BİLGİ SİSTEMLERİ GÜVENLİĞİ KAPSAMINDA

TS ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ DANIŞMANLIK,

TEKNİK AÇIKLIK TESTLERİ

VE

BİLGİ İLETİŞİM GÜVENLİĞİ REHBER UYUMLULUĞU DANIŞMANLIK ALIMI

TEKNİK ŞARTNAMESİ

İÇİNDEKİLER

1. GİRİŞ 3
2. AMAÇ 3
3. BGYS DANIŞMANLIĞI 4
    3. 1. Bilgi Güvenliği Fark Analizi 4
    3.2. BGYS Kurulumu 5
    3.3. BGYS Sertifikası Alımı 8
    3.4. BGYS Eğitimleri 8
4. TEKNİK AÇIKLIK TESTLERİ 9
5. BİLGİ İLETİŞİM GÜVENLİĞİ REHBERİ DANIŞMANLIĞI 18
6. YÖNTEM 18
7. DANIŞMAN PERSONEL NİTELİKLERİ 19
8. GENEL HUSUSLAR 19

1. GİRİŞ

1.2. İşin Tanımı

İstanbul Ticaret Üniversitesi bünyesinde kurulu bulunan bilgi işlem altyapısı kapsamında, TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Danışmanlığı, Teknik Açıklık testlerinin yapılması ve Bilgi ve İletişim Güvenliği Rehberi'ne uyum danışmanlığı hizmeti.

1.2. Tanımlar ve Kısaltmalar

İDARE	İstanbul Ticaret Üniversitesi
BİDB	İstanbul Ticaret Üniversitesi Bilgi Teknolojileri Daire Başkanlığı
YÜKLENİCİ	İdare ile sözleşme imzalayan firma
BTHYS	Bilgi Teknolojileri Hizmet Yönetim Sistemi
BT	Bilgi Teknolojileri
TÜRKAK	Türk Akreditasyon Kurumu
TSE	Türk Standartları Enstitüsü
CISSP	Certified Information Systems Security Professional
PMP	Project Management Professional
CEH	Certified Ethical Hacker
CCEE	Common Criteria Expert Evaluator
ISECOM	The Institute for Security and Open Methodologies
OSSTMM	The Open Source Security Testing Methodology Manual
OPST	OSSTMM Professional Security Tester Accredited Certification
DOS	Denial of Service
ISO	International Organization for Standardization
BGYS	Bilgi Güvenliği Yönetim Sistemi
SOME	Siber Olaylara Müdahale Ekibi

2. AMAÇ

Bu teknik şartname kapsamında alınacak hizmet ile, Bilgi Teknolojileri Dairesi'nin bilişim altyapısında bulunan bileşenlerinin uluslararası standartlara göre fark analizinin yapılması, tespit edilen kavramsal ve teknik açıklıkların giderilmesi sonucunda TS ISO/IEC 27001 BGYS belgesinin Yüklenici tarafından İstanbul Ticaret Üniversitesi Bilgi Teknolojileri Daire Başkanlığı adına alınması ve bu yönetim sisteminin sürdürülebilmesi için yol haritasının çizilmesi ile Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayınlanan Bilgi ve İletişim Güvenliği Rehberi'ne uyumunun sağlanması ve denetime hazırlanması için yapılacak çalışmalara danışmanlık desteği hizmetlerinin verilmesidir.

3. BGYS DANIŞMANLIĞI

BİDB bilişim altyapısı hem tüzel ve gerçek kişilere sunulan hizmetler hem de bünyesinde bulundurduğu bilgiler açısından önem arz etmektedir. Bu altyapının güvenliğinin sağlanması için uluslararası düzeyde kabul görmüş olan TS ISO/IEC 27001:2022'ye uygun BGYS' nin kurulması, barındırılan bilgilerin güvenliğinin sağlanması ve sistematik bir sürecin izlenmesi açısından İdareye katkı sağlayacaktır. Bu kapsamda, tedarik edilecek BGYS Danışmanlığı Hizmeti, Yüklenici tarafından görevlendirilecek Proje Koordinatörünün liderliğinde aşağıdaki ana başlıklar doğrultusunda yürütülecektir:

- Bilgi Güvenliği Fark Analizi
- BGYS Kurulumu
- BGYS Sertifikası Alımı
- BGYS Eğitimleri

Her ana başlık kapsamında gerçekleştirilecek iş ve işlemler aşağıda tanımlanmıştır.

3.1. Bilgi Güvenliği Fark Analizi

Bilgi Güvenliği fark analizi için Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayınlanan Bilgi ve İletişim Güvenliği Rehberi uyum dokümanları ve Bilgi ve İletişim Güvenliği Denetim Sonuçları kullanılacaktır.

3.2. BGYS Kurulumu

Bilgi güvenliği fark analizi başlığı altında tespit edilen uyumsuzluklar ile ilgili çalışmalar yapılarak, TS ISO/IEC 27001:2022 BGYS Standardına uygun bir BGYS'nin kurulması sağlanacaktır. Bu kapsamda Yüklenicinin yapması gereken işler aşağıda belirtilmiştir.

3.2.1. Bilgi Güvenliği Yönetim Sistemi'nin kapsamı tespit edilecektir. Bu kapsama, Uygulanabilirlik Bildirgesi'nde hariç bırakılacak maddelerin tespiti dahildir. Kapsam metni; Bilgi İşlem departmanı özelinde olmakla birlikte İnsan Kaynakları ve Satın alma faaliyetlerini de içerecek şekilde oluşturulacaktır.

