered for review and resolution within a short time frame. These vulnerabilities lead to an attacker gaining non-privileged access (standard user) to a system, or the vulnerability leveraged to gain elevated level of access".
Moderate (3)	11 to 24	"A moderate finding should be considered once the critical and severe findings have been addressed. These vulnerabilities leak sensitive data that an attacker can use to assist in the exploitation of other vulnerabilities. Moderate findings do not pose a substantial threat to business operations".
Low (1)	1 to 10	A low finding should not be considered a moderate risk to the business. These vulnerabilities are obscure and unlikely to be discovered

Table 3. Cost remediation effort score [31]

Effort rating	Cost description
High (5)	Significant multi-resource effort that may span over a considerable amount of time; requires a significant network architecture change or the purchase of additional security products
Moderate (3)	One to several days; requires moderate amount of resources
Low (1)	Less than a day; requires only a minimal amount of resources

3.2.3 Control Analysis

In the third stage, the model analyzes the data and makes recommendations to the decision makers. It consists of two steps:

A. Group Result Analysis

Result estimation focuses on analyzing the findings in varying degrees of detail depending on the criticality of controls and DREAD rating level. Given the availability of the resulting data, quantitative analysis methods were used, employing a scale with numerical values for both severity and remediation effort levels. The quality of the analysis depended on the accuracy and completeness of the numerical values, as well as the validity of the findings. The problem in gathering the data from the second stage was that team members usually had different opinions regarding

the results and the system rating, which resulted in subjective judgments. The results for each security control were analyzed and evaluated by four security experts for vulnerability assessment and by using the pen test to estimate the attack severity and the cost of remediation effort in mitigating these attacks. The attack severity and cost remediation effort scores were used to calculate the influence of the experimental data, as illustrated in Tables 2 and 3.

B. Multi-Control Decision Making

MADM was encountered in various situations, such as when a number of decision makers had several alternatives and when actions had to be selected based on a set of attributes [7]. MADM was conducted to prioritize and select the critical technical controls based on the estimation data of the group of experts. According to the type of information provided by the decision makers, MADM can be classified into: no information, information on the attribute and information on alternatives [7, 32]. Focus was on the type in which the decision makers provide information on the attribute. Therefore, the Technique for Order Performance by Similarity to Ideal Solution (TOPSIS) method was employed. In any multiple-attribute decision-making ranking, a number of fundamental terms, such as the Decision Matrix (DM), the Evaluation Matrix (EM), the alternatives and the criteria, have to be defined. EM consists of m alternatives and n criteria that have to be created. By considering the intersection of each alternative and criteria as x_{ij}, we obtain the matrix $(x_{ij})_{m*n}$:

$$D = \begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \dots & C_n \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{bmatrix} \end{array} \tag{1}$$

where, A_1, $A_2,\dots,A_m$ are possible alternatives from which decision makers have to choose (i.e. technical security controls); C_1, $C_2,\dots,C_n$ are criteria by which alternative performance is measured (i.e. vulnerability, threat, valid vulnerability, severity, cost remediation effort); and x_{ij} is the rating of the alternative A_i with respect to criterion C_j. W_j is the weight of criterion C_j and should thus be equal to 1. A number of processes, such as normalization, maximization indicator and adding the weights, must be performed to rank the alternatives.

4. TOPSIS Method

Step 1: Constructing the Normalized Decision Matrix

In this process, various attribute dimensions are transformed into non-dimensional attributes, thereby allowing a comparison across the attributes. The matrix $(x_{ij})_{m*n}$ is then normalized to the matrix $R = (r_{ij})_{m*n}$ using the normalization method:

$$r_{ij} = x_{ij} / \sqrt{\sum_{i=1}^{m} x_{ij}^2} \tag{2}$$

This process results in a new matrix R, where R is shown as follows:

$$R = \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ r_{21} & r_{22} & \dots & r_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ r_{m1} & r_{m2} & \dots & r_{mn} \end{bmatrix} \tag{3}$$

