BAB 5

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Setelah dilakukan assessment diperoleh current profil serta target profile PT.ABC berkaitan dengan program cybersecurity. Gap tersebut menunjukkan kekurangan yang ada. Sesuai NIST Framework, terdapat 98 subcategory, dimana dari 98 subcategory tersebut terdapat gap sebanyak 39 (sekitar 40%) yang menunjukkan kekurangan PT. ABC dalam melakukan pengamanan terhadap kemungkinan *cyber attack*.

Terhadap 40% gap, PT. ABC dapat mengacu kepada Lampiran 4 perihal Rekomendasi Hasil *Gap Analysis*. Pada lampiran tersebut sudah terdapat kontrol-kontrol yang dapat dijalankan untuk menutup gap atau paling tidak dijadikan sebagai acun dalam memitigasi risiko *cybersecurity* sehingga program-program dan inisiatif terkait *cybersecurity* bisa lebih baik dimasa depan.

5.2. Saran

PT. ABC telah memiliki beberapa key inisiatif untuk cybersecurity program tahun 2018. Namun demikian perlu dilakukan mapping dengan beberapa gap yang sudah dinilai oleh penulis. Diharapkan setelah dilakukan mapping maka diperoleh key inisiatif yang lebih lengkap dan komprehensif sehingga inisiatif-inisiatif tersebut dapat meningkatkan keamanan cybersecurity PT. ABC.

DAFTAR PUSTAKA

Accenture Security (2016). Building Confidence Solving Banking's Cybersecurity Conundrum. Dublin: Accenture Consulting

Information Systems Audit and Control Association-ISACA (2014). Implementing the NIST Cybersecurity Framework. Illinois:ISACA

Fowad Muneer, Senior Manager, ICF International (2014). Cybersecurity Capability Maturity Model (C2M2). Virginia: ICF International

Pamela Curtis, Nader Mehravari, James Stevens, April 2015. Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0. Massachusetts: Software Engineering Institute.

Information Systems Audit and Control Association-ISACA (2013). Transforming Cybersecurity Using COBIT 5. Illinois:ISACA

Information Systems Audit and Control Association-ISACA (2013). Transforming Cybersecurity. Illinois:ISACA

Information Systems Audit and Control Association-ISACA (2014). Implementing the NIST Cybersecurity Framework. Illinois:ISACA

Information Systems Audit and Control Association-ISACA. Advanced Persistent Threats (2016): How to Manage the Risk to Your Business. Illinois:ISACA

ISC2 (2016). The State of Cybersecurity from the Federal Cyber Executive Perspective. Florida: ISC2

Michele Mosca, Ph.D (2015). Cybersecurity in the Quantum World. Illinois:ISACA Journal

National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity Version 1.0. Maryland:NIST

Nasser El-Hout (2015). COBIT 5 For Cyber Security Governance and Management. Riyadh: Service Management Centre of Excellence (SMCE)

Symantec (2011). A Symantec Perspective Preparing the Right Defense for the New Threat Landscape antec Perspective. California:Symantec

Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart (2015). A review of cyber security risk assessment methods for SCADA systems. Amsterdam:Elsevier Ltd

Aniwat Hemanidhi & Sanon Chimmanee (2017). Military-Based Cyber Risk Assessment Framework For Supporting Cyber Warfare In Thailand. Thailand:Journal of Information and Communication Technology (JICT)

Scott J. Shackelford, Zachery Bohm (2016). Securing Critical North American Infrastructure: A Comparatice Case Study in Cybersecurity Regulation. Ohio:Canada-United States Law Journal

Daniel Jardim Pardini, Astrid Maria Carneiro Heinisch, Fernando Silva Parreiras (2017). Cyber Security Governance And Management For Smart Grids in Brazillian Energy Utilities. Brazil:TECSI FEA USP

Halima Ibrahim Kure, Shareeful Islam, Mohammad Abdur Razzaque (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. London:MDPI

.

LAMPIRAN

Lampiran 1. Daftar Fungsi Bisnis dan Tier

Dir -ID	Directorate (L1)	Div-ID	Division (L2)	Dept-ID	Department (L3)	Tier (Department)	Tier (Division)
L1-1	PD	L2-1	Strategy Office	L3-1	Market Research & Banking Strategy	3	3
				L3-2	Transaction Banking Strategy	3	
				L3-3	Transaction Banking Transformation	3	
				L3-4	Retail Banking Strategy	3	
				L3-5	Wholesale Banking Strategy	3	
				L3-6	Change Management & Performance Management	3	
		L2-2	Internal Audit	L3-7	Internal Audit	3	3
L1-2	Information Technology & Operations		Retail Banking Operations	L3-8	Cash Management & Network Operations	1	1
				L3-9	SME Operations	1	
				L3-10	Collateral & Document Management	2	
				L3-11	Consumer Lending Operations	1	
				L3-12	Account Services	1	
				L3-13	CRES Payment & Support	2	
				L3-14	Surabaya Center (1)	1	
			Wholesale Banking Operations	L3-15	Trade Operations	1	1
				L3-16	Security & Agency Operations	1	
				L3-17	Client Services Group	1	
				L3-18	Product Delivery	1	
				L3-19	Global Market Ops & Loan Disbursment Support	1	
				L3-20	Loan Disbursment	1	
			Operation Risk, Process, & Service	L3-21	Operations Risk Management for Operations	3	1

			Management	L3-22	Operations Risk Management for Support Functions	3	
				L3-23	Operations Risk Management for IT	3	
				L3-24	Operations Risk Controls & Management Reports	3	
				L3-25	User Access & Information Security Administration (3)	1	
				L3-26	Operations Procedure Management	3	
				L3-27	Process Re-engineering 1 & Customer Experience	3	
				L3-28	Process Re-engineering 2	3	
				L3-29	Reporting	1	
			Corporate Real Estate Services	L3-30	Health, Safety, and Environment	3	3
				L3-31	Project Management	3	
				L3-32	Facility Management	3	
				L3-33	Database, Helpdesk, Asset & Fleet Management	3	
				L3-34	Security & Business Continutiy Management	3	
				L3-35	General Services Management		
				L3-36	Premises Management	3	
				L3-37	UORM fo Support Function (2)	3	
			Digital Delivery	L3-38	Core Banking & Head Office	2	2
				L3-39	System Integration & Switching	2	
				L3-40	E-Channel, CIS & FES	2	
				L3-41	Loan Origination & Credit Card	2	
				L3-42	Business Analyst Retail Banking & Testing	2	

				L3-43	Business Analyst WB, SF, & Testing	2	
				L3-44	Business Analyst Operation, Finance, Regulatory & Testing	2	
				L3-45	Country Business Intelligence	2	
				L3-46	Project Management Office	2	
			Infrastructure, Services & Operations	L3-47	IT Infrastructure Project	2	2
				L3-48	IT Network & System Management	2	
				L3-49	Data Center Management	2	
				L3-50	IT Security Management	2	
				L3-51	IT Architecture, Planning & Support	2	
				L3-52	Service Delivery Management	2	
				L3-53	Operation Risk for IT (2)	2	
			Chief Information Security Officer	L3-54	Information Security Engineering & Design	2	2
				L3-55	Education, Communication, and Governance	2	
				L3-56	Information Security Operations	2	
				L3-57	Access Management	2	
L1-3	Human Resources		HR & Organization People Development	L3-58	HR Business Partner UUS & RB Non Network	3	3
				L3-59	Talent Management	3	
				L3-60	Learning & Development	3	
			HR Network & Mass Recruitment	L3-61	HR Business Partner (Retail Banking Network I - Region 1, 2, 3, 4, 10, 11, & CE)	3	3
				L3-62	HR Business Partner (Retail Banking Network II - Region 5,6, 7, 8, 9, & NNBS)	3	

				L3-63	Mass Recruitment	3	
			HR (HR, Risk Mgt,Tech&Ops,Legal &Compl.)	L3-64	HR Business Partner (Technology & Operations)	3	3
				L3-65	HR Business Partner (Risk Management)	3	
				L3-66	HR Business Partner (HR, Legal & Compliance)	3	
			HR (Wholesale Banking & VPD's Office)	L3-67	HR Business Partner, Wholesale Banking & VPD's Office	3	3
				L3-68	Resourcing Support Wholesale Banking	3	
			HR Governance & Infrastructure	L3-69	Budget & Analytics		3
				L3-70	Operational Risk, Policy & Procedure	3	
				L3-71	Performance & Rewards	3	
			HR Service Delivery & IR	L3-72	Industrial Relations	2	2
				L3-73	HR Care & UORM	2	
				L3-74	HR OPEX & Information System	2	
				L3-75	HR Payroll	2	
				L3-76	HR Benefit Admin & Loan	2	
			HR(PD's Off,Fin,Exec) Empl.Rel.&Culture	L3-77	HR Business Partner	3	3
				L3-78	Employee Relations & Employee Branding	3	
L1-4	Legal & Compliance		Compliance & Monitoring Advisory	L3-79	Assets Compliance Advisory	1	1
				L3-80	Liabilities Compliance Advisory	1	
				L3-81	Conglomeration & Core Compliance Advisory	1	
				L3-82	Compliance Monitoring	1	
			Anti Money Laundering (AML)	L3-83	AML Operations	1	1
				L3-84	AML Advisory	1	
			Fraud Risk Management	L3-85	Fraud Risk Advisory	1	1
				L3-86	Fraud Examination	1	
			Legal	L3-87	Legal Assets Advisory	3	3

				L3-88	Legal Liabilities Advisory	3	
				L3-89	Legal Core Advisory	3	
				L3-90	Legal Business Support	3	
				L3-91	Credit Litigation	3	
				L3-92	Non Credit Litigation	3	
L1-5	Vice President Director		Corporate Affairs	L3-93	Internal Communication	2	2
				L3-94	External Communication & Stakeholder Management	2	
				L3-95	Corporate Social Responsibility	2	
				L3-96	Business Administration & Monitoring	2	
			Corporate Secretary	L3-97	BOC Secretariat	3	3
				L3-98	Board Support, Administration & Protocol	3	
				L3-99	Regulatory & Governance	3	
				L3-100	Management of Board Processes	3	
L1-6	Finance		Retail Banking, Client Relationship & Syariah Business Finance	L3-101	Client Relationship, Transaction Banking & Syariah Business Finance	3	3
				L3-102	Retail Liabilities, Wealth Management, E-Channel, CSM & NNBS Business Finance	3	
				L3-103	Consolidation & Support Business Finance	3	
				L3-104	Network, Consumer Lending, & SME Business Finance	3	
			Corporate Planning	L3-105	Corporate Finance	3	3
				L3-106	Business Planning & Investor Relations	3	
			Finance & Global Markets Business Finance	L3-107	Performance Management & MIS Reporting	3	3

				L3-108	Global Markets Business Finance	3	
			Procurement Vendor Management	L3-109	Procurement Category IT		3
				L3-110	Procurement Category CRES	3	
				L3-111	Procurement Category Corporate Service	3	
				L3-112	PVM Operations Support	3	
				L3-113	PVM ORM	3	
			Financial Controller	L3-114	Finance Operational Risk Management	1	1
				L3-115	Account Payable & Assets Control	1	
				L3-116	Reconciliation & System Support	1	
				L3-117	Accounting & Other Reporting	1	
				L3-118	BI & OJK Reporting	1	
				L3-119	Tax Control	1	
L1-7	Retail Banking		Network	L3-120	Network Region 1 - 11	2	2
				L3-121	Sales Performance & Branch Delivery / Strategy	2	
				L3-122	Network Service and Operation (Customer Experience Process and Control Management)	3	
			SQ, OpEx & Contact Center	L3-123	Service Quality	3	1
				L3-124	Customer Care Center	3	
				L3-125	Operational Excellence	3	
				L3-126	Contact Center	1	
			Wealth Management, Retail Liability Products & E-Channel	L3-127	GM Sales RB	3	3
				L3-128	Wealth Management Specialist & Products Distribution	3	

