

**LAMPIRAN A**  
***PENETRATION TESTING***

## Lampiran A-1 Hasil Pengujian untuk mengetahui Alamat IP di Kali Linux

```
(root@ DESKTOP-05879J4)-[~/home/fitri]
# ping siakad.untirta.ac.id
PING siakad.untirta.ac.id (103.142.195.98) 56(84) bytes of data.
64 bytes from 103.142.195.98: icmp_seq=1 ttl=50 time=48.4 ms
64 bytes from 103.142.195.98: icmp_seq=2 ttl=50 time=45.7 ms
64 bytes from 103.142.195.98: icmp_seq=3 ttl=50 time=51.5 ms
64 bytes from 103.142.195.98: icmp_seq=4 ttl=50 time=33.0 ms
64 bytes from 103.142.195.98: icmp_seq=5 ttl=50 time=37.9 ms
64 bytes from 103.142.195.98: icmp_seq=6 ttl=50 time=47.2 ms
64 bytes from 103.142.195.98: icmp_seq=7 ttl=50 time=38.2 ms
64 bytes from 103.142.195.98: icmp_seq=8 ttl=50 time=37.3 ms
64 bytes from 103.142.195.98: icmp_seq=9 ttl=50 time=57.0 ms
64 bytes from 103.142.195.98: icmp_seq=10 ttl=50 time=42.9 ms
64 bytes from 103.142.195.98: icmp_seq=11 ttl=50 time=43.3 ms
64 bytes from 103.142.195.98: icmp_seq=12 ttl=50 time=36.9 ms
64 bytes from 103.142.195.98: icmp_seq=13 ttl=50 time=36.9 ms
64 bytes from 103.142.195.98: icmp_seq=14 ttl=50 time=34.0 ms
64 bytes from 103.142.195.98: icmp_seq=15 ttl=50 time=38.1 ms
64 bytes from 103.142.195.98: icmp_seq=16 ttl=50 time=32.1 ms
64 bytes from 103.142.195.98: icmp_seq=17 ttl=50 time=33.0 ms
64 bytes from 103.142.195.98: icmp_seq=18 ttl=50 time=38.7 ms
64 bytes from 103.142.195.98: icmp_seq=19 ttl=50 time=30.6 ms
64 bytes from 103.142.195.98: icmp_seq=20 ttl=50 time=36.0 ms
64 bytes from 103.142.195.98: icmp_seq=21 ttl=50 time=40.0 ms
64 bytes from 103.142.195.98: icmp_seq=22 ttl=50 time=44.9 ms
64 bytes from 103.142.195.98: icmp_seq=23 ttl=50 time=41.6 ms
64 bytes from 103.142.195.98: icmp_seq=24 ttl=50 time=46.7 ms
64 bytes from 103.142.195.98: icmp_seq=25 ttl=50 time=35.9 ms
64 bytes from 103.142.195.98: icmp_seq=26 ttl=50 time=36.0 ms
```

## Lampiran A-2 Hasil Pengujian Menggunakan *Tools* whois

```
(root@ DESKTOP-05879J4)-[~/home/fitri]
# whois 103.142.195.98
% [whois.apnic.net]
% whois data copyright terms http://www.apnic.net/db/dbcopyright.html
% Information related to '103.142.194.0 - 103.142.195.255'
% Abuse contact for '103.142.194.0 - 103.142.195.255' is 'hostmaster@untirta.ac.id'

inetnum:          103.142.194.0 - 103.142.195.255
netname:          IDNIC-UNTIRTA-ID
descr:            Universitas Sultan Ageng Tirtayasa
descr:            Education / Direct member IDNIC
descr:            Jl. Raya Jakarta Km 4
descr:            Pakupatan Kota Serang
admin-c:          AS2042-AP
tech-c:           AS2042-AP
country:         ID
mnt-by:          PMT-APJXX-ID
mnt-irt:         IRT-UNTIRTA-ID
mnt-routes:     PAINT-ID-UNTIRTA
status:          ASSIGNED PORTABLE
last-modified:   2019-09-04T04:44:20Z
source:         APNIC

irt:              IRT-UNTIRTA-ID
address:          Universitas Sultan Ageng Tirtayasa
address:          Jl. Raya Jakarta Km 4
address:          Pakupatan Kota Serang
e-mail:          hostmaster@untirta.ac.id
abuse-mailbox:   hostmaster@untirta.ac.id
admin-c:         AS2042-AP
tech-c:          AS2042-AP
auth:            # Filtered
mnt-by:         PAINT-ID-UNTIRTA
last-modified:   2019-09-04T04:39:23Z
source:         APNIC

person:          Aep Saepudin
address:         Jl. Raya Jakarta Km 4 Pakupatan Kota Serang
address:         Serang 42133, Indonesia
country:         ID
phone:           +62-254-280330
e-mail:         hostmaster@untirta.ac.id
```

