UTM UNIVERSITI TEKNOLOGI MALAYSIA | Unit Audit Dalam

Kerana Tuhan Untuk Manusia

Sesi Perkongsian Ilmu Zon Selatan

PELAKSANAAN AUDIT ICT UADUTM

oleh Kamarudin Osman

2130.A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts.


PS 8.1

KERAJAAN MALAYSIA

Pelaksanaan Audit Dalam Di Kementerian Atau Jabatan Persekutuan Dan Kerajaan Negeri

4.2 Bidang tugas Unit Audit Dalam adalah untuk:

i. mengkaji kebolehpercayaan dan keberkesanan sistem kewangan serta kawalan dalaman organisasi;

ii. mengkaji tahap pematuhan kepada segala dasar, undang-undang, peraturan dan arahan yang berkuat kuasa;

iii. mengkaji aktiviti organisasi diuruskan secara berhemat, cekap dan berkesan;

iv. mengkaji aset dan kepentingan organisasi dilindungi dari segi kehilangan, penipuan dan penyelewengan;

v. memberi nasihat/pandangan mengenai kawalan dalaman terhadap semua sistem termasuk sistem ICT;


KERAJAAN MALAYSIA

SURAT PEKELILING AM BILANGAN 5 TAHUN 2024

GARIS PANDUAN MENGENAI PENGURUSAN DAN TATAKELOLA BADAN BERKANUN PERSEKUTUAN

(iv) menilai sistem ICT sedia ada untuk memastikan ia telah diuruskan dengan teratur selaras dengan dasar dan peraturan serta diuruskan dengan berhemat, cekap dan berkesan;

Kenapa ?

Agenda Strategik UA

- Digital Transformation, Governance & Compliance
- Digital Lifestyle

TINDAKAN UAD

GUEST AUDITOR

- 1 - 5 Oktober 2023

- Latihan 1 hari (semua staf UAD)
- Liputan & prestasi wifi (kolej kediaman)
- Pusat data - server
- Sistem (MyAIMS - Kewangan Pelajar)

UTHM
Universiti Tun Hussein Onn Malaysia

OJT
ISMS AUDIT

- 1 Nov - 5 Dis 2023

- Latihan 2 hari (3 orang staf UAD)
- Pematuhan ISO 27001
- Perkhidmatan Rangkaian
- Perkhidmatan Pusat Data
- Pembangunan Aplikasi & Penyelenggaraan
- Perkhidmatan Multimedia

UNIVERSITY OF MALAYA

- Governan ICT + WiFi + Pusat Data + MyAIMS
- Pengurusan Perolehan Aset ICT
- Ujian ke atas MyAIMS (Perunding Dalaman)

Akan dilaksanakan

- DRC UTM
- Pematuhan ANSI 942 (Pusat Data)

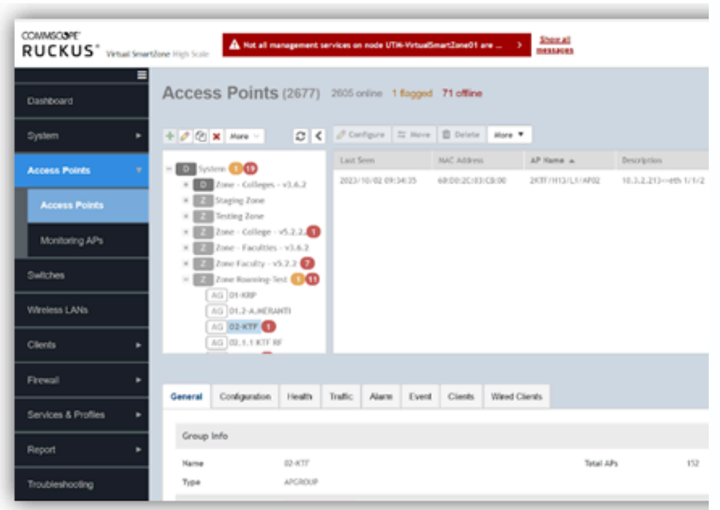
PEMERHATIAN AUDIT

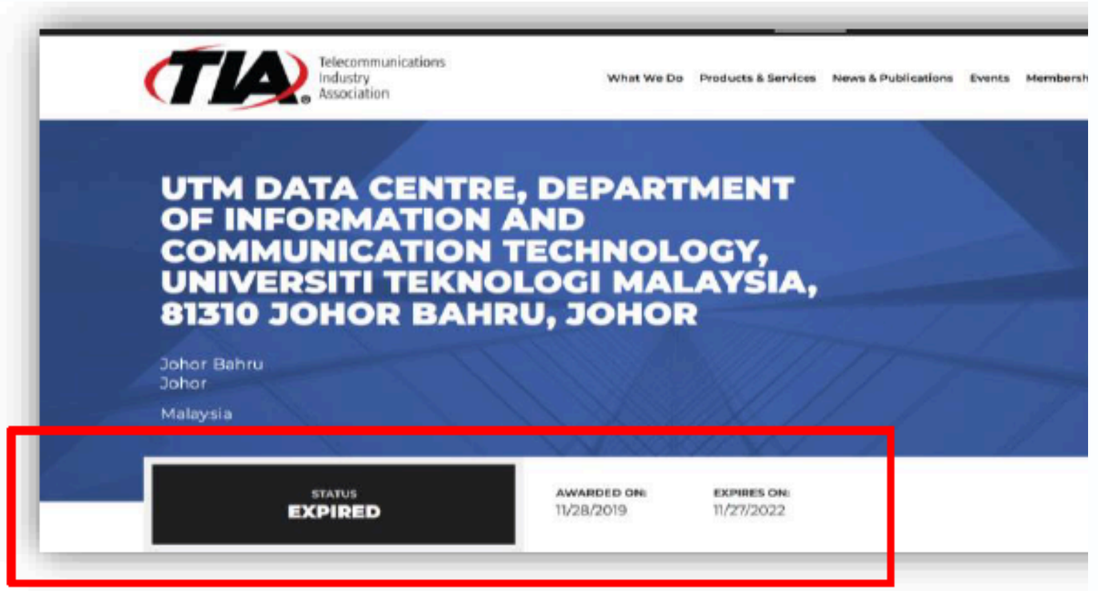
- 71 AP berstatus offline semasa lawatan tapak
- Beberapa lokasi di Kolej, liputan dan kelajuan WiFi tidak memuaskan (lap top dan hp) tetapi masih lebih tinggi yang ditetapkan DePAN2.0.
- Pengiktirafan TIA-942, Rated 3 Pusat Data telah tamat tempoh hampir 1 tahun
- 53 Server OS telah EOL, 50 akan EOL akhir Okt 2023
- Tempoh akses secara VPN kontraktor melebihi keperluan sebenar
- Sistem MyAIMS masih mempunyai CR (change request) dan SL (suggestion list), telah digunakan dalam pendaftaran pelajar baru sesi 2023/2024.
- Modul laporan masih belum berfungsi sepenuhnya.

