Bilgi Teknolojileri Yönetişim ve Denetim Konferansı

BTYD 2010

ISACA Serving IT Governance Professionals

Türkiye Bilişim Derneği 1971

Türkiye İç Denetim Enstitüsü 1995

eDem TODAİE eDevlet Merkezi

ISO/IEC 27001
DENETİM VE BELGELENDİRMESİ

OGÜN KÖSE
KALİTEST BELGELENDİRME
GENEL MÜDÜRÜ

İçindekiler

Tanımlar

- **Kuruluş (organizasyon):** Düzenlenmiş sorumlulukları, yetkileri ve ilişkileri olan insanlar ve tesisler grubu
- **Belgelendirme kuruluşu:** Belirlenen standartlara veya teknik düzenlemelere uygunluğun belgelendirmesini yapan kuruluş
- **Akreditasyon:** Laboratuarların, muayene ve belgelendirme kuruluşlarının ulusal ve uluslararası kabul görmüş teknik kriterlere göre değerlendirilmesi, yeterliliğinin onaylanması ve düzenli aralıklarla denetlenmesi

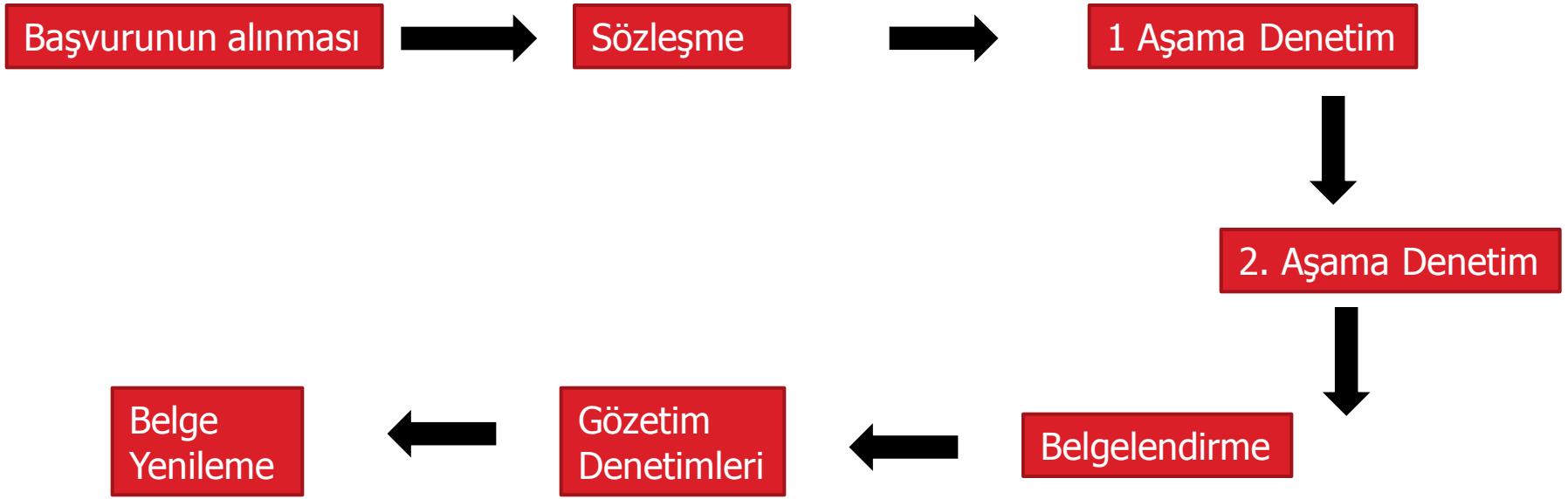
Tanımlar

- **Denetim (tetkik):** Denetim kriterinin tam olarak karşılandığının tespiti ve denetim delillerinin elde edilmesi amacı ile uygulanan sistematik, bağımsız ve dokümante proses
- **Denetçi:** Yeterli kalifikasyona sahip ve kalite sisteminin tümünün veya bir kısmının denetimin gerçekleştirebileceği onaylanmış kişi
- **Baş denetçi:** Yeterli kalifikasyona sahip ve kalite sistem denetimini yönetmesi onaylanmış kişi

Tanımlar

- **1 taraf denetim:** Birinci Taraf (İç) denetimler eğitimli iç denetçiler tarafından firmanın kendi yönetim sistemini değerlendirme amacı ile yapılır.
- **2.taraf denetim:** İkinci taraf denetimler firmada müşteri tarafından gerçekleştirilir. Denetimler bir sözleşmenin veya gelecekte yapılacak olan bir sözleşmenin şartları doğrultusunda yapılır.
- **3.taraf denetim:** Üçüncü taraf denetimler tanınmış bir standardın şartları doğrultusunda firmada bağımsız bir kuruluş tarafından gerçekleştirilir.

