

## LAMPIRAN A DATA LOG SERVER UNTIRTA

Pada tanggal 12 Agustus 2022 Server UNTIRTA Terkena DDOS/serangan

Berikut hasil Torch dari sisi Router UNTIRTA terdapat DDOS/serangan ke arah IP Server UNTIRTA (103.142.195.252).

Eth...	Prot...	Src.	Dst.	VLAN ...	DSCP	Tx Ra...	Rx Ra...	Tx Pack...	Rx Pack...
800 (...)		2.112.245.3	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.117.198.155	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.109.108.193	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.97.54.96	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.42.55.110	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.79.255.217	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.86.154.192	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.85.125.201	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.63.44.148	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.59.9.187	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.81.227.176	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.41.241.228	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.77.159.112	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.45.88.160	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.111.209.106	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.96.242.239	103.142.195.252			0 bps	528 bps	0	1
800 (...)		2.69.102.115	103.142.195.252			0 bps	528 bps	0	1
700 items		Total Tx: 377.5 kbps	Total Rx: 17.5 Mbps	Total Tx Packet: 552		Total Rx Packet: 31 448			

Log dari sisi Server

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 103.142.195.252:2406    182.0.183.189:58411    ESTABLISHED
tcp        0      1 103.142.195.252:57594  74.125.24.26:25       SYN_SENT
tcp6       0      0 103.142.195.252:80    140.213.138.40:11387  FIN_WAIT2
tcp6       0      0 103.142.195.252:443   114.119.155.96:51383   TIME_WAIT
tcp6       0      0 103.142.195.252:443   114.119.152.108:27539 TIME_WAIT
tcp6       0      0 103.142.195.252:443   114.119.155.96:50921  TIME_WAIT
tcp6       0      0 103.142.195.252:443   182.3.40.223:37048    TIME_WAIT
tcp6       0      0 103.142.195.252:443   182.3.40.223:37050    TIME_WAIT
tcp6       0      0 103.142.195.252:443   182.3.40.223:37044    TIME_WAIT
tcp6       0      0 103.142.195.252:80    140.213.136.168:12594 SYN_RECV
tcp6       0      0 103.142.195.252:443   182.3.39.246:55525    TIME_WAIT
tcp6       0      0 103.142.195.252:443   182.3.38.117:59403    ESTABLISHED
tcp6       0      0 103.142.195.252:443   182.3.39.234:55529    ESTABLISHED
tcp6       0      0 103.142.195.252:443   182.3.40.223:37046    TIME_WAIT
tcp6       0      0 103.142.195.252:443   114.119.152.108:28473 TIME_WAIT
tcp6       0      0 103.142.195.252:443   114.119.141.173:52255 TIME_WAIT
tcp6       0      0 103.142.195.252:2222  182.0.183.189:45223   ESTABLISHED
tcp6       0      0 103.142.195.252:443   182.0.147.147:42056   TIME_WAIT
tcp6       0      0 103.142.195.252:443   140.213.132.195:54882 ESTABLISHED
```

Berikut salah satu IP Address yang terdeteksi melakukan DDOS/serangan ke arah IP Server UNTIRTA.

#### IP Address Location Information for 2.112.245.3

City: Milan

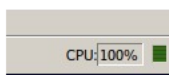
State: Lombardia

Country: Italy

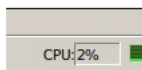
Postal Code: 20131

Time Zone: +02:00

Dampaknya Load CPU Router UNTIRTA full 100%, Sehingga koneksi internet semua site UNTIRTA dan Servers Down.



Action sementara dari sisi kami dilakukan Drop/Blackhole IP Server UNTIRTA (103.142.195.252) ke arah internet internasional, Load CPU Router UNTIRTA sudah normal kembali dan Internet sudah bisa digunakan, namun Server tidak dapat dapat di akses dari beberapa Proviser seperti Indihome.



Pada tanggal 28 Agustus 2022 hasil monitoring sudah tidak ditemukan DDOS/serangan ke arah Server UNTIRTA, Sehingga kami lakukan disable IP Server UNTIRTA dari list Drop/Blackhole

Internet dan Server untirta sudah normal kembali.