## Lampiran A-3 Hasil Pengujian Menggunakan *Tools* DNSrecon

```
(root@ DESKTOP-05879J4)-[~/home/fitri]
# dnsrecon -d siakad.untirta.ac.id
[*] std: Performing General Enumeration against: siakad.untirta.ac.id...
[-] DNSSEC is not configured for siakad.untirta.ac.id
[*] A siakad.untirta.ac.id 103.142.195.98
[*] Enumerating SRV Records
[+] 0 Records Found
```

### Lampiran A-4 Hasil Pengujian Menggunakan *Tools* whatweb

```
(root@ DESKTOP-05879J4)-[~/home/fitri]
# whatweb siakad.untirta.ac.id
http://siakad.untirta.ac.id [200 OK] HTML5, HTTPServer[nginx/1.10.3], IP[103.142.195.98], Meta-Refresh-Redirect[http://sia.untirta.ac.id/portal/], Script[text/javascript], Title[Page Redirection], nginx[1.10.3]
ERROR Opening: http://sia.untirta.ac.id/portal/ - no address for sia.untirta.ac.id
```

### Lampiran A-5 Hasil Pengujian Menggunakan *Tools* sslscan

```
root@DESKTOP-05879J4: /home/fitri
# sslscan siakad.untirta.ac.id
Version: 2.0.10-static
OpenSSL 1.1.1u-dev xx XXX xxxx
Connected to 103.142.195.98
Testing SSL server siakad.untirta.ac.id on port 443 using SNI name siakad.untirta.ac.id

SSL/TLS Protocols:
SSLv2 disabled
SSLv3 enabled
TLSv1.0 enabled
TLSv1.1 enabled
TLSv1.2 enabled
TLSv1.3 disabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Secure session renegotiation supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed

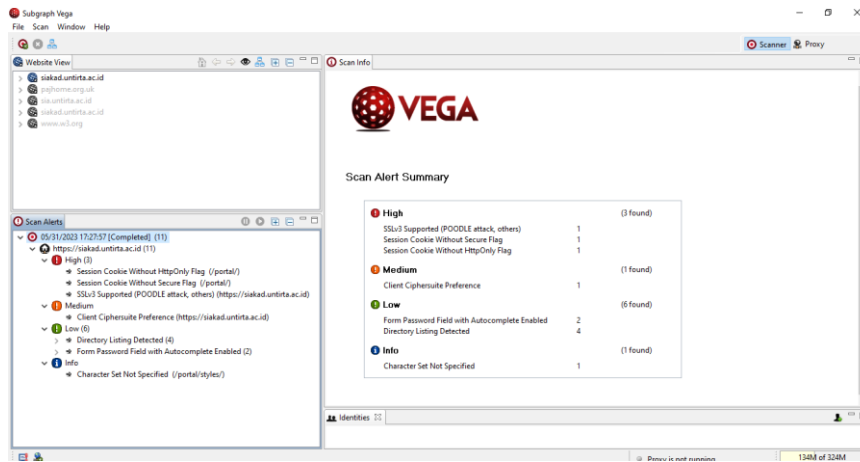
Supported Server Cipher(s):
Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 1024 bits
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 1024 bits
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 1024 bits
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits DHE-RSA-AES128-SHA256 DHE 1024 bits
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA DHE 1024 bits
Accepted TLSv1.2 256 bits DHE-RSA-CAMELLIA256-SHA DHE 1024 bits
```

