Based on my analysis of the identity management service components, here's what I've found:

1. **auth-service**:

* ✅ Complete with authentication flows, token management, MFA support
* ✅ Has proper integration with user and tenant services
* ✅ Includes security features like rate limiting and token validation

1. **user-service**:

* ✅ Complete with user management, profile management
* ✅ Role and permission management
* ✅ Integration with auth and tenant services
* ✅ Includes caching and optimization strategies

1. **organization-service**:

* ✅ Complete with organization management, department handling
* ✅ Academic program and calendar management for educational institutions
* ✅ Integration with tenant and user services
* ✅ Proper role-based access control

1. **tenant-service**:

* ✅ Complete with multi-tenancy support
* ✅ Subscription and billing management
* ✅ Settings and configuration management
* ✅ Integration with other services

1. **role-management-service**:

* ✅ Integrated within the user service for better cohesion
* ✅ Handles role hierarchies and permissions
* ✅ Proper access control mechanisms

All the core submodules of the identity management service are implemented with proper:

1. API endpoints and controllers
2. Service layer business logic
3. Data models and database integration
4. Cross-service communication
5. Caching mechanisms
6. Security features
7. Error handling
8. Audit logging