A Network Service-Based Risk Assessment Model with Case Study on an Educational Organization *

Islam Amro **

* Recieved: 20/9/2014 , Accepted: 22/11/2014.

** Information Technology and Communication Center, Al-Quds Open University, Palestine.

نموذج تقويم مخاطر شبكات الاتصال بالاعتماد
على طبيعة خدمات الشبكة وتطبيق النموذج على الشبكات التعليمية

ملخص:

تهدف الدراسة إلى تقويم مخاطر أنظمة المعلومات المحوسبة في مؤسسات لا تحتوي على أسس مرجعية لتقويم المخاطر. تبدأ الدراسة بتحديد الإطار المفاهيمي للخدمات التي تقدمها المؤسسة، يؤدي هذا الإطار دور البديل للأسس المرجعية التي يعتمد عليها تقويم المخاطر في أية مؤسسة، حيث تكون هذه الأسس المرجعية المكون الأساس في استراتيجية أمن المعلومات للمؤسسة. ونظراً لعدم وجود هذه الاستراتيجية في كثير من الأحيان تبرز مشكلة تقويم المخاطر. ومن هنا يعمل هذا البحث على إيجاد مقاربة لاحتساب هذه المخاطر بالاعتماد على طبيعة الخدمات المقدمة بالشبكة في حال عدم وجود استراتيجية وأمن المعلومات، حيث يتم ذلك من خلال ربطها بإطار مفاهيمي ناتج عن طبيعة الخدمات التي تقدمها المؤسسة. وتحدَّد هذه الخدمات ضمن مجموعات عمل رئيسة مثل خدمات أكاديمية أو خدمات بحثية إلخ، يتم تصنيف مجموعات العمل الرئيسة تحت عنوان: خدمات الشبكة، ومن ثم نأخذ كل خدمة على حدة، ونقوم بتحديد الأجهزة والخوادم المضطلعة بتقديم هذه الخدمة، وفي حال معرفة قيمة الضعف الأمني على كل جهاز، نستطيع تحديد الضعف الأمني للخدمة الواحدة، وفي حال تحديد الضعف الأمني للخدمة الواحدة نستطيع تحديد الضعف الامني لجميع الخدمات المقدمة على الشبكة وفق آلية محددة. وفي حال معرفة قيمة الضعف الأمني للشبكة ككل نستطيع احتساب المخاطر على المستوى العام، وتحديد قراءة تمثل نسبة المخاطرة العامة على الشبكة. هذه القراءة تؤسس لتقديم قيمة للمخاطرة على الشبكة دون وجود وثيقة استراتيجية أمنية، وفي إطار منهج البحث وعلى مستوى الخدمات المقدمة، قمنا ببناء نموذج احتمالي لحدوث المخاطر، إضافة إلى نموذج يحدد تأثير المخاطر في حال حدوثها. كما قمنا بتحديد أوزان المخاطر باستخدام عداد (بوردا) مع تحديد آلية رياضية لتقدير المخاطر الكلية. يتناول البحث آلية محددة خطوة بخطوة لبناء منظومة مخاطر متكاملة. وقد اُستخدمت شبكة جامعة القدس المفتوحة كبيئة لاختبار هذه المقاربة، مع الأخذ بعين الاعتبار أن هذه الشبكة المذكورة شبكة أكاديمية تعليمية. وبذلك يكون البحث قدم آلية مفصلة حول احتساب المخاطر للشبكات المشابهة من حيث طبيعة الخدمات المقدمة، وهي الخدمات التعليمية.

Abstract:

This paper addresses risk assessment in organizations lacking benchmarking and risk assessment references. We started with a strategic conceptualization of information technology services that an organization depends on, these services were seen as network services that are redistributed into basic service elements; these service elements are expressed in terms of hosts running these services and their interconnections. Eventually; we were able to express strategic services' vulnerabilities in terms of host vulnerabilities. Closing this gap led us to construct a risk reference for the organizational strategic services. Using relevant information about these vulnerabilities we were able to introduce a risk probability model, a risk impact model and a risk weighting approach using Borda Count. We followed a step-by-step approach to build the risk with a holistic view. We implemented the suggested model on Al-Quds Open University's (QOU) IT infrastructure as a case study and we were able to derive the strategic services' risks and the overall organizational IT risk.

Keywords- Risk Assessment, Vulnerability Management, Information Security, Business Continuity, Borda Count.

1. Introduction:

Information systems risk assessment is becoming more and more a vital issue within information systems lifecycle. A key problem in risk assessment rises from the lack of organizational benchmarks and references in order to assess the overall information system's risk. Therefore organizations tend to go through vulnerability management rather than going over risk assessment. Depending on ISO/IEC IS 13335-1 and ISO 27001, the essential concepts of IT security Risk, namely: asset, threat and Vulnerability. Assets refers to anything that has value to the organization, in the context of information systems; an asset might be tangible or intangible components, it can be hardware, software, data or infrastructure, it can also be products, knowledge, customer relations or reputation. These Assets are expressed in term of their values, their values are determined by the impact they have on business continuity or opportunities, and the determination of these values consequences defines the "impact assessment". The second concept is threat; it identified any action or event causes harm, which might be environmental, organizational, human error, technical failure or deliberate acts as in hacking, phishing, fraud, malicious codes. The last concept is the concept of Vulnerability which expresses the weakness of the asset, which can exist in all parts of a system, this can be categorized into physical, Logical or network. In the light of the previous three terms, the IT security risk identified as a potential events that a threat will meet vulnerability in a asset to harm an organization. Therefore, these risks have to be assessed and managed.

