IJCSN International Journal of Computer Science and Network, Volume 3, Issue 5, October 2014
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.274

Risk Indicators for Information Security Risk Identification

[1] Upasna Saluja, [2] Norbik Idris

[1, 2] Faculty of Computing, University of Technology (UTM), Malaysia

Abstract - Risk Identification, the foundation of Information Security Risk Management is asset-centric, which makes the process tedious, time consuming and inappropriate for today's environment. It is subjective and depends a lot on expertise of information security practitioners conducting the risk assessment. This paper has proposed a methodology for Risk Identification that drives away from an asset-centric approach by incorporating the concept of Risk Indicators, which is the foundation of Risk Identification in the fields of finance and medicine. This Risk Identification approach enables statistical analysis for Risk Assessment making it objective and scientific thus inspiring greater confidence among stakeholders.

Keywords - *Information Security, Risk Assessment, Risk Identification.*

1. Introduction

In colloquial language the word "risk" refers to the possibility of something undesirable happening [1]. According to ISO 31000, Risk is considered to be the "effect of uncertainty on objectives" [2]. In simple terms, risk is an uncertain situation with possible negative outcomes.

The dependency of organizations on IT and information brings certain inherent risks. Yazar [3] stressed that while networked information systems have created many new opportunities for businesses, they have also introduced considerable risks in return. Organizations face risks because information which is the lifeline of business, can be accessed or modified in an unauthorized manner, further it can be destroyed, copied or even stolen easily if not protected adequately. That is why it is imperative for organizations to safeguard the confidentiality, integrity and availability of information that empowers their business processes and systems. Management of information security risks entails establishing of a framework [4]. Risk assessment focuses on three core phases namely Risk Identification, Risk Analysis and Risk Treatment. Within the context of the overall risk management process, risk identification is the foundation of information security risk assessment.

2. Related Study of Risk Identification

The very first step towards risk identification is the identification of the physical and software assets determined through interviews where asset owners identify threats and vulnerabilities to their respective assets. The researcher studied the approach to Risk Identification in some of the well-known risk management methodologies namely CRAMM, OCTAVE, NIST SP 800-30 and ISO 27005. The key findings are summarized below.

2.1 CRAMM

The researcher determined that CRAMM has a qualitative approach, is clearly dependent upon asset inventory and relies a lot on participation of asset owners. The remaining steps focus on assessing risks to the relevant assets.

2.2 OCTAVE-Allegro

The key step in the eight step process according to OCTAVE-Allegro is the asset profile creation phase. Participants create a profile of each information asset that establishes clear boundaries for the asset, identifies its security requirements, and identifies all of its technical, physical and people containers.

Subsequently the threats and risks are identified by stakeholders for each of the assets. Actual threats are not listed in the methodology. An assessor is expected to come up with threats based upon possible threat scenarios considered likely with an asset - container combination.

The further risk identification phase in OCTAVE involves creation of four types of Threat Trees involving Threat Actor (Inside / outside), Motive (Accidental / Deliberate), Outcome (Disclosure, Modification, Interruption, Destruction or Loss).

OCATVE – Allegro risk management methodology relies upon asset profiles for the main steps in risk management and requires the assessor to have expertise to draw out the threats for assets. Thus, OCTAVE Allegro clearly follows an asset-centric approach to risk identification and relies on expert judgment for threat identification

2.3 ISO 27005 - ISO 27005

Under risk identification – the ISO 27005 standard refers to ISO/IEC 27001, Clause 4.2.1 (d) 1 which requires that the assets within the established scope should be identified as the first step. When defining the scope and boundaries of the risk assessment, the standard emphasizes that all relevant assets must be taken into account in the risk assessment. For each asset or asset category, threats and corresponding vulnerabilities are mapped out in a table. Subsequently, assets are valued qualitatively, further threat likelihood and severity of vulnerability is also assessed qualitatively. Thus, the approach supported by ISO 27005 is asset centric since the entire process has its foundation on physical and software assets.

2.4 NIST SP 800-30 Revision 1, NIST 800-39

NIST guidance requires that risk assessments must address the potential adverse impacts to assets besides organizational operations and individuals. NIST lays considerable emphasis on assets while it defines organizational assets as any resource or set of resources which the organization values. The standard has mentioned rating scales (qualitative Very High, High, medium, Low, Very low) and semi-quantitative (numbers from 1 to 10). In summary, it was noticed that traditionally, risk identification process starts with consideration of assets under scope, followed by listing of applicable threats to information assets while considering possible vulnerabilities. Further, the risk identification process relies a lot on expert judgment.

