6.23	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Tidak Dilakukan
6.24	III	2	Apakah instansi/perusahaan anda secara rutin menganalisa dan menetapkan website yang membahayakan perusahaan atau tidak seharusnya diakses karyawan? Untuk selanjutnya website tersebut diblok agar tidak dapat diakses.	Diterapkan Secara Menyeluruh
6.25	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Diterapkan Secara Menyeluruh
6.26	III	2	Apakah instansi/perusahaan anda sudah menetapkan prinsip pengembangan aplikasi yang aman (*secure coding*) yang digunakan untuk pengembangan aplikasi secara internal (*in-house*) maupun yang melibatkan pihak eksternal? misal: menggunakan standard OWASP 10	Diterapkan Secara Menyeluruh
6.27	III	2	Apakah instansi/perusahaan anda sudah menerapkan proses perencanaan pengembangan sistem? (Dengan mempertimbangkan hasil pemrograman yang tidak baik/laik pada sistem sebelumnya, konfigurasi *software development tool* yang aman (*secure*), kontrol terhadap lingkungan pengembangan, desain arsitektur yang aman)	Diterapkan Secara Menyeluruh
6.28	III	2	Apakah instansi/perusahaan anda menerapkan proses *source code review* (baik secara manual atau menggunakan piranti lunak) sebelum dijalankan di lingkungan produksi?	Diterapkan Secara Menyeluruh
6.29	II	1	Apakah instansi/perusahaan anda menerapkan kontrol akses untuk *source code* apliksi ?	Diterapkan Secara Menyeluruh
6.30	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Diterapkan Secara Menyeluruh
6.31	III	3	Apakah instansi/perusahaan anda secara rutin menganalisa dan memperbaiki jika ditemukenali ancaman baru (misal adanya laporan kelemahan dan/atau teknik eksploit baru) yang berdampak pada keamanan sistem aplikasi?	Dalam Perencanaan
6.32	III	3	Apakah instansi/perusahaan anda menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?	Tidak Dilakukan
6.33	III	3	Apakah instansi/perusahaan sudah menerapkan proses atau mekanisme untuk mencegah terungkapnya informasi sensitif ke luar dari perusahaan (misal membatasi/mengkarantina lampiran email atau memblokir pengiriman dokumen/data ke	Tidak Dilakukan