3.2.2. Fark analizi sonuçlarını, proje planını, organizasyon yapısını ve üst yönetici bilgi güvenliği farkındalık konularını içeren üst yönetim sunumu yapılacaktır.

3.2.3. BGYS çalışmalarının başlaması için belirlenmiş kapsam dahilinde gerekli olan, temel dokümanlar hazırlanacaktır.

3.2.4. Oluşturulan temel dokümanlar İdarenin onayına sunulacaktır.

3.2.5. Yapılacak birebir görüşmeler ile "Bilgi Varlık Envanteri" tespiti yapılacaktır. Envanter, Bilgi ve İletişim Güvenliği Rehberi şartlarına uygun olacaktır.

3.2.6. Oluşturulan varlık envanterine göre kavramsal ve teknik risk analizi yapılacaktır.

3.2.7. Teknik risk analizi ile ilgili detaylar Teknik Açıklık Testleri başlığı altında detaylandırılacaktır. Kavramsal risk analizi yapılırken en az aşağıdaki hususlar dikkate alınacaktır.

3.2.7.1. Kavramsal risk analizi İdare ile birebir görüşülerek yapılacaktır.

3.2.7.2. Fark analizi sonuçları dikkate alınacaktır.

3.2.7.3. Varlığın/sürecin gizliliğini, bütünlüğünü veya erişilebilirliğini tehdit eden unsurlar ve bu tehdide neden olacak zafiyetler tespit edilecektir ve buna göre kavramsal risk analizi yapılacaktır.

3.2.7.4. Kavramsal risk analizi en az aşağıdaki tehdit ve zafiyet alanlarını içerecek şekilde yapılacaktır.

- Dış kurum, kişiler ve paydaşlardan gelecek tehditler
- Bilişim sistem operasyonları ve işletmesinden kaynaklanacak tehditler
- Bilişim eleman ve kullanıcılarından gelecek tehditler
- Organizasyon ve iş sorumluluklarından gelecek tehditler
- Yazılım geliştirme ortamlarından gelebilecek tehditler
- Bilişim ağ ve sunucu sistem yönetim işlevlerinden gelebilecek tehditler
- Fiziksel ve mantıksal erişim tehditleri
- Doğal koşul ve felaketlerden gelecek tehditler

3.2.8. Riskin varlık veya süreç üzerindeki etkisi ve oluşma olasılığına göre risk puanı hesaplanacaktır.

3.2.9. Risk puanına göre alınması gereken risk işleme kararı belirlenecektir.

3.2.10. Tespit edilen riskler ve risk işleme kararları İdare proje ekibi ile değerlendirilecektir.

3.2.11. Risk analizi sonucunda tehdit ve zafiyetleri içeren bir risk listesi oluşturulacaktır. Oluşturulacak liste ISO 27005 ve ISO 31000 ile uyumlu olacaktır.

3.2.12. Risk işleme planından sonra Uygulanabilirlik Bildirgesi hazırlanacaktır. Bildirgede en az "TS ISO/IEC 27001 Kontrol konusu", "TS ISO/IEC 27001 Kontrol maddesi", "Kontrol maddesinin uygulanıp uygulanmadığı" ve "Referans dokümanı" bilgileri yer alacaktır.

3.2.13. Uygulanabilirlik bildirgesinde belirtilen referans dokümanları İdarenin iş hedeflerine ve mevzuata uyumlu, hedef kullanıcı ve sorumluları tarafından anlaşılır nitelikte olacak şekilde yüklenici tarafından oluşturulacaktır.

3.2.14. İdare tarafından onaylanan Doküman Yönetimi Prosedürüne uygun şekilde kapsama uygun ve ihtiyaç duyulan dokümanlar oluşturulacaktır. Yönetim sistemlerinin uyumu ve entegrasyonunu sağlamak amacıyla mevcut Yönetim Sistemleri'nin ortak dokümanları kullanılacaktır.

3.2.15. Oluşturulacak dokümanlar İdare tarafından kontrol edilecek ve değişiklik talepleri Yükleniciye bildirilecektir. Yüklenici her bir doküman için bildirim tarihinden sonra en geç 3 (üç) iş günü içerisinde revize dokümanı İdare ile paylaşacaktır.

3.2.16. Dokümanların son hali İdare tarafından onaylanacaktır.

3.2.17. Dokümanların ilgili kullanıcılara duyurulması ve yaygınlaştırılması İdarenin sorumluluğundadır.

3.2.18. Risk işleme faaliyetleri tanımlandıktan sonra İdare personeli tarafından danışmanların desteğiyle iç tetkik gerçekleştirilecektir. İç tetkikler aşağıdaki hususlar göz önüne alınarak yapılacaktır.

3.2.18.1. İç tetkik planı prosedürde belirtildiği şekilde oluşturulacak ve İdare ile paylaşılacaktır.

3.2.18.2. İç tetkik TS ISO/IEC 27001 Baş Denetçi sertifikasına sahip bir denetçi tarafından gerçekleştirilecektir.

3.2.18.3. İç tetkik raporu tetkikin tamamlanmasından en geç 5 (beş) iş günü içerisinde danışmanca kontrol edildikten sonra İdareye teslim edilecektir.

