UINSSC
UNIVERSITAS ISLAM NEGERI SIBER
SYEKH NURJATI CIREBON

AKREDITASI UNGGUL

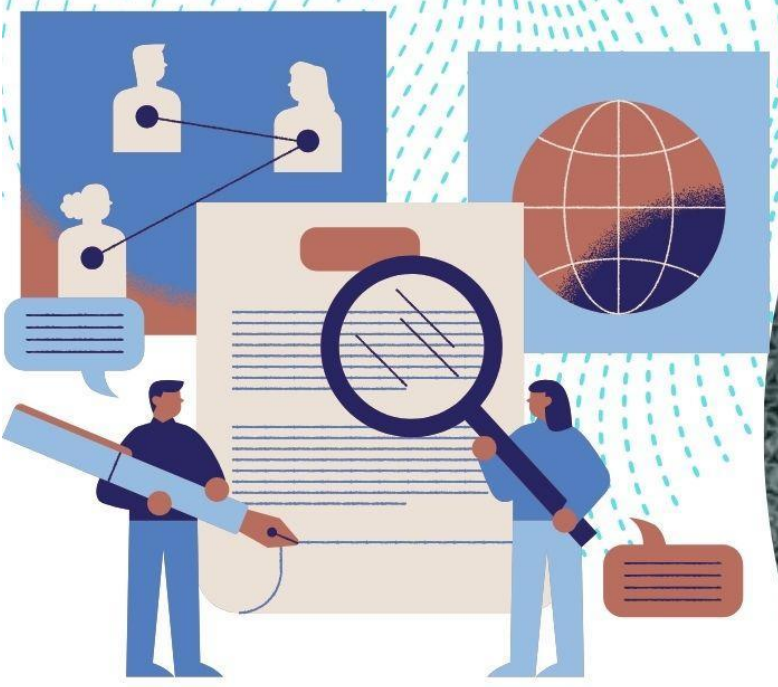
BLU SPEED

CYBER ISLAMIC UNIVERSITY

PUSTIKOM
UIN SIBER SYEKH NURJATI CIREBON

ANALISIS SWOT

IT Master Plan UIN Siber Syekh Nurjati Cirebon



pustikom.uinssc.ac.id

LEMBAR PENGESAHAN

DOKUMEN ANALISIS SWOT IT MASTER PLAN UIN SIBER SYEKH NURJATI CIREBON PELAKSANA UPT TIK TAHUN 2026

Dokumen DOKUMEN ANALISIS SWOT IT MASTER PLAN UIN SIBER SYEKH NURJATI CIREBON ini telah diperiksa, disetujui, dan ditetapkan untuk digunakan sebagai acuan dalam pelaksanaan Sistem Manajemen Mutu di lingkungan UPT TIK Universitas Islam Negeri Siber Syekh Nurjati Cirebon.

Cirebon, 24 Februari 2026

Jabatan	Nama/TTD	Tanda Tangan
Penyusun	Tim UPT TIK	
Kepala UPT TIK	Riyanto, S.T. M.Kom.	
Wakil Rektor II	Prof. Dr. Ilman Nafia, M.Ag.	
Rektor	Prof. Dr. Aan Jaelani, M.Ag.	

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar Belakang

Transformasi digital dalam dunia pendidikan tinggi terus mengalami percepatan seiring dengan perkembangan teknologi informasi dan komunikasi. Tahun 2026 menjadi fase krusial dalam perjalanan implementasi IT Master Plan, di mana institusi tidak lagi hanya berfokus pada pembangunan fondasi teknologi, tetapi mulai memasuki tahap integrasi, optimalisasi, dan inovasi layanan berbasis digital. Perubahan ini menuntut kesiapan yang lebih matang, baik dari sisi infrastruktur, sistem, maupun sumber daya manusia.

Pada tahun sebelumnya, berbagai upaya telah dilakukan untuk membangun infrastruktur dasar, mengembangkan sistem informasi, serta meningkatkan kapasitas SDM. Namun demikian, hasil evaluasi menunjukkan bahwa masih terdapat sejumlah tantangan, seperti belum optimalnya integrasi antar sistem, keterbatasan dokumentasi, serta perlunya peningkatan standar keamanan informasi. Oleh karena itu, tahun 2026 diarahkan sebagai fase akselerasi untuk menutup kesenjangan tersebut sekaligus meningkatkan kualitas layanan secara menyeluruh.

Perkembangan teknologi seperti Artificial Intelligence (AI), Cloud Computing, Big Data, dan Internet of Things (IoT) memberikan peluang besar bagi institusi untuk meningkatkan efisiensi operasional dan kualitas layanan. Pemanfaatan teknologi tersebut tidak hanya mendukung proses akademik dan administratif, tetapi juga membuka peluang inovasi dalam pembelajaran digital, pengelolaan data, serta pengambilan keputusan berbasis analitik.

Di sisi lain, meningkatnya ancaman keamanan siber, tuntutan layanan digital yang cepat dan user-friendly, serta persaingan antar institusi pendidikan menjadi faktor eksternal yang perlu diantisipasi. Tanpa strategi yang tepat, institusi berisiko mengalami ketertinggalan dalam hal inovasi dan kualitas layanan.

Dengan demikian, penyusunan dokumen Analisis SWOT IT Master Plan Tahun 2026 menjadi sangat penting sebagai landasan dalam merumuskan strategi pengembangan teknologi informasi yang terarah, terukur, dan berkelanjutan. Dokumen ini diharapkan mampu memberikan gambaran menyeluruh mengenai kondisi internal dan eksternal serta menjadi acuan dalam pengambilan keputusan strategis.

