KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
	ACCESS CONTROLS													
AC-1	**Access Control Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
AC-2	**Account Management**	x	x	x	x	x	x	x	x	x				x
AC-2(1)	*account management | automated system account management*		x	x	x	x	x	x	x	x				
AC-2(2)	*account management | removal of temporary / emergency accounts*		x	x	x	x	x	x	x	x				
AC-2(3)	*account management | disable inactive accounts*		x	x	x	x	x	x	x	x				
AC-2(4)	*account management | automated audit actions*		x	x	x	x	x	x	x	x				
AC-2(5)	*account management | inactivity logout*			x										x
AC-2(6)	*account management | dynamic privilege management*													
AC-2(7)	*account management | role-based schemes*													
AC-2(8)	*account management | dynamic account creation*				x	x	x	x	x	x	x	x	x	x
AC-2(9)	*account management | restrictions on use of shared / group accounts*													
AC-2(10)	*account management | shared / group account credential termination*													
AC-2(11)	*account management | usage conditions*			x			x			x			x	
AC-2(12)	*account management | account monitoring / atypical usage*			x			x			x			x	
AC-2(13)	*account management | disable accounts for high-risk individuals*			x			x			x			x	
AC-3	**Access Enforcement**	x	x	x	x	x	x	x	x	x				
AC-3(1)	*access enforcement | restricted access to privileged functions*													
AC-3(2)	*access enforcement | dual authorization*													
AC-3(3)	*access enforcement | mandatory access control*													
AC-3(4)	*access enforcement | discretionary access control*				x	x	x	x	x	x				
AC-3(5)	*access enforcement | security-relevant information*													
AC-3(6)	*access enforcement | protection of user and system information*	*Incorporated into MP-4 and SC-28.*												
AC-3(7)	*access enforcement | role-based access control*													
AC-3(8)	*access enforcement | revocation of access authorizations*													
AC-3(9)	*access enforcement | controlled release*													
AC-3(10)	*access enforcement | audited override of access control mechanisms*													
AC-4	**Information Flow Enforcement**		x	x	x	x	x	x	x	x				
AC-4(1)	*information flow enforcement | object security attributes*													
AC-4(2)	*information flow enforcement | processing domains*													
AC-4(3)	*information flow enforcement | dynamic information flow control*													
AC-4(4)	*information flow enforcement | content check encrypted information*													
AC-4(5)	*information flow enforcement | embedded data types*													
AC-4(6)	*information flow enforcement | metadata*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
AC-4(7)	*information flow enforcement | one-way flow mechanisms*													
AC-4(8)	*information flow enforcement | security policy filters*													
AC-4(9)	*information flow enforcement | human reviews*													
AC-4(10)	*information flow enforcement | enable / disable security policy filters*													
AC-4(11)	*information flow enforcement | configuration of security policy filters*													
AC-4(12)	*information flow enforcement | data type identifiers*													
AC-4(13)	*information flow enforcement | decomposition into policy-relevant subcomponents*													
AC-4(14)	*information flow enforcement | security policy filter constraints*													
AC-4(15)	*information flow enforcement | detection of unsanctioned information*													
AC-4(16)	*information flow enforcement | information transfers on interconnected systems*													
AC-4(17)	*information flow enforcement | domain authentication*													
AC-4(18)	*information flow enforcement | security attribute binding*													
AC-4(19)	*information flow enforcement | validation of metadata*													
AC-4(20)	*information flow enforcement | approved solutions*													
AC-4(21)	*information flow enforcement | physical / logical separation of information flows*													
AC-4(22)	*information flow enforcement | access only*													
AC-5	**Separation of Duties**		x	x	x	x	x	x	x	x				
AC-6	**Least Privilege**		x	x	x	x	x	x	x	x				x
AC-6(1)	*least privilege | authorize access to security functions*		x	x	x	x	x	x	x	x				x
AC-6(2)	*least privilege | non-privileged access for nonsecurity functions*		x	x	x	x	x	x	x	x				x
AC-6(3)	*least privilege | network access to privileged commands*			x			x			x				
AC-6(4)	*least privilege | separate processing domains*													
AC-6(5)	*least privilege | privileged accounts*		x	x	x	x	x	x	x	x				x
AC-6(6)	*least privilege | privileged access by non-organizational users*						x			x				x
AC-6(7)	*least privilege | review of user privileges*													
AC-6(8)	*least privilege | privilege levels for code execution*													
AC-6(9)	*least privilege | auditing use of privileged functions*		x	x	x	x	x	x	x	x				
AC-6(10)	*least privilege | prohibit non-privileged users from executing privileged functions*		x	x	x	x	x	x	x	x				
AC-7	**Unsuccessful Logon Attempts**	x	x	x	x	x	x	x	x	x	x	x	x	
AC-7(1)	*unsuccessful logon attempts | automatic account lock*					x	x		x	x				
AC-7(2)	*unsuccessful logon attempts | purge / wipe mobile device*													
AC-8	**System Use Notification**	x	x	x	x	x	x	x	x	x				
AC-9	**Previous Logon (Access) Notification**								x	x				
AC-9(1)	*previous logon notification | unsuccessful logons*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
AC-9(2)	*previous logon notification | successful / unsuccessful logons*													
AC-9(3)	*previous logon notification | notification of account changes*													
AC-9(4)	*previous logon notification | additional logon information*													
AC-10	**Concurrent Session Control**			x					x	x		x	x	
AC-11	**Session Lock**		x	x	x	x	x	x	x	x				
AC-11(1)	*session lock | pattern-hiding displays*		x	x	x	x	x							
AC-12	**Session Termination**		x	x	x	x	x	x	x	x				
AC-12(1)	*session termination | user-initiated logouts / message displays*													
AC-13	**Supervision and Review — Access Control**													
AC-14	**Permitted Actions without Identification or Authentication**	x	x	x	x	x	x	x	x	x				
AC-14(1)	*permitted actions without identification or authentication | necessary uses*													
AC-15	**Automated Marking**													
AC-16	**Security Attributes**													
AC-16(1)	*security attributes | dynamic attribute association*													
AC-16(2)	*security attributes | attribute value changes by authorized individuals*													
AC-16(3)	*security attributes | maintenance of attribute associations by information system*													
AC-16(4)	*security attributes | association of attributes by authorized individuals*													
AC-16(5)	*security attributes | attribute displays for output devices*													
AC-16(6)	*security attributes | maintenance of attribute association by organization*													
AC-16(7)	*security attributes | consistent attribute interpretation*													
AC-16(8)	*security attributes | association techniques / technologies*													
AC-16(9)	*security attributes | attribute reassignment*													
AC-16(10)	*security attributes | attribute configuration by authorized individuals*													
AC-17	**Remote Access**	x	x	x	x	x	x	x	x	x				x
AC-17(1)	*remote access | automated monitoring / control*		x	x	x	x	x	x	x	x				
AC-17(2)	*remote access | protection of confidentiality / integrity using encryption*		x	x	x	x	x	x	x	x				
AC-17(3)	*remote access | managed access control points*		x	x	x	x	x	x	x	x				
AC-17(4)	*remote access | privileged commands / access*		x	x	x	x	x	x	x	x				
AC-17(5)	*remote access | monitoring for unauthorized connections*	Incorporated into SI-4												
AC-17(6)	*remote access | protection of information*				x	x	x							x
AC-17(7)	*remote access | additional protection for security function access*	Incorporated into AC-3												
AC-17(8)	*remote access | disable nonsecure network protocols*	Incorporated into CM-7												
AC-17(9)	*remote access | disconnect / disable access*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
AC-18	**Wireless Access**	x	x	x	x	x	x	x	x	x				x
AC-18(1)	*wireless access | authentication and encryption*		x	x	x	x	x	x	x	x				
AC-18(2)	*wireless access | monitoring unauthorized connections*	Incorporated into SI-4												
AC-18(3)	*wireless access | disable wireless networking*				x	x	x	x	x	x				
AC-18(4)	*wireless access | restrict configurations by users*			x										
AC-18(5)	*wireless access | antennas / transmission power levels*			x										
AC-19	**Access Control for Mobile Devices**	x	x	x	x	x	x	x	x	x				
AC-19(1)	*access control for mobile devices | use of writable / portable storage devices*	Incorporated into MP-7												
AC-19(2)	*access control for mobile devices | use of personally owned portable storage devices*	Incorporated into MP-7												
AC-19(3)	*access control for mobile devices | use of portable storage devices with no identifiable owner*	Incorporated into MP-7												
AC-19(4)	*access control for mobile devices | restrictions for classified information*													
AC-19(5)	*access control for mobile devices | full device / container-based encryption*		x	x	x	x	x	x	x	x				
AC-20	**Use of External Information Systems**	x	x	x	x	x	x	x	x	x				x
AC-20(1)	*use of external information systems | limits on authorized use*		x	x	x	x	x	x	x	x				x