## LAMPIRAN B HASIL NETWORK SCANNING

### Lampiran B.1 Network Scanning SIAKAD Untirta

<b>Domain Name</b>		siakad.untirta.ac.id	
<b>Host IP</b>		103.142.195.98	
<b>Sistem Operasi</b>		OpenBSD 4.0 (86%)	
No	Port/Protokol	Status	Service
1	25/tcp	<i>Filtered</i>	<i>smtp</i>
2	80/tcp	<i>Open</i>	<i>http</i>
3	111/tcp	<i>Open</i>	<i>rpcbind</i>
4	139/tcp	<i>Filtered</i>	<i>netbios-ssn</i>
5	443/tcp	<i>Open</i>	<i>https</i>
6	445/tcp	<i>Filtered</i>	<i>microsoft-ds</i>
7	3306/tcp	<i>Open</i>	<i>mysql</i>
8	5678/tcp	<i>Filtered</i>	<i>rrac</i>

### Lampiran B.2 Network Scanning SPADA Untirta

<b>Domain Name</b>		spada.untirta.ac.id	
<b>Host IP</b>		103.142.195.106	
<b>Sistem Operasi</b>		OpenBSD 4.0 (86%)	
No	Port/Protokol	Status	Service
1	25/tcp	filtered	smtp
2	80/tcp	open	http
3	139/tcp	filtered	netbios-ssn
4	443/tcp	open	https
5	445/tcp	filtered	microsoft-ds
6	888/tcp	open	accessbuilder
7	2000/tcp	open	cisco-sccp
8	3003/tcp	open	cgms
9	5060/tcp	open	sip
10	5678/tcp	filtered	rrac

11	8080/tcp	open	http-proxy
12	8888/tcp	open	sun-answerbook

Lampiran B.3 *Network Scanning e-Administrasi Untirta*

<b>Domain Name</b>		eadministrasi.untirta.ac.id	
<b>Host IP</b>		103.142.195.194	
<b>Sistem Operasi</b>		OpenBSD 4.0 (86%)	
No.	Port/Protokol	Status	Service
1.	25/tcp	Filtered	smtp
2.	80/tcp	Open	http
3.	139/tcp	Filtered	netbios-ssn
4.	443/tcp	Open	https
5.	445/tcp	Filtered	microsoft-ds
6.	5678/tcp	filtered	rrac

Lampiran B.4 *Network Scanning Website Untirta dan FT Untirta*

<b>Domain Name</b>		untirta.ac.id/ft.untirta.ac.id	
<b>Host IP</b>		103.142.195.199	
<b>Sistem Operasi</b>		FreeBSD 6.2-RELEASE (87%)	
No.	Port/Protokol	Status	Service
1.	20/tcp	closed	ftp-data
2.	21/tcp	open	ftp
3.	22/tcp	closed	ssh
4.	53/tcp	open	domain
5.	80/tcp	open	http
6.	110/tcp	open	pop3
7.	143/tcp	open	imap
8.	443/tcp	open	https
9.	465/tcp	open	smtps
10.	587/tcp	open	submission
11.	993/tcp	open	imaps

12.	995/tcp	open	pop3s
13.	2222/tcp	open	EtherNetIP-3
14.	35500/tcp	closed	unknown

## LAMPIRAN C HASIL *VULNERABILITY SCANNING*

Lampiran C.1 *Vulnerability Scanning* SIAKAD Untirta

<b>Domain Name</b>	siakad.untirta.ac.id	
<b>Host IP</b>	103.142.195.98	
<b>Sistem Operasi</b>	Linux Kernel 2.6.32-754.23.1.el6.x86_64	
<b>Tingkat Kerentanan</b>	<b>Celah Keamanan</b>	<b>Skor</b>
<i>Critical</i>	PHP 5.4.x < 5.4.38 Multiple Vulnerabilities (GHOST)	9.8
9	PHP 5.4.x < 5.4.39 Multiple Vulnerabilities	9.8
	PHP 5.4.x < 5.4.40 Multiple Vulnerabilities	9.8
	PHP 5.4.x < 5.4.41 Multiple Vulnerabilities	9.8
	PHP 5.4.x < 5.4.42 Multiple Vulnerabilities	9.8
	PHP 5.4.x < 5.4.43 Multiple Vulnerabilities (BACKRONYM)	9.8
	SSL Version 2 and 3 Protocol Detection	9.8
	PHP Unsupported Version Detection	10
	PHP 5.4.x < 5.4.5 _php_stream_scandir Overflow	10
<i>High</i>	PHP 5.4.x < 5.4.17 Buffer Overflow	9.3
16	CGI Generic SQL Injection (blind)	8.3
	PHP < 7.3.24 Multiple Vulnerabilities	7.5
	SSL Medium Strength Cipher Suites Supported (SWEET32)	7.5
	ADODB tmsql.php do Parameter Arbitrary PHP Function Execution	7.5
	PHP 5.4.x < 5.4.23 OpenSSL openssl_x509_parse() Memory Corruption	7.5
	PHP 5.4.x < 5.4.30 Multiple Vulnerabilities	7.5
	PHP 5.4.x < 5.4.34 Multiple Vulnerabilities	7.5
	PHP 5.4.x < 5.4.36 'process_nested_data' RCE	7.5
	SNMP Agent Default Community Name (public)	7.5
	PHP 5.4.x < 5.4.13 Information Disclosure	7.3