### Lampiran A-6 Hasil Pengujian Menggunakan *Tools* Nmap

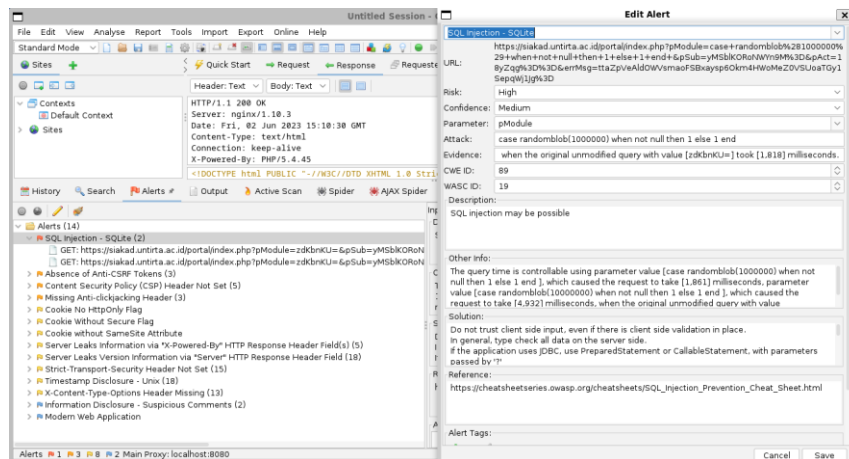
```
(root@ DESKTOP-05879J4)-[~/home/fitri]
# nmap siakad.untirta.ac.id
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 16:22 WIB
Nmap scan report for siakad.untirta.ac.id (103.142.195.98)
Host is up (0.047s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
25/tcp    filtered smtp
80/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
3306/tcp  open  mysql
5678/tcp  filtered rrac

Nmap done: 1 IP address (1 host up) scanned in 37.82 seconds
```

## Lampiran A-7 Hasil Pengujian Menggunakan *Tools Vega*



## Lampiran A-8 Hasil Pengujian Menggunakan *Tools Owasp Zap*



## Lampiran A-9 Hasil Pengujian Simulasi Serangan Sql injection Menggunakan Tools sqlmap

```
└─$ sqlmap -u https://stakad.untirta.ac.id/portal/index.php?id=1 --db=
[1.7.2#stable]
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 21:24:13 /2023-06-02/

[21:24:14] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=3gv3bph935b...4qhw7o61S'). Do you want to use those [Y/n] y
[21:25:07] [INFO] testing if the target URL content is stable
[21:25:15] [INFO] target URL content is stable
[21:25:15] [INFO] testing if GET parameter 'id' is dynamic
[21:25:20] [WARNING] GET parameter 'id' does not appear to be dynamic
[21:25:30] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[21:25:37] [INFO] testing for SQL injection on GET parameter 'id'
[21:25:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:25:45] [INFO] testing 'boolean-based blind - Parameter replace (original value)'
[21:25:46] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:25:47] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[21:25:49] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (ID)'
[21:25:50] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (SQLType)'
[21:25:57] [INFO] testing 'Generic inline queries'
[21:25:57] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[21:25:57] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[21:25:59] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[21:26:00] [INFO] testing 'Oracle stacked queries (DUMP_PIPE_RECEIVE MESSAGE - comment)'
[21:26:01] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[21:26:07] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[21:26:08] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[21:26:10] [INFO] testing 'Oracle AND time-based blind'
It is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you
[21:26:49] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[21:27:07] [WARNING] GET parameter 'id' does not seem to be injectable
[21:27:07] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If
you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch
to '--random-agent'

[*] ending @ 21:27:07 /2023-06-02/
```

