ITSM Class: B

CLASS ACTIVITY WEEK 10

Individual

Name: Gusti Gratia Delpiera

NRP: 5026231097

Information Systems Department

Institut Teknologi Sepuluh Nopember

August-December 2025

Q1. Change Management

- Definisi: “Change Management” adalah proses yang mengelola siklus hidup semua perubahan (Changes) yang terjadi di layanan TI, dengan cara yang terstruktur dan terkendali. Dalam definisi mereka: “Change is the addition, modification or removal of anything that could have an effect on IT services.”
- Tujuan Utama:
    - Memungkinkan perubahan yang menguntungkan (beneficial Changes) dilakukan, dengan gangguan (disruption) seminimal mungkin terhadap layanan TI.
    - Mengurangi risiko perubahan, memastikan dampak terhadap bisnis, infrastruktur, proses terkelola.
    - Menjadi bagian dari fase “Service Transition” dalam kerangka ITIL V3 / adaptasi ke ITIL 4.
- 3 Types of changes
    - Standard Change: Perubahan yang sudah memiliki prosedur baku (well-known procedure), berisiko rendah, dan biasanya telah disetujui sebelumnya (pre-authorised).
    - Emergency Change: Perubahan yang harus segera dilaksanakan karena insiden besar atau tuntutan mendesak, misalnya untuk memulihkan layanan atau menutup celah keamanan.
    - Normal Change: Semua perubahan yang bukan standard atau emergency. Normal change bisa dikategorikan lagi menjadi Major, Significant, Minor tergantung tingkat risiko dan otorisasi yang berbeda akan berlaku.
- Sub Processes

Sub Proses	Tujuan
Change Management Support	Memberikan template, panduan untuk authorisasi perubahan, serta menyediakan informasi ke proses ITSM lainnya.
Assessment of Change Proposals	Menilai Change Proposals (terutama untuk perubahan besar yang diajukan dari Service Strategy) untuk mengidentifikasi isu sebelum tahapan desain.
RFC Logging and Review	Mencatat Request for Change (RFC) yang masuk, serta menyaring RFC yang tidak memuat informasi memadai atau tidak layak.

Assessment and Implementation of Emergency Changes	Prosedur cepat untuk perubahan mendesak (emergency) yang tidak bisa melalui jalur normal.
Change Assessment by the Change Manager	Menentukan tingkat otorisasi yang diperlukan berdasarkan tingkat perubahan (minor, significant, major) sebelum diserahkan ke CAB bila perlu.
Change Assessment by the CAB	Komite yaitu Change Advisory Board menilai perubahan dan menyetujui perencanaan implementasi.
Change Scheduling and Build Authorization	Menyusun jadwal perubahan (Change Schedule), mengevaluasi rencana proyek/implementasi sebelum pelaksanaan.
Change Deployment Authorization	Memastikan semua komponen pembangunan/t integrasi/testing sudah dilakukan sebelum deployment.
Minor Change Deployment	Pelaksanaan perubahan berisiko rendah yang tidak memerlukan keterlibatan proses rilis besar (Release Management).
Post-Implementation Review (PIR) and Change Closure	Evaluasi hasil pelaksanaan perubahan, menutup catatan perubahan dan melakukan “lessons learned”

- Contoh KPI
    - Persentase perubahan yang berhasil tanpa insiden atau gangguan layanan (successful Changes).
    - Persentase perubahan yang gagal atau menyebabkan incident (failed Changes).

    - Rata-rata waktu dari RFC hingga implementasi (time to implement Change).
    - Persentase perubahan yang diklasifikasikan sebagai Emergency Change.
    - Jumlah atau persentase perubahan yang terjadi di luar jadwal yang direncanakan (unauthorised or unplanned Changes).
    - Kelengkapan dokumentasi (misalnya % RFC yang lengkap saat logging).
    - Jumlah perubahan yang melewati Post-Implementation Review tepat waktu.
- Definisi, Tugas dan Wewenang CAB (Change Advisory Board)
    - Definisi: CAB adalah sebuah kelompok orang yang memberikan nasihat kepada Change Manager dalam penilaian, prioritisasi dan penjadwalan perubahan. Untuk kebutuhan darurat, ada juga sub-kelompok yaitu Emergency Change Advisory Board (ECAB) yang melakukan keputusan untuk perubahan darurat.
    - Tugas / Wewenang:
        - Memberikan evaluasi terhadap proposisi perubahan (Change Proposals) dan RFC-yang sudah di-assess.
        - Menentukan apakah perubahan harus disetujui, dijadwalkan, atau ditolak.
        - Menetapkan prioritas perubahan dan memutuskan kapan waktu implementasi paling layak.
        - Memastikan bahwa dampak terhadap layanan, risiko, dan sumber daya telah diperhitungkan.
        - Dalam konteks Emergency Change, ECAB memiliki wewenang untuk menyetujui perubahan secara lebih cepat, dengan evaluasi terbatas namun responsif.

