# Manajemen Risiko Keamanan Informasi pada Sistem Informasi Pemantauan Tindak Lanjut Studi Kasus: Badan Pemeriksa Keuangan = Information Security Risk Management on The Monitoring Follow-up Information Systems A Case Study: The Audit Board of The Republic of Indonesia

Afwan Badru Naim, author



---

Abstrak

BPK telah mengimplementasikan Sistem Informasi Pemantauan Tindak Lanjut (SIPTL) untuk melaksanakan dan memantau tindak lanjut rekomendasi hasil pemeriksaan. Sejalan dengan mandat yang diberikan Undang-Undang Dasar 1945 untuk melaksanakan pemeriksaan atas pengelolaan dan tanggung jawab keuangan negara secara bebas dan mandiri, keamanan informasi hasil pemeriksaan merupakan hal penting bagi BPK. Namun demikian, dalam operasionalnya, pemanfaatan SIPTL belum sesuai dengan standar manajemen risiko keamanan informasi. Penelitian ini bertujuan untuk mendapatkan rancangan manajemen risiko keamanan informasi SIPTL. Penelitian ini menggunakan metode kualitatif dan pengumpulan data melalui wawancara dan studi literatur. Wawancara dilakukan dengan pejabat eselon III dan IV pada Biro TI BPK. Kerangka kerja yang digunakan pada penelitian ini berdasarkan SNI ISO/IEC 27005:2018 dengan penanganan risiko menggunakan SNI ISO/IEC 27001:2013, dan SNI ISO/IEC 27002:2013. Hasil yang didapatkan dari penelitian ini adalah 13 skenario risiko di mana dua risiko mempunyai level yang tinggi, lima risiko mempunyai level sedang, dan enam risiko memiliki level rendah. Berdasarkan skenario risiko selanjutnya disusun rancangan manajemen risiko keamanan informasi SIPTL, yang dapat digunakan sebagai bahan pertimbangan dalam penerapan manajemen risiko keamanan informasi di BPK.

.....BPK has implemented the Follow-up Monitoring Information Systems (SIPTL) to conduct and monitor follow-up of recommendations-audit result. In line with the mandate given by the 1945 Constitution to audit towards management of and accountability for the state’s finances a free and independent, the information security of audit results is an important matter for BPK. However, in its operations, the utilization of SIPTL is not in accordance with information security risk management standards. This study aims to obtain a SIPTL information security risk management design. This research uses qualitative methods and data collection through interviews and literature studies. Interview was conducted with middle level official at BPK’s Bureau of IT. The framework used in this research is based on SNI ISO / IEC 27005: 2018, and risk treatment based on SNI ISO / IEC 27001: 2013 also SNI ISO / IEC 27002: 2013. The results obtained from this study are 13 risk scenarios including two high level risks, five medium level risks, and six low level risks. Based on the risk scenario, the SIPTL information security risk management design is then prepared, which can be used as recommendation towards the implementation of information security risk management at BPK.