3. Challenges in Risk Identification

Having studied the risk identification methods in existing information security risk management methodologies, as covered in section 2 above, the researcher identified the following issues in traditional risk identification approaches. Existing Risk Identification approaches rely on asset inventory which in today's IT landscape, is quite challenging to create and maintain.

Organizations are faced with the challenge of determining asset ownership in IT environments that deploy cloud technologies or virtualization where organizations do not always own or manage the information assets. Information assets are dynamic and change hands within the organization as well with third parties which are part of the extended enterprise today.

An organization faces the challenge of maintaining control over assets since information is mobile and is being accessed not only from within the organisation but also from outside of the organization. At the end of the working day, employees walk out with their computing devices and access information from anywhere. Some employees telecommute and work out of the office accessing corporate resources remotely [5].

The follow on step in traditional Risk Identification after determining asset inventories involves mapping of Asset – Threat – Vulnerability using trees or tables. Considering today's diverse set ups in multi-national organizations, it is very difficult to define the large number of possible assets-threats-vulnerability combinations.

4. Need for A Novel Approach

The above points are suggestive that there is a need to develop a fresh approach to risk identification that allows for today's complex technology landscape (cloud, virtualization, outsourcing, mobility) and does away with asset-centric tedious risk identification methods. This paper provides an overview of a novel risk identification methodology supported by a case study.

5. Drawing Lessons from Risk Identification in Medical and Finance Fields

In order to find a solution to the mentioned challenges, the researcher discovered that the approach of Risk Identification is very different in the field of medicine and finance. Risk Assessments in the fields of finance and medicine rely on Risk Indicators, rather than assets.

5.1 Adapting the Concept of Risk Indicators

There has been extensive use of Risk Indicators in the fields of finance and medicine, which could be adapted

for the field of information security risk identification. With an endeavour to explore adaptation of risk indicators towards information risk identification, researcher delved further into Risk Indicators being used for assessing risks in the fields of finance and medicine, and incorporated risk indicators into information security risk assessment.
On the one hand, the study determined that Risk Indicators take account of historical risks and on the other hand, they help in predicting potential risk. Further it became clear that Risk Indicators are best suited for quantitative analysis. [6].

Lessons drawn from the fields of Finance and Medicine which use Risk Indicators extensively have been briefly highlighted below:

Financial Risk Indicators: Researcher discovered that risk indicators are extensively used for risk management in various areas of finance. In Credit Risk financial organizations use risk indicators such as "financial ratios", "credit ratings", "Credit Default Swap (CDS)", "Probability of Default (PD)", "Number of days in credit limit overrun" and "number / amount of credit limit breached" to determine triggers that could result in a rise in credit risk. While managing Fraud Risk, banks use indicators such as "anomalous behaviours" in loan applications to recognize suspicious behaviour. In Financial Markets, risk indicators such as "Breach of Daily trading limits", "Abnormal Trading patterns such as number of deals amended or cancelled", "Number of deals with deferred start dates without any reason provided", "Number of non-reconciled deals", "Number of staff without financial background", "Number of transactions per staff member" as potential indicators of staff misuse or risks. Similarly Risk Indicators in Market Risk focus on "Value at Risk" as the main risk indicator to determine risk of losses due to the changes in the market factors [7].

Further, Operational Risk Management in banks has been in place for many years as an operational metric that provides information on the level of exposure to a given operational risk that the organisation is experiencing at any time (Institute of Operational Risk 2010). Operational key risk indicators (KRIs) such as processing errors, rogue trading, "Number of loans with missing documentation" are key risk indicators which banks have been using for years to identify and track risks [8].

Medical Risk Indicators: Medical field uses risk indicators in multiple diverse areas. Risk Indicators in medicine are also called biomarkers, which are defined as measurable risk indicators which signify the severity or presence of disease. There are well known Physiological risk indicators (biomarker) such as "blood pressure or heart rate showing the risk of stroke" while "body temperature is considered a risk indicator (biomarker) for fever". Molecular risk indicator (biomarker), such as Elevated prostate specific antigen as a biomarker for prostate cancer, cholesterol values as a risk indicator for potential coronary and vascular disease, C-reactive protein (CRP) is considered a risk indicator or biomarker for inflammation, enzyme assays are used for Liver function tests which point towards risk of Liver disease. Similarly changes in tumor cell DNA is used as a risk indicator to estimate a person's risk for developing cancer.

