



Kurumsal Kimlik Yönetimi ve Güçlü Kimlik Doğrulama

Yılmaz Çankaya

Mart, 2010

Kaynak (Resource)

Uygulamaları oluşturan ve kullanılması hedeflenen bütün yetki seviyelerinin kontrolünü sağlayabilecek nesnelerdir.

Kimlik (Identity)

Kimlik Doğrulama (Authentication)

Sistemi kullanmak isteyen kimliğin bilgilerinin, sistemde tutulan kimlik bilgileri ile doğrulanmasıdır.



Tümleşik Oturum (Single Sign-On, SSO)

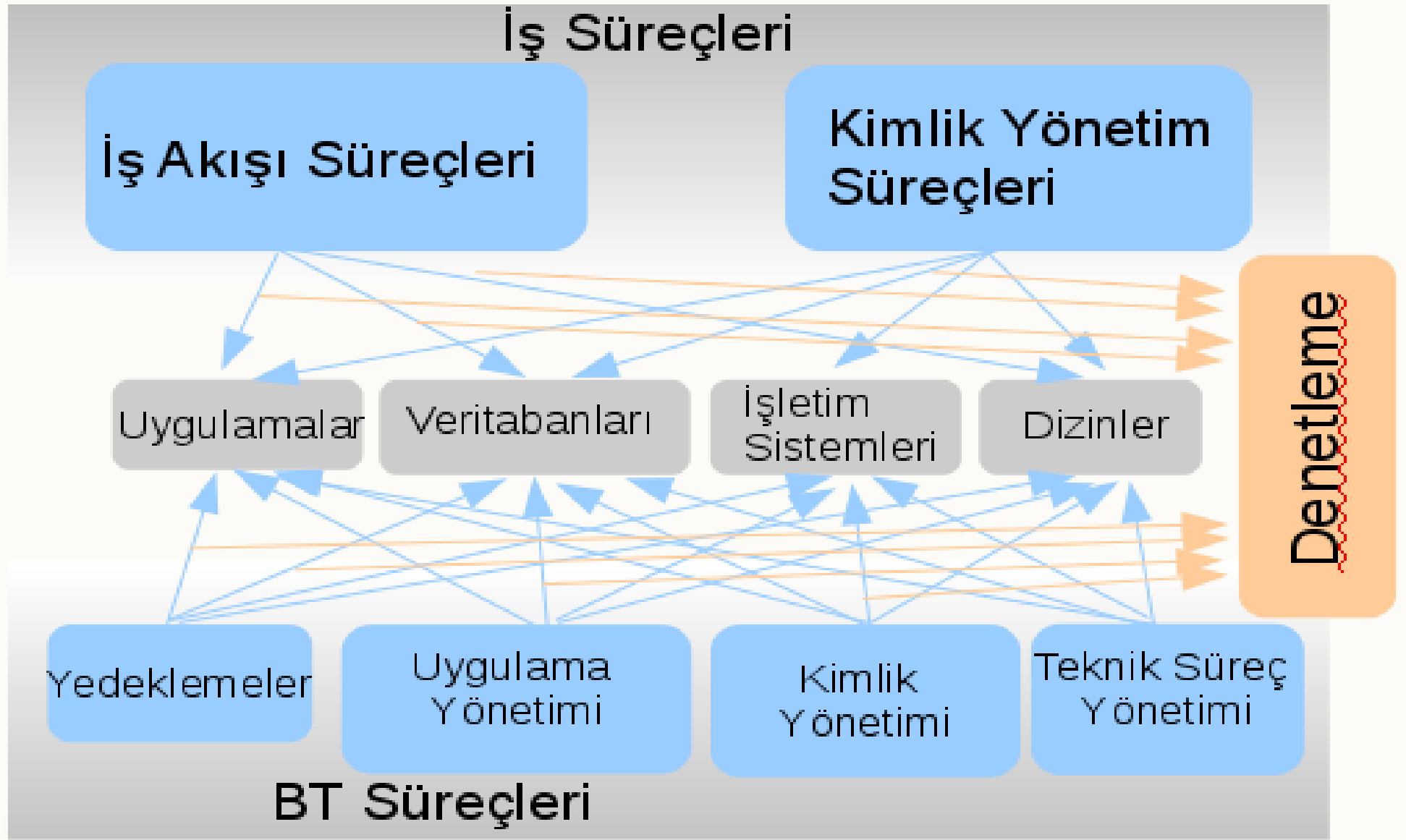
Kimlik doğrulama işleminin, ekosistem dahilindeki bütün uygulamalar için merkezileştirilmesi olarak tanımlanabilir.