				L3-129	Wealth Management Product Development & Governance	3	
				L3-130	Retail Liability Products	3	
				L3-131	E-Channel	3	
				L3-132	UORM Wealth Management, Retail Liability & E-Channel	3	
				L3-133	Business Performance Manager, Wealth Management, Retail Liability & E-Channel	3	
			Customer Segmentation & Marketing	L3-134	Preffered & Priority Segment	3	3
				L3-135	Personal Segment & Project Management	3	
				L3-136	Marketing Communication	3	
				L3-137	Strategic Partnership & Alliances	3	
				L3-138	Business Enablement	3	
			Consumer Lending	L3-139	Mortgage Business	3	3
				L3-140	Credit Card Business	3	
				L3-141	Personal Loan Business	3	
				L3-142	CCPL Network Acquistion, Business Project & Process Management	3	
				L3-143	Indirect Consumer Financing (ICF)	3	
				L3-144	Consumer Lending Operational Risk & Sales Governance	3	
			National Non Branch Sales	L3-145	Permata@Work Astra	3	3
				L3-146	Permata@Work Non Astra Jabodetabek	3	
				L3-147	Permata@Work Non Astra Up	3	

					Country		
				L3-148	Consumer Lending Sales	3	
				L3-149	Telesales & VRM	3	
				L3-150	NNBS Retail Operation & Process Improvement	3	
				L3-151	BD, Process Excellence & Process Improvement	3	
				L3-152	UORM Telesales & VRM	3	
			Loan Approval	L3-153	Consumer Loan & EMA Approval	3	3
				L3-154	Loan Approval Project & Process Improvement	3	
			Business Operational Risk Management (BORM)	L3-155	Business Money Laundring Prevention	3	3
				L3-156	Products Operational Risk Management	3	
				L3-157	Distribution Channels Operational Risk Management	3	
				L3-158	Operational Risk Reporting & Analysis	3	
			SME Banking	L3-159	SME Region 1 - 11	3	3
				L3-160	Head, Product, Buss. Support & UORM	3	
				L3-161	Head, Product Specialist	3	
				L3-162	Head, BIL	3	
L1-8	Syariah Business Unit		Syariah Consumer Financing	L3-163	Syariah Personal Financing Acquisition	3	3
				L3-164	Syariah Mortgage Business	3	
				L3-165	Syariah JF Business	3	
			Syariah Network	L3-166	Regional Sales Syariah	2	2

				L3-167	Syariah Regional Sales Support	2	
			Syariah Wealth Management Product & Operational Risk	L3-168	Syariah UORM, Oversight Report & Cost Monitoring	3	3
				L3-169	Syariah Wealth Management Specialist	3	
				L3-170	Syariah WM Product	3	
			Syariah Product, Marketing & System Support	L3-171	Syariah Liabilities & Wealth Management	3	3
				L3-172	Syariah SME & WB Financing Product	3	
				L3-173	Syariah Consumer Financing	3	
			Syariah SME & Wholesale Banking	L3-174	Syariah SME & Wholesale Banking	3	3
			Syariah Treasury & ALCO	L3-175	Syariah Treasury & ALCO	1	1
			Syariah Strategic Planning & Business Development	L3-176	Syariah Strategic Planning & Business Development	3	3
L1-9	Wholesale Banking		Commercial Banking	L3-177	Commercial Jakarta 1	3	3
				L3-178	Commercial Jakarta 2	3	
				L3-179	Commercial Jabar	3	
				L3-180	Commercial Jateng	3	
				L3-181	Commercial Jatim & East Indonesia	3	
				L3-182	Commercial Sumatera	3	
				L3-183	Value Chain Group	3	
			Corporate Banking 1	L3-184	Corporate Group 1	3	3
				L3-185	Corporate Group 2	3	
				L3-186	Corporate Group 3	3	

				L3-187	Corporate Group 4	3	
				L3-188	Financial Instututions	3	
				L3-189	Corporates Credit Analyst	3	
			Corporate Banking 2	L3-190	Corporate Group 5	3	3
				L3-191	Corporate Group 6	3	
				L3-192	Corporate Group 7	3	
				L3-193	Corporate Group 8	3	
				L3-194	Multi Finance	3	
				L3-195	Corporates Credit Analyst	3	
			Corporate Banking 3	L3-196	Senior Banker	3	3
			WB Ops Risk & Business Support	L3-197	WB Business Strategic Business Planning	3	3
				L3-198	WB Business Process	3	
				L3-199	WB Ops Risk Governance & QA	3	
				L3-200	BMLPO & CDD Analyst	3	
				L3-201	COBAM	3	
			WB Trade & SAS	L3-202	Trade Product	3	3
				L3-203	Trade Sales & Client Delivery	3	
				L3-204	Security & Sales Agency Services	3	
		50	WB Cash & Value Chain	L3-205	WB Funding	3	3
				L3-206	Cash Product & Channel	3	
				L3-207	Cash Sales	3	
				L3-208	Value Chain Program	3	
				L3-209	Value Chain Sales	3	
				L3-210	Cash Client Delivery	3	
		L2-51	Global Markets	L3-211	GM Trading	1	1
				L3-212	Asset Liability Management	1	

				L3-213	GM Sales WB	1	
				L3-214	GM Product	1	
				L3-215	GM Sales RB	1	
L1-10	Risk Management	L2-52	Basel & Market Risk	L3-216	Monitoring & Reporting	1	1
				L3-217	Risk Analytical	1	
		L2-53	CORAM & Integrated Risk Management	L3-218	Operational Risk Assurance (ORA)	3	3
				L3-219	Operational Risk Governance & Integrated Risk Management	3	
				L3-220	Special Project Management Support	3	
		L2-54	Special Asset Management	L3-221	RM Technical Advisor	3	3
				L3-222	Loan Workout SME 1	3	
				L3-223	Loan Workout SME 2	3	
				L3-224	Loan Workout WB 1	3	
				L3-225	Loan Workout WB 2	3	
				L3-226	Loan Workout WB 3	3	
				L3-227	ASM & Property Management	3	
				L3-228	MIS	3	
		L2-55	Senior Credit Officer	L3-229	Deputy Senior Credit Officer 1	3	3
				L3-230	Deputy Senior Credit Officer 2	3	
				L3-231	Deputy Senior Credit Officer 3	3	
				L3-232	WB Credit Policy, Process & MIS	3	
				L3-233	Credit Risk Control	3	
		L2-56	Risk Retail & SME Banking	L3-234	Portfolio Management	3	2
				L3-235	Risk Analytic, MIS & Financial Reporting	3	
				L3-236	Credit SME Segment	3	

				L3-237	OPEX & Fraud Control Unit	3	
				L3-238	Credit Policy Retail & SME	3	
				L3-239	Collection & Recoveries	2	

Contoh cara perhitungan tier fungsi bisnis X di PT. ABC

Dampak Non-Finansial			Rating of Function
Nama Fungsi Kerja		**Skor**	
FTP	A		8
LHBU form 405 dan 406	C, D		10
Likuiditas Harian/Mingguan	C, D		9
ALCO Daily Monitoring	A		6
LCR	C, D		9
NSFR	C, D		9
Capital Management	C, D		3
TOTAL			54
AVERAGE			7.714285714285714

Ketentuan nilai per-TIER adalah sebagai berikut :

Score	Tier
8.0 s/d 10	1
6.0 s/d 7.9	2
0 s/d 5.9	3

Jika mengacu ke ketentuan nilainya maka fungsi binis X ada pada **Tier 2**

Lampiran 2. Daftar Aplikasi dan Risk Level

No	Nama Aplikasi	Deskripsi	Group Aplikasi	Risk Level
1	ESB	Switching Integration Application	Back End	High
2	Base24-eps	Aplikasi Swicthing	Back End	High
3	Informatica etl tools	Aplikasi untuk extract Data dari TP ke Sybase DW	Back End	Low
4	IF400 - interface system & dqm	Interface System - Middleware	Back End	High
5	Gateway ICS / OCS	Penghubung komunikasi anataraICS / OCS dengan JHA	Back End	Low
6	Interface RTGS	Gateway RTGS antara Core & RTGS	Back End	Low
7	Instinct monitoring	sistem fraud untuk persetujuan aplikasi	Funding Applications	Moderate
8	Autodebet	Bill Payments / Repayments yang telah teregistrasi dan dijalankan NCO	Funding Applications	Low
9	Jack Henry	System to handle CASA and TD	Funding Applications	High
10	Sub account	Host to Host denga akses KSEI System	Funding Applications	Moderate
11	Arwana	Host to Host system dengan ACC untuk proses pembukaan rekening	Funding Applications	Low
12	FES (front end system)	Sistem untuk transaksi Teller	Funding Applications	Moderate
13	SNS	Sistem untuk transaksi di Customer Services	Funding Applications	Moderate
14	Pinpad	Aplikasi untuk aktifitas Pin kartu di cabang, bisa untuk Issuing kartu, buat PIN dan verifikasi kartu nasabah	Funding Applications	Moderate
15	IVR call center	Aplikasi Call Center untuk mengakomodasi / melayani nasabah Permatabank	Funding Applications	Low
16	Autopayment	Proses upload payroll/ autopayment nasabah	Funding Applications	Low
17	BPM	System Pengajuan Persetujuan Special Interest Rate TD	Funding Applications	Low
18	Bill payment	pembayaran tagihan melalui autodebet	Funding Applications	Low
19	SVS web	Verifikasi Tanda Tangan via web	Funding Applications	Moderate
20	SVS	Sistem untuk verifikasi tandatangan	Funding Applications	Moderate
21	Eform	Mengotomasikan aktifitas pembukaan rekening.	Funding Applications	Low
22	SAP finance	Pencatatan Jurnal Financial	Internal	Low

			Applications	
23	Share point (hr employee self service, pv online, logistic online, orms, bussiness travel,alco,fleet management)	Portal untuk Employee Self Service & Informasi	Internal Applications	Moderate
24	Permata On Line System (pols)	e-learning sistem	Internal Applications	Moderate
25	Elearning	New Elearning System	Internal Applications	Moderate
26	SAP -HR	Applikasi untuk HR	Internal Applications	Moderate
27	Ario (remittance reconcile)	Sistem rekonsiliasi akun antar kantor	Internal Applications	Low
28	E-proc	Sistem untuk proses pengadaan barang dan jasa	Internal Applications	Low
29	PnP	Web Posting semua Prosedur	Internal Applications	Moderate
30	HSE	Pelaporan tentang Health, Safety & Environment Permata Bank	Internal Applications	Moderate
31	E-BCP	Pengelolaan BCP untuk cabang	Internal Applications	Moderate
32	E-Cres	Pengelolaan request/complaint terkait layanan cres	Internal Applications	Low
33	CRM	Penyediaan Leads Product Cross Sell Untuk Branch Frontl Liners	internal Applications	Moderate
34	Ibm cognos business intelligence	Pembuatan Pelaporan Dataware House dalam bentuk Web	Internal Applications	Low
35	MYWay / BIU	Untuk request data ke CBI	Internal Applications	Low
36	CBT	transaksi antar bank (Cross Banking Transaction)	Internal Applications	Low
37	Report manager	Reporting Server	Internal Applications	Low
38	INT gate	Tool untuk pengiriman data dari mitra ke bank permata dan sebaliknya : VA share folder dengan mitra dan BB Astra group (AHM & AAB) dan SCB	Internal Applications	Low
39	CFES	Sistem untuk mengakomodasi komplain nasabah	Internal Applications	Low
40	Permata Q	Pengaturan Antrian Nasabah Di Cabang	Internal Applications	Low
41	Permatabank.com	Website Permatabank	Internal Applications	Low