From the study of Risk Indicators used across mature disciplines such as Finance and Medical. Researcher concluded that organizations stand to benefit immensely from the implementation of concept of risk indicators. Organizations are able to assign explicit responsibility to rightful functional owners for specific risk indicators. This brings accountability and ensures availability of risk related data on a consistent basis.

5.2 Adapting the Concept of Observation of the Subject over a Period of Time

When the researcher delved further into risk management in finance and medical fields researcher determined that the concept of observing the subject / risk indicators over time proved beneficial and could be adapted for information security risk management as well. This study adapted the concept of observing the risk indicator over time in order to obtain a holistic understanding of risk. In pre-clinical trials, the situation is observed over a period of time with recordings done for specific indicators also termed as medical markers. Similarly in clinical trials, observing the subject or indicators help the person conducting the clinical trial to understand the trend and impact of drugs over the defined period of observation. The researcher picked up this concept and incorporated it in the Information Security Risk Identification methodology.

5.3 Adapting Statistical Regression to Determine the Relationship between Cause and Effect Variables

The researcher also derived the fact that both finance and medical risk assessment approaches conduct statistical analysis to analyze data. This study decided to take this approach of statistical analysis towards Information Security Risk Management. Typically regression analysis is used in medicine field which is known to demonstrate

the relationship between predictor variables and response variables.

6. Risk Identification based on Risk Indicators

This study of Risk Identification is a part of Statistical Quantitative Risk Calculator (SQRC) Information Security Risk Management methodology. In order to ensure successful implementation of risk indicators, it is critical that Information Security Risk Indicators are defined and managed according to a formal process that should be incorporated in a policy with clearly indicated roles and responsibilities of stakeholders involved.

SQRC designed the approach for defining and managing Information Security Risk Indicators. The deployment approach and an overview of the results of the study are covered in the following section.

APPROACH: An overview of the approach for designing, defining and managing Information Security Risk Indicators is given below:

- **Obtain Management Support**: Highlight to senior management the importance of Info Sec Risk Indicators. Bring out how Risk Indicators would allow senior management to monitor risk and compliance in an on-going manner. Identify the business leader who would be the main supporter for the project and convey a top-down message to internal stakeholders responsible for supporting the process and providing data in an on-going manner.
- **Initiate the process for Defining and Managing Risk Indicators**: Ensure adequate staffing for sustaining the process and determine the individuals from relevant functions who would work on the process on an ongoing manner. Train the relevant individuals on the steps involved in the process for defining and maintaining information security risk indicators.
- **Development of SQRC Information Security Risk Indicators:** Develop Risk Indicators appropriate for Information Technology environment. The detailed process of this is captured in the following section 7.3.
- **Dealing with Anomalies or Escalations:** Establish a process for Dealing with Anomalies in gathered data and other escalations. This should include notification process for anomalies in gathered data and other escalations such as a risk indicator being above the defined baseline. Define methods to assign and track corrective actions to closure.
- **Governance:** Assign responsibility for the overall Risk Indicator administration and monitoring process to a committee or individual(s). Further, determine frequency for review of metrics by Information Security as well for conduct of review meetings with business executives. Define baselines for risk indicators above which escalations need to be made to respective escalation points. Establish process for revisiting existing risk indicators in order to assure relevance and where needed define fresh Info Sec Risk Indicators.
- **Communication and Review:** Establish a process for keeping executive management informed. Senior management should receive status reports on an ongoing basis. Escalation processes should define the triggers for escalation to senior management. Establish process to revisit Risk Indicators upon critical changes in internal and external environment and on a defined periodicity.

7. Case Study

7.1 Field Setting

For the purpose of SQRC Information Security Risk identification, a subsidiary of a multi-national organisation headquartered in Bangalore, India was selected. This organization provides software products for equity trading to stock brokers and stock exchanges. Their main products are equity trading systems, data on the financial market and connectivity solutions for sell-side firms. The scope of Risk Identification included the product development, management, infrastructure, and support organization. A total of 130 staff members including senior management were considered in scope of the case study, where risk indicators were defined and observed for seven months, from Jun 2013 to Dec 2013.