**LAMPIRAN B**

**RACI CHART**

### Lampiran B-1 Raci Chart APO13

APO13 RACI CHART	
Key Management Practice	
	Board
	Chief Executive Officer
	Chief Financial Officer
	Chief Operating Officer
	Business Executives
	Business Process Owners
	Strategy Executives Committee
	Steering (Programmes/Project)
	Project Management Office
	Value Management Office
	Chief Risk Officer
	Chief Information Security
	Architecture Board
	Enterprise Risk Committee
	Head Human Resources
	Compliance
	Audit
	Chief Information Officer
	Head Architect
	Head Development
	Head IT Operations
	Head IT Administration
	Service Manager
	Information Security Manager
	Business Continuity Manager
	Privacy Officer
APO13-1	C
APO13-2	C
APO13-3	C

### Lampiran B-2 Raci chart DSS05

DSS05 RACI CHART	
Key Management Practice	
	Board
	Chief Executive Officer
	Chief Financial Officer
	Chief Operating Officer
	Business Executives
	Business Process Owners
	Strategy Executives Committee
	Steering (Programmes/Project)
	Project Management Office
	Value Management Office
	Chief Risk Officer
	Chief Information Security
	Architecture Board
	Enterprise Risk Committee
	Head Human Resources
	Compliance
	Audit
	Chief Information Officer
	Head Architect
	Head Development
	Head IT Operations
	Head IT Administration
	Service Manager
	Information Security Manager
	Business Continuity Manager
	Privacy Officer
DSS5-1	R I
DSS5-2	I
DSS5-3	I
DSS5-4	R
DSS5-5	I
DSS5-6	I
DSS5-7	C

**LAMPIRAN C**  
**HASIL REKOMENDASI**



Lampiran C-1 Hasil Rekomendasi *Vulnerability Assessment*

No	Kerentanan	Rekomendasi
1	<i>Session cookie without Httponly flag</i>	Mengkonfigurasi dengan mengatur <i>session cookie HttpOnly Flag set</i>
2	<i>Session cookie without secure flag</i>	Konfigurasi dengan mengatur <i>session cookie secure flag set.</i>
3	<i>SSLv3 supported (POODLE attack, others)</i>	Menonaktifkan SSLv3, kemungkinan server https harus di restart agar perubahan konfigurasi dapat diterapkan
4	<i>Client ciphersuite preference</i>	Server https harus menkonfigurasi untuk menerapkan preferensi <i>ciphersuite server.</i>
5	<i>Directory listing detected</i>	Untuk Apache, tambah “indexIgnore*” pada direktori file .htaccess. Mengubah “dir-listing.activate = “aktif” ke “dir-listing.activate = “non-aktif” dalam konfigurasi lighttpd.
6	<i>Missing anti-clickjacking-header</i>	Gunakan X-frame-options untuk menghindari website dari penyerang.
7	<i>Sql injection</i>	Memeriksa semua data di server, apabila ada validasi sisi klien.
8	<i>Absence of anti-CSRF tokens</i>	Gunakan anti-CSRF.
9	<i>Content-security-policy (CSP) header not set</i>	Konfigurasi server web untuk mengembalikan header HTTP <i>content-security -policy (CSP)</i>

No	Kerentanan	Rekomendasi
10	<i>Cookie without samesite attribute</i>	Memilih atribut <i>website</i> yang sama lalu atur ke <i>lax</i> idealnya <i>strict</i> untuk <i>cookie</i> .
11	<i>Server leak information via x-powered-By HTTP response header field(s)</i>	Memilih <i>web, application, load balancer</i> lalu dikonfigurasi untuk mengklik <i>x-powered-by</i> header.
12	<i>Server leaks version information via server HTTP response header field</i>	Memilih <i>web, application, load balancer</i> dikonfigurasi untuk menekan server header.
13	<i>strict-transport-security header not set</i>	Konfigurasi keamanan transportasi yang ketat agar memastikan hanya permintaan HTTPS yang dianggap valid dan sangat mengurangi resiko mengakses halaman yang mencurigakan.
14	<i>Timestamp Disclosure – Unix</i>	Mengkonfirmasi secara manual bahwa data stempel waktu tidak sensitif, dan data tidak dapat digabungkan untuk diungkapkan yang dapat dieksploitasi.
15	<i>X-content-type-options header missing</i>	Memastikan web mengaktifkan header tipe konten yang tepat, dan menngaktifkan header <i>x-content-type-options</i> ke <i>nosniff</i> untuk semua halaman web.