Risk assessment focuses on acquiring a snap shot of the current system risks; this is done through threat identification, threat characterization which is specifying the impact on assets, exposure assessment which places vulnerabilities of a certain asset and risk characterization which is identifying risks impact on business. The risk assessment founds for the concept of risk management, which is the process of taking actions against these risks after being assessed, these actions might be risk treatment, acceptance and/or communication. Risk treatment is the process of implementing controls to mitigate, transfer, avoid and/or eliminate risks. Incase of risk treatment is not feasible; it might be accepted, but the risk acceptance is never a technical decision, it should obtain management level approval after being well demonstrated. [1]

Based on previous concepts; several standards and frameworks were identified for information systems risk assessment and/or risk management, such as the Austrian security handbook, Dutch A&K Analysis, Ebios, ISO/IEC 13335-2, ISO/IEC IS 17799, ISO 270001, IT Grundshutz, Mehari. [2]

There are two key problems in using these frameworks:

A. First is how to integrate the information security risks as a business risk for nontechnical people.

B. Second is how to calculate the framework parameters.

On Problem A, the risk assessment frameworks exploited several methods to express business risks according to technical risks, and this integration might be on business strategic level as in [3] that provides a model to observe the differences in executive responses to cyber threats and risk assessments. Risk Assessment might be business domain specific as in [4] which addresses cloud computing, we can see that business terms are dominating the risk assessment terms. In [5], the research addresses a similar problem for IT services outsourcing, which expresses the difficulties incorporated with ICT outsourcing and discusses approaches for risk identification, analysis, treatment plans, implementations, monitoring and control when technical issues of business environment are reflected in Service Levels Agreements (SLA) rather than infrastructures. In reference [6], the impact of institutional structure conjunctions with technology-based security systems in information security tools and fault-tolerant control. Risk Assessment might depend on the technology architecture as well, for the case of Service Oriented Architecture (SOA), in [7] a specific risk model is suggested for SOA. Giving a deep look into this model we find it is very similar to conventional risk models which are based on risk probability and the value of the assets. The true value of this research from our point of view is its focus on the business components of the SOA, Risk Assessment for the case of web services built over multiple applications SOA if found in [8], A similar work concept to [9] was found in [10], and the maturity measures risk assessment for SOA can be found [11], this reference addresses covering the services components inclusion in the risk assessment process and how to test is ability to cover the aspects covered by services and assign proper weights to them. Where reference [12] discusses how to integrate business analysis risk with IT security Risk, it suggests an approach to classify services according to strategic services of an organization.

On problem B which is how to calculate the framework parameters, all of the previous methods such as ISO/IEC 13335-2, ISO/IEC IS 17799, ISO 270001 would still require a certain mechanisms for quantitative risk assessment, estimating the values of assess values, risk impact and is a set of questionnaires found in security plans for organization [1]. Unfortunately; security plan that doesn’t exist for a broad range of organizations [3], the importance of this plan that it is the meeting point between the business and the technical terms, for this kind of organizations we see that concept of risk management is reproduced in technical terms into Vulnerability management due to dependence on commercial tools to manage risk and vulnerability. Although vulnerability management is very important, it is governed by the values of vulnerability over a given set of hosts only, it doesn’t help in the containment according to asset values and risk probabilities, and these are the key issues for business sustainability rather than the vulnerability values itself. The key problem of risk assessment from previous terms arises from specifying assets values, risk probability and risk impact, and how to exploit these values in any risk assessment and or/management framework. And after specifying these values we have to reflect them into business terms.

The problem of probability calculation and impact assessment was addressed using several approaches . A interesting work we found in [9], where a multi stage procedural approach were followed in estimating risk probability, impact and weights for. In [14] a heuristic neural network method were used to optimize weights obtained from an adaptive hierarchical process, this issue included extensive calculations for the weights of risk assets which we do not think risk assessment should go through due to the dynamic nature of risks. The same problems of extensive calculations can be found in [14]. Although building a risk model on a specific technical framework as in [7] might be useful, it might be a repetition of the classic problem that risk models should be built on business models rather than being built on technical models. In [7] a specific risk model is suggested for a Service Oriented Architecture (SOA). Additional of work is found in Paper [15] which used the Borda count in giving weights to risks after building business risk elements.

in order to build a proper risk assessment and containment plan as in know frameworks or Information Security Management System (ISMS), three documents should be referenced (Business Strategy, IT strategy and Security Strategy), these documents are essential to assess the values related to risk, which is the Business Assists, the Assets Values and the related impacts on business. Unfortunately many organizations have no IT strategy or no Security Strategy or even both. We will still need organizational references to assess the values of our assets. Although the technical information's related to vulnerabilities are available. In addition to this the calculation of risk model has to be quantified.