Step 2: Constructing the Weighted Normalized Decision Matrix

A set of weights $w = w_1, w_2, w_3,\dots,w_j,\dots w_n$ from the decision maker is accommodated in this process in order to normalize the decision matrix. Each column from the normalized decision matrix (R) can be multiplied by its associated weight w_j in order to get the resulting matrix. The following set of weights is equal to 1:

$$\sum_{j=1}^{m} w_j = 1 \tag{4}$$

This process would result in a new matrix V, where V is as follows:

$$V = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{bmatrix} = \begin{bmatrix} w_1 r_{11} & w_2 r_{12} & \cdots & w_n r_{1n} \\ w_1 r_{21} & w_2 r_{22} & \cdots & w_n r_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ w_1 r_{m1} & w_2 r_{m2} & \cdots & w_n r_{mn} \end{bmatrix} \quad (5)$$

Step 3: Determining the Ideal and Negative Ideal Solutions

Two artificial alternatives A^* (the ideal alternative) and A^- (the negative ideal alternative) are expressed as:

$$A^* = \left\{ \begin{pmatrix} \left(\max_i \max_i v_{ij} \mid j \in J \right), \\ \left(\min_i \min_i v_{ij} \mid j \in J^- \right) \mid i = 1,2,...,m \end{pmatrix} \right\} = \left\{ v_1^*, v_2^*, ..., v_j^*, Lv_n^* \right\} \quad (6)$$

$$A^- = \left\{ \begin{pmatrix} \left(\min_i \min_i v_{ij} \mid j \in J \right), \\ \left(\max_i \max_i v_{ij} \mid j \in J^- \right) \mid i = 1,2,...,m \end{pmatrix} \right\} = \left\{ v_1^-, v_2^-, ..., v_j^-, Lv_n^- \right\} \quad (7)$$

where J is a subset of $\{i = 1,2,\ldots,m\}$ that represents "the size, robustness and complexity". J^- is the complement set of J, noted as J^c, referring to the set of cost attributes.

Step 4: Separation Measurement Calculation Based on Euclidean Distance

Calculating the distance between each alternative in V and the ideal vector A^* using the Euclidean distance is given by:

$$S_{i^*} = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^* \right)^2}, \; i = (1,2,...m) \quad (8)$$

Likewise, the calculation of separation measurement for each alternative in V from the negative ideal A^- is given as:

$$S_{i^-} = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^- \right)^2}, \; i = (1,2,...m) \quad (9)$$

Eventually in Step 4, two values, namely, S_{i^*} and S_{i^-}, were counted for each alternative. These represent the distance of each alternative from the ideal.

Step 5: Ideal Solution Calculation Closeness

A_i closeness to the ideal solution A^* is calculated as:

$$C_{i^*} = S_{i^-} / \left(S_{i^-} + S_{i^*} \right), 0 < C_{i^*} < 1, \; i = (1,2,...m) \quad (10)$$

Where $C_{i^*} = 1$ once only ($A_i = A^*$). Then, $C_{i^*} = 0$ once ($A_i = A^-$).

Step 6: Alternatives Ranking based on Closeness to the Ideal Solution

Alternative A_i rank according to the descendant order of C_{i^*}; a higher value corresponds to better performance.

5. Results

This section shows the results obtained from a test conducted in the organization as specified in the section on the ISCP model. The paper only shows one case study testing the newly proposed ISCP model because in the risk assessment field, publishing results or data about an organization's position and assets is not encouraged, as they do not want to share confidential or sensitive information and the limited scope of the experiment. The prioritization model was employed in conducting the risk assessment for the organization. One of the researchers and a group of experts with more than 10 years of experience, who are certified ISMS lead auditors, were designated as risk assessors. The test was

conducted according to the phases of the model. First, the scope and infrastructure boundaries of the security controls were determined, categorized as technical or non-technical controls. This study evaluates the technical information security controls.

Stage 1: Control Aggregation

It is important to mention that all tests were conducted in a real network setting. First, 18 technical security controls were identified (as in Table 4). Then, the attacks were classified into more than seven classes based on the type of organization. Finally, the evaluation criteria have been identified earlier and summarized as shown in Table 4.

Table 4. Business Impact Criteria

Known vulnerabilities
Valid vulnerabilities
Attack class
Severity
Remediation effort level

Stage 2: Control Assessment

The goal of this stage is to test the strengths and weaknesses of the security controls. The research started with the first evaluation criterion, which identifies vulnerabilities as shown in Table 5.

