Desain dan Evaluasi Perencanaan dalam Penanganan Bukti Digital pada Sistem Peradilan Pidana Terpadu Berdasarkan NIST SP800-53 Revision 5 Menggunakan NIST Maturity = Design and Evaluation Planning in Digital Evidence Handling on Integrated Criminal Justice System based on NIST SP800-53 Revision 5 Using NIST Maturity

Chandra Tirta Aditya Gunawan, author

Abstrak

Tantangan penanganan bukti digital dalam sistem peradilan terpadu adalah rentan, mudah diubah, dan dimusnahkan, sehingga perlu dilindungi dari ancaman keamanan saat disimpan, diproses, dan dikirimkan oleh setiap penegak hukum yang saling berhubungan. Penelitian ini bertujuan merancang desain terintegrasi penanganan bukti digital pada sistem peradilan pidana terpadu berdasarkan Kitab Undang-Undang Hukum Acara Pidana menggunakan NIST SP800-53 Rev 5 sebagai upaya pengendalian keamanan informasi dan privasi. Desain terintegrasi ini memiliki 8 sasaran kontrol, 34 klausul kontrol dan 110 kegiatan pengamanan informasi dan privasi. Selanjutnya melakukan evaluasi perencanaan dengan mengukur maturitas organisasi berdasarkan desain tersebut menggunakan NIST Maturity. Pengukuran dilakukan secara kualitatif, melakukan wawancara dengan purposive sampling dan penentuan responden berdasarkan peran dan tanggung jawab personil menggunakan RACI Matriks. Hasil pengukuran maturitas organisasi XYZ senilai 2,35 (dalam skala 0-5) digunakan sebagai bahan evaluasi perencanaan dalam upaya meningkatkan kontrol keamanan organisasi XYZ sebagai lembaga penegakan hukum. Organisasi secara umum sudah menerapkan kontrol keamanan informasi dengan pola yang berulang namun belum terdokumentasi dengan baik, sehingga penerapannya masih belum konsisten. Hasil yang diharapkan organisasi berada pada tingkat 3, sehingga nilai kesenjangannya senilai 0,65. Organisasi perlu untuk mendokumentasikan kontrol keamanannya dalam bentuk standar operasional atau panduan sehingga memberikan tingkat keamanan informasi dan privasi yang lebih baik. Setelah itu, menguraikan rekomendasi berdasarkan tingkat organisasi pada masing-masing klausul kontrol dan memberikan uraian implementasinya. Terakhir, memberikan urutan prioritas berdasarkan risiko keamanan informasi (confidentiality, integrity, dan availability) pada masing-masing sasaran kontrol yang dipadukan dengan risiko yang tertuang dalam dokumen manajemen risiko organisasi (risiko hukum, risiko kepatuhan, risiko regulasi, dan risiko operasional). Hasilnya, sasaran kontrol yang menjadi prioritas implementasi yaitu Pengiriman Data (DTR), Penyimpanan Data (DST), Pencadangan Data (DBU), Dokumentasi (DOC), Identifikasi dan Klasifikasi Data (DIC), Koleksi dan Akuisisi (CLA), Pengembalian Data (DRT) dan Penghapusan Data (DSN).

.....The challenge of handling digital evidence in an integrated justice system is that it is vulnerable, easy to change, and destroyed, so it requires to be protected from security threats when it is stored, processed, and transmitted by every interconnected law enforcement agency. This study aims to design an integrated design for handling digital evidence in an integrated justice system based on the Criminal Procedure Code using NIST SP800-53 Rev 5 as an effort to control information security and privacy. This integrated design has 8 control targets, 34 control clauses, and 110 information security and privacy activities. Then evaluate the plan by measuring the maturity of the organization based on the design using NIST Maturity. Measurements were carried out qualitatively, using purposive sampling and determining respondents based on the roles and

responsibilities of personnel using the RACI Matrix. The results of measuring the maturity of the XYZ organization of 2.35 (on a scale of 0-5) are used as planning evaluation materials to improve security control of the XYZ organization as a law enforcement agency. Organizations, in general, have implemented information security controls with repetitive patterns but have not been well documented, so the implementation is still inconsistent. The expected result of the organization is at level 3, so the value of the gap is 0.65. Organizations need to document their security controls in the state of operational standards or guidelines to provide a better level of information security and privacy. After that, it outlines the recommendations based on the organizational level in each control clause and describes its implementation. Finally, assigning a priority order based on information security risks (confidentiality, integrity, and availability) for each control target combined with the risks contained in the organization's risk management documents (legal risk, compliance risk, regulatory risk, and operational risk). As a result, the control targets that become implementation priorities are (DTR) data transfer, (DST) data storage, (DBU) data backup, (DOC) documentation, (DIC) data identification and classification, (CLA) collection and acquisition, (DRT) data return and (DSN) data sanitization.