Scopus

Documents

Chandra, N.A.[a] , Ramli, K.[a] , Ratna, A.A.P.[a] , Gunawan, T.S.[b]

Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools
(2022) *Risks*, 10 (8), art. no. 165, .

DOI: 10.3390/risks10080165

[a] Electrical Engineering, The University of Indonesia, Depok, 16424, Indonesia
[b] Electrical and Computer Engineering Department, Kulliyyah of Engineering, International Islamic University Malaysia, P.O. Box 10, Kuala Lumpur, 50728, Malaysia

Abstract
This paper describes the development of situational awareness models and applications to assess cybersecurity risks based on Annex ISO 27001:2013. The risk assessment method used is the direct testing method, namely audit, exercise and penetration testing. The risk assessment of this study is classified into three levels, namely high, medium and low. A high-risk value is an unacceptable risk value. Meanwhile, low and medium risk values can be categorized as acceptable risk values. The results of a network security case study with security performance index indicators based on the percentage of compliance with ISO 27001:2013 annex controls and the value of the risk level of the findings of the three test methods showed that testing with the audit method was 38.29% with a moderate and high-risk level. While the test results with the tabletop exercise method are 75% with low and moderate risk levels. On the other hand, the results with the penetration test method are 16.66%, with moderate and high-risk levels. Test results with unacceptable risk values or high-risk corrective actions are taken through an application. Finally, corrective actions have been verified to prove there is an increase in cyber resilience and security. © 2022 by the authors.

Author Keywords
audit; exercise; penetration test; risk; situational awareness

References

- Afulani, P.A., Dyer, J., Calkins, K., Aborigo, R.A., Mcnally, B., Cohen, S.R.
  Provider knowledge and perceptions following an integrated simulation training on emergency obstetric and neonatal care and respectful maternity care: A mixed-methods study in Ghana
  (2020) *Midwifery*, 85, p. 102667.

- Akinrolabu, O., Nurse, J.R.C., Martin, A., New, S.
  Cyber risk assessment in cloud provider environments: Current models and future needs
  (2019) *Computers & Security*, 87, p. 101600.
  a

- Akinrolabu, O., New, S., Martin, A.
  CSCCRA: A Novel Quantitative Risk Assessment Model for SaaS Cloud Service Providers
  (2019) *Computers*, 8.
  b

- Aksu, M.U., Dilek, M.H., Tatlı, E.İ., Bicakci, K., Dirik, H.I., Demirezen, M.U., Aykır, T.
  A Quantitative CVSS-Based Cyber Security Risk Assessment Methodology For IT Systems
  (2017) *Paper presented at the 2017 International Carnahan Conference on Security Technology (ICCST)*,
  Madrid, Spain, October 23–26

- Borgardt, J., Canaday, J., Chamberlain, D.
  Results from the second Galaxy Serpent web-based table top exercise utilizing the concept of nuclear forensics libraries

(2017) *Journal of Radioanalytical and Nuclear Chemistry*, 311, pp. 1517-1524.

- Burke, G., Saxena, N.
  Cyber Risks Prediction and Analysis in Medical Emergency Equipment for Situational Awareness
  (2021) *Sensor*, 21.

- Caputo, F., Carrubbo, L., Sarno, D.
  The influence of cognitive dimensions on the consumer-SME relationship: A sustainability oriented view
  (2018) *Sustainability*, 10.

- Chandra, N.A., Ratna, A.A.P., Ramli, K.
  Development and Simulation of Cyberdisaster Situation
  (2022) *Sustainability*, 14.

- (2012) *Guide for Conducting Risk Assessments*,
  National Institute of Standards and Technology Special Publication 800-30 Revision 1, Computer Security Division, Washington, DC

- Corrales-Estrada, A.M., Gómez-Santos, L.L., Bernal-Torres, C.A., Rodriguez-López, J.E.
  Sustainability and resilience organizational capabilities to enhance business continuity management: A literature review
  (2021) *Sustainability*, 13.

- de Gusmão, A.P.H., Silva, M.M., Poleto, T., Silva, L.C.E., Costa, A.P.C.S.
  Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory
  (2018) *International Journal of Information Management*, 43, pp. 248-260.