Identified open source tools to determine the vulnerabilities for the technical controls has been utilized; Nessus, Nmap, Dumpsec, Kismet and Acunetix Web Vulnerability Scanner were used. Over 50 tests were conducted to identify the vulnerabilities according to the seven classes identified in Table 1. The researchers ran the assessment for all security

Table 5. Identified known vulnerabilities by Expert 1

No	Technical Security Controls
1	Router
2	Firewall
3	Web Application
4	Web server
5	DHCP Server
6	Active Directory
7	CCTV Server
8	File server
9	Antivirus Server
10	Database
11	Active Mail Server
12	Windows Update Server
13	Vmware ESX Server
14	Passive Mail Server
15	Wireless AP
16	E-mail Gateway
17	DNS
18	Development Server

controls and altogether 527 vulnerabilities were identified. Then based on the identified research classes, the team verified the attacks based on the technical control's type and function. Table 6 illustrates the attack classes used.

Table 6. Threat Classifications

Authentication
Authorization
Client-side attack
Command execution
Information disclosure
Logical Attacks
Insider Attacks

Stage 3: Control Analysis

In this stage, the attack severity, threat classes, along with the cost of remediation effort were evaluated, as shown in Tables 2 and 3. The data were validated prior to analysis to obtain accurate result estimations. Severity estimation assigns values to the consequences of a risk from low to critical. The estimation of cost and remediation effort were conducted through group analysis and expert evaluation. The last step in this stage is validating the vulnerabilities identified in the previous step, using penetration testing. The main objective of the penetration test is to demonstrate the impact of the encountered vulnerabilities, issues and risks. Then, over 100 tests were run using different penetration testing tools, Metasploit, AirSnort, Nstealth, Paros Proxy, ISS Database Scanner and Spike, to validate the data obtained from the vulnerability assessment. The results show fewer technical control vulnerabilities than in the findings identified in the first stage as shown in Table 7. Then the team ordered the output according to the classification of attacks exploiting the vulnerabilities. Attack classes were aligned and linked to each technical security control. Table 8 shows the output of the attack classes that directly exploit the findings or vulnerabilities and Table 9 shows Remediation Effort Level.

Table 7. Identified known vulnerabilities by Expert 1

Technical Security Controls	**Valid Vulnerabilities**	**Ranking**
Router	27	9
Firewall	3	18
Web Application	96	1
Web server	50	2
DHCP Server	25	10
Active Directory	23	13
CCTV Server	33	14
File server	27	8
Antivirus Server	28	6
Database	29	5
Active Mail Server	33	4
Windows Update Server	25	11
VMware ESX Server	41	3
Passive Mail Server	19	15
Wireless AP	4	17
E-mail Gateway	12	16
DNS	28	7
Development Server	24	12
Total	**527**	

Table 8. Identified valid vulnerabilities by Expert 1

Technical Security Controls	Valid Vulnerabilities	Ranking
Router	14	2
Firewall	2	16
Web Application	88	1
Web server	14	3
DHCP Server	5	11
Active Directory	5	9
CCTV Server	8	6
File server	5	12
Antivirus Server	5	8
Database	7	7
Active Mail Server	5	10
Windows Update Server	4	15
VMware ESX Server	8	5
Passive Mail Server	9	4
Wireless AP	1	17
E-mail Gateway	1	18
DNS	5	13
Development Server	5	14
Total	**191**	

Table 9. Attack Classes Results by Expert 1

Technical Security Controls	Authentic-ation	Authoriz-ation	Client-side attacks	Command Execution	Information Disclosure	Logical Attacks	Insider Attacks
Router	4	3	2	0	0	5	0
Firewall	2	0	0	0	0	0	0
Web Application	14	8	15	38	3	2	8
Web server	4	6	2	2	0	0	0
DHCP Server	0	4	0	0	1	0	0
Active Directory	0	4	0	0	1	0	0
CCTV Server	4	4	0	0	0	0	0
File server	1	4	0	0	0	0	0
Antivirus Server	3	2	0	0	0	0	0
Database	2	4	0	1	0	0	0
Active Mail Server	5	0	0	0	0	0	0
Windows Update Server	4	0	0	0	0	0	0
VMware ESX Server	3	0	4	1	0	0	0

