



## Document details

&lt; Back to results | 1 of 1

[Export](#)
[Download](#)
[Print](#)
[E-mail](#)
[Save to PDF](#)
[Add to List](#)
[More... >](#)

 ARPN Journal of Engineering and Applied Sciences [Open Access](#)  
 Volume 10, Issue 23, 2015, Pages 17607-17613

## Risk assessment model for organizational information security (Article)

 Dioubate, B.M.<sup>a</sup>  Molok, N.N.A.<sup>a</sup>, Talib, S.<sup>a</sup>, Tap, A.O.M.<sup>b</sup> 
<sup>a</sup>Department of Information System, International Islamic University Malaysia, Kuala Lumpur, Malaysia<sup>b</sup>Department of Computer Sciences, International Islamic University Malaysia, Kuala Lumpur, Malaysia


## Abstract

[View references \(26\)](#)

Information security risk assessment (RA) plays an important role in the organization's future strategic planning. Generally there are two types of RA approaches: Quantitative RA and qualitative RA. The quantitative RA is an objective study of the risk that use numerical data. On the other hand, the qualitative RA is a subjective evaluation based on judgment and experiences which does not operate on numerical data. It is difficult to conduct a purely quantitative RA method, because of the difficulty to comprehend numerical data alone without a subjective explanation. However, the qualitative RA does not necessarily demand the objectivity of the risks, although it is possible to conduct RA that is purely qualitative in nature. If implemented in silos, the limitations of both quantitative and qualitative methods may increase the likelihood of direct and indirect losses of an organization. This paper suggests a combined RA model from both quantitative and qualitative RA methods to be used for assessing information security risks. In order to interpret and apply the model, a prototype of RA for information security risks will be developed. This prototype will be evaluated by information security risk management experts from the industry. Feedback from the experts will be used to improve the proposed RA model. The implementation of an appropriate model ensures a successful RA method and prevent the organization from the natural and causal risks that are related to securing information assets.

SciVal Topic Prominence 

Topic: Risks | Risk management | Multiple regression

Prominence percentile: 42.242 

## Author keywords

[Information Security Risk Assessment](#)
[Qualitative Risk Assessment](#)
[Quantitative Risk Assessment](#)

ISSN: 18196608

Source Type: Journal

Original language: English


Document Type: Article

Publisher: Asian Research Publishing Network

## References (26)

[View in search results format >](#)
 All
 [Export](#)
[Print](#)
[E-mail](#)
[Save to PDF](#)
[Create bibliography](#)

- 1 Boltz, J. (1999) *Informational Security Risk Assessment: Practices of Leading Organizations*. Cited 41 times. DIANE Publishing

Metrics PlumX Metrics 

Usage, Captures, Mentions, Social Media and Citations beyond Scopus.

## Cited by 0 documents

Inform me when this document is cited in Scopus:

[Set citation alert >](#)[Set citation feed >](#)

## Related documents

Analysis and selection of risk assessment frameworks for cloud based enterprise applications.

Vijayakumar, K. , Arun, C. (2017) *Biomedical Research (India)*

Current challenges in information security risk management

Fenz, S. , Heurix, J. , Neubauer, T. (2014) *Information Management and Computer Security*

The use of the "rational" system of global marketing communications in management of international enterprises

Obolenska, T. , Shatarska, I. , Shevtsov, Y. (2019) *Problems and Perspectives in Management*[View all related documents based on references](#)

Find more related documents in Scopus based on:

[Authors >](#) [Keywords >](#)

- 2 Mouw, E., van't Noordende, G., Louter, B., Olabarriaga, S.D.  
(2013) *A Model-based Information Security Risk Assessment Method for Science Gateways*  
In IWSG
- 
- 3 (2014) *Information technology-Security techniques-Information security management systems-Overview and vocabulary*. Cited 155 times.  
ISO/IEC 27000:2014(E)
- 
- 4 (2014) *Risk-Assessment-Process-Information-Security.pdf*  
Retrieved August 13, 2015  
<https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf>
- 
- 5 Bojanc, R.  
(2012) *Quantitative model for information security risk management*, pp. 267-275. Cited 3 times.
- 
- 6 Bojanc, R.  
(2013) *A Quantitative model for information-security risk management*. Cited 3 times.
- 
- 7 Kleckner, M.  
(2001)  
[Facilitating-qualitative-securityassessment-overview-process-defining-deliverin-431.pdf](#)
- 
- 8 Bojanc, R., Jerman-Blažic, B.  
Quantitative Model for Economic Analyses of information Security investment in an Enterprise information System  
(2012) *Organizacija*, 45 (6), pp. 276-288. Cited 11 times.
- 
- 9 Wawrzyniak, D.  
(2008) *Information security risk assessment-the development of the standard approaches*, pp. 759-764.
- 
- 10 *Security Standards Council*
- 
- 11 Rot, A.  
World Congress on Engineering and Computer Science  
(2008) *WCECS 2008*  
San Francisco, USA, 22-24 October, (2008) Hong Kong: IAENG International Association of Engineers
-