Considering the above mentioned steps in section 6, SQRC Risk Identification was implemented. At the outset, management support was obtained as the first step of the implementation of the process for defining risk indicators. Subsequently, representatives from information security, HR, Physical security, Facilities, Product management and support functions were briefed and trained about defining and maintaining information security risk indicators.

Additionally, processes for anomaly detection and escalation, were defined in consultation with the representatives of the functions responsible for risk indicators. Further, the process for governance including

regular reviews, definition of roles and responsibility of key stakeholders, were defined. The process was notified within the organization. As mentioned earlier, communication and review was conducted at the organization under the scope of Risk Assessment with the cross functional team. The head of Information Security was given the overall responsibility for governing the Risk Indicators Program.

7.2 Development of Risk Indicators

Risk Identification approach entails the development of context specific information security risk indicators, through the steps explained below:

Initial Pool of Risk Indicators: Drawing from various threats and risk scenarios described in Octave-Allegro, NIST guidelines and ISO 27005, researcher assimilated a list of potential risk indicators. The list of threats provided by ISO 27005 was found closest to the concept of Risk Indicators and that is why this list was considered as the foundation for Risk Indicators while relevant risk indicators from other methodologies were also considered.

Interviews to Define Context Specific Risk Indicators: In order to identify and define Risk Indicators, the researcher engaged the Head of Security, one information security manager, a security analyst and 4 functional managers from Operations, Product Management, Facilities and HR. They were interviewed to identify, define and refine the Risk Indicators which are applicable and appropriate to the organisation. Researcher derived the context of business, technology and supporting operations. This step deliberated and refined the reference risk indicators; it also added risk indicators as further deliberations were undertaken with the company internal stakeholders. Further, some risk indicators were dropped since they were not considered appropriate to the organizational information security context. Following aspects were considered during the definition of context specific risk indicators during the case study:

- *Geographical context:* Risk indicators were defined based upon geographical context. For instance since the region in India is not prone to multiple natural phenomena, diverse natural disasters, i.e. Flood, Earthquake, and Volcanic phenomenon etc. were clubbed into one risk indicator rather than retain natural phenomenon as a separate category and each of these as separate risk indicators.

- *Operational Context:* In addition, since the organization had faced critical Issues due to lack of operational training of staff members (e.g. data entry errors, accidental data deletion, information sent to wrong recipient) on the one hand and lack of expertise in technology and security administrators (e.g. configuration error) on the other hand, these were added as risk indicators.

- *Business Context:* Since the organization is in the growth stage and has been adding newer facilities, the business owners also saw potential risks due to lack of appropriate workplace health, safety or wellbeing measures provided to staff. This was also added as a new risk indicator.
- *Risks not faced by the Organization but Faced by Peer Organizations:* Recent breach in a peer organization involved damage of hard copy documents kept in storage. This prompted the company to include the risk indicator "Deterioration of storage media (hard copy documents)".
- *Industry Trends:* Due to a large emphasis in recent times on outsourcing during the organizational restructuring in view of the economic downturn, a separate risk category "Unauthorized actions by Third Party" was introduced to cover potential "Errors or unauthorized action (improper access, disclosure, alteration or destruction of information) by third party staff members- Vendor / Supplier / outsourced provider".

7.3 Risk Indicators

Following these steps the researcher arrived at a finalized list of 43 Risk Indicators under 7 categories defined for IT environment. The list is appended below in Table 1.

Table 1: 43 Risk Indicators for IT Environment

#	*Category*	*Risk Indicator*
1	Physical Damage	Damage or Destruction of equipment or media
		Natural Disasters (Flood, Earthquake, Volcanic phenomenon etc.)
		Fire (Natural or Man-made)
		Man-made Disaster (Bomb / Terrorist attacks, riots, other disruptions)
		Climatic Phenomenon (Dust, Corrosion, Freezing…)
2	Loss of Essential services	Failure of air-conditioning or water supply system
		Issues due to Power Supply
		Business Disruption due to telecommunications
3	Technical Issues	Failure or degradation of Internet Connectivity