3.2.18.4. İç tetkikte tespit edilen bulguların giderilmesi için İdareye yol göstericilik yapılacaktır.

3.3. BGYS Sertifikası Alımı

3.3.1. Proje kapsamında kurulan BGYS, Türk Akreditasyon Kurumu tarafından TS EN ISO/IEC 27001 standardı kapsamında akredite edilen belgelendirme kuruluşları tarafından denetlenecektir.

3.3.2. Yüklenici, yer tesliminden sonra en geç 240 (ikiyüzkırk) gün içerisinde sözleşme kapsamında yer alan iş ve işlemleri tamamlamak ve İDARE 'nin de onayladığı bağımsız bir denetçi kuruluş tarafından TS ISO/IEC 27001 standardına uygunluk belgesini alınmasını sağlamakla yükümlüdür.

3.3.3. Sertifikasyona ait tüm maliyetler Yüklenici tarafından karşılanacaktır.

3.3.4. Yüklenici, denetimler esnasında tespit edilecek bulguların giderilmesi konusunda İdareye danışmanlık vermeye devam edecektir.

3.3.5. Danışmanlık hizmeti, kurulacak Bilgi Güvenliği Yönetim Sisteminin Türk Akreditasyon Kurumu tarafından TS EN ISO/IEC 27001 standardı kapsamında Akredite edilen belgelendirme kuruluşu tarafından, TS ISO/IEC 27001 standardına uygunluk belgesinin alınması ile tamamlanacaktır.

3.4. BGYS Eğitimleri ve Kvkk Yazılımı

3.4.1. Eğitimler ile ilgili genel hususlar aşağıda belirtilmiştir.

3.4.1.1. Eğitimlerin dili Türkçe olacaktır.

3.4.1.2. Eğitimler ile ilgili notlar İdare ile eğitimlerden önce paylaşılacaktır.

3.4.1.3. BGYS eğitimlerini verecek kişi TS ISO/IEC 27001 Baş Denetçi sertifikasına sahip olacaktır.

3.4.1.4. Eğitimler İdarenin kendi lokasyonunda gerçekleştirilecektir.

3.4.2. TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Temel Eğitimi ve TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Risk Değerlendirme ve Analizi Eğitimi sonrası katılımcılara birer katılım belgesi veya sertifika verilecektir.

3.4.3. Eğitimlerin adları ve süreleri aşağıdaki tabloda belirtilmiştir:

Eğitim Adı	**Süresi**
Bilgi Güvenliği Farkındalık Eğitimi	4 saat
TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Temel Eğitimi	1 gün

TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi İç Tetkikçi Eğitimi	2 gün
KVKK Farkındalık Eğitimi	2 gün

3.4.4. Eğitimlerin içerikleri aşağıda açıklanmıştır.

3.4.4.1. TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Temel Eğitimi

- Bilgi ve Bilgi Güvenliği Kavramları, Terimler
- Risk Analizi
- TS ISO/IEC 27001 Standardı Maddelerinin Yorumlanması
- Güvenlik Kontrolleri ve Önlemler
- Kritik Başarı Faktörleri
- Belgelendirme Süreci
- Pratik ve Örnek Çalışmalar

3.4.4.2. TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi İç Tetkikçi Eğitimi

- Denetim Türleri
- Denetim Süreci
- Denetim Planlama
- Denetim Uygulamaları
- ISO 27001 BGYS Standart ve Ek.A Maddelerinin Yorumlanması

3.4.4.3. KVKK Farkındalık Eğitimi

KVKK Farkındalık Eğitimi Bilgi ve İletişim Güvenliği Rehberi'nin ilgili maddesine uygun içerikte olacaktır.

4. TEKNİK AÇIKLIK TESTLERİ

4.1. Yüklenici Sızma testi ve güvenlik denetimi süresince, kurumun domain ve subdomain'lerinde ve internet üzerinden erişilebilirliği olan IP adres aralığında çalışan sunucularındaki güvenlik açıklarını tarayacak, güvenlik açıkları ve riskleri tespit edecektir.

4.2. Güvenlik denetimi sırasında İdare hakkında edinilebilecek bilgiler nedeniyle söz konusu denetimi gerçekleştirecek yüklenicinin, bu işlevi T.C. vatandaşı olan bir ekip ile Türkiye sınırları dâhilinden gerçekleştirmesi zorunludur. Yurtdışından gerçekleştirilecek güvenlik denetimi işlemleri kabul edilmeyecektir.

4.3. Yüklenici, denetimi gerçekleştirecek uzman/uzmanların açık özgeçmişleri ve projede alacakları görevleriyle birlikte tanıtacaktır.

4.4. Denetimi gerçekleştirecek uzmanda/uzmanlarda ile aşağıda belirtilen özellikler aranacaktır:

- Başarılı olarak sonuçlandırılmış en az 1 (bir) adet Üniversite Teknik Açıklık Testi Projesi gerçekleştirmiş olmak

4.5. Yüklenici, işe başlamadan önce , söz konusu güvenlik denetimini nasıl bir metodoloji kullanarak gerçekleştireceğini, adımları ile detaylı olarak açıklamalıdır. Bu metodoloji adımlarının gerçekleştirilmesinde kullanılan metot ve araçlar açıkça tarif edilmelidir. Sunulacak metodoloji asgari olarak bu şartnamenin "Test Metodolojisi" başlığı altında yer alan yöntemleri içerecektir. Sadece otomatik güvenlik tarama araçlarıyla gerçekleştirilen güvenlik tarama işlemleri kabul edilmeyecektir.