AC-20(2)	*use of external information systems | portable storage devices*		x	x										
AC-20(3)	*use of external information systems | non-organizationally owned systems / components / devices*													
AC-20(4)	*use of external information systems | network accessible storage devices*													
AC-21	**Information Sharing**		x	x	x	x	x	x	x	x				
AC-21(1)	*information sharing | automated decision support*													
AC-21(2)	*information sharing | information search and retrieval*													
AC-22	**Publicly Accessible Content**	x	x	x	x	x	x							x
AC-23	**Data Mining Protection**													
AC-24	**Access Control Decisions**													
AC-24(1)	*access control decisions | transmit access authorization information*													
AC-24(2)	*access control decisions | no user or process identity*													
AC-25	**Reference Monitor**													
AWARENESS AND TRAINING CONTROLS														
AT-1	**Security Awareness and Training Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
AT-2	**Security Awareness Training**	x	x	x	x	x	x	x	x	x	x	x	x	x
AT-2(1)	*security awareness | practical exercises*													
AT-2(2)	*security awareness | insider threat*		x	x										
AT-3	**Role-Based Security Training**	x	x	x	x	x	x	x	x	x	x	x	x	
AT-3(1)	*role-based security training | environmental controls*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
AT-3(2)	*role-based security training | physical security controls*													
AT-3(3)	*role-based security training | practical exercises*													
AT-3(4)	*role-based security training | suspicious communications and anomalous system behavior*													
AT-4	**Security Training Records**	x	x	x	x	x	x	x	x	x	x	x	x	x
AT-5	**Contacts with Security Groups and Associations**	Incorporated into PM-15												
AUDIT AND ACCOUNTABILITY CONTROLS														
AU-1	**Audit and Accountability Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
AU-2	**Audit Events**	x	x	x	x	x	x	x	x	x				
AU-2(1)	*audit events | compilation of audit records from multiple sources*	Incorporated into AU-12												
AU-2(2)	*audit events | selection of audit events by component*	Incorporated into AU-12												
AU-2(3)	*audit events | reviews and updates*		x	x	x	x	x	x	x	x				
AU-2(4)	*audit events | privileged functions*	Incorporated into AC-6 (9)												
AU-3	**Content of Audit Records**	x	x	x	x	x	x	x	x	x				
AU-3(1)	*content of audit records | additional audit information*		x	x	x	x	x	x	x	x				
AU-3(2)	*content of audit records | centralized management of planned audit record content*			x	x	x	x	x	x	x				x
AU-4	**Audit Storage Capacity**	x	x	x							x	x	x	
AU-4(1)	*audit storage capacity | transfer to alternate storage*													
AU-5	**Response to Audit Processing Failures**	x	x	x							x	x	x	
AU-5(1)	*response to audit processing failures | audit storage capacity*			x							x	x	x	
AU-5(2)	*response to audit processing failures | real-time alerts*			x								x	x	
AU-5(3)	*response to audit processing failures | configurable traffic volume thresholds*													
AU-5(4)	*response to audit processing failures | shutdown on failure*													
AU-6	**Audit Review, Analysis, and Reporting**	x	x	x	x	x	x	x	x	x				x
AU-6(1)	*audit review, analysis, and reporting | process integration*		x	x		x	x		x	x				
AU-6(2)	*audit review, analysis, and reporting | automated security alerts*	Incorporated into SI-4												
AU-6(3)	*audit review, analysis, and reporting | correlate audit repositories*		x	x	x	x	x	x	x	x				
AU-6(4)	*audit review, analysis, and reporting | central review and analysis*													
AU-6(5)	*audit review, analysis, and reporting | integration / scanning and monitoring capabilities*			x										
AU-6(6)	*audit review, analysis, and reporting | correlation with physical monitoring*			x										
AU-6(7)	*audit review, analysis, and reporting | permitted actions*													
AU-6(8)	*audit review, analysis, and reporting | full text analysis of privileged commands*													
AU-6(9)	*audit review, analysis, and reporting | correlation with information from nontechnical sources*													
AU-6(10)	*audit review, analysis, and reporting | audit level adjustment*													
AU-7	**Audit Reduction and Report Generation**		x	x		x	x		x	x				

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
AU-7(1)	*audit reduction and report generation | automatic processing*		x	x		x	x		x	x				
AU-7(2)	*audit reduction and report generation | automatic sort and search*													
AU-8	**Time Stamps**	x	x	x				x	x	x				
AU-8(1)	*time stamps | synchronization with authoritative time source*		x	x				x	x	x				
AU-8(2)	*time stamps | secondary authoritative time source*													
AU-9	**Protection of Audit Information**	x	x	x	x	x	x	x	x	x				
AU-9(1)	*protection of audit information | hardware write-once* media													
AU-9(2)	*protection of audit information | audit backup on separate physical systems / components*			x								x	x	
AU-9(3)	*protection of audit information | cryptographic protection*			x						x				
AU-9(4)	*protection of audit information | access by subset of privileged users*		x	x				x	x	x				x
AU-9(5)	*protection of audit information | dual authorization*													
AU-9(6)	*protection of audit information | read-only access*													
AU-10	**Non-repudiation**			x					x	x				
AU-10(1)	*non-repudiation | association of identities*													
AU-10(2)	*non-repudiation | validate binding of information producer identity*													
AU-10(3)	*non-repudiation | chain of custody*													
AU-10(4)	*non-repudiation | validate binding of information reviewer identity*													
AU-10(5)	*non-repudiation | digital signatures*	Incorporated into SI-7							x	x				
AU-11	**Audit Record Retention**	x	x	x							x	x	x	x
AU-11(1)	*audit record retention | long-term retrieval capability*													
AU-12	**Audit Generation**	x	x	x	x	x	x	x	x	x	x	x	x	
AU-12(1)	*audit generation | system-wide / time-correlated audit trail*			x						x				
AU-12(2)	*audit generation | standardized formats*													
AU-12(3)	*audit generation | changes by authorized individuals*			x										
AU-13	**Monitoring for Information Disclosure**													x
AU-13(1)	*monitoring for information disclosure | use of automated tools*													
AU-13(2)	*monitoring for information disclosure | review of monitored sites*													
AU-14	**Session Audit**													
AU-14(1)	*session audit | system start-up*													
AU-14(2)	*session audit | capture/record and log content*													
AU-14(3)	*session audit | remote viewing / listening*													
AU-15	**Alternate Audit Capability**													
AU-16	**Cross-Organizational Auditing**													
AU-16(1)	*cross-organizational auditing | identity preservation*													
AU-16(2)	*cross-organizational auditing | sharing of audit information*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
SECURITY ASSESSMENT AND AUTHORIZATION CONTROLS														
CA-1	**Security Assessment and Authorization Policies and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
CA-2	**Security Assessments**	x	x	x	x	x	x	x	x	x	x	x	x	
CA-2(1)	*security assessments | independent assessors*		x	x	x	x	x	x	x	x	x	x	x	x
CA-2(2)	*security assessments | specialized assessments*			x			x			x			x	
CA-2(3)	*security assessments | external organizations*													
CA-3	**System Interconnections**	x	x	x	x	x	x	x	x	x				
CA-3(1)	*system interconnections | unclassified national security system connections*				x	x	x							x
CA-3(2)	*system interconnections | classified national security system connections*					x	x							x
CA-3(3)	*system interconnections | unclassified non-national security system connections*													
CA-3(4)	*system interconnections | connections to public networks*													
CA-3(5)	*system interconnections | restrictions on external system connections*		x	x										
CA-4	**Security Certification**													
CA-5	**Plan of Action and Milestones**	x	x	x	x	x	x	x	x	x	x	x	x	
CA-5(1)	*plan of action and milestones | automation support for accuracy / currency*													
CA-6	**Security Authorization**	x	x	x	x	x	x	x	x	x	x	x	x	
CA-7	**Continuous Monitoring**	x	x	x	x	x	x	x	x	x	x	x	x	
CA-7(1)	*continuous monitoring | independent assessment*		x	x	x	x	x	x	x	x	x	x	x	x
CA-7(2)	*continuous monitoring | types of assessments*													
CA-7(3)	*continuous monitoring | trend analyses*													
CA-8	**Penetration Testing**			x			x			x			x	
CA-8(1)	*penetration testing | independent penetration agent or team*													
CA-8(2)	*penetration testing | red team exercises*													
CA-9	**Internal System Connections**	x	x	x	x	x	x	x	x	x	x	x	x	
CA-9(1)	*internal system connections | security compliance checks*													
CONFIGURATION MANAGEMENT CONTROLS														
CM-1	**Configuration Management Policy and Procedures**	x	x	x	x	x	x	x	x	x				x
CM-2	**Baseline Configuration**	x	x	x				x	x	x				
CM-2(1)	*baseline configuration | reviews and updates*		x	x					x	x				
CM-2(2)	*baseline configuration | automation support for accuracy / currency*			x						x				
CM-2(3)	*baseline configuration | retention of previous configurations*		x	x					x	x				
CM-2(4)	*baseline configuration | unauthorized software*													