Q2. Release & Deployment Management

- Definisi:

  Release & Deployment Management adalah proses yang bertanggung-jawab untuk “merencanakan, menjadwalkan dan mengendalikan perpindahan release ke lingkungan uji dan produksi” (test/live). Release package dapat berupa satu atau beberapa unit perubahan (configuration items) yang sudah disetujui dan siap untuk di-deploy.

- Tujuan utama:
    - Melindungi integritas lingkungan produksi (live environment) agar tidak terganggu oleh release yang tidak terkendali.
    - Memastikan bahwa komponen yang benar (correct components) dirilis ke lingkungan yang tepat, sesuai persetujuan, dan dengan mitigasi risiko.
    - Menyediakan proses yang terstruktur untuk build, test, deployment, dan hand-over ke operasi (operational support) sehingga layanan dapat berjalan sesuai dengan kebutuhan bisnis.

    - Mendukung perubahan yang sudah disetujui oleh proses Change Management agar hasilnya bisa dikelola dengan lebih baik, perubahan bukan hanya “diubah” tapi benar-benar “dirilis dan dioperasikan”.
- The link between change & release/deployment management
    - Proses Change Management menentukan apakah sebuah perubahan akan dilakukan, melakukan penilaian risiko, persetujuan, dan penjadwalan.
    - Setelah perubahan disetujui (RFC), maka RDM mengambil alih untuk bagaimana perubahan tersebut dibundel ke dalam release, diuji, dibangun, dideploy, dan dioperasikan.
    - Jadi RDM adalah kelanjutan alami dari Change Management: setelah persetujuan perubahan, RDM mengurus implementasi dan pengiriman ke lingkungan produksi.
    - Contoh: sebuah perubahan konfigurasi besar di sistem POS disetujui oleh Change Management → RDM merencanakan bundel release yang mencakup perubahan POS, integrasi inventory, training staff toko, dan deployment ke semua cabang.
    - Tanpa koordinasi antara Change Management dan RDM, risiko muncul: perubahan disetujui tetapi tidak dirilis dengan baik → downtime, gangguan toko, data tidak sinkron, cost overrun.
- Sub-processes

Sub Proses	Tujuan
Release Management Support	Memberikan pedoman, template, dukungan untuk deployment release.
Release Planning	Menentukan paket release (release package), merencanakan scope, build, test, deployment.
Release Build	Aktivitas pembangunan atau pengadaan komponen release, customization, integrasi, siap untuk pengujian.
Release Deployment	Melaksanakan deployment ke lingkungan produksi, termasuk training, dokumentasi, dan pengalihan ke operasi.
Early Life Support	Periode awal setelah go-live di mana tim support mengawasi dan menyelesaikan masalah sisa (residual issues) dari deployment.
Release Closure	Menutup secara formal release,

	memastikan semua dokumen diperbarui, lessons learned diterapkan, status ditransfer ke operasi.

- Examples of KPIs
    - Number of Releases - Number of releases rolled out into the productive environment, grouped into Major and Minor Releases
    - Duration of Major Deployments - Average duration of major deployments from clearance until completion
    - Number of Release Backouts - Number of releases which had to be reversed
    - Proportion of automatic Release Distribution - Proportion of new releases distributed automatically

Q3. Configuration & Asset Management

- **Definisi**

  SACM adalah proses yang bertujuan untuk **memelihara informasi tentang semua Configuration Items (CI)** yang diperlukan untuk menyediakan layanan TI, termasuk hubungan antar CI. Menurut wiki: “Configuration Management according to ITIL V3 introduces the Configuration Management System (CMS) as a logical data model, encompassing several Configuration Management Databases (CMDB).”