Belgelendirme Genel İş Akışı



Başvurudan önce yapılması gerekenler…

- Bu aşamada gerekli bilinçlendirme, iç denetçi, dokümantasyon ve diğer eğitimlerin alınması
- BGYS'nin kapsamının ve varsa hariç tutmaların belirlenmesi
- BGYS politikasının oluşturulması
- Risk analizinin yapılması (Risk tanımlama, çözümleme, derecelendirme, risklerin işlenmesi için seçenekleri tanımlama ve derecelendirme, risklerin işlenmesi için kontrol amaçları ve kontrolleri seçme, artık risk onayı ve işletme)

Başvurudan önce yapılması gerekenler…

- Uygulanabilirlik bildirgesi hazırlanması
- BGYS'nin uygulanması ve işletilmesi
- BGYS'nin izlenmesi ve gözden geçirilmesi
- BGYS'nin devamlılığının sağlanması ve iyileştirilmesi
- İç denetimlerin yapılması
- Yönetimin gözden geçirilmesi
- DÖF'lerin uygulanması
- Ek A'daki kontrollerin uygulanması ve etkinliğin ölçümü

Başvurudan önce yapılması gerekenler…

- ISO 27001 standardına göre dokümante edilmesi gerekenler;
  - BGYS politikası, amaç ve hedefleri
  - Kapsamı
  - BGYS'ni destekleyici prosedür ve kontroller
  - Risk değerlendirme metodunun tanımı
  - Risk değerlendirme raporu
  - Risk işleme planı
  - Kuruluşun kendi BGYS proseslerinin kontrolü için ihtiyaç duyacağı dokümante prosedürler
  - Kayıtlar
  - Uygulanabilirlik bildirgesi

Başvuruda istenen bilgiler..

- Firma unvan bilgileri
- Adres bilgileri (Çok işletmeli kuruluşlar için belgelendirmeye tabi tüm adresler)
- Çalışan sayısı
- Kapsam
- Hariç tutulan maddeler
- Daha önce alınmış olan sertifika bilgisi
- Kullanıcı sayısı
- Sunucu Sayısı
- Workstation + PC + laptop sayısı
- Network ve şifreleme teknolojisi
- Servis seviyesi anlaşmaları (SLA)nın önem derecesi
- Kapsam içerisinde yer alan faaliyetler ile ilgili olarak alınması gereken yasal izin ve onayları

Denetim Süresinin Belirlenmesi

ÇALIŞAN SAYISI	BELGELENDİRME DENETİM ZAMANI (denetçi/gün)
1-10	5
11-25	7
26-45	8.5
46-65	10
66-85	11
86-125	12
126-175	13
176-275	14
276-425	15
426-625	16.5
626-875	17.5
876-1175	18.5
1176-1550	19.5
1551-2025	21
2026-2675	22
2676-3450	23
3451-4350	24
4351-5450	25
5451-6800	26
6801-8500	27
8501-10700	28
>10700	Yukarıya benzer arttırılır

Risk Seviyesinin Belirlenmesi

- BGYS Komplekslik seviyesi yüksek, orta, düşük olarak 3 kategoriye ayrılmıştır. Komplekslik seviyesi ISO/IEC 27006-2 Tablo A.1: BGYS Komplekslik kriterlerine göre belirlenir.
- Yüksek kategorideki firmaların denetim süreleri azaltılmaz.
- Orta kategorideki firmaların denetim süreleri yukarıda verilmiş denetim süresini arttırmayı/azaltmayı etkileyen faktörler dikkate alınarak artırılabilir veya azaltılabilir.
- Düşük kategorideki firmaların denetim süreleri önemli bir arttırıcı faktör yoksa azaltılabilir.