This this paper we work on building a risk assessment model for networks that has vulnerability values only, without having referencing documents that is essential for calculating risk values and impacts, the following section we explain our problem, then we relate it to the literature we used, the section discusses the research problem and methodology, section 3 discusses Network Service-Based Risk Assessment Model we are proposing, it explains the roadmap for building the model components, its organized into several steps, the first step, we build the Testing environment, which is the network we based our simulation on, and then we work on Vulnerability Calculation Model , then we explain the method we used in Risk Probability and Risk Impact Estimation, then we work on the Determination of the Risk Rank Reference, after the we determine the risk rank , we calculate Risk Weight Estimation, this will be used in the Overall Risk Calculation, then we give a final flow chart summary for a step-by-step summary flowchart on how to exploit this approach for similar networks. In section 4 we implement our model into a testing environment as a case study, we go over the steps of section 3 one by one and generate the risk of an educational organization, then we conclude our research as a finalization.

2. Research Problem and Solution Methodology:

in order to build a proper risk assessment and containment plan as in know frameworks or Information Security Management System (ISMS), three documents should be referenced (Business Strategy, IT strategy and Security Strategy), these documents are essential to assess the values related to risk, which is the Business Assists, the Assets Values and the related impacts on business. Unfortunately many organizations have no IT strategy or no Security Strategy or even both. We will still need organizational references to assess the values of our assets. Although the technical information's related to vulnerabilities are available. In addition to this the calculation of risk model has to be quantified. In this research we address the following problems:

A. How to build a network services risk assessment model without that reflects Business levels strategies without having It Strategy or Security Strategy.

B. How to create a certain composition between Business strategies and information system components and infrastructure components that provides strategic services.

C. How to exploit system vulnerability information to generate a risk model and avoid heuristic calculations.

D. Introduce a simpler adaptive approach for risk probability and impact calculation.

E. Integrate the previous concepts into a functioning model that can generate the overall risk that might be used in any ISMS.

The essential need for IT strategy and Security for building a risk assessment model is explained in references like [1],[4],[5],[6].these references addresses the importance of expressing technical terms into business terms, and we work in our research to derive the risk assessment model based on business terms similar to approach in [4] but using educational organizations as a reference environment. We used the concepts found [7], [8], [12] used to express the organizational business strategies in term of services of SOA, we adapted these concept in expressing business strategies in term of information systems services and infrastructure services which is not an SOA, we used a combination of infrastructure components and information systems resources "which we can measure its vulnerability" in expressing them into services, then reflect these services on the business strategies. This is how we overcome the problem of not having an IT strategy and a security strategy stated in A and B. And in the following sections we explain how we achieved the rest of the points.

The research methodology followed following steps explain in the following section (section 3), the first step, we build the Testing environment, which is the network we based our simulation on, and then we work on Vulnerability Calculation Model , then we explain the method we used in Risk Probability and Risk Impact Estimation, then we work on the Determination of the Risk Rank Reference, after the we determine the risk rank , we calculate Risk Weight Estimation, this will be used in the Overall Risk Calculation, then we give a final flow chart summary for a step-by-step summary flowchart on how to exploit this approach for similar networks.

3. Network Service-Based Risk Assessment Model:

A. Testing environment:

Suppose we have a computer network for an academic organization as represented in Figure 1. The figure suggests a topology based representation for the network which has one broadcasting domain around its central switch and protected behind a firewall. The network can be accessed through two router ports, one is internal and the other is external. The routers represent a separation point between the routing domain and the broadcasting domain.

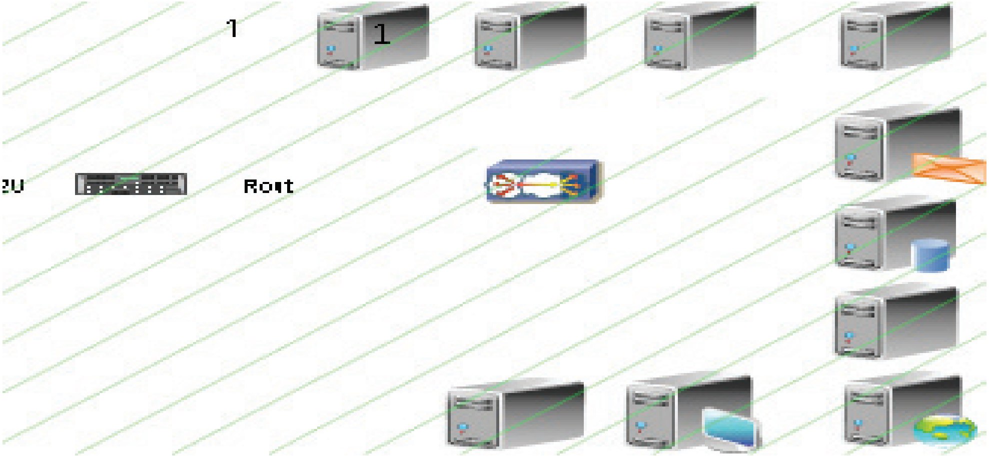


Figure (1)

