TARAFSIZLIĞIN YÖNETİLMESİ PROSEDÜRÜ

1. AMAÇ:

Bu prosedürün amacı; Şirketimizde uygunluk değerlendirme süreçlerinde gizlilik, tarafsızlık ve bağımsızlığın yönetilmesi ile tüm kuruluşlara eşit ve tarafsız hizmet verebilmek amacı ile uygunluk değerlendirme faaliyetlerinde eşit ve tarafsız hizmetin gerçekleşmesine engel olabilecek risklerin belirlenmesi, değerlendirmesi, kontrol edilmesi, önlenmesi ve/veya en aza indirilmesidir.

2. UYGULAMA DETAYI:

2.1 TARAFSIZLIĞIN YÖNETİLMESİ

2.1.1. Gizlilik, Bağımsızlık ve Tarafsızlık Politikası

CyberCert bünyesi içinde belgelendirme faaliyetlerinin yapılmasında, tarafsızlığın öneminin anlaşıldığını, çıkar çatışmasının yönetildiğini ve yönetim sistemi belgelendirme faaliyetlerinin objektifliğinin güvenceye alındığının sağlandığını belirten bir kuruluş politikasına sahiptir.

Şirketimiz hiçbir şirket, kurum, kuruluş, varlık veya kişiye bağımlı değildir. Tek işi uygunluk değerlendirme, eğitim ve test hizmetlerini sunmaktır.

CyberCert Yönetimi, Halka web sitesi kanalı ile açık Tarafsızlık ve Bağımsızlık Taahhüdü, Belgelendirme programları, personel ve müşterileri ile yaptığı sözleşmeler ile sır tutmayı, bağımsızlığı ve tarafsızlığı taahhüt eder.

Ayrıca kullanmakta olduğu portallar vasıtası ile objektif ve şeffaflık ilkesi ile sır tutmayı, bağımsızlığı ve tarafsızlığı taahhüt eder.

Yine kullanmakta olduğu portallar başvuru, planlama ve denetim aşamalarında yine personel ve müşterilerden aldığı taahhütler ile de sır tutmayı, bağımsızlığı ve tarafsızlığı taahhüt eder.

Uygunluk değerlendirme faaliyetlerinde yer alan tüm şirket personeli (şirket içi veya şirket dışı) imzaladıkları gizlilik, bağımsızlık ve tarafsızlık ilkelerini iş sözleşmeleri ve hizmet alım sözleşmeleri ile sır tutmayı, bağımsızlığı ve tarafsızlığı taahhüt edecek bir şekilde hareket eder.

Yine gizlilik, bağımsızlık ve tarafsızlık ilkelerini içeren imzaladıkları kişisel taahhüt ile sır tutmayı, bağımsızlığı ve tarafsızlığı taahhüt edecek bir şekilde hareket eder.

Yine kullanmakta oldukları portallar ile başvuru, planlama ve denetim aşamalarında verdikleri gizlilik bağımsızlık ve tarafsızlık ilkelerini içeren taahhütler ile de sır tutmayı, bağımsızlığı ve tarafsızlığı taahhüt ederler.

Ayrıca her belgelendirme kararlarında, yılda en az bir defa yapılan iç denetimler (müşteri ve denetçi dosya kontrolleri, finansal veri kontrolleri ile) ve yönetim gözden geçirme toplantılarında tarafsızlık ilkesi gözden geçirilir.

Şirketimiz belgelendirdiği kuruluşların iç tetkiklerini yapmayacaktır. İç tetkikini gerçekleştirdiği kuruluşların da belgelendirmesini takip eden 2 yıl içerisinde gerçekleştirmeyecektir.

Çıkar çatışmasının olmamasını sağlamak için, yönetimde yer alanlar dâhil olmak üzere yönetim sistem danışmanlığı sağlayan personel, aynı yönetim sistemi için yönetim sistem danışmanlığına son iki yıl içerisinde katılmışlar ise, belgelendirme prosesinde yer alamazlar. Bu husus yapılan denetim görevlendirmelerde, iş ve hizmet alım sözleşmelerinde yerine almıştır.

Şirketimiz ve/veya olası durumda tüzel kişiliğinin bir parçası yönetim sistemleri konusunda danışmanlık hizmeti sunmaz. Şirketimiz belgelendirme yaptığı konular da tüzel kişiliğinin bir parçası ve organizasyonel olarak kontrolü altında olan bir birime herhangi bir danışmanlık faaliyetinde bulunmaz.