Fasa 3
2021-2025

Minimum 10Gbps capaian internet *(streaming of Full HD videos, tele-presence).*

2.5Mbps/pelajar dan 100% liputan.



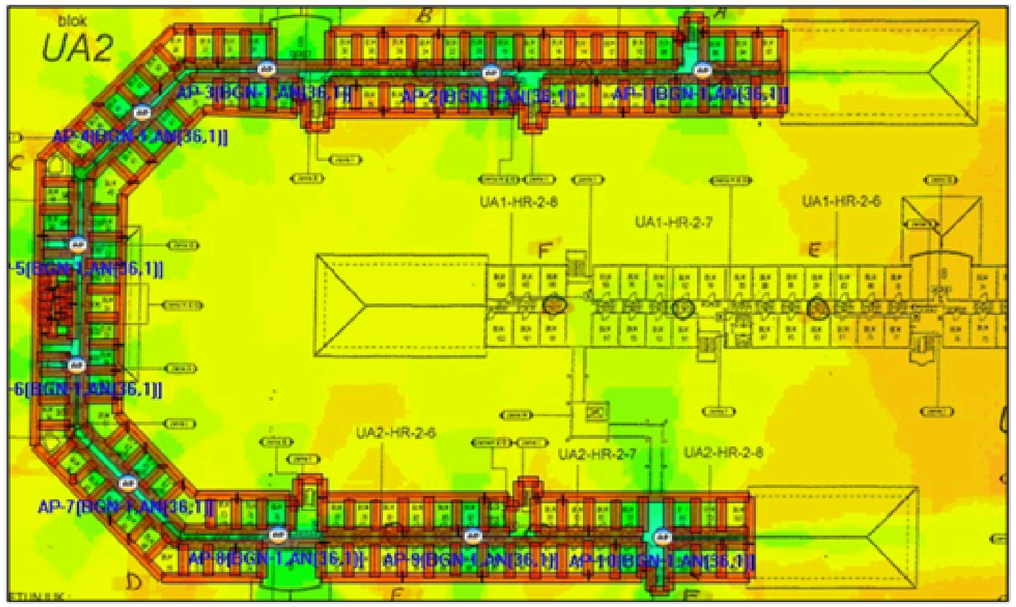


PENENTUAN LOKASI AP

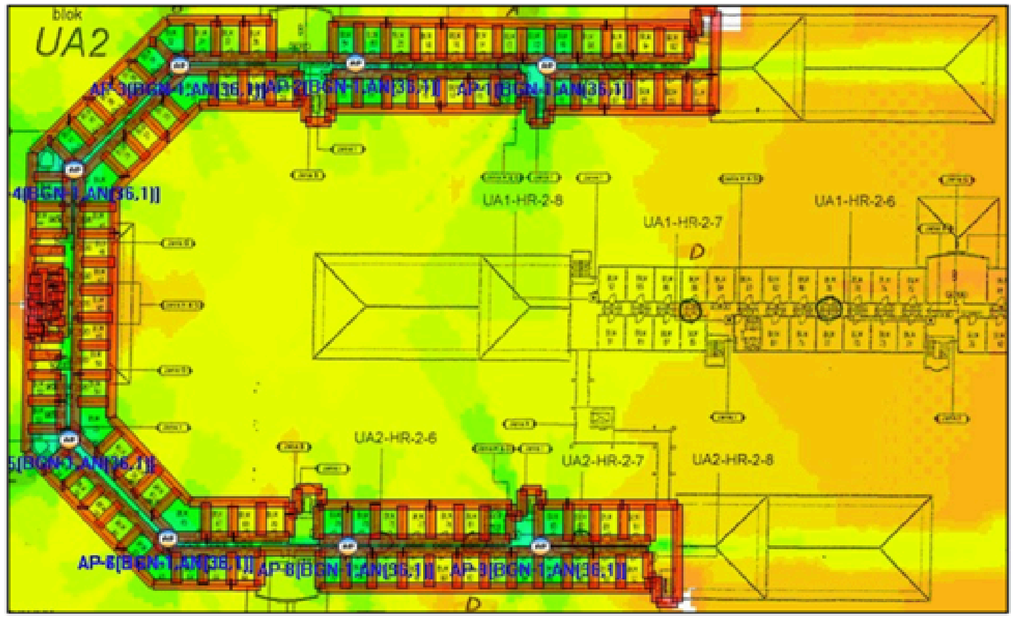
Laporan coverage heat map

- -30 dBm to -50 dBm: Excellent signal.
- -50 dBm to -60 dBm: Good signal.
- -60 dBm to -70 dBm: Fair signal.
- -70 dBm to -80 dBm: Weak signal.
- -80 dBm to -90 dBm: Very weak signal, possibly no connection.

