BAB 5
PENUTUP

5.1. Kesimpulan

Berdasarkan hasil dan pembahasan yang telah dilakukan mengenai analisis manajemen risiko keamanan sistem informasi ujian CBT *Online* pada Instansi XYZ dengan menggunakan metode NIST SP 800-30, maka dapat disimpulkan bahwa hasil analisis dapat digunakan untuk mencapai standar dari sistem manajemen risiko keamanan sistem informasi dengan menggunakan metode NIST SP 800-30. Hasil dari analisis manajemen risiko menunjukkan bahwa terdapat satu nilai risiko *level* tinggi yaitu server dengan kriteria *risk transfer*. Dengan mentransfer risiko kepada pihak ketiga atau penyedia layanan sehingga mengurangi dampak yang ditimbulkan. Tiga risiko *level* signifikan yang terdiri dari sistem informasi ujian CBT *Online* dengan kriteria r*isk reduction, bandwidth* dengan kriteria *risk acceptance*, dan jaringan kriteria r*isk reduction.* Selanjutnya, empat risiko *level* sedang yaitu komputer, peralatan jaringan dan komunikasi, basis data dan staf IT pelaksana sistem informasi ujian CBT *Online*. Berdasarkan keempat *level* risiko sedang tersebut, masing-masing memiliki kriteria yang sama yaitu *risk acceptance.*

Sebagai pendukung analisis, terdapat hasil *assessment* dengan menggunakan *tools Nessus* menghasilkan 1 *level high*, 3 *level* medium, dan 34 informasional. Pengujian yang dilakukan dengan *tools Nessus* menunjukkan positif pada SSL Sweet32, sertifikat SSL yang tidak dapat dipercaya, versi TLS 1.0 masih aktif, dan kerentanan pengungkapan informasi karena versi aplikasi *nginx* yang belum *update*. Sedangkan *tools Acunetix* menghasilkan *level* ancaman di *level* ke-3 yaitu, 2 *high*, 5 medium, 7 *low*, dan 6 informasional. Pengujian yang dilakukan dengan *tools Acunetix* menunjukkan positif pada *cross site scripting*, aktifnya TLS 1.0 dan 1.1, terdapat *file* konfigurasi pengembangan, kerentanan TLS/SSL Sweet32 dan rangkaian sandi, serta kerentanan pada *JavaScript libraries*.

Analisis manajemen risiko keamanan sistem informasi ujian CBT *Online* dengan metode NIST SP 800-30 dapat diberikan rekomendasi dengan memperbarui perangkat lunak dan protokol yang digunakan, menutup *port*

yang tidak digunakan, menggunakan *enkripsi* yang kuat pada *port* tersebut dan melakukan *training* karyawan tentang kesadaran keamanan informasi serta membuat sistem dan jaringan yang aman. Terakhir, dapat diberikan rekomendasi berupa pembangunan sistem penilaian risiko keamanan informasi ujian CBT *Online.*

5.2. Saran

Berdasarkan penelitian yang telah dilakukan analisis manajemen risiko keamanan sistem informasi ujian CBT *Online* pada Instansi XYZ dengan menggunakan metode NIST SP 800-30 memiliki cakupan yang luas untuk lebih di kembangkan lagi. Oleh sebab itu, peneliti dapat memberikan saran untuk penelitian selanjutnya sebagai berikut:

1. Diharapkan penelitian selanjutnya dapat melakukan *vulnerability assessment* lebih dalam pada sistem CBT *Online* dengan menggunakan *tools* lainnya.
2. Penelitian selanjutnya dapat melakukan analisis pada kondisi kesiapan dari manajemen insiden pada Instansi XYZ dengan menggunakan *Framework* ITIL.
3. Diharapkan penelitian selanjutnya dapat melakukan pengembangan sistem penilaian risiko keamanan sistem informasi ujian CBT *Online.*