1.2 Tujuan

Dokumen ini disusun dengan tujuan sebagai berikut:

1. Mengevaluasi kondisi teknologi informasi tahun sebelumnya
   Evaluasi ini dilakukan untuk mengetahui sejauh mana implementasi IT Master Plan tahun 2025 telah berjalan, termasuk capaian, kendala, dan area yang masih memerlukan perbaikan. Dengan evaluasi ini, institusi dapat memahami posisi saat ini secara objektif.
2. Mengidentifikasi kekuatan, kelemahan, peluang, dan ancaman
   Analisis SWOT dilakukan untuk memetakan faktor internal dan eksternal yang mempengaruhi pengembangan teknologi informasi. Hasil analisis ini menjadi dasar dalam menyusun strategi yang tepat dan relevan.
3. Menyusun strategi pengembangan teknologi informasi
   Berdasarkan hasil analisis, disusun strategi yang mampu mengoptimalkan kekuatan dan peluang serta meminimalkan kelemahan dan ancaman. Strategi ini diarahkan untuk mendukung transformasi digital yang berkelanjutan.
4. Mendukung pengambilan keputusan berbasis data
   Dokumen ini memberikan informasi yang komprehensif dan terstruktur sehingga dapat digunakan oleh pimpinan sebagai dasar dalam menentukan kebijakan dan arah pengembangan teknologi informasi.

1.3 Manfaat

Penyusunan dokumen ini diharapkan memberikan manfaat sebagai berikut:

1. Menjadi acuan strategis pengembangan teknologi informasi
   Dokumen ini dapat digunakan sebagai panduan dalam merencanakan, melaksanakan, dan mengevaluasi program kerja di bidang teknologi informasi.
2. Meningkatkan kualitas layanan digital
   Dengan adanya strategi yang jelas, institusi dapat meningkatkan kualitas layanan kepada pengguna, baik mahasiswa, dosen, maupun tenaga kependidikan.
3. Mendukung pengambilan keputusan yang lebih efektif
   Informasi yang tersaji dalam dokumen ini membantu pimpinan dalam mengambil keputusan yang tepat dan berbasis data.
4. Meningkatkan efisiensi dan efektivitas operasional
   Implementasi strategi yang tepat dapat membantu mengoptimalkan penggunaan sumber daya, baik dari sisi teknologi maupun SDM.
5. Memperkuat daya saing institusi
   Dengan pengelolaan teknologi informasi yang baik, institusi dapat meningkatkan daya saing di tingkat nasional maupun internasional.

BAB II

PROFIL UPT TEKNOLOGI INFORMASI DAN KOMUNIKASI

2.1 Visi dan Misi

Visi: Menjadi pusat layanan teknologi informasi yang handal, aman, inovatif, dan berdaya saing global dalam mendukung transformasi digital institusi.

Misi:

1. Mengembangkan layanan digital terintegrasi
   Menghadirkan sistem informasi yang saling terhubung (integrated system) sehingga seluruh layanan akademik dan non-akademik dapat diakses dalam satu ekosistem digital yang terpadu.
2. Menyediakan infrastruktur yang andal dan scalable
   Membangun dan mengelola infrastruktur TI yang stabil, memiliki tingkat ketersediaan tinggi (high availability), serta mampu berkembang sesuai kebutuhan institusi.
3. Meningkatkan kapasitas dan kompetensi SDM TI
   Melakukan pelatihan, sertifikasi, dan pengembangan kompetensi SDM agar mampu mengikuti perkembangan teknologi terbaru seperti cloud, AI, dan cybersecurity.
4. Mendukung transformasi digital layanan institusi
   Mengubah proses bisnis konvensional menjadi layanan berbasis digital yang efisien, transparan, dan mudah diakses.

2.2 Ruang Lingkup

1. Pengelolaan Data dan Informasi
   Bertanggung jawab terhadap pengumpulan, pengolahan, penyimpanan, dan distribusi data secara terpusat guna mendukung pengambilan keputusan berbasis data.
2. Infrastruktur Teknologi Informasi
   Meliputi pengelolaan jaringan, server, data center, serta perangkat pendukung lainnya untuk memastikan operasional sistem berjalan optimal.
3. Pengembangan Sistem dan Aplikasi
   Merancang, membangun, dan memelihara aplikasi yang digunakan dalam kegiatan akademik dan administrasi.
4. Layanan Pengguna (Helpdesk)
   Memberikan dukungan teknis kepada pengguna dalam menyelesaikan permasalahan terkait penggunaan sistem dan teknologi.
5. Keamanan Informasi
   Menjamin kerahasiaan, integritas, dan ketersediaan data melalui penerapan kebijakan dan teknologi keamanan informasi.

2.3 Peran dan Fungsi

1. Penyedia Infrastruktur TI
   Menyediakan sarana dan prasarana teknologi informasi yang menjadi fondasi utama operasional digital institusi.
2. Pengembang Sistem Informasi
   Mengembangkan aplikasi dan sistem yang mendukung proses bisnis institusi secara menyeluruh.
3. Pengelola Keamanan Informasi
   Melindungi data dan sistem dari ancaman siber melalui penerapan standar keamanan dan kontrol akses.
4. Pusat Layanan Digital
   Menjadi pusat pelayanan teknologi bagi seluruh civitas akademika, termasuk mahasiswa, dosen, dan tenaga kependidikan.
5. Motor Penggerak Transformasi Digital
   Berperan sebagai leading sector dalam mendorong inovasi dan digitalisasi di lingkungan institusi.