CM-2(5)	*baseline configuration | authorized software*													
CM-2(6)	*baseline configuration | development and test environments*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
CM-2(7)	*baseline configuration | configure systems, components, or devices for high-risk areas*		x	x					x	x				
CM-3	**Configuration Change Control**		x	x				x	x	x				x
CM-3(1)	*configuration change control | automated document / notification / prohibition of changes*			x						x				
CM-3(2)	*configuration change control | test / validate / document changes*		x	x					x	x				
CM-3(3)	*configuration change control | automated change implementation*													
CM-3(4)	*configuration change control | security representative*							x	x	x				x
CM-3(5)	*configuration change control | automated security response*													
CM-3(6)	*configuration change control | cryptography management*													
CM-4	**Security Impact Analysis**	x	x	x				x	x	x				
CM-4(1)	*security impact analysis | separate test environments*			x					x	x				
CM-4(2)	*security impact analysis | verification of security functions*							x	x	x				
CM-5	**Access Restrictions for Change**		x	x				x	x	x				
CM-5(1)	*access restrictions for change | automated access enforcement / auditing*			x										
CM-5(2)	*access restrictions for change | review system changes*			x				x	x	x				
CM-5(3)	*access restrictions for change | signed components*			x						x				
CM-5(4)	*access restrictions for change | dual authorization*													
CM-5(5)	*access restrictions for change | limit production / operational privileges*							x	x	x				x
CM-5(6)	*access restrictions for change | limit library privileges*							x	x	x				x
CM-5(7)	*access restrictions for change | automatic implementation of security safeguards*													
CM-6	**Configuration Settings**	x	x	x				x	x	x				
CM-6(1)	*configuration settings | automated central management / application / verification*			x					x	x				
CM-6(2)	*configuration settings | respond to unauthorized changes*			x						x				
CM-6(3)	*configuration settings | unauthorized change detection*													
CM-6(4)	*configuration settings | conformance demonstration*													
CM-7	**Least Functionality**	x	x	x	x	x	x	x	x	x				
CM-7(1)	*least functionality | periodic review*		x	x	x	x	x	x	x	x				
CM-7(2)	*least functionality | prevent program execution*		x	x		x	x		x	x				
CM-7(3)	*least functionality | registration compliance*				x	x	x	x	x	x				x
CM-7(4)	*least functionality | unauthorized software / blacklisting*		x											
CM-7(5)	*least functionality | authorized software / whitelisting*			x										
CM-8	**Information System Component Inventory**	x	x	x				x	x	x				
CM-8(1)	*information system component inventory | updates during installations / removals*		x	x				x	x	x				
CM-8(2)	*information system component inventory | automated maintenance*			x						x				

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
CM-8(3)	*information system component inventory | automated unauthorized component detection*		x	x						x				
CM-8(4)	*information system component inventory | accountability information*			x				x	x	x				
CM-8(5)	*information system component inventory | no duplicate accounting of components*		x	x				x	x	x				
CM-8(6)	*information system component inventory | assessed configurations / approved deviations*													
CM-8(7)	*information system component inventory | centralized repository*													
CM-8(8)	*information system component inventory | automated location tracking*													
CM-8(9)	*information system component inventory | assignment of components to systems*													
CM-9	**Configuration Management Plan**		x	x				x	x	x				
CM-9(1)	*configuration management plan | assignment of responsibility*													
CM-10	**Software Usage Restrictions**	x	x	x										
CM-10(1)	*software usage restrictions | open source software*													
CM-11	**User-Installed Software**	x	x	x										
CM-11(1)	*user-installed software | alerts for unauthorized installations*													
CM-11(2)	*user-installed software | prohibit installation without privileged status*													
CONTINGENCY PLANNING CONTROLS														
CP-1	**Contingency Planning Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
CP-2	**Contingency Plan**	x	x	x							x	x	x	
CP-2(1)	*contingency plan | coordinate with related plans*		x	x								x	x	
CP-2(2)	*contingency plan | capacity planning*			x								x	x	x
CP-2(3)	*contingency plan | resume essential missions / business functions*		x	x								x	x	x
CP-2(4)	*contingency plan | resume all missions / business functions*			x								x	x	x
CP-2(5)	*contingency plan | continue essential missions / business functions*			x									x	x
CP-2(6)	*contingency plan | alternate processing / storage site*												x	x
CP-2(7)	*contingency plan | coordinate with external service providers*													
CP-2(8)	*contingency plan | identify critical assets*		x	x										
CP-3	**Contingency Training**	x	x	x							x	x	x	
CP-3(1)	*contingency training | simulated events*			x									x	
CP-3(2)	*contingency training | automated training environments*													
CP-4	**Contingency Plan Testing**	x	x	x							x	x	x	
CP-4(1)	*contingency plan testing | coordinate with related plans*		x	x								x	x	
CP-4(2)	*contingency plan testing | alternate processing site*			x									x	
CP-4(3)	*contingency plan testing | automated testing*													
CP-4(4)	*contingency plan testing | full recovery / reconstitution*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
CP-5	**Contingency Plan Update**													
CP-6	**Alternate Storage Site**		x	x								x	x	x
CP-6(1)	*alternate storage site | separation from primary site*		x	x								x	x	x
CP-6(2)	*alternate storage site | recovery time / point objectives*			x									x	x
CP-6(3)	*alternate storage site | accessibility*		x	x								x	x	x
CP-7	**Alternate Processing Site**		x	x								x	x	
CP-7(1)	*alternate processing site | separation from primary site*		x	x								x	x	x
CP-7(2)	*alternate processing site | accessibility*		x	x								x	x	x
CP-7(3)	*alternate processing site | priority of service*		x	x								x	x	
CP-7(4)	*alternate processing site | preparation for use*			x								x	x	
CP-7(5)	*alternate processing site | equivalent information security safeguards*													
CP-7(6)	*alternate processing site | inability to return to primary site*													
CP-8	**Telecommunications Services**		x	x								x	x	x
CP-8(1)	*telecommunications services | priority of service provisions*		x	x								x	x	x
CP-8(2)	*telecommunications services | single points of failure*		x	x								x	x	x
CP-8(3)	*telecommunications services | separation of primary / alternate providers*			x									x	x
CP-8(4)	*telecommunications services | provider contingency plan*			x									x	x
CP-8(5)	*telecommunications services | alternate telecommunication service testing*													
CP-9	**Information System Backup**	x	x	x	x	x	x	x	x	x	x	x	x	
CP-9(1)	*information system backup | testing for reliability / integrity*		x	x				x	x	x	x	x	x	
CP-9(2)	*information system backup | test restoration using sampling*			x						x			x	
CP-9(3)	*information system backup | separate storage for critical information*			x									x	x
CP-9(4)	*information system backup | protection from unauthorized modification*													
CP-9(5)	*information system backup | transfer to alternate storage site*			x								x	x	
CP-9(6)	*information system backup | redundant secondary system*													
CP-9(7)	*information system backup | dual authorization*													
CP-10	**Information System Recovery and Reconstitution**	x	x	x							x	x	x	
CP-10(1)	*information system recovery and reconstitution | contingency plan testing*													
CP-10(2)	*information system recovery and reconstitution | transaction recovery*		x	x				x	x	x	x	x	x	
CP-10(3)	*information system recovery and reconstitution | compensating security controls*													
CP-10(4)	*information system recovery and reconstitution | restore within time period*			x										
CP-10(5)	*information system recovery and reconstitution | failover capability*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
CP-10(6)	*information system recovery and reconstitution | component protection*													
CP-11	**Alternate Communications Protocols**													
CP-12	**Safe Mode**													
CP-13	**Alternative Security Mechanisms**													
IDENTIFICATION AND AUTHENTICATION CONTROLS														
IA-1	**Identification and Authentication Policy and Procedures**	x	x	x	x	x	x	x	x	x				x
IA-2	**Identification and Authentication (Organizational Users)**	x	x	x	x	x	x	x	x	x				
IA-2(1)	*identification and authentication (organizational users) | network access to privileged accounts*	x	x	x	x	x	x	x	x	x				
IA-2(2)	*identification and authentication (organizational users) | network access to non-privileged accounts*		x	x		x	x		x	x				
IA-2(3)	*identification and authentication (organizational users) | local access to privileged accounts*		x	x		x	x		x	x				
IA-2(4)	*identification and authentication (organizational users) | local access to non-privileged accounts*			x		x	x		x	x				
IA-2(5)	*identification and authentication (organizational users) | group authentication*				x	x	x	x	x	x				