4.6. Güvenlik Denetimi çalışmasının tamamlanmasını izleyen 15 (onbeş) iş günü içerisinde yüklenici, denetim raporunu İdareye iletecek ve takip eden 10 (on) iş günü içerisinde İdare tarafından uygun görülecek zamanda sunumunu gerçekleştirecektir.

4.7. Denetim çalışması kapsamında mesai saatleri içinde hizmet kesintisi (Denial of Service vb.) saldırıları gerçekleştirilmeyecektir. YÜKLENİCİ, istenmeden neden olunabilecek hizmet kesintileri durumunda İdareyi en kısa sürede bilgilendirecektir.

4.8. Denetim çalışması kapsamında gerçekleştirilecek saldırı simülasyonları, yalnızca saldırıların gerçekleştirilebilirliğinin gösterilmesi amacıyla düzenlenecektir. Yüklenicinin sızmayı, diğer bir deyişle uzaktan kumanda etmeyi başardığı durumda, İdarenin sistemleri üzerinde yer alan hiçbir veriyi (dosya, veri tabanı vb.) okumaması, kopyalamaması ve değiştirmemesi gerekmektedir. Aykırı durumların tespiti, İdare tarafından sözleşmenin ihlali olarak değerlendirilecektir ve gerekli yasal işlem başlatılacaktır.

4.9. Test aşağıda belirtilen kapsamda gerçekleştirilecektir.

- İletişim Altyapısı Ve Aktif Cihazlar
- DNS Servisleri
- Etki Alanı ve Kullanıcı Bilgisayarları
- E-Posta Servisleri
- Veri tabanı Sistemleri
- Web Uygulamaları
- Kablosuz Ağ Sistemleri
- Dağıtık Servis Dışı Bırakma Testleri
- Sosyal Mühendislik Testleri
- Sanallaştırma Sistemleri

4.10. Testler, ihtiyaç halinde testin türüne göre aşağıdaki kullanıcı tipleri ile yapılacaktır.

- <u>İnternet Kullanıcısı Profili:</u> İnternet üzerinde İdarenin İnternet servislerine erişebilen ve İnternet uygulamasına giriş yetkilerine sahip olmayan kullanıcıyı temsil eder. İdareye ait İnternet uygulamasına giriş yetkilerine sahip olmayan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılacaktır.
- <u>Misafir Profili:</u> İdare personeli dışında, İdarenin kablolu ve kablosuz ağını kullanarak kurumun bilişim hizmetlerinden yararlanacak kullanıcı profili üzerinden test edilecektir.
- <u>Uygulama Kullanıcısı Profili:</u> internet üzerinde İdarenin İnternet servislerine erişebilen ve internet uygulamasına giriş yetkilerine sahip olan kullanıcıyı temsil eder. İdareye ait internet uygulamasına giriş yetkilerine

sahip olan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılacaktır.

- E-posta Kullanıcısı Profili: Gerek internet gerekse iç ağdan e-posta servislerini kullanabilen kullanıcıları temsil eder. Bu yetkiye sahip kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılacaktır.
- İdare Personeli Profili: Personelin çalışma ortamını kullanarak sahip olduğu yetkiler ile sistemde oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılacaktır. Bu profil ile gerçekleştirilecek testlerde, kurum çapında en yaygın olarak kullanılan çalışan profilinin seçilmesinin yanında, yerel yönetici (local admin) yetkisine sahip çalışan profilleri ile de sızma testleri gerçekleştirilecektir. Testi yapan kişi/kuruluşa idare tarafından tanımlanan erişim yetkileri ve verilen izinler raporda açıkça ifade edilecektir.
- Diğer kullanıcı profilleri: Sızma testlerinin, yukarıda tanımlanan diğer kullanıcı profiline uymayan bir kullanıcı profili ile gerçekleştirilmesi durumunda, kullanılan her bir profil için tanımlanan hak ve yetkiler bu başlık altında açıkça ifade edilir.

4.11. Testler, aşağıdaki erişim noktaları üzerinden gerçekleştirilecektir.

- Kurum Dışı Ağı: Kurumun internet üzerinden erişilebilen tüm sunucu ve servislerine internet üzerinden erişilerek sızma testleri gerçekleştirilir.
- Kurum İç Ağı: Kurumun iç ağında yer alan ve test kapsamında ele alınan sunuculara Kurum iç ağı üzerinden erişilerek sızına testleri gerçekleştirilir. Ağ ve ağ trafiği üzerinde gerçekleştirilecek testler için de bu ağ kullanılır ve testi gerçekleştirecek şahıslara kullanımı en yaygın olan çalışan bilgisayarı profilinde bilgisayarlar sağlanır.
- Sunucu Konsolu: Bazı testler için sunucu konsolundan erişim ihtiyacı oluşması durumunda, sistem yöneticilerinin kontrolünde ve gözetiminde erişim sağlanarak testler gerçekleştirilecektir.