BAB III

ANALISIS SWOT

Tabel Analisis SWOT

Strengths (Kekuatan)	**Weaknesses (Kelemahan)**
Infrastruktur jaringan kampus sudah berbasis fiber optic dan memiliki redundansi	Belum adanya implementasi Single Sign-On (SSO) secara menyeluruh
Data center internal sudah tersedia dan mulai terstandarisasi	Integrasi API antar sistem masih terbatas
Sebagian sistem sudah berbasis web dan terpusat	Belum menerapkan arsitektur microservices
Dukungan pimpinan terhadap digitalisasi sangat kuat	Proses deployment belum menggunakan DevOps secara optimal
SDM TI memiliki kemampuan dasar pengembangan aplikasi	Dokumentasi teknis masih kurang lengkap
Sudah memiliki beberapa sistem inti (SIAKAD, LMS, dll)	Monitoring sistem belum real-time dan terintegrasi
Tersedia jaringan internet kampus yang memadai	Belum ada SOC (Security Operation Center)
Mulai mengarah ke penggunaan cloud hybrid	Backup dan disaster recovery belum optimal

Opportunities (Peluang)	**Threats (Ancaman)**
Adopsi teknologi AI untuk layanan akademik	Serangan siber seperti ransomware dan phishing
Implementasi cloud computing untuk efisiensi	Kebocoran data akibat kelemahan sistem
Integrasi big data untuk pengambilan keputusan	Perubahan teknologi yang cepat
Dukungan pemerintah terhadap digitalisasi kampus	Keterbatasan SDM TI profesional
Kolaborasi dengan startup dan industri teknologi	Vendor lock-in
Pengembangan smart campus	Downtime sistem kritikal
Tren e-learning dan hybrid learning	Ketergantungan pada konektivitas internet
Standarisasi keamanan (ISO 27001)	Ancaman insider (human error)

Narasi SWOT (Mendalam)

Strengths (Kekuatan)

Kekuatan utama institusi terletak pada infrastruktur teknologi informasi yang sudah mulai matang dan terstandarisasi. Penggunaan jaringan berbasis fiber optic dengan dukungan redundansi memberikan kestabilan konektivitas yang sangat penting dalam menunjang layanan digital. Selain itu, keberadaan data center internal memungkinkan pengelolaan sistem yang lebih terkontrol serta memberikan fleksibilitas dalam pengembangan layanan ke depan.

Dari sisi organisasi, dukungan pimpinan terhadap transformasi digital menjadi faktor kunci yang mempercepat implementasi berbagai inisiatif TI. Hal ini didukung oleh ketersediaan sistem inti seperti SIAKAD dan LMS yang sudah berjalan, serta SDM TI yang memiliki kemampuan dasar dalam pengembangan aplikasi. Kombinasi antara dukungan kebijakan dan kesiapan teknis ini menjadi fondasi kuat untuk pengembangan sistem yang lebih kompleks.

Namun demikian, kekuatan ini perlu terus ditingkatkan melalui modernisasi teknologi, seperti penerapan cloud hybrid dan peningkatan kualitas layanan berbasis data. Dengan memanfaatkan kekuatan yang ada, institusi memiliki peluang besar untuk mempercepat transformasi digital secara menyeluruh.

Weaknesses (Kelemahan)

Kelemahan utama terletak pada aspek integrasi sistem yang belum optimal. Belum adanya implementasi Single Sign-On (SSO) menyebabkan pengguna harus melakukan login berulang pada berbagai sistem, yang berdampak pada pengalaman pengguna yang kurang efisien. Selain itu, keterbatasan integrasi API membuat pertukaran data antar sistem belum berjalan secara real-time.

Dari sisi pengembangan, belum diterapkannya arsitektur modern seperti microservices dan praktik DevOps menyebabkan proses deployment dan pengelolaan aplikasi menjadi kurang efisien. Dokumentasi teknis yang belum lengkap juga menjadi kendala dalam proses pengembangan dan pemeliharaan sistem, terutama ketika terjadi pergantian personel.

Selain itu, aspek keamanan dan monitoring masih perlu ditingkatkan. Belum adanya Security Operation Center (SOC) serta sistem monitoring yang terintegrasi menyebabkan potensi gangguan tidak dapat terdeteksi secara dini. Hal ini menunjukkan perlunya peningkatan dalam tata kelola TI dan penerapan standar operasional yang lebih baik.

Opportunities (Peluang)

Perkembangan teknologi digital memberikan peluang besar bagi institusi untuk meningkatkan kualitas layanan. Adopsi teknologi seperti Artificial Intelligence (AI), Big Data, dan Cloud Computing memungkinkan pengolahan data yang lebih

canggih serta peningkatan efisiensi operasional. Hal ini dapat dimanfaatkan untuk mendukung pengambilan keputusan berbasis data dan meningkatkan pengalaman pengguna.

Selain itu, dukungan pemerintah terhadap digitalisasi pendidikan serta peluang kolaborasi dengan industri teknologi membuka ruang bagi institusi untuk mengembangkan inovasi baru. Implementasi konsep smart campus juga menjadi peluang strategis untuk meningkatkan daya saing institusi di tingkat nasional maupun internasional.

Dengan memanfaatkan peluang ini secara optimal, institusi dapat mempercepat transformasi digital serta menciptakan layanan yang lebih adaptif terhadap kebutuhan pengguna.

Threats (Ancaman)

Ancaman utama yang dihadapi adalah meningkatnya risiko keamanan siber, seperti serangan ransomware, phishing, dan kebocoran data. Tanpa sistem keamanan yang memadai, institusi berisiko mengalami gangguan operasional serta kerugian reputasi.

Selain itu, perkembangan teknologi yang sangat cepat menuntut institusi untuk terus beradaptasi. Keterbatasan SDM TI profesional serta potensi vendor lock-in menjadi tantangan tersendiri dalam pengelolaan teknologi informasi.

Faktor lain seperti downtime sistem kritikal dan ketergantungan terhadap konektivitas internet juga dapat mempengaruhi kualitas layanan. Oleh karena itu, diperlukan strategi mitigasi risiko yang komprehensif untuk menghadapi berbagai ancaman tersebut.