Passive Mail Server	2	3	0	0	4	0	0
Wireless AP	1	0	0	0	0	0	0
E-mail Gateway	1	0	0	0	0	0	0
DNS	0	4	0	0	1	0	0
Development Server	2	1	2	2	0	0	0

Table 10. Remediation Effort Level Results of Expert 1

Technical Security Controls	Critical	High	Moderate	Ranking
Router	0	8	5	4
Firewall	0	0	0	17
Web application	3	80	4	1
Web server	4	7	1	2
DHCP server	0	4	0	14
Active directory	0	4	0	13
CCTV server	0	7	0	9
File server	0	4	0	15
Anti-virus server	0	4	0	12
Database	0	6	0	10
Active mail server	0	2	1	7
Windows update server	0	3	0	16
VMware ESX server	2	5	0	3
Passive mail server	0	8	0	8
wireless AP	1	0	0	6
Email gateway	0	1	0	18
DNS	1	3	0	5
Development server	0	5	0	11

Table 11. Ranking Summary of Expert 1

Technical Security Controls	Known Vulnerabilities	Valid Vulnerabilities	Attack Class	Severity	Remediation Effort level	Ranking
Router	9	2	2	2	4	2
Firewall	18	16	16	17	17	17
Web application	1	1	1	1	1	1
Web server	2	3	4	8	2	2
DHCP server	10	11	6	14	14	11
Active directory	13	9	7	13	13	14
CCTV server	14	6	5	9	9	8
File server	8	12	10	11	15	14
Anti-virus server	6	8	11	12	12	12
Database	5	7	9	4	10	4
Active mail server	4	10	8	16	7	9
Windows update server	11	15	15	15	16	16
VMware ESX server	3	5	14	10	3	6
Passive mail server	15	4	3	3	8	5
Wireless AP	17	17	17	7	6	15
Email gateway	16	18	18	18	18	18
DNS	7	13	12	6	5	7
Development server	12	14	13	5	11	10

Finally, the results were analyzed by the TOPSIS method to achieve data prioritization. TOPSIS was programmed with Java to automate the analysis process. The resulting data were analyzed to rank the results and identify the vulnerable technical controls based on the evaluation criteria. Security controls were rated on a scale of 1 to 18 based on the maximum number of security controls, with 1 denoting the most critical risk and 18 denoting the lowest. The top eight critical risks of ISC to the organization were then selected. To validate and evaluate the proposed model, the researchers have compared the results of the proposed model with the ISO/IEC 27005 risk management method in similar scope. The ISO/IEC 27005 risk assessment method was chosen because not only is it applicable to all types of organization, but also the risk assessment process that would be the same for all other ISRA models. However, it was soon realized that a comparison of these results would be inconclusive because there was very little difference between the scopes of this methods and approaches. As a result, four experts from different reputable organizations who have experience in the field of ISRA were interviewed to evaluate the current behaviours of the proposed model compared to ISO/IEC 27005. This study had already investigated the challenges and shortcomings of the ISO/IEC 27005 risk assessment (see section 2 above). The success measurements factor such as risk assessment time, cost, uncertainty, and usefulness were used in the comparison between the ISCP model and ISO/IEC 27005 method, as shown in Table 13. The comparison results were examined based on the rating score (low, medium, high) [31]. The results of these scores for the ISCP model factors were revealed from the experts' feedback during the interviews in order to assess the effectiveness of the ISCP model.