42	Datawarehouse (sybase iq data warehouse)	Konsolidasi Data yang berasal dari TP System untuk kepertluan Reconsile, Pelaporan Regulator & Pelaporan Bisnis	Internal Applications	Low
43	RMS 2 -credit	Risk Management System -Credit	Internal Applications	High
44	Amlock	aplikasi untuk deteksi pencucian uang	Internal Applications	High
45	PLUS Consumer	Loan Origination System untuk CCPL, Mortgage dan KTA-BIL	Lending Applications	Moderate
46	Debtector	Proses BI Checking, Biro Scoring, Eyeball Automation	Lending Applications	Moderate
47	New Joint Financing	Sistem for Multifinance Lending	Lending Applications	Moderate
48	Iloan Integrated Loan	System for Consumer & Corporate	Lending Applications	High
49	IIF	Loan sistem (tanpa GL, DWH), mengelola dana untuk Loan dari IIF	Lending Applications	High
50	SFS (supply financing sys.)	layanan supply financing system (pencairan, pembayaran & extend top)	Lending Applications	Moderate
51	Core banking syariah (t24)	Syariah Banking Financing System	Lending Applications	High
52	Joint Financing Syariah	Sistem untuk Multifinance Lending Syariah	Lending Applications	Moderate
53	LTV (loan to value - collateral monitory system)	Tools untuk menghitung Nilai Collateral , dibandingkan Outstanding Pinjaman	Lending Applications	High
54	Amadeus	Maintain NPL & pelaporan	Lending Applications	Moderate
55	Web Appraisal	Layanan Appraisal Agunan	Lending Applications	Moderate
56	DX system	Tools pengiriman scan doc dari cabang untuk proses kredit nasabah sme, wb & mortgage	Lending Applications	Moderate
57	Data matching / internal database permata bank (idpb)	Tools untuk mempercepat proses Analisis Aplikasi Kredit di Credit underwriting (CU)	Lending Applications	Low
58	NBSM	memberikan rekomendasi terhadap proses underwriting ke applikasi PLUS	Lending Applications	Low
59	Mobile Appraisal	Revamp Appraisal PDA, Aplikasi ini berbasis Web untuk appraisal proses yang dapat di akses dari mobile device	Lending Applications	Low
60	Fats barcode system	Pengelolaan penyimpanan dokumen agunan kredit (BPKB)	Lending Applications	Low
61	CLS	sistem liability terpusat	Lending Applications	Low

62	RTGS konvensional	Transaksi RTGS untuk Konvensional	Payment & Transfer Applications	High
63	RTGS syariah	Transaksi RTGS untuk Syariah	Payment & Transfer Applications	High
64	SKN - Konvensional	System Kliring Nasional	Payment & Transfer Applications	High
65	SKN - Syariah	System Kliring Nasional - Syariah	Payment & Transfer Applications	High
66	BI- S4 konvensional	Pelaporan S4 Konvensional ke- BI	Payment & Transfer Applications	High
67	BI- S4 syariah	Pelaporan S4 Syariah ke- BI	Payment & Transfer Applications	High
68	Swift	EFT Sistem	Payment & Transfer Applications	High
69	Taremas	Sistem untuk International Remittance, Demand Draft, TC dan Collection	Payment & Transfer Applications	High
70	KSEI payment bank	Layanan Payment Bank	Payment & Transfer Applications	Moderate
71	Proactive reconcile system	Nostro reconciliation, account payable -incoming/outgoing transfer & bank draft reconciliation	Payment & Transfer Applications	Low
72	Merchant Payment Verification(mpv)	Verifikasi Pembayaran Merchant Permata (melalui EDC)	Payment & Transfer Applications	Moderate
73	OCS	sistem kliring untuk outgoing	Payment & Transfer Applications	High
74	ICS	sistem kliring untuk incoming	Payment & Transfer Applications	High
75	CBR Central Bank Reporting	-laporan keuangan ke bank Indonesia	Regulatory & Tax Applications	Moderate
76	Ppn online	Pendaftaran, Pembuatan dan Pelaporan Faktur Pajak	Regulatory & Tax Applications	Moderate
77	BI-S4 Subreg	Layanan jual beli obligasi	Regulatory & Tax Applications	High
78	Bvl & LBU Permata	Laporan Harian Bank Umum	Regulatory & Tax Applications	High
79	LBU-BI basel ii	Pelaporan LBU ke- BI	Regulatory & Tax Applications	High
80	LBUS-XBRL	Pembuatan laporan keuangan ke bank indonesia	Regulatory & Tax	High

			Applications	
81	RWA LBBU	Laporan Bulanan Komersial Bank	Regulatory & Tax Applications	High
82	PSAK	Laporan Bulanan Komersial Bank	Regulatory & Tax Applications	Moderate
83	LBU basel	Laporan Bulanan Komersial Bank	Regulatory & Tax Applications	High
84	SID otomasi Permatabank	Pelaporan Regulator ke- BI mengenai Sistem Informasi Debitur	Regulatory & Tax Applications	High
85	SID-BI	Pelaporan Regulator ke- BI mengenai Proses Pengiriman	Regulatory & Tax Applications	High
86	LHBU/LKPBU	Laporan Harian Bank Umum	Regulatory & Tax Applications	High
87	CTR	Converter untuk crate XML untuk laporan PPATK	Regulatory & Tax Applications	Low
88	Pajak Gen-2	Tax Payment	Regulatory & Tax Applications	Low
89	Asccend	Sistem untuk mengelola bisnis kartu kredit	Retail Applications	Moderate
90	Visa Master	Sistem yang menghubungkan bisnis kartu kredit Permata dengan VISA MASTER	Retail Applications	Moderate
91	Falcon Monitoring	sistem fraud untuk transaksi kartu	Retail Applications	Moderate
92	CWX (collection works exchequer)	Program Collection System	Retail Applications	Low
93	Reconcile systems	Tools rekonsiliasi data transaksi e-channel	Retail Applications	Moderate
94	Sprint	Sistem untuk notifikasi SMS & SMS Token	Retail Applications	Low
95	Token server	applikasi velis token untuk hardtoken PEB - Link to Permata E-Business (PeB)	Retail Applications	Moderate
96	New Permatanet	Internet Banking Sistem	Retail Applications	Moderate
97	Permata e-business	Aplikasi Internet Banking untuk Corporate Multi CCY	Retail Applications	Moderate
98	Permata mobile	Internet banking melalui perangkat selular	Retail Applications	Moderate
99	Mobile i-banking	Layanan Transaksi Nasabah Melalui I Mobile	Retail Applications	Moderate

100	SCS (sypnatic core system)	Aplikasi Web untuk retur transaksi PeB dan reporting transaksi	Retail Applications	Moderate
101	Loyalty system	Sistem untuk Point Reward	Retail Applications	Moderate
102	Merchant Exception Report	Monitoring Transaksi Credit Card di-Merchant	Retail Applications	Moderate
103	Delivery Tracking System	Pengelolaan catatan pengiriman kartu kredit	Retail Applications	Low
104	ICR data capture	Data capture untuk aplikasi ccpl	Retail Applications	Low
105	CCPL application tracking	sistem untuk informasi status dokumen aplikasi CCPL yang diinput melalui cabang	Retail Applications	Low
106	BBmoney	Transaksi lewat BBM	Retail Applications	Low
107	E-statement / consolidated statement	Laporan statement Rekening	Retail Applications	Low
108	Permata me	Permintaan Cetak Kartu Nasabah	Retail Applications	Low
109	Card Delivery System	Aplikasi untuk administrasi data pengiriman kartu debit dan kredit ke kurir	Retail Applications	Low
110	Saldo atm monitoring	Tools monitoring posisi saldo pada mesin atm permata	Retail Applications	Low
111	E-billing credit card	sistem untuk tagihan kartu kredit	Retail Applications	Low
112	Host to host payment	Aplikasi disisi Nasabah	Retail Applications	Low
113	TI Plus	Sistem untuk Trade Finance dan Bank Guarantee	Trade Financing Applications	High
114	Fitas	Sistem untuk Trade Finance dan Bank Guarantee	Trade Financing Applications	High
115	Hi-Port	Capital Market transaction	Treasury Applications	High
116	Opics syariah	aplikasi Treasury Syariah	Treasury Applications	High
117	Opics	treasury F/O, M/O & B/O Treasury System	Treasury Applications	High
118	MRAS (treasury automation)	Market Risk portfolio & reporting	Treasury Applications	Moderate
119	RET	sistem untuk transaksi valas	Treasury Applications	Moderate
120	Probe	Strategic portfolio management system (memberikan rekomendasi terhadap portfolio yang sudah ada)	Treasury Applications	Moderate
121	Ori	upload Layanan jual beli obligasi	Treasury Applications	Moderate

122	Sao efilingsystem	Tools penyimpanan dokumen (scan) data nasabah sao (securities & agency operations)	Treasury Applications	Moderate
123	Situs	Tools perhitungan unit saham, obligasi & deposito (sebagai bank custodian)	Treasury Applications	Moderate
124	SIAR/WMS	Jual Beli Reksadana & Obligasi	Wealth Management Applications	Moderate
125	Avantrade / sao	Registry System Unit	Wealth Management Applications	Low
126	Wmo integrated tools system (wits)	Konverter nav dari bank custody ke selling agent reksadana & rekonsiliasi inputan transaksi reksadana	Wealth Management Applications	Low
127	Payment Voucher Online (PVO)	Aplikasi pembayaran kepada vendor/pihak ketiga	Internal Applications	Low
128	BI - Electronic Trading Platform	Aplikasi BI untuk perdagangan secara elektronik	Regulatory & Tax Applications	Moderate
129	Odyssey		Lending Applications	Moderate
130	CMS		Lending Applications	High
131	SSG		Lending Applications	Low
132	Host to Host Web Service		Retail Applications	Low

Keterangan:

Tabel ini merupakan hasil identifikasi dan perhitungan skala peioritas atau risk level dari aplikasi, apakah high risk, medium risk, atau low risk

Lampiran 3. Hasil Assessment Current Profile, Target Profile dan Gap

Function	Category	Subcategory	Current Profile	Target Profile	Current Profile	Target Profile	Gap
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	F	F	4	4	0
		ID.AM-2: Software platforms and applications within the organization are inventoried	F	F	4	4	0
		ID.AM-3: Organizational communication and data flows are mapped	N	L	1	3	2
		ID.AM-4: External information systems are catalogued	N	L	1	3	2
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	P	L	2	3	1
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	P	L	2	3	1
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	P	L	2	3	1
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	P	L	2	3	1
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	P	L	2	3	1
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	L	L	3	3	0

		ID.BE-5: Resilience requirements to support delivery of critical services are established	P	L	2	3	1
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	F	F	4	4	0
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	F	F	4	4	0
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	L	L	3	3	0
		ID.GV-4: Governance and risk management processes address cybersecurity risks	L	L	3	3	0
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	N	L	1	3	2
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	L	L	3	3	0
		ID.RA-3: Threats, both internal and external, are identified and documented	L	L	3	3	0
		ID.RA-4: Potential business impacts and likelihoods are identified	P	L	2	3	1
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	P	L	2	3	1
		ID.RA-6: Risk responses are identified and prioritized	P	L	2	3	1
	Risk Management Strategy (ID.RM): The organization's priorities,	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	L	L	3	3	0

	constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-2:** Organizational risk tolerance is determined and clearly expressed	L	L	3	3	0
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	P	L	2	3	1
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	P	L	2	3	1
		PR.AC-2: Physical access to assets is managed and protected	F	F	4	4	0
		PR.AC-3: Remote access is managed	F	F	4	4	0
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	P	L	2	3	1
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	F	F	4	4	0
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	P	L	2	3	1
		PR.AT-2: Privileged users understand roles & responsibilities	L	L	3	3	0
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	F	F	3	3	0
		PR.AT-4: Senior executives understand roles & responsibilities	L	L	3	3	0
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	F	F	4	4	0
	Data Security (PR.DS):	**PR.DS-1:** Data-at-rest is protected	F	F	4	4	0

