BAB V
KESIMPULAN, IMPLIKASI, DAN REKOMENDASI

Berdasarkan penelitian yang telah dilakukan, didapatkan kesimpulan, implikasi dan saran seperti berikut ini:

5.1 Kesimpulan

Melalui tahapan penelitian yang telah dilakukan, maka didapatkan kesimpulan diantaranya:

1. Hasil identifikasi risiko keamanan pada Sistem Informasi Akademik (SIAK) UPI teridentifikasi sebanyak delapan ancaman. Ancaman tersebut meliputi serangan *virus,* serangan *ransomware*, serangan *browser hijacking*, jaringan server *down,* kesalahan pada sistem, distribusi data yang tidak terdeteksi, listrik yang padam serta terjadi kerusakan bencana alam
2. Hasil penilaian risiko berdasarkan kerangka kerja NIST SP 80-30 pada Sistem Informasi Akademik (SIAK) UPI didapatkan 2 risiko *high level*, 2 risiko *medium level* serta 4 risiko *low level*. Tingkat penilaian risiko didapatkan berdasarkan analisis ancaman yang ada. Risiko *high level* meliputi serangan *browser hijacking* dan distribusi data yang tidak terdeteksi. Risiko *medium level* meliputi serangan *ransomware* dan jaringan server *down*. Risiko *low level* meliputi serangan virus, kesalahan yang terjadi pada sistem, listrik yang padam serta terjadi kerusakan akibat bencana alam.
3. Rekomendasi manajemen risiko yang diberikan pada Sistem Informasi Akademik (SIAK) UPI didapatkan berdasarkan analisis rekomendasi kontrol melalui tahapan kerangka kerja NIST SP 800-30. Rekomendasi kontrol tersebut berjumlah sembilan yang dikelompokan berdasarkan jenis risiko yang ada. Rekomendasi tersebut meliputi penggunaan jenis anti virus yang sama agar memudahkan proses maintenance, melakukan update secara berkala pada aplikasi proteksi keamanan minimal tiga bulan sekali, melakukan testing atau pengujian berkala baik dari luar atau dalam organisasi agar dapat mendeteksi celah keamanan, melakukan pengujian pada sistem sebelum diluncurkan guna menghindari kesalahan konfigurasi pada sistem, mengupayakan penggunaan WAF (*Web Application Firewall*) guna

memperkuat perlindungan pada data yang dimiliki khususnya melewati firewall, menghindari penggunaan jaringan public (seperti *bluetooth*, *wifi public*), membuat regulasi berupa SOP atau public policy, penambahan *UPS* dan pemeliharaan *UPS* secara berkala, dan membuat sosialisasi perlindungan perangkat pada saat terjadi bencana.

5.2 Implikasi

Implikasi yang didapatkan berdasarkan penelitian yang telah dilakukan diantaranya:

5.2.1 Secara Teoretis

Berdasarkan penelitian yang telah dilakukan, secara teoretis menunjukkan bahwa adanya kebutuhan bagi setiap pengguna sistem informasi untuk dapat memiliki hak keamanan atas data dan informasi yang dimilikinya. Hal ini mendasari bahwa pentingnya manajemen risiko dalam penerapan keamanan informasi bagi setiap pemilik layanan sistem informasi. Dengan menerapkan manajemen risiko keamanan informasi yang baik, tentunya akan menghindari penyalahgunaan data dan infromasi agar menciptakan kepercayaan serta otoritas pada sistem informasi.

5.2.2 Secara Praktis

Pada penelitian ini dilakukan analisis mengenai manajemen risiko yang perlu dilakukan SIAK UPI dalam meningkatkan keamanan informasi dari berbagai aspek. Berdasarkan hasil penelitian, ditemukan beberapa kekurangan dalam penerapan keamanan informasi yang telah dilakukan. Maka dari itu dibutuhkan pula proses mitigasi dan evaluasi berdasarkan rekomendasi manajemen risiko yang ada, sehingga keamanan informasi dapat ditingkatkan secara mendalam.

5.3 Rekomendasi

Berdasarkan kesimpulan dan implikasi yang telah didapatkan, terdapat rekomendasi yang dapat disampaikan diantaranya:

1. Bagi pemilik layanan SIAK UPI: Hasil penelitian menunjukkan beberapa ancaman risiko keamanan informasi pada SIAK UPI yang dapat diminimalisir dengan melakukan manajemen risiko yang disampaikan. Melalui penelitian ini, diharapkan terdapat tindak mitigasi serta evaluasi

keamanan informasi yang dilakukan agar dapat menjadi kontrol keamanan pada Sistem Informasi Akademik (SIAK) UPI.

2. Bagi pengguna SIAK UPI: Pengguna SIAK UPI yang meliputi seluruh civitas akademik UPI memiliki keterlibatan dalam keamanan layanan SIAK UPI. Pelaksanaan praktik atau usaha manajemen risiko keamanan informasi tentunya tidak luput dari dukungan dan upaya seluruh pengguna. Kedepannya pengguna disarankan agar lebih sadar akan pentingnya kerahasiaan, ketersediaan, dan integritas data dan informasi yang dimiliki.
3. Bagi peneliti lain: Penelitian ini dapat dijadikan sumber referensi penelitian selanjutnya agar dapat dikembangkan tentunya dengan berbagai macam kerangka kerja lainnya. Melihat bahwa sedang dilakukannya *security assessment* dengan aplikasi Indeks KAMI yang berpedoman pada ISO 27001, maka hal itu dapat dijadikan sebagai referensi penelitian manajemen risiko selanjutnya agar memperkaya kajian keilmuan mengenai analisis keamanan sistem informasi.