Denetim Süresinin Hesaplanması

- Denetim süresi toplam sahadaki denetim süresinin %70'inden daha az olamaz (Saha denetimi süresi en fazla %30 azaltılabilir).
- Tetkik zamanını azaltan faktörler bir araya gelse de, belgelendirme tetkiki için belirlenen zaman bu faaliyetlerin etkisiyle toplam olarak %30'dan fazla azaltılmamalıdır
- Tetkik için ayrılan toplam zaman içinde planlama, doküman gözden geçirme (1. Aşama) ve rapor yazma faaliyetleri, Tabloda belirlenen toplam sürenin %30'undan fazla yer tutmamalıdır.
- Gözetim tetkikleri için belgelendirme tetkiki için ayrılan sürenin yaklaşık 1/3'ü yeniden belgelendirme tetkikleri için 2/3'ü ayrılmalıdır. Bu süreleri arttırabilecek veya azaltabilecek faktörler varsa Baş Denetçi tarafından dikkate alınmalı ve kayıt altına alınmalıdır.

Denetimin Gerçekleştirilmesi

- Denetim iki aşamadan oluşur.

  Birinci aşama:

- Formal denetimin birinci aşamasıdır. Bu aşamada belgelendirme v.s tavsiye kararı verilmez, sadece 2. aşama denetimi için yönetim sistemi uygulamalarının hazır olup olmadığını değerlendirmek üzere ön hazırlık mahiyeti taşır. BGYS denetimleri için 1. Aşama her zaman yerinde yapılır.

1. Aşama Denetiminde incelenen konular…

- BGYS Kapsam Değerlendirme
- Risk Yönetim Süresi
- Politika
- Süreçler
- Dokümante Prosedürler
- Uygulanabilirlik Bildirimi
- Varlık envanteri,
- Yasal ve mevzuat gerekliliklerinin belirlenmesi,
- Bilgi Güvenliği Organizasyonu, Güvenlik rol ve sorumlulukları

1. Aşama Denetiminin Amacı

- Müşterinin sistem dokümantasyonunun denetlenmesi
- Kuruluşa ait yerlerin ve lokasyona özgü koşullarının değerlendirilmesi ve 2.aşama denetim hazırlıkları için kuruluş personeli ile görüşmelerin yapılması,
- Kuruluşun statüsünün ve standard şartlarını kavrayışının gözden geçirilmesi(özellikle uygulanan yönetim sisteminin işletilmesinin, performansının ve önemli yönlerinin, proseslerinin gözden geçirilmesi)
- Yönetim sisteminin kapsamı, prosesler, kuruluşun yeri(lokasyon),yasal düzenlemeler ile ilgili gerekli bilgilerin toplanması,

1. Aşama Denetiminin Amacı

- İkinci aşama denetim için gerekli kaynakları gözden geçirmek ve 2. aşama denetimin detayları ile ilgili olarak müşteri kuruluşla anlaşma sağlamak,
- Müşteri kuruluşun yönetim sistemi ile ilgili yeterli bilginin kazanılmasını takiben, ikinci aşama denetimin planlanmasına odaklanmak,
- Müşterinin iç denetimlerini ve yönetim gözden geçirmelerini etkin bir şekilde planlayıp gerçekleştirdiğinin ve yönetim sisteminin uygulama seviyesinin yeterliliğinin belirlenmesi ile müşterinin ikinci aşama denetim için hazır olup olmadığının değerlendirilmesi, amacıyla gerçekleştirilir.

Süre…

- 1. Aşama denetimleri; toplam denetim süresinin **%30'unu** aşmayacak şekilde planlanmalıdır.

Denetim Planının Oluşturulması

- Denetim planı firmanın başvuru kapsamını karşılayacak şekilde olmalıdır,
- En az 8 saat / gün olmalıdır
- BGYS için toplam denetim süresine planlama ve rapor yazma faaliyetleri dahildir ve bu faaliyetler saha denetimi süresini toplam denetim süresinin %70'inden daha aza düşürmeyecek şekilde planlanır.
- Standardın tüm maddelerini kapsamalıdır,
- Mantıksal bir akış izlemelidir (genelden özele doğru)

Denetim Planının Oluşturulması

- Firmanın işleyişine uygun olmalıdır, (örneğin çalışma saatleri, öğle araları v.s)
- Denetlenen içinde yol gösterici olmalıdır,
- Tüm denetim ekiplerini kapsayacak şekilde olmalıdır,

