



Bilgi Teknolojileri Güvenliđi

alanında

Ortak Kriterler Belgelerinin Tanınmasına ilişkin
DÜZENLEME

Mayıs
2000

Katılımcılar

Avustralya ve Yeni Zelanda
Savunma Sinyalleri Müdürlüğü ve Devlet İletişim Güvenliği Bürosu

ve

Kanada
İletişim Güvenlik Kurumu

ve

Finlandiya
Maliye Bakanlığı

ve

Fransa
Merkezi Bilgi Sistemleri Güvenliği Teşkilatı

ve

Almanya
Federal Bilgi Teknolojisi Güvenliği Bürosu

ve

Yunanistan
İçişleri Bakanlığı

ve

İtalya
**Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
CESIS III Reparto – UCSi
(Başbakanlık, Ulusal Güvenlik İşleri
Başkanlığı-İstihbarat ve Güvenlik
Hizmetleri III – Güvenlik Merkez
Bürosu)**

ve

Hollanda
İçişleri ve Kraliyet İlişkileri Bakanlığı

ve

**Norveç Savunma Komuta Karargahı/Güvenlik
Dairesi**

ve

İspanya
Kamu Yönetimi Bakanlığı

ve

Birleşik Krallık
Ticaret ve Sanayi Bakanlığı
İletişim-Elektronik Güvenlik Grubu

ve

Amerika Birleşik Devletleri
Ulusal Standartlar ve Teknoloji Enstitüsü
Ulusal Güvenlik Teşkilatı

**AŞAĞIDAKİ GİBİ İŞBİRLİĞİ YAPMAYI
PLANLAMAKTADIR,**

Giriş

Düzenlemenin Amacı

Bu Düzenlemeye Katılanlar aşağıdaki hedefleri paylaşırlar:

- a) *Bilgi Teknolojisi (BT) ürünlerine ve koruma profillerine ilişkin değerlendirmelerin* yüksek ve uygun standartlarda yapılmasının ve bu ürün ve profillerin güvenliğine duyulan güvene önemli ölçüde katkılarının görünmesini sağlamak;
- b) Değerlendirilmiş, güvenliği yükseltilmiş BT ürünlerinin ve koruma profillerinin sağlanabilirliğinin geliştirilmesi;
- c) BT ürün ve koruma profillerine yönelik değerlendirmelerin tekrarlanması yükünün ortadan kaldırılması;
- d) Değerlendirmenin verimliliğinin ve maliyet etkinliğinin ve BT ürün ve koruma profillerine yönelik *Belgelendirme/Onaylama*¹ sürecinin sürekli olarak geliştirilmesi.

Bu Düzenlemenin amacı, bir *Ortak Kriterler belgesine* sahip olan BT ürünlerinin ve koruma profillerinin daha fazla değerlendirmeye gerek olmaksızın temin edilebilmesi ve kullanılabilmesine olanak sağlayan bir durumu oluşturarak söz konusu hedefleri iletmeektir. Ortak Kriterler belgelerini düzenleyen bir *Belgelendirme/Onaylama Kuruluşunun (CB)* yüksek ve uygun standartları karşılamaını zorunlu kılarak orijinal belgenin dayandırıldığı değerlendirmelerin güvenilirliğine itimat edilmesi için gerekli temeli sağlamayı amaçlar.

Büyük olasılıkla iki taraflı veya çok taraflı ayrı anlaşmalar kapsamında bazı hassas yönetim sistemleri temin edilecek, onaylanacak ve tanınacaktır. Bu Düzenleme o tür anlaşmaları kısıtlamaz. Özellikle Madde 3'te belirtilen istisnalar bu tür ayrı olarak görüşülmüş anlaşmalara uygulanmaz.

Hem devlete ait hem de devlet dışı CB'lerin belgelendirme/onaylama işlemini güvenilir biçimde yapma yeteneğine sahip oldukları ve her iki tip kuruluş için de yasal koşulların sağlanması gerektiği kabul edilmektedir. Ancak diğer ülkelerde düzenlenmiş olan belgelerin hükümetin alacağı karar ve taahhütlere bağlıdır. Bu nedenle belgelerin düzenlenmesi ve tanınması işlevleri bu Düzenlemede ayrı tutulmuştur.

Düzenlemenin Ruhu

Bilgi sistemlerinin karmaşıklığı, en dikkatli biçimde yazılmış olan güvenlik kriterleri ve değerlendirme yöntemlerinin her olasılığı kapsayamamasına yol açmaktadır. Birçok durumda kriterlerin uygulanması ve bu kriterlerin uygulanmasının gözetimi uzman profesyonellerin değerlendirmesini gerektirecektir. Bu tür bir değerlendirmeyi yaparken Katılımcılar değerlendirilen BT ürününün sahip olduğu güven seviyesini kendi ölçüleri olarak kullanmaya gayret edecektir. Bu nedenle Düzenlemenin Katılımcıları, birbirlerinin teknik değerlendirmelerine yönelik ortak bir anlayışı ve güveni geliştirmeyi ve sürdürmeyi ve açık görüşme ve tartışmalar aracılığıyla genel uyumu sürdürmeyi planlamaktadırlar.

Katılımcılar, örneğin daha fazla maliyet etkinliğine sahip güvence paketlerini geliştirerek ve oluşturarak ve güvenceye önemli bir katkısı olmayan koşulları saptayarak ve ortadan kaldırarak kriterlerin ve yöntemlerin uygulanmasını geliştirmek için etkin bir biçimde çalışma yapmaya çaba gösterecektir. Katılımcılar ayrıca, örneğin değerlendirmelerin sponsorlarını bu tür bilgileri ilgili taraflara sağlamaları konusunda teşvik ederek değerlendirme sonuçlarının ekonomik biçimde yeniden kullanımını geliştirmeyi planlamaktadırlar.

¹ Bazı Eylem Programları belgelendirme yerine onaylama terimini kullanmayı seçebilir. Bu tanıma düzenlemesinin amaçları açısından terimler Ek A'da yer alan Terimler Sözlüğünde yansıtılan anlamları ve beyan edilen amaçları açısından

eşdeğer olarak kabul edilmiştir.

Article 1

Üyelik

Bu Düzenlemenin Katılımcıları, kendi ülke veya ülkelerini temsil eden hükümet kurumları veya hükümet kuruluşlarıdır. Katılımcılar değerlendirme belgelerinin üreticileri, değerlendirme belgelerinin kullanıcıları ya da her ikisi birlikte olabilir. Bir BT güvenlik değerlendirmesi yeteneğine sahip olmayabilecek olmakla birlikte, *Belge kullanan* Katılımcılar yine de belgelendirilmiş/onaylanmış ürünlerin ve koruma profillerinin kullanılmasına yönelik beyan edilmiş bir ilgiye sahiptirler. *Belge onaylayan Katılımcılar, kendi ülke veya ülkelerinde faaliyetlerini sürdüren* ve belgelerini *onaylayan uyumlu CB'lerin* (Madde 5'de tanımlanan) *Sponsorlarıdır*. Kuruluşları uyumlu bir CB'nin kaynaklarına ve uzmanlığına hükmeden Belge onaylayan Katılımcılar, *Nitelikli Katılımcılar* olarak tanımlanır.

Madde 2

Kapsam

BT ürünleri ve koruma profilleri açısından Katılımcıların, bu Sözleşmenin koşullarına ve her bir Katılımcının ilgili yasa ve mevzuatına uygun olarak belge veren herhangi bir başka Katılımcı tarafından verilmiş olan Ortak Kriterler belgelerini tanımayı planlamaktadırlar. Bu Düzenleme, 1 den 4 e kadarki Değerlendirme Güvencesi Seviyeleri için gerekli olan Ortak Kriterler güvence bileşenlerine karşı uygunluk iddialarını kapsar. Kapsamın genişletilmesine bu Düzenleme içinde Katılımcılar tarafından herhangi bir zamanda, Madde 14'ün hükümlerine uygun olarak diğer güvence seviyeleri ya da bileşenleri eklenerek karar verilebilir.

Madde 3

İstisnalar

Bir Ortak Kriterler belgesinin tanınması bir Katılımcının ilgili ulusal, uluslararası veya Avrupa Topluluğu yasa veya mevzuatı ile uyumlu olmayan bir biçimde hareket etmesine yol açacaksa, o Katılımcı bu tür bir belgeyi tanımayı kabul etmeyebilir. Özellikle, ulusal yasalar, bağlı mevzuat, idari yönetmelikler veya resmi yükümlülüklerin hükümleri kapsamında zorunlu veya yetkilendirilmiş olan bir *güvenlik sınıflandırması* ya da eşdeğer *koruyucu markalamayı* içeren bir BT ürünü veya bir koruma profilinin düşünüldüğü durumlarda Katılımcılar yalnızca o uygulamaya ilişkin olarak bir belgeyi tanımayı kabul etmeyebilirler.

Madde 4

Tanımlar

Bu Düzenlemenin anlamı açısından önemli olan veya bu Düzenlemeye özgü bir anlamda kullanılmış olan terimler bu Düzenlemenin A Ekindeki Terimler Sözlüğünde tanımlanmıştır. Bu tür terimler bu Düzenlemenin metninde geçtikleri ilk yerde italik olarak yazılmıştır.

Article 5

Tanım Koşulları

Bu Düzenlemede aksi belirtilmedikçe, her Katılımcı herhangi bir belge veren Katılımcı tarafından verilmiş olan ilgili Ortak Kriterler belgelerini tanıyacaktır. Bu tür bir belge değerlendirme ve serti/onaylama süreçlerinin aşağıdaki şekillerde layıkıyla profesyonel bir şekilde yürütüldüğünü teyit eder

- a. kabul edilmiş olan BT güvenliği değerlendirme kriterleri
- b. kabul edilmiş olan BT *güvenlik değerlendirme yöntemleri*,
- c. düzenleyen Katılımcı ülkedeki *uyumlu CB* tarafından yönetilen bir *Değerlendirme ve Belgelendirme/Onaylama Programı bağlamında*,
- d. ve verilen Ortak Kriterler belgelerinin ve düzenlenen *Belgelendirme/Doğrulama Raporlarının* bu Düzenlemenin hedeflerini sağlaması.

Bu koşulların tümünü karşılayan Belgeler bu Düzenlemenin amaçları bakımından eşittir. BT güvenliği değerlendirme kriterleri, Yönetim Komitesinin onayladığı düzenlemesi ile Bilgi Teknolojisi Güvenliği Değerlendirme Ortak Kriterlerinde (OK) ortaya konmuş olanlar olacak ve değerlendirme yöntemlerinde belirtilmiş olanlar olacaktır. Belgelendirme/Onaylama Raporları için asgari koşullar bu Düzenlemenin I Ekinde belirtilmiştir. Bir Değerlendirme ve Belgelendirme/Onaylama Programı için asgari koşullar bu Düzenlemenin B Ekinde belirtilmiştir. Bir değerlendirme ve Belgelendirme/onaylama en azından aşağıdaki koşulların yerine getirilmiş olması durumunda layıkıyla profesyonel bir biçimde yürütülmüş olarak addedilecektir:

a) *Değerlendirme Tesisin*

- ya kendi ülkesinde EN 45001 veya ISO Kılavuz 25 e uygun olarak tanınmış olan bir Akreditasyon Kuruluşu ya da bunların tüm Katılımcılar tarafından onaylanmış olan bir yorumuna uygun olarak tanınması ve Ek B.3 uyarınca *lisanslanmış veya onaylanmış* olması,
- ya da söz konusu ülkede geçerli olan yasalar, ikincil mevzuat veya diğer resmi idari prosedürler tarafından oluşturulmuş olması ve bu Düzenlemenin B.3. Ekinde belirtilen koşulları sağlaması;

ve

b) CB'nin uygun olduğunun kabul edilmesi ve

- ya kendi ülkesinde tanınmış olan bir Akreditasyon Kuruluşu tarafından ya EN 45011 ya da ISO Kılavuz 25 e göre veya EN 45011 veya ISO Kılavuzu 25'in bu Düzenlemenin C Ekinde belirtilmiş olan koşulları asgari ölçüde sağlayan ulusal bir yorumu uyarınca onaylanmış olması,
- ya da söz konusu ülkenin yasaları, ikincil mevzuatı veya diğer resmi idari prosedürler kapsamında oluşturulmuş olması ve EN 45011 veya ISO Kılavuz 65 ya da bu Düzenlemenin C Ekinde belirtilmiş olan koşulları sağlıyor olması.