		System non-availability, System hardware failure or Malfunction
		Network equipment failure or Malfunction
		Software Malfunction or Failure
		Degradation of the information system
		Malicious code (Malware) e.g. Virus, Trojan horse
		Obsolence of Hardware including network equipment
		Obsolence of software or applications
		Network performance degradation or connectivity issues
		Damage to Network Cables
		Deterioration/Loss of storage media (such as Back-up, databases and
		Wireless network issues
		Inadequate Vulnerability Management
		Inadequate maintenance practices and measures for technology equipment
		Disturbance due to Radiation
4	Compromise of information	Social Engineering
		Physical Theft or robbery of media, documents or equipment
		Theft of and/or unauthorized access to information held within systems
		Information Retrieval from recycled or discarded media
		Unauthorized Disclosure of confidential information
		Breach of employee's / customer's private information
		Tampering (unauthorized modification) of Data / Hardware / Software
		Spoofing / impersonation / masquerading / Abuse or Forging of
5	Unauthorized actions	Unauthorized use of systems or internet access
		Unauthorized downloading or use of unauthorized software
		Unauthorized physical access
		Cyber Attack
		Unrestricted use of storage or computing devices/systems
6	Operational Issues	Issues due to lack of operational training of staff members (e.g. data entry errors, accidental data deletion, information sent to wrong recipient)
		Lack of expertise in technology and security administrators (e.g. configuration error)
		Lack of staff members with required skill or experience (Inability to attract, retain or effectively deploy capable)
		Lack of appropriate workplace health, safety or wellbeing measures provided to staff
		Information Security awareness of staff members
		Deterioration of storage media (hard copy documents)
7	Unauthorized actions by Third Party	Errors or unauthorized action (improper access, disclosure, alteration or destruction of information) by third party staff members Vendor / Supplier / outsourced provider.

7.4 Adaptation of Statistical Analysis

Referring to section 6 above, this study looked into the feasibility of applying statistics to information security risk analysis. Going by Risk Assessment in medical and finance world, it was realised that regression model can be quite useful considering Risk Indicators tabulated above as predictor variables that have the potential to bring risk to Information security of the organisation. Further, Consequence Indicators that represent the areas where an organisation is expected or likely to observe impact were taken as response variables for the statistical analysis.

Since information security deals with confidentiality, availability and integrity of information, this study also looked into impact in these three areas. Availability aspect is somewhat tangible while confidentiality and integrity are generally non-tangible aspects. Additionally, it was realized that organisational processes and infrastructure too bear impact. The key question which surfaced was "How to measure impact?" In order to determine appropriate unit of measurement, each risk indicator was deliberated. Result was three different units of measurement namely downtime which is appropriate for "downtime of systems, applications and networking equipment" for which unit of measurement is Hour; secondly "Frequency of incidents" where each incident counts, and thirdly binary format (Yes / No) where the data represents presence or absence of a control. Accordingly consequence variables got defined as given in Table 2:

Table 2: List of Consequence Indicators

Variable	***Area***
Y1	Information Availability
Y2	Information Confidentiality & Integrity

Y3	Infrastructure & Organisational Processes

8. Information Security Risk Analysis

Data was collected from organization's systems and processes regarding the defined Risk Indicators for a period of seven months. Data set was prepared and analyzed statistically. Regression model was developed by using predictors Xi's as well as response variables Yj's.

Using Risk Indicators as Input for Statistical Risk Analysis: Medical risk assessment uses first generation of statistical regression which was found to be inappropriate for Information technology environment considering the assumptions of traditional regression on one hand and the complex environment of IT on other. Further, first generation regression works only with independent variables making it unsuitable for situations where multi-collinearity exists i.e. variables are interrelated on each other. SQRC referred to second generation statistical data analysis technique Structured Equation Modeling (SEM) and further focused on Partial Least Square technique [10] for information security risk analysis ~~Steven M Shugan~~ [11].

When organizations wish to assess risk in IT scenarios of today, they have access to lot of relevant data from a large number of tools and systems such as IDS, IPS, SIEM, Antivirus etc. SQRC is based on the foundation of PLS and conducts analysis considering data collated. SQRC analyses data measured in diverse units. When an Info Sec incident occurs, it often has cascading effects on different assets which is not supported by First generation regression, though SQRC analysis takes into account this interdependence.

9. Overview of Results

SQRC conducted statistical analysis for the data set generated in Risk Identification. The following graph displays the number of Consequence Area impacted by each Risk Indicator.

