“iRisk”- A Software Based Solution to Effectively Manage Information Security Risks in Organizations Using ISO 27001 Approach

K.D.Dinusha Chathurangi[1], J.A.D.C. Anuradha Jayakody[2]
Department of Information Systems Engineering, Sri Lanka Institute of Information Technology (SLIIT), Malabe, Sri Lanka.
[1]dinushachathu91@gmail.com , [2]anuradha.j@sliit.lk

Abstract— **In the era of information technology, aligning organizations to meet the security is a demanding challenge, so in complex organizations aligning IT security risk management with overall security risk management is an essential task. This paper presents a feasible solution, the “iRisk” framework by combines with the ISO 27001 Toolkit. The proposed framework minimizes the hassle and complexity of carrying out the information security risk assessment, saving time and resources by automating the existing system. Furthermore, this allows the user-friendly interface to feed information and identify the high risk areas, calculating impact and probability analysis and compliance reports to be generated. Finally, the sample risk assessment provides a prepopulated list of assets, assigned to a standard set of asset owners; for a typical organization. Each asset features a series of potential pre-assigned risks, in addition to the corresponding controls relevant to those risks from ISO 27001:2013.**

Keywords— **Information Security, ISO 27001, risk assessment**

I. Introduction

Risks grow due to the increased dynamic, complex and interrelated economy and enhanced threats from a wide range of forces[1], such as financial instability, political movements, terrorism, societal requirements, extreme nature events, product recalls over more levels of the supply chain, pandemics, technical failures, frauds, espionage, sabotage, cyber-attacks and others. In the last years there were different low-probability and high-impact events, Black Swan events [2], which are almost impossible to forecast (e.g., drought, earthquake, floods, cyber-attacks). Depending on how uncertainty is handled, it can become opportunity or threat [3]. Thus, organizations have to meet different stakeholders’ risk management requirements to promote trust and long term organizations’ success. A large number of organizations are reducing their business risks by seeking assurance of supplier and partners to properly manage their risks. During the last years ISO/IEC 27001 certificated for Information Security management has increased over 20%. At the end of 2010 more than 15,600 organizations worldwide were implementing information security management and obtained certification according to ISO 27001 [4]. Several best practices (e.g., COBIT, ITIL) and national guidelines (e.g., NIST 800-53, German IT Security Guidelines) for information security management are widely used in practice. Therefore, implemented system “iRisk” would be a good automated software based on ISO 27001and it is for the people who suffer from manual hassle and complexity of carrying out an information security risk assessment.

“iRisk” focuses on developing a unique software based application. The main objective of an iRisk is to capture and manage all business and IT risk centrally. Making more efficiency by reducing search time. The implemented solution allows to import, generate risk register, risk analysis, easily view the high risk areas, and calculate impact and probability analysis and compliance report. The process is done by the software and it will send the data a to Microsoft SQL database.

The ISO/IEC 27001 family for information security management requires the following core principles [5]:

•The defined corporate security policy regards legal/regulatory requirements and is approved by the management.

• A risk assessment must be conducted to establish the risk treatment plan in order to reduce risks to acceptable levels of risk. For the identified remaining risks the business continuity plan must be developed, implemented, maintained, tested and updated regularly.

• The needed resources must be determined and provided. All collaborators must be competent to perform their tasks. They must be aware of their activities’ security impact and how they can contribute to achieving established objectives.

• The effectiveness, adequacy and compliance of the management system must be continually improved using measurements, monitoring, audits, management reviews and by applying corrective and preventive actions in the sense of a PDCA (plan, do, check, act) cycle.

The management system must be systematically documented, communicated, implemented and continually improved.

This paper is organized as follows: Section II illustrates Literature survey. The system overview of the conducted research is explained in Section III. The results and discussion of the research are presented in Section IV.Finally, the conclusions and the future work are stated.

II. LITERATURE SURVEY

Software tools that been designed to assist in ISO 27001 risk assessment and, although their use is not mandatory in the standard. It is practically impossible to carry out and maintain a useful risk assessment for an organization that has more than about four workstations without using such a tool. It is essential that the risk assessment is completed methodically, systematically and comprehensively. An appropriate software tool, designed with ISO27001 in mind and kept up-to-date regarding changing information security issues, can be effective in this process. Hence, the risk assessment is a complex and data-rich process. In any organization of any size, the only practical way to carry it out is to create a database that contains details of all the assets within the scope of the ISMS, and then link to each asset, the details of its (multiple) threats and (multiple) vulnerabilities, and their likelihood and resulting impacts, together with details of the asset ownership and its confidentiality classification.