Kimlik Yetkilendirme (Authorization)

Kimlik Bilgilerinin Koordinasyonu (Provisioning)

Kimlik Yönetim Sistemi (Identity Management System)

Kaynakların, kimlik bilgilerinin saklandığı dizinlerin, kimlik yetki atamalarının yönetimini sağlayan sistemdir





KYS Avantajları

Daha Az Şifre

Program Geliştirme ve Güvenlik

Kod içinde güvenlik tabakasının oluşturulması yükünün, programcının omuzlarından alınmış olması işte hızlanma ve verimlilik getirecektir.

Uygunluk Kriterleri ve Denetim

Kim ne zaman hangi kaynaklara erişme yetkisinin olduğu ve hangi kaynaklara kimin ne zaman eriştiği raporlanabilmeli.

Uçtan Uca Otomasyon

Insan faktörü. Takip, izleme, denetleme ve hesap sorabilme konularında raporlama sürecinde zaman kaybı, sonucu doğru olmayan raporlamalar

Kimlik Verilerinin Konsolidasyonu

Kullanıcının Kendi Kendine Yönetimi (Self-Service)

Sağlıklı İzleme Mekanizmaları



Maymuncuk Anahtarı

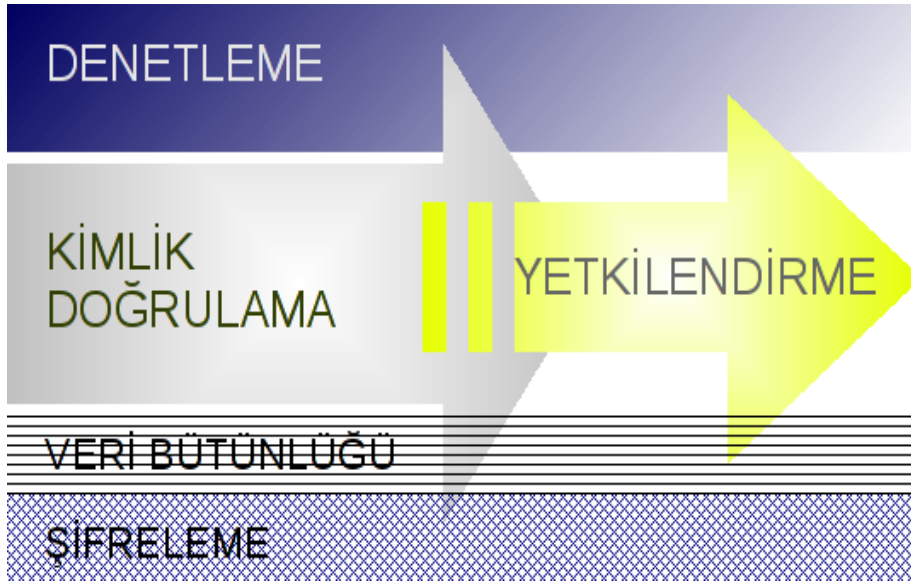
Tek şifre ile bütün sistemleri yönetiyor olmak, bu şifrenin istenmeyen bir kişinin eline geçmesi durumunda, birkaç sistemin birden erişilebiliyor olması anlamına gelecektir.

Mevcut Uygulamaların Entegrasyonu

KYS'ye geçiş aşamasında en sancılı ve maliyetli kalem, varolan sistemlerin KYS yapısına geçirilmesi olacaktır.

İş Akışlarının Yönetimi

Kimlik oluşturma, güncelleme ve kimlik yetkilendirme iş akışlarının oluşturulması ve otomatize edilmesi, süregelen şirket içi alışkanlıkların yıkacaktır. Yönetim süreçlere dahil olacaktır.