Article 5

Ortak Kriterlerin ve Ortak Metodolojinin Deęerlendirme ve Belgelendirme/Onaylama Yöntemleri arasında tutarlı bir biçimde uygulanmasına yardımcı olmak için Katılımcılar halihazırda uygulanan Ortak Kriterler ve Ortak Metodolojinin yeknesak bir biçimde yorumlanmasına yönelik bir çalışma yapmayı planlamaktadır.

Katılımcılar bu hedefe ulaşmaya çalışırken aynı zamanda yorumlama farklarını çözmek için gerekli olan yorumlama ve tartışmalara ilişkin olarak düzenli bilgi alışverişinde bulunmayı planlarlar. Ortak Kriterler ve Ortak Metodolojinin tutarlı, güvenilir ve ehil bir biçimde uygulanması hedefine daha fazla yardımcı olmak üzere CB, Yöntem içinde yürütülmekte olan tüm değerlendirmeleri uygun bir seviyede izleme ve CB ile bağlantılı olan tüm BT Güvenliği Değerlendirme Tesislerinin aşağıdaki hususları yerine getirmesini sağlamak için diğer prosedürleri yürütme sorumluluğunu üstlenmelidir:

a) Değerlendirmelerin tarafsız bir şekilde yürütülmesi;

b) Ortak Kriterlerin ve Ortak Metodolojinin doğru ve tutarlı bir biçimde uygulanması; ve c) *Korunan bilgilerin* gizliliğinin yeterli düzeyde korunması.

Madde 6

İsteğe Bağlı Dönemsel Değerlendirmeler

Bu Düzenlemenin amaçlarını paylaşmaya devam ettiklerini ve bu Düzenlemenin amaçlarını geliştirmek için gayret göstereceklerini güvence altına almak amacıyla uyumlu *CB'lere yönelik değerlendirmeler bu süreyi aşmamak üzere yaklaşık beş yıllık süreler içinde yapılmalıdır*. Bu tür değerlendirmelerin profili bu Düzenlemenin D Ekinde belirtilmiştir.

Madde 7

Yayınlar

Belge veren Katılımcılar tarafından verilen Ortak Kriterler belgeleri, Katılımcıya veya onun Değerlendirme ve Belgelendirme/Onaylama Programına özgü herhangi bir logo veya ayırt edici işaretlere ek olarak belirgin bir biçimde Tanıma Düzenlemesinin işaretini ve standart biçimdeki sözcükleri ihtiva etmelidirler. İşaret ve sözcüklerin biçimi bu Düzenlemenin A Ekinde ve J Ekinde verilmiştir.

Belge veren her bir Katılımcı Belgelenmiş/Onaylanmış Ürünler Listesinin bir bölümünde veya başka bir biçimde düzenlenen şekilde, bu Düzenlemenin 3. Maddesinde belirtilmiş olan nedenler dahil, ancak bunlarla sınırlı olmaksızın bu Düzenleme kapsamında bu şekilde hareket etmeyi engelleyen bir neden olmadıkça, başka bir belge veren Katılımcı tarafından verilen belgelere sahip olan tüm BT ürünlerinin ve koruma profillerinin kısa özelliklerini yayınlacaktır.

Madde 8

Bilgi Paylaşımı

Bilginin açıklanmasının bir Katılımcının ulusal yasaları veya düzenlemelerine uygun olduğu ölçüde, her bir Katılımcı bu Düzenlemenin uygulanması ile ilgili tüm bilgi ve belgeleri diğer Katılımcılara sağlamak için çaba göstermelidir.

Bu yükümlülük yerine getirilirken, üçüncü taraflara ait ticari sırlar veya korunan bilgiler yalnızca ilgili üçüncü tarafın yazılı onayının önceden alınmış olması koşuluyla bir Bilgi Teknolojisi Güvenliği Değerlendirme Tesisi, CB ya da Katılımcı tarafından açıklanabilir.

Özellikle her bir Katılımcı, bu Düzenlemenin tanınması için gerekli koşulları yerine getirme yeteneğini etkileyebilecek veya bunun dışında bu Düzenlemenin işlemlerini veya amacını engelleyebilecek olası değişikliklere ilişkin bilgileri derhal sağlamalıdır.

Katılımcıların paylaşması beklenen bilgi ve belgelerin niteliği ve kapsamı bu Düzenlemenin F Ekinde daha ayrıntılı olarak açıklanmıştır.

Madde 9

Yeni Katılımcılar

Katılımcılar

Bu Düzenlemeye katılım, mevcut Katılımcıların oybirliğiyle verilmiş olan onayına bağlı olarak bu Düzenlemeyi desteklemeyi planlayan ülkelerin temsilcilerine açıktır.

Belgelendirme/Onaylama Kuruluşları

Bir CB'nin bu Düzenlemenin 5. Maddesinin amaçlarına uygun olduğu, mevcut Katılımcıların söz konusu kuruluşun bu Düzenlemenin 5. Maddesinde ve 5. Maddede zikredilen Eklerde belirtilmiş olan tanıma koşullarını yerine getireceğinden ve Belgelendirme/onaylamanın gözlenmesi de dahil olmak üzere bu Düzenlemenin G Ekinde belirtilmiş olan prosedürlere uygun olarak uygunluk koşullarını sağlayacağından emin olmaları halinde oybirliğiyle verdikleri onayla belirlenir.

Madde 10

Bu Düzenlemenin İdare Edilmesi

Bu Düzenleme bir Yönetim Komitesi tarafından idare edilmelidir. Yönetim Komitesi, bu Düzenlemenin durumunu, koşullarını ya da uygulanmasını ele almak için gereken sıklıkta toplanmalıdır. Tüm Katılımcılar Yönetim Komitesinde temsil edilmelidir. Yönetim Komitesinin prosedürleri ve asli sorumlulukları bu Düzenlemenin H Ekinde belirtilmiştir.

Madde 11

Anlaşmazlıklar

Katılımcılar arasındaki anlaşmazlıklar görüşmeler yoluyla çözümlenmelidir. Katılımcılar aralarındaki anlaşmazlıkları müzakereler yoluyla çözmek için her türlü gayreti göstermelidir. Bunun mümkün olmaması durumunda, anlaşmazlıklar ilk önce Yönetim Komitesine götürülecektir. Yönetim Komitesinin anlaşmazlığa ilişkin bulgularını Belgelendirmesi beklenir. Anlaşmazlığın görüşme veya müzakere yoluyla çözülememesi durumunda münferit Katılımcılar etkilenen Ortak Kriterler belgelerini tanınamayı ve bu tanınamayı Yönetim Komitesine bildirmeyi seçebilirler.

Article 12

Yükleniciler Kullanılması

Katılımcıların, başta bu Düzenlemenin D Ekinde veya G.3 veya G.4. Ekinde ya da H Ekinde belirtilen prosedürler olmak üzere bu Düzenlemenin uygulanması ve işletilmesinde yüklenicilerin devreye sokulmasını önermeleri durumunda bu yüklenicilerin uygun uzmanlığa sahip olduklarından emin olmaları ve diğer Katılımcılara bildirimde bulunmaları gerekir. Korunan bilgiler yalnızca F.4. Ekinde belirtilen şekilde oluşturucunun onayı ile yükleniciye aktarılmalıdır.

Madde 13

Bu Düzenlemeye İlişkin Masraflar

Bu Düzenlemenin başka yerinde aksi belirtilmedikçe, her bir Katılımcının bu Düzenlemeye katılımından kaynaklan kendi masraflarını karşılaması beklenmektedir.

Madde 14

Değişiklik

Bu Düzenlemenin koşullarında yapılacak herhangi bir değişiklik Katılımcıların oybirliğiyle onay vermesini gerektirecektir. Kabul edilmiş olan herhangi bir değişiklik tüm Katılımcılar tarafından imzalanmış olan yazılı bir belgeye kaydedilmelidir.

Madde 15

Süre

Bu Düzenleme kapsamında yapılacak işbirliğinin Katılımcıların sonlandırılmasına oybirliğiyle karar vermesine kadar sürmesi beklenmektedir.

Madde 16

Katılımın İsteğe Bağlı Olarak Sonlandırılması

Herhangi bir Katılımcı bu Düzenlemeye katılımını veya temsil ettiği herhangi bir CB'nin uygunluk durumunu diğer Katılımcılara yazılı bildirimde bulunarak sonlandırabilir.

Madde 17

Başlangıç

Bu Düzenleme kapsamındaki faaliyetler 23 Mayıs 2000 tarihinde başlayacaktır.

Bu Düzenlemenin Etkisi

Bu Düzenlemenin, bu Düzenlemeye imza koyan kişilere dahil olmayanlarca başvurulabilecek maddi ve usule ilişkin haklar, sorumluluklar veya yükümlülükler oluşturmadığı her bir Katılımcı tarafından onaylanır ve kabul edilir. Ayrıca her bir Katılımcı, bu Düzenlemenin ulusal, uluslararası veya Avrupa Topluluğu yasalarında herhangi biri veya tümü için bir bağlayıcılığı olmadığını ve bu Düzenlemeyi herhangi bir yerel veya uluslararası mahkeme ya da adalet divanı aracılığıyla uygulama girişimde bulunmayacağını onaylar ve kabul eder Bir CB tarafından düzenlenen raporlar veya bir Katılımcı tarafından verilen Ortak Kriterler belgeleri BT ürünleri veya koruma profillerine ilişkin olarak söz konusu Belgelendirme/Onaylama Kuruluşu veya Katılımcı tarafından verilmiş bir onay, garanti veya teminat oluşturmaz ne de belgelendirme/onaylama faaliyetleri sonucunda verilmiş olan Ortak Kriterler belgelerinin tanınması, başka bir CB tarafından düzenlenmiş Belgelendirme/Onaylama Raporları veya bunun sonucu olarak başka bir Katılımcı tarafından verilen belgeler açısından bir onay, garanti veya teminat oluşturmaz.

Ek A

Sözlük

Bu sözlük bu Düzenlemenin metninde veya eklerinde yer alan ve bu Düzenlemeye özgü anlamda kullanılan ya da bu Düzenlemenin yorumlanması açısından önemli bir anlama sahip olan belirli terimlerin tanımlarını içerir. Bu sözlük ayrıca bu Ek'te kullanılan diğer bazı terimlerin tanımlarını da içerir. Bu Ek'te yer alan tanımların aynı terimlere ilişkin olarak CC veya CM'de verilen tanımlardan farklı olması durumunda, bu Düzenleme'de amaçlanan anlamı belirlemek için bu Ek'te yer alan tanımlar kullanılacaktır. Bu tür tanımlar CC ve CM'de verilenlerle genel olarak uyumlu olup genellikle geçerliliklerini sürdürürler. Farklılıklar bu Düzenlemenin özgün bağlamı içinde daha fazla açıklık getirmek içindir. Tanımlarda kullanılan ve kendileri başka bir yerde tanımlanan terimler Sözlükte italik olarak yazılmıştır.

Onaylanmış:

Bir *Akreditasyon Kuruluşu* tarafından önceden belirlenmiş bir tarafsızlık ve genel teknik, metodolojik ve prosedür konusunda yeterlilik standardını karşıladığı resmi olarak onaylanmış.