  - ***Firmanın denetçiye ve plana itiraz etme hakkı bulunmaktadır***

2. Aşama Denetiminin Amacı

- Müşteri kuruluşun kendi politikası, amaçları ve prosedürlerine,
- BGYS'nin tüm ISO/IEC 27001 gereklilikleri ve kuruluşun politika ve amaçlarına uygunluğunu doğrulamak

2. aşama denetiminin genel başlıkları

- Açılış toplantısı, gündemin eksiksiz sunulması önemli
- Standarda uygunluk için objektif delillerin toplanması (örnekleme metoduyla)
  - Sorumlu kişilerle görüşmeler yaparak
  - Uygulama kayıtlarının incelenmesi ile
  - Gözlemleyerek
- Denetim heyetinin ara ve son değerlendirmelerini yapması
- Uygunsuzluk varsa, uygunsuzluk raporlarının düzenlenmesi
- Denetim raporunun tamamlanması
- Kapanış toplantısı, gündemin eksiksiz ve sırasına uygun sunulmalıdır. Tartışma gerekebilecek konular en son sunulmalıdır.

Uygunsuzluk

- **MAJOR:** standart şartlarının tamamen karşılanmaması veya sistemin çökmesine sebep olabilecek eksik uygulamalar. Belirli sayıda minör hatanın toplam etkisinin sistemi çökertecek nitelikte olması.
- **MİNOR:** sistemi çökertmeyecek nitelikteki eksik/yanlış uygulamalar.
- **GÖZLEM:** minör uygunsuzluk tanımlanacak şekilde açık olmayan veya ilgili standarda refere edilemeyen, ilerde minör uygunsuzluk olabilme riski taşıyan faaliyetler.

Uygunsuzluk

- Minör uygunsuzluk raporunda kaydedilen düzeltici faaliyetle belgelendirme tavsiye edilir.
- Şu kadar minör bir majör (örnek 7 minör = 1 majör) eder diye herhangi bir standart / kural yoktur.
- Uygunsuzluklarla ilgili muhakkak müşteri teyidi alınmalıdır.
- Uygunsuzluklar muhakkak açık bir şekilde objektif delillerle desteklenmelidir.
- Gözlemler açık ifade edilmelidir, minör uygunsuzluk statüsünde olmamalıdır.

Denetim sonunda uygunsuzluk var ise;

- Bir majör uygunsuzluk varsa, kuruluş kalite yönetim sisteminin belgelendirilmesi tavsiye edilemez.
- Tüm uygunsuzluklar kapatılmadan ve belgelendirme kuruluşu tarafından kuruluş yerinde veya ofiste doğrulanmadan belgelendirme yapılamaz.
- Uygunsuzluk major ise takip denetimi gerekir.

Denetimde Uygunsuzluk Yazılması Durumunda Yapılması Gerekenler…

Durum	***Firmanın yapması gereken***	***Baş denetçinin yapması gerekenler***
Minör uygunsuzluk	**Uygunsuzluğun tekrarını engelleyecek ve kök sebebini ortadan kaldıracak şekilde düzeltici faaliyet planlamalı, uygulamalı ve başlatılan *düzeltici faaliyetin* amacına ulaşıp ulaşmadığını doğrulamalıdır.**	**Firma tarafından belirlenen düzeltici faaliyetin kabul edilebilirliğinin kontrolü ve sonraki gözetim denetiminde uygulama delilleri kontrol edilmelidir.**
Majör uygunsuzluk	**Uygunsuzluğun tekrarını engelleyecek ve kök sebebini ortadan kaldıracak şekilde düzeltici faaliyet planlamalı, uygulamalı ve başlatılan *düzeltici faaliyetin* amacına ulaşıp ulaşmadığını doğrulamalıdır.**	**Firma tarafından belirlenen düzeltici faaliyetin kabul edilebilirliğinin kontrolü ve uygulama sonucu çıkan objektif delili takip denetimi yaparak doğrulamalıdır.**

Belgelendirme Kararının Verilmesi

- Raporun eksiksiz doldurulup doldurulmadığı, belgelendirme kapsamı, denetim planının uygunluğu, denetim bulgularının yeterliliği, tespit edilen uygunsuzlukların anlaşılır olması ve kapanmış olması açısından, Belgelendirme Müdürü gözden geçirme yaparak karar verir.
- Başdenetçi belgelendirmeye karar veremez sadece tavsiyede bulunur.
- Belgelendirme kararının denetim heyetinin tavsiye kararından farklı olması durumunda, ret kararının gerekçesi Belgelendirme Müdürü tarafından yayınlanır.
- Denetimi gerçekleştiren belgelendirmeye karar veremez.
- Belgelendirme kararı belgelendirme kuruluşunun sorumluluğundadır, Hiçbir zaman taşere edilemez.