	PHP 5.4.x < 5.4.19 Multiple Vulnerabilities	7.3
	PHP 5.4.x < 5.4.37 Multiple Vulnerabilities	7.3
	PHP 5.4.x < 5.4.44 Multiple Vulnerabilities	7.3
	PHP 5.4.x < 5.4.45 Multiple Vulnerabilities	7.3
	PHP 5.4.x < 5.4.28 FPM Unix Socket Insecure Permission Escalation	7.2
<i>MEDIUM</i>	PHP 5.4.x < 5.4.32 Multiple Vulnerabilities	6.8
19	TLS Version 1.0 Protocol Detection	6.5
	TLS Version 1.1 Protocol Deprecated	6.5

	Browsable Web Directories	5.3
	PHP 5.4.x < 5.4.12 Information Disclosure	5.3
	PHP < 7.3.28 Email Header Injection	5.3
	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	5.3
	Web Server info.php / phpinfo.php Detection	5.3
	nginx < 1.17.7 Information Disclosure	5.3
	Git Repository Served by Web Server	5.0
	PHP 5.4.x < 5.4.16 Multiple Vulnerabilities	5.0
	PHP 5.4.x < 5.4.24 Multiple Vulnerabilities	5.0
	PHP 5.4.x < 5.4.26 Multiple Vulnerabilities	5.0
	PHP 5.4.x < 5.4.27 awk Magic Parsing BEGIN DoS	5.0
	PHP 5.4.x < 5.4.29 'src/cdf.c' Multiple Vulnerabilities	5.0
	PHP 5.4.x < 5.4.35 'donote' DoS	5.0
	SNMP 'GETBULK' Reflection DDoS	5.0
	SSH Weak Algorithms Supported	4.3
	Web Application Potentially Vulnerable to Clickjacking	4.3
<i>LOW</i>	Web Server Allows Password Auto-Completion	N/A
6	Weak Key Exchange Algorithms Enabled	3.7
	PHP 5.4.x < 5.4.31 CLI Server 'header' DoS	2.6
	SSH Server CBC Mode Ciphers Enabled	2.6
	SSH Weak MAC Algorithms Enabled	2.6
	Web Server Transmits Cleartext Credentials	2.6

Lampiran C.2 *Vulnerability Scanning SPADA Untirta*

<b>Domain Name</b>	spada.untirta.ac.id	
<b>Host IP</b>	103.142.195.106	
<b>Sistem Operasi</b>	Linux Kernel 4.15.0-211-generic	
<b>Tingkat Kerentanan</b>	<b>Celah Keamanan</b>	<b>Skor</b>
<i>CRITICAL</i> 1	PHP Unsupported Version Detection	10
<i>HIGH</i> 1	SNMP Agent Default Community Name (public)	5.9
<i>MEDIUM</i>	TLS Version 1.0 Protocol Detection	6.5
6	TLS Version 1.1 Protocol Deprecated	6.5
	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	5.3
	Web Server info.php / phpinfo.php Detection	5.3
	nginx < 1.17.7 Information Disclosure	5.3
	SNMP 'GETBULK' Reflection DDoS	5.0
<i>LOW</i> 1	Web Server Allows Password Auto-Completion	N/A

Lampiran C.3 *Vulnerability Scanning* E Administrasi Untirta

<b>Domain Name</b>	eadministrasi.untirta.ac.id	
<b>Host IP</b>	103.142.195.98	
<b>Sistem Operasi</b>	Linux Kernel 2.6	
<b>Tingkat Kerentanan</b>	<b>Celah Keamanan</b>	<b>Skor</b>
<i>CRITICAL</i> 1	PHP Unsupported Version Detection	10
<i>HIGH</i>	CGI Generic SQL Injection (blind)	8.3
4	DNS Server Spoofed Request Amplification DDoS	7.5
	PHP < 7.3.24 Multiple Vulnerabilities	7.5
	CGI Generic SQL Injection (blind, time based)	7.5
	<i>MEDIUM</i>	JQuery 1.2 < 3.5.0 Multiple XSS
5	PHP < 7.3.28 Email Header Injection	5.3
	Web Server info.php / phpinfo.php Detection	5.3
	DNS Server Recursive Query Cache Poisoning Weakness	5.0
	Web Application Potentially Vulnerable to Clickjacking	4.3
<i>LOW</i> 1	Web Server Allows Password Auto-Completion	N/A

Lampiran C.4 *Vulnerability Scanning* Web Untirta

<b>Domain Name</b>	untirta.ac.id	
<b>Host IP</b>	103.142.195.199	
<b>Sistem Operasi</b>	Linux Kernel 2.6	
<b>Tingkat Kerentanan</b>	<b>Celah Keamanan</b>	<b>Skor</b>
<i>HIGH</i> 1	DNS Server Spoofed Request Amplification DDoS	7.5
<i>MEDIUM</i>	DNS Server Cache Snooping Remote Information Disclosure	5.3