According to the researches it was identified that very few amounts of similar deployments had been made similar to "iRisk".Moreover, none of them were implemented based on ISO 27001.Every design that has been made was based on this idea has or had its advantages and disadvantages. The following designs have been implemented:

The most well known risk frameworks OCTAVE comes in three sizes depending on the organization size (small, medium or large). One of the benefits of the OCTAVE series is that each of the frameworks provides templates for worksheets to document each step in the process. Templates can be used directly or customized for a particular organization [6].

The NIST framework, described in NIST Special Publication 800-30, is a general one that can be applied to any asset. It follows a similar structure like OCTAVE, but uses a little bit different terminology. NIST doesn't provide plenty of templates such as OCTAVE but it is relatively easy to follow. Since it has a focus on concrete components as systems, it can be easily used for Organizations that are new to risk assessment. Also, because the methodology is defined by NIST, it is approved for the use by US government agencies and organizations that work with them [7].

ISACA's COBIT is an IT management framework while the ISO 27xxx is a security framework that require organizations to have a risk management program. They recommend repeatable methodologies and specify when risk assessments should take place. Risk assessment in COBIT, described in RISK IT goes beyond security risks and includes development, business continuity, and other types of operational risk in IT [8], whereas ISO 27005 concentrates on security exclusively.

ISO 27005 follows a similar structure to NIST, but the terms are defined differently. ISO 27005 includes annexes with forms and examples, but like other risk frameworks, it's up to the organization implementing it to evaluate or quantify risk in ways that are relevant to its particular business.

Organizations that do not have a formal risk assessment methodology could firstly review the risk assessment requirements in ISO 27001 and 27002 and consider the 27005 or NIST approach. The ISO standards provide a good justification for formal risk assessments and outline requirements, while the NIST document provides a good introduction to a risk assessment framework.

The tools conforming to the above Risk Management framework will be categorized to more details in Table I. Further, Risk Management (RM) supported phases are divided into the below categories.

RM phases supported,

1. Risk Assessment
   (a) Risk Identification
   (b) Risk Analysis
   (c) Risk Evaluation
2. Risk treatment
3. Risk communication

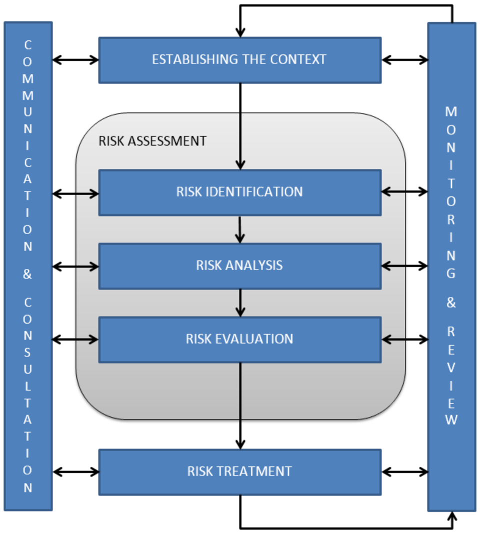


Fig. 1 Risk Management Framework

TABLE I
DESCRIPTON OF EXISTING RISK MANAGEMENT TOOL [9]

Tool	RM phases supported					RM methods supported
	1.RA			2	3	
	1.(a)	1.(b)	1.(c)			
Acuity Stream	X	X	X	X	X	ISO 27002, ISO 27005
Callio secura 17799	X	-	X	X	X	ISO 27002,

						ISO 27005
CCS Risk Manager	X	X	X	X	X	AS/NZS 4346, ISO 27002, ISO 27005, FRAP, Risk IT
CORAS Tool	X	X	X	X	-	CORAS
SAVe	X	X	X	X	X	ISO 27002, ISO 27005
TRICK light	X	X	X	X	X	ISO 27002, ISO 27005
vsRisk	X	X	X	X	X	ISO 27002, ISO 27005, FRAP

III. SYSTEM OVERVIEW

The implemented system “iRisk” is straightforward and so quick to use that it can save a significant proportion of the budget, you might otherwise spend on consultancy advice when conducting a risk assessment. The main objective of this project is implementing software for the organization to capture and manage all business and IT risk centrally. Making it more efficient by reducing the search time.

.