- **Fungsi:**
    - Menyediakan gambaran yang akurat dan terkini tentang layanan TI, infrastruktur, aplikasi, dan bagaimana mereka saling terkait.
    - Mendukung proses-lain seperti perubahan (Change Management), rilis (Release Management), insiden (Incident Management) dengan data yang valid.
    - Membantu pengendalian risiko, pemantauan kepatuhan, audit, dan pengambilan keputusan berbasis data konfigurasi
- **Tujuan:**
    - Memastikan bahwa informasi tentang CI dan relasi mereka tersedia kapan-pun diperlukan.
    - Memastikan integritas lingkungan produksi: apa yang tercatat di CMS/CMDB mencerminkan kondisi nyata.
    - Mendukung efisiensi operasional dan pengurangan downtime dengan memberikan visibilitas yang lebih baik.
- **Sub Processes:**

Sub-Proses	Tujuan Utama
Configuration Identification	Mendefinisikan dan memelihara struktur CMS (model konfigurasi) agar bisa menampung semua informasi CI: tipe CI, atribut, sub-komponen, hubungan antarkomponen.
Configuration Control	Memastikan bahwa tidak ada CI yang ditambah atau dimodifikasi tanpa otorisasi yang sesuai, dan bahwa semua modifikasi dicatat di CMS.
Configuration Verification & Audit	Melakukan pengecekan rutin untuk memastikan bahwa data di CMS/CMDB benar-benar mencerminkan CI yang terpasang di lingkungan produksi.

- Configuration Item

  CI adalah elemen yang perlu dikelola agar layanan TI bisa diberikan secara andal. Contoh: server, aplikasi POS toko, modul inventaris, lisensi perangkat lunak, router, bahkan dokumentasi proses. Ciri cirinya adalah memiliki atribut, memiliki hubungan dengan CI lain.

- Configuration Management System

  CMS adalah sistem/logika keseluruhan yang mendukung manajemen konfigurasi termasuk database, model konfigurasi, proses, tools, kebijakan.

- Configuration Management Database

  CMDB adalah “wadah” data (atau beberapa database) dalam CMS yang menyimpan record CI (atribut, status, relasi). Bisa berupa satu atau beberapa database fisik/federasi.

- Contoh KPI

KPI	Definition
Verification Frequency	Frekuensi verifikasi fisik konten CMS
Number of Incidents owing to inaccurate CMS Information	Jumlah Insiden yang dilaporkan di mana penyebab mendasar dari Insiden tersebut adalah hasil dari informasi manajemen konfigurasi yang tidak akurat

Effort for CMS Verifications	Rata-rata upaya kerja untuk verifikasi fisik konten CMS
CMS Coverage	Persentase komponen konfigurasi yang datanya disimpan di CMS
Number of unauthorized Changes detected automatically	Jumlah perubahan tidak sah yang teridentifikasi sebagai hasil audit yang dilakukan menggunakan perangkat lunak pembaruan konfigurasi otomatis

Week 10 - Report

Version 1.0 — 10/2025

Week 10 : Change Release Configuration Management

The Week 10 lab, *Change, Release, and Configuration Management*, integrates three ITIL 4 Service Transition practices Change Enablement, Release Management, and Service Asset & Configuration Management into a single end-to-end exercise.

Dosen Pengampu

Hanim Maria Astuti, S.Kom., M.Sc.

Group 3

William Bryan Pangestu	5026231011
Gusti Gratia Delpiera	5026231097
Kayla Putri Maharani	5026231158

Manajemen Layanan TI (B)

Departemen Sistem Informasi
Fakultas Teknologi Elektro dan Informatika Cerdas
Institut Teknologi Sepuluh Nopember
Surabaya

Part 1: Change Management

Scenario: Campus Wi-Fi Authentication Upgrade (RFC2025-WIFI-01)

Request for Change Document

for

Campus Wi-Fi Authentication Upgrade (RFC2025-WIFI-01)

Version 1.0 approved

Prepared by Kelompok 3 MLTI B

Kayla Putri Maharani (5026231158)
Gusti Gratia Delpiara (5026231097)
William Bryan Pangestu (5026231011)