IA-2(6)	*identification and authentication (organizational users) | network access to privileged accounts - separate device*													
IA-2(7)	*identification and authentication (organizational users) | network access to non-privileged accounts - separate device*													
IA-2(8)	*identification and authentication (organizational users) | network access to privileged accounts - replay resistant*		x	x	x	x	x	x	x	x				
IA-2(9)	*identification and authentication (organizational users) | network access to non-privileged accounts - replay resistant*			x		x	x		x	x				
IA-2(10)	*identification and authentication (organizational users) | single sign-on*													
IA-2(11)	*identification and authentication (organizational users) | remote access - separate device*		x	x										
IA-2(12)	*identification and authentication (organizational users) | acceptance of piv credentials*	x	x	x										
IA-2(13)	*identification and authentication | out-of-band authentication*													
IA-3	**Device Identification and Authentication**		x	x	x	x	x	x	x	x				
IA-3(1)	*device identification and authentication | cryptographic bidirectional authentication*													
IA-3(2)	*device identification and authentication | cryptographic bidirectional network authentication*													
IA-3(3)	*device identification and authentication | dynamic address allocation*													
IA-3(4)	*device identification and authentication | device attestation*													
IA-4	**Identifier Management**	x	x	x	x	x	x	x	x	x				x
IA-4(1)	*identifier management | prohibit account identifiers as public identifiers*													
IA-4(2)	*identifier management | supervisor authorization*													
IA-4(3)	*identifier management | multiple forms of certification*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
IA-4(4)	*identifier management | identify user status*													
IA-4(5)	*identifier management | dynamic management*													
IA-4(6)	*identifier management | cross-organization management*													
IA-4(7)	*identifier management | in-person registration*													
IA-5	**Authenticator Management**	x	x	x	x	x	x	x	x	x				x
IA-5(1)	*authenticator management | password-based authentication*	x	x	x	x	x	x	x	x	x				
IA-5(2)	*authenticator management | pki-based authentication*		x	x				x	x	x				
IA-5(3)	*authenticator management | in-person or trusted third-party registration*		x	x				x	x	x				x
IA-5(4)	*authenticator management | automated support for password strength determination*				x	x	x	x	x	x				
IA-5(5)	*authenticator management | change authenticators prior to delivery*													
IA-5(6)	*authenticator management | protection of authenticators*													
IA-5(7)	*authenticator management | no embedded unencrypted static authenticators*													
IA-5(8)	*authenticator management | multiple information system accounts*													
IA-5(9)	*authenticator management | cross-organization credential management*													
IA-5(10)	*authenticator management | dynamic credential association*													
IA-5(11)	*authenticator management | hardware token-based authentication*	x	x	x										
IA-5(12)	*authenticator management | biometric-based authentication*													
IA-5(13)	*authenticator management | expiration of cached authenticators*													
IA-5(14)	*authenticator management | managing content of pki trust stores*													
IA-5(15)	*authenticator management | ficam-approved products and services*													
IA-6	**Authenticator Feedback**	x	x	x	x	x	x							
IA-7	**Cryptographic Module Authentication**	x	x	x	x	x	x	x	x	x				
IA-8	**Identification and Authentication (Non-Organizational Users)**	x	x	x	x	x	x	x	x	x				
IA-8(1)	*identification and authentication (non-organizational users) | acceptance of piv credentials from other agencies*	x	x	x										
IA-8(2)	*identification and authentication (non-organizational users) | acceptance of third-party credentials*	x	x	x										
IA-8(3)	*identification and authentication (non-organizational users) | use of ficam-approved products*	x	x	x										
IA-8(4)	*identification and authentication (non-organizational users) | use of ficam-issued profiles*	x	x	x										
IA-8(5)	*identification and authentication (non-organizational users) | acceptance of piv-i credentials*													
IA-9	**Service Identification and Authentication**													
IA-9(1)	*service identification and authentication | information exchange*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
IA-9(2)	*service identification and authentication | transmission of decisions*													
IA-10	**Adaptive Identification and Authentication**													
IA-11	**Re-authentication**													
INCIDENT RESPONSE CONTROLS														
IR-1	**Incident Response Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
IR-2	**Incident Response Training**	x	x	x	x	x	x	x	x	x	x	x	x	
IR-2(1)	*incident response training | simulated events*			x			x			x			x	
IR-2(2)	*incident response training | automated training environments*			x						x			x	
IR-3	**Incident Response Testing**		x	x	x	x	x	x	x	x	x	x	x	
IR-3(1)	*incident response testing | automated testing*													
IR-3(2)	*incident response testing | coordination with related plans*		x	x										
IR-4	**Incident Handling**	x	x	x	x	x	x	x	x	x	x	x	x	x
IR-4(1)	*incident handling | automated incident handling processes*		x	x	x	x	x	x	x	x	x	x	x	x
IR-4(2)	*incident handling | dynamic reconfiguration*													
IR-4(3)	*incident handling | continuity of operations*				x	x	x	x	x	x	x	x	x	
IR-4(4)	*incident handling | information correlation*			x	x	x	x	x	x	x	x	x	x	x
IR-4(5)	*incident handling | automatic disabling of information system*													
IR-4(6)	*incident handling | insider threats - specific capabilities*													
IR-4(7)	*incident handling | insider threats - intra-organization coordination*													
IR-4(8)	*incident handling | correlation with external organizations*													
IR-4(9)	*incident handling | dynamic response capability*													
IR-4(10)	*incident handling | supply chain coordination*													
IR-5	**Incident Monitoring**	x	x	x	x	x	x	x	x	x	x	x	x	x
IR-5(1)	*incident monitoring | automated tracking / data collection / analysis*			x						x			x	x
IR-6	**Incident Reporting**	x	x	x	x	x	x	x	x	x	x	x	x	x
IR-6(1)	*incident reporting | automated reporting*		x	x	x	x	x	x	x	x	x	x	x	x
IR-6(2)	*incident reporting | vulnerabilities related to incidents*				x	x	x	x	x	x	x	x	x	x
IR-6(3)	*incident reporting | coordination with supply chain*													
IR-7	**Incident Response Assistance**	x	x	x	x	x	x	x	x	x	x	x	x	x
IR-7(1)	*incident response assistance | automation support for availability of information / support*		x	x	x	x	x	x	x	x	x	x	x	x
IR-7(2)	*incident response assistance | coordination with external providers*				x	x	x	x	x	x	x	x	x	x
IR-8	**Incident Response Plan**	x	x	x	x	x	x	x	x	x	x	x	x	x
IR-9	**Information Spillage Response**													
IR-9(1)	*information spillage response | responsible personnel*													
IR-9(2)	*information spillage response | training*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
IR-9(3)	*information spillage response | post-spill operations*													
IR-9(4)	*information spillage response | exposure to unauthorized personnel*													
IR-10	**Integrated Information Security Analysis Team**													
MAINTENANCE CONTROLS														
MA-1	**System Maintenance Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
MA-2	**Controlled Maintenance**	x	x	x	x	x	x	x	x	x	x	x	x	
MA-2(1)	*controlled maintenance | record content*													
MA-2(2)	*controlled maintenance | automated maintenance activities*			x			x			x			x	
MA-3	**Maintenance Tools**		x	x				x	x	x	x	x	x	
MA-3(1)	*maintenance tools | inspect tools*		x	x					x	x		x	x	x
MA-3(2)	*maintenance tools | inspect media*		x	x				x	x	x	x	x	x	
MA-3(3)	*maintenance tools | prevent unauthorized removal*			x	x	x	x							
MA-3(4)	*maintenance tools | restricted tool use*													
MA-4	**Nonlocal Maintenance**	x	x	x				x	x	x				
MA-4(1)	*nonlocal maintenance | auditing and review*													
MA-4(2)	*nonlocal maintenance | document nonlocal maintenance*		x	x				x	x	x				
MA-4(3)	*nonlocal maintenance | comparable security / sanitization*			x	x	x	x	x	x	x	x	x	x	
MA-4(4)	*nonlocal maintenance | authentication / separation of maintenance sessions*													
MA-4(5)	*nonlocal maintenance | approvals and notifications*													
MA-4(6)	*nonlocal maintenance | cryptographic protection*													
MA-4(7)	*nonlocal maintenance | remote disconnect verification*													
MA-5	**Maintenance Personnel**	x	x	x	x	x	x	x	x	x	x	x	x	
MA-5(1)	*maintenance personnel | individuals without appropriate access*			x	x	x	x	x	x	x	x	x	x	
MA-5(2)	*maintenance personnel | security clearances for classified systems*													x
MA-5(3)	*maintenance personnel | citizenship requirements for classified systems*													x
MA-5(4)	*maintenance personnel | foreign nationals*													
MA-5(5)	*maintenance personnel | non-system-related maintenance*													
MA-6	**Timely Maintenance**		x	x								x	x	
MA-6(1)	*timely maintenance | preventive maintenance*													
MA-6(2)	*timely maintenance | predictive maintenance*													
MA-6(3)	*timely maintenance | automated support for predictive maintenance*													
MEDIA PROTECTION CONTROLS														