CyberCert'in üst yönetimi farklı tüzel kişiliğin kurumsal danışmanlık faaliyetinde yer almaz.

CyberCert, uygunluk değerlendirme süreçlerindeki tüm sorumluluğu ilgili taraflar ile yaptığı sözleşmelerle (taşeron, müşteri, personel, komite vb.) kendi sorumluluğuna alır.

CyberCert, Uygunluk değerlendirmenin karar süreçlerini hiçbir şekilde taşere etmez. ilgili personel yaptığı sözleşmelerle (iş sözleşmeleri, bireysel hizmet alım sözleşmeleri) kendi sorumluluğuna alır.

CyberCert, akreditasyon kapsamı dahilinde müşterilerine uygunluğu değerlendirilen sistemlerin ve ögelerin kurucusu, tasarımcısı, imalatçısı, tedarikçisi, montajcısı, satın alıcısı, sahibi, kullanıcısı veya bakımcısı nede bu kesimlerin yetkili temsilcisi olacak fiyat teklifi sunmaz veya bu konularda hizmet sunmaz ve danışmanlık sağlamaz.

Farklı bir tüzel kişilik adı altında CyberCert'in yönetimindeki personeli, test/muayene/denetim/değerlendirmedeki personeli, ve Uygunluk değerlendirme karar, teknik onay personeli uygunluğu değerlendirilen sistemin ve ögelerin kurucusu, tasarımcısı, imalatçısı, tedarikçisi, montajcısı, satın alıcısı, sahibi, kullanıcısı, bakımcısı bu kesimlerin yetkili temsilcisi olacak şekilde hizmet sunarsa veya danışmanlık sağlarsa, uygunluğu değerlendirilen o sistemin ve ögelerin test / muayene / denetim / değerlendirmelerinde ve karar sürecinde yer alamaz.

CyberCert olası durumda herhangi bir şubesine, yan kuruluşuna, ortağı olduğu bir şirketine yoktur belgelendirme hizmeti verilmeyecektir.

Şirketimiz, çıkarlarının olduğu sektörlerde veya konularda (tamamen şirketimize bağlı bir kuruluşun belgelendirme istemesi gibi tarafsızlığa kabul edilemez bir tehdit ortaya çıkması durumunda) belgelendirme yapmaz. Ortaklıklarının bulunduğu tüzel kişiliklere, çıkar çatışmasına yol açacak veya kendi faaliyet göstermiş olduğu sektör ve konularda belgelendirme faaliyetinde bulunmaz.

Şirketimiz herhangi bir danışmanlık kuruluşu ile iş birliği veya ortak çalışma içerisinde değildir. Danışman olup denetçi ve karar havuzunda yer alan personel danışmanlık hizmeti verdikleri kuruluşlara denetim hizmeti ve belge kararı vermemektedir. Firmamız denetçi havuzundaki tüm personel ile bu konuda sözleşmelerini imzalamış, aynı zaman da her denetim öncesi bu husus ile ilgili

denetçi, uzmanlardan taahhütname alınmaktadır. Risk analizi talimatında danışman firmalardan kaynaklanabilecek riskler analiz edilmiştir.

Belgelendirme faaliyetlerinin herhangi bir aşaması herhangi bir yönetim sistem danışmanlık firmasına taşere edilmez.

Şirketimiz, kuruluşlara tarafsızlığı etkilemeden, çıkar çatışması yapmadan seminerler, özel çözüm önerileri dışında genel bilgilerin verilmesi, eğitimler, belgelendirme prosedürleri, ön tetkikler, akreditasyon kapsamı dışında bulunan harici standartlara ya da düzenlemelere göre ikinci ve üçüncü taraf denetimler sağlayabilir.

CyberCert Uygunluk değerlendirme şartlarına ilişkin eğitimler düzenlerse, eğitim sadece genel bilgileri kapsar, Uygunluk değerlendirmeye konu ögeye özel çözümler üretmez ve belge müşterisiyle birebir yürütülmez.