Proposed Organization of the Academic Network

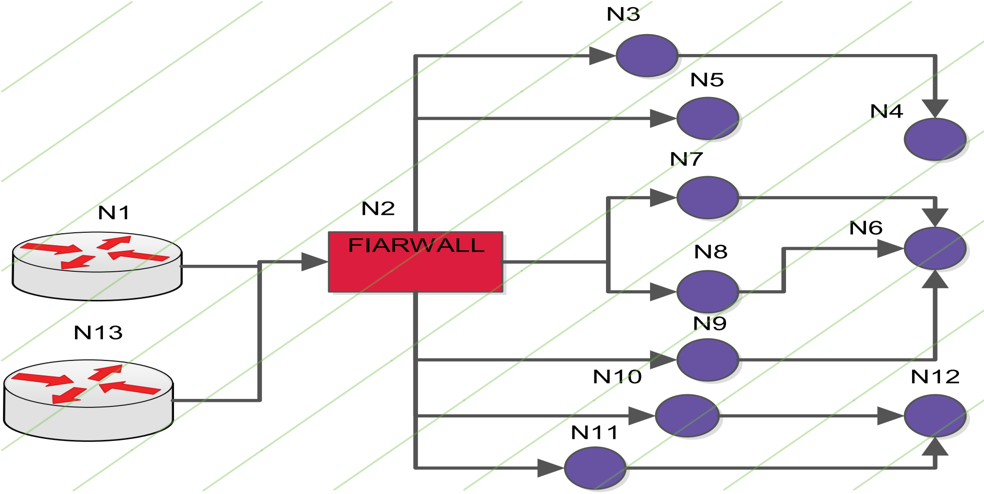


Figure (2)

Network Graph Configuration

Figure 2 represents the configuration of the same network as a graph representation. Each node represents the hosting machine(s) for the provided services over the network. Each node N is associated with a vulnerability vector V, this vector is calculated using Qualys Vulnerability Assessment Tool [16]. The vulnerability number for each node represents the average of vulnerabilities for this host. The problem with this number is that it comes with a high dimension vector that varies in its norm after each scan, and the rating of each vulnerability is given according to Qualys Standard which is beyond the scope of this paper. However; for the nodes from 1 to 12 in figure 2 the vulnerabilities were (2, 3, 4, 1, 3, 4, 3, 2, 4, 3, 4, and 3) respectively. Table 2 maps service elements with corresponding nodes (i.e. the service path scenarios based on the network predefined access plan).

Suppose that we have the following strategic items that we would like to investigate and asses their risk, these strategic services are running on the mentioned network in figure 1. These services are seen in table 1

Table (1)

BUSINESS RISK ITEM

Risk Item	Description
Students Electronic Services (S1)	Includes students management system, online academic services, students personal profiles
Academic Systems (S2)	Registration systems, class scheduling, tutor scheduling, students' academic records.
Human Resource Systems (S3)	University personal self-services, human resources information.
Financial Systems (S4)	Payroll, Budgeting, back office financial systems, students grants, student loans.
Research Systems (S5)	Lab applications, Lab inventory, journal systems, library.
Infrastructure Components (S6)	Systems infrastructural components, IT systems services, Mail systems, web servers, database engines

Table 1 represents the network service level, below in table 2 we explain the hosts and the network paths running these services mentioned in table 1.

Table (2)

SERVICE PATH ACCESS SCENARIOS

Element	Service Elements	Related Nodes
1	E-larning	N1,N12,N2,N3,N4
2	MAIL	N1,N12,N2,N5
3	Registration and Student portal	N1,N2,N12N7,N6
4	HR portal	N1,N12,N2,N8,N6
5	Financial system	N1,N2,N9,N6
6	Journals portal	N1,N2,N10,N12
7	Library portal	N1,N12N2,N11,N12
8	Infrastructure	All Nodes

To express the strategic services in term of hosts, we need to incorporate Table 1 and Table 2 by mapping service elements into a higher level for business related purposes since risks are addressed on a higher level of the servers and other connectivity issues. Table 3 maps the major risk items that we have identified in Table 1 (S1 to S6) with service elements. It is worth mentioning that this issue is a network-scenario specific and it might vary from one network to another. And the same approach afterwards can be followed to build this distribution of network services over an arbitrary network.

Table (3)

SERVICE ELEMENTS INCORPOTATION WITH RISK ELEMENT

Risk Item	Service Elements
Student electronic Services (S1)	Mail, e-Learning, registration and student portal, Library portal
Academic Systems (S2)	Mail, e-learning, registration and student portal, Library portal, Journal System
Human Resource Systems(S3)	Mail, HR Portal.
Financial Systems (S4)	Financial system, HR Portal
Research Systems(S5)	Library portal, Journal System
Infrastructure Components(S6)	All Service Elements in table 1.

