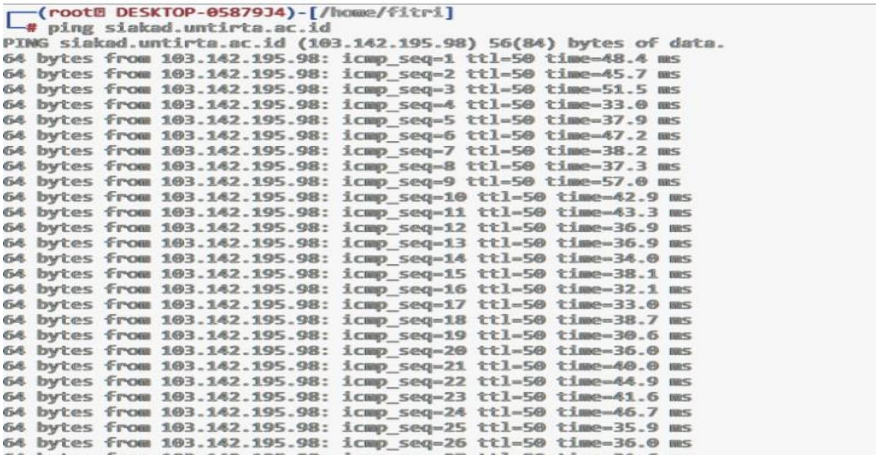
LAMPIRAN A

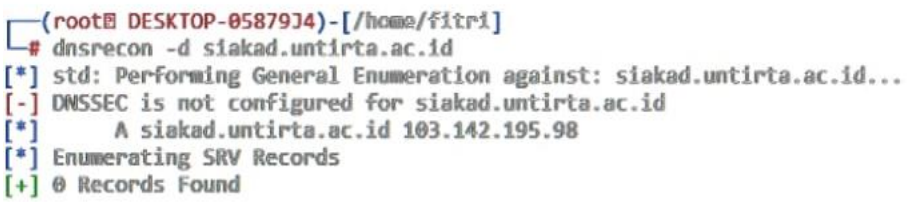
PENETRATION TESTING

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



Lampiran A-2 Hasil Pengujian Menggunakan *Tools* whois

Lampiran A-3 Hasil Pengujian Menggunakan *Tools DNSrecon*



Lampiran A-4 Hasil Pengujian Menggunakan *Tools* whatweb

```
┌──(root㉿ DESKTOP-0587QJ4)-[/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[1.1
0.3]
ERROR Opening: http://sia.untirta.ac.id/portal/ - no address for sia.untirta.ac.id
```

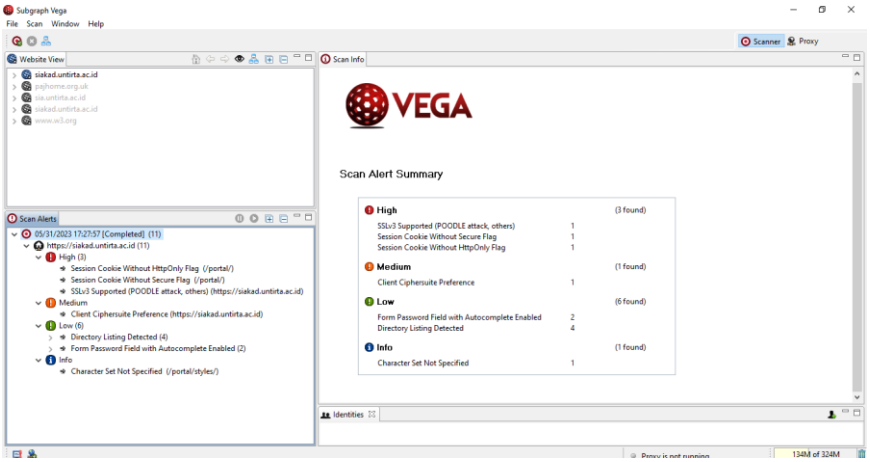
Lampiran A-5 Hasil Pengujian Menggunakan *Tools* sslscan

```
root@DESKTOP-0587QJ4: /home/fitri
┌──(root㉿ DESKTOP-0587QJ4)-[/home/fitri]
└─# sslscan siakad.untirta.ac.id
Version: 2.0.16-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:
TLSv1.2 not vulnerable to 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
```

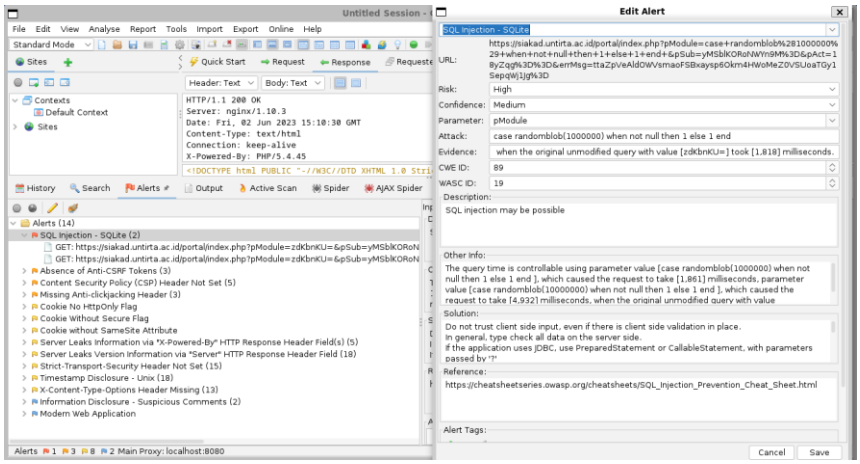
Lampiran A-6 Hasil Pengujian Menggunakan *Tools* Nmap

```
┌──(root㉿ DESKTOP-0587QJ4)-[/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

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	Bussiness Executives	Bussiness 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	Bussiness Continuity Manager	Privacy Officer
APO13-1		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C C	
APO13-2		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
APO13-3					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

Lampiran B-2 Raci chart DSS05

DSS05 RACI CHART																										
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Bussiness Executives	Bussiness 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	Bussiness Continuity Manager	Privacy Officer
DSS5-1						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS5-2						I					C	A				C	C	C	I	R	R		I	R		
DSS5-3						I					C	A				C	C	C	I	R	R		I	R		
DSS5-4						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS5-5						I					C	A				C	C	C	I	C	R		I	R	I	
DSS5-6											I					C	C	A			R					
DSS5-7				I		C					I	A				C	C	C	I	C	R		I	R	I	I

LAMPIRAN C

HASIL REKOMENDASI

Lampiran C-1 Hasil Rekomendasi *Vulnerability Assessment*

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

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

Lampiran C-2 Hasil Rekomendasi COBIT 5

No	Proses	Rekomendasi
1	APO13	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.
2	DSS05	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.

LAMPIRAN D

KUESIONER

Keterangan Level Kuisioner

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 berjalanUniversitas 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. Pengisisan 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	Bagaiman pelibatan secara rinci dari tingkat pengesahan untuk setiap pembedaan 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 persedian 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 diingikan?												

Memeriksa dan memantau SMKI

APO13.03 digunakan untuk pengelolaan berulang, hubungan dan maanfaat 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 pengarahan 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 *user* 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 *password* 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 (*hardware*, *software*, 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 sinkronsasi semua peran didentifikasi?												
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?												