Danışmanlık niteliği kazanabilecek eğitim faaliyetlerinde bulunmaz. Sadece genel nitelikte sektöre ve/veya müşteri kuruluşa özgü çözümler içermeyen eğitimler organize eder ve gerçekleştirir. Tarafsızlık ilkesi paralelinde eğitimler ile ilgili faaliyetlere çeşitli sınırlandırmalar getirilmiştir. (Örn: eğitim süresi, programı ve benzeri.)

Verilecek eğitimler proseslerin veya sistemin gelişmesi için müşteriye özgü çözümler sağlamaması kaydıyla verilen genel bilgileri içerir. Bu bilgiler aşağıdakileri içerebilir:
- Belgelendirme kriterinin anlamının ve amacının açıklanması,
- Geliştirme imkânlarının belirlenmesi,
- İlgili teoriler, yöntemler, teknikler ve araçların açıklanması,
- İlgili iyi uygulama örneklerinden gizli olmayan bilgilerin paylaşımı,
- Tetkik edilen yönetim sistemlerinde yer almayan diğer yönetim hususları.

Ayrıca daha önceki 2 yılda kurumsal ya da personeli eğitim almış belgelendirme başvurusu yapan kuruluşta eğitim verdiği kişi sayısı 3'ü geçer ve/veya bu kişiler eğitim katılımcılarının %30'unu geçmiş olursa ilgili başvurunun gerekçesi ile birlikte reddini sağlar.

CyberCert, ilişkisinin olduğu farklı tüzel kişiliklerin faaliyetlerinin, Uygunluk değerlendirme faaliyetleri tarafsızlığını riske atmamasını sağlar.

Şirketimiz yönetim sistemleri tetkikini ve belgelendirmesini yapan diğer kuruluşların kalite yönetim sistemi belgelendirmelerini yapmaz. Diğer başka kuruluşların faaliyetinden kaynaklanan çıkar çatışmasına yol açan durumlardan sakınmaya yönelik tedbirlerini almaktadır. Risk Analizi Tablosunda değerlendirmeler yapılmıştır.

Şirketimiz hizmetleri veya faaliyetleri herhangi bir şekilde danışmanlık kuruluşu ile ilişkili imiş gibi satılamaz, pazarlanamaz. Şirketimiz herhangi bir başvuru sahibi kuruluşun yönetim sistemini, belirli bir kişi veya kuruluştan almış olduğu danışmanlık hizmeti veya iç denetim hizmeti sonucuna göre belgelendirmemektedir. Belgelendirme kararı sadece kendi denetçilerinin yapacağı denetimlerin sonucuna göre Yönetim Sistemleri Belgelendirme Karar Prosedürüne göre verilecektir. Şirketimiz bağımsızlığı tehlikeye düşürebilecek veya öyle imiş gibi anlaşılabilecek şekilde danışmanlık firmaları ile ilişki içerisine girmeyecektir. Danışmanlık firmalarının denetçilere ulaşımları Yönetim Kurulu Üyesi tarafından engellenecektir. Danışmanlık firmaları ile belgelendirme faaliyetleri için sözlü veya yazılı herhangi bir sözleşme yapılmaz.

CyberCert, müşteri tarafından belirli bir danışmanlık kuruluşu kullanıldığında, belgelendirmenin, daha basit, kolay, hızlı veya daha ucuz olacağını ifade veya ima etmez.

CyberCert'in faaliyetleri, herhangi bir aracı kuruluş tarafından Uygunluk değerlendirmenin daha kolay, hızlı ve ucuz olacağını ima ederek uygunluğu değerlendirilen ögelerin tasarımcısı, imalatçısı, tedarikçisi, montajcısı, satın alıcısı, sahibi, kullanıcısı veya bakımcısı nede bu kesimlerin yetkili temsilcisi hizmeti veren bir kuruluşun faaliyetleriyle bağlantılı olarak pazarlanmaz veya fiyat teklif sunulmaz.

Şirketimize gelen şikayet veya itirazın değerlendirilmesi sürecinde herhangi bir çıkar çatışmasının olmadığından emin olmak için uygunluğu değerlendirilen sistemin ve ögelerin kurucusu, tasarımcısı, imalatçısı, tedarikçisi, montajcısı, satın alıcısı, sahibi, kullanıcısı veya bakımcısı nede bu kesimlerin yetkili temsilcisi veya bir müşteri tarafından istihdam edilen personel (yönetim kapasitesinde çalışanlar dahil), CyberCert tarafından Uygunluk değerlendirme kararları alma ya da teknik onay veya istihdamın bitiminden sonraki iki (2) yıl içinde şikayet veya itirazın çözümünü incelemek veya onaylamak için kullanılmaz.