Table 12. Ranking Summary of Expert 1

Technical Security Controls	Expert 1	Expert 2	Expert 3	Expert 4	Ranking
Router	2	3	3	2	2
Firewall	17	17	18	17	17
Web application	1	1	1	1	1
Web server	2	2	2	3	2
DHCP server	11	11	7	10	9
Active directory	14	13	11	9	12
CCTV server	8	8	6	5	7
File server	14	14	9	15	13
Anti-virus server	12	12	13	11	12
Database	4	4	4	8	5
Active mail server	9	9	15	7	10
Windows update server	16	16	14	14	15
VMware ESX server	6	6	5	4	5
Passive mail server	5	5	8	6	6
Wireless AP	15	15	16	18	16
Email gateway	18	18	17	16	17
DNS	7	**7**	10	12	9
Development server	10	**10**	12	13	12

Table 13. Comparison between ISO/IEC 27005 and the ISCP model

Factor	ISO/IEC 27005 method	ISCP model
Assessment time	High	Low
Assessment cost	High	Low
Uncertainty	Medium	Low
Usefulness	Medium	High

6. Discussion

It is important to mention that we have reported the result for the first expert in details, but the rest of the experts are summarized in Table 12. As previously stated, inaccurate selection and evaluation of ISC can result in inaccurate risk assessment. The ISCP model helps decision makers to decide which controls are critical or important and which threats to consider. The model was used to improve the risk assessment and achieve effective security decision making. Aside from risk assessment, understanding the critical security controls in an organization is important for other reasons. During the group analysis of the data, the experts had different opinions, so the results had to be compared again with TOPSIS (see Table 12). The table lists critical security controls which indicate that that the Web application had to be addressed with the highest priority, followed by the router, the Web server, the VMware ESX server, the Passive Mail server, the database, the CCTV server and the DHCP server. These controls were evaluated for the known vulnerabilities with different evaluation criteria, such as cost of remediation effort. Then the controls for each criterion were ranked using TOPSIS, as were the data estimated by the experts.

Findings shows that firewall and wireless AP were considered as significant controls in the organization, suggesting that firewalls are most effective in countering attacks. Although there are several ISRA methods, there are some shortcomings and challenges. The ISCP model used the TOPSIS method to prioritize selection among all the results; however, the weighting steps within TOPSIS were unable to accommodate all the controls because of the lack of a benchmark for the importance of these assets to all organizations. In this study, the researchers had to set an equal weight and let the organization choose the best weight for the threats based on the criticality of the controls. The authors intended to compare the results of the case study with previous case study of risk assessment of similar scope.

However, it was soon realized that a comparison of these results would be inconclusive because there was very little difference between the methods and approach in the two scenarios. Although there are many ISRA methods, the literature reveals a lack of sufficient research focusing on developing or enhancing these existing methods [7, 32]]. The scores for the ISCP model factors were revealed from the feedback of the group of experts and the literature review, based on the rating score (low, medium, high). The ISCP model was compared with the ISO 27005 risk assessment method to measure its performance. The results showed better performance, as the ISCP model dramatically reduced the risk assessment time, cost and uncertainty. In contrast, the usefulness parameter of the proposed model increased.

7. Conclusion

The control assessment method is a vital step in information security risk management, providing continuous defense against threats. A limited number of researchers have studied risk assessment methods, and to gain further insight the present research has identified and clarified issues and challenges to existing methods. The current frameworks and methodologies do not give sufficient practical details on how to select and evaluate ISC. Furthermore, the assessment process requires that resource protection be conducted by the organization, which is difficult to realize with a limited budget and expertise. The proposed model enhances the risk assessment process through a multi- and dynamic evaluation model that assists organizations in evaluating ISC accurately. The model enables good security decision making throughout by considering the weight of each criterion in the organization. It helps the organization to identify only the critical vulnerable controls that need to be managed, and to identify the most effective or better-performing of all these security controls.

In future, the data will be run using different multi-attribute decision-making methods, the results from this study compared with those from other methods to determine the most effective method. The model will be evaluated by expert's similar industries to the organization in question.

Acknowledgements

The authors thank the ISRA group of experts and MPDSS community for their valuable contribution to reviewing and evaluating this result. The Multi-Purpose Decision-Support System is a free simulation of Individual and Group Multi-Criteria Decision-Making techniques.

REFRENCES:

[1] ISO/IEC, "ISO 27005 information technology security techniques information security risk management.," 2008.

[2] H. Van der Haar and R. Von Solms, "A model for deriving information security control attribute profiles," *Computers & Security,* vol. 22, pp. 233-244, 2003.