KOLEJ 10 – BLOK UA2 – ARAS 2

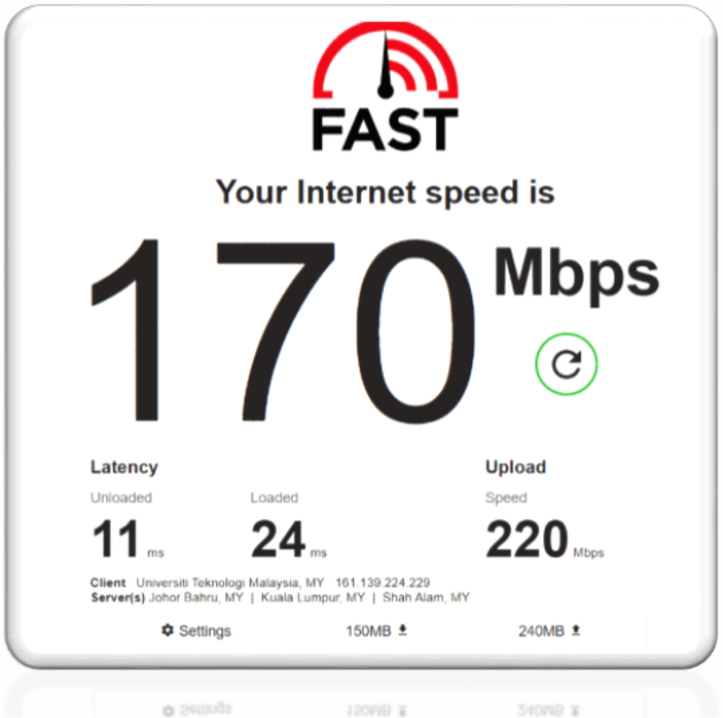


2. **KOLEJ 10 – BLOK UA2 – ARAS 3**

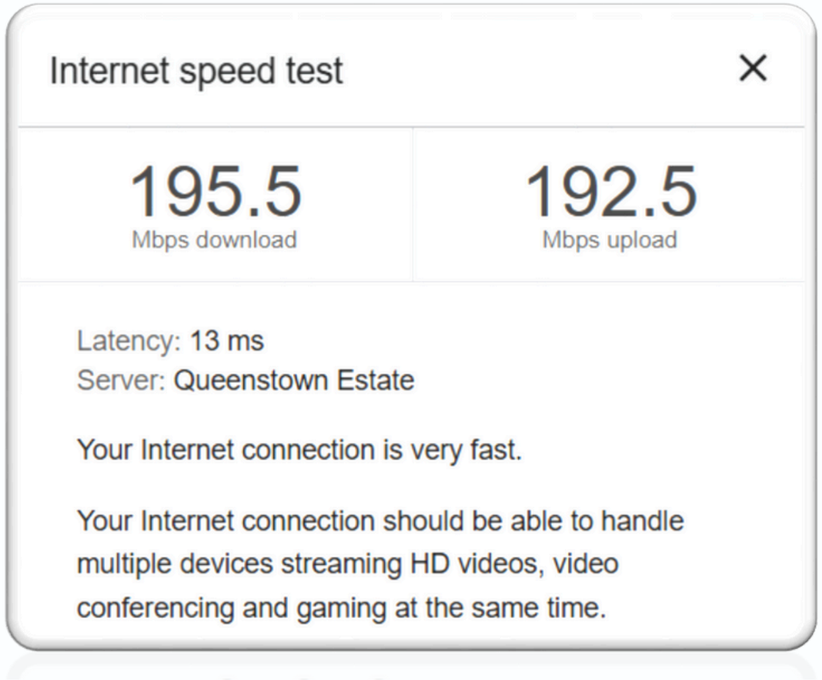


- **Jom Test Kelajuan WiFi di Dewan Banquet**

FAST.COM



GOOGLE SPEED TEST



- bergantung kepada spesifikasi perkakasan yang digunakan

PEMERHATIAN AUDIT

UJIAN KE ATAS MYAIMS - PERUNDING DALAMAN

Production server

Mengukur prestasi sistem dalam pelbagai keadaan penggunaan melalui:

1. **Load Test** – uji masa pemuatan halaman ketika bilangan pengguna normal atau puncak.
2. **Stress Test** – uji keupayaan maksimum sistem menampung pengguna hingga gagal.
3. **Spike Test** – uji reaksi sistem terhadap kenaikan pengguna secara mendadak.
4. **Extended Period Test** – uji kestabilan prestasi sistem untuk jangka masa panjang.

Penemuan Penting

Jenis Ujian	Pengguna	Apdex	Prestasi Sistem	Purata Response Time
Normal Load	Bendahari	0.932	Sangat Baik	0.56 saat
	PTJ	0.072	Sangat Lemah	56.64 saat
Peak Load	Bendahari	0.801	Baik	0.99 saat
	PTJ	0.015	Lemah + Banyak gagal	3.41 minit
Spike Load	Bendahari	0.749	Sederhana	1.17 saat
	PTJ	0.361	Lemah	50.93 saat
Extended Period Normal Load	Bendahari	0.953	Stabil	0.41 saat
	PTJ	0.019	Lemah	1.02 minit
Stress Load (uji tahap maks)	Bendahari	0.02	Mula gagal pada 536 user	48.24 saat (hingga 3.64 minit)
	PTJ	0.02	Gagal pada 545 user	3.05 minit (hingga 9.38 minit)

PEMERHATIAN AUDIT

Penarafan Ujian keselamatan

Jadual 4. Panduan Penarafan Risiko Common Vulnerability Scoring System (CVSS) 3.1.