4.12. Test Metodolojisi aşağıda tanımlandığı şekilde uygulanacaktır.

- Sızma testleri, yukarıda detaylandırılan kullanıcı profilleri ile tanımlanan erişim noktalarından gerçekleştirilecek temel sızma testleri ve detaylı sızma testlerinden oluşacaktır.
- Temel sızma testleri sistem tespiti, servis tespiti ve açıklık taraması/araştırması adımları ile başlayacak ve her bir erişim noktası kapsamında uygulanacak adımlar ile devam edecektir.
- Temel sızına testleri sonrası saptanan açıklık ve bulgular, detaylı sızma testlerinin gerçekleştirilmesi suretiyle ayrıntılı olarak incelenerek raporlanacaktır.
- Temel sızına testi, bilgi toplama, zafiyet taraması, ağ haritası tespiti, envanter tespiti vb. adımlardan oluşmaktadır.

- Detaylı sızma testi, temel sızına testinde elde edilen bilgiler ışığında otomatik ve manuel araçlar kullanılarak sistemlere sızma çalışmalarının gerçekleştirilmesidir.
- Sızma testleri gerçekleştirilirken her bir test başlığı kapsamında saptanan açıklık ve bulgular, ayrı ayrı değerlendirilmenin yanında, bir araya geldiklerinde oluşturabilecekleri riskler ve açıklıklar açısından da değerlendirilecek ve bu birlikte değerlendirme sonucu ortaya çıkan yeni açıklık ve bulgular da raporlanacaktır.
- Sızma testleri gerçekleştirilirken, İdare faaliyetlerinin aksamamasına ve hizmet kesintisine yol açmayacak yöntemler kullanılmasına dikkat edilecektir. Hizmet kesintisine yol açabilecek tüm testler Kurum ile koordineli bir şekilde planlanarak gerçekleştirilecektir.

4.13. Teknik açıklık testleri kapsamında en az aşağıdaki alanlarda testler gerçekleştirilecektir.

4.13.1. İdarenin ağ altyapısı ve aktif ağ cihazlarına yönelik asgari olarak aşağıdaki testler gerçekleştirilecektir.

- İdarede kullanılan ağ cihazlarının genel mimari içindeki yeri incelenecektir.
- Tüm ağ cihazları açıklık bulma araçları ile taranacaktır.
- Tespit edilen açıkların uygulanabilirlikleri sınanacaktır.
- Ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenecektir.
- Aktif cihaz üzerindeki port güvenliği, VLAN ve trunk yapısı incelenecektir. * Ağ topolojisi ve alt bölümleri incelenerek kullanıcı-sunucu ağları arasında erişim kontrolünün olup olmadığı kontrol edilecektir.
- Paket dinlemesi yoluyla ağ üzerinden geçebilecek VolP paketleri yakalanmaya ve konuşmalar dinlenmeye çalışılacaktır.
- Aktif cihaz üzerinde çalışan servisler incelenecektir.
- Kullanılan servislerin servis dışı bırakılmayla sonuçlanabilecek saldırılara karşı (ARP zehirlemesi, CDP DOS, DHCP DOS, SNMP Dos vb.) durumu incelenecektir. * Cihazlar üzerinde açık olan Telnet, HTTP, FTP, SNMP, TFTP, SSH vb. servislerine sözlük saldırısı veya kaba güç kullanılarak erişim sağlanmaya çalışılacaktır. * Erişim sağlanan cihazlar üzerinden alınan bilgilerle diğer cihazlara erişilmeye çalışılacaktır.
- Aktif cihazlar için uzak/yerel erişim kontrolü, yönetim, kayıt ve kimlik doğrulama mekanizmaları incelenecektir.
- Cihazların merkezi şekilde yönetilmesini ve gözetlenmesini sağlayan yönetim sistemlerinin varlığı araştırılacak, bu sistemlere sızma girişimlerinde bulunulacaktır. * Cihazlarda ortak parolanın kullanılıp kullanılmadığı test edilecektir.
- İdare çalışanları için kullanılan içerik filtreleme sistemleri atlatılmaya çalışılacaktır.

- Kurum içinden dışarı tünel kurulmasıyla, kurum dışından kurum içine yetkisiz bağlantı gerçekleştirilmeye çalışılacaktır.
- Kurum dışına açık yönetim ara yüzlerinin varlığı kontrol edilecektir.

4.13.2. Kurumun DNS servislerine yönelik asgari olarak aşağıdaki testler gerçekleştirilecektir.

- DNS sunucuların topolojik konumu incelenecektir.
- DNS Sunucusunun alan yapılandırmasında yer alan kayıtlar ortaya çıkarılmaya çalışılacaktır.
- Sunucu üzerinden alan transferi (zone transfer) yapılmaya çalışılacaktır.
- NXT ve NSEC kaynak kayıtları üzerinden bilgi elde edilmeye çalışılacaktır. * Netcraft, Google, Whois sorguları yapılarak Kurum alanında yer alan sunucular tespit edilmeye çalışılacaktır.
- DNS sunucular için ön bellek zehirlemesi gerçekleştirilmeye çalışılacaktır.
- DNS sunucular üzerindeki kaynak kayıt girdileri incelenecektir.
- DNS sunucular üzerindeki ters kaynak kayıt girdileri incelenecektir.
- DNS sunucuların sürüm bilgisi elde edilmeye çalışılacaktır.
- Kurum dışı alan isimleri sorgulanmaya çalışılacaktır.
- Sunucular üzerinde DNS dışında bir servisin çalışıp çalışmadığı incelenecektir.
- Güvenlik Duvarında DNS sunucular için izin verilen portlar incelenecektir.
- DNS sunucuları güvenlik taramasına tabi tutulacaktır.
- DNS servisini veren yazılımın açıklıkları araştırılacaktır.