Akreditasyon Kuruluşu:

Kabul edilmiş bir standarda göre diğer kuruluşların performansını değerlendirmekten ve standardı karşılayan kuruluşların durumunu resmi olarak onaylamaktan sorumlu olan bağımsız bir kuruluş.

Onaylanmış: Bkz

yetkili.

Onaylama İlkesi:

Bkz yetkilendirme

ilkesi.

Uyumlu CBlerin Değerlendirilmesi:

Belirli bir *uyumlu CB* tarafından yürütülen *değerlendirmeler ve belgelendirmeler/onaylamaların* bu Düzenlemede belirtilen şekilde sürdürüldüğünün belirlenmesini sağlayan bir prosedür.

Yetkilendirme:

Uygun bir CB tarafından, CC belgelendirme işaretinin kullanılmasına izin veren bir *Ortak Kriterler belgesinin* düzenlenmesine bir Katılımcı tarafından verilen izin.

CB:

Belgelendirme/Onaylama Kuruluşu.

İlgili CB:

Bir *Nitelikli Katılımcı* ile bağlantılı *uyumlu CB*.

Uyumlu CB:

Ek K 'da uygun olarak kaydedilmiş bir *CB*.

CC:

Bilgi Teknolojisi Güvenlik Değerlendirmesi Ortak Kriterleri, özel bir *BT güvenlik değerlendirme kriterleri* dizisini tanımlayan bir belgenin başlığı (sürüm 2.01, ISO-IEC-15408 ile aynıdır).

Belgelendirme/Onaylama:

Bir *CB* tarafından yürütülen ve bir *Ortak Kriterler sertifikasının* düzenlenmesine yol açan süreç.

Belgelendirme/Onaylama Kuruluşu:

Belgelendirme/onaylama işlemlerini yürütmekten ve bir *Değerlendirme ve Belgelendirme/Onaylama Programının* günlük işleyişini denetlemekten sorumlu olan bir kuruluş.

Belgelendirme/Onaylama Raporu:

Bir *CB* tarafından düzenlenen ve bir değerlendirmenin sonuçlarını özetleyerek genel sonuçları örn: değerlendirmenin gerektiği şekilde yürütüldüğü, *değerlendirme yöntemlerinin* ve diğer prosedürlerin doğru bir biçimde uygulandığı ve *Değerlendirme Teknik Raporunun* sonuçlarının gösterilen kanıtlarla tutarlı olduğunu onaylayan resmi bir belge.

Belgelendirilmiş/Onaylanmış Ürünler Listesi:

Bu Düzenlemeye uygun olarak halihazırda geçerli olan *Ortak Kriterler* sertifikalarının kısa özelliklerini veren resmi bir belge.

Müşteri:

Bir değerlendirme için bir *ITSEF*'le sözleşme yapmış olan bir taraf.

CM:

Bilgi Teknolojisi Güvenlik Değerlendirmesi için Ortak Metodoloji, özel bir *BT güvenlik değerlendirme kriterleri* dizisini tanımlayan teknik bir belgenin başlığı.

Ortak Kriterler Sertifikası:

Uygun bir CB tarafından düzenlenen ve belirli bir *BT ürünü veya koruma profilinin* bir *ITSEF* tarafından yapılan değerlendirmeyi başarılı bir şekilde tamamladığını onaylayan bir *Katılımcı* tarafından onaylanan resmi bir belge. Bir *Ortak Kriterler sertifikası* her zaman bir *Belgelendirme/Onaylama Raporu* ile bağlantılıdır.

Değerlendirme:

Şikayetlerin haklı olup olmadığını belirlemek için *Ortak Metodoloji* kullanılarak bir *BT ürünü* veya bir *koruma profilinin* Ortak Kriterler açısından değerlendirilmesi.

Değerlendirme Programı: Belgelendirme/Onaylama

Yüksek yeterlilik standartlarının ve tarafsızlığın korunmasını ve tutarlılığın elde edilmesini sağlamak için bir *CB'nin* yetkisi dahilinde *değerlendirme* ve *belgelendirme/onaylama* işlevlerinin sistematik organizasyonu.

**Değerlendirme
Tesis:**

Değerlendirilen *BT ürünleri* veya *koruma profilleri* için *geliştiricilerinden* bağımsız olarak ve genellikle ticari bazda *değerlendirmeler* yapan bir kuruluş.

**Değerlendirme
yöntemleri:**

Bkz BT güvenlik değerlendirmesi yöntemleri.

**Değerlendirme Teknik
Raporu:**

Belgelendirme/Onaylama Raporunun temel dayanağı olarak *Değerlendirme Tesis* tarafından *CB*'ye sunulan ve bir *değerlendirmenin* ayrıntılarını veren bir rapor.

Yorumlama:

Kriterlerin veya metodolojinin herhangi bir teknik yönünün anlamı veya uygulanma yöntemine ilişkin olarak gerektiğinde sağlanan uzman teknik görüşü.

BT ürünü:

Bir *sistem* çeşitliliği içinde kullanılmak veya dahil edilmek üzere tasarlanmış işlevsellik sağlayan bir *BT yazılım* veya donanım paketi.

**BT güvenlik değerlendirmesi
kriterleri:**

Değerlendirmelerin bir *Değerlendirme ve Belgelendirme/Onaylama Programı* içinde etkin bir biçimde ve uygun bir standartta yürütüleceği konusunda güven duyulmasına zemin hazırlamak için sağlanması gereken bilgilerin ve yapılacak işlemlerin bir derlemesi.

**BT güvenlik değerlendirme
yöntemleri:**

Değerlendirmelerin bir *Değerlendirme ve Belgelendirme/Onaylama Programı* içinde etkin bir biçimde ve uygun bir standartta yürütüleceği konusunda güven duyulmasına zemin hazırlamak için *BT güvenlik değerlendirme kriterlerinin* uygulamasında *Değerlendirme Tesisleri* tarafından kullanılması gereken yöntemlerin bir derlemesi.

ITSEF:

IT Bilgi Güvenliği Değerlendirme Tesis, belirli bir *BT Güvenlik Değerlendirmesi* ve *Belgelendirme/Onaylama Programı* bağlamında *değerlendirmeler* yapmak üzere yetkili veya onaylanmış bir *akredite Değerlendirme Tesis*.

Yetkili:

Özel *BT güvenlik değerlendirme* alanında bir *CB* tarafından teknik açıdan yeterli olarak değerlendirilen ve belirli bir *Değerlendirme ve Belgelendirme/Onaylama Programı* bağlamında resmi olarak *değerlendirmeler* yapmasına izin verilen.

**Yetkilendirme
ilkesi:**

Yetkilendirilmek veya onaylanmak için başvuru yapılmasına ve bu tür başvuruların işleme tabi tutulmasına ve bir başvuru sahibinin yeterlilik kazanmak için yerine getirmesi gereken eğitim ve güvenlik koşullarına ilişkin prosedürleri belirleyen her *Değerlendirme ve Belgelendirme/Onaylama Programına* ait temel belgelerin bir bölümü.

Yönetim Komitesi:

Tüm *Katılımcıların* temsil edildiği ve bu Düzenlemenin kurallarına uygun biçimde işlemlerini sağlamak için çaba gösteren kurul.

Değerlendirmelerin izlenmesi:

Bir *CB'nin* temsilcilerinin bir *ITSEF'in işlevlerini* düzgün ve profesyonel bir biçimde yürütmesi konusunda tatmin olmak için sürmekte olan *değerlendirmeleri* izlemede veya tamamlanmış *değerlendirmeleri* gözden geçirmede uyguladıkları prosedür.

Oluşturan taraf:

Örneğin bir *BT ürünü veya koruma profili* geliştiricisi, *ITSEF veya Katılımcı* gibi bir BT güvenlik *değerlendirmesi veya belgelendirme/onaylama* ile bağlantılı korunan bilgiler üreten bir kaynak.

Katılımcı:

Bu Düzenlemeye imza koymuş taraf.

Belgeden Yararlanan Katılımcı:

Ortak Kriterler belgelerini tanımada ulusal çıkarı olan bir Katılımcı.

Belge Veren Katılımcı:

Bir veya daha fazla sayıda uyumlu *CB'leri* temsil eden bir Katılımcı.

Nitelikli Katılımcı:

Aynı zamanda *uygun bir CB* olan bir Katılımcı (ya da *belgelendirme/onaylama işlemlerinin gözlenmesine* ilişkin olarak teknik uzmanlar sağlamak için *uygun bir CB'nin* kaynaklarını ve uzmanlığını yeterli ölçüde kontrol eden). *CB, Nitelikli Katılımcının* bağlantılı *CB'sidir*.

Korunan Bilgi:

Bu Düzenleme içinde yer alan süreç veya faaliyetler kapsamında toplanan veya elde edilen ve izinsiz olarak açıklanmasının sonuçta (i) rekabete dayalı ticari haklara veya mülkiyet haklarına yönelik zarara, (ii) kişisel mahremiyete yönelik açıkça kanunsuz bir tecavüze, (iii) ulusal güvenliğe yönelik bir zarara, veya (iv) başka biçimde, ulusal yasalar, ikincil mevzuat, idari yönetmelikler veya resmi yükümlülüklerle korunan bir hakka yönelik zarara neden olması beklenen bilgiler.

Koruma profili:

CC'de tanımlanmış olan ve belirli tüketici gereksinimlerini karşılayan bir *BT ürünleri* kategorisi için uygulamadan bağımsız bir dizi güvenlik koşullarını belirten resmi bir belge.

Koruyucu işaretleme:

Güvenlik sınıflandırması için artık Birleşik Krallıkta resmi olarak kullanılan alternatif ad.

Ortak Kriterler belgelerinin tanınması:

Uyumlu CBler tarafından yürütülen değerlendirme ve belgelendirme süreçlerinin gerektiği şekilde profesyonel bir biçimde yürütüldüğünün ve bu Düzenlemenin tüm koşullarını karşıladığının ve sonuç olarak ortaya çıkan tüm *CC belgelerine* eşit önem verilmesi niyetinin Katılımcılar tarafından onaylanması.

Tanıma:

Bkz *Ortak Kriterler* belgelerinin tanınması.

**Güvenlik
sınıflandırması:**

Ulusal çıkarlar açısından uygulanması gereken asgari koruma standartlarını belirtmek için korunan bilgilere uygulanan bir işaret.

**Belgelendirme/onaylamanın
gözlenmesi:**

Bir *BT ürününün* değerlendirilmesi ve belgelendirilmesi/onaylanmasının bu Düzenlemeye uygun olarak yapıldığının *Nitelikli Katılımcılardan* en az biri tarafından izlenmesini yoluyla bir *CB'nin* *Değerlendirilmesi*.

**Sponsor (bir
CB'nin):**

Bir *uyumlu CB'nin* (veya aday *uyumlu CB'nin*) çıkarlarını temsil eden ve onun *Ortak Kriterler belgelerini* onaylayan Katılımcı.

Sistem:

Belirli bir amacı ve işletim gereksinimi olan belirli bir *BT tesisi*.

**Değerlendirme
Hedefi:**

Bir *değerlendirmeye* konu olan bir *BT ürünü* ve bununla bağlantılı yönetici ve kullanıcılara yönelik kılavuz belgeleri.

Değerlendirme ve Belgelendirme/Onaylama Programı

B.1 Bir Programın Amacı ve Temel Özelliği

Bir Değerlendirme ve Belgelendirme/Onaylama Programının (bundan böyle bir Program olarak anılacaktır) ana amacı, değerlendirme ve belgelendirme/onaylama işlevlerinin sistematik bir biçimde organize edilmesi ve yönetilmesi suretiyle yüksek yeterlilik ve tarafsızlık standartlarının sürdürülmesinin ve tutarlılığın elde edilmesinin sağlanması.

Bu amaca yönelik olarak her bir Program, yalnızca değerlendirilen ürünlerin ve değerlendirilen koruma profillerinin belgelendirilmesinden/onaylanmasından değil sorumlu olmayıp eşit ölçüde bölüm B.2'de sıralanan diğer işlevlerden de sorumlu olacak olan tek bir Belgelendirme/Onaylama Kuruluşu tarafından yönetilir.

