Evaluasi pengelolaan risiko TI pada instansi pemerintah : studi kasus PPATK = Evaluation of IT risk management in government agencies a case study of PPATK

Bambang Hadi Purnomo, author

Abstrak

Undang-Undang No 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU PP TPPU) menjadikan Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) sebagai focal point dalam upaya Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang di Indonesia. Dalam pelaksanaan tugas pokok dan fungsi PPATK tidak terlepas dari penggunaan Teknologi Informasi (TI) untuk mengumpulkan data, analisis, menyediakan informasi dan layanan Teknologi Infomasi dan Komunikasi (TIK) yang berkualitas.
Direktorat Operasi Sistem (DOS) merupakan salah satu unit kerja bidang TI yang memiliki peranan penting untuk mencapai keberhasilan implementasi fungsi SI/TI. Dalam melaksanakan kegiatan mendukung dan memberi nilai tambah proses kerja, tidak pernah bebas dari dan harus selalu berhadapan dengan kemungkinan timbulnya berbagai macam gangguan TI. Apabila gangguan tersebut tidak ditangani secara serius, selain akan menimbulkan risiko operasional, juga akan mempengaruhi risiko reputasi dan berdampak pada menurunnya tingkat kepercayaan publik. Oleh sebab itu, perlu dilakukan pengelolaan terhadap risiko tersebut.

Untuk mengelola risiko TI salah satunya harus memiliki daftar IT Risk Profile (profil risiko TI) yang diperoleh dengan cara melakukan penilaian risiko pada aset TI yang mendukung proses kerja utama. Dengan memiliki profil risiko TI, DOS dapat mengoptimalkan manfaat dan mengurangi dampak risiko akibat penggunaan TI dalam menjalankan tugas pokok dan fungsi (Tupoksi) mendukung proses kerja utama PPATK. RiskIT sebagai salah satu kerangka kerja manajemen risiko TI dapat dipertimbangkan dan diterapkan oleh PPATK untuk pengelolaan risiko TI.

Hasil dari penulisan ini berupa profil dan langkah mitigasi risiko TI secara lengkap sebagai salah satu langkah terpadu untuk menjamin keberlangsungan layanan agar tetap dapat berfungsi dengan baik. Dengan mengetahui risiko penggunaan TI mendorong kesadaran bagi seluruh pegawai untuk melindungi aset TI dan citra organisasi dan dapat dijadikan masukan atau pertimbangan bagi manajemen dalam mengambil keputusan yang lebih baik berdasarkan pengetahuan risiko yang dimiliki sehingga alokasi penggunaan sumber daya lebih efisien.
.....Law Number 8 Year 2010 Concerning the Prevention and Eradication of Money Laundering (AML Law) has made the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) as the focal point in preventing and eradicating money laundering in Indonesia. In terms of conducting its main duties and functions, PPATK could not be separated from using Information Technology (IT) to collect data, conduct analysis, and provide information and services of Communication and Information Technology (CIT) with high quality.

The Directorate of System Operation (DOS) is one of the working units in IT that has important role in achieving successful implementation on IS/IT functions. In conducting its activity to support and give added-value towards working process, PPATK may deal with possibilities of IT troubles. If those troubles could not be handled seriously, not only they could cause operational risks, but also may influence reputation risk and have an impact to the decrease of public trust. Therefore, the risks should be managed properly.

In order to manage IT risks, one of the solutions is to have IT Risk Profiles gained by assessing risks towards IT assets that support core businesses. By having IT Risk Profiles, DOS can optimize the benefits and mitigate risk impact due to IT application when conducting main duties and functions to support core businesses of PPATK. Risk IT as the working framework of IT risk management could be considered and implemented by PPATK in managing IT risks.

The result from this writing is comprehensive profiles and mitigation steps on IT risks as integrated measures to ensure services sustainability so it can work appropriately. By knowing the risks in IT application, it could raise the awareness to all employees for protecting IT assets and organization image, and can be used as inputs or consideration for management in having better decision-making based on retained risks knowledge to achieve more efficient allocation of resources.