Gözetim Denetimleri

- Belgelendirme kuruluşu belgelendirdiği firmanın risk grubu dikkate alınarak gözetim denetimi planlamalıdır.
- Yılda en az bir kez yapılmalıdır. (Aşama 2 tetkikinin son günü esas alınarak hesaplanır.)
- Belgelendirme denetimi ile aynı prosedür kullanılmalıdır
- Belgelendirme denetiminin en az 1/3'ü zaman ayrılmalıdır
- Bir önceki denetimde belirlenen uygunsuzluklar için düzeltici faaliyetlerin doğrulanması yapılmalıdır
- Logo kullanımı kontrol edilmelidir.
- Tüm sistem 2 yıl içerisinde firma ilgili Yönetim Sisteminin tüm faaliyetleri denetlenmelidir.

Gözetim Denetimleri

- ***BGYS sisteminin devamlılığı***
  - Yönetim gözden geçirme
  - İç denetimler
  - DÖF'ler
  - İlgili dış taraflarla iletişim
  - Doküman sistemindeki değişiklikler
  - Değişen prosesler-alanlar
  - 27001'in seçilen maddeleri
  - Politikanın uygulanma etkinliği
  - BGYS'nin yasal düzenlemelere uygunluğunun periyodik olarak değerlendirilmesi gözden geçirilmesi

Belge Yenileme Denetimi

- Belge yenileme denetimi her 3 yılda bir yapılır.
- Standardın tüm maddelerini kapsayacak şekilde gerçekleştirilir.
- *Belgelendirme denetiminin en az 2/3'ü zaman ayrılmalıdır*
- Belge yenileme denetimlerinde aşağıdaki hususlar dikkate alınır:
- İç ve dış kaynaklı değişiklikler ışığında ışığında, kendi bütünlüğü içerisinde yönetim sisteminin etkinliği,
- Yönetim sistemi etkinliğinin belgelendirme kapsamıyla sürdürülegelen ilgisi ve uygulanabilirliği,
- Toplam performansı arttırmak için yönetim sisteminin etkinliği ve iyileştirilmesini sürdürmeye yönelik gösterilmiş taahhüt,
- Yönetim sisteminin işletilmesinin organizasyonun politika ve hedeflerine ulaşmasında katkı sağlayıp sağlamadığı

Sertifika

Firma Unvan ve Adres Bilgileri

Kapsam

Uygulanabilirlik Bildirgesi

Kalitest

SERTİFİKA–CERTIFICATE OF REGISTRATION

Bu sertifika aşağıdaki kuruluşa
This certificate has been awarded to the company

Uygulanmakta olan bilgi güvenliği yönetim sisteminin
To certify that the implemented information safety management system complies with

ISO/IEC 27001:2005

Standardına uygunluğunu belgelendirmek amacı ile aşağıdaki kapsamda verilmiştir.
For the activities described below

MOBİL RADYO ŞEBEKE PROJELENDİRME, MONTAJ, BAKIM VE ARIZA GİDERME HİZMETLERİ

MOBILE RADIO NETWORK, SETUP DESIGN, MAINTENANCE AND REPAIR SERVICES

SOA Rev 02

Kalitest Belgelendirme ve Eğitim Hizmetleri Ltd. Şti. :

TÜRKAK
Bilgi Güvenliği Y.S.
TS EN ISO/IEC 17021
AB-0017-YS

İmza :
Signed

Bu sertifikanın geçerliliğini 4775682 seri numarasıyla www.kalitest.com.tr adresinden doğrulayabilirsiniz.
Please verify the validity of this certificate with the serial number of 4775682 from the web site of www.kalitest.com.tr