2	DNS Server Recursive Query Cache Poisoning Weakness	5.0
<i>LOW</i>	SSH Weak Key Exchange Algorithms Enabled	3.7
2	SSH Server CBC Mode Ciphers Enabled	2.6



Lampiran C.5 Vulnerability Scanning Web FT Untirta

<b><i>Domain Name</i></b>	ft.untirta.ac.id	
<b><i>Host IP</i></b>	103.142.195.199	
<b><i>Sistem Operasi</i></b>	APC UPS Network Management Card	
<b><i>Tingkat Kerentanan</i></b>	<b><i>Celah Keamanan</i></b>	<b><i>Skor</i></b>
<i>HIGH</i>	DNS Server Spoofed Request Amplification DDoS	7.5
<i>MEDIUM</i>	DNS Server Recursive Query Cache Poisoning Weakness	5.0

## LAMPIRAN D REKOMENDASI

Lampiran D.1 Rekomendasi Keamanan Layanan Teknologi Informasi Untirta

Kerentanan	Rekomendasi
PHP 5.4.x < 5.4.38 Multiple Vulnerabilities (GHOST)	Upgrade PHP ke versi terbaru
PHP 5.4.x < 5.4.39 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.40 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.41 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.42 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.43 Multiple Vulnerabilities (BACKRONYM)	
PHP Unsupported Version Detection	
PHP 5.4.x < 5.4.5 _php_stream_scandir Overflow	
PHP Unsupported Version Detection	
PHP Unsupported Version Detection	
PHP 5.4.x < 5.4.17 Buffer Overflow	
PHP < 7.3.24 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.23 OpenSSL openssl_x509_parse() Memory Corruption	
PHP 5.4.x < 5.4.30 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.34 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.36 'process_nested_data' RCE	
PHP 5.4.x < 5.4.13 Information Disclosure	
PHP 5.4.x < 5.4.19 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.37 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.44 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.45 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.28 FPM Unix Socket Insecure Permission Escalation	
PHP < 7.3.24 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.32 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.12 Information Disclosure	
PHP < 7.3.28 Email Header Injection	
PHP 5.4.x < 5.4.16 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.24 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.26 Multiple Vulnerabilities	
PHP 5.4.x < 5.4.27 awk Magic Parsing BEGIN DoS	
PHP 5.4.x < 5.4.29 'src/cdf.c' Multiple Vulnerabilities	
PHP 5.4.x < 5.4.35 'donote' DoS	

PHP < 7.3.28 Email Header Injection		
PHP 5.4.x < 5.4.31 CLI Server 'header' DoS		
SSL Version 2 and 3 Protocol Detection	Upgrade protokol keamanan ke TLS 1.2 atau 1.3	
SSL Medium Strength Cipher Suites Supported (SWEET32)		
TLS Version 1.0 Protocol Detection		
TLS Version 1.1 Protocol Deprecated		
SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)		
TLS Version 1.0 Protocol Detection		
TLS Version 1.1 Protocol Deprecated		
SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)		
SSH Weak Algorithms Supported		Hubungi vendor atau lihat dokumentasi produk untuk menghapus chipers(sandi) yang lemah
SSH Server CBC Mode Ciphers Enabled		
SSH Weak MAC Algorithms Enabled		
SSH Weak Key Exchange Algorithms Enabled		
SSH Server CBC Mode Ciphers Enabled		
SSH Weak Key Exchange Algorithms Enabled		
DNS Server Spoofed Request Amplification DDoS	Batasi akses ke server DNS dari jaringan publik atau konfigurasi ulang untuk menolak permintaan tersebut.	