Lampiran C-2 Hasil Rekomendasi COBIT 5

No	Proses	Rekomendasi
1	APO13	<p>Pusat Data dan Informasi harus memaksimalkan implementasi sistem keamanan manajemen informasi untuk membenarkan keamanan sistem dijaga dengan baik. Pusat Data dan Informasi memastikan bahwa segala sesuatu yang terkait dengan keamanan informasi didokumentasikan serta dipantau untuk dievaluasi lalu digunakan sebagai tolak ukur perbaikan untuk mengurangi risiko TI.</p>
2	DSS05	<p>Pusat Data dan Informasi harus memiliki program audit internal keamanan yang bertujuan untuk memeriksa dan mengevaluasi apakah peningkatan tindakan dan kebijakan keamanan informasi sudah tepat atau belum. Pusat Data dan Informasi harus meninjau ulang mengenai pelatihan tentang serangan keamanan informasi serta melakukan tes penetrasi untuk memastikan perlindungan dari serangan keamanan.</p>

**LAMPIRAN D**  
**KUESIONER**

Keterangan Level Kuisisioner  
**PROCESS CAPABILITY LEVEL**

Level 0 : Proses tidak lengkap.

Level 1 : Proses dilakukan.

Level 2 : Proses terkelola.

Level 3 : Proses ditetapkan.

Level 4 : Proses yang dapat diprediksi.

Level 5 : Optimasi proses.

A : Proses tidak dilakukan atau tidak mencapai tujuan.

B : Proses berjalan Universitas telah melakukan tujuannya, namun misi tersebut belum berhasil.

C : Proses dilaksanakan menggunakan manajemen proses (rencana, memantauan, dan penilaian) untuk memastikan bahwa produk kerja dari proses dijalankan, dikendalikan, dan dikelola dengan benar.

D : Proses telah ditetapkan untuk mencapai tujuan.

E : Proses telah beroperasi melalui batasan untuk memastikan bahwa tujuan telah terpenuhi.

F : Proses terus meningkatkan pemenuhan tujuan Universitas di masa depan.

Kuesioner tingkat kapabilitas ini dirancang untuk menentukan kemampuan manajemen keamanan, dalam keadaan saat ini dan keadaan yang diharapkan, serta mengidentifikasi prioritas untuk perbaikan. Survei disusun dengan format pilihan ganda dan pertanyaan. Pertanyaan tersebut dikelompokkan berdasarkan subdomain proses, dan setiap pertanyaan memiliki dua jawaban, satu untuk kondisi saat ini dan satu lagi untuk kondisi yang diharapkan. Setiap pertanyaan memiliki enam kemungkinan jawaban yang menyatakan kemampuan proses dalam manajemen keamanan. Setiap opsi terdiri dari pilihan a sampai f, dengan mewakili tingkat kemampuan a=0, b=1, c=2, d=3, e=4, f=5.

Jawaban responden dapat menentukan nilai dan tingkat kemampuan. Rekapitulasi jawaban diambil sebagai ekspresi dari keadaan yang diberikan, yang menunjukkan keadaan saat ini atau keadaan yang diharapkan. Tanda menandai (√) ruang yang tersedia, ini terkait dengan proses kemampuan spesifik dari proses manajemen data. Pengisian kuesioner untuk mendapati kondisi saat ini dan kondisi yang diharapkan, kemudian dianalisis lebih lanjut untuk dilakukan dan dapat menjadi dasar untuk menentukan solusi desain untuk peningkatan proses manajemen konfigurasi.