MP-1	**Media Protection Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
MP-2	**Media Access**	x	x	x	x	x	x							x
MP-2(1)	*media access | automated restricted access*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
MP-2(2)	*media access | cryptographic protection*													
MP-3	**Media Marking**		x	x	x	x	x							
MP-4	**Media Storage**		x	x	x	x	x							
MP-4(1)	*media storage | cryptographic protection*													
MP-4(2)	*media storage | automated restricted access*													
MP-5	**Media Transport**		x	x	x	x	x	x	x	x				x
MP-5(1)	*media transport | protection outside of controlled areas*													
MP-5(2)	*media transport | documentation of activities*													
MP-5(3)	*media transport | custodians*													
MP-5(4)	*media transport | cryptographic protection*		x	x		x	x		x	x				
MP-6	**Media Sanitization**	x	x	x	x	x	x							x
MP-6(1)	*media sanitization | review / approve / track / document / verify*			x		x	x							x
MP-6(2)	*media sanitization | equipment testing*			x	x	x	x							x
MP-6(3)	*media sanitization | nondestructive techniques*			x	x	x	x							x
MP-6(4)	*media sanitization | controlled unclassified information*													
MP-6(5)	*media sanitization | classified information*													
MP-6(6)	*media sanitization | media destruction*													
MP-6(7)	*media sanitization | dual authorization*													
MP-6(8)	*media sanitization | remote purging / wiping of information*													
MP-7	**Media Use**	x	x	x										
MP-7(1)	*media use | prohibit use without owner*		x	x										
MP-7(2)	*media use | prohibit use of sanitization-resistant media*													
MP-8	**Media Downgrading**													
MP-8(1)	*media downgrading | documentation of process*													
MP-8(2)	*media downgrading | equipment testing*													
MP-8(3)	*media downgrading | controlled unclassified information*													
MP-8(4)	*media downgrading | classified information*													
PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS														
PE-1	**Physical and Environmental Protection Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
PE-2	**Physical Access Authorizations**	x	x	x	x	x	x	x	x	x	x	x	x	x
PE-2(1)	*physical access authorizations | access by position / role*													
PE-2(2)	*physical access authorizations | two forms of identification*													
PE-2(3)	*physical access authorizations | restrict unescorted access*													
PE-3	**Physical Access Control**	x	x	x	x	x	x	x	x	x	x	x	x	x
PE-3(1)	*physical access control | information system access*			x			x			x				x
PE-3(2)	*physical access control | facility / information system boundaries*				x	x	x							x
PE-3(3)	*physical access control | continuous guards / alarms / monitoring*				x	x	x							x

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
PE-3(4)	*physical access control | lockable casings*						x			x				x
PE-3(5)	*physical access control | tamper protection*													
PE-3(6)	*physical access control | facility penetration testing*													
PE-4	**Access Control for Transmission Medium**		x	x		x	x		x	x				x
PE-5	**Access Control for Output Devices**		x	x	x	x	x							
PE-5(1)	*access control for output devices | access to output by authorized individuals*													
PE-5(2)	*access control for output devices | access to output by individual identity*													
PE-5(3)	*access control for output devices | marking output devices*													
PE-6	**Monitoring Physical Access**	x	x	x	x	x	x	x	x	x	x	x	x	
PE-6(1)	*monitoring physical access | intrusion alarms / surveillance equipment*		x	x								x	x	
PE-6(2)	*monitoring physical access | automated intrusion recognition / responses*													
PE-6(3)	*monitoring physical access | video surveillance*													
PE-6(4)	*monitoring physical access | monitoring physical access to information systems*			x										
PE-7	**Visitor Control**													
PE-8	**Visitor Access Records**	x	x	x	x	x	x	x	x	x				x
PE-8(1)	*visitor access records | automated records maintenance / review*			x			x							
PE-8(2)	*visitor access records | physical access records*													
PE-9	**Power Equipment and Cabling**		x	x							x	x	x	x
PE-9(1)	*power equipment and cabling | redundant cabling*													
PE-9(2)	*power equipment and cabling | automatic voltage controls*											x	x	
PE-10	**Emergency Shutoff**		x	x							x	x	x	x
PE-10(1)	*emergency shutoff | accidental / unauthorized activation*													
PE-11	**Emergency Power**		x	x								x	x	
PE-11(1)	*emergency power | long-term alternate power supply - minimal operational capability*			x									x	x
PE-11(2)	*emergency power | long-term alternate power supply - self-contained*													
PE-12	**Emergency Lighting**	x	x	x							x	x	x	x
PE-12(1)	*emergency lighting | essential missions / business functions*													
PE-13	**Fire Protection**	x	x	x							x	x	x	x
PE-13(1)	*fire protection | detection devices / systems*			x									x	x
PE-13(2)	*fire protection | suppression devices / systems*			x									x	x
PE-13(3)	*fire protection | automatic fire suppression*		x	x									x	x
PE-13(4)	*fire protection | inspections*												x	x
PE-14	**Temperature and Humidity Controls**	x	x	x							x	x	x	x
PE-14(1)	*temperature and humidity controls | automatic controls*											x	x	x

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
PE-14(2)	*temperature and humidity controls | monitoring with alarms / notifications*											x	x	x
PE-15	**Water Damage Protection**	x	x	x							x	x	x	x
PE-15(1)	*water damage protection | automation support*			x									x	
PE-16	**Delivery and Removal**	x	x	x	x	x	x				x	x	x	
PE-17	**Alternate Work Site**		x	x		x	x		x	x		x	x	
PE-18	**Location of Information System Components**			x										x
PE-18(1)	*location of information system components | facility site*													
PE-19	**Information Leakage**													
PE-19(1)	*information leakage | national emissions / tempest policies and procedures*													
PE-20	**Asset Monitoring and Tracking**													
PLANNING CONTROLS														
PL-1	**Security Planning Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
PL-2	**System Security Plan**	x	x	x	x	x	x	x	x	x	x	x	x	
PL-2(1)	*system security plan | concept of operations*													
PL-2(2)	*system security plan | functional architecture*													
PL-2(3)	*system security plan | plan / coordinate with other organizational entities*		x	x	x	x	x	x	x	x	x	x	x	
PL-3	**System Security Plan Update**													
PL-4	**Rules of Behavior**	x	x	x	x	x	x	x	x	x	x	x	x	
PL-4(1)	*rules of behavior | social media and networking restrictions*		x	x										
PL-5	**Privacy Impact Assessment**													
PL-6	**Security-Related Activity Planning**													
PL-7	**Security Concept of Operations**													
PL-8	**Information Security Architecture**		x	x	x	x	x	x	x	x	x	x	x	
PL-8(1)	*information security architecture | defense-in-depth*													
PL-8(2)	*information security architecture | supplier diversity*													
PL-9	**Central Management**													
PERSONNEL SECURITY CONTROLS														
PS-1	**Personnel Security Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
PS-2	**Position Risk Designation**	x	x	x	x	x	x	x	x	x	x	x	x	x
PS-3	**Personnel Screening**	x	x	x	x	x	x	x	x	x				
PS-3(1)	*personnel screening | classified Information*													
PS-3(2)	*personnel screening | formal indoctrination*													
PS-3(3)	*personnel screening | information with special protection measures*													
PS-4	**Personnel Termination**	x	x	x	x	x	x	x	x	x	x	x	x	
PS-4(1)	*personnel termination | post-employment requirements*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
PS-4(2)	*personnel termination | automated notification*			x										
PS-5	**Personnel Transfer**	x	x	x	x	x	x	x	x	x	x	x	x	
PS-6	**Access Agreements**	x	x	x	x	x	x	x	x	x				x
PS-6(1)	*access agreements | information requiring special protection*													
PS-6(2)	*access agreements | classified information requiring special protection*													
PS-6(3)	*access agreements | post-employment requirements*													
PS-7	**Third-Party Personnel Security**	x	x	x	x	x	x	x	x	x				x
PS-8	**Personnel Sanctions**	x	x	x	x	x	x	x	x	x	x	x	x	x
RISK ASSESSMENT CONTROLS														
RA-1	**Risk Assessment Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
RA-2	**Security Categorization**	x	x	x	x	x	x	x	x	x	x	x	x	
RA-3	**Risk Assessment**	x	x	x	x	x	x	x	x	x	x	x	x	
RA-4	**Risk Assessment Update**													
RA-5	**Vulnerability Scanning**	x	x	x	x	x	x	x	x	x	x	x	x	
RA-5(1)	*vulnerability scanning | update tool capability*		x	x	x	x	x	x	x	x	x	x	x	
RA-5(2)	*vulnerability scanning | update by frequency / prior to new scan / when identified*		x	x	x	x	x	x	x	x	x	x	x	
RA-5(3)	*vulnerability scanning | breadth / depth of coverage*													
RA-5(4)	*vulnerability scanning | discoverable information*			x	x	x	x	x	x	x	x	x	x	
RA-5(5)	*vulnerability scanning | privileged access*		x	x	x	x	x	x	x	x	x	x	x	
RA-5(6)	*vulnerability scanning | automated trend analyses*													
RA-5(7)	*vulnerability scanning | automated detection and notification of unauthorized components*													
RA-5(8)	*vulnerability scanning | review historic audit logs*													
RA-5(9)	*vulnerability scanning | penetration testing and analyses*													
