Perancangan rencana kontingensi Pusat Data: Studi Kasus Kementerian Luar Negeri = Designing data center contingency plan: a case study at the Ministry of Foreign Affairs

Dany Pus Apriyanto, author

Abstrak

Peraturan Pemerintah Nomor 82 Tahun 2012 mewajibkan Penyelenggara Sistem Elektronik melakukan pengamanan terhadap Sistem Elektronik. Kementerian Luar Negeri Kemenlu melakukan evaluasi tingkat kesiapan pengamanan informasi menggunakan Indeks Keamanan Informasi KAMI guna memenuhi standar Sistem Manajemen Pengamanan Informasi.
Hasil penilaian Indeks KAMI Tahun 2015 menyatakan bahwa Sistem Elektronik Kemenlu berada dalam kategori strategis, namun tingkat kesiapan pengamanan informasi Kemenlu berada dalam kategori tidak layak. Berdasarkan kondisi tersebut, aspek availability layanan TIK Kemenlu tidak terpenuhi ketika terjadi pemeliharaan jaringan listrik kantor Kemenlu di Pejambon. Seluruh layanan TIK Kemenlu tidak dapat diakses selama 10 jam, padahal Kemenlu sudah memiliki fasilitas pusat pemulihan bencana di Cijantung. Berdasarkan analisis fishbone, salah satu sebab permasalahan tidak layaknya pengamanan informasi Kemenlu adalah belum adanya rencana keberlangsungan layanan TIK serta rencana pemulihan bencana. Untuk meningkatkan nilai Indeks KAMI dan untuk menjaga keberlangsungan layanan TIK Kemenlu dengan memanfaatkan infrastruktur yang ada maka perlu disusun rancangan rencana kontingensi pusat data Kemenlu. Perancangan rencana kontingensi dalam penelitian ini mengacu pada kerangka kerja NIST 800-34 Rev.1.
Penelitian ini merupakan penelitian kualitatif dengan kategori studi kasus. Pengumpulan data dilakukan melalui wawancara terhadap pejabat pengelola TIK Kemenlu dan pejabat pemilik atau pengguna layanan TIK serta melalui observasi lapangan. Proses analisis dampak bisnis dilakukan guna mendapatkan tingkat kekritisan sistem informasi terhadap kegiatan utama Kemenlu. Strategi pemulihan layanan teknologi informasi disusun berdasarkan urutan tingkat kekritisan sistem informasi dari yang tertinggi hingga terendah.
Penelitian ini berhasil mengidentifikasi tingkat kekritisan layanan sistem informasi yang terkait dengan kegiatan utama Kemenlu beserta kebutuhan sumber daya pendukungnya. Berdasarkan tingkat kekritisan tersebut, tiga layanan membutuhkan strategi pemulihan fault tolerance, 13 hot site, dan sisanya warm site. Strategi kontingensi tersebut kemudian dituangkan dalam dokumen usulan rencana kontingensi pusat data Kemenlu.
<hr><i>Government Regulation Number 82 Year 2012 obligates all electronic system operators to secure their electronic systems. The Ministry of Foreign Affairs of Indonesia Kemenlu has used the Information Security KAMI Index to evaluate the level of information security preparedness to meet the standards of Information System Security Management.
The results of 2015 KAMI Index stated that the Kemenlu rsquo s electronic system is classified as strategic, however its level of information security preparedness is in the category of not reliable. According to these conditions, Kemenlu could not meet the aspect of ICT services availability, for it could not provides its ICT services to users during power outage incidences at Kemenlu Headquarter in Pejambon. Although Kemenlu

has built a Disaster Recovery Center facility in Cijantung, at the time of power outages, the entire Kemenlu rsquo s ICT services could not be accessed, for as long as 10 hours.
According to fishbone analysis, one of causes that contributed to Kemenlu rsquo s information security preparedness unreliability is the lack of continuity plans for ICT services and disaster recovery plans. To increase its KAMI Index and maintain its ICT services continuity, Kemenlu needs to design data center contingency plan by utilizing the existing infrastructure. The design of data center contingency plan in this research is based on NIST 800 34 Rev.1 framework which was adjusted for Kemenlu data center.
This research applies a qualitative research method using a case studies. Data gathering and fact finding were done by interviewing Kemenlu rsquo s ICT supervisors, owners, and users, as well as on site observation. Business impact analysis was performed to evaluate the impact of information system unavailability to Kemenlu rsquo s main activities. Contingency strategies are created based on the order of information system criticality, from most critical to less critical.
This research has successfully identified the degree of criticality of information systems related to Kemenlu rsquo s main activities as well as its necessary ICT resources. Based on the findings of the criticality degree, there are three information system that require fault tolerance as recovery strategy, 13 require hot site and the remaining require warm site.This contingency strategy are then documented into proposed data center contingency plan.</i>