From table 3 we were able to express strategic services in term of its incorporated hosts, for example S4 service is dependant of the nodes of finical system and HR portal, its vulnerability value is calculates using the nodes N1,N12,N2,N8 and N9 found in table 2 and so on.

B. Vulnerability Calculation Model:

Vulnerability management tools work on the host level. This level of representation does not provide an indication about business risk level. Suppose we have N nodes in our network configuration as seen in figure 2; incorporating these nodes forms a set of network services. These services are categorized into service elements E as seen in Table 2. The vulnerability value for host N expressed as V_N is the weighted average of all vulnerabilities over host N, this is an industrial specific mechanism as seen in [16]. Eventually each node is expressed by the vulnerability value v_i where i is the number of nodes forming service element E as specified in Table 2. The resulting vulnerability we suggest for service element E expressed as V_E is calculated by taking the maximum vulnerability value for nodes (N1 to Ni) forming the service element E; or more formally as:

$$V_E = Max\,(\mathrm{V}_{N_1}, \mathrm{V}_{N_2}, \ldots., \mathrm{V}_{N_i}) \qquad (1)$$

We used the maximum reference in equation (1) since the vulnerability value should reflect the maximum value, any other approach like averaging or weighted averaging will cause the vulnerability value to drop which is not logically valid. Now we need to map the service element vulnerability V_E to the total risk items vulnerability Vs. The same logic in selecting the max reference in equation (1) can be used for the same reasons mentioned above. Formally V_S can be expressed as:

$$V_S = Max\,(\mathrm{V}_{E_1}, \mathrm{V}_{E_2}, \ldots., \mathrm{V}_{E_j}) \qquad (2)$$

Where j represents the service element E forming the risk item S. Equations (1) and (2) can enable us to form an organizational level vulnerability reference that can be exploited in risk modeling and calculation. The values calculated for each V_S were (3, 4, 4, 4, 3, and 4) respectively.

C. Risk Probability and Risk Impact Estimation:

The risk probability P and risk impact I are ranked out of 5 stages (very low, low, medium, high, very high). The frequency of met vulnerabilities reflect the risk probability, and the value of the service (service as an asset) reflects the risk impact. Each of Probability and Impact are expressed in two dimensional matrices used to retrieve the values of P and I. The risk probability P is determined by the threats encountered for T times, and can be expressed by the following equations:

$$P = f_1(V, T) \qquad (3)$$

$$T = (t_1, t_2, \ldots\ldots, t_i, \ldots t_m) \quad , \ 1 \le i \le m$$

$$f_1 = \alpha t + \beta v_S$$

$$\alpha = \begin{cases} 2, t \le 3 \\ 3, 3 < t < 5 \\ 4, t = 5 \end{cases} \qquad (4)$$

$$\beta = \begin{cases} 1, v \le 3 \\ 2, 3 < \mathrm{v} < 5 \\ 3, \mathrm{v} = 5 \end{cases}$$

The values for alpha (α) and beta (β) are selected to govern the values for P. In our case we selected these values such that the higher the vulnerability the higher the values for P. the impact I determines the impact of the risk according to the asset value and is expressed by equations 5 and 6:

$$I = f_2(V, A) \qquad (5)$$

$$f_2 = \varphi a + \phi v$$

$$\phi = \begin{cases} 1, a \le 2 \\ 2.5, 2 < a < 5 \\ 3, a = 5 \end{cases}$$

$$\varphi = \begin{cases} 2, v \le 2 \\ 3, 2 < v < 5 \\ 4, v = 5 \end{cases} \qquad (6)$$

$$V = (v_{S1}, v_{S2}, \ldots\ldots, v_j, \ldots v_m), 1 \le j \le n \ .$$

D. Determination of the Risk Rank Reference:

The cross reference seen in Table 4 below explains the risk quantification process; this is achieved by combining the numerical and description levels, the first column represents the risk probability level. There are several levels for impact and they vary from very low (-L) to medium (M) impact levels for the first row, and from in the medium (M) to very high (+H) in last row. Table 4 demonstrates a fine resolution between risk probability levels and risk impact levels.

Table (4)

RELATIONSHIP BETWEEN RISK PROBABILITY AND RISK IMPACT LEVELS

Risk probability	Risk Impact levels				
levels	**1**	**2**	**3**	**4**	**5**
1	0.5 –L	1 -L	1.5 l	2.5 M	3 M
2	1 –L	1.5 –L	2 –L	2.5 M	3.5 H
3	1.5 L	1.5	3 M	3 M	4 H
4	2.5 M	3 M	3 M	3.5 H	4.5 +H
5	3 M	3.5 H	4 H	4.5 + H	5 + H