DNS Server Spoofed Request Amplification DDoS		
DNS Server Spoofed Request Amplification DDoS		
DNS Server Recursive Query Cache Poisoning Weakness	Batasi kueri rekursif ke host yang harus menggunakan nameserver ini	
DNS Server Recursive Query Cache Poisoning Weakness		
DNS Server Recursive Query Cache Poisoning Weakness		
CGI Generic SQL Injection (blind)	Ubah skrip CGI yang terpengaruh sehingga terhindar dari argumen dengan benar	
CGI Generic SQL Injection (blind, time based)		
CGI Generic SQL Injection (blind)		
SNMP Agent Default Community Name (public)	Nonaktifkan layanan SNMP pada host jarak jauh ketika tidak menggunakannya	
SNMP Agent Default Community Name (public)		
SNMP 'GETBULK' Reflection DDoS		
SNMP 'GETBULK' Reflection DDoS		
nginx < 1.17.7 Information Disclosure	Upgrade nginx ke versi terbaru	

nginx < 1.17.7 Information Disclosure	
Web Server info.php / phpinfo.php Detection	Hapus file yang terpengaruh (phpinfo.php)
Web Server info.php / phpinfo.php Detection	
Web Server info.php / phpinfo.php Detection	
Web Server Allows Password Auto-Completion	Tambahkan atribut 'autocomplete=off' untuk mencegah browser menyimpan kredensial dalam cache
Web Server Allows Password Auto-Completion	
Web Server Allows Password Auto-Completion	
Web Application Potentially Vulnerable to Clickjacking	Kembalikan header HTTP X-Frame-Options atau Content-Security-Policy (dengan arahan 'frame-ancestors') dengan respons halaman
Web Application Potentially Vulnerable to Clickjacking	
JQuery 1.2 < 3.5.0 Multiple XSS	Upgrade JQuery ke versi terbaru
DNS Server Cache Snooping Remote Information Disclosure	Hubungi vendor perangkat lunak DNS untuk perbaikan.
ADODB tmssql.php do Parameter Arbitrary PHP Function Execution	Hapus skrip pengujian atau tingkatkan ke ADODB versi 4.70 atau lebih tinggi
Browsable Web Directories	Pastikan direktori yang dapat dijelajahi tidak membocorkan informasi rahasia atau memberikan akses ke sumber daya sensitif. Selain itu, gunakan pembatasan akses atau nonaktifkan pengindeksan direktori untuk semua yang melakukannya
Git Repository Served by Web Server	Verifikasi bahwa repositori Git yang terdaftar disajikan dengan sengaja
Web Server Transmits Cleartext Credentials	Pastikan bahwa setiap formulir sensitif mengirimkan konten melalui HTTPS

Lampiran D.2 Rekomendasi Manajemen Layanan Teknologi Informasi Untirta

No.	Proses	Rekomendasi
1	<i>Service Operation Process in General</i>	Meningkatkan peran, fungsi, kebijakan, serta faktor keberhasilan terutama indikator kinerja utama pada <i>service operation process</i> yang dimiliki oleh UPT Data dan Informasi Untirta.
2	<i>Event Management</i>	Meningkatkan pengelolaan peristiwa terutama dalam peninjauan setiap peristiwa yang ada pada layanan teknologi informasi Untirta.
3	<i>Incident Management</i>	Meningkatkan penanganan insiden terutama dalam pengidentifikasian insiden serta mendokumentasikan insiden yang terjadi pada layanan teknologi informasi Untirta.
4	<i>Request Fullfilment</i>	Meningkatkan bagaimana permintaan untuk pemenuhan kebutuhan dapat terpenuhi untuk pengembangan layanan teknologi informasi.
5	<i>Problem Management</i>	Meningkatkan pencegahan masalah yang ada pada layanan terutama pada pendeteksian kesalahan serta membuat <i>known error database</i> untuk memudahkan diagnosis serta resolusi pada suatu masalah.
6	<i>Access Management</i>	Meningkatkan manajemen dalam pemberian akses terhadap layanan teknologi informasi Untirta
7	<i>Common Service Operation Activities</i>	Meningkatkan manajemen pada aktivitas umum <i>service operation</i> dengan melakukan pemantauan dan kendali layanan, melakukan audit <i>service operation</i> , serta mengukur ketersediaan dari perspektif teknologi informasi dan organisasi

**LAMPIRAN E HASIL KUESIONER ITIL V3 *SERVICE OPERATION***

No	Proses Operasi Layanan		Responden				Total	Count	AVG	Gap