Taraf Risiko	Penjelasan
Kritikal	Kelemahan bertaraf kritikal adalah kelemahan yang memperoleh skor CVSS 9.0 – 1.0. Kelemahan yang memperoleh status kritikal perlu diambil perhatian dan diperbaiki serta-merta kerana kelemahan ini dapat dieksploitasi dengan amat mudah dan akan mendedahkan maklumat sulit.
Tinggi	Kelemahan bertaraf tinggi adalah kelemahan yang memperoleh skor CVSS 7.0 – 7.9. Kelemahan berstatus tinggi perlu diambil perhatian dan diperbaiki serta merta kerana ia mudah dieksploitasi dan akan mendedahkan maklumat sulit.
Sederhana	Kelemahan bertaraf sederhana adalah kelemahan yang memperoleh skor CVSS 4.0 – 6.9. Kelemahan bertaraf sederhana perlu diambil perhatian kerana kelemahan ini adalah kelemahan yang serius dan akan mendedahkan maklumat sulit.
Rendah	Kelemahan bertaraf rendah adalah kelemahan yang memperoleh skor CVSS 0.1 – 3.9. Kelemahan bertaraf rendah adalah akibat daripada percanggahan amalan baik keselamatan sistem maklumat dan tidak mengancam keselamatan dan integriti maklumat secara serta merta.
Info	Kelemahan yang bertaraf info adalah percanggahan amalan baik keselamatan sistem maklumat yang bertujuan untuk memberi cadangan penambahbaikan. Kelemahan yang bertaraf info tidak mempunyai skor CVSS.

Skop ujian ke atas MyAIMS

- Ujian fungsian (Input - Proses - Output)
- Ujian bukan fungsian (Load Test, Stress Test)
- Ujian Keselamatan

Penarafan pemerhatian oleh Pasukan Perunding Dalaman

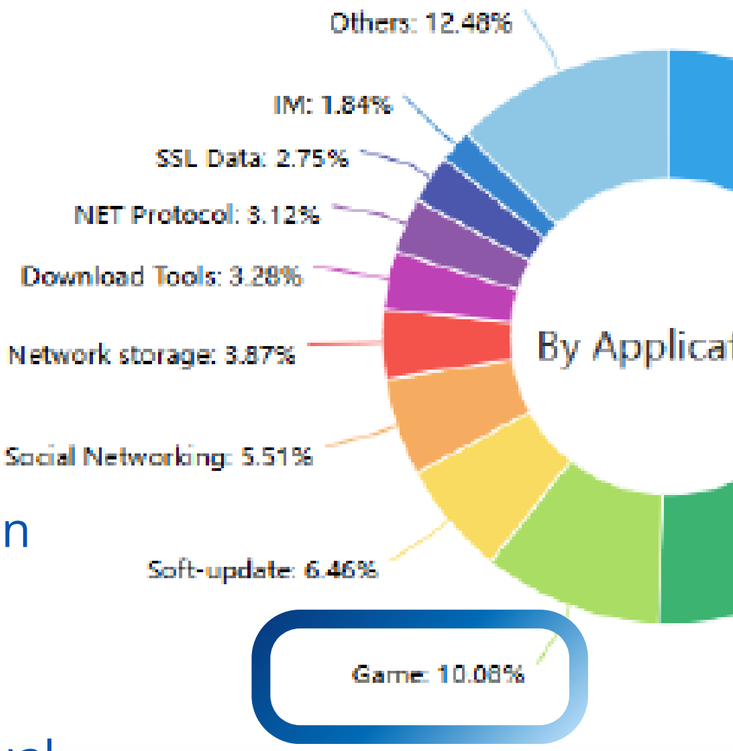
- Penilaian ke atas pemerhatian
- Semakin tinggi penarafan - semakin kritikal

PEMERHATIAN AUDIT

ASET ICT

- Risiko operasi PTJ - 58 berpunca daripada ICT dan 55 daripada aset & fasiliti (tidak diambil kira oleh UTMD)
- Polisi dan prosedur masih peringkat draf (lebih 1 tahun)
- Lebih 65% perkakasan ICT berusia lebih 10 tahun