Temel Veri Eriřim İş Akışı

Uygulama Geliřtirme ve Analiz

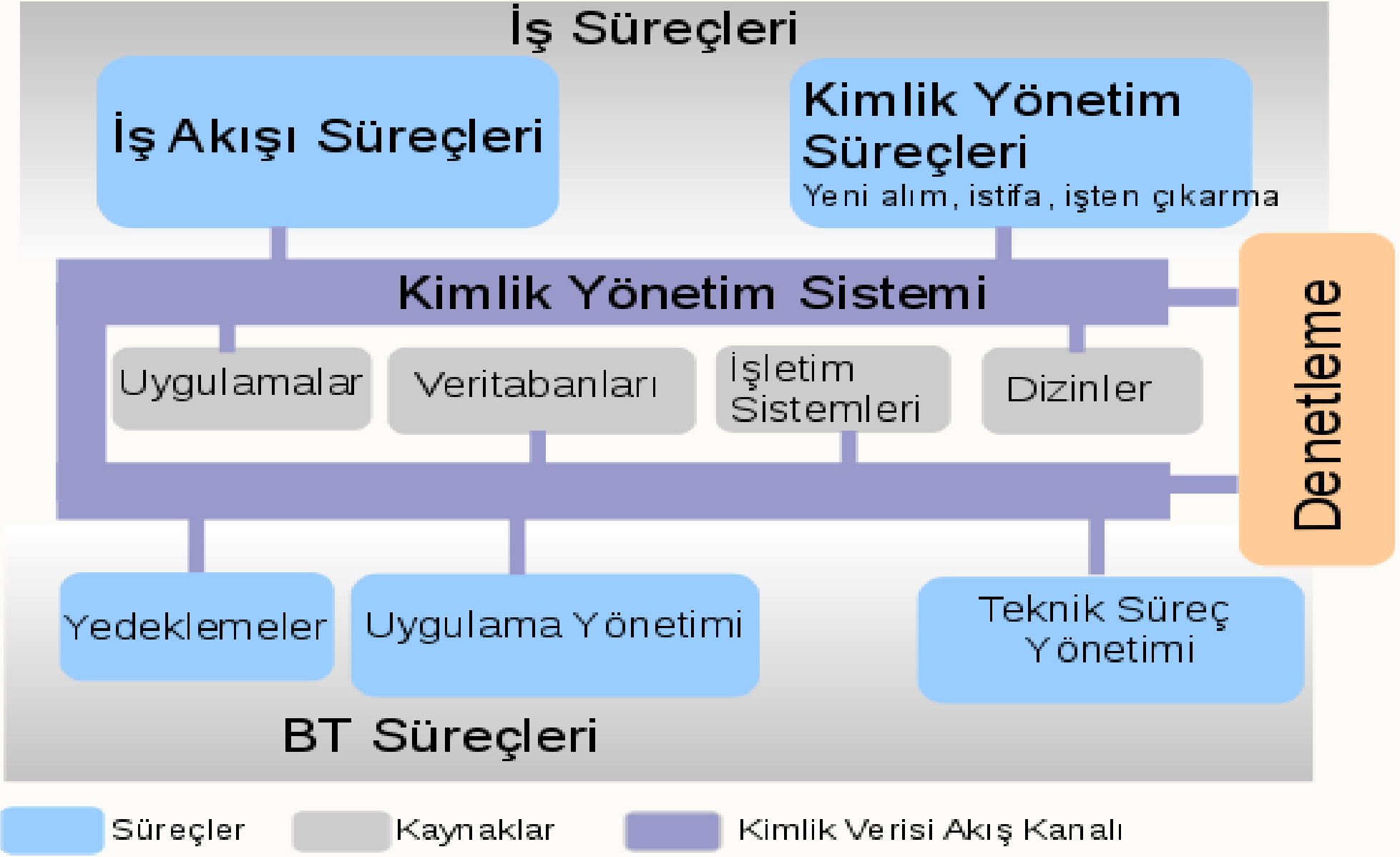
Uygulama geliřtirme projelerinde analiz ařamasının içinde barındırdığı en temel süreçler, kimlerin uygulamayı kullanacağı ve kimin hangi kaynaklara erişmesi gerekeceğinin belirlenmesidir.

Akış Başlangıç Ucu

Son kullanıcı güvenliği. Tarayıcılar ve güçlü kimlik doğrulama yöntemleri.

Akış Bitiş Ucu

Veritabanı ve işletim sistemi erişim denetlemesi. Verinin saklandığı depolama cihazlarının güvenliği.



Uygulamalar

Sunduđu servisler ve servisler üzerinden gerekleřtirilebilen eylemler (Örn. ekle, güncelle, sil)