### **Pengelolaan Keamanan – APO13**

APO13 adalah proses pendefinisian, pengoperasian SMKI.

#### **Tujuan Proses:**

Membatasi dampak insiden keamanan pada tingkat risiko yang dapat diterima Universitas.

#### **Mengerjakan dan merawat SMKI**

APO13.01 memberikan pendekatan yang terstandarisasi, formal, dan berkelanjutan serta menyediakan (SMKI) serta proses bisnis yang selaras dengan kebutuhan keamanan dan Universitas.

No	Pertanyaan	Saat ini						Yang diharapkan						
		a	b	c	d	e	f	a	b	c	d	e	f	
1	Apakah penetapan capaian dan batasan dari SMKI sesuai dengan prosedur dari Universitas?													
2	Bagaimana pelibatan secara rinci dari tingkat pengesahan untuk setiap perbedaan pada capaian SMKI?													
3	Bagaimana pembentukan SMKI yang terkoordinasi prosedur Universitas?													
4	Bagaimana tingkat penyesuaian SMKI dengan prosedur tata kelola keamanan Universitas?													
5	Bagaimana tingkat kekuasaan pihak yang mengatur dan mengimplementasikan SMKI?													
6	Bagaimana persediaan dan penjagaan dokumen yang menjelaskan mengenai capaian SMKI?													
7	Bagaimana penetapan dan penjelasan fungsi dari SMKI?													

No	Pertanyaan	Saat ini						Yang diharapkan						
		a	b	c	d	e	f	a	b	c	d	e	f	
8	Bagaimana hubungan prosedur SMKI dalam Universitas?													



### Memastikan dan menyusun rencana pengelolaan risiko SMKI

APO13.02 digunakan untuk pengelolaan rencana SMKI yang mengartikan terkelola dengan strategi serta infrastruktur Universitas.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	b	c	d	e	f
1	Bagaimana mendeskripsikan dan penjagaan mengenai rencana menanggulangi risiko keamanan yang sesuai dengan misi Universitas?												
2	Bagaimana memilih rencana mengenai penyelesaian risiko keamanan yang cocok dan maksimal sesuai kemampuan yang sudah ditetapkan?												
3	Bagaiman penjagaan dan penyimpanan dari pengelolaan mengenai risiko keamanan?												
4	Bagaimana saran untuk mengimplementasikan rencana penyelesaian risiko keamanan yang didukung dengan pengamatan dari peran dan kewajiban?												
5	Bagaimana perancangan prosedur untuk memberi saran untuk penyusunan dan peningkatan implementasi solusi penyelesaian risiko keamanan?												
6	Bagaimana penetapan kinerja dari hasil perhitungan?												
7	Bagaimana referensi mengenai pelatihan keamanan?												
8	Bagaimana menggabungkan implementasi dan pengamatan dari aturan keamanan yang mampu untuk mencegah dan menangani insiden yang tidak diinginkan?												

### Memeriksa dan memantau SMKI

APO13.03 digunakan untuk pengelolaan berulang, hubungan dan manfaat kebutuhan menggabungkan pemeriksaan data kinerja dari SMKI.

No	Pertanyaan	Saat ini						Yang diharapkan						
		a	b	c	d	e	f	a	b	c	d	e	f	
1	Bagaimana melaksanakan evaluasi kinerja dari SMKI yang menyesuaikan dan mengawasi aktifitas prosedur keamanan?													
2	Bagaimana memperhitungkan hasil audit insiden keamanan dari pihak yang bersangkutan?													
3	Bagaimana penyediaan terkait audit internal SMKI yang sudah dijadwalkan?													
4	Bagaimana melaksanakan pemantauan tata kelola SMKI berulang untuk menentukan pencapaiannya tetap sesuai dengan proses SMKI yang teridentifikasi?													
5	Bagaimana perancangan pengarahannya rencana keamanan atas penemuan dari proses pengamatan?													
6	Bagaimana melaksanakan pendataan dari proses dan kejadian yang dapat berakibat pada kinerja dari sistem keamanan manajemen informasi?													