Şirketimiz bir belgelendirme kurumu olarak yapacağı tüm pazarlama, reklam ve tanıtım faaliyetlerini kendisi veya bir pazarlama ajansı aracılığı ile yapar. Bunun dışında özellikle yönetim sistem danışmanlığı yapan kuruluşların bu konu ile ilgili faaliyetleri gerekirse Yönetim Kurulu Üyesi tarafından hukuki tedbir alınarak engellenir.

Şirketimiz; yönetim, idari personel, komiteler, denetçi ve uzmanlarından kaynaklanabilecek ve tarafsızlığı tehlikeye atabilecek oluşumların (ticari, mali ve diğer baskılar gibi) olmamasına yönelik gerekli tedbirlerini risk analizi çalışmalarına göre yapmıştır.

Uygunluk Değerlendirme kuruluşu olarak müşterilerimizden ve tüm çalışanlarımızdan beklentimiz kendileri veya başka bildikleri kişiler ile ilgili bağımsızlığı tehlikeye düşürücü herhangi bir durum varsa bu durumu yönetimimize bildirmelidirler. Bu bilgiler tarafımızca kayıt altına alınmaktadır. Bu bilgiler daha sonra bağımsızlığı tehlikeye düşürücü bir risk olarak ele alınacak ve bu personel çıkar ilişkisi olmadığını ispatlayıncaya kadar belgelendirme faaliyetlerinde kullanmayacaklardır. Herhangi bir çıkar ilişkisine yer vermemek ve bağımsızlığın tehlikeye düşmemesi için belgelendirme prosesinin hiçbir aşamasında danışmanlık yaptığı bilinen kişi veya kuruluşa görev verilmez.

Bu durum özellikle, sözleşmeli çalışan dış kaynaklı denetçiler bir kuruluşa danışmanlık yapmış ise tehlike arz edecektir. Bu durumun oluşmaması için tüm dış kaynaklı denetçiler ile böyle durumları engelleyen sözleşmeler imzalanmıştır ve ayrıca her görevlendirmede de tekrar imzalanmaktadır.

Bağımsızlığı tehlikeye düşürebilecek veya öyle imiş gibi anlaşılabilecek her türlü duruma karşı Yönetim Kurulu Üyesi risk analizi ile tedbir alacaktır. Böyle bir duruma yol açan kişi, kuruluş veya taraflara karşı her türlü hukuki girişimde dahil faaliyet Yönetim

Kurulu Üyesi tarafından başlatılacaktır. Çıkar çatışmasının önlenmesi için ayrıca aşağıdaki faaliyetler tarafsızlığı etkilemeyecek şekilde yürütülmektedir;

Çeşitli yayınlar aracılığı ile genel olarak standardın nasıl yorumlandığı ve belgelendirme metodolojisinin ne olduğunun açıklanması faaliyetleri (web sitesinde, haber organlarında, v.b.) yapılabilmektedir. Müşteri talebi doğrultusunda denetim faaliyetleri yürütülmesi (tavsiye ve önerileri içermeyecek sadece uygunluk tespiti ve uygunsuzların raporlanmasını içerecek şekilde) hizmeti verilmektedir.

Denetimlerde katma değer sağlayacak şekilde uygunsuzlukların tespiti, olumlu ve olumsuz iyileştirme fırsatlarının gözlemlenmesi ve denetim raporunda ifade edilmesi gerekmektedir. Tavsiye niteliğinde iyileştirme önerileri verilmemesine dikkat edilir. Gözlemler iyileştirme fırsatlarını işaret etmek için raporlanır.