KALİTEST BELGELENDİRME VE EĞİTİM HİZMETLERİ LİMİTED ŞİRKETİ
Merkez: Akatlar Mahallesi Hare Sokak. 2. Söltaş Evleri G-10 No:9 1. Levent / İSTANBUL Tel: 0212 269 37 41–42–43 Faks: 0212 269 37 44
Ankara Şube: Armada Alışveriş ve İş Merkezi Eskişehir Yolu No:6 Kat:12 Söğütözü / ANKARA Tel: 0312 295 62 10 Faks: 0312 295 63 53
İzmir Şube: Cumhuriyet Bulvarı Megapol Apartmanı No:209 Kat:5 Alsancak / İZMİR Tel: 0232 463 76 03 Faks: 0232 464 17 08

Sertifika No: Certificate No K-BG-1005
İlk Belge Tarihi : First Registration Date 08.07.2010
Belge Periyodu : Period of registration : 3 yıl / 3 years
Sertifika Tarihi : Certificate Date 08.07.2010
Bitiş Tarihi : Expiry Date 08.07.2013

Bu sertifikanın geçerliliği firmanın KALİTEST Sertifika Yönetmeliğine uyumuna ve yılda en az bir kez yapılacak gözetim denetimlerinin başarılı geçmesine bağlıdır.

The validity of this certificate depends on the company's conformity with KALİTEST Certificate Regulations and the result of the surveillance audits which will be carried out at least once in a year.

Katma Değer Denetim …

- Denetçilerin tavsiyede bulunması,
- Denetçilerin işin nasıl yapılacağını firmaya göstermesi,
- Denetçilerin denetim esnasında firmaya eğitim vermesi,
- Denetimden sonra aynı denetçinin firmaya danışmanlık hizmeti vermesi,
- Denetimde varsa uygunsuzlukların raporlanması yerine sözlü uyarması,

DEĞİLDİR

Katma Değer Denetim …

Katma değer denetimde;

- Denetim planı doğru olmalıdır,
- Denetim planı etkin uyulmalıdır,
- Denetim ekibi yeterli olmalıdır,
- Kritik ve önemli noktalar muhakkak ziyaret edilmeli ve yeterli zaman ayrılmalıdır
- Sistemin uygulanıp uygulanmadığını gösterir nitelikte doğru örnekleme yapılmalıdır
- Varsa uygunsuzluklar formal olarak raporlanmalıdır
- Denetim dili firmanın kolay anlayabileceği nitelikte olmalıdır

Belgelendirme Kuruluşu Prensipleri

- Tarafsızlık,
- Yeterlilik,
- Sorumluluk,
- Açıklık,
- Gizlilik,
- Şikayetlerin çözümlenmesi

Belgelendirme Kuruluşu Seçerken Dikkat Edilmesi Gereken Konular…

- Akreditasyona sahip olup olmaması,
- Dış akreditasyona sahip ise bu akreditasyonun Türkiye'yi kapsayıp kapsamadığı,
- Sertifikanın üçüncü taraflar tarafından kabul görüp görmediği,
- Belgelendirme kuruluşunun görevlendirdiği denetçilerin yetkinliği,
- Tarafsızlık ve bağımsızlığın sağlanması