Bir Programın genel ilkesi (*Lisanslama* veya *Onaylama İlkesi* de dahil olmak üzere – aşağıya bkz) ya Belgelendirme/Onaylama Kuruluşunun kendisi tarafından ya da bir Yönetim Kurulu tarafından belirlenebilir. İkinci durumda Yönetim Kurulu, Programın kurallarına ve ilkelerine uygun olarak işleminde ve uygun olan durumlarda bu kural ve ilkelerin yorumlanması ve değiştirilmesinde nihai sorumluluğa sahipken Belgelendirme/Onaylama Kuruluşu Programı yönetir ve Yönetim Kurulunun ilkesel yönlendirmesine uygun olarak kural ve ilkeleri uygular. Her iki durumda da, Programın yürütülmesinde değerlendirme ve belgelendirme/onaylama faaliyetlerinde payı olan tüm tarafların çıkarlarına uygun bir ağırlık verilmesini sağlayacak mekanizmaların bulunmasının sağlanması çok önemlidir.

Bu tür bir Programın mevcudiyeti tanıma bağlamında büyük bir öneme sahiptir. Zira ortak değerlendirme kriterleri ve değerlendirme yöntemleri ile birlikte, tüm *ITSEF*lerin aynı yüksek standartlarda çalıştığı konusunda ve dolayısıyla da sonuçların doğruluğu ve bunların bir *ITSEF*'le diğeri arasında tutarlık gösterdikleri konusunda güven duyulmasına yönelik özgün bir zemin hazırlar. Bu tür bir güven, herhangi bir Tanıma Düzenlemesinin zorunlu olarak üzerine inşa edileceği güvenin oluşturulması açısından kaçınılmazdır.

B.2 CB'nin Rolü ve Temel Özelliği

CB, *ITSEF*lerden bağımsızdır ve uygun niteliklere haiz personele sahiptir.

İlgili ülkede geçerli olan yasaların, ikincil mevzuatın veya diğeri resmi idari prosedürlerin hükümleri kapsamında kurulabilir veya uygun bir Akreditasyon Kuruluşu tarafından onaylanabilir. Her iki durumda da ya EN 45011 veya ISO Kılavuz 65'in koşullarını ya da bu Düzenlemenin C Ekinde belirtilmiş olan koşulları karşılaması gereklidir.

Belgelendirme/Onaylama Kuruluşu tarafından yürütülecek temel işlevler şunlardır:

- Değerlendirme Tesislerinin Programa katılımına izin vermek (aşağıya bkz);
- katılan *ITSEF*'lerin performansını ve özellikle kabul edilmiş olan değerlendirme kriterleri ve değerlendirme yöntemlerine bağlı kalmalarını ve bunları uygulama ve yorumlamalarını izlemek;
- Değerlendirilmekte olan ürün ve koruma profilleri ve değerlendirme sürecinin kendisi ile ilişkili hassas bilgilerin uygun bir biçimde ele alınmasını ve gerek duyduğu güvenlik korumasının verilmesi ve bu prosedürlerin düzenli olarak izlenmesini sağlayacak

prosedürlerin varlığıyla ilgilenmek (aşağıya bkz).

- d) ITSEF'ler için gerektiği şekilde ek kılavuzlar düzenlemek;
- e) Program dahilinde yürümekte olan tüm değerlendirmeleri uygun bir seviyede izlemek;
- f) sonuçların öne sürülen kanıtlarla tutarlı olmasını ve kabul edilmiş olan değerlendirme kriterlerinin ve değerlendirme yöntemlerinin doğru bir biçimde uygulanmasını sağlamak için tüm değerlendirme raporlarını (özellikle Değerlendirme Teknik Raporları da dahil olmak üzere) gözden geçirmek;
- g) Programın gözetimi altında tamamlanmış olan her bir değerlendirmeye ilişkin olarak bir Belgelendirme/Onaylama Raporu üretmek;
- h) Ortak Kriterler belgeleri ve bunlarla bağlantılı Belgelendirme/Onaylama Raporlarını yayınlamak;
- i) Program dahilinde değerlendirilmiş olan ve halihazırda geçerli olan bir Ortak Kriterler belgesine sahip olan tüm ürünlerin ve koruma profillerinin kısa özelliklerini veren bir belgeyi düzenli olarak yayınlamak (Belgelendirilmiş/Onaylanmış Ürünler Listesi);
- i) Programın organizasyonunu, ilkelerini, kurallarını ve prosedürlerini belgelemek, bu belgeleri halka açık hale getirmek ve güncel durumda tutmak;
- k) Programın kurallarına uyulmasını sağlamak;
- l) Programın kural ve ilkelerini oluşturmak ve uygun olduğunda değiştirmek;
- m) Programın yürütülmesinde Program faaliyetlerinde pay sahibi olan tüm tarafların çıkarlarına uygun önemin verilmesini sağlamak.

Bu Düzenlemeye dahil olma bağlamında, Nitelikli bir Katılımcı ile bağlantılı Belgelendirme/Onaylama Kuruluşu da bu Düzenlemenin hükümlerine uygun olarak bu Düzenleme ile ilgili faaliyetler için teknik destek sağlamaktan sorumludur.

B.3 Değerlendirme Tesislerinin Akreditasyonu ve Lisanslandırılması

Bir Değerlendirme Tesisi yasalar veya ikincil mevcut kapsamında oluşturulmamışsa, bir Programa katılacak olması durumunda iki koşulu yerine getirmesi gerekir:

- a) ilgili ülkede tanınmış olan bir Akreditasyon Kuruluşu tarafından akredite edilmiş olmak;
ve
- b) Programın yönetiminden sorumlu olan CB tarafından lisanslanmış veya sair biçimde onaylanmış olmak.

Akreditasyon, Değerlendirme Tesisinin tarafsızlığını ve genel teknik, yönetsel ve prosedür konusunda yetkinliğini ve bu koşullar BT güvenliği alanının özellikleri ile uyumlu olduğu ölçüde EN 45001 veya ISO Kılavuz 25'in koşullarını karşıladığını göstermesini zorunlu kılar.

Değerlendirme Tesisi ayrıca CB'yi tatmin edecek biçimde özel BT güvenlik değerlendirmesi alanında teknik açıdan yeterli olduğunu ve söz konusu Programın kurallarına bütünüyle uyacak bir durumda göstermek zorundadır. Buna, ilgili değerlendirme kriterlerini ve değerlendirme yöntemlerini doğru ve tutarlı bir biçimde uygulama yeteneğine sahip olduğunu ve değerlendirilmekte olan BT ürünleri veya koruma profillerine ve değerlendirme sürecinin kendisine ilişkin hassas veya korunan bilgilerin korunması için gerekli olan katı güvenlik

koşullarını karşıladığını göstermesi de dahildir.

Belirli bir Program dahilinde deęerlendirmeler yapmak üzere yetkili kılınmış veya onaylanmış bir Deęerlendirme Tesisi bir BT Güvenlik Deęerlendirme Tesisi (ITSEF) olarak tanınır.

Her bir Program için yetkilendirme veya onaylama ilkesi, güvenlięin ve eęitim gereksinimlerini ve yetkilendirilecek veya onaylanacak bir başvuru yapmak için gerekli prosedürlerin ve bu tür başvuruların işleme tabi tutulmasına ilişkin ayrıntıları içerir.

Belgelendirme/Onaylama Kuruluşu için Koşullar

C.1 Genel Koşullar

CB'nin hizmetleri aşırı mali veya diğer koşullara bağlı olmaksızın sağlanabilmelidir. CB'nin çalışma konusunda bağlı olduğu prosedürler ayırım yapılmaksızın uygulanmalıdır.

C.2 İdari Yapı

CB'nin tarafsız olmalıdır. Özellikle, belgelendirme/onaylama işleminde ticari veya mali çıkarı olan herhangi birinin uygun olmayan etkisi ve denetiminden uzak olarak yürütülen günlük işlemleri olanak sağlayacak olan üst düzey bir yöneticiye karşı sorumlu olan devamlı bir personel kadrosuna sahip olmalıdır.

C.3 Kuruluşun Yapısı

CB aşağıdakilere sahip olmalı ve istek üzerine sağlamalıdır:

- kuruluşun sorumluluğu ve raporlama yapısını açık bir biçimde gösteren bir şema;
- kuruluşun mali destek sağladığı araçların bir tanımı;
- Değerlendirme ve Belgelendirme/Onaylama Programını tanımlayan bir belge;
- yasal durumunu açık olarak belirten bir belge.

C.4 Belgelendirme/Onaylama Personeli

CB'nin personeli yürüttükleri görevler konusunda uzman olmalıdır. Kadroda yer alan her personelin ilgili nitelikleri, eğitimi ve deneyimine ilişkin bilgiler CB tarafından muhafaza edilmeli ve güncel olarak tutulmalıdır.

Görev ve sorumluluklarına ilişkin açık, güncel ve belgelenmiş yönergeler Personele sağlanmalıdır.

İş için dışarıdan bir kuruluşla sözleşme yapılması durumunda CB sözleşme kapsamındaki işi yürüten personelin bu EK'in ilgili koşulları karşıladığını güvence altına almalıdır.

C.5 Belgeler ve Değişiklik Denetimi

CB, kendi Değerlendirme ve Belgelendirme/Onaylama Programına ilişkin tüm belgelerin denetlenmesi için bir sistemi sürdürecektir ve aşağıdaki hususları sağlayacaktır:

- Uygun belgelerde yer alan güncel konuların ilgili tüm konumlarda sağlanabilmesi;
- Belgelerin uygun bir yetkilendirme olmaksızın değiştirilmemesi veya yürürlükten kaldırılmaması;
- Değişikliklerin, bunları bilmesi gereken kişilere derhal bildirilmesini ve acil ve etkin bir biçimde gerekli işlemleri yapacak konumda bulunmalarını;
- Yürürlükten kaldırılan belgelerin kuruluşta ve araçlarında tamamen kullanımdan

kaldırılması;

e) Programla doğrudan ilgisi bulunanların deęişikliklerden haberdar edilmesi.

C.6 Kayıtlar

CB kendi özel koşullarına uygun olacak ve Katılımcının tabi olduğu yargı yetkisi içinde uygulanan ilgili düzenlemelere uyacak bir kayıt sistemini sürdürecektir. Sistem her bir belgelendirme/onaylama ile bağlantılı olarak üretilen tüm kayıtları ve diğer evrakı içerecek, ayrıca her bir belgelendirme/onaylama işleminin gidişatının izlenmesini sağlamak üzere yeterli derecede eksiksiz olacaktır. Tüm kayıtlar en az beş yıllık bir süreyle güvenli ve erişilebilir bir biçimde saklanacaktır.

C.7 Belgelendirme/Onaylama Prosedürleri

CB, BT ürün veya koruma profilinin belgelendirilmesi/onaylanma işleminin ilgili BT güvenlik değerlendirme kriterleri ve yöntemlerine uygun olarak yürütülmesini sağlamak için gerekli tesis ve belgelendirilmiş prosedürlere sahip olacaktır.

C.8 Değerlendirme Tesislerinin Koşulları

CB, BT Güvenlik Değerlendirme Tesislerinin bu Düzenlemede belirtilen koşullara uygun olmasını sağlayacaktır.

CB her bir BT Güvenlik Değerlendirme Tesisi için, korunan bilgilerin ve değerlendirme ve belgelendirme/onaylama süreçlerinin gizliliğini sağlamak için gerekli düzenlemeler de dahil olmak üzere ilgili tüm prosedürleri kapsayan gerektiği şekilde yazılmış bir sözleşme düzenleyecektir.