	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-2:** Data-in-transit is protected	L	L	3	3	0
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	F	F	3	3	0
		PR.DS-4: Adequate capacity to ensure availability is maintained	L	L	3	3	0
		PR.DS-5: Protections against data leaks are implemented	P	L	2	3	1
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	P	L	2	3	1
		PR.DS-7: The development and testing environment(s) are separate from the production environment	F	F	4	4	0
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	L	L	3	3	0
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	F	F	4	4	0
		PR.IP-3: Configuration change control processes are in place	L	L	3	3	0
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	F	F	4	4	0
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	L	L	3	3	0
		PR.IP-6: Data is destroyed according to policy	L	L	3	3	0
		PR.IP-7: Protection processes are continuously improved	L	L	3	3	0

		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	P	L	2	3	1
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	P	L	2	3	1
		PR.IP-10: Response and recovery plans are tested	P	L	2	3	1
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	P	L	2	3	1
		PR.IP-12: A vulnerability management plan is developed and implemented	P	L	2	3	1
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	P	L	2	3	1
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	N	L	1	3	2
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies,	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	P	L	2	3	1
		PR.PT-2: Removable media is protected and its use restricted according to policy	F	L	4	4	0
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	L	L	3	3	0

	procedures, and agreements.	**PR.PT-4:** Communications and control networks are protected	L	L	3	3	0
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	L	L	3	3	0
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	P	L	2	3	1
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	P	L	2	3	1
		DE.AE-4: Impact of events is determined	L	L	3	3	0
		DE.AE-5: Incident alert thresholds are established	P	L	2	3	1
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	P	L	2	3	1
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	L	L	3	3	0
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	P	L	2	3	1
		DE.CM-4: Malicious code is detected	L	L	3	3	0
		DE.CM-5: Unauthorized mobile code is detected	L	L	3	3	0
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	L	L	3	3	0
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	L	L	3	3	0
		DE.CM-8: Vulnerability scans are performed	L	L	3	3	0
	Detection Processes (DE.DP): Detection	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure	L	L	3	3	0

	processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	accountability					
		DE.DP-2: Detection activities comply with all applicable requirements	L	L	3	3	0
		DE.DP-3: Detection processes are tested	P	L	3	3	0
		DE.DP-4: Event detection information is communicated to appropriate parties	L	L	3	3	0
		DE.DP-5: Detection processes are continuously improved	L	L	3	3	0
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	P	L	2	3	1
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	P	L	2	3	1
		RS.CO-2: Events are reported consistent with established criteria	L	L	3	3	0
		RS.CO-3: Information is shared consistent with response plans	P	L	2	3	1
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	L	L	3	3	0
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	L	L	3	3	0
	Analysis (RS.AN): Analysis is	**RS.AN-1:** Notifications from detection systems are investigated	P	L	2	3	1

	conducted to ensure adequate response and support recovery activities.	**RS.AN-2:** The impact of the incident is understood	L	L	3	3	0
		RS.AN-3: Forensics are performed	P	L	2	3	1
		RS.AN-4: Incidents are categorized consistent with response plans	P	L	2	3	1
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	P	L	2	3	1
		RS.MI-2: Incidents are mitigated	L		3	3	0
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	L	L	3	3	0
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	L	L	3	3	0
		RS.IM-2: Response strategies are updated	L	L	3	3	0
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	L	L	3	3	0
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future	**RC.IM-1:** Recovery plans incorporate lessons learned	L	L	3	3	0
		RC.IM-2: Recovery strategies are updated	P	L	2	3	1

	activities.						
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	L	L	3	3	0
		RC.CO-2: Reputation after an event is repaired	L	L	3	3	0
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	L	L	3	3	0

Keterangan:
Tabel ini merupakan hasil perhitungan gap antara curent risk dan target risk.
N=Not Achieved
P=Partially Achieved
L=Largelly Achieved
F=Fully Achieved

Angka merupakan representasi dari masing-masing skala :
N=1
P=2
L=3
F=4

Lampiran 4. Rekomendasi Hasil Gap Analysis

Subcategory Gap	Recomendation
ID.AM-3: Organizational communication and data flows are mapped	AC-4 INFORMATION FLOW ENFORCEMENT Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. CA-3 SYSTEM INTERCONNECTIONS Control: The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency]. CA-9 INTERNAL SYSTEM CONNECTIONS Control: The organization: a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated. PL-8. INFORMATION SECURITY ARCHITECTURE Control: The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions

ID.AM-4: External information systems are catalogued	AC.20 USE OF EXTERNAL INFORMATION SYSTEMS Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems. SA-9. EXTERNAL INFORMATION SYSTEM SERVICES Control: The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.

ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	CP-2. CONTINGENCY PLAN Control: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification. RA-2. SECURITY CATEGORIZATION Control: The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision. SA-14. The organization: a. Identifies critical information system components; and b. Re-implements or custom develops [Assignment: organization-defined critical information system components that require re-implementation or custom development]. CRITICALITY ANALYSIS Control: The organization identifies critical information system components and functions by performing a criticality analysis for [Assignment: organization-defined information systems, information system components, or information system services] at [Assignment: organization-defined decision points in the system development life cycle].

ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CP-2. CONTINGENCY PLAN Control: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification. PS-7. THIRD-PARTY PERSONNEL SECURITY Control: The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures of the organization; c. Documents personnel security requirements; and d. Monitors provider compliance PM-11. MISSION/BUSINESS PROCESS DEFINITION Control: The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained

ID.BE-1: The organization's role in the supply chain is identified and communicated	CP-2. CONTIGENCY PLAN The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and - Is reviewed and approved by [Assignment: organization-defined personnel]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]. SA-12. SUPPLY CHAIN PROTECTION Control: The organization protects against supply chain threats by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	PM-8. CRITICAL INFRASTRUCTURE PLAN Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	PM-11. MISSION/BUSINESS PROCESS DEFINITION Control: The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained. SA-14. CRITICAL INFORMATION SYSTEM COMPONENTS Control: The organization: a. Identifies critical information system components; and b. Re-implements or custom develops [Assignment: organization-defined critical information system components that require re-implementation or custom development].
ID.BE-5: Resilience requirements to support delivery of critical services are established	CP-2. CONTIGENCY PLAN The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and - Is reviewed and approved by [Assignment: organization-defined personnel]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]. CP-11. PREDICTABLE FAILURE PREVENTION Control: The organization: a. Determines mean time to failure (MTTF) for [Assignment: organization-defined information system components] in specific environments of operation; and b. Provides substitute information system components and a means to exchange active and standby components at [Assignment: organization-defined MTTF substitution criteria]. SA-14. CRITICAL INFORMATION SYSTEM COMPONENTS

	Control: The organization: a. Identifies critical information system components; and b. Re-implements or custom develops [Assignment: organization-defined critical information system components that require re-implementation or custom development].
ID.RA-1: Asset vulnerabilities are identified and documented	CA-2 SECURITY ASSESSMENTS Control: The organization: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles]. CA-7 CONTINUOUS MONITORING Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]. CA-8 PENETRATION TESTING Control: The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components]. RA-3 RISK ASSESSMENT Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk

	assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. RA-5 VULNERABILITY SCANNING Control: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response; d. Protects documentation as required, in accordance with the risk

	management strategy; and e. Distributes documentation to [Assignment: organization-defined personnel or roles]. SA-11 DEVELOPER SECURITY TESTING AND EVALUATION Control: The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation. SI-2 FLAW REMEDIATION Control: The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process. SI-4 INFORMATION SYSTEM MONITORING Control: The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c. Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]]. SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES Control: The organization: a. Receives information system security alerts, advisories, and

	directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
ID.RA-4: Potential business impacts and likelihoods are identified	RA-2. SECURITY CATEGORIZATION Control: The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision. RA-3 RISK ASSESSMENT Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. PM-9 RISK MANAGEMENT STRATEGY Control: The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; b. Implements the risk management strategy consistently across the organization; and c. Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes. PM-11 MISSION/BUSINESS PROCESS DEFINITION Control: The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation;

	and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained. SA-14 CRITICALITY ANALYSIS Control: The organization identifies critical information system components and functions by performing a criticality analysis for [Assignment: organization-defined information systems, information system components, or information system services] at [Assignment: organization-defined decision points in the system development life cycle].
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	RA-2. SECURITY CATEGORIZATION Control: The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision. RA-3 RISK ASSESSMENT Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. PM-16 THREAT AWARENESS PROGRAM Control: The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

ID.RA-6: Risk responses are identified and prioritized	PM-4. PLAN OF ACTION AND MILESTONES PROCESS Control: The organization: a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems: - Are developed and maintained; and - Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. PM-9. RISK MANAGEMENT STRATEGY Control: The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and b. Implements that strategy consistently across the organization.
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	PM-8 CRITICAL INFRASTRUCTURE PLAN Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan. PM-9 RISK MANAGEMENT STRATEGY Control: The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; b. Implements the risk management strategy consistently across the organization; and c. Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes. PM-11 MISSION/BUSINESS PROCESS DEFINITION Control: The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained. SA-14 CRITICALITY ANALYSIS Control: The organization identifies critical information system components and functions by performing a criticality analysis for [Assignment: organization-defined information systems, information system components, or information system services] at [Assignment: organization-defined decision points in the system development life cycle].

PR.AC-1: Identities and credentials are managed for authorized devices and users	AC-2. ACCOUNT MANAGEMENT Control: The organization manages information system accounts, including: a. Identifying account types (e.g., individual, shared/group, system, application, guest/anonymous, emergency, and temporary); b. Establishing conditions for group and role membership; c. Specifying authorized users of the information system, group and role membership, and account access authorizations (i.e., privileges) for each account; d. Requiring approvals by [Assignment: organization-defined personnel] for requests to create accounts; e. Creating, enabling, modifying, disabling, and removing accounts (including adding and deleting members from groups or roles); f. Authorizing and monitoring the use of shared/group, guest/anonymous, emergency, and temporary accounts; g. Notifying account managers: - When accounts (including shared/group, emergency, and temporary accounts) are no longer required; - When users are terminated or transferred; or - When individual information system usage or need-to-know changes; h. Associating access authorizations and other attributes as required by the organization with each information system account; i. Granting access to the system based on: - A valid access authorization; - Intended system usage; and - Other attributes as required by the organization or associated missions/business functions; j. Reviewing accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishing a process for modifying shared/group account credentials when individuals are removed from the group.

PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-2 ACCOUNT MANAGEMENT Control: The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. AC-3. ACCESS ENFORCEMENT Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. AC-5. SEPARATION OF DUTIES Control: The organization: a. Separates [Assignment: organization-defined duties of individuals]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties. AC-6. LEAST PRIVILEGE Control: The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. AC-16. SECURITY ATTRIBUTES Control: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment: organization-defined security attribute values] with information in storage, in process, and/or in transmission; and b. Ensures that the security attribute associations are made and retained with the information.