2.1.2. Tarafsızlık Risk Analizi

Şirketimiz devam eden kendi ilişkilerinden kaynaklananlar da dâhil olmak üzere, belgelendirmenin yapılmasından kaynaklanan, tarafsızlığı etkileyebilecek çıkar çatışması ihtimallerinin tanımlanması, analiz edilmesi, ele alınması, değerlendirilmesi, izlenmesi ve dokümante edilmesi için bu el kitabında, risk analizi ve değerlendirme prosedüründe ve risk analizi tablosunda belirtilen bir prosese sahiptir. Bu amaçla tarafsızlığı etkileyebilecek, çıkar çatışması ihtimallerini Risk Analizi Tablosu ile belirlemiştir. İlgili talimatta potansiyel tehditler, tehlikeler ve tehlikeyi bertaraf veya en aza indirebilecek tedbirler belirlenmiştir. Bunu ile birlikte en aza indirilmiş kalan riskler dokümante edilmiş ve üst yönetim tarafından kalan riskin kabul edilebilir risk olup olmadığı gözden geçirilip sonuçları dokümante edilmiştir. Dökümante edilen risk ister **CyberCert**'ten kaynaklansın ister diğer kişi, kuruluş veya yapılardan kaynaklansın, bütün potansiyel tehditleri kapsamaktadır.

CyberCert bu prosedür ve Risk Analizi Tablosu ile riskleri nasıl elimine etiğini veya kabul edilebilir seviyeye çektiğini açıklar.

CyberCert Risk değerlendirme prosesi, uygun ilgili taraflara danışılarak, şeffaflık ve umumi algı dahil tarafsızlığı etkileyen hususların tanımlanmasını kapsayacak şekilde belirlenmiştir. Uygun ilgili taraflarla danışma, tek bir tarafın baskın olmayacağı şekilde dengeli bir kurul yapısına sahiptir. Denetleme ve Tarafsızlık Kurulu çalışma usül ve esasları Komite ve Kurullar Prosedüründe belirtilmiştir.

Not 1 –Tehditlerin kaynakları; mülkiyet, yönetişim, yönetim, personel, paylaşılan kaynaklar, finans, sözleşmeler, eğitim, pazarlama ve satış komisyonunun ödenmesi veya yeni müşteri yönlendirmesi gibi diğer sebeplerle yapılan ödemeler olabilir.

Not 2 – İlgili taraflar; belgelendirme kuruluşunun personeli ve müşterilerini, yönetim sistemleri belgelendirilen kuruluşun müşterilerini, sanayi ticaret birliklerinin temsilcilerini, düzenleyici kamu kuruluşları veya diğer kamu temsilcilerini ya da tüketici kuruluşları dahil sivil toplum kuruluş temsilcilerini kapsayabilir.

2.1.3. Tarafsızlık Anlaşmaları

CyberCert Yönetimi, Halka web sitesi kanalı ile açık Tarafsızlık ve Bağımsızlık Taahhüdü imzalar,

Müşterileri ile sır tutmayı, bağımsızlığı ve tarafsızlığı içeren sözleşmeler imzalar ve portal üzerinden taahhütler alır.

CyberCert, komiteler dahil şirket içi veya şirket dışı çalışanları iş ve hizmet alım sözleşmeleri, kişisel taahhüt ve beyan ile sır tutmayı, bağımsızlığı ve tarafsızlığı taahhüt eder.

Yine kullanmakta olduğu portallar başvuru, planlama ve denetim aşamalarında yine personelden de sır tutmayı, bağımsızlığı ve tarafsızlığı içeren taahhütler alır.

CyberCert, şirket içi veya şirket dışı çalışanları, komite üyeleri ve tedarikçileri haricinde herhangi tarafla ilişkisi varsa, ilgili tarafla Gizlilik ve tarafsızlık sözleşmesi imzalar.

2.1.4. Çıkar Çatışması

Yönetim ve Personel

Kişiler aşağıdaki durumlar olduğunda Uygunluk değerlendirme kararında yada teknik onayda görevlendirilmez:

- Son 2 yıl içerisinde müşteri (resmi veya gayrı resmi) için çalışma
- Gelecekteki 12 ay içinde müşteri için çalışmaya başlamak için herhangi bir anlaşma veya fikri olması
- Son 2 yıl içerisinde müşteri için çalışma ilişkileri olması
- Müşterinin üst düzey yöneticileri ile yakın kişisel ilişkiler olduğunu ilan etmesi
- Son 2 yıl içerisinde uygunluğu değerlendirilen ögelerin tasarımcısı, imalatçısı, tedarikçisi, montajcısı, satın alıcısı, sahibi, kullanıcısı veya bakımcısı nede bu kesimlerin yetkili temsilcisi olması