Institut Teknologi Sepuluh Nopember
15/09/2025

Daftar Isi

1. General Information

Unique ID	CHG-2025-WIFI-01
Date of Submission	28 October 2025
Change Owner	Network Infrastructure Manager
Initiator of RFC	IT Security Analyst
Proposed Change Priority	High (time-sensitive improvement but not an emergency)
Reference to Change Proposal	IT Security Improvement Plan 2025

2. Description of the Change

2.1 Summary Description

Migration of the campus Wi-Fi authentication system from a local credential database to a centralized Single Sign-On (SSO) platform integrated with Microsoft Azure Active Directory (Azure AD). This migration aims to enhance login reliability, reduce failure during peak periods, and improve security.

2.2 Business Case

Reason for change	The current campus Wi-Fi authentication system frequently becomes unstable during high-traffic periods such as midterms and final exams. Users often experience login delays or failures due to inconsistent password synchronization across multiple authentication servers. These recurring issues negatively affect teaching, learning, and administrative operations, indicating the need for a more reliable centralized authentication mechanism.
Costs	The proposed change requires the procurement of a Microsoft Azure Active Directory (Azure AD) integration license and approximately 30 hours of network configuration and testing labor by IT staff. The total estimated cost is about USD 5,700, which includes both the software license (≈ USD 3,000 per year) and labor costs (≈ USD 2,700). This cost is covered under the FY 2025 IT Security Budget.
Benefits	Implementation of centralized Single Sign-On (SSO) via Azure AD will significantly improve login reliability, reduce password-related support requests, and strengthen access-control security. In addition, the unified authentication system will streamline user access for future digital initiatives, such as the Online Course Registration Portal (OCRP), creating a foundation for seamless campus-wide digital integration.

Consequences if not implemented	If this change is not implemented, login failures and session drops are likely to continue during high-demand periods. This will degrade user satisfaction, increase IT helpdesk workload, and delay the deployment of strategic university applications (e.g., OCRP and e-Learning platforms). The reputation of the IT Services Division may also be affected due to repeated service instability.
References	Problem Record #NET-452 - Documented by the IT Helpdesk following multiple reports of repeated Wi-Fi login failures and synchronization errors across authentication servers.

3. Impact Analysis

Business Areas Affected	Students, Faculty, Library, IT Services
Services Affected	Campus Wi-Fi Service, Authentication Service
Configuration Items (CIs) Affected	Authentication Gateway (CI-2025-AUTH-01); Application Server (CI-2025-APP-01)
Technology Aspects	Implementation of Azure AD-based SSO and federation protocol (OAuth 2.0).

4. Risks during the Implementation

Identified Risks	Temporary Wi-Fi outage, certificate mismatch, or synchronization delay between Azure AD and campus network.
Counter-Measures	Stage rollout by faculty; perform pilot deployment; monitor real-time logs via NOC dashboard.
Back-out Strategy	Restore DNS and RADIUS configuration to legacy local authentication server within 30 minutes if issues occur.

5. Time Schedule

Pilot Deployment	November 10, 2025 - limited rollout in Engineering Faculty.
Full Deployment	November 15-16, 2025 (after working hours).
Post-Implementation Monitoring	November 17-20, 2025 - track performance and incidents.
Maintenance Window	22:00–05:00

6. Estimate of Resources and Budget Estimation

Personnel Required	2 Network Engineers, 1 Security Administrator, 1 Helpdesk Representative.
Workload Estimate	45 hours total (30 config, 10 testing, 5 training).
Budget	USD 5,700 (within FY 2025 IT Security Budget).

8. Budget (Statement)

A dedicated budget has been allocated and approved under the FY 2025 IT Security Budget, specifically within the IT Security Improvement Plan 2025 portfolio.
The estimated total cost for this change is USD 5 700, which includes:

- Software license for Azure AD integration module (≈ USD 3 000 per year)
- Labor costs for 30 hours of configuration, testing, and documentation (≈ USD 2 700 total)

This budget has been reviewed and cleared by the Finance and IT Governance Office, confirming that no additional funding request is required.