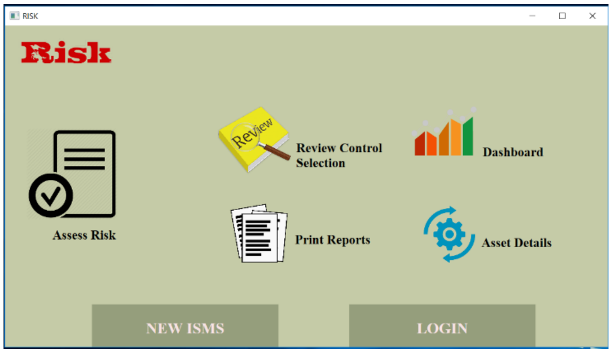


Fig. 2 Main Interface of the iRisk tool

IV. Results and Discussion

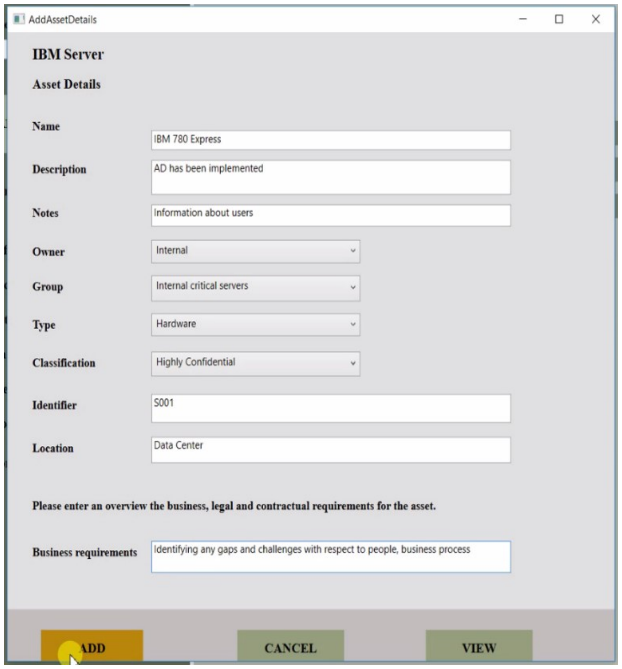
A. *Risk Assessment methodology*

- *Risk Identification*

The main objective of risk identification is to identify the sources of risk, identify the assets within the scope of the Risk Assessment. An inventory of information assets will be produced of all identified assets in the form of an Information Asset Register (IAR).

As part of this step, details of information-related assets, which are being used to carry out the various business functions of company, will be collated in the form of an Information Asset Register. Examples of information-related assets, which will be considered for inclusion in the Information Asset Register, are:

- All proprietary information belonging company.
- All personnel information relating to Employees Company.
- All client information held by company.
- All supplier, contractor and other third party information occupied by the company.
- All software assets such as application software, system software, development tools and utilities belonging to company.
- All property, such as computers, communications equipment, media and equipment relating to facilities.
- All services, such as HVAC, lighting and power, associated with information systems of the company.



IBM Server

Asset Details

Name: IBM 780 Express

Description: AD has been implemented

Notes: Information about users

Owner: Internal

Group: Internal critical servers

Type: Hardware

Classification: Highly Confidential

Identifier: S001

Location: Data Center

Please enter an overview the business, legal and contractual requirements for the asset.

Business requirements: Identifying any gaps and challenges with respect to people, business process

Fig. 3 Asset details interface

- *Risk Analysis*

a) Risk Impact – Analysing Consequence of a Risk

The aim of the step is to identify how valuable the assets are in the business of the company, and what might happen, if their security is compromised. Each Asset defined in the Information Asset Register will be assigned a value (3=High, 2=Medium, 1=Low) for each of the following parameters.

- Financial Impact;
- Operational Impact;
- Confidentiality;
- Integrity; and
- Availability.

The objective of assigning a value to these parameters is to ascertain what might happen if the security is compromised, so that the importance of the asset for the company can be determined.

b) Risk likelihood analysis

The realistic likelihood of the risk materializing shall be calculated as per the below table. Each Asset defined in the Information Asset Register will be assigned a value (3=High, 2=Medium, 1=Low).

TABLE II
RISK LIKELIHOOD ANALYSIS

Risk Likelihood	Rating Guideline
1 – Low	The event could occur annually
2 – Medium	The event may occur bi-annually
3 – High	The event is expected to occur quarterly

c) Calculating the Level of Risk

The level of Risk is a function of the risk impact and risk likelihood. After assigning values to risk impact and risk likelihood, the following formula shall be used to arrive at final Risk value.