4.13.3. Kurum etki alanı (domain) sisteminde ve kullanıcı bilgisayarlarında asgari olarak aşağıdaki testler gerçekleştirilecektir.

- Kullanıcı bilgisayarlarının açılış ayarlarındaki eksiklikler tespit edilip, yerel yönetici hakları elde edilmeye çalışılacaktır.
- Yerel yöneticilerin kullanımındaki zafiyetler ile hak yükseltme saldırıları gerçekleştirilecektir.
- Etki alanındaki şifre politikası ve şifre saklama politikasındaki zafiyetler tespit edilip, kullanıcı hesaplarının şifreleri ele geçirilmeye çalışılacaktır.
- Yama yönetimindeki zafiyetler ve desteği kaldırılmış eski sistemler tespit edilip, uzaktan kod çalıştırma ve hak yükseltme saldırıları gerçekleştirilecektir.
- Yetkisiz erişime imkân tanıyan dosya paylaşımları tespit edilerek, bu paylaşımlar ve paylaşımlardaki hassas veriler yoluyla hak yükseltme saldırıları gerçekleştirilecektir.
- Hak yükseltme saldırıları ile etki alanı kullanıcılarının hesapları ele geçirilmeye çalışılacaktır.
- Etki alanında yönetici haklarına sahip kullanıcı hesapları ve kullanıcı hesabı gruplarının kullanımındaki zafiyetler kullanılarak hak yükseltme saldırıları gerçekleştirilecektir.

- Elde edilen şifre ve haklar ile hassas bilgilerin bulunduğu sunucu ve kullanıcı bilgisayarlarına erişim sağlanmasına çalışılacaktır.

4.13.4. Kurumun e-posta servislerinde asgari olarak aşağıdaki testler gerçekleştirilecektir.

- E-posta sunucularının topolojik konumu incelenecektir.
- Virüs tarayıcı ağ geçitlerinin sürüm bilgileri elde edilmeye çalışılarak bu sürümlerin bilinen açıklıkları araştırılacaktır.
- Sunucular üzerindeki yönlendirme (relaying) zafiyetlerini incelemek üzere bir dizi e-posta gönderilecektir.
- Anti-spam ağ geçitlerinin kurum dışı sahte e-postalara karşı davranışı incelenecektir.
- Sunucular üzerinde e-posta dışında bir servisin çalışıp çalışmadığı incelenecektir. * E-posta sunucusu üzerinde kimlik doğrulamanın aktif olup olmadığını incelenecektir.
- E-posta sunucusu üzerinde POP3, IMAP gibi istemci servislerinin erişime açık olup olmadığı kontrol edilecektir.
- E-posta sunucuları güvenlik taramasına tabi tutulacaktır.
- Sistemlerde kullanılan e-posta içerik kontrolcüleri, anti-virüs ağ geçitleri, spam filtrelerinin kullanıldığı kütüphanelerde var olabilecek muhtemel açıklıklar incelenecektir.
- E-posta servisini veren yazılımların bilinen diğer açıklıkları araştırılacaktır.
- E-posta servislerinin gönderilen e-postaların boyutlarını sınırlayıp sınırlamadığını kontrol etmek amacı ile boyutu büyük e-postalar gönderilecektir.
- Kullanılması muhtemel e-posta listesi yazılımlarının açıklıkları tespit edilmeye çalışılacaktır.

4.13.5. Veritabanı sistemlerine yönelik asgari olarak aşağıdaki testler gerçekleştirilecektir.

- Sistemdeki veritabanı uygulamaları ve bu uygulamaları üzerinde barındıran işletim sistemleri tespit edilerek, tespit edilen bu sistemlere erişimin açık olup olmadığı denetlenecek ve erişimin açık olması halinde çeşitli tarama araçlarıyla veritabanı versiyonu, üretici adı vb. bilgiler ele geçirilmeye çalışılacaktır.
- Elde edilen veritabanı sistem bilgileri kullanılarak, bu sistemlere yönelik kullanıcı adı ve parola deneme saldırıları yapılır. Bu saldırılar sırasında, ön tanımlı kullanıcı adı ve parolaların denenmesinin yanında, Kuruma özel olabilecek ve tahmin edilebilir kullanıcı adı ve parolalar da denenecektir.
- Veritabanı kullanıcı adı ve parola saldırılarının başarısız olması durumunda, işletim sistemi seviyesinden erişim denemeleri yapılır. Windows, Linux vb. ortamlar üzerinden sistem kullanıcıları ile veritabanı uygulamasına bağlanılmaya çalışılacaktır.
- Parola deneme saldırılarının başarılı olması durumunda tespit edilen erişim bilgileriyle sistemlere bağlanılır. Bağlanılan sistemlerde hangi hassas verilerin bulunduğu, kullanıcı adı, parola ve parolalara ait

karmaşıklaştırılmış özet verilerinin bulunup bulunmadığı denetlenecektir.