C.9 Kalite El Kitabı

CB, bu EK'in koşullarına uymak için izlediği prosedürleri düzenleyen bir Kalite El Kitabına ve belgelerine sahip olmalıdır. Bunlara en azından aşağıda belirtilenler dahil olmalıdır:

- a) kalitenin muhafaza edilmesi için bir ilke bildirim;
- b) CB'nin yasal konumuna ilişkin kısa bir tanımlama;
- c) üst düzey yönetici ile diğer belgelendirme/onaylama personelinin adları, nitelikleri ve görevleri;
- d) belgelendirme/onaylama personeli için eğitim düzenlemelerinin ayrıntıları;
- e) üst düzey yöneticiden kaynaklanan yetki, sorumluluk çizgilerini ve görevini gösteren bir organizasyon şeması;
- f) BT ürün veya koruma profili değerlendirmelerini izlemek için gerekli prosedürlerin ayrıntıları;
- g) Ortak Kriterler belgelerinin suistimalini önlemek için gerekli prosedürlerin ayrıntıları;
- h) tüm yüklenicilerin kimlikleri ve bunların ehliyetlerinin değerlendirilmesi ve izlenmesi için belgelendirilmiş prosedürlerin ayrıntıları;
- i) yasal yollara başvurma veya uzlaşmaya ilişkin tüm prosedürlerin ayrıntıları.

C.10 Gizlilik

CB, Katılımcıların ulusal yasalarının, mevzuatının, kararnamelerinin veya yönetmeliklerinin izin verdiđi ölçüde, belgelendirme/onaylama faaliyetleri sırasında elde ettiđi bilgilerin gizliliđini kuruluşunun her seviyesinde sağlamak için gerekli düzenlemeleri yapacak ve bu Düzenleme kapsamındaki belgelendirme/onaylama faaliyetleri sırasında elde ettiđi korunan bilgileri izinsiz olarak açıklamayacaktır.

C.11 Yayınlar

CB bir Belgelendirilmiş/Onaylanmış Ürünler Listesini üretecek ve gerekli olduğu şekilde güncelleyecektir. Bu listede sözü edilen her bir BT ürünü veya koruma profili açık bir biçimde tanımlanmalıdır. Liste halka açık olmalıdır.

Değerlendirme ve Belgelendirme/Onaylama Programının bir açıklaması yayınlanmış olarak sağlanabilmelidir.

C.12 Yasal yollara başvurma veya Uzlaşma

CB kendi içindeki, bağlantılı ITSEFlerle ve bunların *müşterileri* ile olan anlaşmazlıkları ele almak için gerekli prosedürlere sahip olmalıdır.

C.13 Dönemsel Gözden Geçirme

CB, bu Düzenlemenin amaçlarını paylaşmaya devam etmekte olduğunu güvenceye almak için program çalışmalarına yönelik dönemsel gözden geçirmeler yapmalıdır.

C.14 Ortak Kriter Belgelerinin Amaç Dışı Kullanımı

CB Ortak Kriterler belgelerinin kullanımına ilişkin olarak uygun bir denetim uygulayacaktır.

Belgelerin amaç dışı kullanımını önlemek veya karşı koymak ve belgelere yönelik veya Değerlendirme ve Belgelendirme/Onaylama Programı hakkında yanlış, yanıltıcı veya uygun olmayan beyanları önlemek ve karşı koymak için uygun idari, prosedürel veya yasal önlemleri almak CB'nin sorumluluğundadır.

C.15 Ortak Kriterler Belgelerinin İptali

CB, Ortak Kriterler belgelerinin iptal edilmesi için gerekli prosedürleri belgelendirmiş olmalı ve Belgelendirilmiş/Onaylanmış Ürünler Listesinin bir sonraki yayınında iptali duyurmalıdır.

İsteğe Bağlı Dönemsel Değerlendirmeler

Yönetim Komitesi, uyumlu bir CB'ye ilişkin dönemsel bir değerlendirmenin yürütülmesi için bir veya daha fazla sayıda Nitelikli Katılımcıyı (CB'nin sponsoru hariç) seçebilir. Değerlendirmeler Sponsorun yazılı onayı veya talebi dışında yürütülemez ve bu tür bir onay bir değerlendirmeden önce veya değerlendirme sırasında geri çekilebilir veya iptal edilebilir. Sponsor, değerlendirme ekibinin seçimine ilişkin olarak CB'nin sahip olabileceği tereddütleri Yönetim Komitesine iletmesi gerekir. Değerlendirmeler aşağıda belirtildiği şekilde ve değerlendirmelerin yeknesak bir standartta sürdürülmesini ve kaynakların öngörülebilir bir şekilde taahhüt edilmesini sağlamaya yönelik olarak Yönetim Komitesi tarafından yayınlanan kılavuzlara uygun olarak yürütülmelidir.

Değerlendirmeleri yürüten Katılımcı veya Katılımcılar, Yönetim Komitesince kabul edilebilecek olan iki nitelikli uzmandan oluşan birincil değerlendirme ekibi için aday gösterebilirler. Herhangi bir Katılımcı masrafları kendisine ait olmak üzere ilave bir uzman sağlayabilir. *Bağlı* CBler için birincil değerlendirme ekipleri sağlanmasına ilişkin masraflar Nitelikli Ortaklar arasında İcra Alt Komitesi tarafından kabul edilecek olan adil bir biçimde dağıtılmalıdır. Değerlendirilmekte olan CB'nin bağlı bir CB olmaması durumunda, söz konusu CB, birincil değerlendirme ekibinin değerlendirmeden kaynaklanan tüm masraflarını (seyahat, barınma, yaşam masrafları ve maaşlar da dahil olmak üzere²) karşılamalıdır.

Dönemsel değerlendirmeye tabi tutulmakta olan CB bir ay içinde o sırada uygulanmakta olan program belgelerinin tamamını sağlamalıdır. Uzmanlar, CB'nin bu Düzenlemenin amaçlarını paylaştığından emin olmak için belgeleri gözden geçirirler ve bulgularını Yönetim Komitesine rapor ederler.

Doğrudan ilişkili olan Katılımcılar tarafından mutabık kalındığı şekilde uygun bir BT ürünü üzerinde Ortak Kriterler Değerlendirme Notu 3 veya 4. Seviyesinde bir resmi olmayan belgelendirme/onaylama işlemi gerçekleştirilmeli ve söz konusu Katılımcılar arasında bir gizlilik sözleşmesi imzalanmalıdır.

Uzmanlar, dönemsel değerlendirmeye tabi tutulan CB'nin değerlendirme ve belgelendirme/onaylama süreçlerinin tüm yönlerine uygun bir biçimde hareket ettiği konusunda tatmin olmalıdırlar. Bu sorumluluğu yürütürken uzmanlar belgelendirme/onaylama sürecinin bazı yönlerini hariç tutmak isteyebilirler. Değerlendirmeye tabi tutulan bir CB buna olanak sağlamalıdır.

Uzmanlar ayrıca bu Düzenlemede ve özellikle de bu Düzenlemenin B ve C Eklerinde tanımlanmış korunan bilgilerin gizliliğini sağlamak için gerekli olan prosedürlerin uygulanmasını da kontrol edeceklerdir.

Değerlendirme ve belgelendirme/onaylama işleminin uygun aşamalarında, uzmanlar tarafından kontrol edilmek üzere aşağıdaki belgeler sağlanmalıdır:

- a) Güvenlik Hedefi;
- b) Değerlendirme Teknik Raporu;
- c) Yukarıdaki belgelere ilişkin olarak Belgelendirme/Onaylama Kuruluşu tarafından yapılacak yazılı yorumlar;
- d) Belgelendirme/Onaylama Raporu.

Diğer deęerlendirme raporları istek üzerine Yönetim Komitesi tarafından yayınlanan kılavuzlara uygun olarak sağlanmalıdır.

² Deęerlendirmeyi yürüten Nitelikli Katılımcıya ulusal yasalar veya mevzuat nedeniyle bu tür bir ödeme yapılmasının yasaklandığı durumlarda bu koşul kaldırılabilir.

Yukarda atıfta bulunulan tüm belgeler İngilizce ya da uzmanların kabul edeceği bir dilde sağlanmalıdır. Değerlendirme raporları yalnızca gerekli olduğunda tercüme edilmelidir. Bir değerlendirmeye onay veren Katılımcılar, dille ilgili herhangi bir sorun için uzmanların kabul edeceği bir çözümü bulmalı ve uygulamalıdır.

Uzmanlar bulgularını Yönetim Komitesine rapor ederler ve değerlendirmeye ilişkin olarak önerilerde bulunurlar. Yönetim Komitesi resmi olmayan belgelendiricilerin/onaylayıcıların raporlarını gözden geçirir. Yönetim Komitesi, raporun kendi içinde tutarlı olduğu ve sonuçların kanıtlara dayalı olduğu konusunda tatmin olursa, sonuç değerlendirmeye tabi tutulan Belgelendirme/Onaylama Kuruluşuna gönderilir. Değerlendirilmekte olan CB, en fazla altı ay sonra değerlendirmede belirlenen tüm eksiklikleri düzelttiğini göstermelidir.

Ek E

Belge ve Hizmet İşaretleri

Bu Düzenlemenin koşulları kapsamında düzenlenen her bir Ortak Kriterler belgesi aşağıdaki işareti taşımalıdır:



Bu işaret, Ortak Kriterler belgesinin bu Düzenlemenin Katılımcılarından biri tarafından verilmiş olduğunu ve Katılımcısının belgenin bu Düzenlemenin koşullarına uygun olarak düzenlendiğine ilişkin beyanını teyit eder.

Bir Ortak Kriterler belgesinin alınmasının ardından işaret satıcılar tarafından belgenin düzenlendiği ürünün reklamı, pazarlanması ve satışı ile bağlantılı olarak kullanılabilir. Bu Düzenlemenin Katılımcılarından biri işareti kendisine ait olan mal veya hizmetlerin tanıtımını yapmakta kullanmayacaktır.

Bu Tanıma Düzenlemesinin hizmet işareti aşağıda göstermiştir:



Bu hizmet işareti, bu Düzenlemeyle bağlantılı olarak bir Katılımcı (veya uyumlu CBler) tarafından yürütülen hizmetleri belirlemek, reklamını yapmak ya da pazarlamak için kullanılacaktır.

Bu Düzenlemeye katılımın sona ermesinden sonra, sona erdiren Katılımcı hizmet işaretini kullanmayacaktır.

Katılımcılara Sağlanması Gereken Bilgiler

F.1 Program Bilgileri

Her bir uyumlu CB, sorumlu olduğu Değerlendirme ve Belgelendirme/Onaylama Programının aşağıdaki hususlarını kapsayan belgelerin kopyalarını Katılımcılara sağlayacaktır:

- a) karşılıklı olarak mutabık kalınmış olan BT güvenlik değerlendirme kriterleri ve yöntemleri uyarınca değerlendirme ve belgelendirme/onaylama yapılması için ulusal kurallar ve düzenlemeler dizisi;
- b) Programın organizasyonel yapısı;
- c) Belgelendirme/Onaylama Kuruluşunun Kalite El Kitabı;
- d) akreditasyon veya lisanslama/onaylama ilkesi;
- e) Programla bağlantılı olan ITSEFlerin isim ve adresleri ve konumları (örn., resmi veya ticari);
- f) (mümkünse) EN 45001 veya ISO kılavuz 25'in ulusal yorumu.

Bu belgelerde değişiklik yapılan veya yeni uyarlamalarının yayınlandığı her bir durumda, değişikliklerin veya yeni uyarlamaların kopyaları derhal tüm Katılımcılara sağlanacaktır.

F.2 Ortak Kriterler Belgeleri ve Belgelendirme/Onaylama Raporları

Her bir Katılımcı, verdiği Ortak Kriter belgesinin, Belgelendirme/Onaylama Raporunun ve Belgelendirilmiş/Onaylanmış Ürün Listesinin bir kopyasını diğer Katılımcıların her birine sağlayacaktır. Bir uyumlu CB'nin bir BT ürününü veya koruma profilini Belgelendirilmiş/Onaylanmış Ürünler Listesinin dışında bırakması veya bu listeden çıkarması durumunda, söz konusu CB Katılımcılara derhal bildirimde bulunacaktır.