			1	2	3	4				
1	UPT Data dan Informasi memiliki dan menetapkan peran dan fungsi <b>dari setiap proses pada service operation</b> dengan jelas		3	4	4	5	16	4	4	1
2	UPT Data dan Informasi telah menentukan <i>Goal</i> , Objektif, tujuan dan ruang lingkup yang jelas <b>dari setiap proses service operation</b> pada layanan teknologi informasi		3	4	5	5	17	4	4,25	0,75
3	UPT Data dan Informasi telah menentukan nilai bisnis <b>dari setiap proses pada service operation</b>		3	4	3	5	15	4	3,75	1,25
4	UPT Data dan Informasi telah menetapkan kebijakan, prinsip, dan konsep dasar <b>dari setiap proses service operation</b> pada layanan teknologi informasi		3	4	4	5	16	4	4	1
5	UPT Data dan Informasi telah menentukan pemicu, input, output, dan antarmuka <b>dari setiap proses service operation</b> pada layanan teknologi informasi		3	4	5	4	16	4	4	1
6	UPT Data dan Informasi telah menenetapkan IKU dan metrik <b>dari setiap proses pada service operation</b>		3	3	3	4	13	4	3,25	1,75
7	UPT Data dan Informasi telah menentukan pelaporan <b>dari setiap proses service operation</b> pada layanan teknologi informasi		3	4	2	5	14	4	3,5	1,5
8	UPT Data dan Informasi telah menentukan tantangan, faktor keberhasilan dan risiko yang kritis pada <b>setiap proses service operation</b> pada layanan teknologi informasinya		3	4	5	4	16	4	4	1
SCORE			24	31	31	37	123	32	3,84	1,16
No	EM	EVENT MANAGEMENT / MANAJEMEN ACARA								
9	1	UPT Data dan Informasi memiliki cara mengetahui terjadinya suatu peristiwa dari layanan teknologi informasinya	3	3	4	4	14	4	3,5	1,5

10	2	UPT Data dan Informasi memiliki aktivitas pemberitahuan peristiwa dan pendektasian peristiwa pada layanan teknologi informasinya	3	4	4	3	14	4	3,5	1,5
11	3	UPT Data dan Informasi menyaring peristiwa-peristiwa yang terjadi pada layanan teknologi informasinya	3	3	4	4	14	4	3,5	1,5
12	4	UPT Data dan Informasi mengkategorisasi setiap peristiwa yang terjadi dari layanan teknologi informasinya	3	3	5	4	15	4	3,75	1,25
13	5	UPT Data dan Informasi melakukan korelasi antar peristiwa yang terjadi dari layanan teknologi informasinya	3	3	3	4	13	4	3,25	1,75
14	6	UPT Data dan Informasi mengetahui pemicu/penyebab peristiwa yang terjadi dari layanan teknologi informasinya	3	3	4	4	14	4	3,5	1,5
15	7	Setelah peristiwa terjadi, UPT Data dan Informasi memiliki aktivitas untuk memilih tanggapan yang tepat untuk peristiwa pada layanan teknologi informasi tersebut	3	3	5	4	15	4	3,75	1,25
16	8	UPT Data dan Informasi melakukan tinjauan dari hasil tanggapan yang diberikan pada peristiwa yang terjadi dari layanan teknologi informasinya	3	3	3	4	13	4	3,25	1,75
17	9	UPT Data dan Informasi mengetahui jika peristiwa tersebut telah selesai dan dapat ditutup	3	4	4	4	15	4	3,75	1,25
<b>SCORE</b>			30	33	40	39	142	40	3,53	1,47
<b>No</b>	<b>IM</b>	<b>INCIDENT MANAGEMENT / MANAJEMEN INSIDEN</b>								
18	1	UPT Data dan Informasi telah menyepakati rentang waktu untuk semua tahapan penanganan insiden pada layanan teknologi informasinya	3	4	4	3	14	4	3,5	1,5
19	2	UPT Data dan Informasi telah menentukan model insiden yang terjadi pada layanan teknologi informasi	3	3	4	5	15	4	3,75	1,25
20	3	UPT Data dan Informasi telah menentukan Insiden utama ( <i>Major</i> ) yang terjadi pada layanan teknologi informasi	3	4	5	4	16	4	4	1



21	4	UPT Data dan Informasi memiliki aktivitas pengidentifikasian insiden yang terjadi pada layanan teknologi informasi	3	3	3	4	13	4	3,25	1,75
22	5	UPT Data dan Informasi melakukan <i>logging</i> pada setiap insiden yang terjadi pada layanan teknologi informasi	3	3	3	4	13	4	3,25	1,75
23	6	UPT Data dan Informasi melakukan pengelompokan insiden yang terjadi pada layanan teknologi informasi	3	3	4	4	14	4	3,5	1,5
24	7	UPT Data dan Informasi mengurutkan insiden yang terjadi pada layanan teknologi informasi berdasarkan prioritas	3	4	4	4	15	4	3,75	1,25