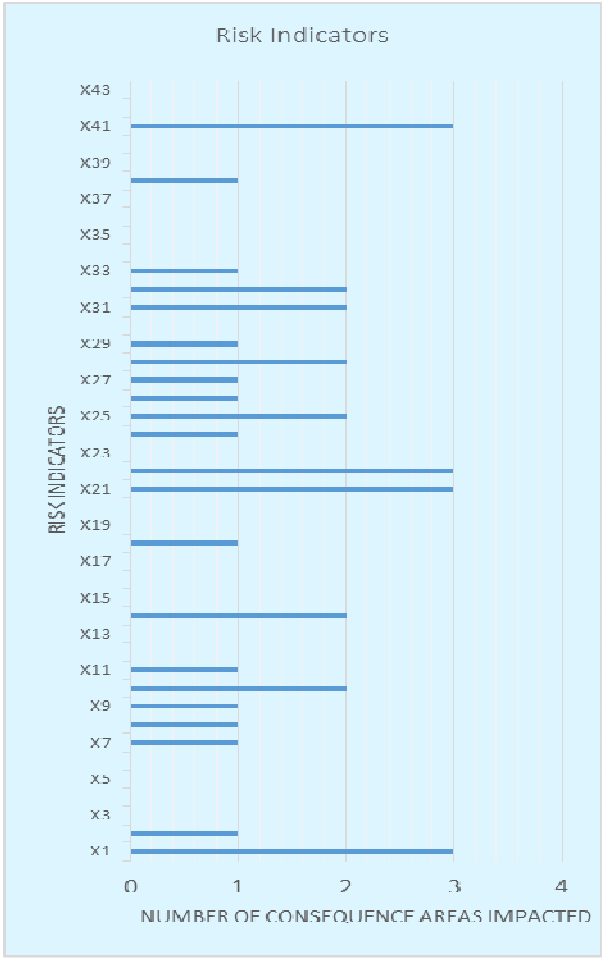

Fig 1: Result of all Risk Indicators

The statistical analysis determined that for the organization four Risk Indicators proved to be statistically significant as they impact information security across CIA of information, organizational processes and infrastructure.

Table 3: Significant Risk Indicators for the Company Studied

#	*Risk Indicator* *	*Significant Risk for the Organization*
1	X1	Damage or Destruction of equipment or media
2	X21	Inadequate vulnerability Management Practices
3	X22	Inadequate maintenance practices and measures for technology equipment
4	X41	Information Security awareness of staff members

**Refer Table 1 and 2 above for description of Xi's*

Besides, there were six risk indicators that impact organization in more than one area pertaining to information security, resulting in having moderate impact. These are listed in Table 4 below.

Table 4: Significant Risk Indicators for the Company Studied

#	Risk Indicator	Significant Risk for the Organization
1	X10	System non-availability, System hardware failure or Malfunction
2	X14	Malicious code (Malware) e.g. Virus, Trojan horse
3	X25	Physical Theft or robbery of media, documents or equipment
4	X28	Unauthorized Disclosure of confidential information
5	X30	Tampering (unauthorized modification) of Data / Hardware / Software
6	X31	Spoofing / impersonation / masquerading / Abuse or Forging of Rights

The organisation's leadership and functional management teams validated that these risks were relevant in the context of their business and took these up as the most important risks to address, from a risk treatment perspective.

In the organization included in the case study, the management was able to prioritize their effort on four top risks and six significant risks with confidence since the identified risks had been analyzed objectively using a statistics based method. Utilizing a structured method and program for administering cross-functional Information Security Risk indicators, the organization was able to bring in better accountability among stakeholders, while establishing a strong security metrics process.

9. Key Benefits of SQRC Risk Identification

This research has contributed a novel approach for Risk Identification based upon Exploratory Sequential Mixed Method Design which provides the organisation with considerable advantages in the overall Risk Management Process. These include:

- Risk Centric rather than Asset Centric – SQRC is more relevant in today's environment as this methodology is risk centric rather than asset centric. In today's technology landscape of outsourcing, cloud and extranets asset ownership are hard to establish and what the industry needs is risk ownership.
- Flexible – Since one size does not fit all, SQRC is flexible enough to adapt to the organisation by considering the size and the industry that the organisation belongs to. When using SQRC in Risk Identification phase, the applicable risk and impact indicators are defined according to organisational context. This makes Risk Management process highly contextual, flexible and aligned with business.
- Leverages Existing Investments – In Risk Identification phase, SQRC leverages the investments that have already been made by the organisation in information security systems and processes through the use of data generated from existing systems and processes.
- Inspires Greater Confidence – SQRC inspires confidence as risk identification of SQRC is derived through hard facts based on observations and data. There is no room for guesses and speculations.
- Results reflect a more comprehensive and holistic picture rather than a mere snapshot, since the observations span over a considerable period of time.

