ABSTRAK

PERBANDINGAN ANTARA ISO/IEC 27035:2011 DENGAN NIST SP.800-61r2

Oleh

Yeni Rimawati

NIM : 23215056

(Tugas Mata Kuliah EL.6115 Tahun 2016)

Tak dapat dipungkiri bahwa saat ini *lifeline* suatu organisasi tidak hanya bergantung pada uang namun juga informasi. Dalam satu dekade terakhir, informasi telah menjadi aset yang paling berharga bagi organisasi [1]. Seperti halnya aset penting lainnya, maka keberadaan informasi hendaknya dilindungi dengan baik. Tujuan keamanan informasi yaitu memastikan bahwa informasi harus terjaga kerahasiaannya (*confidentiality*), keutuhannya (*integrity*) dan ketersediaannya (*availability*) [2]. Namun, dalam menjaga aspek-aspek tersebut tidak menutup kemungkinan terjadi hal yang tidak diinginkan. Ancaman terhadap informasi dan sistem TI jumlahnya semakin meningkat dari hari ke hari. Selain itu, organisasi juga harus menghadapi *attackers* dengan *skills* yang dapat melakukan serangan hingga berdampak pada kerusakan infrastruktur TI [3].

Pendekatan sistematis untuk mengendalikan insiden keamanan informasi adalah dengan menerapkan manajemen insiden keamanan informasi [3]. Penerapan manajemen insiden keamanan informasi dapat diadopsi dari standar ISO/IEC 27035:2011 maupun beberapa *guideline* seperti NIST, ENISA, dan SANS yang secara umum memiliki ide yang hampir sama [4].

Pada dokumen ISO/IEC 27035:2011 penanganan insiden keamanan informasi dibagi menjadi lima tahap. Sedangkan pada dokumen NIST SP.800-61r2 tahapan penanganan insisen dibagi menjadi empat tahap. Makalah ini bertujuan untuk menggali lebih dalam lagi perbedaan antara standar ISO/IEC 27035:2011 dengan *guideline* NIST SP.800-61r2.

Daftar Pustaka

[1] A. L. Mesquida and A. Mas, "Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension," *Computers & Security*, vol. 48, pp. 19–34, Feb 2015. Available: http://www.sciencedirect.com/science/article/pii/S0167404814001345

[2] Information technology – Security techniques – Information security management systems - Requirements, ISO/IEC 27001, 2013. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

[3] K. Bernsmed and I. A. Tondel, "Forewarned is Forearmed: Indicators for Evaluating Information Security Incident Management," in *2013 Seventh International Conference on IT Security Incident Management and IT Forensics (IMF)*, 2013, pp. 3–14. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6568549&newsearch=true&queryText=Karin%20Bernsmed

[4] M. B. Line, I. A. Tondel, and M. G. Jaatun, "Information Security Incident Management: Planning for Failure," in *2014 Eighth International Conference on IT Security Incident Management and IT Forensics (IMF)*, 2014, pp. 47–61. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6824081&newsearch=true&queryText=Maria%20B.%20Line

[5] Information technology – Security techniques – Information security incident management, ISO/IEC 27035, 2011. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379

[6] Computer Security Incident Handling Guide, NIST SP.800-61r2, 2012. Available: http://dx.doi.org/10.6028/NIST.SP.800-61r2

[7] C. Hove, M. Tarnes, M. B. Line, and K. Bernsmed, "Information Security Incident Management: Identified Practice in Large Organizations," in *2014 Eighth International Conference on IT Security Incident Management and IT Forensics (IMF)*, 2014, pp. 27–46. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6824080&newsearch=true&queryText=Cathrine%20Hove

[8] I. A. Tondel, M. B. Line, and M. G. Jaatun, “Information security incident management: Current practice as reported in the literature,” *Computers & Security*, vol. 45, pp. 42–57, Sep. 2014. Available: http://www.sciencedirect.com/science/article/pii/S0167404814000819

[9] R. Baskerville, P. Spagnoletti, and J. Kim, “Incident-centered information security: Managing a strategic balance between prevention and response,” *Information & Management*, vol. 51, no. 1, pp. 138–151, Jan. 2014. Available: http://www.sciencedirect.com/science/article/pii/S0378720613001171

[10] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, “Incident response teams – Challenges in supporting the organisational security function,” *Computers & Security*, vol. 31, no. 5, pp. 643–652, Jul. 2012. Available: http://www.sciencedirect.com/science/article/pii/S0167404812000624

[11] N. H. Ab Rahman and K.-K. R. Choo, “A survey of information security incident handling in the cloud,” *Computers & Security*, vol. 49, pp. 45–69, Mar. 2015. Available: http://www.sciencedirect.com/science/article/pii/S0167404814001680