- Endsley, M.R.
  Toward a Theory of Situation Awareness in Dynamic Systems
  (1995) *Human Factors Journal*, 37, pp. 32-64.

- Fogli, D., Greppi, C., Guida, G.
  Design patterns for emergency management: An exercise in reflective practice
  (2017) *Information & Management*, 54, pp. 971-986.

- Franke, U., Brynielsson, J.
  Cyber situational awareness e A systematic review of the literature
  (2014) *Computer & Security*, 46, pp. 18-31.

- Gencer, K., Başçiftçi, F.
  The fuzzy common vulnerability scoring system (F-CVSS) based on a least squares approach with fuzzy logistic regression
  (2021) *Egyptian Informatics Journal*, 22, pp. 145-153.

- Ghanem, M.C., Chen, T.M.
  Reinforcement Learning for Efficient Network Penetration Testing
  (2020) *Information*, 11.

- Gomes, J.O., Borges, M., Huber, G.J., Carvalho, P.V.R.
  Analysis of the resilience of team performance during a nuclear emergency response exercise
  (2014) *Applied Ergonomics*, 45, pp. 780-788.

- Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., Good, T.
  (2006) *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, Special Publication (NIST SP)*,
  National Institute of Standards and Technology, Gaithersburg, Available online

- Griogoriadis, C., Laborde, R., Verder, A., Kotzanikolaou, P.
  An Adaptive, Situation-Based Risk Assessment and Security Enforcement Framework for the Maritime Sector
  (2022) *Sensor*, 22.

- (2022),
  Available online

- (2009) *Guidelines for Risk Management—Risk Assessment Techniques*, p. 22.
  ISO, Geneva

- (2018) *Guidelines for Auditing Management Systems*, p. 8.
  ISO, Geneva

- (2018) *Information Technology—Security Techniques—Information Security Risk Management by International Electrotechnical Commission*, p. 1.
  ISO, Geneva

- (2018) *Guidelines for Cybersecurity*, pp. 5-11.
  ISO, Geneva

- (2018) *Risk Management-Guideline by International Electrotechnical Commission*, p. 1.
  ISO, Geneva

- (2013) *Information Technology—Security Techniques—Information Security Management Systems—Requirements*,
  ISO, Geneva

- Ji, X., Wei, H., Chen, Y., Ji, X.-F., Wu, G.
  Three-Stage Dynamic Assessment Framework for Industrial Control System Security Based on a Method of W-HMM
  (2022) *Sensor*, 22.

- Jiang, L., Jayatilaka, A., Nasim, M., Grobler, M., Zahedi, M., Babar, M.A.
  Systematic Literature Review on Cyber Situational Awareness Visualizations
  (2022) *IEEE Access*, 10, pp. 57525-57554.

- Jofre, M., Navarro-Llobet, D., Agulló, R., Puig, J., Gonzalez-Granadillo, G., Zamorano, J.M., Romeu, R.
  Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach
  (2021) *Applied Sciences*, 11.

- Knowles, W., Baron, A., McGarr, T.
  The simulated security assessment ecosystem: Does penetration testing need standardisation?
  (2016) *Computers & Security*, 62, pp. 296-316.

- Kure, H.I., Islam, S., Razzaque, M.A.
  An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System
  (2018) *Applied Science*, 8.

- Leszczyna, R.
  Standards on cyber security assessment of smart grid
  (2018) *International Journal of Critical Infrastructure Protection*, 22, pp. 70-89.

- Li, J., Ou, X., Rajagopalan, R.
  Uncertainty and Risk Management in Cyber Situational Awareness
  (2010) *Cyber Situational Awareness*, pp. 51-68.
  Springer, New York

- Musharraf, M., Khan, F., Veitch, B.
  Modeling and simulation of offshore personnel during emergency situations
  (2019) *Safety Science*, 111, pp. 144-153.

- Nikoloudakis, Y., Kefaloukos, I., Klados, S., Panagiotakis, S., Pallis, E., Skianis, C., Markakis, E.K.
  Towards a Machine Learning Based Situational Awareness Framework for Cybersecurity: An SDN Implementation
  (2021) *Sensor*, 21.