Level of Risk = Risk Impact * Risk Likelihood → (1)

The following tables detail, how the risks shall be treated when the risk values fall within the defined ranges

TABLE III
POSSIBLE RISK VALUES

Level of Risk	Risk Likelihood	Low (1)	Medium (2)	High (3)
Risk Impact	Low (1)	1	2	3
	Medium (2)	2	4	6
	High (3)	3	6	9

TABLE IV
RISK TREATMENT CRITARIA

Risk Measure	Risk Treatment Required
1-3	Risk Acceptable. No further action required.
4-6	Medium Priority - Risk Treatment Required. Implement controls within the time-period specified by the business. Such risks could be accepted if approved.
7-9	High Priority - Risk Treatment Required. Implement controls immediately to mitigate risks. Such risks could be accepted if approved.

- *Risk Treatment*

Taking into consideration Risk impact and Risk likelihood, risk treatment procedures shall be identified and implemented.

A formal risk treatment plan should be prepared. The risk treatment could be any of the following:

i. Avoiding the risk;
ii. Implementation of additional controls to reduce the impact of risk – Controls can be selected from ISO/IEC 27001:2013 Annexure A.
iii. Transfer of risk – outsourcing, insurance, etc.; and
iv. Risk acceptance – in line with the risk acceptance criteria stated in this risk assessment procedure.

The existing and planned controls will be mapped to the ISO/IEC 27001:2013 Annexure – A control.

The Residual Risk value will be calculated after considering the risk treatment option. Using the same formula (2) mentioned below.

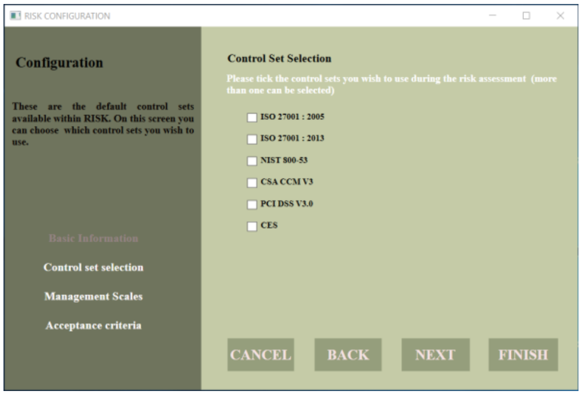
Residual Risk Level = Risk Impact * Risk Likelihood→ (2)

- *Risk Acceptance Criteria*

The information security risk acceptance shall be based on the following criteria's:

I. The cost of controls are significantly higher than the possible benefits gained from implementing ISO 27001:2013 controls;
II. Acceptance of risk does not violate any legal or statutory requirements;
III. Regional, socioeconomic and environmental aspects that prevent the implementation of controls;
IV. The possible adverse impacts on business operations due to implementation of the controls and the related stakeholders' concerns and priorities;

Fig. 4 shows the iRisk tool risk configuration interface. The standard should be selected before configure the risk. Currently implemented tool is working only for ISO 27001:2013 control set. Then, likelihood and Probability range can be selected according to the scale shows in the Fig 5. After that Risk acceptance criteria shall be identified related to the above mentioned criteria. It is shown in Fig 6.Finally the asset based risk assessment can be done according to above mentioned Risk assessment methodology. "Assess Risk" option in the main interface helps to get the "Risk management" interface which shows in the Fig. 7.



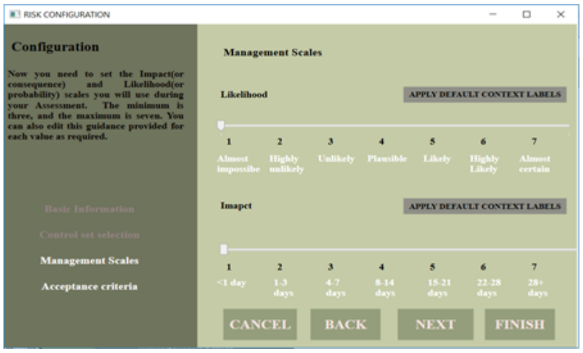
These are the default control sets available within RISK. On this screen you can choose which control sets you wish to use.

Control Set Selection

Please tick the control sets you wish to use during the risk assessment (more than one can be selected)

- □ ISO 27001 : 2005
- □ ISO 27001 : 2013
- □ NIST 800-53
- □ CSA CCM V3
- □ PCI DSS V3.0
- □ CES

Fig. 4 Control set selection



Now you need to set the Impact(or consequence) and Likelihood(or probability) scales you will use during your Assessment. The minimum is three, and the maximum is seven. You can also edit this guidance provided for each value as required.