F.3 Bu Düzenlemenin Koşullarını Etkileyen Genel Bilgiler

Her bir Katılımcı söz konusu ülkede geçerli olan ve Ortak Kriterler belgelerinin tanınmasını doğrudan etkileyen tüm ulusal yasaların, ikincil mevzuatın, idari düzenlemelerin ve resmi yükümlülüklerin etkisine ilişkin bir beyanda bulunacaktır.

Her bir Katılımcı, aşağıda belirtilen hususlarda yapılan veya yapılacak olan ve Katılımcının bu Düzenlemenin koşullarına uygun olarak hareket etme yeteneğini etkileyebilecek olan tüm değişiklikleri derhal Yönetim Komitesinin dikkatine sunacaktır:

- a) ulusal yasalar, idari düzenlemeler veya resmi yükümlülükler; ya da
- b) kendisine ait Değerlendirme ve Belgelendirme/Onaylama Programı/Programlarının işleme veya süreçleri

F.4 Gizlilik Kuralları

Bu Düzenleme kapsamında yer alan bazı prosedürler zaman zaman, izinsiz olarak açıklanması BT

ürünlerinin imalatçıları da dahil, ancak bunlarla sınırlı olmamak üzere Katılımcılara, Katılımcılarla bağlantılı taraflara veya bu Düzenlemeye dahil olan taraflara fiilen zarar verebilecek olan korunan bilgilerin deęiş tokuşunu gerekli kılabilir.

Bu bilgilerin uygun biçimde ele alınması ve bu tür bir korumanın gerçekleştirilmesini sağlamak için gerekli prosedürlerin tanımlanmış olması çok önemlidir.

Bir belge basılı (basılı kopya) veya elektronik biçimde olabilir.

Korunan bilgileri içeren belgeler "RA in Confidence" şeklindeki özel bir işaret sayesinde tanınacaktır. Gönderen taraf bu özel işareti uygulayacaktır.

Her bir Katılımcı izleyen koruma kurallarını uygulamak ve bunları uygulamak için bir sistem oluşturmak için çaba gösterecektir.

F.4.1 Korunan bilgilerin oluşturulması ve yönetilmesi

Korunan bilgi içeren her belge gönderenin kimliğine ilişkin kısa, ancak belirgin bir ifade ile düzenlenme tarihini taşıyacaktır. Ayrıca bu belge kendisini özgün kılacak bir tanıtıcıya da sahip olacaktır (örn. Birer birer artan bir seri numarası?) Bir belgenin değiştirilmesi durumunda, belgenin tanıtıcısı da en azından bir sürüm numarası ve düzenleme tarihi kadarıyla değiştirilmelidir.

Bir belge ya üzerinde belirtilmiş olan süre içinde ya da böyle belirli bir ifadenin bulunmadığı durumlarda gönderen tarafın korunan belge için koruma talebini bıraktığı ana kadar korunan belge olarak kalır.

F.4.2 Korunan bilgilerin ele alınma prosedürleri

Korunan bilgilerin işaretlenmesi

Belgelerin korunan bilgileri içeren basılı kopyalarının her sayfasında "RA in Confidence" kelimeleri ve özgün tanıtıcı yer alacaktır. Koruma gerektiren süre birinci sayfada gösterilebilir.

Korunan bilgileri içeren bilgisayarlar için çıkarılabilir manyetik ortam en azından "RA in Confidence" kelimelerini ve özgün tanıtıcıyı içeren bir etikete sahip olmalıdır. Bir Katılımcıdan başka bir katılımcıya nakledilirken içeriğini belirten basılı bir liste manyetik ortama iliştilmelidir.

Depolama ve korunan bilgilerin emniyetine ilişkin kurallar

Depolama ve koruma kuralları taslak uyarlamalar da dahil olmak üzere korunan bilgileri içeren belgelere uygulanır.

Korunan bilgiler bir bilgisayarda işlendiğinde veya depolandığında uygun biçimde korunmalıdır. Korunan bilgilerin depolandığı herhangi bir çıkarılabilir manyetik ortam, aynı bilgileri içeren bir belgeymiş gibi korunmalıdır.

Korunan bilgilerin iletilmesi

Korunan bilgileri içeren ve posta ile yollanması gereken belgeler bir iç ve dış zarf sistemi içine yerleştirilmelidir. Dış zarfın üzerinde RA yazışması için alıcı taraf olan Katılımcının temas noktası olarak görevlendirdiği kişinin adresi yer alacaktır. İç zarf/zarflar korunan bilgileri içerecek ve üstlerinde istenilen alıcının adı ile birlikte "RA in Confidence" kelimeleri yer alacaktır.

Korunan bilgilerin elektronik olarak iletilmesi durumunda, iletim güvenli elektronik araçlar kullanılarak yapılacaktır.

Korunan bilgilerin kopyalanması

Korunan bilgiler yalnızca çalışmalar açısından açıkça haklı görülecek nedenlerle bir alıcı tarafından kopyalanabilir.

Çıkarılabilir manyetik ortamların ve korunan bilgilerin yok edilmesi

Artık gerek duyulmadığında, korunan bilgileri içeren çıkarılabilir manyetik ortamlar güvenli bir biçimde yok edilmeli ve bu işlem uygun bir kayıt defterine kaydedilmelidir.

Korunan bilgiler yok edilmeden önce manyetik ortamdan tamamen silinmelidir.

Korunan bilgilere erişim

Gönderici ile aksi şekilde mutabık kalınmadığı sürece ve yasalar tarafından izin verilen ölçüde, bir Katılımcı tarafından alınmış korunan bilgilere erişim doğrudan Katılımcı tarafından çalıştırılan personel ya da Katılımcı kuruluşunun başkanının takdirinde olmak üzere bilmesi gereken resmi görevlilerle sınırlı olacaktır. Korunan bilgilerin gizli tutulması yükümlülüğünün bu Düzenlemeyi yaşatması beklenmektedir.

F.4.3 Ek koruma derecesi

Arada sırada bilgiler daha yüksek derecede bir korumayı gerekli kılabilir. Bu gereksinim duruma göre belirlenecektir.

Yeni Uyumlu Belgelendirme/Onaylama Kuruluşları

G.1 Resmi Talep

Bir CB'nin bu Düzenleme kapsamında uyumlu CB statüsünü kazanmak istemesi ve Madde 5 de ve Madde 5 de belirtilen Eklerde ortaya konan koşulları yerine getirdiğine inanması durumunda, kendi ülkesindeki Katılımcı aracılığıyla yazılı bir başvuruda bulunması gerekir. (Not: CB ve Katılımcı bir ve aynı kuruluş olabilir). Katılımcı başvuruyu desteklerse CB'nin Sponsoru olur ve başvuruyu Yönetim Komitesine iletmesi gerekir. İletilen başvuru, başvuranın bu Düzenlemede belirtilen koşulları karşılama yeteneğinin Sponsor tarafından resmen onaylandığı anlamına gelmeyecektir.

Başvuru, başvuranın bu Düzenleme ve planlar kapsamında aşağıdakilere uymayı kabul ettiğine ilişkin yazılı bir beyanı içermelidir:

- a) yapılan başvurunun sonucu olumlu olsun veya olmasın, başvurudan veya başvuruyu kabul edip işleme almaktan kaynaklanan (seyahat, konaklama ve yaşam masrafları ve başvuran Sponsorunun bağlı CB'si olmak için başvuruyorsa ayrıca birincil değerlendirme ekibinin maaşları da dahil olmak üzere³) birincil değerlendirme ekibinin tüm masraflarının karşılanması (Bkz aşağıda G. 3);
- b) aşağıda ayrıntıları verilen belgelerin sağlanması, ve
- c) başvuranın gözetiminde değerlendirilecek ve belgelendirilecek/onaylanacak olan uygun bir ürünün Katılımcıların bir veya birden fazla temsilcisine resmi olmayan belgelendirme/onaylama için sunulması.

G.2 Sağlanacak Belgeler

Uygunluk sürecinde elde edilen tüm belge ve bilgiler Ek F.4 hükümleri uyarınca işlemde geçirilecektir. Bu gizlilik kuralları gizlilik sözleşmesi/sözleşmeleri aracılığıyla tamamlanabilir.

Aşağıdaki belgeler sağlanacaktır:

a) aşağıdakiler de dahil olmak üzere başvuranın Değerlendirme ve Belgelendirme/Onaylama Programının kapsamı, organizasyonu ve işlemesine ilişkin eksiksiz bir tanımlama:

- CB'nin adı, adresi ve birincil temas noktası;
- CB Kalite El Kitabı;
- CB'nin bağlı kılınması ve yetkisinin yasal veya diğer temeli;
- Programın genel yönetiminin denetlenmesi, ilke sorunlarına karar verilmesi ve anlaşmazlıkların giderilmesine yönelik sistem;
- belgelendirme/onaylama için prosedürler;
- Programa katılan ITSEFlerin adları ve adresleri ve konumları (ticari veya resmi);

³ Değerlendirmeyi yürüten Nitelikli Katılımcının ulusal yasalar veya mevzuata bağlı olarak bu tür bir ödemeyi almasının yasaklandığı durumlarda bu koşul kaldırılabilir.

- akredite eden Değerlendirme Tesisleri için lisanslama/onaylama ilke ve prosedürleri;
- ticari sırların ve diğer hassas bilgilerin korunması için Program dahilinde uygulanan kurallar;
- CB'nin ITSEFLerin aşağıdaki hususları yerine getirmesini sağlamakta izlediği prosedürler:
 - değerlendirmelerin tarafsız olarak yürütülmesi;
 - karşılıklı mutabık kalınmış BT kriterlerinin ve yöntemlerinin doğru ve tutarlı bir biçimde uygulanması; ve
 - söz konusu gizli bilgilerin korunması.

b) Programın Belgelendirilmiş/Onaylanmış Ürünler

Listesinin son yayını;

- c) başvuranın gözetimi altında yayınlanan iki veya daha fazla Ortak Kriterler belgeleri ve Belgelendirme/Onaylama Raporları;
- d) başvuranın ülkesinde uygulanan ve değerlendirmeleri ve belgelendirme/onaylamaları ya da Ortak Kriterler belgelerinin tanınmasını doğrudan etkileyen tüm ulusal yasalar, ikincil mevzuat, idari düzenlemeler ve resmi yükümlülüklerin etkilerine ilişkin bir beyan; ve
- e) başvuranın, kendisine veya Ortak Kriterler belgeleri verdiği BT ürünlerine ve koruma profillerine bu Düzenleme kapsamında adil olmayan bir avantaj sağlayacak veya başka bakımlardan bu Düzenlemenin işlemlerini ya da amacına zarar verecek herhangi bir yasa, ikincil mevzuat veya resmi idari buyruğa bağlı olmadığına ya da bağlı olmak üzere olmadığına ilişkin bir beyan.

G.3 Yönetim Komitesinin Yanıtı

Yönetim Komitesi, başvuruyu almasını izleyen üç hafta içinde kabul edecek ve hedef olarak üç aylık bir süre içinde başvuruya bir ön yanıt verecektir. Ön yanıt, belgelerin teknik değerlendirmesinin ve resmi olmayan belgelendirme/onaylamanın başarılı olduğu varsayımıyla başvurunun kabul edilebilir olduğunu belirtecektir.

Yönetim Komitesinin başvuran tarafından sağlanan bilgilerin tatminkar olduğunu ve herhangi bir açıklama veya ek bilgiye gerek duyulmadığını kabul etmesi durumunda başvurudan, resmi olmayan belgelendirme/onaylama için Ortak Kriterler Değerlendirme Notu 3 veya 4. Seviyesinin talep edildiği en az iki ürünü aday göstermesi istenecektir.