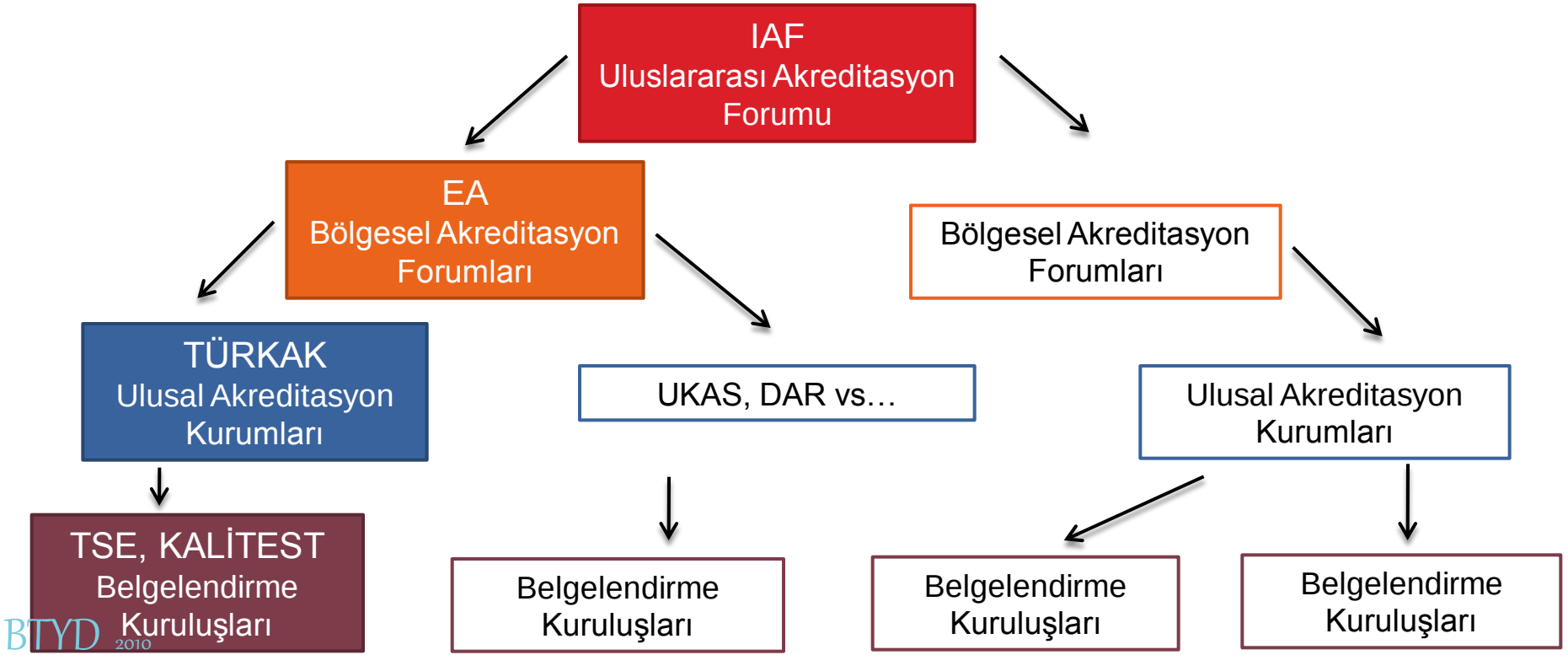
Belgelendirme Kuruluşu Seçerken Dikkat Edilmesi Gereken Konular…

- Danışmanlık ve belgelendirme ilişkisi (ISO 17021 şartları)
- Denetim ekibinin (baş denetçi ve denetçilerin) denetlenen kuruluştan bağımsız olmalıdır.
- Belgelendirme kuruluşunun danışmanlık şirketi ile çıkar ilişkisinin olmaması gerekir (komisyon alma verme gibi)

Akreditasyon

- Belirli bir konuda yetkilendirme
- Uluslar arası tanınabilirlik, Belgelendirme etik ve kurallarının ciddiyetle uygulanması ve güvenilirlik
- Ülkeler arası farklılıkların ortadan kaldırılabilmesi ve aynı standardın uygulamasını her yerde asgari müştereklerde aynı olabilmesi için uluslar arası akreditasyon kuralları ve birlikleri vazgeçilmezdir

Akreditasyon Sistematiği



TÜRKAK…

- Türk Akreditasyon Kurumu (TÜRKAK), laboratuar, belgelendirme ve muayene hizmeti veren yurt içi ve yurt dışındaki Uygunluk Değerlendirme Kuruluşlarını akredite etmek, bu kuruluşların belirlenen ulusal ve uluslararası standartlara göre faaliyetlerde bulunmalarını ve ürün/hizmet, sistem, personel ve laboratuvar belgelerinin ilgili taraflar nezdinde güvenilir hale gelmesini ve böylece ulusal ve uluslararası alanda kabul edilebilirliğini temin etmek amacıyla 4 Kasım 1999 tarihli Resmi Gazete'de yayımlanan 4457 sayılı Kanun'la kurulmuştur.
- Kurum, 2001 yılı içinde akreditasyon hizmetini sunmaya başlamıştır.

TÜRKAK…

- TÜRKAK Türkiye'de tek yetkili akreditasyon kurumudur. IAF (International Accreditation Forum) ile MLA (Multi Lateral Agreement) anlaşması vardır. TÜRKAK akrediteli belgelerin dünyada tanınması anlamındadır.
- Türkiye'de üretim / hizmet sunan bir firmanın TÜRKAK akrediteli belgelendirme kuruluşundan belge alması, uluslar arası akreditasyon kurallarının istediği bir durumdur. Çünkü belgeli firmadan hizmet alan tüketici, belgeyi veren kurum, akreditasyon kurumu vb. ilgili kuruluşlar zincirinin güven ve izlenebilirliği sağlanmalıdır.

