Perancangan Manajemen Risiko Keamanan Informasi Menggunakan International Organization for Standardization / International Electrotechnical Commission 27005:2018: Studi Kasus Badan Narkotika Nasional = Information Security Risk Management Design Using the International Organization for Standardization / International Electrotechnical Commission 27005:2018: A Case Study of the National Narcotics Board

Hasan Shahab, author

Abstrak

Badan Narkotika Nasional (BNN) adalah lembaga pemerintahan yang bertugas untuk Pencegahan dan Pemberantasan Penyalah gunaan dan Peredaran Gelap Narkotika (P4GN). BNN memiliki Pusat Penelitian Data dan Informasi (Puslitdatin) yang bertanggung jawab dalam pengelolaan teknologi informasi dan komunikasi (TIK). Masalah utama yang dihadapi adalah adanya risiko serangan siber yang masuk ke BNN tinggi yang juga diperkuat dengan hasil evaluasi SPBE (Sistem Pemerintahan Berbasis Elektronik) BNN di tahun 2021 berada pada angka indeks 2,21 dari skala 5. Rendahnya indeks SPBE tahun 2021, salah satunya disebabkan karena indikator 21 (Pelaksanaan Manajemen Risiko) masih berada pada level 1. Penelitian ini bertujuan untuk menghasilkan perancangan manajemen risiko keamanan informasi yang dapat mendukung pelaksanaan SPBE pada Badan Narkotika Nasional. Penelitian ini bermanfaat untuk mengetahui identifikasi risiko dalam penilaian risiko keamanan informasi, sehingga dapat memberikan penilaian konsekuensi dan dampak risiko keamanan informasi serta dapat memberikan rekomendasi kontrol terkait pengelolaan risiko (mitigasi risiko) kepada organisasi. Penelitian ini menggunakan metode kualitatif, yang dilakukan dengan wawancara kepada tim teknis TIK di Puslitdatin BNN serta menggunakan teknik analisis tematik. Kerangka kerja manajemen risiko keamanan informasi yang digunakan dalam penelitian ini adalah International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27005:2018, ISO/IEC 27002:2022, dan National Institute of Standards and Technology Special Publication 800-30 Revision 1 (NIST SP 800-30 Rev.1). Aset adalah segala sesuatu yang memiliki nilai bagi Puslitdatin dan karenanya memerlukan perlindungan, sedangkan ancaman adalah peristiwa apa pun yang berpotensi berdampak buruk pada operasi dan aset Puslitdatin melalui perusakan, pengungkapan, atau modifikasi informasi yang tidak sah, dan penolakan atau penghentian layanan. Dari penelitian didapatkan 78 aset yang teridentifikasi berkaitan dengan kegiatan Puslitdatin BNN dan terdapat 570 skenario peristiwa ancaman dari 16 sumber ancaman. Hasil penilaian tingkat risiko menunjukan sebanyak 37 skenario perlu dimitigasi dan 533 skenario diterima oleh Puslitdatin BNN. Pada penanganan risiko keamanan informasi dihasilkan 20 jenis rekomendasi kontrol yang diantaranya yaitu membuat kebijakan keamanan informasi, penerapan kontrol hak akses, penerapan secure authentication, pengadaan genset khusus data center, penerapan manajemen screen and desk policy, dan melakukan enkripsi data/informasi penting. Hasil penelitian ini adalah rancangan dokumen manajemen risiko keamanan informasi BNN.

.....The National Narcotics Board (BNN) is a government agency tasked with the Prevention and Eradication of Narcotics Abuse and Illicit Trafficking (P4GN). BNN has a Data and Information Research Center (Puslitdatin) which is responsible for managing information and communication technology (ICT).

The main problem faced is the high risk of cyber attacks entering the BNN which is also reinforced by the evaluation results of the BNN's SPBE (Electronic Based Government System) in 2021 which is at an index number of 2.21 on a scale of 5. The low SPBE index in 2021, one of them because indicator 21 (Implementation of Risk Management) is still at level 1. This study aims to produce an information security risk management design that can support the implementation of SPBE at the National Narcotics Agency. This research is useful for knowing risk identification in information security risk assessment, so that it can provide an assessment of the consequences and impacts of information security risks and can provide control recommendations related to risk management (risk mitigation) to organizations. This study used a qualitative method, which was conducted by interviewing the ICT technical team at the BNN Research and Data Center, and using thematic analysis techniques. The information security risk management framework used in this study is the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27005:2018, ISO/IEC 27002:2022, and National Institute of Standards and Technology Special Publication 800-30 Revision 1 (NIST SP 800-30 Rev.1). Assets are anything that has value to Puslitdatin and therefore requires protection, while threats are any events that have the potential to adversely affect Puslitdatin operations and assets through unauthorized destruction, disclosure or modification of information, and/or denial of service. From the research, it was found that 78 assets were identified as related to Puslitdatin BNN activities and 570 threat event scenarios from 16 threat sources. The results of the risk level assessment show that as many as 37 scenarios need to be mitigated and 533 scenarios are accepted by the BNN Research and Data Center. In handling information security risks, 20 types of control recommendations were produced, including making information security policies, implementing access rights controls, implementing secure authentication, procuring special data center generators, implementing screen and desk management policies, encrypting important data/information, and others. The result of this research is the design of BNN's information security risk management document.