Veritabanları

LDAP üzerinden erişim kontrolü

İřletim sistemleri

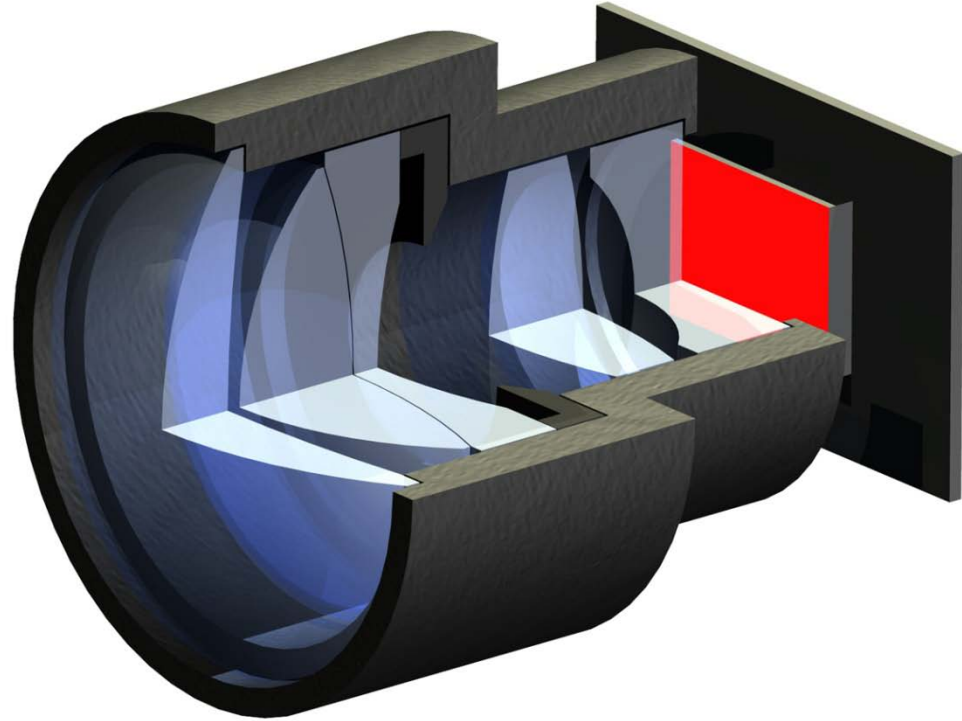
LDAP üzerinden erişim kontrolü
Sudoers

Dizin sistemleri

Yetki paylaşımı

Diđer

Depolama aygıtları ve ađ cihazları



Tümleşik Oturum Yönetimine Geçiş

KYS tümleşik oturum yönetim sunucusu bütün web uygulamalarına erişim öncesi araya girer ve kullanıcı için oluşturulmuş bir çerezin varlığını kontrol eder.

Uygulama Ajanları ve Tipleri

Ajan uygulamalar, asıl kaynağa erişim için kullanıcı tarafından gönderilen talepleri keser ve KYS tümleşik oturum sunucusu tarafından oluşturulan ve internet tarayıcısı tarafından gönderilen çerezin varlığını kontrol ederler.

Kimlik Doğrulama ve Yetkilendirme Program Arayüzleri

KYS uygulamaları, kimlik doğrulama ve yetkilendirme sorgularının herhangi bir ajan uygulama kurulumuna ihtiyaç olmadan programatik olarak gerçekleştirilebilmesi için yazılım arayüzleri (API) sunarlar.

```
<filter>
  <filter-name>J2eeAjan</filter-name>
  <filter-class> com.sun.identity.agents.filter.AmAgentFilter </filter-class>
</filter>
<filter-mapping>
  <filter-name>J2eeAjan</filter-name>
```

```
boolean isManager = request.isUserInRole("MANAGER_ROLE");
boolean isEmployee = request.isUserInRole("EMPLOYEE_ROLE");
StringBuffer buff = new StringBuffer();
buff.append("Kullanıcı \").append(user).append("\": ");
if (isManager)
    buff.append("Yönetici");
if (isEmployee)
    buff.append("Çalışan.");
```

```
/usr/local/linux_agent_apache/agents/apache/lib/libamapc2.so
```

```
include /etc/opt/agents/apache/config/_etc_httpd_conf/AMAgent.properties
```

Tümleşik Oturum Yönetimi

Kaynak Erişim Atamaları

Kullanıcı Grupları (Roller)

İş Akışları

Kimlik oluşturma ve yetkilendirme otomasyonu

Veritabanı Entegrasyonu

Açık kaynak kodlu veritabanlarında yetkilendirme yönetimi eksikliği

İşletim Sistemi Entegrasyonu

Çeşitli Topolojiler Uygulanabilir
Hibrit olabilir

Dizin Yönetim Arayüzü

Şifreleme ve Veri Bütünlüğü

İnternet tarayıcısı ayarları ve kütüphaneler
E-Posta uygulamalarının entegrasyonu

Linux tabanlı işletim sistemlerinin entegrasyonu

Merkezi Kayıt Yönetimi

Üstün Yetkili Kullanıcıların Yönetimi

İşletim sistemleri

Veritabanları

Dizinler

Depolama aygıtları ve ağ cihazları

Raporlamalar

Sistemlerin Ana İşlevleri

Atanan yetkiler çerçevesinde veriye erişim ve verinin yönetimi

Kimlik Yönetiminin Getirileri

Kim neleri yapabilir?

Kim ne yapıyor?

Kim ne zaman, ne yaptı?

Kontrol edilemeyen yetkilendirmeleri denetleyebiliyor muyum?

Bütün Bilgi Sistemleri Sisteme Dahil Edilmeli

BGYS

Bilinçlendirme

Son kullanıcı tarafında güvenlik

Sistemin haritasının çıkarılması

Risk Yönetimi

Yama Yönetimi

ÖRNEK UYGULAMA



Tümleşik Oturum

Kaynak - Rol Atamaları

Güvenlik Etki Alanları

Akıllı Kart Kullanımı

Denetleme