- Poller, B., Hall, S., Bailey, C., Gregory, S., Clark, R., Roberts, P., Tunbridge, A., Evans, C.
  'VIOLET': A fluorescence-based simulation exercise for training healthcare workers in the use of personal protective equipment
  (2018) *Journal of Hospital Infection*, 99, pp. 229-235.

- Porcuna-Enguix, L., Bustos-Contell, E., Serrano-Madrid, J., Labatut-Serer, G.
  Constructing the Audit Risk Assessment by the Audit TeamLeader When Planning: Using Fuzzy Theory
  (2021) *Mathematics*, 9.

- Ramanauskaitė, S., Urbonaitė, N., Grigaliūnas, Š., Preidys, S., Trinkūnas, V., Venčkauskas, A.
  Educational Organization's Security Level Estimation Model
  (2021) *Applied Science*, 11.

- Rapuzzi, R., Repetto, M.
  Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model
  (2018) *Future Generation Computer Systems*, 85, pp. 235-249.

- Sandström, B.E., Eriksson, H., Norlander, L., Thorstensson, M., Cassel, G.
  Training of public health personnel in handling CBRN emergencies: A table-top exercise card concept
  (2014) *Environment International*, 72, pp. 164-169.

- Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M.
  Taxonomy of information security risk assessment (ISRA)
  (2016) *Computer & Security*, 57, pp. 14-30.

- Shamala, P., Ahmad, R., Zolait, A.H., Sahib, S.B.
  Collective information structure model for Information Security Risk Assessment (ISRA)
  (2015) *Journal of Systems and Information Technology*, 17, pp. 193-219.

- Silva, M.M., Gusmão, D., Gusmão, A.P.H., Poleto, T., Silva, L.C.E., SeixasCosta, A.P.C.
  A multidimensional approach to information security risk management using FMEA and fuzzy theory
  (2014) *International Journal of Information Management*, 34, pp. 733-740.

- Silva, C., Magano, J., Moskalenko, A., Nogueira, T., Dinis, M.A.P., Sousa, H.F.P.E.
  Sustainable Management Systems Standards (SMSS): Structures, Roles, and Practices in Corporate Sustainability
  (2020) *Sustainability*, 12.

- Skryabina, E.A., Betts, N., Reedy, G., Riley, P., Amlôt, R.
  The role of emergency preparedness exercises in the response to a mass casualty terrorist incident: A mixed methods study
  (2020) *International Journal of Disaster Risk Reduction*, 46, p. 101503.
  33312855

- Taherdoost, H.
  A Review on Risk Management in Information Systems: Risk Policy, Control and Fraud Detection
  (2021) *Electronic*, 10.

- Walkowski, M., Oko, J., Sujecki, S.
  Vulnerability Management Models Using a Common Vulnerability Scoring System
  (2021) *Applied Science*, 22.

- Wangen, G., Hallstensen, C., Snekkenes, E.
  A framework for estimating information security risk assessment method completeness, Core Unified Risk Framework, CURF
  (2018) *International Journal Information Security*, 17, pp. 681-699.

- Webb, J., Ahmad, A., Maynard, S.B., Shanks, G.
  A Situation awareness model for information security risk management
  (2014) *Computers & Security*, 44, pp. 1-15.

- Xi, R., Yun, X., Hao, Z.
  Framework for risk assessment in cyber situation awareness
  (2018) *IET Information Security*, 13, pp. 149-156.

- Yusgiantoro, P.
  (2014) *Pedoman Pertahanan Siber, Peraturan Menteri Pertahanan Republik Indonesia, Jakarta*, p. 14.
  Available online

- Zhou, S., Liu, J., Hou, D., Zhong, X., Zhang, Y.
  Autonomous Penetration Testing Based on Improved Deep Q-Network
  (2021) *Applied Science*, 11.

Correspondence Address
Ramli K.; Electrical Engineering, Indonesia; email: kalamullah.ramli@ui.ac.id

Publisher: MDPI

ISSN: 22279091
Language of Original Document: English
Abbreviated Source Title: Risks
2-s2.0-85137366773
Document Type: Article
Publication Stage: Final
Source: Scopus