- Görüntülenebilen kullanıcı adı ve parola özet bilgileri çeşitli araçlarla tespit edilmeye çalışılarak zayıf olarak belirlenmiş parolalar tespit edilecektir.
- Erişilebilen sistemlerde yama bilgisi kontrol edilir. Bilinen açıklıkları içeren ve gerekli güncellemeleri yapılmamış sistemlerde hak yükselme vb. saldırılarla erişim sağlanan kullanıcının hakları genişletilmeye çalışılacaktır.
- Erişilebilen sistemlerden diğer erişilemeyen sistemlere tanımlanmış bağlantılar varsa bu bağlantılar kullanılarak diğer veritabanı uygulamalarına geçilmeye çalışılacaktır.
- Hassas verileri ihtiva eden sistemlere erişilebilmesi halinde yetki seviyesi arttırılmaya çalışılır. Erişim bilgisi elde edilecek sistemlerin sayısı arttıkça, her sistem için yukarda bahsi geçen adımlar tekrarlanır ve mevcut tüm veri tabanlarının güvenliği bu şekilde kontrol edilecektir.

4.13.6. Yüklenici, Kurumun bildireceği web uygulamalarına aşağıdaki testleri uygulayacaktır.

- Girdi Denetimi
- Çıktı Denetimi
- Değiştirilen İçeriğin Tespiti
- HTML Etiketlerinin Filtrelenmesi
- SQL Enjeksiyonu
- URL Yönlendirmeler
- XSS Enjeksiyonu (XSS ınjection)
- Oturum Yönetimi
- Giriş Sonrası Oturum Bilgisi Yenileme, Oturum Sabitleme,
- Çerezlerin İçeriği,
- Oturum Sonlandırma,
- Oturum Çalma (Session Riding),
- Yetki Artırımı,
- Yetki Dışı İşlem,
- Şifre Politikaları,
- Bilenen Hesap/Şifre Bileşenlerinin Denenmesi,
- Basit Kimlik Doğrulama Kullanımı,
- Kimlik Doğrulamanın Atlatılması,
- Çıkış (Logout) İşlevi,
- Tersine Yol (Path Traversal),
- Yetki Atlatma (Bypass Authorization),
- Web Servis Testleri,
- Yetki Artırımı (Privilege escalation),
- SSL Kullanımı,
- HTML Yorumları
- Sunucu Bilgisinin Kısıtlanması,
- Hata Sayfalarının Gösterimi,
- Yönetici Arayüzü Erişim Testi,

- Güvenlik Resmi (Captcha) Kullanımı,
- HTTP Yanıt Bölme (HTTP Response Spliüing)
- Siteler Arası İstek Sahteciliği (Cross-Site Request Forgery, CSRF)

4.13.7. Kablosuz ağlara yönelik asgari olarak aşağıdaki testler gerçekleştirilecektir.

- Kurumda kullanılan kablosuz ağ cihazlarının genel mimari içindeki yeri incelenecektir. Kablosuz ağlardan kurum içi ağlara erişim olup olmadığı incelenecek ve kablosuz ağlardan kurum ağına sızılmaya çalışılacaktır.
- İstemcilerin kablosuz ağ yapılandırmaları incelenecektir.
- Kurumda bulunan kablosuz ağlar taranarak özellikleri keşfedilmeye çalışılacaktır. * Kablosuz ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenecektir. * Kablosuz ağlarda kullanılan şifreleme ayarları incelenecektir.
- Kablosuz ağ erişiminde kullanılan şifreleme ve kimlik denetimi yöntemleri incelenerek ağ şifresi ele geçirilmeye çalışılacak ya da kimlik doğrulama yöntemi atlatılmaya çalışılacaktır.
- Sahte kablosuz ağ erişim noktaları oluşturularak kurumda bulunan istemciler ele geçirilmeye çalışılacaktır.
- İstemciler üzerinden kablosuz ağ taraması yapılarak, kurum etrafında bulunan diğer kablosuz ağlar keşfedilmeye çalışılacaktır.
- İstemciler üzerinden kablosuz ağ kullanılarak kurum dışına bağlantı yapılıp yapılamayacağı incelenecektir.

4.13.8. DDOS testleri Kurumun en az servis verdiği saatlerde ve sistem yöneticileri ile koordine olarak gerçekleştirilir. Bu kapsamda asgari olarak aşağıdaki testler gerçekleştirilecektir

- IP seviyesinde DDOS testleri gerçekleştirilecektir.
- DNS sunucularına yönelik dağıtık aşırı paket gönderimi ile trafiğin üzerinden geçtiği güvenlik duvarı gibi aktif cihazlara yönelik yük testi gerçekleştirilecektir. * Web sunucularına yönelik dağıtık aşırı paket gönderimi ile trafiğin üzerinden geçtiği güvenlik duvarı gibi aktif cihazlara yönelik yük testi gerçekleştirilecektir.
- Herkese hizmet veren servisler tespit edilerek, bu servislere yönelik dağıtık aşırı paket gönderimi ile trafiğin üzerinden geçtiği güvenlik duvarı gibi aktif cihazlara yönelik yük testi gerçekleştirilecektir.
- Uygulama seviyesinde DDOS testleri gerçekleştirilecektir.
- DNS sunucularına yönelik rastgele istek gönderimi ile DNS sunucu yük testi gerçekleştirilecektir.
- Web sunucularına yönelik aşırı paket gönderimi ile web sunucu testi gerçekleştirilecektir.