Matriks Strategi SWOT

Strategi SO	**Strategi WO**
Mengembangkan smart campus berbasis AI dan Big Data	Implementasi SSO dan integrasi API
Optimalisasi cloud hybrid untuk efisiensi	Penerapan DevOps dan microservices
Penguatan layanan digital berbasis data	Peningkatan dokumentasi sistem

Strategi ST	**Strategi WT**
Implementasi keamanan berstandar ISO 27001	Penguatan disaster recovery system

Strategi ST	Strategi WT
Peningkatan monitoring dan sistem alert	Pelatihan SDM TI secara berkelanjutan
Penguatan infrastruktur jaringan	Pengurangan ketergantungan vendor

Roadmap Implementasi

No	Program	Aksi	KPI	Target
1	Integrasi Sistem	Implementasi SSO	1 sistem SSO aktif	2026
2	Integrasi Sistem	Pengembangan API gateway	80% sistem terintegrasi	2026
3	Infrastruktur	Upgrade server dan storage	Uptime 99%	2026
4	Keamanan	Implementasi SOC	Monitoring 24/7	2026
5	SDM	Pelatihan DevOps dan Cloud	70% staf tersertifikasi	2026

Opportunities (Peluang)	Threats (Ancaman)
Perkembangan teknologi AI, Cloud, dan Big Data	Ancaman keamanan siber (hacking, ransomware, phishing)
Dukungan kebijakan pemerintah terhadap digitalisasi	Perubahan teknologi yang sangat cepat
Peluang kolaborasi dengan institusi lain dan industri	Keterbatasan anggaran pengembangan TI
Tuntutan layanan digital yang tinggi dari pengguna	Ketergantungan vendor (vendor lock-in)
Potensi pengembangan smart campus	Risiko downtime layanan kritikal

Opportunities	Threats
AI dan Cloud	Ancaman siber
Kolaborasi	Perubahan teknologi cepat
Dukungan pemerintah	Keterbatasan anggaran

3.1 Strengths (Kekuatan)

UPT TIK memiliki fondasi yang semakin kuat dengan infrastruktur teknologi yang mulai stabil dan mampu mendukung operasional layanan digital secara lebih konsisten. Stabilitas ini mencerminkan keberhasilan fase awal pembangunan sistem

yang dilakukan pada tahun sebelumnya, sehingga pada tahun 2026 institusi dapat lebih fokus pada peningkatan kualitas layanan dan integrasi sistem.

Selain itu, dukungan manajemen yang kuat serta adanya roadmap pengembangan TI yang jelas menjadi faktor pendorong utama keberhasilan transformasi digital. Peningkatan kapasitas SDM melalui pelatihan dan sertifikasi juga menjadi kekuatan penting dalam menghadapi tantangan teknologi yang semakin kompleks.

3.2 Weaknesses (Kelemahan)

Meskipun mengalami perkembangan, integrasi sistem masih belum sepenuhnya optimal dan sebagian layanan masih berjalan secara terpisah. Hal ini berdampak pada efisiensi operasional serta kualitas layanan yang belum maksimal.

Selain itu, dokumentasi sistem dan standar pengembangan aplikasi masih perlu ditingkatkan agar mendukung keberlanjutan sistem. Ketergantungan pada vendor eksternal juga menjadi tantangan, terutama dalam pengelolaan sistem kritikal yang membutuhkan kemandirian teknologi.

3.3 Opportunities (Peluang)

Perkembangan teknologi seperti Artificial Intelligence, Cloud Computing, dan Big Data memberikan peluang besar untuk meningkatkan kualitas layanan dan efisiensi operasional. Teknologi ini dapat dimanfaatkan untuk mengembangkan sistem yang lebih cerdas, adaptif, dan berbasis data.

Selain itu, adanya dukungan pemerintah serta peluang kolaborasi dengan berbagai pihak membuka kesempatan untuk mempercepat transformasi digital. Kolaborasi ini dapat berupa pengembangan sistem, peningkatan kapasitas SDM, maupun penelitian dan inovasi teknologi.

3.4 Threats (Ancaman)

Ancaman keamanan siber menjadi salah satu tantangan utama yang harus dihadapi. Risiko seperti peretasan, kebocoran data, dan serangan ransomware dapat berdampak besar terhadap operasional dan reputasi institusi.

Selain itu, perkembangan teknologi yang sangat cepat serta keterbatasan anggaran dapat menjadi hambatan dalam menjaga keberlanjutan sistem. Oleh karena itu, diperlukan strategi yang adaptif dan berkelanjutan untuk menghadapi berbagai ancaman tersebut

BAB IV

STRATEGI DAN RENCANA IMPLEMENTASI

4.1 Prinsip Strategi Pengembangan TI

Pengembangan teknologi informasi tahun 2026 mengacu pada prinsip-prinsip berikut:

1. Terintegrasi
   Seluruh sistem harus saling terhubung melalui API dan arsitektur terstandar untuk menghindari duplikasi data dan meningkatkan efisiensi.
2. Berorientasi Layanan
   Sistem dikembangkan dengan fokus pada pengalaman pengguna (user experience), kemudahan akses, dan kecepatan layanan.
3. Berbasis Keamanan
   Setiap pengembangan wajib menerapkan prinsip security by design, termasuk enkripsi, kontrol akses, dan audit log.
4. Skalabilitas
   Infrastruktur dan aplikasi harus mampu berkembang sesuai kebutuhan jumlah pengguna dan data.
5. Berbasis Data
   Pengambilan keputusan harus didukung oleh data yang valid, terintegrasi, dan mudah diakses.