E. Risk Weight Estimation:

An important issue also stems from the determination of risk weight which transfers the values from qualitative to quantitative! Borda count is being used to achieve that. Suppose we have a total risk factors set of N, suppose I is a specific risk of set N with a criterion of k, then the value for any given risk in N can be given as:

$$b_i = \sum_{k=1}^{n} (\mathrm{N} - r_{ik}) \qquad (7)$$

And the total risk value can be calculated as:

$$B = \sum_{i=1}^{N} b_i \qquad (8)$$

And the weight for a given risk RW_i can is given by:

$$RW_i = {}^{b_i}\!/_{B} \qquad (9)$$

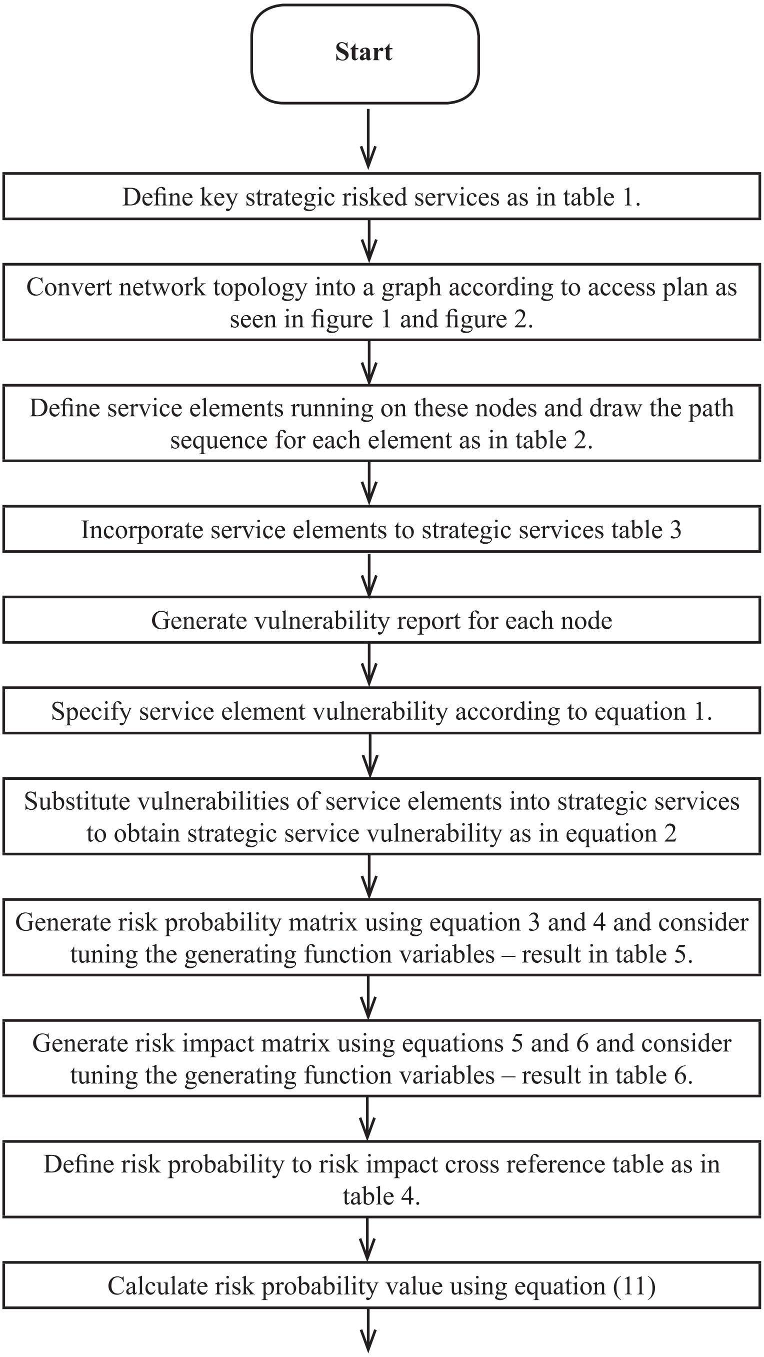
F. Overall Risk Calculation:

Upon completion of the risk judgment matrix, the security risk rank can be calculated by the following equation:

$$RRT = \sum_{i=1}^{k} (\mathrm{RR}_i \, \mathrm{xRW}_i) \qquad (10)$$

G. Model Summary:

The model is summarized in the following flow chart



Define key strategic risked services as in table 1.

Convert network topology into a graph according to access plan as seen in figure 1 and figure 2.

Define service elements running on these nodes and draw the path sequence for each element as in table 2.

Incorporate service elements to strategic services table 3

Generate vulnerability report for each node

Specify service element vulnerability according to equation 1.

Substitute vulnerabilities of service elements into strategic services to obtain strategic service vulnerability as in equation 2

Generate risk probability matrix using equation 3 and 4 and consider tuning the generating function variables – result in table 5.

Generate risk impact matrix using equations 5 and 6 and consider tuning the generating function variables – result in table 6.

Define risk probability to risk impact cross reference table as in table 4.