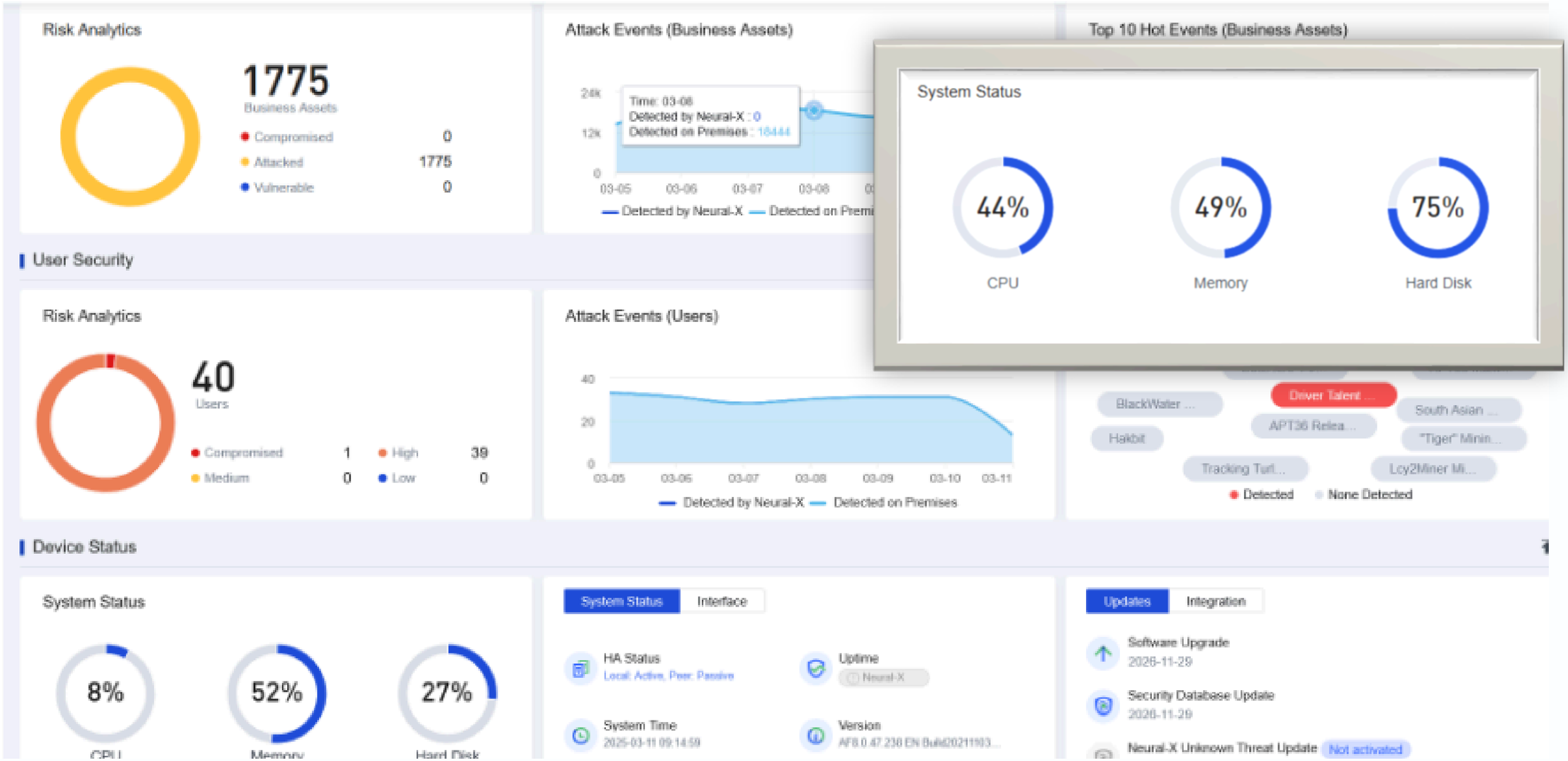
Analisis Trafik Internet

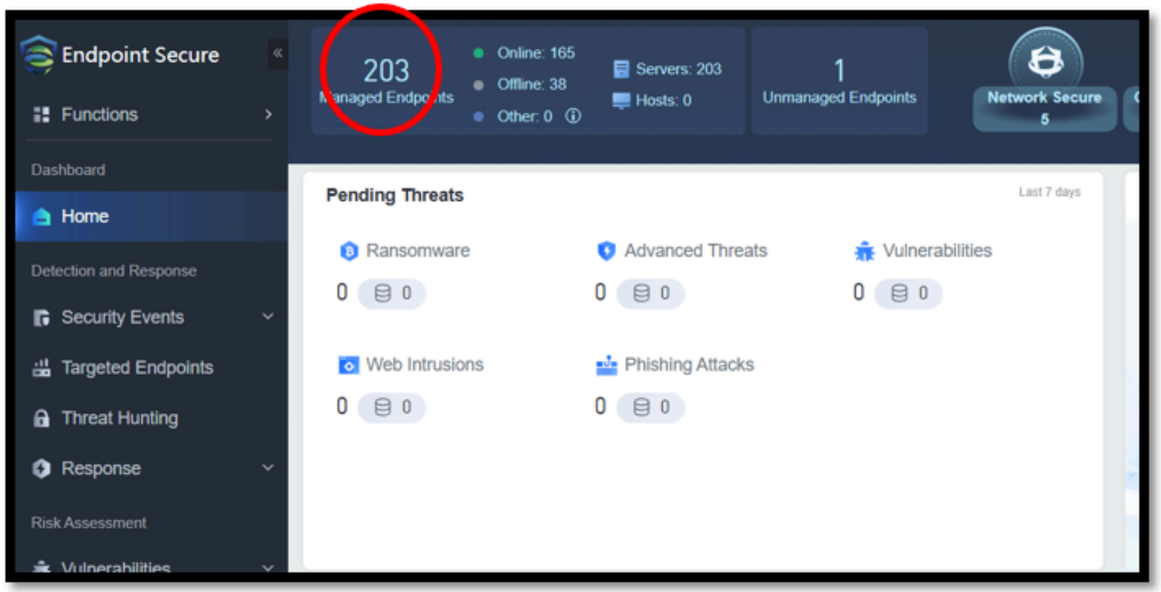


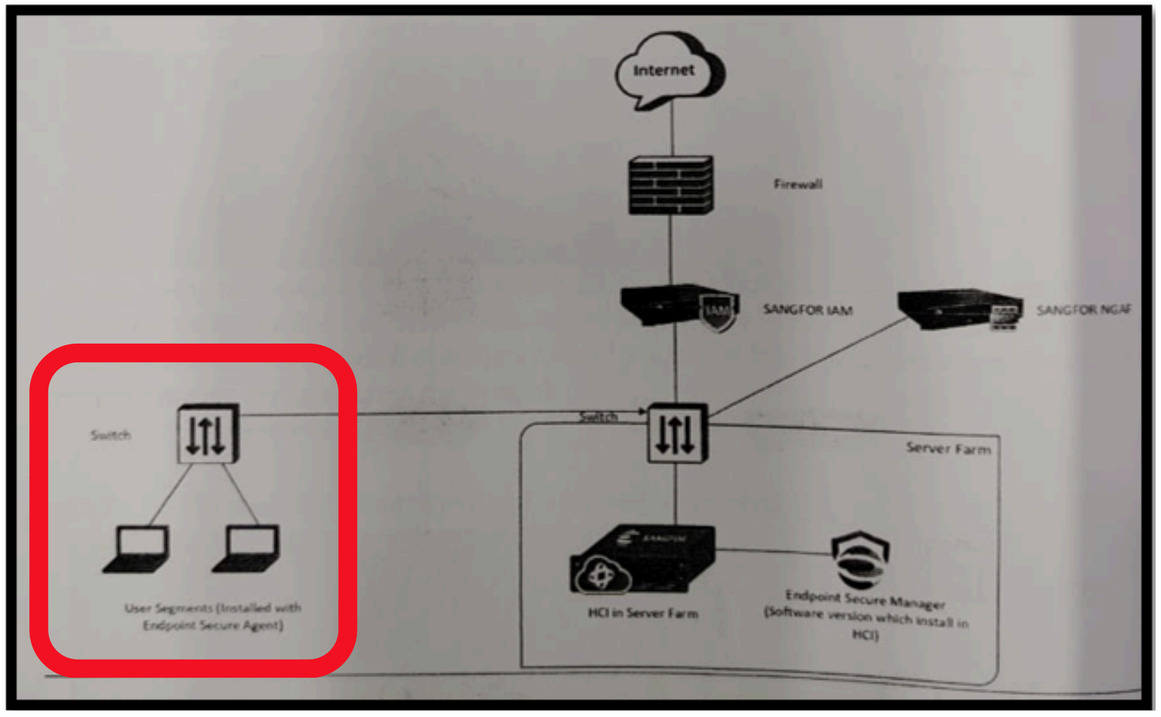
SISTEM KESELAMATAN - SANGFOR

- Sistem keselamatan EDR tidak digunakan sepenuhnya (203 / 400) diaktifkan
- EDR hanya ke peringat Server (tidak sama seperti carta topologi)
- Penyelenggaraan dan pengujian ke atas sistem keselamatan tidak ikut jadual
- Pembayaran dibuat sebelum perkhidmatan disempurnakan