4.2 Program Strategis 2026

1. Integrasi Sistem Informasi
   Fokus pada implementasi SSO dan API Gateway untuk menyatukan seluruh layanan dalam satu ekosistem digital.
2. Penguatan Infrastruktur
   Melakukan upgrade server, storage, dan jaringan untuk meningkatkan performa dan keandalan sistem.
3. Peningkatan Keamanan Informasi
   Membangun SOC, menerapkan standar ISO 27001, dan melakukan audit keamanan secara berkala.
4. Pengembangan SDM TI
   Pelatihan DevOps, Cloud, Cybersecurity, serta sertifikasi profesional bagi staf TI.
5. Inovasi Layanan Digital
   Implementasi AI, dashboard analitik, dan pengembangan smart campus.

BAB V
MONITORING DAN EVALUASI

5.1 Mekanisme Monitoring

Monitoring merupakan proses penting dalam memastikan bahwa seluruh program dan kegiatan pengembangan teknologi informasi berjalan sesuai dengan rencana yang telah ditetapkan dalam IT Master Plan. Monitoring tidak hanya berfungsi sebagai alat pengawasan, tetapi juga sebagai mekanisme kontrol untuk mendeteksi permasalahan secara dini serta memastikan keberlanjutan layanan digital. Dengan sistem monitoring yang baik, institusi dapat meningkatkan keandalan sistem, efisiensi operasional, serta kualitas layanan kepada pengguna.

1. Monitoring Harian

Monitoring harian dilakukan secara real-time untuk memantau kondisi operasional sistem teknologi informasi, termasuk server, jaringan, dan aplikasi. Proses ini umumnya didukung oleh dashboard monitoring yang terintegrasi, yang menampilkan berbagai indikator kinerja seperti penggunaan CPU, memori, bandwidth jaringan, serta status layanan aplikasi. Dengan adanya monitoring harian, tim teknis dapat dengan cepat mendeteksi anomali atau gangguan yang terjadi pada sistem.

Selain itu, monitoring harian juga mencakup sistem notifikasi atau alert otomatis yang akan memberikan peringatan jika terjadi gangguan, seperti penurunan performa atau kegagalan layanan. Hal ini memungkinkan tim untuk melakukan tindakan responsif secara cepat sebelum gangguan tersebut berdampak luas terhadap pengguna. Monitoring harian menjadi fondasi utama dalam menjaga stabilitas dan ketersediaan layanan TI.

2. Monitoring Bulanan

Monitoring bulanan dilakukan untuk mengevaluasi kinerja sistem dan program secara lebih komprehensif dalam periode tertentu. Evaluasi ini mencakup analisis terhadap capaian indikator kinerja, identifikasi kendala yang dihadapi, serta efektivitas solusi yang telah diterapkan. Monitoring bulanan biasanya dilakukan melalui rapat evaluasi yang melibatkan tim TI dan pihak terkait lainnya.

Dalam proses ini, dilakukan juga analisis tren terhadap performa sistem, seperti frekuensi downtime, jumlah insiden, serta tingkat penggunaan layanan. Hasil evaluasi bulanan digunakan sebagai dasar untuk melakukan perbaikan berkelanjutan (continuous improvement), termasuk penyesuaian strategi, peningkatan kapasitas sistem, serta optimalisasi proses operasional.

3. Monitoring Tahunan

Monitoring tahunan merupakan evaluasi menyeluruh terhadap implementasi IT Master Plan dalam satu tahun berjalan. Evaluasi ini bertujuan untuk mengukur sejauh mana target strategis telah tercapai serta mengidentifikasi gap antara kondisi

aktual dengan rencana yang telah ditetapkan. Monitoring tahunan mencakup aspek teknis, operasional, serta tata kelola teknologi informasi.

Selain itu, monitoring tahunan juga digunakan sebagai dasar dalam penyusunan rencana kerja tahun berikutnya. Hasil evaluasi ini akan memberikan gambaran yang lebih luas mengenai keberhasilan program, tantangan yang dihadapi, serta peluang pengembangan ke depan. Dengan demikian, monitoring tahunan menjadi bagian penting dalam siklus perencanaan strategis TI.

5.2 Indikator Kinerja (KPI)

Indikator kinerja atau Key Performance Indicators (KPI) digunakan sebagai alat ukur untuk menilai keberhasilan implementasi program teknologi informasi. KPI yang ditetapkan harus bersifat terukur, relevan, dan selaras dengan tujuan strategis institusi. Dengan adanya KPI yang jelas, institusi dapat melakukan evaluasi secara objektif serta memastikan bahwa setiap program memberikan kontribusi nyata terhadap peningkatan layanan.

1. Uptime Sistem Minimal 99%

Uptime sistem merupakan indikator utama dalam mengukur ketersediaan layanan teknologi informasi. Target uptime minimal 99% menunjukkan bahwa sistem harus dapat diakses oleh pengguna hampir sepanjang waktu, dengan tingkat downtime yang sangat minim. Pencapaian target ini memerlukan dukungan infrastruktur yang andal, sistem monitoring yang efektif, serta mekanisme pemulihan yang cepat.

Selain itu, uptime juga berkaitan erat dengan kepercayaan pengguna terhadap layanan digital. Semakin tinggi tingkat ketersediaan sistem, maka semakin tinggi pula tingkat kepuasan pengguna. Oleh karena itu, pengelolaan uptime harus menjadi prioritas utama dalam operasional TI.

2. Tingkat Kepuasan Pengguna Minimal 85%

Kepuasan pengguna merupakan indikator penting dalam menilai kualitas layanan teknologi informasi. Pengukuran tingkat kepuasan biasanya dilakukan melalui survei yang melibatkan mahasiswa, dosen, dan tenaga kependidikan. Aspek yang dinilai meliputi kemudahan penggunaan sistem, kecepatan layanan, serta kualitas dukungan teknis.