Calculate risk probability value using equation (11)

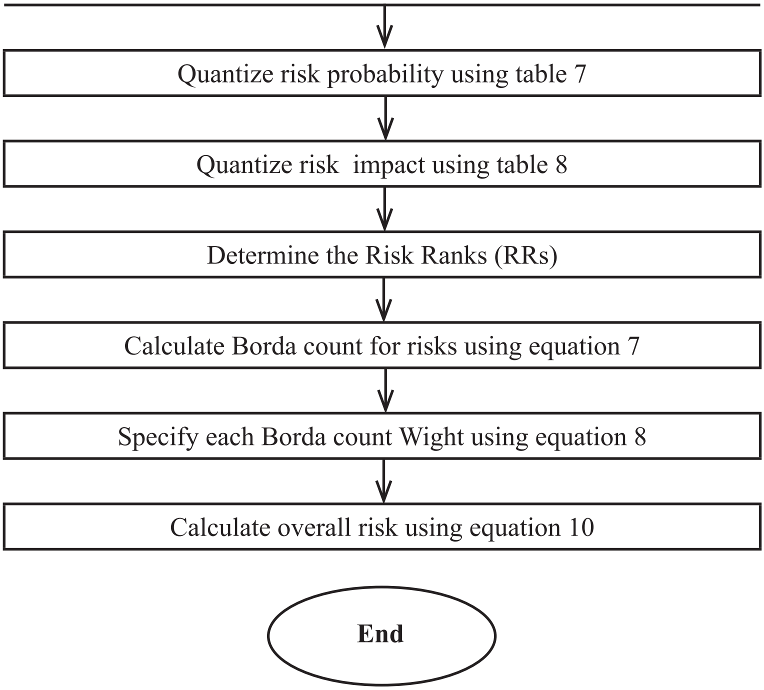

Quantize risk probability using table 7
Quantize risk impact using table 8
Determine the Risk Ranks (RRs)
Calculate Borda count for risks using equation 7
Specify each Borda count Wight using equation 8
Calculate overall risk using equation 10
End

Figure (3)

Risk Assessment Model Flowchart

4. CASE Implantation: Model Implementation on an Acemdemic Network:

The implementation goes through the following steps of flowchar in figure 3, We have implemented the previously mentioned steps to construct the general risk matrix seen in Table 9. The steps from1 to 6 have been previously implanted and explained. The resulting risk for 6 strategic services were (3, 4, 4, 4, 3, and 4) respectively. Then we implemented step 7 to generate the risk probability and step 9 to generate the risk impact matrix. The matrices are given in Tables 5 and 6 respectively. For Table 5 (representing P); we assume the T values to be (5, 2, 2, 1, 3, and 4) respectively. For Table 6 (representing I) we assume A to be (3, 3, 5, 2, 2, and 5) respectively.

Table (5)

RISK PROBABILITY MATRIX

$P = f_1(V, T)$		V				
T		1	2	3	4	5
	1	3	4	5	10	12
	2	5	6	7	12	14
	3	7	8	9	14	16
	4	13	14	15	20	22
	5	16	17	18	23	25

Table (6)

RISK IMPACT MATRIX

$I = f_2(V, A)$		V				
A		1	2	3	4	5
	1	3	5	10	13	16
	2	4	6	11	14	17
	3	9.5	11.5	16.5	19.5	22.5
	4	12	14	19	22	25
	5	14.5	16.5	21.5	24.5	27.5

Using table 5; the risk probability for given values for V and T were (23, 7, 12, 20, and 20), and the impact of these vulnerabilities were (19.5, 16.5, 24.5, 14, 11, and 27.5). For step 10 we need to specify the risk probability value, this was achieved by equation 11:

$$r = {Risk \quad \mathrm{Pr}obability} \Big/ {TotalRisk} \tag{11}$$

Total risks are 25 from table 5, and thus the value of r becomes (19.5/25) and so on. These values were (0.92, 0.28, 0.48, 0.8, 0.36, and 0.84). In steps 12 and 13 we quantize R values and I values using Tables 7 and 8. The quantization in both tables are done by finding the interval P and I, the quantization values for P are (5, 2, 3, 4, 2, and 4). For I the quantization values are (4, 4, 5, 4, 3, and 5).

Table (7)

RISK PROBABILITY QUANTIZATION

Probability P	1—5	6—11	12—16	17—21	22—25
P Level	1	2	3	4	5

Table (8)

RISK IMPACT LEVEL QUANTIZATION

Impact I	1-5.5	6—11	12—15.5	16—22.5	23—27.5
Impact level	1	2	3	4	5

In step 14, we use the quantized values of P and I to refine the risk rank. This was done by substituting P and I into table 4. The values of risk rank (RR) were (4.5H, 3M, 4H, 3.5H, 1.5L, and 3.5H) as seen in Table 9.