Muhtemel bir çıkar çatışması belirlenirse, Uygunluk değerlendirme personeli ise ilgili Uygunluk değerlendirme süreci tekrar edilir, Karar personeli ise karar süreci tekrar edilir.
Çıkar çatışmasına konu personel hakkında risk analizi tablosu ve sözleşmelerindeki hüküm uygulanır.
Uygunluk değerlendirme personeli, Uygunluk değerlendirme kararlarını alırken fiili veya algılanan çıkar çatışmalarından kaçınmak için yerine getirilmesi gereken uygun hükümlerden sorumludur.
Tüm CyberCert personeli kendi kişisel veya kurumsal muhtemel çıkar çatışmalarının belirlenmesinden ve üst yönetimiz dikkatine sunulmasından sorumludur.
Tüm CyberCert personeli, CyberCert'e Çıkar Çatışması Kayıt Formu ile çıkar çatışmalarını bildirmekle sorumludur.
CyberCert her denetim için muhtemel çıkar çatışmalarını sözleşmelerindeki beyanları ve her denetim öncesi aldığı taahhüt uyarınca kontrol eder.

2.2. TARAFSIZLIĞA AİT RİSKLERİN ANALİZ EDİLMESİ DEĞERLENDİRİLMESİ VE YÖNETİLMESİ

2.2.1 Tanımlar

Tehlike: İnsanların yaralanması, hastalanması, malın veya malzemenin zarar görmesi, işyeri ortamının zarar görmesi veya bunların birlikte gerçekleşmesine sebep olabilecek potansiyel kaynak veya durum.

Tehlike Tanımlaması: Bir tehlikenin varlığını tanıma ve özelliklerini tarif etme prosesi.
Risk : Tehlikeli bir olayın meydana gelme olasılığı ile sonuçlarının bileşimi. (Risk = Olasılık x Etki).
Risk Değerlendirmesi: Riskin büyüklüğünü tahmin etmek ve riske tahammül edilip edilemeyeceğine karar vermek için kullanılan prosesin tamamı.
Katlanılabilir/Kabul edilebilir Risk: Kuruluşun, yasal zorunluluklara ve kendi İSG politikasına göre, tahammül edebileceği düzeye indirilmiş risk.

2.2.2. Tarafsızlık Prensibi

Risklerin yönetiminde en önemli unsur tarafsızlığın sağlanmasıdır. Tarafsızlık; gerçekliği anlaşılır ve objektifliğin varlığı fark edilir olması için yapılan her türlü uygunluk değerlendirme faaliyetlerinde sürekliliği ve güven sağlamak için tarafsızlık temel şartını gösterir takipler ve kayıtlar oluşturulmuştur.

Şirketimizde. Tarafsızlık aşağıdakilerin bir ya da birkaçı ile karakterize edilir;

- Objektiflik,
- Bağımsızlık,
- Yansızlık,
- Doğruluk,
- Açık fikirlilik,
- Tarafsızlık, uygunluk,
- Denge,
- Çelişkilerden kaçınma,
- Önyargıdan kaçınma,
- Kamuya açık olma,

Bu temel ilkeleri sağlamak amacı ile tarafsızlığı etkileyen riskler belirlenmesi, değerlendirilmesi, kontrol edilmesi, önlenmesi ve personel bilincinin oluşturulması amacıyla risk analizi tablosu oluşturulmuştur. Risk Analizi tablosu; ISO 17001 göre aşağıda belirtilen gelen yanlılığı içerir hazırlanmıştır.

Gelen yanlılık (tarafsızlığı etkileyen riskler) ;
a) Kişisel çıkar: hizmet ya da ücret için yapılacak anlaşmada bağımsız olması, müşteri kaybetme korkusu ya da işsiz kalma korkusu, uygunluk değerlendirmenin gerçekleştirilmesi sırasında kötü etki altında kalma,

b) Özeleştiri: kendi kendini değerlendirmenin gerçekleştirilmesi,

c) Taraf tutma: Uygunluk değerlendirme kuruluşunun ya da personelinin aynı zamanda onun müşterisi olan bir şirkete uyuşmazlık ya da yasal işlem kararında karşı ya da destekleyici davranması