Target minimal 85% menunjukkan bahwa sebagian besar pengguna merasa puas terhadap layanan yang diberikan. Hasil survei ini juga dapat digunakan untuk mengidentifikasi area yang perlu ditingkatkan, sehingga institusi dapat terus melakukan perbaikan dalam memberikan layanan yang lebih baik.

3. Integrasi Sistem Minimal 80%

Integrasi sistem menjadi salah satu fokus utama dalam implementasi IT Master Plan. Indikator ini mengukur sejauh mana sistem-sistem yang ada telah terhubung dan dapat saling bertukar data secara otomatis. Target minimal 80% menunjukkan bahwa sebagian besar sistem sudah berada dalam satu ekosistem digital yang terintegrasi.

Pencapaian KPI ini memerlukan penerapan teknologi seperti API, ESB, dan SSO. Dengan integrasi yang baik, institusi dapat mengurangi duplikasi data, meningkatkan efisiensi operasional, serta mendukung pengambilan keputusan berbasis data yang lebih akurat.

4. Jumlah Insiden Keamanan Menurun

Indikator ini digunakan untuk mengukur efektivitas sistem keamanan informasi yang diterapkan. Penurunan jumlah insiden keamanan menunjukkan bahwa sistem semakin aman dan mampu melindungi data dari berbagai ancaman. Insiden yang dimaksud dapat berupa percobaan akses ilegal, serangan malware, maupun kebocoran data.

Untuk mencapai target ini, diperlukan penerapan sistem keamanan yang komprehensif, termasuk monitoring keamanan secara real-time, penggunaan firewall, serta peningkatan kesadaran keamanan pengguna. Evaluasi terhadap setiap insiden juga perlu dilakukan untuk mencegah kejadian serupa di masa depan.

5. Persentase SDM Tersertifikasi Meningkat

Pengembangan sumber daya manusia merupakan faktor penting dalam keberhasilan implementasi teknologi informasi. Indikator ini mengukur jumlah staf TI yang telah memiliki sertifikasi profesional di bidang tertentu, seperti cloud computing, cybersecurity, dan DevOps.

Peningkatan jumlah SDM tersertifikasi menunjukkan bahwa institusi memiliki tenaga ahli yang kompeten dalam mengelola teknologi yang semakin kompleks. Hal ini juga berdampak pada kualitas layanan serta kemampuan institusi dalam beradaptasi dengan perkembangan teknologi.

5.3 Evaluasi dan Tindak Lanjut

Evaluasi merupakan tahap lanjutan dari proses monitoring yang bertujuan untuk menganalisis hasil pengukuran kinerja serta menentukan langkah perbaikan yang diperlukan. Evaluasi dilakukan secara sistematis dan terstruktur untuk memastikan bahwa setiap permasalahan yang ditemukan dapat ditangani dengan tepat.

1. Perbaikan Sistem yang Bermasalah

Hasil monitoring digunakan untuk mengidentifikasi sistem atau layanan yang mengalami gangguan atau tidak mencapai target kinerja. Perbaikan dilakukan melalui proses troubleshooting, peningkatan kapasitas, atau pembaruan sistem. Tindakan ini bertujuan untuk memastikan bahwa seluruh layanan dapat kembali beroperasi secara optimal.

2. Penyesuaian Strategi

Evaluasi juga digunakan untuk menilai efektivitas strategi yang telah diterapkan. Jika ditemukan bahwa strategi yang ada belum memberikan hasil yang optimal, maka perlu dilakukan penyesuaian agar lebih sesuai dengan kondisi dan kebutuhan

saat ini. Penyesuaian ini dapat mencakup perubahan prioritas program, alokasi sumber daya, maupun pendekatan teknis yang digunakan.

3. Peningkatan Kualitas Layanan

Selain perbaikan teknis, hasil evaluasi juga digunakan untuk meningkatkan kualitas layanan secara keseluruhan. Hal ini mencakup peningkatan user experience, kecepatan layanan, serta kualitas dukungan teknis. Dengan melakukan perbaikan secara berkelanjutan, institusi dapat memberikan layanan yang lebih baik dan memenuhi harapan pengguna.

BAB VI
MANAJEMEN RISIKO

6.1 Identifikasi Risiko

1. Risiko Keamanan Siber

Risiko keamanan siber merupakan salah satu ancaman paling kritikal dalam pengelolaan teknologi informasi. Dengan meningkatnya ketergantungan terhadap sistem digital, institusi menjadi target potensial berbagai jenis serangan seperti ransomware, phishing, malware, hingga serangan Distributed Denial of Service (DDoS). Serangan tersebut tidak hanya berpotensi mengganggu operasional sistem, tetapi juga dapat menyebabkan kebocoran data sensitif yang berdampak pada reputasi institusi.

Selain faktor eksternal, risiko keamanan juga dapat berasal dari kelemahan internal, seperti konfigurasi sistem yang tidak optimal, kurangnya pembaruan (patching), serta rendahnya kesadaran keamanan pengguna. Oleh karena itu, keamanan siber harus dipandang sebagai aspek strategis yang memerlukan pendekatan menyeluruh, baik dari sisi teknologi, proses, maupun sumber daya manusia.

2. Risiko Downtime Sistem

Downtime sistem merupakan kondisi di mana layanan teknologi informasi tidak dapat diakses oleh pengguna, baik sebagian maupun seluruhnya. Risiko ini dapat disebabkan oleh berbagai faktor, seperti kegagalan perangkat keras (hardware failure), gangguan jaringan, kesalahan konfigurasi, maupun beban sistem yang melebihi kapasitas.