10. Conclusion

This paper has presented a new approach for Information Security Risk Identification which is objective in nature. Being more objective, this approach provides scientifically determined Risk Indicators as a reliable input for Statistical Risk Analysis. Further it reduces subjectivity, assessor bias that is mandatory for qualitatively managed risk assessments. Thus this reduces the need for organizations to retain subject matter expertise. This approach does away with the tedious Asset-Threat- Vulnerability Trees.

The study and validated results help create the appropriate inputs for Information Security Risk Analysis which has a statistical foundation. This Risk Identification enables a specific, accurate and reliable risk analysis which caters for diverse units of measurement. Leads to an efficient, repeatable, more realistic risk analysis catering for interdependence among Risk Indicators. Based on factual analysis that inspires greater confidence. Enables risk analysis that caters for trend rather than a snapshot. Additionally, information security risk indicators bring in better accountability among stakeholders, while laying down the foundation of a strong security metrics process.

Information Security Risk Indicators program can lay a firm foundation for risk analytics to generate risk trends,

predict future risks better and detect possible outliers through risk analytics over time. This also sets the foundation for further study towards improving risk identification through incorporating data analytics into risk management.

References

[1] Rowe, W.D., *An anatomy of risk*. 1977: Wiley.
[2] ISO, *ISO 31000 - Risk management*. 2009.
[3] Yazar, Z. *A qualitative risk analysis and management tool*. GSEC 2002 [cited Version 1.3.
[4] Radack, S., *CONDUCTING INFORMATION SECURITY-RELATED RISK ASSESSMENTS*. 2012, National Institute of Standards and Technology U.S. Department of Commerce].
[5] Clint Witchalls, J.C., *Information risk Managing digital assets in a new technology landscape*, in *The Economist*. 2013.
[6] Chapelle, A. *The importance of preventative KRIs*. Operational Risk & Regulation 2013.
[7] Jorion, P., *Financial Risk Manager Handbook Second Edition* 2003, USA: John Wiley & Sons.
[8] Young, P.J., *THE USE OF KEY RISK INDICATORS BY BANKS AS AN OPERATIONAL RISK MANAGEMENT TOOL*, in *International conference "Improving Financial institutions: the proper balance between regulation and governance"*. 2012: Helsinki,.
[9] Leisch, A.M.a.F., *semPLS: Structural Equation Modeling Using Partial Least Squares*. 2012.
[10] Svante Wold, M.S., Lennart Eriksson, *PLS-regression: a basic tool of chemometrics*. Chemometrics and Intelligent Laboratory Systems 58 2001 109–130 Ž, 2001.
[11] Shugan, S.M., *Marketing Science, Models, Monopoly Models, and Why We Need Them*. MARKETING SCIENCE Vol. 21, No. 3, Summer 2002, pp. 223–228, 2002.

Upasna Saluja has a Masters in Statistics and is pursuing her PhD in Computer Science with specialization in Information Security, from University of Technology, Malaysia. She is an Information Risk professional having rich experience in Information Security, Business Continuity and Disaster Recovery Management. She is currently working in Operational Risk and Compliance for Australia and New Zealand Banking Group, after having worked in companies like Thomson Reuters and HP. She has industry leading security certifications such as CISSP, CISA, CRISC, ISO 27001 and BS 25999. She has over 20 publications to her credit. She won a best paper award for her paper "Information Risk Management - Qualitative or Quantitative? Cross Industry lessons from the medical and financial field" at The 8th International Symposium on Risk Management and Cyber-Informatics: RMCI 2011, held in Florida, USA.

Norbik Idris is Professor of "Software Engineering & Information Security" at Advanced Informatics School, Universiti Teknologi Malaysia. He is also Founder of the SCAN Group of companies with a niche on information security. He is a CISSP and CISM.