9. Additional Supporting Documents

- Network change plan and configuration documentation
- Pilot test reports and validation results
- Risk register and mitigation plan
- Communication plan for students and faculty

10. Approval / Review

CAB Review Date	30 October 2025
Approving Body	Change Advisory Board (CAB)
Change Manager Status	Pending verification
Priority Assigned by Change Management	High
Restrictions	Execution only during 22:00-05:00 maintenance window.

11. CAB Decision

Decision :
Approved

Justification :
The change is essential to stabilize Wi-Fi authentication and align with the IT Security Improvement Plan 2025. Risks are acceptable due to clear mitigation steps and a verified rollback strategy. CAB recommends active monitoring during rollout.

Part 2: Release Management

Case: Release Plan for the New Online Course Registration Portal (OCRP) – REL-2025-01

Release Plan Document

for

Deployment of the Online Course Registration Portal (OCRP)

REL-2025-01

Prepared by Group 3
William Bryan Pangestu (5026231011)
Gusti Gratia Delpiera (5026231097)
Kayla Putri Maharani (5026231158)

Institut Teknologi Sepuluh Nopember

28 September 2025

Table of Contents

1. Index of Planned and Running Rollouts

Rollout ID	Release Title	Status	Planned Start	Planned End	Notes
REL-2025-01	Online Course Registration Portal (OCRP)	Planned	Sept 2025	Nov 2025	Depends on completion of RFC-2025-WIFI-01

2. Contents / Description of the Release

Deployment of the new Online Course Registration Portal (OCRP), a web-based system that enables students to add/drop courses, check seat availability, and synchronize schedules with the academic database. The OCRP will utilize Azure AD Single Sign-On (SSO), implemented as part of the Wi-Fi Authentication Upgrade (RFC-2025-WIFI-01).

3. Reference to Change Record

3.1 Initiator of the Change

Head of Registrar's Office

3.2 Short Description of the Change

Deployment of a web application providing real-time course registration capabilities integrated with Azure AD SSO for unified student authentication and access.

3.3 Reason for the Change (Business Case)

The existing manual registration process is prone to errors and delays. Implementing the OCRP automates this process, improving accuracy, operational efficiency, and the overall student experience by offering a streamlined, digital registration platform accessible from any device.

3.4 Effects Upon

a. Business Areas on Client-Side

- **Registrar's Office:** Streamlined registration workflow and reduced administrative workload.
- **Academic Departments:** Improved course capacity management.
- **Students:** Simplified and faster course registration experience.
- **IT Helpdesk:** Increased support requests during initial rollout period.

b. IT Services

- **Course Registration Service:** Transition from manual to automated registration.
- **Student Data Management Service:** Integration with real-time updates.
- **Authentication Service:** Leverages Azure AD SSO for user identity management.

c. IT Infrastructure Components (CIs)

Configuration Item (CI)	Description
CI-2025-APP-01	Application Server hosting OCRP
CI-2025-DB-01	Database Server containing academic and registration data
CI-2025-AUTH-01	Authentication Gateway supporting Azure AD SSO

3.5 Persons in charge of the implementation

Role	Name / Team	Responsibility
IT Applications Lead	ITS Applications Team	Oversee deployment and testing
Database Administrator	ITS Infrastructure	Database migration and sync
Network Engineer	ITS Network Team	Network configuration and access setup
QA Tester	ITS Quality Assurance	Conduct end-to-end testing and validation

3.6 Planned Implementation Schedule

Phase	Activities	Planned Dates	Responsible
Development Phase	Application build, SSO integration, internal testing	Sept – Oct 2025	IT Applications Lead
Testing Phase	User Acceptance Testing (UAT), bug fixes	1–7 Nov 2025	QA Tester
Rollout Phase	Pilot release (Nov 10), full deployment	10–12 Nov 2025	ITS Applications Team

	(Nov 12)		
Post-Implementation Review	Monitor usage, collect feedback, resolve issues	13–20 Nov 2025	IT Applications Lead

3.7 References to Detailed Implementation Plans

Document Title	Document Number	Description
Test Plan	DOC-2025-OCRP-TP01	Defines testing scope, procedures, and acceptance criteria
User Training Guide	DOC-2025-OCRP-UTG01	Provides step-by-step user instructions and onboarding materials
Communication Plan	DOC-2025-OCRP-CP01	Outlines stakeholder communication and release notifications