Dashboard Keselamatan Rangkaian





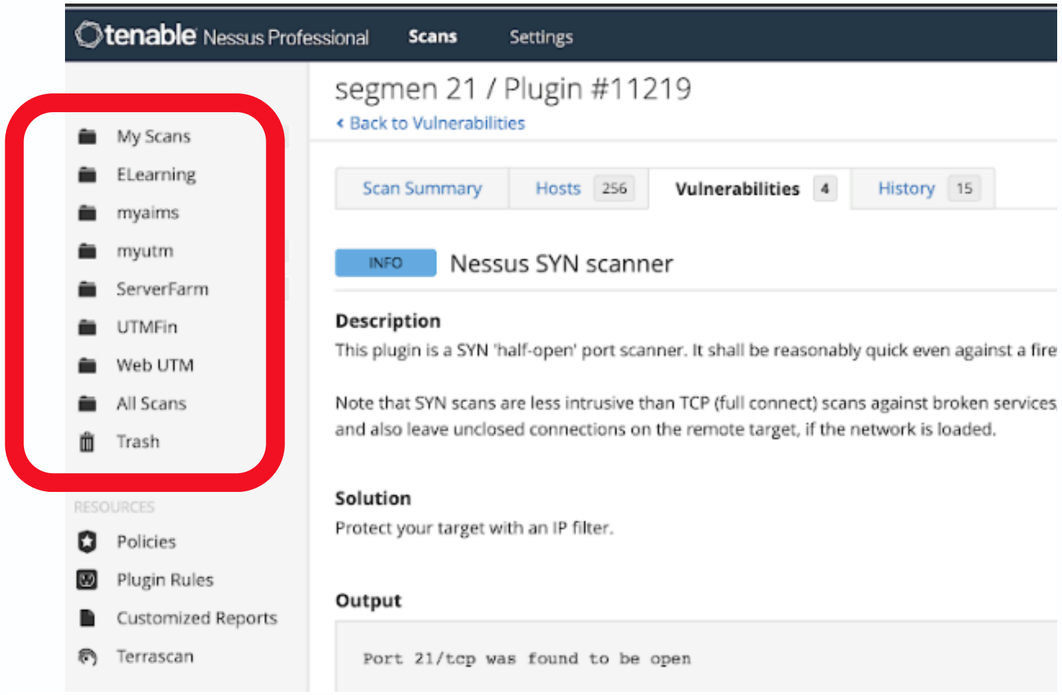


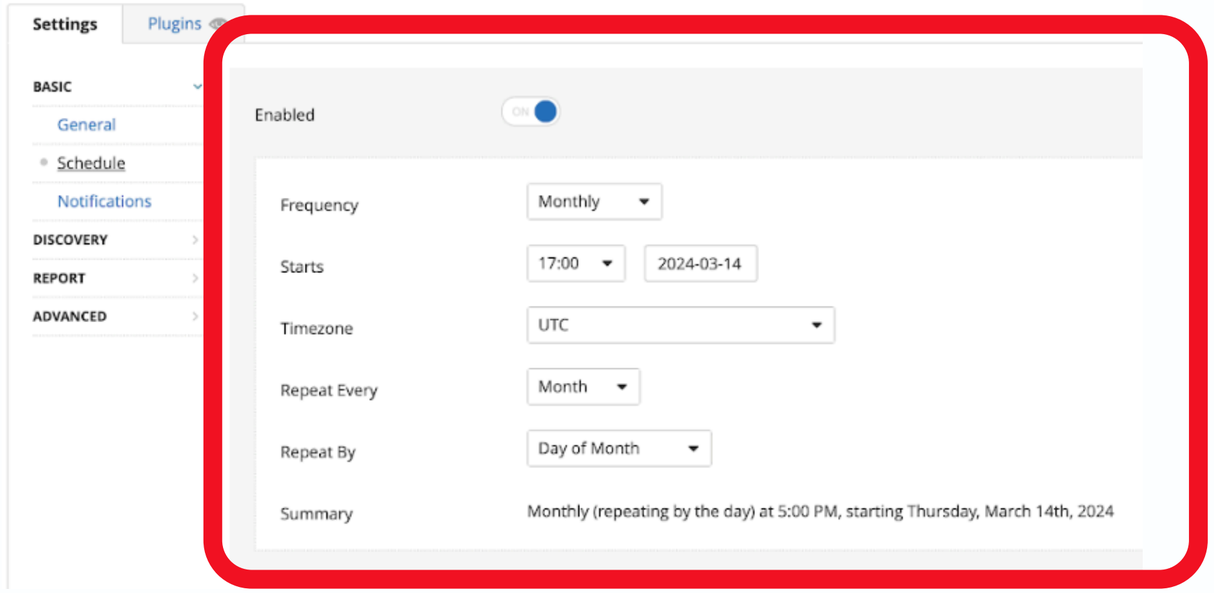
SPESIFIKASI AM

Successful bidder shall provide UTM with related quarterly on-site maintenance services which the Bidder shall execute the related activities:

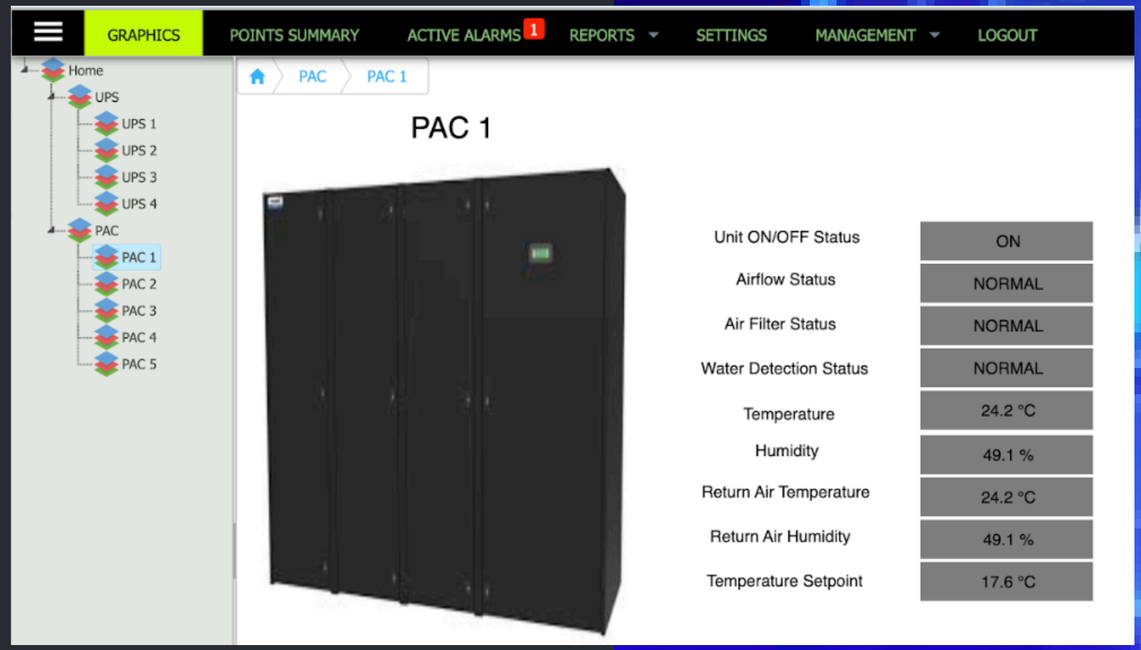
a. Security management audit and health checking.
b. User's accounts audit and health checking.
c. Having problem(s) escalation procedures in review.
e. Administrative logs information review.
f. Interoperability systems & application suggestions and review.
g. Management logs and review.
h. Improvement the process and procedure escalation review.
i. Physical health condition & checking.

- **Dokumen kontrak**
- **Controller / Dashboard**
- **Senarai System Keselematan = Aset Universiti**


tenable Nessus Professional
Scans
Settings
My Scans
ELearning
myaims
myutm
ServerFarm
UTMFin
Web UTM
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
segmen 21 / Plugin #11219
Back to Vulnerabilities
Scan Summary
Hosts 256
Vulnerabilities 4
History 15
INFO
Nessus SYN scanner
Description
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a fire
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services and also leave unclosed connections on the remote target, if the network is loaded.
Solution
Protect your target with an IP filter.
Output
Port 21/tcp was found to be open


Settings
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
REPORT
ADVANCED
Enabled
Frequency
Monthly
Starts
17:00
2024-03-14
Timezone
UTC
Repeat Every
Month
Repeat By
Day of Month
Summary
Monthly (repeating by the day) at 5:00 PM, starting Thursday, March 14th, 2024