PR.AT-1: All users are informed and trained	AT-2. SECURITY AWARENESS Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. PM-13. INFORMATION SECURITY WORKFORCE Control: The organization establishes an information security workforce development and improvement program.
PR.DS-5: Protections against data leaks are implemented	AC-4 INFORMATION FLOW ENFORCEMENT Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. AC-5 SEPARATION OF DUTIES Control: The organization: a. Separates [Assignment: organization-defined duties of individuals]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties. AC-6 LEAST PRIVILEGE Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. PE-19 INFORMATION LEAKAGE Control: The organization protects the information system from information leakage due to electromagnetic signals emanations. PS-3 PERSONNEL SCREENING Control: The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening]. PS-6 ACCESS AGREEMENTS Control: The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency]. SC-7 BOUNDARY PROTECTION

	Control: The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY Control: The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information. SC-13 CRYPTOGRAPHIC PROTECTION Control: The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards SC-31 COVERT CHANNEL ANALYSIS Control: The organization: a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and b. Estimates the maximum bandwidth of those channels. SI-4 INFORMATION SYSTEM MONITORING Control: The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c. Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7. SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY Control: The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	AC-21. COLLABORATION AND INFORMATION SHARING Control: The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [Assignment: organization-defined information sharing circumstances and automated mechanisms or manual processes required] to assist users in making information sharing/collaboration decisions. CA-7 CONTINUOUS MONITORING Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]. SI-4. INFORMATION SYSTEM MONITORING Control: The organization: a. Monitors the information system to detect attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring

	activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	CP-2. OK IR-8. INCIDENT RESPONSE PLAN Control: The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and - Is reviewed and approved by [Assignment: organization-defined personnel]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]. IR-8 INCIDENT RESPONSE PLAN Control: The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-

	defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification.
PR.IP-10: Response and recovery plans are tested	CP-4. CONTINGENCY PLAN TESTING Control: The organization: a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions. IR-3. INCIDENT RESPONSE TESTING Control: The organization tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results. PM-14. OPERATIONS SECURITY PROGRAM Control: The organization establishes and implements an Operations Security (OPSEC) program.
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES PS-2 POSITION RISK DESIGNATION PS-3 PERSONNEL SCREENING PS-4 PERSONNEL TERMINATION PS-5 PERSONNEL TRANSFER PS-6 ACCESS AGREEMENTS PS-7 THIRD-PARTY PERSONNEL SECURITY PS-8 PERSONNEL SANCTIONS

PR.IP-12: A vulnerability management plan is developed and implemented	RA-3. RISK ASSESSMENT Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; and d. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. VULNERABILITY SCANNING Control: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). FLAW REMEDIATION Control: The organization: a. Identifies, reports, and corrects information system flaws; b. Installs security-relevant software and firmware updates; c. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and d. Incorporates flaw remediation into the organizational configuration management process.

PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	MA-2. CONTROLLED MAINTENANCE Control: The organization: a. Schedules, performs, documents, and reviews records of, maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that [Assignment: organization-defined personnel] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records. MA-3. MAINTENANCE TOOLS Control: The organization approves, controls, and monitors information system maintenance tools. MA-5. MAINTENANCE PERSONNEL Control: The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that personnel performing maintenance on the information system or maintenance personnel in physical proximity to the system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	MA-4. NON-LOCAL MAINTENANCE Control: The organization: a. Approves and monitors non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of non-local maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed.

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**Audit and Accountability** AU-1 Audit and Accountability Policy and Procedures AU-2 Audit Events AU-3 Content of Audit Records AU-4 Audit Storage Capacity AU-5 Response to Audit Processing Failures AU-6 Audit Review, Analysis, and Reporting AU-7 Audit Reduction and Report Generation AU-8 Time Stamps AU-9 Protection of Audit Information AU-10 Non-repudiation AU-11 Audit Record Retention AU-12 Audit Generation AU-13 Monitoring for Information Disclosure AU-14 Session Audit AU-15 Alternate Audit Capability AU-16 Cross-Organizational Auditing
DE.AE-2: Detected events are analyzed to understand attack targets and methods	AU-6. AUDIT REVIEW, ANALYSIS, AND REPORTING Control: The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity; b. Reports findings to [Assignment: organization-defined personnel]; c. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information; and d. Specifies the permitted actions for each [Selection (one or more): information system process; role; user] associated with the review, analysis, and reporting of audit information. CA-7. CONTINUOUS MONITORING Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and assessments; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel] [Assignment: organization-defined frequency]. IR-4. INCIDENT HANDLING Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

	b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. SI-4. INFORMATION SYSTEM MONITORING Control: The organization: a. Monitors the information system to detect attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING Control: The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and b. Reports findings to [Assignment: organization-defined personnel or roles]. CA-7 CONTINUOUS MONITORING Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]. IR-4 INCIDENT HANDLING Control: The organization: a. Implements an incident handling capability for security incidents

	that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly. IR-5. INCIDENT MONITORING Control: The organization tracks and documents information system security incidents. IR-8. INCIDENT RESPONSE PLAN Control: The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and - Is reviewed and approved by [Assignment: organization-defined personnel]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]. SI-4. INFORMATION SYSTEM MONITORING Control: The organization: a. Monitors the information system to detect attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring

	activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
DE.AE-5: Incident alert thresholds are established	IR-4 INCIDENT HANDLING Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly. IR-5 INCIDENTMONITORING Control: The organization tracks and documents information system security incidents. IR-8 INCIDENT RESPONSE PLAN Control: The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification.

DE.CM-1: The network is monitored to detect potential cybersecurity events	AC-2. ACCOUNT MANAGEMENT Control: The organization manages information system accounts, including: a. Identifying account types (e.g., individual, shared/group, system, application, guest/anonymous, emergency, and temporary); b. Establishing conditions for group and role membership; c. Specifying authorized users of the information system, group and role membership, and account access authorizations (i.e., privileges) for each account; d. Requiring approvals by [Assignment: organization-defined personnel] for requests to create accounts; e. Creating, enabling, modifying, disabling, and removing accounts (including adding and deleting members from groups or roles); f. Authorizing and monitoring the use of shared/group, guest/anonymous, emergency, and temporary accounts; g. Notifying account managers: - When accounts (including shared/group, emergency, and temporary accounts) are no longer required; - When users are terminated or transferred; or - When individual information system usage or need-to-know changes; h. Associating access authorizations and other attributes as required by the organization with each information system account; i. Granting access to the system based on: - A valid access authorization; - Intended system usage; and - Other attributes as required by the organization or associated missions/business functions; j. Reviewing accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishing a process for modifying shared/group account credentials when individuals are removed from the group. AU-12. AUDIT GENERATION Control: The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 at [Assignment: organization-defined information system components]; b. Allows [Assignment: organization-defined personnel] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the audited events defined in AU-2 with the content defined in AU-3. CA-7. CONTINUOUS MONITORING Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and assessments; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related

	information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel] [Assignment: organization-defined frequency]. CM-3 CONFIGURATION CHANGE CONTROL Control: The organization: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]]. SC-5 DENIAL OF SERVICE PROTECTION Control: The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. SC-7 BOUNDARY PROTECTION Control: The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. SI-4 INFORMATION SYSTEM MONITORING Control: The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c. Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

	d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	AC-2. ACCOUNT MANAGEMENT Control: The organization manages information system accounts, including: a. Identifying account types (e.g., individual, shared/group, system, application, guest/anonymous, emergency, and temporary); b. Establishing conditions for group and role membership; c. Specifying authorized users of the information system, group and role membership, and account access authorizations (i.e., privileges) for each account; d. Requiring approvals by [Assignment: organization-defined personnel] for requests to create accounts; e. Creating, enabling, modifying, disabling, and removing accounts (including adding and deleting members from groups or roles); f. Authorizing and monitoring the use of shared/group, guest/anonymous, emergency, and temporary accounts; g. Notifying account managers: - When accounts (including shared/group, emergency, and temporary accounts) are no longer required; - When users are terminated or transferred; or - When individual information system usage or need-to-know changes; h. Associating access authorizations and other attributes as required by the organization with each information system account; i. Granting access to the system based on: - A valid access authorization; - Intended system usage; and - Other attributes as required by the organization or associated missions/business functions; j. Reviewing accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishing a process for modifying shared/group account credentials when individuals are removed from the group. AU-12 AUDIT GENERATION Control: The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

	AU-13. MONITORING FOR INFORMATION DISCLOSURE Control: The organization monitors [Assignment: organization-defined open source information] [Assignment: organization-defined frequency] for evidence of unauthorized exfiltration or disclosure of organizational information. CA-7. CONTINUOUS MONITORING Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and assessments; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel] [Assignment: organization-defined frequency]. CM-10 SOFTWARE USAGE RESTRICTIONS Control: The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. CM-11 USER-INSTALLED SOFTWARE Control: The organization: a. Establishes [Assignment: organization-defined policies] governing the installation of software by users; b. Enforces software installation policies through [Assignment: organization-defined methods]; and c. Monitors policy compliance at [Assignment: organization-defined frequency].

RS.RP-1: Response plan is executed during or after an event	CP-2 CONTINGENCY PLAN Control: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification. CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. IR-4 INCIDENT HANDLING Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly IR-8 INCIDENT RESPONSE PLAN Control: The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization;

	4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification.
RS.CO-1: Personnel know their roles and order of operations when a response is needed	CP-2 CONTINGENCY PLAN Control: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification. CP-3 CONTINGENCY TRAINING Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

	a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. IR-3 INCIDENT RESPONSE TESTING Control: The organization tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results. IR-8 INCIDENT RESPONSE PLAN Control: The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification.

RS.CO-3: Information is shared consistent with response plans	CA-2. SECURITY ASSESSMENTS Control: The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used to determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].
RS.AN-1: Notifications from detection systems are investigated	AU-6. AUDIT REVIEW, ANALYSIS, AND REPORTING Control: The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity; b. Reports findings to [Assignment: organization-defined personnel]; c. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information; and d. Specifies the permitted actions for each [Selection (one or more): information system process; role; user] associated with the review, analysis, and reporting of audit information. CA-7. CONTINUOUS MONITORING Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and assessments; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel] [Assignment: organization-defined frequency]. IR-4 INCIDENT HANDLING Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment,

	eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly IR-5 INCIDENTMONITORING Control: The organization tracks and documents information system security incidents PE-6. MONITORING PHYSICAL ACCESS Control: The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs [Assignment: organization-defined frequency] and, upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinates results of reviews and investigations with the organizational incident response capability. SI-4 INFORMATION SYSTEM MONITORING Control: The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c. Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

RS.AN-3: Forensics are performed	AU-7. AUDIT REDUCTION AND REPORT GENERATION Control: The organization employs an audit reduction and report generation capability that: a. Supports expeditious, on-demand audit review, analysis, and reporting requirements and afterthe- fact investigations of security incidents; and b. Does not alter original audit records. IR-4. INCIDENT HANDLING Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.
RS.AN-4: Incidents are categorized consistent with response plans	CP-2 CONTINGENCY PLAN Control: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification IR-4 INCIDENT HANDLING Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning

	activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly. IR-5. INCIDENT MONITORING Control: The organization tracks and documents information system security incidents. IR-8 INCIDENT RESPONSE PLAN Control: The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification.
RS.MI-1: Incidents are contained	IR-4. INCIDENT HANDLING Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

RC.IM-2: Recovery strategies are updated	CP-2 CONTINGENCY PLAN Control: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification. IR-4 INCIDENT HANDLING Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly. IR-8. INCIDENT RESPONSE PLAN Control: The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively

	maintain and mature an incident response capability; and - Is reviewed and approved by [Assignment: organization-defined personnel]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements].