Başvuran her bir ürün için bir profil özeti ve bunların değerlendirilmesi ve belgelendirilme/onaylanmasına yönelik düzenlemelerin ayrıntılarını sunacaktır. Yönetim Komitesi aday bilgilerini almasının ardından hedef olarak bir aylık bir süre içinde ürünlerde birini resmi olmayan belgelendirme/onaylama için seçecek ve başvurana gerekli bildirim yapacaktır.

Yönetim Komitesi resmi olmayan belgelendirme/onaylama işlemini yürütmek için bir veya daha fazla sayıda Nitelikli Katılımcı (Sponsor dışında) seçecektir. Seçilen Katılımcı veya Katılımcılar iki uzmandan oluşacak bir birincil değerlendirme ekibi için aday göstereceklerdir. Katılımcılardan herhangi biri (Sponsor dahil) masrafları kendine ait olmak üzere ek bir uzman sağlayabilir. Yönetim Komitesi başvurana uzmanların adlarını ve ana kuruluşları bildirecektir.

G.4 Resmi Olmayan Belgelendirme/Onaylama Prosedürü

Yönetim Komitesi tarafından yayınlanan kılavuzlara dayalı olarak (değerlendirmelerin yeknesak bir standartta yapılmasını sağlayacak olan) ve kendilerine sağlanan tüm bilgilerin ışığında değerlendirme ve belgelendirme/onaylama sürecinin ne kadarını izlemeleri (shadow) gerektiğine uzmanlar karar verecektir. Yönetim Komitesi kılavuzu değerlendirmenin gerektireceği kaynakların bir tahminine olanak sağlamak için başvuran CB'ye sağlanacaktır.

Uzmanlar, araştırmalarını tamamlamalarının ardından bir ay içinde ve seçilen ürüne ilişkin değerlendirme ve belgelendirme/onaylama sürecinin tamamlanmasının ardından en geç bir ay içinde bulgularını yazılı olarak adayın başvurusunun kabul veya reddedilmesine ilişkin tavsiyeleriyle birlikte Yönetim Komitesine rapor edecektir. Yönetim Komitesi hedef olarak uzmanların raporunun alınmasını izleyen iki ay içinde kararını başvurana yazılı olarak iletacaktır. Reddetme durumunda Komite kararın nedenlerinin bir özetini ve kararın dayandığı temel kanıtları sağlayacaktır. Kabul etmesi durumunda Komite Ek K'yı uygun biçimde güncelleyerek kararı kayda geçirecektir.

Düzenlemenin İdaresi

H.1 Sorumluluklar ve Yetkiler

Yönetim Komitesi, bu Düzenlemenin konumu, koşulları ve işlemesiyle ilgili tüm ilke konularında hareket eder. Yeni Katılımcıların kabulü, yeni CBlerin uyumluluğu ve Düzenlemenin kapsamında yapılan değişiklikler konusunda karar verir.

H.2 Oluşum

Tüm Katılımcılar Yönetim Komitesinde temsil edilecektir. Yönetim Komitesinin Başkanı bir yılı aşmayacak bir süre için görev yapmak üzere Katılımcılar arasından Yönetim Komitesi tarafından atanacaktır. Katılımcıların her biri sırayla başkanlık yapacaktır. Mevcut başkan Yönetim Komitesine idari destek sağlayacaktır.

H.3 Kararlar

Yönetim Komitesinde temsil edilen her ülke bir oya sahip olacaktır. Bu Düzenlemenin başka bir yerinde oybirliği için özel bir koşul getirilen durumlar dışında kararlar salt çoğunlukla alınacaktır.

H.4 Katılım

Yönetim Komitesi belirli konularda bilgi vermek üzere uzmanları veya teknik danışmanları toplantılarına katılmak için davet edebilir.

H.5 Uzmanlardan Yararlanma

Yönetim Komitesi gerektiğinde destek ve öneri sağlamaları için amaca özel uzman grupları oluşturabilir.

H.6 Toplantıların Sıklığı

Yönetim Komitesi tüm üyelerin katılımıyla yılda bir kez veya uygun gördüğü şekilde toplanacaktır.. Uygulanabilir olması halinde kararlar e-posta ile alınacaktır.

H.7 İcra Alt Komitesi

Yönetim Komitesi, Düzenleme Grubunun günlük işlerini yönetmek ve Yönetim Komitesine teknik danışmanlık ve tavsiyeler sağlamak için bir İcra Alt Komitesi kuracaktır.

İcra Alt Komitesi, Yönetim Komitesince belirlenen sayı ile sınırlı olmak üzere Nitelikli Katılımcılardan ve isteğe bağlı ek Katılımcılardan oluşacaktır. İcra Alt Komitesinin işi şunları içerir:

a) Düzenleme Grubunun işlerinin yürütülmesi için prosedürlerin geliştirilmesi ve önerilmesi;

b) yeni CBlerin teknik uyumlarının değerlendirilmesi;

- c) bu Düzenlemede yapılacak deęişikliklerin önerilmesi;
- d) sürekli izleme faaliyetlerinin yönetilmesi;
- e) bu Düzenlemenin koşulları ve uygulamasına ilişkin teknik anlaşmazlıkların çözülmesi;
- f) BT güvenlik değerlendirme kriterlerinin ve BT güvenlik değerlendirme yöntemlerinin geliştirilmesinin yönetilmesi;
- g) kriterlerin veya metodolojinin gelecekteki uyarlamalarını etkileyebilecek olan yorumlara ve sonuç olarak ortaya çıkan tüm kararlara arka plan oluşturması açısından geçmişe yönelik veritabanlarının muhafazasının yönetilmesi.

Belgelendirme/Onaylama Raporlarının İçerikleri

I.1 Belgelendirme/Onaylama Raporu ve bu Raporun Kullanımı

Değerlendirme Teknik Raporu (ETR) Değerlendirme Tesisi tarafından Belgelendirme/Onaylama Kuruluşu için hazırlanır ve Belgelendirme/Onaylama Raporunun temel dayanağı görevini görür. ETR'nin amacı tüm kararları, bunların gerekçelerini ve BT ürünü veya koruma profilinin geliştirilmesi sırasında tespit edilen hatalar ve değerlendirme sırasında fark edilen tüm istismar edilebilecek güvenlik açıkları da dahil olmak üzere değerlendirme sırasında yürütülen çalışmalardan elde edilen tüm bulguları sunar. ETR, değerlendirme sonuçlarını gerekçelendirmek için korunan bilgileri gerekli oranda içerebilir.

Belgelendirme/Onaylama Raporu, ilgilenen tüm taraflar için BT ürünü veya koruma profiline ilişkin ayrıntılı güvenlik bilgisinin kaynağıdır. Amacı, BT ürünü veya koruma profili hakkında tüketicilere yararlı bilgiler sağlamaktır. Korunan bilgiler, Güvenlik Hedefi ile aynı şekilde değerlendirilmiş olan BT ürününün güvenli biçimde yerleştirilmesi açısından tüketici için gerekli olan bilgileri içerdiğinden, Belgelendirme/Onaylama Raporunun bu bilgileri içermesi gerekli olmayıp hatta bu bilgileri içermemelidir.

I.2 Yönetici Özeti

Yönetici özeti tüm raporun kısa bir özetidir. Bu bölümde yer alan bilgiler hedef kitleye değerlendirme sonuçlarına ilişkin açık ve öz bir genel görünüm sunmalıdır. Bu bölümün hedef kitlesi güvenli BT sistemlerinin ve ürünlerinin geliştiricilerini, tüketicilerini ve değerlendiricilerini içerebilir. Yönetici özeti ile okuyucu BT ürünü veya koruma profiline ve raporun sonuçlarına ilişkin temel bir aşinalık kazanabilir. Bazı müşterilerin (örn: akreditörler, yönetim) raporun yalnızca bu bölümünü okuma olasılığı olduğundan tüm önemli değerlendirme bulgularının bu bölümde yer alması önemlidir. Bir yönetici özeti bunlarla sınırlı olmamak kaydıyla aşağıdaki hususları içermelidir:

- a) Değerlendirilen BT ürününün adı, değerlendirmenin parçası olan ürüne ait bileşenlerin dökümü, geliştiricinin adı ve sürümü;
- b) BT güvenlik değerlendirme tesisinin adı;
- c) Değerlendirmenin tamamlanma tarihi, ve
- d) Raporun sonuçlarının kısa bir açıklaması:
 - güvence paketi;
 - işlevsellik;
 - değerlendirilen BT ürünü tarafından ele alınan tehdit ve Örgütsel Güvenlik İlkelerinin (OSP'ler) özeti;
 - özel yapılandırma gereksinimleri;
 - işletim ortamına ilişkin varsayımlar;
 - sorumluluğun reddi.

I.3 Tanıtma

Değerlendirilen BT ürününün açık bir şekilde tanıtılması gerekir. Yazılım sürüm numarası, ilgili tüm yazılım yamaları, donanım sürüm numarası ve çevreirim aygıtlarının (örn: manyetik bant

sürücüler, yazıcılar, vs) tanıtılması ve kaydedilmesi gerekir. Bu işlem, değerlendirilen BT ürününü eksiksiz biçimde tanıtmak için gerekli olan etiketleme ve açıklayıcı bilgileri sağlar. Değerlendirilen BT ürününün eksiksiz biçimde tanıtılması, kullanılmak veya gelecekteki değerlendirme çalışmaları için BT ürününe ilişkin tam ve doğru bir betimlemenin oluşturulmasını sağlayacaktır.

I.4 Güvenlik İlkesi

Güvenlik ilkesi bölümü BT ürününün güvenlik ilkesinin tanımını içermelidir. Güvenlik ilkesi BT ürününü güvenlik hizmetlerinin bir araya getirilmesi olarak tanımlar. Güvenlik ilkesi tanımı değerlendirilen BT ürününün uyması veya uygulaması gereken ilkeleri veya kuralları içerir.

I.5 Varsayımlar ve Kapsamın Açıklanması

BT ürününün kullanılması beklenen ortamın/konfigürasyonun güvenlik unsurları bu bölüme dahil edilmelidir. Bölüm, bertaraf edilmeyen tehditler açısından değerlendirmenin kapsamının açıklanmasının net bir biçimde ifade edilmesi için bir olanak sağlar. Kullanıcılar BT ürününün kullanımı ile bağlantılı tehlikelere ilişkin olarak bilgili kararlar verebilirler. Kullanım, ortamsal varsayımlar ve değerlendirme kapsamının bertaraf edilmeyen tehditler açısından açıklanması bu bölümde belirtilmelidir.

I.5.1 Kullanım Varsayımları

Değerlendirme çalışmaları sırasında ürün için bir taban çizgisi sağlamak için BT ürününün kullanımına ilişkin belirli varsayımlarda bulunulması gerekir. Kurulum ve yapılandırmanın düzgün yapıldığı, asgari donanım gereksinimlerinin karşılandığı vs gibi hususların hepsinin varsayılması gerekir. Bu bölüm değerlendirme sırasında BT ürünü hakkında yapılan kullanıma ilişkin tüm varsayımları belgeler.

I.5.2 Ortamsal varsayımlar

Değerlendirme çalışması sırasında BT ürünü için bir taban çizgisi oluşturmak için, ürünün kullanılacağı ortama ilişkin bazı varsayımlarda bulunulması gerekir. Bu bölüm değerlendirme sırasında BT ürününe ilişkin olarak yapılan tüm ortamsal varsayımları belgeler.

I.5.3 Kapsamın Açıklanması

Bu bölüm, ürünün değerlendirilmiş olan güvenlik fonksiyonları tarafından bertaraf edilmeyen BT ürününe yönelik tehditleri tanımlar. Bazı müşteriler bazı tehditlere BT ürününün karşılık verdiğini sanmalarına rağmen gerçekte durum böyle olmayabilir. Bu nedenle bertaraf edilmeyen bu tehditlerin açıklanmak üzere listelenmesi gerekir. Yine de tek bir ürün tarafından bertaraf edilemeyecek olan olası tüm tehditleri listelemek mümkün olmayabilir..