[3] E. Wheeler, "Building an Information Security Risk Management Program from the Ground Up," *Wheeler, Ed. Waltham,* 2011.

[4] L. A. Gordon and M. P. Loeb, "Budgeting process for information security expenditures," *Communications of the ACM,* vol. 49, pp. 121-125, 2006.

[5] A. Singh and D. Lilja, "Improving risk assessment methodology: a statistical design of experiments approach," in *Proceedings of the 2nd international conference on Security of information and networks*, 2009, pp. 21-29.

[6] EBIOS. (2004). *Expression of needs and identification of security objectives*.

[7] C. Kahraman and S. Çebı, "A new multi-attribute decision making method: Hierarchical fuzzy axiomatic design," *Expert Systems with Applications,* vol. 36, pp. 4848-4861, 2009.

[8] S. Lauesen and H. Younessi, "Six Styles for Usability Requirements," in *REFSQ*, 1998, pp. 155-166.

[9] C. Andersen, "Successful security control selection using NIST SP 800-53," *ISSA I*, vol. 1, pp. 12-17, 2009.
[10] ITGI, "COBIT4.1. IT Governance Institute (ISACA)," *Rolling Meadows, USA*, 2010.
[11] N. Feng and M. Li, "An information systems security risk assessment model under uncertain environment," *Applied Soft Computing*, vol. 11, pp. 4332-4340, 2011.
[12] A. Ekelhart, S. Fenz, and T. Neubauer, "Aurum: A framework for information security risk management," in *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*, 2009, pp. 1-10.
[13] T. Llansó, "CIAM: A data-driven approach for selecting and prioritizing security controls," in *Systems Conference (SysCon), 2012 IEEE International*, 2012, pp. 1-8.
[14] M. I. Fofana, "e-Government Technical Security Controls Taxonomy for Information Assurance Contractors-A Relational Approach," 2010.
[15] A. R. Otero, C. E. Otero, and A. Qureshi, "A multi-criteria evaluation of information security controls using boolean features," *International Journal of etwprk Security & its application (IJNSA)*, vol. 2, 2010.
[16] J. Jones, "An introduction to factor analysis of information risk (fair)," *Norwich Journal of Information Assurance*, vol. 2, p. 67, 2006.
[17] J. Breier and L. Hudec, "Risk analysis supported by information security metrics," in *Proceedings of the 12th International Conference on Computer Systems and Technologies*, 2011, pp. 393-398.
[18] ENISA, "Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools," *Technical Department of ENISA Section Risk Management, ENISA, Paris, France*, 2006.
[19] G. Stoneburner, A. Goguen and A. Feringa, "Risk management guide for information technology systems," *Technical Report, Department of Commerce, National Institute of Standards and Technology Gaithersburg, NIST Special Publication 800-30, MD, USA*, 2002.
[20] J. Allen, "Mastering the risk/reward equation: Optimizing information risks to maximize business innovation rewards," USA2008.
[21] C. J. Alberts, A. J. Dorofee, and J. H. Allen, "OCTAVE Catalog of Practices, Version 2.0," Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst2001.
[22] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST2003.
[23] A. Asosheh, B. Dehmoubed, and A. Khani, "A new quantitative approach for information security risk assessment," in *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, 2009, pp. 222-227.
[24] A. Singh, "Improving information security risk management," 2009.
[25] A. Phyo and S. Furnell, "A detection-oriented classification of insider it misuse," in *Third Security Conference*, 2004.
[26] D. W. Hubbard, *The failure of risk management: Why it's broken and how to fix it*: John Wiley & Sons, 2009.
[27] M. S. B. Mahmoud, N. Larrieu, and A. Pirovano, "A risk propagation based quantitative assessment methodology for network security-aeronautical network case study," in *Network and Information Systems Security (SAR-SSI), 2011 Conference on*, 2011, pp. 1-9.
[28] R. L. Plackett and J. P. Burman, "The design of optimum multifactorial experiments," *Biometrika*, vol. 33, pp. 305-325, 1946.
[29] J.-J. Lv, Y.-S. Zhou, and Y.-Z. Wang, "A multi-criteria evaluation method of information security controls," in *Computational Sciences and Optimization (CSO), 2011 Fourth International Joint Conference on*, 2011, pp. 190-194.
[30] WASC, "WASC threat classification," *Web Application Security Consortium.* , 2010.
[31] J. Meier, A. Mackman, and B. Wastell, "Threat modeling web applications," *Microsoft Corporation*, pp. 05-2005, 2005.