Keterangan:
Tabel ini merupakan rekomendasi yang diberikan kepada PT.ABC terhadap gap yang sudah di identifikasi.
Source: Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53 Revision 4

Lampiran 5. Hasil Assessment Framework Implementation Tier

Framework Implementation Tier	Tier Category	Characteristics	C2M2 Reference			Implementation	
			MIL1	MIL2	MIL3	Current Profile	Target Profile
Tier 1 : Partial	Risk Management Process	Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.	RM-2a			F	F
		Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements	RM-2a			F	F
	Integrated Risk Management Program	There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established.	RM-2a			F	F
		The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources.	RM-2a			F	F
		The organization may not have processes that enable cybersecurity information to be shared within the organization.	RM-2a			F	F
	External Participation	An organization may not have the processes in place to participate in coordination or collaboration with other entities	RM-2a			F	F
Tier 2: Risk Informed	Risk Management Process	Risk management practices are approved by management but may not be established as organizational-wide policy.		RM-3a		F	F
		Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.			RM-1c	L	L
	Integrated Risk Management Program	There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established.	RM-2a			F	F

		Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties.	CPM-2a			L	L
		Cybersecurity information is shared within the organization on an informal basis.	ISC-1a			F	F
	External Participation	The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally	EDM-1a			P	L
Tier 3: Repeatable	Risk Management Process	The organization's risk management practices are formally approved and expressed as policy.			RM-3e	F	F
		Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.			CPM-1g	L	L
	Integrated Risk Management Program	There is an organization-wide approach to manage cybersecurity risk.	CPM-1a			F	F
		Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.			RM-3e	F	F
		Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.		WM-3b		F	F
	External Participation	The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.	EDM-2a			P	L
Tier 4: Adaptive	Risk Management Process	The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.			RM-1d	F	F

		Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner			RM-1d	F	F
	Integrated Risk Management Program	There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.		TVM-1d		L	L
		Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.			SA-3d	P	L
	External Participation	The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs			ISC-1h	F	F

Keterangan:
Tabel ini merupakan hasil perhitungan tier implementasi cybersecurity di PT.ABC
N=Not Achieved
P=Partially Achieved
L=Largelly Achieved
F=Fully Achieved

Contoh perhitungan sebagai berikut mengacu ke Lampiran 6. Objective dan Practice C2M2

Example: RM-1a
Domain Abbreviation-Objective Number Practice Letter

1. Establish Cybersecurity Risk Management Strategy	
MIL1	No practice at MIL 1
MIL2	a. There is a documented cybersecurity risk management strategy b. The strategy provides an approach for risk prioritization, including consideration of impact
MIL3	c. Organizational risk are defined (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available d. The risk management strategy is periodically updated to reflect the current threat environment e. An organization-specific risk taxonomy is documented and is used in risk management activities

Lampiran 6. Objective dan Practice C2M2

(1) RISK MANAGEMENT (RM)		
Objective and Practice		
1. Establish Enterprise Cybersecurity Risk Management Strategy		
MIL1		No practice at MIL1
MIL2	a.	There is a documented cybersecurity risk management strategy
MIL2	b.	The strategy provides an approach for risk prioritization, including consideration of impact and resource requirements
MIL3	c.	Organizational risk criteria (criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available
MIL3	d.	The risk management strategy is periodically updated to reflect the current threat environment
MIL3	e.	An organization-specific risk taxonomy is documented and is used in risk management activities
2. Manage Enterprise Cybersecurity Risk		
MIL1	a.	Cybersecurity risks are identified, at least in an ad hoc manner
MIL1	b.	Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner
MIL2	c.	Risk assessments are performed to identify risks in accordance with the risk management strategy
MIL2	d.	Identified risks are documented
MIL2	e.	Identified risks are analyzed to prioritize response activities in accordance with the risk man-agement strategy
MIL2	f.	Identified risks are monitored in accordance with the risk management strategy
MIL2	g.	Current network and/or system architecture documentation is used to support risk analysis
MIL3	h.	The risk management program defines and operates risk management policies and procedures that implement the risk management strategy
MIL3	i.	Current cybersecurity architecture documentation is used to support risk analysis
MIL3	j.	A risk register (a structured repository of identified risks) is used to support risk management activities
3. Institutionalization Activities for RM Domain		
MIL1		No practice at MIL1
MIL2	a.	Documented practices are followed for risk management activities

MIL2	b.	Stakeholders for risk management activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support risk management ac-tivities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform risk management ac-tivities
MIL3	e.	Risk management activities are guided by documented policies or other organizational direc-tives
MIL3	f.	Risk management policies include compliance requirements for specified standards, guide-lines, and best practices
MIL3	g.	Risk management activities are periodically reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of risk management activities are assigned to personnel
MIL3	i.	Personnel performing risk management activities have the skills and knowledge needed to per-form their assigned responsibilities
(2) ASSET, CHANGE, AND CONFIGURATION MANAGEMENT (ACM)		
Objectives and Practices		
1. Manage Asset Inventory		
MIL11	a.	There is an inventory of technology assets (e.g., computers and telecommunication equipment, data centers, and emergency power generators) that are important to the delivery of IT ser-vices; management of the inventory may be ad hoc
MIL1	b.	There is an inventory of information assets (e.g., customer information, financial data, and configuration items) that are important to the delivery of IT services; management of the inventory may be ad hoc
MIL2	c.	Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards)
MIL2	d.	Inventoried assets are prioritized based on their importance to the delivery of IT services
MIL3	e.	The asset inventory describes (physical and logical) connections among technology assets
MIL3	f.	The asset inventory is current (as defined by the organization) at least for assets of importance to enterprise IT services
2. Manage Asset Configuration		
MIL1	a.	Configuration baselines are established, at least in an ad hoc manner, for inventoried assets where it is desirable to ensure that multiple assets are configured similarly
MIL1	b.	Configuration baselines are used, at least in an ad hoc manner, to configure assets at deploy-ment

MIL2	c.	The design of configuration baselines includes cybersecurity objectives
MIL3	d.	Configurations of assets are monitored for consistency with baselines throughout the assets' lifecycles
MIL3	e.	Configuration baselines are reviewed and updated at an organization-defined frequency
3. Manage Changes to Assets		
MIL1	a.	Proposed changes to inventoried assets are evaluated, at least in an ad hoc manner, before being implemented
MIL1	b.	Changes to inventoried assets are logged, at least in an ad hoc manner
MIL2	c.	Changes to assets are tested prior to being deployed, whenever possible
MIL2	d.	Change management practices address the full lifecycle of assets (i.e., acquisition, deploy-ment, operation, retirement)
MIL3	e.	Changes to assets are tested for cybersecurity impact prior to being deployed
MIL3	f.	Change logs include information about modifications that impact the cybersecurity require-ments of assets (availability, integrity, confidentiality)
4. Institutionalization Activities for ACM Domain		
MIL1		No practice at MIL1
MIL2	a.	Documented practices are followed for asset inventory, configuration, and change manage-ment activities
MIL2	b.	Stakeholders for asset inventory, configuration, and change management activities are identi-fied and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support asset inventory, con-figuration, and change management activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform asset inventory, configuration, and change management activities
MIL3	e.	Asset inventory, configuration, and change management activities are guided by documented policies or other organizational directives
MIL3	f.	Asset inventory, configuration, and change management policies include compliance require-ments for specified standards, guidelines, and best practices
MIL3	g.	Asset inventory, configuration, and change management activities are periodically reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of asset inventory, configuration, and change management activities are assigned to personnel

MIL3	i.	Personnel performing asset inventory, configuration, and change management activities have the skills and knowledge needed to perform their assigned responsibilities
(3) IDENTITY AND ACCESS MANAGEMENT (IAM)		
Objectives and Practices		
1. Establish and Maintain Identities		
MIL1	a.	Identities are provisioned, at least in an ad hoc manner, for personnel and other entities (e.g., services, devices) that require access to assets (note that this does not preclude shared identi-ties)
MIL1	b.	Credentials (e.g., passwords, smart cards, certificates, keys, lock combinations) are issued to identities that require access to assets, at least in an ad hoc manner
MIL1	c.	Identities are deprovisioned and credentials revoked, at least in an ad hoc manner, when no longer required
MIL2	d.	Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access)
MIL2	e.	Credentials are periodically reviewed to ensure that they are associated with the correct person or entity
MIL2	f.	Identities are deprovisioned within organization-defined time thresholds when no longer re-quired
MIL3	g.	Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RM-1c)
2. Control Access		
MIL1	a.	Access requirements, including those for remote access, are determined, at least in an ad hoc manner (i.e., access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentica-tion parameters)
MIL1	b.	Access is granted, at least in an ad hoc manner, to identities based on requirements
MIL1	c.	Access is revoked, at least in an ad hoc manner, when no longer required
MIL2	d.	Access requirements incorporate least privilege and separation of duties principles
MIL2	e.	Access requests are reviewed and approved by the asset owner
MIL2	f.	Root privileges, administrative access, emergency access, and shared accounts receive addi-tional scrutiny and monitoring
MIL3	g.	Access privileges are reviewed and updated to ensure validity, at an organization-defined fre-quency

MIL3	h.	Access to assets is granted by the asset owner based on risk to IT services
MIL3	i.	Anomalous access attempts are monitored as indicators of cybersecurity events
3. Institutionalization Activities for IAM Domain		
MIL1		No practice at MIL1
MIL2	a.	Documented practices are followed to establish and maintain identities and control access
MIL2	b.	Stakeholders for identity and access management activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support identity and access management activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform identity and access management activities
MIL3	e.	Identity and access management activities are guided by documented policies or other organi-zational directives
MIL3	f.	Identity and access management policies include compliance requirements for specified stand-ards, guidelines, and best practices
MIL3	g.	Identity and access management activities are periodically reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of identity and access management activities are assigned to personnel
MIL3	i.	Personnel performing identity and access management activities have the skills and knowledge needed to perform their assigned responsibilities
(4) THREAT AND VULNERABILITY MANAGEMENT (TVM)		
Objectives and Practices		
1. Identify and Respond to Threats		
MIL1	a.	Information sources to support threat management activities are identified (e.g., US-CERT, in-dustry associations, vendors, federal briefings), at least in an ad hoc manner
MIL1	b.	Cybersecurity threat information is gathered and interpreted for IT services, at least in an ad hoc manner
MIL1	c.	Threats that are considered important to IT services are addressed (e.g., implement mitigating controls, monitor threat status), at least in an ad hoc manner
MIL2	d.	A threat profile for IT services is established that includes characterizations of likely intent, ca-pability, and targets
MIL2	e.	Threat information sources that address all components of the threat profile are prioritized and monitored
MIL2	f.	Identified threats are analyzed and prioritized
MIL2	g.	Threats are addressed according to the assigned priority