Management Scales

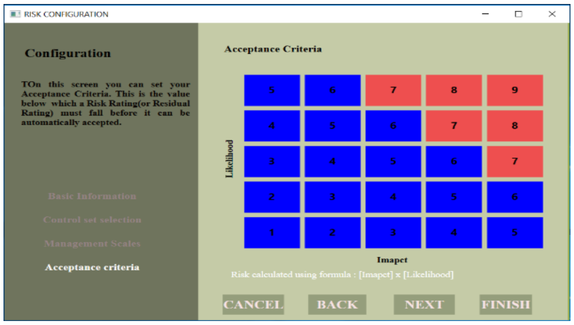
Likelihood

1	2	3	4	5	6	7
Almost impossibe	Highly unlikely	Unlikely	Plausible	Likely	Highly Likely	Almost certain

Imapct

1	2	3	4	5	6	7
<1 day	1-3 days	4-7 days	8-14 days	15-21 days	22-28 days	28+ days

Fig. 5 Management scale



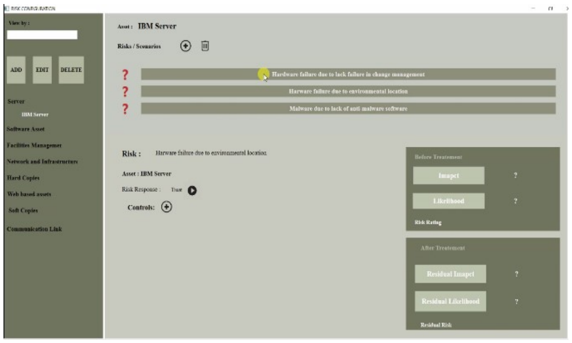
TOn this screen you can set your Acceptance Criteria. This is the value below which a Risk Rating(or Residual Rating) must fall before it can be automatically accepted.

Acceptance Criteria

5	6	7	8	9
4	5	6	7	8
3	4	5	6	7
2	3	4	5	6
1	2	3	4	5

Risk calculated using formula : [Imapct] x [Likelihood]

Fig. 6 Acceptance criteria



Asset : IBM Server

? Hardware failure due to lack failure in change management

? Harware failure due to environmental location

? Malware due to lack of anti malware software

Risk : Harware failure due to environmental location

Asset : IBM Server

Risk Response : Treat

Controls:

Fig. 7 Asset based risk management

V. Conclusions and Future Work

This research work demonstrated that the implemented tool gives a unique opportunity to apply to the real scenarios in the case of risk identification, analysis and treatment. Implemented tool "iRisk" will help to minimize the manual hassle and complexity of carrying out an information security risk assessment and also saving time and resources. Further risk assessments can be repeated easily in a standard format year after year and generate reports for exporting, editing sharing across the business and the auditors.

In the future work planned to implement the same procedure for other standards as well. This will assist to identify a large amount of Risk in the organizations.

Acknowledgment

This work has been supported by the Sri Lanka Institute of the Information Technology, Malabe Sri Lanka.

References

[1] Margareth Stoll, "From Information Security Management to Enterprise Risk Management" 2015.

[2] N. Taleb, the Black Swan, the Impact of the Highly Improbable, Random House, New York, 2007.

[3] M. Power, Organized Uncertainty. Oxford University Press, New York, NY 2007.

[4] International Standard Organization (ISO). ISO Survey of Certifications 2010, http://www.iso.org/iso/iso-survey2010.pdf.

[5] ISO/IEC27001, ISO/IEC 27001:2005, Information Technology, Security techniques, Information security management systems requirements. Geneva: International Standard Organization, 2005.

[6] Carnegie Mellon University, Software Engineering Institute http://www.cert.org/resilience/products-services/octave/index.cfm.

[7] National Institute of Standards and Technology: Managing Information Security Risk, Organization, Mission, and Information System View, NIST Special

Publication 800-39, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, USA, 2011, http://csrc.nist.gov/publications/PubsSPs.html#800-30.

[8] ISACA: Risk IT Framework for Management of IT Related Business Risks, USA, http://www.isaca.org/knowledgecenter/risk-it-it-risk-management/pages/default.aspx.

[9] Dan Ionita, "Current Established Risk Assessment Methodologies and Tools" 31 July 2013.