Dampak dari downtime sangat signifikan, terutama jika terjadi pada sistem kritikal seperti SIAKAD, LMS, atau sistem keuangan. Gangguan ini dapat menghambat proses akademik, administrasi, serta menurunkan tingkat kepercayaan pengguna terhadap layanan institusi. Oleh karena itu, diperlukan sistem yang memiliki tingkat ketersediaan tinggi (high availability) serta mekanisme pemulihan yang cepat.

3. Risiko Kegagalan Integrasi

Seiring dengan implementasi IT Master Plan, integrasi antar sistem menjadi salah satu fokus utama. Namun demikian, proses integrasi memiliki risiko kegagalan yang cukup tinggi, terutama jika tidak didukung oleh standar arsitektur yang jelas. Kegagalan integrasi dapat menyebabkan data tidak sinkron, inkonsistensi informasi, serta terjadinya duplikasi data antar sistem.

Selain itu, perbedaan teknologi, struktur database, serta kurangnya standar API juga dapat menjadi kendala dalam proses integrasi. Jika tidak ditangani dengan baik, hal ini dapat menghambat terciptanya ekosistem digital yang terintegrasi dan mengurangi efektivitas pengambilan keputusan berbasis data.

4. Risiko Keterbatasan SDM

Sumber daya manusia merupakan faktor kunci dalam keberhasilan implementasi teknologi informasi. Keterbatasan SDM, baik dari sisi jumlah maupun kompetensi, dapat menjadi hambatan dalam pengembangan, pengelolaan, dan pemeliharaan sistem. Hal ini terutama terlihat dalam penguasaan teknologi baru seperti cloud computing, DevOps, cybersecurity, dan data analytics.

Selain itu, ketergantungan pada individu tertentu (key person dependency) juga menjadi risiko yang perlu diantisipasi. Jika tidak ada transfer knowledge dan dokumentasi yang memadai, maka keberlanjutan sistem dapat terganggu ketika terjadi pergantian personel. Oleh karena itu, pengembangan SDM harus menjadi prioritas utama dalam strategi TI.

5. Risiko Ketergantungan Vendor

Dalam pengelolaan teknologi informasi, penggunaan layanan atau produk dari vendor eksternal merupakan hal yang umum. Namun, ketergantungan yang tinggi terhadap vendor tertentu dapat menimbulkan risiko, seperti keterbatasan fleksibilitas, biaya yang meningkat, serta kesulitan dalam melakukan migrasi sistem.

Vendor lock-in menjadi salah satu bentuk risiko yang sering terjadi, terutama dalam penggunaan layanan cloud atau sistem berbasis proprietary. Selain itu, jika vendor mengalami gangguan layanan atau berhenti beroperasi, maka sistem institusi juga dapat terdampak. Oleh karena itu, diperlukan strategi pengelolaan vendor yang baik serta perencanaan jangka panjang untuk mengurangi ketergantungan tersebut.

6.2 Mitigasi Risiko

1. Implementasi Firewall, IDS/IPS, dan Enkripsi

Untuk mengurangi risiko keamanan siber, institusi perlu menerapkan sistem keamanan berlapis (layered security). Firewall berfungsi sebagai penghalang utama untuk menyaring lalu lintas jaringan, sedangkan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) digunakan untuk mendeteksi dan mencegah aktivitas mencurigakan secara real-time.

Selain itu, penggunaan enkripsi pada data, baik saat disimpan (data at rest) maupun saat dikirim (data in transit), menjadi langkah penting dalam menjaga kerahasiaan informasi. Implementasi kebijakan keamanan, seperti multi-factor authentication (MFA) dan audit log, juga perlu diterapkan untuk meningkatkan kontrol akses dan akuntabilitas sistem.

2. Penyediaan Backup dan Disaster Recovery Plan

Untuk mengantisipasi risiko downtime dan kehilangan data, institusi perlu memiliki mekanisme backup yang terjadwal dan sistematis. Backup data harus dilakukan secara berkala dengan penyimpanan di lokasi yang berbeda (offsite) untuk menghindari kehilangan data akibat bencana.

Selain itu, penyusunan Disaster Recovery Plan (DRP) menjadi sangat penting untuk memastikan bahwa sistem dapat dipulihkan dalam waktu yang cepat setelah terjadi

gangguan. Implementasi Disaster Recovery Center (DRC) sebagai lokasi cadangan juga dapat menjadi solusi untuk meningkatkan ketersediaan layanan dan mengurangi downtime.

3. Penggunaan Standar API

Untuk mengatasi risiko kegagalan integrasi, institusi perlu menerapkan standar API yang terstruktur dan terdokumentasi dengan baik. Penggunaan API Gateway dan Enterprise Service Bus (ESB) dapat membantu dalam mengelola komunikasi antar sistem secara lebih terpusat dan terkontrol.

Standarisasi ini mencakup format data, protokol komunikasi, serta mekanisme autentikasi. Dengan adanya standar yang jelas, proses integrasi dapat dilakukan secara lebih efisien, fleksibel, dan mudah dikembangkan di masa depan.

4. Pelatihan SDM

Mitigasi risiko keterbatasan SDM dilakukan melalui program pelatihan dan pengembangan kompetensi secara berkelanjutan. Pelatihan ini mencakup berbagai bidang, seperti cloud computing, DevOps, cybersecurity, serta pengembangan aplikasi modern.

Selain pelatihan, institusi juga perlu mendorong sertifikasi profesional serta membangun budaya knowledge sharing antar tim. Dokumentasi sistem yang baik juga menjadi bagian penting dalam memastikan transfer pengetahuan berjalan dengan optimal dan mengurangi ketergantungan pada individu tertentu.

5. Diversifikasi Vendor

Untuk mengurangi risiko ketergantungan vendor, institusi perlu menerapkan strategi diversifikasi dalam penggunaan layanan dan produk TI. Hal ini dapat dilakukan dengan menggunakan lebih dari satu vendor (multi-vendor strategy) serta memilih solusi berbasis open standard atau open source.