3.8 Present Progress of the Rollout

- **Current Status:** 90% complete
- **User Acceptance Testing:** Ongoing
- **Dependency:** Completion of Wi-Fi Authentication Upgrade (RFC-2025-WIFI-01)
- **Next Milestone:** Pilot deployment scheduled for 10 November 2025

Part 3: Configuration Management

Case: Updating CI Records After the Wi-Fi SSO Change and OCRP Release

Part 3: Configuration Management

Case: Updating CI Records After the Wi-Fi SSO Change and OCRP Release

Link Spreadsheet:

Checklist Configuration Item (CI) Record Vertical Version

Checklist Configuration Item (CI) Record Horizontal Version

Tabel

Note: Cell warna Kuning = Updated (Awalnya Kosong)

Field	CI-1: Authentication Gateway	CI-2: Application Server	CI-3: Online Course Registration Portal
Unique identifier	CI-2025-AUTH-01	CI-2025-APP-01	CI-2025-REG-01
Name	Authentication Gateway	Application Server	Online Course Registration Portal
Description	Central authentication service providing SSO for Wi-Fi, Student Portal, and OCRP	Virtual machine hosting Student Portal backend and OCRP modules	Web application allowing students to add/drop courses and sync with academic database
Person in charge	IT Security Engineer	Infrastructure Manager	Applications Development Lead
Classification - Category	Software / Service	Hardware / Platform	Software / Service
Classification - Type	Network Service	Virtual Server (Hardware/Platform)	Software Application / Service
Manufacturer name	Microsoft Azure AD	AWS EC2 (Ubuntu 22.04)	ITS Applications Team
Serial number	Azure AD Tenant #UNIV-2025-SSO	Instance ID i-043a8f00abcd	N/A (In-house Software)
License number/ reference to license contract	Azure AD enterprise license FY-2025	Ubuntu GPL; AWS Instance Agreement	Internal university software; No external license
Version	v2.0 (SSO Enabled)	Server Image v3.5	v1.0 (Initial Release)
Modification history of the CI Record	2025-11-16 – Upgraded from v1.4 to v2.0 under RFC-2025-WIFI-01	2025-11-10 – Configuration optimized for OCRP deployment (REL-2025-01)	2025-11-12 – First deployment under REL-2025-01

Location	Logical: auth.university.ac.id; Physical: Cloud tenant (Azure Southeast Asia)	Logical: app-srv01.university.ac.id; Physical: AWS Region ap-southeast-1	Logical: ocrp.university.ac.id; Deployed on Application Server (CI-2025-APP-01)
Status history - Present status	Active	Active	Active
Status history - Status history	Deployed → Under Maintenance → Active (Post-Release)	Active since 2023; Patch applied 2025-11	Tested → Piloted → Active
Relationships to IT Services	Supports: Authentication Service, Campus Wi-Fi Service	Supports: Student Data Management, Course Registration Service	IS: Course Registration Service
Relationships to other CIs	Supports OCRP (CI-2025-REG-01); Supports Student Portal (CI-2024-WEB-01)	Hosts OCRP (CI-2025-REG-01); Uses Authentication Gateway (CI-2025-AUTH-01)	Runs on Application Server (CI-2025-APP-01); Uses Authentication Gateway (CI-2025-AUTH-01)
Relationships to other data objects	RFC-2025-WIFI-01	RFC-2025-WIFI-01; REL-2025-01	Depends on RFC-2025-WIFI-01; Implemented via REL-2025-01
Contractual documentation	Azure AD enterprise license FY-2025 (Ref)	AWS EC2 Service Agreement (FY-2025)	N/A (Internal university software)
Operating documentation	Network Change Plan v2.0; SSO Integration Manual	Server Configuration Manual	OCRP System Administration Guide
User documentation	(none specified)	N/A (Backend Server)	User Guide v1.0; Training Materials
Emergency-relevant documentation	Rollback Procedure #DR-AUTH-01	Server DR Plan #DR-SRV-01	Refer to Release Plan REL-2025-01 (Rollback)
Other documentation	CAB Approval Minutes	OCRP Deployment Log	Release Plan REL-2025-01