25	8	UPT Data dan Informasi melakukan diagnosa awal dari insiden yang terjadi pada layanan teknologi informasi	3	4	3	4	14	4	3,5	1,5
26	9	UPT Data dan Informasi melakukan eskalasi insiden pada beberapa insiden yang terjadi pada layanan teknologi informasi	3	4	5	4	16	4	4	1
27	10	UPT Data dan Informasi melakukan investigasi pada insiden yang terjadi pada layanan teknologi informasi	3	4	3	4	14	4	3,5	1,5
28	11	UPT Data dan Informasi melakukan pemulihan pasca insiden yang terjadi pada layanan teknologi informasi	3	4	4	5	16	4	4	1
29	12	UPT Data dan Informasi mengetahui jika insiden tersebut telah selesai ditangani dan dapat ditutup	3	4	4	4	15	4	3,75	1,25
<b>SCORE</b>			39	48	50	53	190	52	3,65	1,35
<b>No</b>	<b>RF</b>	<b>REQUEST FULLFILMENT / PEMENUHAN PERMINTAAN</b>								
30	1	UPT Data dan Informasi memiliki pilihan untuk meminta kebutuhan apa saja yang ingin dipenuhi untuk mengembangkan layanan teknologi informasi	3	3	3	4	13	4	3,25	1,75
31	2	Dalam permintaan pemenuhan kebutuhan, UPT Data dan Informasi memerlukan persetujuan keuangan dari pihak yang berwenang	3	4	3	3	13	4	3,25	1,75
32	3	Dalam permintaan pemenuhan kebutuhan, UPT Data dan Informasi juga memerlukan persetujuan lainnya dari pihak yang berwenang	3	4	3	3	13	4	3,25	1,75

33	4	UPT Data dan Informasi mendapatkan permintaan kebutuhan yang teepenuhi untuk layanan teknologi informasi	3	4	3	3	13	4	3,25	1,75
34	5	UPT Data dan Informasi mengetahui kapan permintaan kebutuhan telah selesai	3	4	4	4	15	4	3,75	1,25
SCORE			18	23	20	21	82	24	3,35	1,65
No	PM	PROBLEM MANAGEMENT / MANAJEMEN MASALAH								
35	1	UPT Data dan Informasi memiliki aktivitas untuk mendeteksi masalah pada layanan teknologi informasi	3	3	4	5	15	4	3,75	1,25
36	2	UPT Data dan Informasi melakukan <i>logging</i> /membukukan masalah yang terjadi pada layanan teknologi informasi	3	3	3	5	14	4	3,5	1,5
37	3	UPT Data dan Informasi mengkategorisasi setiap masalah yang terjadi dari layanan teknologi informasinya	3	3	4	4	14	4	3,5	1,5
38	4	UPT Data dan Informasi mengurutkan masalah yang terjadi pada layanan teknologi informasi berdasarkan priotitas	3	4	3	4	14	4	3,5	1,5
39	5	UPT Data dan Informasi melakukan penyelidikan dan diagnosis masalah yang terjadi pada layanan teknologi informasi	3	4	4	4	15	4	3,75	1,25
40	6	UPT Data dan Informasi melakukan pencarian solusi masalah yang terjadi	3	4	5	3	15	4	3,75	1,25
41	7	UPT Data dan Informasi menambahkan masalah layanan kedalam catatan kesalahan yang telah diketahui ( <i>known error record</i> )	3	3	5	3	14	4	3,5	1,5
42	8	UPT Data dan Informasi melakukan proses pemecahan masalah	3	4	4	4	15	4	3,75	1,25
43	9	UPT Data dan Informasi mengetahui jika suatu masalah telah selesai ditangani dan dapat ditutup	3	4	3	4	14	4	3,5	1,5
44	10	UPT Data dan Informasi melakukan peninjauan kembali jenis masalah pada layanan teknologi informasi	3	4	4	4	15	4	3,75	1,25
45	11	UPT Data dan Informasi melakukan pendeteksian kesalahan dalam lingkungan pengembangan	3	3	3	4	13	4	3,25	1,75

46	12	UPT Data dan Informasi memanfaatkan CMS ( <i>Configuration Management System</i> ) sebagai sumber yang berharga untuk manajemen masalah	3	3	5	3	14	4	3,5	1,5
47	13	UPT Data dan Informasi memiliki database kesalahan yang diketahui ( <i>Known Error Database</i> ) untuk memungkinkan diagnosis dan resolusi yang lebih cepat	3	3	3	4	13	4	3,25	1,75
SCORE			42	48	53	55	198	56	3,56	1,44
<b>No</b>	<b>AM</b>	<b>ACCESS MANAGEMENT / MANAJEMEN AKSES</b>								
48	1	UPT Data dan Informasi memiliki aktivitas permintaan untuk mengakses layanan	3	4	3	3	13	4	3,25	1,75
49	2	UPT Data dan Informasi melakukan verifikasi dari permintaan akses layanan tersebut	3	4	3	4	14	4	3,5	1,5
50	3	UPT Data dan Informasi menyediakan hak untuk mengakses layanan	3	4	4	3	14	4	3,5	1,5