d) Aşırı yakınlık: Kurum ya da personelin aşırı yakınlıktan ya da uygunluğunu kanıtlamak yerine fazla güvenmekten kaynaklanan tehlikeler yönetim sistemleri uygunluk değerlendirme bağlamında; objektifliğin kötü etkilenmesiyle kuruluş ya da müşteri personeli ile personel uygunluğunun değerlendirilmesi arasında ilişkilerin aşırı gelişimi; ürün sertifikasyonu ve laboratuar kapsamında, bu risk yönetim için oldukça zordur çünkü personel değerlendirmeleri için gerekli ihtiyaçlar, özel uzmanlıkla, bireysel niteliklerin ulaşılabilirlikleri sınırlandırılır,

e) Yıldırma: Uygunluk değerlendirme kuruluşu ya da personelleri; diğer ilgili taraflar ya da müşterileri korkusu ya da risklerden dolayı objektif davranışlardan caydırılabilir,

f) Rekabet: değerlendirilen kurum ile bağlantılı olduğu teknik uzman arasında olarak tanımlanır.

2.2.3. Risklerin ve Kaynaklarının Belirlenmesi

Tarafsızlığa etki edebilecek potansiyel riskler için Risk analizi tablosunda belgelendirmeye (ürün, sistem) ait tüm basamaklar madde 2.2. dikkate alınarak ilgili belgelendirme müdürü ve operasyon müdürü tarafından belirlenir. Belirlenen basamaklar için risk oluşturabilecek faaliyetler belirlenir. Faaliyetler belirlenirken standartlar, yönetmelikler, geçmiş tecrübeler, sektör paydaşlarından gelen geri beslemeler, bilimsel veriler dikkate alınır. Aynı zamanda belgelendirmeye (ürün, sistem) ait oluşturulan basmaklar risk danışma kurulu üyelerine yönetim temsilcisi tarafından mail veya elden ulaştırılarak yada toplantı yolu ile görüş alınır risk oluşturabilecek faaliyetler hakkında görüş alınır. Elde edilen veriler analiz edilerek potansiyel riskler ve kaynağı bulunarak yönetim temsilcisi tarafından risk analiz talimatındaki tabloya kaydedilir.

2.2.4. Risklerin Değerlendirilmesi ve Kabul Edilebilir Seviyelere İndirilmesi

Tarafsızlığa etki edebilecek potansiyel riskler aşağıda verilen tabloya göre genel müdür, yönetim temsilcisi ve ilgili teknik düzenleme sorumlusu / teknik yönetici / ilgili belgelendirme müdürü tarafından risk analiz talimatında değerlendirmeye tabi tutulur. Riskin bir tarafın baskın olmayacağı dengeli bir şekilde belirlenmesi ve değerlendirilmesi amacı ile ilgili riski içeren talimat risk danışma kurulu üyelerine yönetim temsilcisi tarafından mail veya elden ulaştırılarak ya da toplantı yolu ile görüş alınır. Bu görüş ilk belirlemede ve her yeni revizyon durumunda gerçekleştirilir. Alınan görüş doğrultusunda ilgili belgelendirme müdürü ve yönetim temsilcisi riskin nihai değerlendirilmesi ile alınacak önlemleri belirler. Önlem sonunda riskin kabul edilebilir seviyeye indiği kontrolü Yönetim Kurulu Başkanı tarafından kontrol edilerek onaylanır. Risk kabul edilebilir seviyeye ininceye kadar kontrol önlem kombinasyonları uygulanır.

2.2.5. Risk Değerlendirme:

Hazırlanan risk analizinde her bir Konu, Kişi, Faaliyet için tarafsızlığı tehdit eden potansiyel tüm tehlike/ler birer birer dökümante edilir. Tehlikelerin belirlenmesinde geçmiş tecrübeler, bilgi paylaşımı, tetkik tecrübeleri vb. yöntemler kullanılır. Daha sonra belirlenen her tehlikenin kabul edilebilir seviyeye çekilmesi için yapılacak tedbir ve faaliyetler belirlenir.

Risk değerlendirmede "**Risk= Etki X Olasılık"** yöntemi kullanılır.