Selain itu, perlu dilakukan evaluasi berkala terhadap kinerja vendor serta penyusunan kontrak yang fleksibel dan tidak mengikat secara jangka panjang. Dengan demikian, institusi memiliki fleksibilitas dalam mengelola sistem serta mengurangi risiko vendor lock-in

BAB VII
PENUTUP

7.1 Kesimpulan

Dokumen Analisis SWOT IT Master Plan Tahun 2026 ini disusun sebagai landasan strategis dalam pengembangan dan pengelolaan teknologi informasi di lingkungan institusi. Melalui pendekatan analisis SWOT (Strengths, Weaknesses, Opportunities, Threats), institusi dapat memperoleh gambaran yang komprehensif mengenai kondisi internal dan eksternal yang memengaruhi implementasi teknologi informasi.

Hasil analisis menunjukkan bahwa institusi memiliki potensi yang besar dalam mengembangkan sistem informasi yang terintegrasi dan modern, namun masih menghadapi sejumlah tantangan, seperti keterbatasan sumber daya manusia, kebutuhan peningkatan infrastruktur, serta ancaman keamanan siber yang semakin kompleks. Oleh karena itu, diperlukan strategi yang tepat, terarah, dan berkelanjutan untuk memaksimalkan kekuatan dan peluang yang ada, sekaligus meminimalkan kelemahan dan ancaman.

Dengan adanya dokumen ini, diharapkan seluruh pemangku kepentingan memiliki acuan yang jelas dalam merencanakan, melaksanakan, dan mengevaluasi program pengembangan teknologi informasi. Dokumen ini juga menjadi bagian penting dalam mendukung tercapainya visi institusi dalam transformasi digital yang efektif, efisien, dan berdaya saing tinggi.

7.2 Rekomendasi

1. Meningkatkan Komitmen Pimpinan terhadap Digitalisasi

Keberhasilan implementasi IT Master Plan sangat bergantung pada dukungan dan komitmen dari pimpinan institusi. Oleh karena itu, diperlukan peran aktif pimpinan dalam mendorong transformasi digital, baik melalui kebijakan, pengambilan keputusan strategis, maupun penyediaan sumber daya yang diperlukan.

Komitmen ini juga harus tercermin dalam integrasi program teknologi informasi ke dalam rencana strategis institusi secara keseluruhan. Dengan adanya dukungan yang kuat dari pimpinan, proses implementasi akan berjalan lebih efektif, terarah, dan memiliki legitimasi yang kuat di seluruh unit kerja.

2. Mengalokasikan Anggaran yang Memadai

Pengembangan teknologi informasi memerlukan investasi yang tidak sedikit, baik untuk infrastruktur, pengembangan sistem, maupun peningkatan kapasitas sumber

daya manusia. Oleh karena itu, institusi perlu mengalokasikan anggaran yang memadai dan berkelanjutan untuk mendukung implementasi IT Master Plan.

Pengelolaan anggaran juga harus dilakukan secara efektif dan transparan, dengan mempertimbangkan prioritas program yang memberikan dampak terbesar terhadap peningkatan layanan. Selain itu, institusi juga dapat mempertimbangkan alternatif pendanaan, seperti kerja sama dengan pihak eksternal atau pemanfaatan layanan berbasis cloud untuk efisiensi biaya.

3. Melakukan Evaluasi Berkala

Evaluasi berkala merupakan langkah penting dalam memastikan bahwa implementasi IT Master Plan berjalan sesuai dengan rencana dan target yang telah ditetapkan. Evaluasi ini mencakup aspek teknis, operasional, serta tata kelola teknologi informasi.

Melalui evaluasi yang dilakukan secara rutin, institusi dapat mengidentifikasi kendala yang dihadapi serta melakukan perbaikan secara cepat dan tepat. Selain itu, evaluasi juga memungkinkan adanya penyesuaian strategi agar tetap relevan dengan perkembangan teknologi dan kebutuhan pengguna.

4. Mengembangkan SDM TI Secara Berkelanjutan

Sumber daya manusia merupakan aset utama dalam pengelolaan teknologi informasi. Oleh karena itu, institusi perlu melakukan pengembangan kompetensi SDM TI secara berkelanjutan melalui pelatihan, workshop, serta sertifikasi profesional.

Selain peningkatan kompetensi teknis, pengembangan soft skills seperti manajemen proyek, komunikasi, dan kolaborasi juga perlu diperhatikan. Dengan SDM yang kompeten dan adaptif, institusi akan lebih siap dalam menghadapi tantangan serta memanfaatkan peluang dalam era transformasi digital.

7.3 Penutup

Dokumen Analisis SWOT IT Master Plan Tahun 2026 ini diharapkan dapat menjadi pedoman utama dalam pelaksanaan dan pengembangan teknologi informasi di lingkungan institusi. Dokumen ini tidak hanya berfungsi sebagai acuan perencanaan, tetapi juga sebagai alat pengendalian dan evaluasi dalam memastikan keberhasilan implementasi program TI.

Dengan adanya perencanaan yang matang, dukungan dari seluruh pemangku kepentingan, serta pelaksanaan yang konsisten, transformasi digital diharapkan dapat berjalan secara optimal. Hal ini akan memberikan dampak positif terhadap peningkatan kualitas layanan, efisiensi operasional, serta daya saing institusi di tingkat nasional maupun internasional.

Akhirnya, dokumen ini diharapkan dapat terus dikembangkan dan disempurnakan sesuai dengan dinamika perkembangan teknologi dan kebutuhan institusi, sehingga tetap relevan dan mampu memberikan kontribusi nyata dalam mendukung visi dan misi institusi.