ISO 27001 denetçi seçme ve atama kriterleri

	Temel Öğretim	Denetçi Eğitimi	Tecrübe		Denetim Tecrübesi
			Toplam iş	Yönetim Sistemi	
Denetçi	En az yüksek okul veya üniversite mezunu ***Söz konusu kişinin sektöre uygun yüksek okul veya üniversite öğretim varsa iş tecrübesi şartı 1 yıl düşürülebilir.***	5 günlük denetçi eğitimi ***BGYS denetimleri ve denetim yönetimi kapsamını içeren 5 günlük denetçi eğitimi.***	4 yıl ***Bilgi Teknolojisi ile ilgili en az dört yıllık tam zamanlı iş deneyimi. Bunun iki yılı bilgi güvenliği ile ilgili bir görevde olmalı. Deneyim güncel olmalıdır.***	2 yıl	Yetkin baş denetçinin yönlendirmesi ve rehberliğinde **4 tam** denetim en az **20 gün** Denetimler ardışık son 2 yıl içerisinde tamamlamış olmalıdır ***Tam denetim belgelendirme veya belge yenileme denetimi anlamındadır. Doküman inceleme, risk analizi, denetim uygulaması ve raporlama bu süreye dahildir.***
Baş denetçi	En az yüksek okul veya üniversite mezunu	5 günlük denetçi eğitimi	4 yıl	2 yıl	Yetkin baş denetçinin yönlendirmesi ve rehberliğinde denetçi rolü ile **3 tam** denetimde görev almak Denetimler ardışık son 2 yıl içerisinde tamamlamış olmalıdır

ISO 27001 denetçi seçme ve atama kriterleri

Denetçiler aşağıdaki konularda yetkin olmalıdır;

- Denetim planlama ve programlama,
- Denetim tipi ve yöntemleri,
- Denetim riski,
- Karmaşık işlemlere geniş çerçeveden bakabilme ve büyük kuruluşlardaki her bir birimin görevini algılayabilme,
- Bilgi güvenliği proses analizi,
- Sürekli iyileştirme,
- Bilgi güvenliği iç denetimi

ISO 27001 denetçi seçme ve atama kriterleri

Denetçiler aşağıdaki konularla ilgili yasal gereklilikleri bilmelidir.

- Entelektüel varlık,
- Kuruluş kayıtlarının içeriği, korunması ve muhafazası,
- Veri korunması ve gizliliği,
- Şifreleme kontrolleri yönetmelikleri,
- Anti- terör,
- Elektronik ticaret,
- Elektronik ve sayısal imza,
- İşyeri gözetimi,
- Verilerin izlenmesi ve telekomünikasyon engellemesi (ör: e-posta),
- Bilgisayarlı kötüye kullanma,
- Elektronik kanıt toplanması,
- Penetrasyon deneyleri,
- Ulusal ve uluslar arası Sektörel şartları (ör: bankacılık)

ISO 27001 denetçi seçme ve atama kriterleri

Denetçiler aşağıdaki yönetsel konularda yetkin olmalıdır

- Bilgi güvenliği risklerinin ele alınması,
- ICT (bilgi ve telekomünikasyon teknolojileri) dış kaynak kullanımı ile ilgili güvenlik riskleri,
- Tedarik zinciri bilgi güvenliği riskleri

Denetçinin Pozitif Özellikleri

- Profesyonel
- Gözlemci
- Tarafsız
- Disiplinli
- Bağımsız
- Diplomatik
- Dikkatli
- İyi dinleyici
- Sabırlı
- Objektif
- Analitik
- Etik

Denetçinin Negatif Özellikleri

- Hazırlık ve planlamada yetersizlik
- Çok Katı Olmak
- İnatçı
- Kötü iletişim
- Tartışmacı
- Kararsız
- Kolay etkilenen
- Ofiste kalmak
- Zamanı kötü kullanmak
- Karar vermede güvensiz

Teşekkürler….

ogun@kalitest.com.tr

BTYD 2010

www.btyd.org