MIL3	h.	The threat profile for IT services is validated at an organization-defined frequency
MIL3	i.	Analysis and prioritization of threats are informed by the defined risk criteria (RM-1c)
MIL3	j.	Threat information is added to the risk register (RM-2j)
2. Reduce Cybersecurity Vulnerabilities		
MIL1	a.	Information sources to support cybersecurity vulnerability discovery are identified (e.g., US-CERT, industry associations, vendors, federal briefings), at least in an ad hoc manner
MIL1	b.	Cybersecurity vulnerability information is gathered and interpreted for IT services, at least in an ad hoc manner
MIL1	c.	Cybersecurity vulnerabilities that are considered important to IT services are addressed (e.g., implement mitigating controls, apply cybersecurity patches, plan for software end of life), at least in an ad hoc manner
MIL2	d.	Cybersecurity vulnerability information sources that address all assets important to IT services are monitored
MIL2	e.	Cybersecurity vulnerability assessments are performed (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification using specialized tools)
MIL2	f.	Identified cybersecurity vulnerabilities are analyzed and prioritized (e.g., NIST Common Vulner-ability Scoring System could be used for software vulnerabilities)
MIL2	g.	Cybersecurity vulnerabilities are addressed according to the assigned priority
MIL2	h.	Operational impact to IT services is evaluated prior to deploying cybersecurity patches
MIL3	i.	Cybersecurity vulnerability assessments are performed for all assets important to the delivery of IT services, at an organization-defined frequency
MIL3	j.	Cybersecurity vulnerability assessments are informed by the defined risk criteria (RM-1c)
MIL3	k.	Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of IT services
MIL3	l.	Analysis and prioritization of cybersecurity vulnerabilities are informed by the defined risk criteria (RM-1c)
MIL3	m.	Cybersecurity vulnerability information is added to the risk register (RM-2j)
MIL3	n.	Risk monitoring activities validate the responses to cybersecurity vulnerabilities (e.g., deployment of patches)
3. Institutionalization Activities for TVA Domain		
MIL1		No practice at MIL1

MIL2	a.	Documented practices are followed for threat and vulnerability management activities
MIL2	b.	Stakeholders for threat and vulnerability management activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support threat and vulnerabil-ity management activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform threat and vulnerability management activities
MIL3	e.	Threat and vulnerability management activities are guided by documented policies or other or-ganizational directives
MIL3	f.	Threat and vulnerability management policies include compliance requirements for specified standards, guidelines, and best practices
MIL3	g.	Threat and vulnerability management activities are periodically reviewed to ensure conform-ance with policy
MIL3	h.	Responsibility and authority for the performance of threat and vulnerability management activi-ties are assigned to personnel
MIL3	i.	Personnel performing threat and vulnerability management activities have the skills and knowledge needed to perform their assigned responsibilities
(5) SITUATIONAL AWARENESS (SA)		
Objectives and Practices		
1. Perform Logging		
MIL1	a.	Logging is occurring, at least in an ad hoc manner, for assets important to IT services where possible
MIL2	b.	Logging requirements have been defined for all assets important to IT services (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availabil-ity])
MIL2	c.	IT services log data are being aggregated
MIL3	d.	Logging requirements are based on the risk to IT services
MIL3	e.	Log data support other business and security processes (e.g., incident response, asset man-agement)
2. Monitor IT Services		
MIL1	a.	Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner
MIL1	b.	IT services' operational environments are monitored, at least in an ad hoc manner, for anoma-lous behavior that may indicate a cybersecurity event (e.g., web response rates are exception-ally slow)
MIL2	c.	Monitoring and analysis requirements have been defined for IT services and address timely re-view of event data

MIL2	d.	Alarms and alerts are configured to aid the identification of cybersecurity events (IR-1b)
MIL2	e.	Indicators of anomalous activity have been defined and are monitored across the operational environment
MIL2	f.	Monitoring activities are aligned with IT services' threat profile (TVA-1d)
MIL3	g.	Monitoring requirements are based on the risk to IT services
MIL3	h.	Monitoring is integrated with other business and security processes (e.g., incident response, asset management, vulnerability and threat management)
MIL3	i.	Continuous monitoring is performed across the operational environment to identify anomalous activity
MIL3	j.	Risk register (RM-2j) content is used to identify indicators of anomalous activity
MIL3	k.	Alarms and alerts are configured according to indicators of anomalous activity
3. Establish and Maintain a Common Operating Picture		
MIL1		No practice at MIL 1
MIL2	a.	Methods of communicating the current state of cybersecurity for IT services are established and maintained
MIL2	b.	Monitoring data are aggregated to provide near-real-time understanding of the operational state of IT services (i.e., a common operating picture; a COP may or may not include visualiza-tion)
MIL2	c.	Information from across the organization is available to enhance the common operating picture
MIL3	d.	Monitoring data are aggregated to provide near-real-time understanding of the cybersecurity state for IT services to enhance the common operating picture
MIL3	e.	Information from outside the organization is collected to enhance the common operating picture
MIL3	f.	Predefined states of operation are documented and invoked (manual or automated process) based on the common operating picture
4. Institutionalization Activities for SA Domain		
MIL1		No practice at MIL 1
MIL2	a.	Documented practices are followed for logging, monitoring, and COP activities
MIL2	b.	Stakeholders for logging, monitoring, and COP activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support logging, monitoring, and COP activities

MIL2	d.	Standards, guidelines, and best practices have been identified to inform logging, monitoring, and COP activities
MIL3	e.	Logging, monitoring, and COP activities are guided by documented policies or other organizational directives
MIL3	f.	Logging, monitoring, and COP policies include compliance requirements for specified standards, guidelines, and best practices
MIL3	g.	Logging, monitoring, and COP activities are periodically reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of logging, monitoring, and COP activities are assigned to personnel
MIL3	i.	Personnel performing logging, monitoring, and COP activities have the skills and knowledge needed to perform their assigned responsibilities
(6) INFORMATION SHARING AND COMMUNICATIONS (ISC)		
Objectives and Practices		
1. Share Cybersecurity Information		
MIL1	a.	Cybersecurity information is collected from and provided to selected individuals and/or organi-zations, at least in an ad hoc manner
MIL1	b.	Responsibility for cybersecurity reporting obligations is assigned to personnel (e.g., internal re-porting, US-CERT, law enforcement), at least in an ad hoc manner
MIL2	c.	Information-sharing stakeholders are identified based on their relevance to the continued oper-ation of IT services (e.g., connected organizations, vendors, internal entities)
MIL2	d.	Information is collected from and provided to identified information-sharing stakeholders
MIL2	e.	Technical resources are identified that can be consulted on cybersecurity issues
MIL2	f.	Provisions are established and maintained to enable secure sharing of sensitive cybersecurity information
MIL2	g.	Information-sharing practices address both standard operations and emergency operations
MIL3	h.	Information-sharing stakeholders are identified based on common interests and risks
MIL3	i.	The organization participates with external information sharing and analysis organizations
MIL3	j.	Information-sharing requirements have been defined for IT services and address timely dissemination of cybersecurity information
MIL3	k.	Procedures are in place to analyze and deconflict received information

MIL3	l.	A network of internal and external trust relationships (formal and/or informal) has been established to vet and validate information about cyber events
2. Institutionalization Activities for ISC Domain		
MIL1		No practice at MIL 1
MIL2	a.	Documented practices are followed for information-sharing activities
MIL2	b.	Stakeholders for information-sharing activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support information-sharing activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform information-sharing activities
MIL3	e.	Information-sharing activities are guided by documented policies or other organizational direc-tives
MIL3	f.	Information-sharing policies include compliance requirements for specified standards, guide-lines, and best practices
MIL3	g.	Information-sharing policies address protected information, ethical use and sharing of infor-mation, including sensitive information as appropriate
MIL3	h.	Information-sharing activities are periodically reviewed to ensure conformance with policy
MIL3	i.	Responsibility and authority for the performance of information-sharing activities are assigned to personnel
MIL3	j.	Personnel performing information-sharing activities have the skills and knowledge needed to perform their assigned responsibilities
(7) EVENT AND INCIDENT RESPONSE, CONTINUITY OF OPERATIONS (IR)		
Objectives and Practices		
1. Detect Cybersecurity Events		
MIL1	a.	A point of contact (person or role) to whom cybersecurity events can be reported has been identified, at least in an ad hoc manner
MIL1	b.	Detected cybersecurity events are reported, at least in an ad hoc manner
MIL1	c.	Cybersecurity events are logged and tracked, at least in an ad hoc manner
MIL2	d.	Criteria are established for cybersecurity event detection (e.g., what constitutes an event, where to look for events)
MIL2	e.	There is a repository where cybersecurity events are logged based on the established criteria
MIL3	f.	Event information is correlated to support incident analysis by identifying patterns, trends, and other common features

MIL3	g.	Cybersecurity event detection activities are adjusted based on information from the organiza-tion's risk register (RM-2j) and threat profile (TVA-1d) to help monitor for identified risks and de-tect known threats
MIL3	h.	The common operating picture for IT services is monitored to support the identification of cy-bersecurity events (SA-3a)
2. Escalate Cybersecurity Events		
MIL1	a.	Criteria for cybersecurity event escalation are established, including cybersecurity incident dec-laration criteria, at least in an ad hoc manner
MIL1	b.	Cybersecurity events are analyzed, at least in an ad hoc manner, to support escalation and the declaration of cybersecurity incidents
MIL1	c.	Escalated cybersecurity events and incidents are logged and tracked, at least in an ad hoc manner
MIL2	d.	Criteria for cybersecurity event escalation, including cybersecurity incident criteria, are estab-lished based on the potential impact to IT services
MIL2	e.	Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are updated at an organization-defined frequency
MIL2	f.	There is a repository where escalated cybersecurity events and cybersecurity incidents are logged and tracked to closure
MIL3	g.	Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are adjusted according to information from the organization's risk register (RM-1c, RM-2j) and threat profile (TVM-1d)
MIL3	h.	Escalated cybersecurity events and declared cybersecurity incidents inform the common oper-ating picture (SA-3a) for IT services
MIL3	i.	Escalated cybersecurity events and declared inci
3. Respond to Escalated Cybersecurity Events		
MIL1	a.	Cybersecurity event and incident response personnel are identified and roles are assigned, at least in an ad hoc manner
MIL1	b.	Responses to escalated cybersecurity events and incidents are implemented, at least in an ad hoc manner, to limit impact to IT services and restore normal operations
MIL1	c.	Reporting of escalated cybersecurity events and incidents is performed (e.g., internal reporting, IS-CERT), at least in an ad hoc manner

MIL2	d.	Cybersecurity event and incident response is performed according to defined procedures that address all phases of the incident lifecycle (e.g., triage, handling, communication, coordination, and closure)
MIL2	e.	Cybersecurity event and incident response plans are exercised at an organization-defined fre-quency
MIL2	f.	Cybersecurity event and incident response plans address all assets important to the delivery of IT services
MIL2	g.	Training is conducted for cybersecurity event and incident response teams
MIL3	h.	Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed and corrective actions are taken
MIL3	i.	Cybersecurity event and incident responses are coordinated with law enforcement and other government entities as appropriate, including evidence collection and preservation
MIL3	j.	Cybersecurity event and incident response personnel participate in joint cybersecurity exercises with other organizations (e.g., table top, simulated incidents)
MIL3	k.	Cybersecurity event and incident response plans are reviewed and updated at an organization-defined frequency
MIL3	l.	Cybersecurity event and incident response activities are coordinated with relevant external en-tities
MIL3	m.	Cybersecurity event and incident response plans are aligned with defined risk criteria (RM-1c) and threat profile (TVA-1d)
MIL3	n.	Policy and procedures for reporting cybersecurity event and incident information to designated authorities conform with applicable laws, regulations, and contractual agreements
MIL3	o.	Restored assets are configured appropriately and inventory information is updated following execution of response plans
4. Plan for Continuity		
MIL1	a.	The activities necessary to sustain minimum operations of IT services are identified, at least in an ad hoc manner
MIL1	b.	The sequence of activities necessary to return IT services to normal operation is identified, at least in an ad hoc manner
MIL1	c.	Continuity plans are developed, at least in an ad hoc manner, to sustain and restore IT services
MIL2	d.	Business impact analyses inform the development of continuity plans
MIL2	e.	Recovery time objectives and recovery point objectives for IT services are incorporated into continuity plans
MIL2	f.	Continuity plans are evaluated and exercised
MIL3	g.	Business impact analyses are periodically reviewed and updated