Etki Derecelendirme
1önemsiz:İlgili taraflardan herhangi birini etkilemeyen, belgelendirme prosesinin hiçbir aşamasına ve ilgili standartların hiçbir maddesinde zaafiyete rol açmayan olay ve durumlar
2 sınırda: İlgili tarafların minör derecede etki altında bırakan, belgelendirme prosesinin işleyişine ve sonucuna, ilgili standartların herhangi bir maddesini ihlale sebep **olmayan**
3 kritik: İlgili tarafları etkileyen, sonucunda bir düzeltmeye ihtiyaç duyacak durumlar
4 yıkıcı: İlgili tarafları etkileyen, IAF dökümanları, 17021 vb standardın maddesini ihlale sebep olan durumlar

Olasılık Derecelendirme

1imkazsız: İmkansız diye adlandırılır. Bugüne kadar Şirketimizde ya da diğer tecrübelerde benzer durumların hiç görülmemiş, sektörde duyulmamış ve mantıken ortaya çıkması ihtimali bulunmayan.
2 çok düşük: İmkansıza yakın olarak adlandırılır. Bugüne kadar Şirketimizde ve diğer tecrübelerde benzer durumların hiç görülmemiş, fakat sektörde duyulmamış fakat mantıken vuku bulması imkansız değildir.
3 uzak: Olma olasılığı düşük olan, Bugüne kadar Şirketimizde ya da diğer tecrübelerde benzer durumların hiç görülmemiş, sektörde duyulmuş.
4 arasıra: Olma olasılığı bulunan, Bugüne kadar Şirketimizde yaşanmamasına rağmen diğer tecrübelerde benzer durumların görüldüğü olasılıklar
5 muhtemel: Olma olasılığı yüksek, Bugüne kadar Şirketimizde benzer durumların ortaya çıktığı olasılıklar
6 sık: Olma olasılığı çok yüksek. Bugüne kadar birkaç kez tecrübe edinilmiş.

Olasılık	**Etki**			
	4 Yıkıcı	3 Kritik	2 Sınırda	1 Önemsiz
6: Sık	24	18	12	6
5: Muhtemel	**20**	**15**	**10**	**5**
4: Arasıra	**16**	**12**	**8**	**4**
3: Uzak	**12**	**9**	**6**	**3**
2: Çok Düşük Olasılık	**8**	**6**	**4**	**2**
1: İmkânsız	**4**	**3**	**2**	**1**

YAPILACAK FAALIYETLER:

	16-24	Yüksek - Kabul Edilemez	Riski azaltmak için acil önlem gerekli
	10-12	Orta- İstenmeyen/Arzu edilmeyen	Riski azaltmak için önlem gerekli
	5-9	Düşük - Gözden geçirme ile kabul edilebilir.	Herhangi bir faaliyet gerekip gerekmediğini belirlemek için gözden geçirme gerekli
	1-4	Önemsiz - Gözden geçirmeden kabul edilebilir.	Hiçbir eyleme gerek yok.

2.2.6. Risklerin İzlenmesi, Gözden Geçirilmesi ve Revize Edilmesi

Risk durumları ilgili Belgelendirme Müdürü ve Yönetim temsilcisi tarafından sürekli olarak izlenir. Riskler, ilgili Belgelendirme Müdürü ve Yönetim Temsilcisi tarafından rutin olarak 6 ayda bir ve / veya proseslerin izlenmesi neticesinde ve / veya her yeni faaliyet alanlarının oluşması, akreditasyon kurallarının, proseslerin, kaynakların değişimi durumunda gözden geçirilir. Varsa yeni belirlenen riskler ya da mevcut olan ancak koşullar nedeni ile risk seviyesi değişen, risk durumu kalkan vb. riskler için madde 2.4 teki süreç uygulanır, sonuçlar risk izleme ve değerlendirme formu ile kayıt altına alınır ve alınan kayıtlara göre risk analizi tablosu yönetim temsilcisi tarafından revize edilerek Yönetim Kurulu Başkanı onayı ile uygulamaya alınır.

Belirlenen riskler her yıl ygg toplantılarında gözden geçirilir.

3 . İLGİLİ DÖKÜMANLAR:

Yönetim Sistemleri Belgelendirme Programı
Yönetim Sistemleri Belgelendirme Karar Prosedürü
Doküman Edilmiş Bilginin Kontrolü Prosedürü
İlgili Denetim Prosedürleri
Risk Analizi Tablosu
Mesleki Sorumluluk Sigortası Risk Analizi
Risk İzleme ve Değerlendirme Formu
Bireysel Hizmet Alım Sözleşmesi
İş Sözleşmesi
Kişisel Taahhüt ve Beyan
Denetçi Görevlendirme Formu
Çıkar İlişkisi Formu
Mesleki Sorumluluk Sigortası Poliçesi,