RA-5(10)	*vulnerability scanning | correlate scanning information*													
RA-6	**Technical Surveillance Countermeasures Survey**													
SYSTEM AND SERVICES ACQUISITION CONTROLS														
SA-1	**System and Services Acquisition Policy and Procedures**	x	x	x	x	x	x	x	x	x				x
SA-2	**Allocation of Resources**	x	x	x				x	x	x				
SA-3	**System Development Life Cycle**	x	x	x				x	x	x				
SA-4	**Acquisition Process**	x	x	x				x	x	x				
SA-4(1)	*acquisition process | functional properties of security controls*		x	x					x	x				x
SA-4(2)	*acquisition process | design / implementation information for security controls*		x	x						x				x
SA-4(3)	*acquisition process | development methods / techniques / practices*									x				x
SA-4(4)	*acquisition process | assignment of components to systems*													
SA-4(5)	*acquisition process | system / component / service configurations*									x				x

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
SA-4(6)	*acquisition process | use of Information assurance products*													
SA-4(7)	*acquisition process | niap-approved protection profiles*				x	x	x							x
SA-4(8)	*acquisition process | continuous monitoring plan*													
SA-4(9)	*acquisition process | functions / ports / protocols / services in use*		x	x										
SA-4(10)	*acquisition process | use of approved piv products*	x	x	x										
SA-5	**Information System Documentation**	x	x	x				x	x	x				
SA-5(1)	*information system documentation | functional properties of security controls*													
SA-5(2)	*information system documentation | security-relevant external system interfaces*													
SA-5(3)	*information system documentation | high-level design*													
SA-5(4)	*information system documentation | low-level design*													
SA-5(5)	*information system documentation | source code*													
SA-6	**Software Usage Restrictions**													
SA-7	**User-Installed Software**													
SA-8	**Security Engineering Principles**		x	x				x	x	x				x
SA-9	**External Information System Services**	x	x	x				x	x	x				
SA-9(1)	*external information systems | risk assessments / organizational approvals*							x	x	x				
SA-9(2)	*external information systems | identification of functions / ports / protocols / services*		x	x										
SA-9(3)	*external information systems | establish / maintain trust relationship with providers*													
SA-9(4)	*external information systems | consistent interests of consumers and providers*													
SA-9(5)	*external information systems | processing, storage, and service location*													
SA-10	**Developer Configuration Management**		x	x				x	x	x				
SA-10(1)	*developer configuration management | software / firmware integrity verification*													
SA-10(2)	*developer configuration management | alternative configuration management processes*													
SA-10(3)	*developer configuration management | hardware integrity verification*													
SA-10(4)	*developer configuration management | trusted generation*													
SA-10(5)	*developer configuration management | mapping integrity for version control*													
SA-10(6)	*developer configuration management | trusted distribution*													
SA-11	**Developer Security Testing and Evaluation**		x	x				x	x	x				
SA-11(1)	*developer security testing and evaluation | static code analysis*									x				
SA-11(2)	*developer security testing and evaluation | threat and vulnerability analyses*									x				
SA-11(3)	*developer security testing and evaluation | independent verification of assessment plans / evidence*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
SA-11(4)	*developer security testing and evaluation | manual code reviews*													
SA-11(5)	*developer security testing and evaluation | penetration testing*													
SA-11(6)	*developer security testing and evaluation | attack surface reviews*													
SA-11(7)	*developer security testing and evaluation | verify scope of testing / evaluation*													
SA-11(8)	*developer security testing and evaluation | dynamic code analysis*													
SA-12	**Supply Chain Protection**			x	x	x	x	x	x	x	x	x	x	x
SA-12(1)	*supply chain protection | acquisition strategies / tools / methods*													
SA-12(2)	*supply chain protection | supplier reviews*													
SA-12(3)	*supply chain protection | trusted shipping and warehousing*													
SA-12(4)	*supply chain protection | diversity of suppliers*													
SA-12(5)	*supply chain protection | limitation of harm*													
SA-12(6)	*supply chain protection | minimizing procurement time*													
SA-12(7)	*supply chain protection | assessments prior to selection / acceptance / update*													
SA-12(8)	*supply chain protection | use of all-source intelligence*													
SA-12(9)	*supply chain protection | operations security*													
SA-12(10)	*supply chain protection | validate as genuine and not altered*													
SA-12(11)	*supply chain protection | penetration testing / analysis of elements, processes, and actors*													
SA-12(12)	*supply chain protection | inter-organizational agreements*													
SA-12(13)	*supply chain protection | critical information system components*													
SA-12(14)	*supply chain protection | identity and traceability*													
SA-12(15)	*supply chain protection | processes to address weaknesses or deficiencies*													
SA-13	**Trustworthiness**													
SA-14	**Criticality Analysis**													
SA-14(1)	*criticality analysis | critical components with no viable alternative sourcing*													
SA-15	**Development Process, Standards, and Tools**			x										
SA-15(1)	*development process, standards, and tools | quality metrics*													
SA-15(2)	*development process, standards, and tools | security tracking tools*													
SA-15(3)	*development process, standards, and tools | criticality analysis*													
SA-15(4)	*development process, standards, and tools | threat modeling / vulnerability analysis*													
SA-15(5)	*development process, standards, and tools | attack surface reduction*													
SA-15(6)	*development process, standards, and tools | continuous improvement*													
SA-15(7)	*development process, standards, and tools | automated vulnerability analysis*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
SA-15(8)	*development process, standards, and tools | reuse of threat / vulnerability information*													
SA-15(9)	*development process, standards, and tools | use of live data*													
SA-15(10)	*development process, standards, and tools | incident response plan*													
SA-15(11)	*development process, standards, and tools | archive information system / component*													
SA-16	**Developer-Provided Training**			x										
SA-17	**Developer Security Architecture and Design**			x										
SA-17(1)	*developer security architecture and design | formal policy model*													
SA-17(2)	*developer security architecture and design | security-relevant components*													
SA-17(3)	*developer security architecture and design | formal correspondence*													
SA-17(4)	*developer security architecture and design | informal correspondence*													
SA-17(5)	*developer security architecture and design | conceptually simple design*													
SA-17(6)	*developer security architecture and design | structure for testing*													
SA-17(7)	*developer security architecture and design | structure for least privilege*													
SA-18	**Tamper Resistance and Detection**													
SA-18(1)	*tamper resistance and detection | multiple phases of sdlc*													
SA-18(2)	*tamper resistance and detection | inspection of information systems, components, or devices*													
SA-19	**Component Authenticity**													
SA-19(1)	*component authenticity | anti-counterfeit training*													
SA-19(2)	*component authenticity | configuration control for component service / repair*													
SA-19(3)	*component authenticity | component disposal*													
SA-19(4)	*component authenticity | anti-counterfeit scanning*													
SA-20	**Customized Development of Critical Components**													
SA-21	**Developer Screening**													
SA-21(1)	*developer screening | validation of screening*													
SA-22	**Unsupported System Components**													
SA-22(1)	*unsupported system components | alternative sources for continued support*													
SYSTEM AND COMMUNICATIONS PROTECTION CONTROLS														
SC-1	**System and Communications Protection Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
SC-2	**Application Partitioning**		x	x	x	x	x	x	x	x				
SC-2(1)	*application partitioning | interfaces for non-privileged users*													
SC-3	**Security Function Isolation**			x						x				

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
SC-3(1)	*security function isolation | hardware separation*													
SC-3(2)	*security function isolation | access / flow control functions*													
SC-3(3)	*security function isolation | minimize nonsecurity functionality*													
SC-3(4)	*security function isolation | module coupling and cohesiveness*													
SC-3(5)	*security function isolation | layered structures*													