51	4	UPT Data dan Informasi melakukan pemantauan status identitas	3	4	4	4	15	4	3,75	1,25
52	5	UPT Data dan Informasi melakukan pencatatan dan penelusuran kegiatan akses	3	4	4	5	16	4	4	1
53	6	UPT Data dan Informasi dapat menghapus atau mengurangi hak akses	3	4	4	3	14	4	3,5	1,5
SCORE			21	28	26	25	100	28	3,58	1,42
OVERALL SCORE SOP			159	192	201	211	763	212	3,60	1,40
<b>Kegiatan Umum Operasi Layanan</b>										
1		UPT Data dan Informasi melakukan kegiatan pemantauan dan kendali pada layanan dengan teratur dan berkelanjutan	3	4	4	2	13	4	3,25	1,75
2		UPT Data dan Informasi memastikan bahwa kondisi tertentu dipenuhi (atau tidak terpenuhi) dan jika tidak, maka akan menaikkan	3	4	3	2	12	4	3	2

	peringatan ke grup yang sesuai (mis. Ketersediaan perangkat jaringan utama)								
3	UPT Data dan Informasi memastikan bahwa kinerja atau pemanfaatan komponen atau sistem berada dalam kisaran yang ditentukan (mis. Ruang disk atau pemanfaatan memori)	3	4	4	4	15	4	3,75	1,25
4	UPT Data dan Informasi mendeteksi jenis atau tingkat aktivitas yang abnormal dalam infrastruktur (mis. Ancaman keamanan potensial)	3	4	3	4	14	4	3,5	1,5
5	UPT Data dan Informasi mendeteksi perubahan yang tidak sah (mis. Pengenalan perangkat lunak baru)	3	4	4	4	15	4	3,75	1,25
6	UPT Data dan Informasi memastikan kepatuhan terhadap kebijakan organisasi (mis. Penggunaan email yang tidak tepat)	3	4	4	3	14	4	3,5	1,5
7	UPT Data dan Informasi melacak informasi apa pun yang digunakan untuk mengukur indikator kinerja utama	3	2	4	5	14	4	3,5	1,5
8	UPT Data dan Informasi menafsirkan makna sebuah informasi dengan tepat	3	4	3	4	14	4	3,5	1,5
9	UPT Data dan Informasi dapat menentukan dimana informasi akan digunakan (mis. data masalah di suatu divisi dapat diakses divisi yang bertanggung jawab)	3	4	4	4	15	4	3,75	1,25
10	UPT Data dan Informasi memastikan bahwa pembuat keputusan memiliki akses ke informasi yang akan memungkinkan mereka untuk membuat keputusan	3	4	4	3	14	4	3,5	1,5
11	UPT Data dan Informasi merutekan informasi yang dilaporkan ke orang, kelompok, atau alat yang tepat	3	4	4	4	15	4	3,75	1,25
12	UPT Data dan Informasi menggunakan alat untuk menentukan kondisi apa yang mewakili operasi normal atau abnormal	3	4	4	3	14	4	3,5	1,5
13	UPT Data dan Informasi memiliki kegiatan dalam mengatur kinerja perangkat, sistem atau layanan	3	3	3	2	11	4	2,75	2,25

14	UPT Data dan Informasi mengukur ketersediaan dari perspektif TI dan organisasi	3	3	5	2	13	4	3,25	1,75
15	UPT Data dan Informasi memulai tindakan korektif, yang dapat diotomatisasi (mis. Reboot perangkat dari jarak jauh atau jalankan skrip), atau manual	3	4	5	4	16	4	4	1
16	UPT Data dan Informasi melakukan audit operasi layanan	3	4	4	2	13	4	3,25	1,75
17	Dalam operasi TI UPT Data dan Informasi memiliki peran penjadwalan pekerjaan, peran cadangan dan pemulihan, dan peran cetak dan output yang ditentukan	3	4	2	5	14	4	3,5	1,5
18	UPT Data dan Informasi memiliki manajemen mainframe	3	4	4	4	15	4	3,75	1,25
19	UPT Data dan Informasi memiliki manajemen dan dukungan server	3	4	4	4	15	4	3,75	1,25
20	UPT Data dan Informasi memiliki manajemen Jaringan	3	4	4	4	15	4	3,75	1,25
21	UPT Data dan Informasi memiliki penyimpanan dan arsip	3	4	4	4	15	4	3,75	1,25
22	UPT Data dan Informasi memiliki Administrasi Database	3	4	4	4	15	4	3,75	1,25
23	UPT Data dan Informasi memiliki Manajemen Layanan Direktori	3	4	4	4	15	4	3,75	1,25
24	UPT Data dan Informasi memiliki Dukungan desktop	3	4	4	4	15	4	3,75	1,25
25	UPT Data dan Informasi memiliki Manajemen Middleware	3	4	4	4	15	4	3,75	1,25
26	UPT Data dan Informasi memiliki Manajemen Internet/Web	3	4	4	3	14	4	3,5	1,5
27	UPT Data dan Informasi memiliki Fasilitas dan manajemen pusat data	3	4	4	3	14	4	3,5	1,5
28	UPT Data dan Informasi memiliki Manajemen Keamanan Informasi dalam Operasi Layanan	3	4	4	4	15	4	3,75	1,25
OVERALL SCORE CSOA		84	108	108	99	399	112	3,56	1,44