### **Pengelolaan Layanan Keamanan – DSS05**

DSS05 adalah Proses pengolahan informasi dan hak akses untuk melaksanakan pemantauan dari ancaman keamanan.

Tujuan Proses:

Untuk mengurangi kelemahan keamanan pada Universitas.

### **Melindungi dari Serangan**

DSS05.01 digunakan untuk menyelidiki, mencegah, dan memperbaiki TI dari insiden keamanan seperti, bug, worm, spyware dan lain-lain.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	B	c	d	e	f
1	Bagaimana informasi pemahaman mengenai serangan keamanan?												
2	Bagaimana pihak yang bertanggung jawab melakukan prosedur pencegahan serangan keamanan?												
3	Bagaimana melaksanakan penjagaan alat-alat mengenai serangan keamanan yang terus diperbaiki?												
4	Bagaimana teknologi keamanan dikirimkan secara terhimpun?												
5	Bagaimana melaksanakan hasil mengenai insiden keamanan modern?												
6	Bagaimana menjaga informasi dari pembersihan data?												
7	Sejauh mana pelatihan yang dilakukan mengenai serangan keamanan?												
8	Sejauh mana melaporkan kepada <i>user</i> agar tidak memasang aplikasi yang tidak dikenal oleh Universitas?												

### Pengelolaan konektivitas jaringan

Subdomain DSS05.02 digunakan untuk tindakan serta proses administratif mengenai penjagaan informasi seluruh hubungan.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	B	c	d	e	f
1	Sejauh mana peraturan keamanan koneksi mempertimbangkan evaluasi ancaman?												
2	Bagaimana cakupan hak yang mengenai teknologi yang membuka data Universitas?												
3	Bagaimana menentukan teknologi yang dijaga oleh <i>password</i> Universitas?												
4	Sejauh mana prosedur pembersihan jaringan untuk menata data masuk keluar Universitas?												
5	Sejauh mana data dienkripsi selama mengirim informasi tersembunyi?												
6	Bagaimana pelaksanaan aturan konektivitas yang diterima Universitas?												
7	Sejauh mana pengarahan konfigurasi mengenai pelaksanaan keamanan?												
8	Sejauh mana penyusunan sistem untuk membantu transfer dan perolehan data?												
9	Sejauh mana melaksanakan tes penetrasi untuk menentukan penjagaan terhadap jaringan Universitas?												
10	Sejauh mana melaksanakan penjagaan tes sistem keamanan Universitas agar berfungsi?												

### Pengelolaan perangkat

Subdomain DSS05.03 proses menentukan teknologi (seperti komputer, desktop, dan lain-lain) dilindungi oleh kualifikasi keamanan untuk memproses, menyimpan, serta mengirimkan data.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	b	c	d	e	f
1	Sejauh mana menentukan perangkat akan digunakan untuk memenuhi penunjang keamanan?												
2	Bagaimana melaksanakan prosedur penjagaan akses teknologi yang diimplementasikan?												
3	Sejauh mana melaksanakan enkripsi data di area pengolahan tersembunyi?												
4	Sejauhmana mengelola pengaruh fasilitas perangkat Universitas?												
5	Bagaimana manajemen konfigurasi mematuhi penunjang keamanan?												
6	Bagaimana pelaksanaan pemfilteran jaringan ke seluruh teknologi yang dipergunakan?												
7	Sejauh mana menentukan seluruh perangkat ( <i>hardware</i> , <i>software</i> , dan data) yang wajib untuk dijalankan sistem yang sudah dilindungi?												
8	Sejauh mana memberikan penjagaan teknologi yang digunakan? (misalnya, melindungi terhadap kehilangan).												
9	Srjauh mana mencegah informasi dan akses yang sensitif disimpan di perangkat Universitas yang dijual atau sudah tidak digunakan lagi?												

### **Pengelolaan identitas dan fasilitas jangka panjang**

Subdomain DSS05.04 digunakan untuk menentukan seluruh pemakai teknologi mempunyai hak yang diperlukan.