SC-4	**Information in Shared Resources**		x	x	x	x	x							
SC-4(1)	*information in shared resources | security levels*													
SC-4(2)	*information in shared resources | periods processing*													
SC-5	**Denial of Service Protection**	x	x	x							x	x	x	
SC-5(1)	*denial of service protection | restrict internal users*										x	x	x	
SC-5(2)	*denial of service protection | excess capacity / bandwidth / redundancy*											x	x	
SC-5(3)	*denial of service protection | detection / monitoring*													
SC-6	**Resource Availability**												x	
SC-7	**Boundary Protection**	x	x	x	x	x	x	x	x	x				
SC-7(1)	*boundary protection | physically separated subnetworks*													
SC-7(2)	*boundary protection | public access*													
SC-7(3)	*boundary protection | access points*		x	x	x	x	x	x	x	x				
SC-7(4)	*boundary protection | external telecommunications services*		x	x	x	x	x	x	x	x				
SC-7(5)	*boundary protection | deny by default / allow by exception*		x	x	x	x	x	x	x	x				
SC-7(6)	*boundary protection | response to recognized failures*													
SC-7(7)	*boundary protection | prevent split tunneling for remote devices*		x	x	x	x	x	x	x	x				
SC-7(8)	*boundary protection | route traffic to authenticated proxy servers*			x	x	x	x	x	x	x				
SC-7(9)	*boundary protection | restrict threatening outgoing communications traffic*													
SC-7(10)	*boundary protection | prevent unauthorized exfiltration*													
SC-7(11)	*boundary protection | restrict incoming communications traffic*													
SC-7(12)	*boundary protection | host-based protection*													
SC-7(13)	*boundary protection | isolation of security tools / mechanisms / support components*													
SC-7(14)	*boundary protection | protects against unauthorized physical connections*													
SC-7(15)	*boundary protection | route privileged network accesses*													
SC-7(16)	*boundary protection | prevent discovery of components / devices*													
SC-7(17)	*boundary protection | automated enforcement of protocol formats*													
SC-7(18)	*boundary protection | fail secure*			x	x	x	x	x	x	x	x	x	x	
SC-7(19)	*boundary protection | blocks communication from non-organizationally configured hosts*													
SC-7(20)	*boundary protection | dynamic isolation / segregation*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
SC-7(21)	*boundary protection | isolation of information system components*			x										
SC-7(22)	*boundary protection | separate subnets for connecting to different security domains*													
SC-7(23)	*boundary protection | disable sender feedback on protocol validation failure*													
SC-8	**Transmission Confidentiality and Integrity**		x	x				x	x	x				
SC-8(1)	*transmission confidentiality and integrity | cryptographic or alternate physical protection*		x	x					x	x				
SC-8(2)	*transmission confidentiality and integrity | pre / post transmission handling*													
SC-8(3)	*transmission confidentiality and integrity | cryptographic protection for message externals*													
SC-8(4)	*transmission confidentiality and integrity | conceal / randomize communications*													
SC-9	**Transmission Confidentiality**													
SC-10	**Network Disconnect**		x	x	x	x	x	x	x	x				
SC-11	**Trusted Path**													
SC-11(1)	*trusted path | logical isolation*													
SC-12	**Cryptographic Key Establishment and Management**	x	x	x	x	x	x	x	x	x				x
SC-12(1)	*cryptographic key establishment and management | availability*			x							x	x	x	
SC-12(2)	*cryptographic key establishment and management | symmetric keys*													
SC-12(3)	*cryptographic key establishment and management | asymmetric keys*													
SC-12(4)	*cryptographic key establishment and management | pki certificates*													
SC-12(5)	*cryptographic key establishment and management | pki certificates / hardware tokens*													
SC-13	**Cryptographic Protection**	x	x	x	x	x	x	x	x	x				
SC-13(1)	*cryptographic protection | fips-validated cryptography*													
SC-13(2)	*cryptographic protection | nsa-approved cryptography*													
SC-13(3)	*cryptographic protection | individuals without formal access approvals*													
SC-13(4)	*cryptographic protection | digital signatures*													
SC-14	**Public Access Protections**													
SC-15	**Collaborative Computing Devices**	x	x	x	x	x	x							
SC-15(1)	*collaborative computing devices | physical disconnect*													
SC-15(2)	*collaborative computing devices | blocking inbound / outbound communications traffic*													
SC-15(3)	*collaborative computing devices | disabling / removal in secure work areas*													
SC-15(4)	*collaborative computing devices | explicitly indicate current participants*													
SC-16	**Transmission of Security Attributes**													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
SC-16(1)	*transmission of security attributes | integrity validation*													
SC-17	**Public Key Infrastructure Certificates**		x	x	x	x	x	x	x	x				x
SC-18	**Mobile Code**		x	x				x	x	x				
SC-18(1)	*mobile code | identify unacceptable code / take corrective actions*													
SC-18(2)	*mobile code | acquisition / development / use*													
SC-18(3)	*mobile code | prevent downloading / execution*													
SC-18(4)	*mobile code | prevent automatic execution*													
SC-18(5)	*mobile code | allow execution only in confined environments*													
SC-19	**Voice Over Internet Protocol**		x	x	x	x	x	x	x	x				
SC-20	**Secure Name /Address Resolution Service (Authoritative Source)**	x	x	x				x	x	x				
SC-20(1)	*secure name / address resolution service (authoritative source) | child subspaces*													
SC-20(2)	*secure name / address resolution service (authoritative source) | data origin / integrity*													
SC-21	**Secure Name /Address Resolution Service (Recursive or Caching Resolver)**	x	x	x				x	x	x				
SC-21(1)	*secure name / address resolution service (recursive or caching resolver) | data origin / integrity*													
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**	x	x	x	x	x	x	x	x	x	x	x	x	
SC-23	**Session Authenticity**		x	x				x	x	x				
SC-23(1)	*session authenticity | invalidate session identifiers at logout*													
SC-23(2)	*session authenticity | user-initiated logouts / message displays*													
SC-23(3)	*session authenticity | unique session identifiers with randomization*													
SC-23(4)	*session authenticity | unique session identifiers with randomization*													
SC-23(5)	*session authenticity | allowed certificate authorities*													
SC-24	**Fail in Known State**			x	x	x	x	x	x	x				
SC-25	**Thin Nodes**													
SC-26	**Honeypots**													
SC-26(1)	*honeypots | detection of malicious code*													
SC-27	**Platform-Independent Applications**													
SC-28	**Protection of Information at Rest**		x	x	x	x	x	x	x	x				
SC-28(1)	*protection of information at rest | cryptographic protection*													
SC-28(2)	*protection of information at rest | off-line storage*													
SC-29	**Heterogeneity**													
SC-29(1)	*heterogeneity | virtualization techniques*													
SC-30	**Concealment and Misdirection**													
SC-30(1)	*concealment and misdirection | virtualization techniques*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
SC-30(2)	*concealment and misdirection | randomness*													
SC-30(3)	*concealment and misdirection | change processing / storage locations*													
SC-30(4)	*concealment and misdirection | misleading information*													
SC-30(5)	*concealment and misdirection | concealment of system components*													
SC-31	**Covert Channel Analysis**													
SC-31(1)	*covert channel analysis | test covert channels for exploitability*													
SC-31(2)	*covert channel analysis | maximum bandwidth*													
SC-31(3)	*covert channel analysis | measure bandwidth in operational environments*													
SC-32	**Information System Partitioning**													
SC-33	**Transmission Preparation Integrity**													
SC-34	**Non-Modifiable Executable Programs**													
SC-34(1)	*non-modifiable executable programs | no writable storage*													
SC-34(2)	*non-modifiable executable programs | integrity protection / read-only media*													
SC-34(3)	*non-modifiable executable programs | hardware-based protection*													
SC-35	**Honeyclients**													
SC-36	**Distributed Processing and Storage**													
SC-36(1)	*distributed processing and storage | polling techniques*													
SC-37	**Out-of-Band Channels**													
SC-37(1)	*out-of-band channels | ensure delivery / transmission*													
SC-38	**Operations Security**													
SC-39	**Process Isolation**	x	x	x	x	x	x	x	x	x	x	x	x	
SC-39(1)	*process isolation | hardware separation*													
SC-39(2)	*process isolation | thread isolation*													
SC-40	**Wireless Link Protection**													
SC-40(1)	*wireless link protection | electromagnetic interference*													
SC-40(2)	*wireless link protection | reduce detection potential*													
SC-40(3)	*wireless link protection | imitative or manipulative communications deception*													
SC-40(4)	*wireless link protection | signal parameter identification*													