10:51
5G
Ekova - UTM Skudai
13 members
Charge Remaining : 48.7%)
10:31
February 7
EkovaSystem
(ekoSYSTEM Alert) (UTM Skudai)Health Check at 2025/02/07 09:00:00
09:00
February 8
EkovaSystem
(ekoSYSTEM Alert) (UTM Skudai)Health Check at 2025/02/08 09:00:00
09:00
EkovaSystem
(ekoSYSTEM ALARM-ACK) (UTM Skudai) (UPS 2 - Estimated Charge Remaining:99.8 %) at 2025/02/08 11:42:17 (ekova : (1) Comment:UPS charge - normal:EN AKAMAL)
11:42


GRAPHICS
POINTS SUMMARY
ACTIVE ALARMS 1
REPORTS
SETTINGS
MANAGEMENT
LOGOUT
Home
UPS
UPS 1
UPS 2
UPS 3
UPS 4
PAC
PAC 1
PAC 2
PAC 3
PAC 4
PAC 5
PAC
PAC 1
PAC 1
Unit ON/OFF Status
ON
Airflow Status
NORMAL
Air Filter Status
NORMAL
Water Detection Status
NORMAL
Temperature
24.2 °C
Humidity
49.1 %
Return Air Temperature
24.2 °C
Return Air Humidity
49.1 %
Temperature Setpoint
17.6 °C

PENDEKATAN AUDIT ICT

Prestasi

- Governan
- Pembangunan / Perubahan Sistem
- Pengurusan Aset / Perkakasan
- Pengurusan DRC.

Pematuhan

- UTMFin (Sistem Kewangan) - SAGA
- Pusat Data - ANSI 942, Rated 3
- Kawalan - ISMS 27001

Pemantauan berterusan

- Prestasi perkhidmatan ICT
- Keselamatan ICT

	AUDIT UNIVERSE	SKOP AUDIT UNIVERSE
1	**Governan ICT**	1.1 Strategik (Std 6) 1.2 Pengurusan risiko (Std 8.2 & 8.3) 1.3 Kewangan (Std 7.1) 1.4 Polisi & prosedur (5.1) 1.5 Struktur, pihak berkuasa ICT (5.2,5.3,5.4) 1.6 Perkhidmatan pelanggan / pihak berkepentingan (6.1.4, Std 4.2)
2	**Operasi & Keselamatan - insiden & ancaman - A.16**	2.1 Prosedur pegendalian insiden keselamatan 2.2 Pemantauan aktiviti / log / ancaman A.12.4 2.3 Pasukan CERT UTMD 2.4 Sistem dalam production - scanning / VA A.12.6 2.5 Pemantauan aktiviti akses istemewa (privilege access) A9.2 2.6 Pemantauan prestasi, ketersediaan, keupayaan perkakasan dan aplikasi
3	**Aset ICT A.8. A.11**	3.1 Daftar aset / inventori (Kew.PA) A.8.1, A8.3 3.2 Daftar aset ICT dalam sistem / tools (Ruckus - perkakasan rangkaian dsb) 3.3 Kawalan fizikal aset A.11.1, A.11.2 3.4 Kawalan hak akses (staf dan vendor) 3.5 Klasifikasi maklumat yang terdapat dalam aset ICT (server / sistem) A.8.2
4	**Pembangunan / perubahan aplikasi A.14**	4.1 Perancangan (keperluan spesifikasi aplikasi, kelulusan) 4.2 Elemen kawalan (jejak audit, auto logoff, kaedah encryption) 4.3 Dokumentasi (akses matrik, diagram sistem, rekabentuk sistem dan rangkaian) 4.4 Web based (privacy & disclaimer statment, katalaluan, kriptografi) 4.5 Perubahan sistem (kelulusan, semakan/ujian teknikal) 4.6 Ujian keselamatan - Pen test, vulnerable assessment - sebelum production
5	**Pengurusan pusat data**	5.1 Pengurusan server (pengasingan fungsi, OS, akses matriks, penyelenggaraan) 5.2 Pengurusan back up 5.3 Kawalan & keselamatan Fizikal 5.4 Pemantauan operasi (kapasiti dan ketersediaan)
6	**Rangkaian ICT (wifi dan wired)**	6.1 Topology rangkaian (kemasini, diluluskan, selari dengan strategik ICT) 6.2 Kawalan akses pengguna (staf, pelajar, orang luar) 6.3 Pemantauan prestasi (availability) 6.4 Kawalan akses perkakasan & tools rangkaian (akses matriks- pentadbir, user) 6.5 Kawalan akses secara VPN dan bypass
7	**Pelan Kesinambungan operasi / perkhidmatan (PKO) - A.17**	7.1 Polisi / prosedur / strategi dan tadbir urus PKO 7.2 Analisis risiko 7.3 Pengurusan DRC (i.e rangkaian, pangakalan data, aplikasi, komunikasi) 7.4 Simulasi PKO dan laporan
8	**Pengkomputeran awan**	8.1 Polisi pengkomputeran awan & perolehan CSP 8.2 Analisis risiko keselamatan 8.3 Pengurusan maklumat terperingkat 8.4 Kontrak dan terma keselamatan 8.5 Pelindungan data dan maklumat 8.6 Kesinambungan perkhidmatan , kebolehsediaan & sandaran data

Kerana Tuhan Untuk Manusia

“Ya Allah, bimbinglah kami supaya sentiasa bekerja dengan ikhlas, dan berilah rahmat kejayaan ke atas usaha kami, moga ianya dapat membantu perjalanan kami meningkatkan ketaatan kepadaMU ”

TERIMA KASIH