I.6 Mimari Bilgiler

Bu bölüm, Geliştirme – Üst Düzey Tasarım (ADV_HLD) başlıklı Ortak Kriterler güvence ailesinde (?) tanımlanmış olan teslim edilecek malzemelere dayalı olarak BT ürününe ve ana bileşenlerine ilişkin üst düzey bir tanımlama sağlar. Bölümün amacı ana bileşenlerin mimari ayrışma derecesinin nitelendirilmesidir.

I.7 Belgeler

Geliştirici tarafından tüketiciye ürünle birlikte sağlanan BT ürününe ait belgelerin tam listesi bu bölümde verilmektedir. İlgili tüm belgelerin sürüm numaralarını içermesi önemlidir. Belgeler en azından kullanıcı, yönetim ve kurulum kılavuzlarını tanımlarlar. Yönetim ve kurulum kılavuzu bilgilerinin tek bir belgede yer alması söz konusu olabilir.

I.8 BT Ürünün Test Edilmesi

Bu bölüm hem geliştiricinin hem de değerlendiricinin test çalışmalarını tanımlarken aynı zamanda test yaklaşımını, konfigürasyonunun, derinliğini ve sonuçlarını ortaya koyar.

I.9 Değerlendirilmiş Konfigürasyon

Bu bölüm BT ürününün değerlendirme sırasındaki konfigürasyonunu belgeler. Genel olarak yönetici veya kurulum kılavuzu BT ürününün doğru konfigürasyonu için gerekli ayrıntıları sağlayacaktır. BT ürünü, kullanıldığı ortama veya çalıştığı kuruluşun güvenlik ilkelerine bağlı olarak bir kaç şekilde yapılandırılabilir.

Bu tercihlere ilişkin kesin ayarlar ve yapılandırma ayrıntıları eşlik eden gerekçeleriyle birlikte bu bölümde ortaya konulmuştur. Tüm ek işletimsel notlar ve gözlemler ayrıca dahil edilebilir. Değerlendirilmiş olan ürünün kurulumu için bir taban çizgisi oluşturduğundan bu bölüm özel bir öneme sahiptir.

I.10 Değerlendirme Sonuçları

Bu bölüm BT ürününün karşıladığı güvence koşullarını belgeler. Bu koşulların ayrıntılı bir tanımı ve ürünün bunların her birini ne şekilde karşıladığına ilişkin ayrıntılar Güvenlik Hedefinde bulunabilir.

I.11 Değerlendirenin Yorumları/Önerileri

Bu bölüm değerlendirme sonuçlarına ilişkin olarak ek bilgi vermek için kullanılır. Bu yorumlar/öneriler BT ürününe ilişkin olarak değerlendirme sırasında keşfedilen eksiklikler biçiminde olabileceği gibi bilhassa yararlı olan özelliklerin bahsi şeklinde de olabilir.

I.12 Ekler

Ekler raporun hitap ettiği kitle için yararlı olabilecek herhangi bir ek bilgiyi ortaya koymak için kullanılırken raporun öngörülen başlıklarına mantıklı bir biçimde uymaz (örn. Güvenlik ilkesinin eksiksiz tanımı).

I.13 Güvenlik Hedefi

Güvenlik Hedefi Belgelendirme/Onaylama Raporuna dahil edilmelidir. Ancak patentli teknik bilgiler ayıklanarak veya başka biçimde ifade edilerek temiz bir hale getirilmelidir.

I.14 Sözlük

Sözlük, anlamları o anda açık olmayan kısaltmaların veya terimlerin tanımlarını sağlayarak raporun okunabilirliği arttırmakta kullanılır.

I.15 Kaynakça

Kaynakça bölümü raporun derlenmesinde kaynak malzeme olarak kullanılan tüm atıfta bulunulmuş belgeleri sıralar. Bu bilgiler bunlarla sınırlı olmamak kaydıyla aşağıdakileri içerebilir:

- a) kriterler, metodoloji, program taslağına ait belgeler;
- b) teknik referans belgeleri, ve
- c) değerlendirme çalışmasında kullanılan

geliştirici belgeleri.

Çoğaltılabilirlik açısından tüm geliştirici belgelerinin özgün bir biçimde ve doğru yayın tarihi ve doğru sürüm numarası ile birlikte belirlenmesi önemlidir.

Ortak Kriter Belgeleri

Aşağıdaki bilgiler bu Tanıma Düzenlemesinin Katılımcıları adına düzenlenen tüm Ortak Kriter belgelerinde yer almak üzere sağlanmıştır.

J.1 BT Ürünlerinin Değerlendirilmesi ile İlgili Ortak Kriter Belgeleri

Bir BT ürününün değerlendirilmesinin belgelendirilmesi/onaylanması sonucunda bir Katılımcı tarafından verilen bir Ortak Kriterler belgesi aşağıdaki bilgileri içermelidir:

- a) Ürünün İmalatçısı;
- b) Ürün Adı;
- c) Ürün Türü;
- d) Sürüm ve Yayın Numaraları;
- e) Koruma Profili Uygunluğu (uygulanabilir olması durumunda);
- f) Değerlendirme Platformu (isteğe bağlı);
- g) BT Güvenlik Değerlendirme Tesisinin Adı (isteğe bağlı);
- h) Belgelendirme/Onaylama Kuruluşunun Adı;
- i) Belgelendirme/Onaylama Rapor Tanıtıcısı;⁴
- j) Düzenleme Tarihi; ve
- k) Güvence Paketi.⁵

Belge ayrıca aşağıdaki ifadeleri içermelidir:

Bu belgede tanımlanan BT ürünü, [akredite ve lisanslı/onaylanmış değerlendirme tesisi veya [Katılımcının ülkesinin adını girin] yasaları, ikincil mevzuatı veya diğer resmi idari prosedürleri kapsamında kurulmuş olan bir değerlendirme tesisinde] BT Güvenliği Değerlendirmesi için Ortak Kriterlere [sürüm numarasını girin] uygunluğun belirlenmesi için BT Güvenliği Değerlendirmesi için Ortak Metodoloji kullanılarak değerlendirilmiştir. Bu belge yalnızca ürünün değerlendirilmiş olan konfigürasyonu kapsamındaki özel sürüme ve yayına ve Belgelendirme/Onaylama raporunun tamamıyla bağlantılı olarak uygulanır. Değerlendirme [programın resmi adını girin] hükümlerine uygun olarak yapılmıştır ve değerlendirme tesisinin değerlendirme teknik raporunda yer alan sonuçları ileri sürülen kanıtlarla uyumludur. Bu belge BT ürününün [Katılımcının adını girin] tarafından veya bu belgeyi tanıyan ya da yürürlüğe koyan herhangi bir başka kuruluş tarafından onaylandığı ve

⁴ Belgelendirme/Onaylama raporu tanıtıcısı belgeyi özgün bir biçimde tanıtmalıdır. Rapor en azından

Belgelendirme/Onaylama Kuruluşunun adını, kullanılan değerlendirme kriterlerini, rapor numarasını ve düzenleme yılını içerecektir..

⁵ Teyit edilen güvence paketi, Ortak Kriterler Değerlendirme Güvence Seviyesi 3'e uygun ile Ortak Kriterler Değerlendirme Güvence Seviyesi 3 yükseltilmiş arasında ayırım yapacaktır. Yükseltme bir artı ile belirtilmelidir, (örn., EAL 3+).

BT ürününün *[Katılımcının adını girin]* veya bu belgeyi tanıyan veya yürürlüğe koyan herhangi bir başka kuruluş tarafından açık veya zımni olarak garanti edildiği anlamına gelmez.

Sıralanan bilgilere ek olarak, Ek A'da atıfta bulunulan işaret, Katılımcılar tarafından verilen her bir BT ürünü ile ilgili Ortak Kriterler belgesine konulacaktır.

J.2 Koruma Profili Değerlendirmeleri ile Bağlantılı Ortak Kriter Belgeleri

Bir koruma profilinin değerlendirilmesinin belgelendirilmesi/onaylanması sonucunda bir Katılımcı tarafından verilen bir Ortak Kriterler belgesi aşağıdaki bilgileri içermelidir:

- a) Koruma Profili Geliştiricisi;
- b) Koruma Profili Adı/Tanıtıcısı;
- c) Sürüm Numarası;
- d) BT Güvenlik Değerlendirmesi Tesisinin Adı (isteğe bağlı);
- e) Belgelendirme/Onaylama Kuruluşunun Adı;
- f) Belgelendirme/Onaylama Raporunun Numarası;
- g) Düzenleme Tarihi; ve
- h) Güvence Paketi.⁶

Belge ayrıca aşağıdaki ifadeleri içermelidir:

Bu belgede tanımlanan koruma profili, *[akredite ve lisanslı/onaylanmış değerlendirme tesisi veya [Katılımcının ülkesinin adını girin] yasaları, ikincil mevzuatı veya diğer resmi idari prosedürleri kapsamında kurulmuş olan bir değerlendirme tesisinde]* BT Güvenliği Değerlendirmesi için Ortak Kriterlere *[sürüm numarasını girin]* uygunluğun belirlenmesi için BT Güvenliği Değerlendirmesi için Ortak Metodoloji kullanılarak değerlendirilmiştir. Bu belge yalnızca bu belge içinde listelenen koruma profilinin özel sürümüne ve Belgelendirme/Onaylama raporunun tamamıyla bağlantılı olarak uygulanır. Değerlendirme *[programın resmi adını girin]* hükümlerine uygun olarak yapılmıştır ve değerlendirme tesisinin değerlendirme teknik raporunda yer alan sonuçları ileri sürülen kanıtlarla uyumludur. Bu belge, koruma profilinin *[Katılımcının adını girin]* tarafından veya bu belgeyi tanıyan ya da yürürlüğe koyan herhangi bir başka kuruluş tarafından onaylandığı ve koruma profilinin *[Katılımcının adını girin]* veya bu belgeyi tanıyan veya yürürlüğe koyan herhangi bir başka kuruluş tarafından açık veya zımni olarak garanti edildiği anlamına gelmez

Sıralanan bilgilere ek olarak, Ek E'de atıfta bulunulan işaret, Katılımcılar tarafından verilen her bir koruma profili ile ilgili Ortak Kriterler belgesine konulacaktır.

⁶ Teyit edilen güvence paketi, Ortak Kriterler Değerlendirme Güvence Seviyesi 3'e uygun ile Ortak Kriterler Değerlendirme Güvence Seviyesi 3 yükseltilmiş arasında ayırım yapacaktır.

Ek K

Uyumlu CBler

Avustralya ve Yeni Zelanda

Savunma Sinyalleri Mdrlg ve Devlet İletiřim Gvenliđi Brosu
sponsorluđunda
Avustralasya Bilgi Gvenliđi Deđerlendirme Programı

Kanada

İletiřim Gvenliđi Kurumu
sponsorluđunda
Ortak Kriterler Deđerlendirme ve Belgelendirme

Fransa

Service Central de la Scurit des Systmes d'Information,
sponsorluđunda
Schema d'Evaluation et Certification Francais

Almanya

sponsorluđunda
Bundesamt fr Sicherheit in der Informationstechnik
(Zertifizierungsstelle)

Birleřik Krallık

İletiřim-Elektronik Gvenlik Grubu ve Ticaret ve Sanayi Bakanlıđı
Sponsorluđunda
BK BT Gvenlik Deđerlendirme ve Belgelendirme Programı

Amerika Birleřik Devletleri

Ulusal Standartlar ve Teknoloji Enstits ve Ulusal Gvenlik Teřkilatı
sponsorluđunda
Ulusal Bilgi Gvencesi Ortaklıđı Ortak Kriterleri