No	Pertanyaan	Saat ini						Yang diharapkan						
		a	b	c	d	e	f	a	b	C	d	e	f	
1	Bagaimana mengelola hak pemakai teknologi berlandaskan tujuan dan kualifikasi prosedur?													
2	Sejauh mana menyesuaikan hak pengguna untuk menangkap intruksi kewajiban berlandaskan ketentuan?													
3	Bagaimana pemberian proses data berlandaskan tujuan fungsionalnya?													
4	Sejauh mana melaksanakan sinkronisasi semua peran diidentifikasi?													
5	Sejauh mana melakukan pemberian informasi terhadap pihak lain untuk memberikan hak pemakai teknologi?													
6	Bagaimana ruang lingkup seluruh pertukaran hak pengguna?													
7	Bagaimana melakukan pengarahan terhadap seluruh pengguna?													

### **Pengelolaan fasilitas pada perangkat TI**

DSS05.05 digunakan untuk melakukan implementasi proses untuk memberi, membatasi, serta mencabut hak pengguna. Semua persyaratan berlaku untuk semua pihak.

No	Pertanyaan	Saat ini						Yang diharapkan						
		a	b	c	d	e	f	a	B	c	d	e	f	
1	Bagaimana proses permintaan serta pemberian akses fasilitas TI yang berjalan?													
2	Bagaimana menjaga agar dokumentasi akses tetap mutakhir berdasarkan fungsi kerja serta kewajiban pekerjaannya?													
3	Bagaimana cakupan penyusunan dan pemantauan seluruh kanal dalam sarana teknologi?													
4	Sejauh mana fasilitas teknologi dengan kerentanan tinggi terlindungi?													
5	Bagaimana melaksanakan pembelajaran terhadap pemahaman keamanan teknologi yang dilakukan terstruktur?													

### **Pengelolaan data kerentanan dan instrument keluaran**

Subdomain DSS05.06 digunakan untuk menyediakan keamanan fisik, aktivitas pelaporan, dan pencatatan administrasi peralatan teknologi misalnya, surat, atau kode keamanan.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	b	c	D	e	f
1	Sejauh mana prosedur untuk mengontrol penerimaan, pelaksanaan, penghapusan informasi tertentu?												
2	Sejauh mana pelaksanaan untuk mengakses data rentan dan instrument keluaran minimal menyetarakan akibat kualitas Universitas?												
3	Bagaimana manufaktur yang terlibat terutama dalam menyimpan data dan instrument keluaran dalam melaksanakan audit?												
4	Sejauh mana area penyimpanan informasi khusus dan perangkat sensitif dilindungi?												
5	Bagaimana menghilangkan dokumen kerentanan yang tidak digunakan lagi?												



### Mengamati prasarana terkait keamanan

DSS05.07 digunakan untuk mendeteksi insiden, memantau prasarana, mencegah hak aspek tidak valid serta menentukan seluruh kejadian terpadu ke dalam pemantauan inti dan proses manajemen.

No	Pertanyaan	Saat ini						Yang diharapkan					
		a	b	c	d	e	f	a	b	c	d	e	f
1	Sejauh mana aktifitas pemantauan mencatat laporan insiden keamanan dan menentukan sejauh mana data tersimpan berlandaskan akibat peninjauan?												
2	Bagaimana memproses insiden kerentanan yang disimpan untuk mendukung penyelidikan?												
3	Sejauh mana menentukan karakter kejadian kerentanan untuk diidentifikasi dampak dan dikelola dengan tepat?												
4	Sejauh mana tinjauan keamanan yang dilakukan untuk mengidentifikasi insiden yang tidak diinginkan?												
5	Bagaimana pengaturan proses untuk dokumentasi yang dipertahankan agar memastikan bahwa semua staf mengetahui persyaratan atau kebutuhan prosedur keamanan?												
6	Sejauh mana insiden keamanan dicatat ketika proses pemantauan mengidentifikasi insiden keamanan yang mungkin akan berdampak lebih jauh?												