Table (9)

GENERAL RISK MATRIX

Service (Risk)	P%	Quantized I	Quantized P	RR	Quantized value Rank	Borda P criterion r_{11}	Borda I criterion r_{12}	b_i	b_i Wight	Risk Wight RW
S1	92	4	5	4.5	H	0	0	12	0.23	1
S2	28	4	3	3	M	5	1	6	0.16	0.35
S3	48	5	2	4	H	3	0	9	0.17	0.69
S4	80	4	2	3.5	H	2	0	10	0.12	0.67
S5	36	3	4	1.5	L	4	4	4	0.08	0.11
S6	84	5	5	3.5	H	1	0	11	0.21	0.74

Now we need to specify the Risk Wight (RW) for each case as we have explained in steps 15 and 16 using the Borda Count. Recall that in equation 7 we have N elements which are also the number of our 6 strategic services. We have built our Borda voting based on two criteria: first is the risk probability and second is the risk impact. In this case for equation 7, k= 2. For each service S there exists a Borda sequence for its risk rank namely bi. Now we need to make an assumption about risk probability and risk impact using the information we have in Table 9 in order to specify the values of ri,j which stands for the risk probability criterion. Since S1 has the highest probability we set its r_{11} to 0, next highest value to 1 and so on until we reach 6, for r_{12} which stands for impact value, we set all impacts with H to 0, medium impacts to 1 and low impacts to 4 (again, these values are assumptions). An example is seen below for b_1 :

$$b_1 = \sum_{k=1}^{2} (N - r_{ik}) = (6 - r_{11}) + (6 - r_{12}) = (6 - 0) + (6 - 0) = 12$$

All of the Borda values are filled accordingly in Table 9. In step 16, we find the Wight for each Borda value using equations 8 and 9. The summation of all Borda values were 52. Dividing each value by 52 we obtain the Borda Wight for each risk. In the last step, multiplying RR in Table 9 with its incorporating Borda weight and do summation for all of the elements as in equation 10, we obtain the Overall Risk which in our case was (3.6).

5. Conclusion:

In this paper we have developed a mathematical service-based risk assessment model and demonstrated it using a case study of the network of a higher-education organization in Palestine. Eventually, our model aims at calculating a number that represents the overall risk for the case at hand. We started by identifying a set of risk items and mapped them to specific components (nodes) in the network. Then we incorporated the service elements to strategic services and generated the vulnerabilities for the nodes in the network. We used these to generate the risk probability matrix and risk impact matrix, and created a cross-reference between risk probability and risk impact levels. We then determined the Risk Ranks (RRs) using the quantized values of risk probabilities and risk impacts and used them to calculate the Borda weights which we then used to calculate overall risk by an averaging mechanism. Compared to other works, this is a very simple calculation method that avoids heuristic calculation and can be adapted using weights functions mentioned in previous equation, for our future work will be building a wizard based software that will be easily handled in order to automate the model steps, in order to give and overall risk can be exploited in ISMS systems.

References:

1. The ISO 27001 standard on information security matters, http://www.27000.org/

2. Lonita, “Current Established Risk Assessment Methodologies and Tools”, Faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS) Department of Computer Science – Information Systems group, University of Twenty Publications, 2013.

3. E. Anderson, “Firm objectives, IT alignment, and information security ”, IBM Journal of Research and Development, Volume: 54 , Issue: 3, 2010.

4. Bernardo,” Utilizing Security Risk Approach in Managing Cloud Computing Services “, IEEE 16th internationalconference on network based information systems proceeding, South Korea, 2013

5. N. Zulkarnean et al., «Information Security Risk Management-An Empirical Study on Difficulties and Practices in ICT Outsourcing “, Second International Conference on Network Applications Protocols and Services, Malasia, 2010.

6. S. Amin et al., “in quest of benchmarking security risks to cyber-physical systems ”, IEEE Transaction on Networks, Volume: 27 , Issue: 1, 2013.

7. R.W. Maule et al., ”Risk Management Framework for Service-Oriented Architecture”, IEEE International Conference on Web Services, USA , 2009. M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

8. Cong Li et al., “Research and design of one security model for service-oriented multi-application architecture ”, Advanced Computing: An International Journal (ACIJ), Vol.2, No.4, July 2011.

9. Asosheh et al., “A New Quantitative Approach For Information Security Risk Assessment”, 2nd IEEE International Conference on Computer Science and Information Technology, China, 2009.

10. Asosheh et al., “A New Quantitative Approach For Information Security Risk Assessment”, 2nd IEEE International Conference on Computer Science and Information Technology, China, 2009.

11. M. Kassou et al., "SOASMM: A novel service oriented architecture Security Maturity Model ", World Academy of Science, Engineering and Technology, International Journal of Computer, Information, Systems and Control Engineering Vol:7 No:12, 2013.

12. M, Saleem et al., "Model Driven Security framework for definition of security requirements for SOA based applications", International Conference on Computer Applications and Industrial Electronics (ICCAIE), 2010.

13. Xi et al., «The Comprehensive Assessment method for Community Risk Based on AHP and Neural Network", Second IEEE International Conference on Networks Security, Wireless Communications and Trusted Computing, China, 2010.

14. Junsong et al., "Risk Evaluation of Network Security Based on NLPCA-RBF Neural Networks", IEEE International Conference on Multimedia Information Networking and Security, 2010, China.

15. R. Liu, " Preliminary Analysis of Smart Grid Risk Index System and Evaluation Methods, Energy and Power Engineering Scientific Research Journal Portal, China, 2013.

16. Qualys vulnerability calculation white paper, www.Qualys.com