[32] G.-H. Tzeng and J.-J. Huang, *Multiple attribute decision making: methods and applications*: CRC press, 2011.

Nadher Al-safwani received his PhD in computer science in Risk Assessment from University Utara Malaysia. He currently serves as the Cybersecurity consultant in ITU Arab Regional Cybersecurity Center in Oman (ITU-ARCC). Prior joining ITU-ARCC, he was working as Manager Security Assurance in IMPACT (Malaysia). In his previous work in IMPACT. Dr. Nadher was involving with many projects and services worldwide such as establishment and assessments of CIRT and improving the cybersecurity security posture. He was responsible for the deployment of security assurance products and services that are specifically dedicated to enabling better information security readiness for public sector agencies and industry. Dr. Nadher was actively involved in various IT programmes, amongst; IT security compliance program, cybersecurity training and awareness programme, and CIRT capability assessment. He also successfully orchestrated the setting up the IT security facilities, developed excellent capability in cybersecurity and computer network communications for different projects. In his current capacity in ITU-ARCC, he is responsible to provide assistance to Arab member states on cybersecurity. To date, he actively participated in national cybersecurity strategy (NCS) and critical information infrastructure protection (CNIIP).

Yousef Fazea received his B.S. and M.S. degrees, in Information Technology from the Universiti Utara Malaysia, in 2010 and the Ph.D degree in Computer Science from School of Computing, Universiti Utara Malaysia in 2017. Dr. Fazea during his study, awarded a postgraduate scholarship from Universiti Utara Malaysia and honors by the college of Arts and Sciences Dean as a second runner-up in the 3-minutes thesis competition (3MT). He is a member of IEEE and actively involved in IEEE activities, also was an executive member of the student chapter for two consecutive terms. In addition, he is a member of IAES, IAENG and ISOC Malaysia chapter. Dr. Fazea has published more than 18 scientific papers and served on the Editorial Board of Optical Engineering (OE), Journal of Electrical Systems and Information Technology – Elsevier (JESIT), and many international conferences. Dr. Fazea current area of research focuses on the enabling technologies such as SDM, MDM, WDM, FSO, Ro-FSO, fabrications of FMF as a sensor, and Future Internet infrastructure.

Huda Ibrahim received her Ph.D. in System Science and Management (2006) from Universiti Kebangsaan Malaysia, Master of Computer System and Computer Management (1995) from Creighton University, Omaha, Nebraska, USA, and B.A. in Mathematics (1988) from University of Arkansas at Little Rock, Arkansas, USA. She is a professor, Assistant Vice Chancellor under the College of Arts and Sciences and also a Dean of School of computing at Universiti Utara Malaysia (UUM) since July 2011. She has a vast knowledge and teaching areas are Information Technology, System Analysis, and Design, Information System Development, and Mathematics. She has been actively involved in research, consultation and publication as well as has led a few national research grants and university's research grants. Three of her research projects have received bronze medal in Malaysian Technology Expo (MTE); Portal Desa: A Collaboration of Institution of Higher Learning in Telecentre Implementation' in MTE 2013, 'Automated Data Updating Among Heterogeneous Systems on Cloud Computing' and 'An Ethical Cyber Cafe Model' in MTE 2012. Another project 'An Ethical Framework of Cyber Cafe Usage in Malaysia' has won a bronze medal in Ekspo lnovasi Islam 2011 (1-lnova 2011). She has also been honored as a keynote speaker and invited speaker at conferences in Bali, Indonesia (ICNABU 2017), Thailand (INCIT 2016), Malaysia (COMSET 2015, MSIS SIGISDC 2013, and MTCP-MRRD-CIRDAP 2013), Indonesia (SAINTIKS 2014 and ICoApICT 2013). She is also currently a member of IEEE, ACM, AIS, Malaysia Chapter
of AIS (MyAIS), and MNCC.