SC-41	**Port and I/O Device Access**													
SC-42	**Sensor Capability and Data**													
SC-42(1)	*sensor capability and data | reporting to authorized individuals or roles*													
SC-42(2)	*sensor capability and data | authorized use*													
SC-42(3)	*sensor capability and data | prohibit use of devices*													
SC-43	**Usage Restrictions**													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
SC-44	**Detonation Chambers**													
	SYSTEM AND INFORMATION INTEGRITY CONTROLS													
SI-1	**System and Information Integrity Policy and Procedures**	x	x	x	x	x	x	x	x	x	x	x	x	x
SI-2	**Flaw Remediation**	x	x	x				x	x	x				
SI-2(1)	*flaw remediation | central management*			x										
SI-2(2)	*flaw remediation | automated flaw remediation status*		x	x					x	x				x
SI-2(3)	*flaw remediation | time to remediate flaws / benchmarks for corrective actions*													
SI-2(4)	*flaw remediation | automated patch management tools*													
SI-2(5)	*flaw remediation | automatic software / firmware updates*													
SI-2(6)	*flaw remediation | removal of previous versions of software / firmware*													
SI-3	**Malicious Code Protection**	x	x	x				x	x	x				
SI-3(1)	*malicious code protection | central management*		x	x				x	x	x				x
SI-3(2)	*malicious code protection | automatic updates*		x	x				x	x	x				
SI-3(3)	*malicious code protection | non-privileged users*													
SI-3(4)	*malicious code protection | updates only by privileged users*													
SI-3(5)	*malicious code protection | portable storage devices*													
SI-3(6)	*malicious code protection | testing / verification*													
SI-3(7)	*malicious code protection | nonsignature-based detection*													
SI-3(8)	*malicious code protection | detect unauthorized commands*													
SI-3(9)	*malicious code protection | authenticate remote commands*													
SI-3(10)	*malicious code protection | malicious code analysis*													
SI-4	**Information System Monitoring**	x	x	x				x	x	x				
SI-4(1)	*information system monitoring | system-wide intrusion detection system*							x	x	x				
SI-4(2)	*information system monitoring | automated tools for real-time analysis*		x	x				x	x	x				
SI-4(3)	*information system monitoring | automated tool integration*													
SI-4(4)	*information system monitoring | inbound and outbound communications traffic*		x	x	x	x	x	x	x	x				
SI-4(5)	*information system monitoring | system-generated alerts*		x	x				x	x	x				
SI-4(6)	*information system monitoring | restrict non-privileged users*													
SI-4(7)	*information system monitoring | automated response to suspicious events*													
SI-4(8)	*information system monitoring | protection of monitoring information*													
SI-4(9)	*information system monitoring | testing of monitoring tools*													
SI-4(10)	*information system monitoring | visibility of encrypted communications*													
SI-4(11)	*information system monitoring | analyze communications traffic anomalies*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
SI-4(12)	*information system monitoring | automated alerts*													
SI-4(13)	*information system monitoring | analyze traffic / event patterns*													
SI-4(14)	*information system monitoring | wireless intrusion detection*													
SI-4(15)	*information system monitoring | wireless to wireline communications*													
SI-4(16)	*information system monitoring | correlate monitoring information*													
SI-4(17)	*information system monitoring | integrated situational awareness*													
SI-4(18)	*information system monitoring | analyze traffic / covert exfiltration*													
SI-4(19)	*information system monitoring | individuals posing greater risk*													
SI-4(20)	*information system monitoring | privileged user*													
SI-4(21)	*information system monitoring | probationary periods*													
SI-4(22)	*information system monitoring | unauthorized network services*													
SI-4(23)	*information system monitoring | host-based devices*													
SI-4(24)	*information system monitoring | indicators of compromise*													
SI-5	**Security Alerts, Advisories, and Directives**	x	x	x				x	x	x				x
SI-5(1)	*security alerts, advisories, and directives | automated alerts and advisories*			x				x	x	x				x
SI-6	**Security Function Verification**			x				x	x	x				
SI-6(1)	*security function verification | notification of failed security tests*													
SI-6(2)	*security function verification | automation support for distributed testing*													
SI-6(3)	*security function verification | report verification results*													
SI-7	**Software, Firmware, and Information Integrity**		x	x						x				
SI-7(1)	*software, firmware, and information integrity | integrity checks*		x	x						x				
SI-7(2)	*software, firmware, and information integrity | automated notifications of integrity violations*			x						x				
SI-7(3)	*software, firmware, and information integrity | centrally managed integrity tools*													
SI-7(4)	*software, firmware, and information integrity | tamper-evident packaging*													
SI-7(5)	*software, firmware, and information integrity | automated response to integrity violations*			x										
SI-7(6)	*software, firmware, and information integrity | cryptographic protection*													
SI-7(7)	*software, firmware, and information integrity | integration of detection and response*		x	x										
SI-7(8)	*software, firmware, and information integrity | auditing capability for significant events*													
SI-7(9)	*software, firmware, and information integrity | verify boot process*													
SI-7(10)	*software, firmware, and information integrity | protection of boot firmware*													

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
SI-7(11)	*software, firmware, and information integrity | confined environments with limited privileges*													
SI-7(12)	*software, firmware, and information integrity | integrity verification*													
SI-7(13)	*software, firmware, and information integrity | code execution in protected environments*													
SI-7(14)	*software, firmware, and information integrity | binary or machine executable code*			x										
SI-7(15)	*software, firmware, and information integrity | code authentication*													
SI-7(16)	*software, firmware, and information integrity | time limit on process execution without supervision*													
SI-8	**Spam Protection**		x	x				x	x	x	x	x	x	
SI-8(1)	*spam protection | central management*		x	x				x	x	x	x	x	x	x
SI-8(2)	*spam protection | automatic updates*		x	x				x	x	x	x	x	x	
SI-8(3)	*spam protection | continuous learning capability*													
SI-9	**Information Input Restrictions**													
SI-10	**Information Input Validation**		x	x					x	x				
SI-10(1)	*information input validation | manual override capability*													
SI-10(2)	*information input validation | review / resolution of errors*													
SI-10(3)	*information input validation | predictable behavior*													
SI-10(4)	*information input validation | review / timing interactions*													
SI-10(5)	*information input validation | review / restrict inputs to trusted sources and approved formats*													
SI-11	**Error Handling**		x	x				x	x	x				
SI-12	**Information Handling and Retention**	x	x	x	x	x	x	x	x	x				
SI-13	**Predictable Failure Prevention**												x	
SI-13(1)	*predictable failure prevention | transferring component responsibilities*													
SI-13(2)	*predictable failure prevention | time limit on process execution without supervision*													
SI-13(3)	*predictable failure prevention | manual transfer between components*													
SI-13(4)	*predictable failure prevention | standby component installation / notification*													
SI-13(5)	*predictable failure prevention | failover capability*													
SI-14	**Non-Persistence**													
SI-14(1)	*non-persistence | refresh from trusted sources*													
SI-15	**Information Output Filtering**													
SI-16	**Memory Protection**		x	x										
SI-17	**Fail-Safe Procedures**													
PROGAM MANAGEMENT CONTROLS														
PM-1	**Information Security Program Plan**				x	x	x	x	x	x	x	x	x	x

KODE NO.	Uraian Detail Kontrol Keamanan	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
		R	S	T	R	S	T	R	S	T	R	S	T	
PM-2	Senior Information Security Officer				x	x	x	x	x	x	x	x	x	x
PM-3	Information Security Resources				x	x	x	x	x	x	x	x	x	x
PM-4	Plan Of Action And Milestones Process				x	x	x	x	x	x	x	x	x	x
PM-5	Information System Inventory				x	x	x	x	x	x	x	x	x	x
PM-6	Information Security Measures Of Performance				x	x	x	x	x	x	x	x	x	x
PM-7	Enterprise Architecture				x	x	x	x	x	x	x	x	x	x
PM-8	Critical Infrastructure Plan				x	x	x	x	x	x	x	x	x	x
PM-9	Risk Management Strategy				x	x	x	x	x	x	x	x	x	x
PM-10	Security Authorization Process				x	x	x	x	x	x	x	x	x	x
PM-11	Mission/Business Process Definition				x	x	x	x	x	x	x	x	x	x
PM-12	Insider Threat Program				x	x	x	x	x	x	x	x	x	x
PM-13	Information Security Workforce				x	x	x	x	x	x	x	x	x	x
PM-14	Testing, Training, And Monitoring				x	x	x	x	x	x	x	x	x	x
PM-15	Contacts With Security Groups And Associations				x	x	x	x	x	x	x	x	x	x
PM-16	Threat Awareness Program				x	x	x	x	x	x	x	x	x	x