

Abstract

In the era of information technology, people increasingly crave fast government services and unlimited distance, space, and time. Therefore, the government responds to these needs by implementing an Electronic-Based Governance System (SPBE). SIPP is one of the services that the court provides as a service provider to the community. In providing good services, integration between good information is required so that the services provided are fast and precise. In addition to being an information service, SIPP also serves as one of the tools used by the Supreme Court of the Republic of Indonesia in overseeing the performance of courts in all corners of Indonesia. In the Road Map of the Supreme Court in the year SIPP is part of one of the Quick Win programs of the Supreme Court that has been adapted to the Blueprint of the Supreme Court in 2010-2035, namely in the Information Technology Development program.

In 2020 the Court will have many problems in the field of information security, especially on the websites of courts across the country including SIPP. More than 20 courts throughout Indonesia experienced hacker attacks. Which damage to both the website, the SIPP web feature and the court library featured.

Based on the Minister of Communication and Informatics Regulation No. 4 of 2016 in article 7, every SPBE organizer must implement information security following the information security standards described by the Ministry of Communication and Information. Since this regulation is conceived to minimize the risk of security breach on SPBE, and there is such numerous security breach in 2020, therefore this indicates poorly implemented of the regulation. Based on this finding, this research aims to investigate which area is neglected. To achieve this, this research employs gap analysis using ISO/IEC 27001 and maturity level to reveal the neglected areas in information security.

In this research, the method used is qualitative, the data collection, and data validation using triangulation techniques, namely through interviews, observations, and documentation. Gap analysis is used in data analysis and to measure maturity levels using CMMI(Capability Maturity Model for Integration).

The results showed that of the ten annexes that were tested, the SIPP level of information security in the Court was at level 3 (Defined), which means that the Court knows there are problems that must be addressed, there are several processes that have not been standardized and documented and are more likely to handle problems per case.

Keywords: *ISO 27001, Assesment, Information Security, CMMI, SIPP*