MIL3	h.	Recovery time objectives and recovery point objectives are aligned with defined risk criteria (RM-1c)
MIL3	i.	The results of continuity plan testing and/or activation are compared to recovery objectives, and plans are improved accordingly
MIL3	j.	Continuity plans are periodically reviewed and updated
MIL3	k.	Restored assets are configured appropriately and inventory information is updated following execution of continuity plans
5. Institutionalization Activities for IR Domain		
MIL1		No practice at MIL 1
MIL2	a.	Documented practices are followed for cybersecurity event and incident response and continu-ity of operations activities
MIL2	b.	Stakeholders for cybersecurity event and incident response and continuity of operations activi-ties are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support cybersecurity event and incident response and continuity of operations activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform cybersecurity event and incident response and continuity of operations activities
MIL3	e.	Cybersecurity event and incident response and continuity of operations activities are guided by documented policies or other organizational directives
MIL3	f.	Cybersecurity event and incident response and continuity of operations policies include compli-ance requirements for specified standards, guidelines, and best practices
MIL3	g.	Cybersecurity event and incident response and continuity of operations activities are periodi-cally reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of cybersecurity event and incident response and continuity of operations activities are assigned to personnel
MIL3	i.	Personnel performing cybersecurity event and incident response and continuity of operations activities have the skills and knowledge needed to perform their assigned responsibilities
(8) SUPPLY CHAIN AND EXTERNAL DEPENDENCIES MANAGEMENT (EDM)		
Objectives and Practices		
1. Identify Dependencies		
MIL1	a.	Important supplier dependencies are identified (i.e., internal and external parties on which the delivery of IT services depends), at least in an ad hoc manner

MIL1	b.	Important customer dependencies are identified (i.e., internal and external parties that depend on the delivery of IT services), at least in an ad hoc manner
MIL2	c.	Supplier dependencies are identified according to established criteria
MIL2	d.	Customer dependencies are identified according to established criteria
MIL2	e.	Single-source and other essential dependencies are identified
MIL2	f.	Dependencies are prioritized
MIL3	g.	Dependency prioritization and identification are based on defined risk criteria (RM-1c)
2. Manage Dependency Risk		
MIL1	a.	Significant cybersecurity risks due to suppliers and customers are identified and addressed, at least in an ad hoc manner
MIL1	b.	Cybersecurity requirements are considered, at least in an ad hoc manner, when establishing relationships with suppliers and customers
MIL2	c.	Identified cybersecurity dependency risks are entered into the risk register (RM-2j)
MIL2	d.	Contracts and agreements with suppliers and customers incorporate sharing of cybersecurity threat information
MIL2	e.	Cybersecurity requirements are established for suppliers according to a defined practice, in-cluding requirements for secure software development practices where appropriate
MIL2	f.	Agreements with suppliers and customers include cybersecurity requirements
MIL2	g.	Evaluation and selection of suppliers includes consideration of their ability to meet cybersecu-rity requirements
MIL2	h.	Agreements with suppliers require notification of cybersecurity incidents related to the delivery of their products or services
MIL2	i.	Suppliers are periodically reviewed for their ability to meet the cybersecurity requirements
MIL3	j.	Cybersecurity risks due to external dependencies are managed according to the organization's risk management criteria and process
MIL3	k.	Cybersecurity requirements are established for supplier dependencies based on defined risk criteria (RM-1c)
MIL3	l.	Agreements with suppliers require notification of product vulnerabilities throughout the intended lifecycle of the products
MIL3	m.	Acceptance testing of procured assets includes testing for cybersecurity requirements
MIL3	n.	Information sources are monitored to identify and avoid supply chain threats (e.g., counterfeit parts, software, and services)

3. Institutionalization Activities for EDM Domain		
MIL1		No practice at MIL 1
MIL2	a.	Documented practices are followed for managing dependency risk
MIL2	b.	Stakeholders for managing dependency risk are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support dependency risk management activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform managing dependency risk
MIL3	e.	Dependency risk management activities are guided by documented policies or other organizational directives
MIL3	f.	Dependency risk management policies include compliance requirements for specified standards, guidelines, and best practices
MIL3	g.	Dependency risk management activities are periodically reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of dependency risk management are assigned to personnel
MIL3	i.	Personnel performing dependency risk management have the skills and knowledge needed to perform their assigned responsibilities
(9) WORKFORCE MANAGEMENT (WM)		
Objectives and Practices		
1. Assign Cybersecurity Responsibilities		
MIL1	a.	Cybersecurity responsibilities for IT services are identified, at least in an ad hoc manner
MIL1	b.	Cybersecurity responsibilities are assigned to specific people, at least in an ad hoc manner
MIL2	c.	Cybersecurity responsibilities are assigned to specific roles, including external service providers (e.g., Internet service providers, security as a service providers, cloud service providers)
MIL2	d.	Cybersecurity responsibilities are documented (e.g., in position descriptions)
MIL3	e.	Cybersecurity responsibilities and job requirements are reviewed and updated as appropriate
MIL3	f.	Cybersecurity responsibilities are included in job performance evaluation criteria
MIL3	g.	Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage
2. Control the Workforce Lifecycle		

MIL1	a.	Personnel vetting (e.g., background checks, drug tests) is performed, at least in an ad hoc manner, at hire for positions that have access to the assets required for delivery of IT services
MIL1	b.	Personnel termination procedures address cybersecurity, at least in an ad hoc manner
MIL2	c.	Personnel vetting is performed at an organization-defined frequency for positions that have access to the assets required for delivery of IT services
MIL2	d.	Personnel transfer procedures address cybersecurity
MIL3	e.	Risk designations are assigned to all positions that have access to the assets required for delivery of IT services
MIL3	f.	Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation
MIL3	g.	Succession planning is performed for personnel based on risk designation
MIL3	h.	A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures
3. Develop Cybersecurity Workforce		
MIL1	a.	Cybersecurity training is made available, at least in an ad hoc manner, to personnel with assigned cybersecurity responsibilities
MIL2	b.	Cybersecurity knowledge, skill, and ability gaps are identified
MIL2	c.	Identified gaps are addressed through recruiting and/or training
MIL2	d.	Cybersecurity training is provided as a prerequisite to granting access to assets that support the delivery of IT services (e.g., new personnel training, personnel transfer training)
MIL3	e.	Cybersecurity workforce management objectives that support current and future operational needs are established and maintained
MIL3	f.	Recruiting and retention are aligned to support cybersecurity workforce management objectives
MIL3	g.	Training programs are aligned to support cybersecurity workforce management objectives
MIL3	h.	The effectiveness of training programs is evaluated at an organization-defined frequency and improvements are made as appropriate
MIL3	i.	Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities
4. Increase Cybersecurity Awareness		

MIL1	a.	Cybersecurity awareness activities occur, at least in an ad hoc manner
MIL2	b.	Objectives for cybersecurity awareness activities are established and maintained
MIL2	c.	Cybersecurity awareness content is based on the defined threat profile (TVA-1d)
MIL3	d.	Cybersecurity awareness activities are aligned with the predefined states of operation (SA-3f)
MIL3	e.	The effectiveness of cybersecurity awareness activities is evaluated at an organization-defined frequency and improvements are made as appropriate
5. Institutionalization Activities for WM Domain		
MIL1		No practice at MIL1
MIL2	a.	Documented practices are followed for cybersecurity workforce management activities
MIL2	b.	Stakeholders for cybersecurity workforce management activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support cybersecurity workforce management activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform cybersecurity work-force management activities
MIL3	e.	Cybersecurity workforce management activities are guided by documented policies or other organizational directives
MIL3	f.	Cybersecurity workforce management policies include compliance requirements for specified standards, guidelines, and best practices
MIL3	g.	Cybersecurity workforce management activities are periodically reviewed to ensure conform-ance with policy
MIL3	h.	Responsibility and authority for the performance of cybersecurity workforce management activi-ties are assigned to personnel
MIL3	i.	Personnel performing cybersecurity workforce management activities have the skills and knowledge needed to perform their assigned responsibilities
(10) CYBERSECURITY PROGRAM MANAGEMENT (CPM)		
Objectives and Practices		
1. Establish Cybersecurity Program Strategy		
MIL1	a.	The organization has a cybersecurity program strategy, which may be developed and/or man-aged in an ad hoc manner
MIL2	b.	The cybersecurity program strategy defines objectives for the organization’s cybersecurity ac-tivities
MIL2	c.	The cybersecurity program strategy and priorities are documented and aligned with the organi-zational and enterprise strategic objectives and risk to the enterprise and its mission

MIL2	d.	The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities
MIL2	e.	The cybersecurity program strategy defines the structure and organization of the cybersecurity program
MIL2	f.	The cybersecurity program strategy is approved by senior management
MIL3	g.	The cybersecurity program strategy is updated to reflect business changes, changes in the op-erating environment, and changes in the threat profile (TVA-1d)
2. Sponsor Cybersecurity Program		
MIL1	a.	Resources (people, funding, and tools) are provided, at least in an ad hoc manner, to support the cybersecurity program
MIL1	b.	Senior management provides sponsorship for the cybersecurity program, at least in an ad hoc manner
MIL2	c.	The cybersecurity program is established according to the cybersecurity program strategy
MIL2	d.	Adequate resources are provided to establish and operate a cybersecurity program aligned with the program strategy
MIL2	e.	Senior management sponsorship for the cybersecurity program is visible and active (e.g., the importance and value of cybersecurity activities is regularly communicated by senior manage-ment)
MIL2	f.	If the organization develops or procures software, secure software development practices are sponsored as an element of the cybersecurity program
MIL2	g.	The development and maintenance of cybersecurity policies is sponsored
MIL2	h.	Responsibility for the cybersecurity program is assigned to a role with requisite authority
MIL3	i.	The performance of the cybersecurity program is monitored to ensure it aligns with the cyber-security program strategy
MIL3	j.	The cybersecurity program is independently reviewed for achievement of cybersecurity pro-gram objectives
MIL3	k.	The cybersecurity program addresses and enables the achievement of regulatory compliance as appropriate
MIL3	l.	The cybersecurity program monitors and/or participates in selected industry cybersecurity standards or initiatives
3. Establish and Maintain Cybersecurity Architecture		
MIL1	a.	A strategy to segment and isolate IT service delivery systems, where feasible, is implemented, at least in an ad hoc manner
MIL2	b.	A cybersecurity architecture is in place to enable segmentation, isolation, and other require-ments that support the cybersecurity strategy

MIL2	c.	Architectural segmentation and isolation is maintained according to a documented plan
MIL3	d.	Cybersecurity architecture is updated at an organization-defined frequency to keep it current
4. Perform Secure Software Development		
MIL1		No practice at MIL1
MIL2	a.	Software to be deployed on assets that are important to the delivery of IT services is developed using secure software development practices
MIL3	b.	Policies require that software to be deployed on assets that are important to the delivery of IT services be developed using secure software development practices
5. Institutionalization Activities for CPM Domain		
MIL1		No practice at MIL1
MIL2	a.	Documented practices are followed for managing cybersecurity program activities
MIL2	b.	Stakeholders for cybersecurity program management activities are identified and involved
MIL2	c.	Standards, guidelines, and best practices have been identified to inform cybersecurity program management activities
MIL3	d.	Cybersecurity program management activities are guided by documented policies or other or-ganizational directives
MIL3	e.	Cybersecurity program management activities are periodically reviewed to ensure conformance with policy
MIL3	f.	Personnel performing cybersecurity program management activities have the skills and knowledge needed to perform their assigned responsibilities

Keterangan:
Tabel ini merupakan objective dan practice dari C2M2
Source: Pamela Curtis , Nader Mehravari , James Stevens (April 2015). Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0