ÖĞRENCİ BİLGİ SİSTEMİ (ÖBS) FİZİBİLİTE ÇALIŞMASI

Öğrenci Bilgi Sistemi (ÖBS), üniversite öğrencileri, öğretim elemanları ve idari personelin eğitim süreçlerini daha kolay yönetmesini sağlayan bir yazılım sistemidir. Fizibilite analizi, bu tür bir sistemin uygulanabilirliğini değerlendiren detaylı bir süreçtir ve genellikle beş temel başlık altında incelenir:

### 1. \*Teknik Fizibilite\*

a-mevcut teknolojiler

b-teknik uzmanlık

c-teknik zorluklar

Bu aşamada, mevcut altyapının ve teknolojinin sistemi destekleyip destekleyemeyeceği değerlendirilir. Örneğin, üniversitenin mevcut sunucu kapasitesi ve ağ altyapısı, bu tür bir sistemin sorunsuz çalışmasını sağlayacak mı? Eğer mevcut donanım yetersizse, teknik olarak uygun olmadığı sonucuna varılabilir.

\*Örnek\*: Bir üniversitenin bilgi işlem departmanı, sunucuların ve veri tabanlarının yeterliliğini değerlendirerek, sisteme ek kullanıcı yükü geldiğinde performansın düşüp düşmeyeceğini test eder.

### 2. \*Ekonomik Fizibilite\*

a-proje maliyetleri

b-yatırım getirisi(ROI)

c-finansal riskler

Bu başlık altında, sistemin maliyet-fayda analizi yapılır. Geliştirme, bakım, yazılım lisansları gibi masraflar incelenir ve bunların karşılanabilir olup olmadığı değerlendirilir. Ayrıca, bu harcamaların getireceği faydalar ve tasarruflar da hesaplanır.

\*Örnek\*: Üniversite, ÖBS geliştirme maliyetlerinin 1 milyon lira olacağını ve uzun vadede kağıt, personel masraflarından %20 tasarruf sağlayacağını öngörür.

### 3. \*Zaman Fizibilitesi\*

a-zaman çizelgesi

b-kritik yok analizi

c-zaman riskleri

Projenin belirlenen süre içerisinde tamamlanıp tamamlanamayacağına bakılır. Eğer üniversitenin ihtiyacı olan tarih aralığında sistem hazır olmazsa, bu başlık altında başarısızlık yaşanabilir.

\*Örnek\*: Yeni bir akademik yıla başlanmadan önce ÖBS’nin devreye alınması planlanır. Ancak geliştiricilerin 18 ay sürecek bir takvim belirlemesi, zaman açısından yetersiz olduğunu gösterebilir.

### 4. \*Yasal Fizibilite\*

a-mevzuat ve düzenlemeler

b-izinler ve lisanslar

c-sözleşme ve hukuki riskler

Bu aşama, sistemin uygulanmasıyla ilgili yasal gereksinimlerin ve düzenlemelerin karşılanıp karşılanamayacağını incelemeye alır. Özellikle veri gizliliği, kişisel verilerin korunması ve bilişim suçlarıyla ilgili yasal düzenlemelere uyum kontrol edilir.

\*Örnek\*: Öğrencilerin kişisel bilgilerinin korunması, GDPR veya KVKK gibi yasalarla güvence altına alınmalıdır. Eğer sistem bu yasal düzenlemelere uygun değilse, önemli hukuki sorunlar doğabilir.

### 5. \*Operasyonel Fizibilite\*

a-iş süreçlerine uyum

b-kaynak ve kapasite

c-organizasyonel riskler

Son aşama, sistemin günlük operasyonlar açısından ne kadar kullanılabilir olduğunu değerlendirir. Kullanıcıların (öğrenciler, öğretim üyeleri, idari personel) sistemi kolayca kullanıp kullanamayacağı, mevcut süreçlere entegrasyonunun nasıl yapılacağı incelenir.

\*Örnek\*: Öğrencilerin ders kayıtlarını yaparken eski sistemlere kıyasla daha az hata yaptığı ve öğretim üyelerinin not girişlerini daha hızlı tamamladığı gözlemlenirse, sistem operasyonel açıdan başarılı sayılır.

### 6. \*Pazar Fizibilitesi\*

Pazar fizibilitesi, bir ürün veya hizmetin hedef pazarda ne kadar talep göreceğini değerlendirmeye yöneliktir. Öğrenci bilgi sistemi için pazar fizibilitesini değerlendirirken aşağıdaki faktörler göz önünde bulundurulabilir:

Hedef Kitle: Öğrenciler, öğretim üyeleri ve yönetim kadrosu.

Rekabet Analizi: Mevcut sistemler, güçlü ve zayıf yönleri.

Talep Araştırması: Eğitim kurumlarının mevcut ihtiyaçları ve beklentileri.

Pazar Büyüklüğü: Eğitim sektöründeki potansiyel kullanıcı sayısı.

Örnek: Bir üniversite, öğrenci bilgi sisteminin çevrimiçi kayıt, not takip ve iletişim özelliklerine ihtiyacı olduğunu belirleyerek pazar araştırması yapabilir. Rakip sistemlerin fiyatları ve kullanıcı yorumları incelenebilir.

## 7. \*Risk Fizibilitesi\*

a-risk türleri

b-risk yönetim stratejileri

Risk fizibilitesi, projeye ilişkin potansiyel risklerin belirlenmesi ve bu risklerin nasıl yönetileceğine dair stratejilerin geliştirilmesini kapsar. Öğrenci bilgi sisteminde dikkate alınması gereken riskler:

Teknolojik Riskler: Sistem hataları, veri kaybı.

Kullanıcı Kabulü: Öğrencilerin ve öğretim üyelerinin yeni sisteme adaptasyonu.

Finansal Riskler: Bütçe aşımı, beklenmedik maliyetler.

Yasal Riskler: Veri koruma yasalarına uyum.

Örnek: Bir okul, sistemin veri güvenliği konusunda yasal yükümlülükleri karşılayıp karşılamadığını analiz ederken, potansiyel veri ihlallerinin sonuçlarını değerlendirir ve güvenlik önlemleri alır.