4.13.9. İdare çalışanlarının bilgi güvenliği farkındalıklarının sınanması amacıyla asgari olarak aşağıdaki sosyal mühendislik testleri gerçekleştirilecektir.

- Sosyal ağlar, arama motorları ve İdare web siteleri kullanılarak İdare ve çalışanları hakkında bilgi elde edilmeye çalışılacaktır. Elde edilecek bu bilgilerle alttaki adımlarda detayları verilen; telefon

görüşmesi, e-posta gönderimi ve kurum dışından yapılabilecek benzeri saldırı teknikleriyle hassas verilere ulaşılmaya çalışılacaktır.

- Kurum içinden veya dışından yapılacak telefon görüşmeleri ile hassas bilgilere ulaşılmaya çalışılacaktır.
- Rastgele seçilen Kurum çalışanlarından çeşitli bilgiler elde edilmeye çalışılarak, çalışanların farkındalıkları ölçülecektir.
- Kurum çalışanlarının ilgisini çekebilecek ve kurum içine sızmaya imkân tanıyacak nitelikte özenle hazırlanmış, İdare içinden veya dışından gönderilecek epostalar ile kullanıcı bilgisayarlarına sızma denemesi gerçekleştirilecektir.
- Kurum sistemine sızabilmek için hazırlanan özel materyallerin kullanıcılar tarafından çalıştırılmasına yönelik ortam hazırlanacak, bu ortam sadece test gerçekleştirilirken kullanılacak ve test sonrası internet erişimine kapatılarak elde edilen hassas verilerin yetkisiz kişilerin eline geçmesini önleyecek gerekli güvenlik tedbirleri alınacaktır.

4.13.10. Sanallaştırma Sistemleri ve sistemler üzerindeki sanal sunucular ve sunucular üzerinde çalışan servislerle ile ilgili bilgiler toplanacaktır. Sistemler açıklık bulma araçları ile taranacak ve tespit edilen açıkların uygulanabilirlikleri sınanacaktır.

4.14. Gerçekleştirilen testler sonucunda aşağıdaki gereklilikleri karşılayacak şekilde raporlama yapılacaktır.

4.14.1. Yüklenici, test ve değerlendirme çalışması sonucunda Detaylı Teknik Test Sonuç Raporu ile Yönetici Test Sonuç Raporu'nu hazırlayarak İdareye sunacaktır. Teknik rapor yeterince açık ve sözlü açıklamaya gerek bırakmayacak biçimde net olacaktır.

4.14.2. Yapılan testler sonucunda oluşturulacak rapor, testin bitiminden sonra en geç 15 (onbeş) iş günü içerisinde idareye teslim edilmelidir.

4.14.3. Denetim raporu asgari şu konuları kapsamalıdır: Derlenen veriler, tespit edilen zafiyetler, zafiyetlerin risk düzeyleri ve gerçekleşmeleri durumunda oluşabilecek zararların ölçekleri, zafiyetlerin giderilmesine ilişkin (varsa alternatifli) öneriler ve Yüklenicinin diğer notları.

4.14.4. Dokümanda ayrıca testlerde elde edilen bulgular ve yapılmış olan belirlemeler ışığında, kurum bilişim ağı yapılanmasına ilişkin geliştirme ve değişiklik önerilerine yer verilecek bir strateji belgesi üretilerek İdareye sunulacaktır.

4.14.5. Denetim ve analiz sırasında ortaya çıkan kritik güvenlik konularının karşılıklı olarak görüşülerek hızlıca giderilmesi için öneriler sunulacaktır. Bu açıklıklar için raporlama beklenmeyecektir. İdare, sözleşme süreleri içerisinde kalmak koşulu ile, belirlendikten sonra giderilen açıklıkların güncel bir testini talep edebilecektir. Bu testler için ilave ücret talep edilemeyecektir.

5. BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ DANIŞMANLIĞI

Yüklenici, işin kapsamında aşağıdaki hizmetleri verecektir.

5.1. Sınıflanmış varlıkların gruplanmasına destek vermek
5.2. Sınıflanmış ve gruplanmış varlıkların kritiklik derecelerinin belirlenmesine destek vermek
5.3. Tüm varlık gruplarının tabi olduğu rehber maddelerinin tespitine destek vermek
5.4. Tüm varlık gruplarının tabi olduğu rehber maddelerinin şartlarını sağlama durumunun tespitine destek vermek
5.5. Rehbere uyumun sağlanması için izlenecek yola ait çalışma planının oluşturulmasına destek vermek
5.6. Proje dahilinde yapılacak farkındalık çalışmalarına destek vermek
5.7. Çalışma planının uygulanması için yürütülecek projenin yönetimine destek vermek
5.8. Proje sonuçlarının ve etkinliğinin kontrolüne destek vermek
5.9. Yaptırılacak sızma test(ler)inin sonuçlarının değerlendirilmesine destek vermek
5.10. Çalışmalar sırasında yapılacak veya yaptırılacak teknik kontrollerin sonuçlarının değerlendirilmesine destek vermek
5.11. Proje süresince rehbere uyum için çalışması gereken birimlerinin koordinasyon faaliyetlerine destek vermek
5.12. Rehbere uyumun kontrolü için yapılacak denetimlerde İdare Denetçilerine planlama desteği vermek

6. YÖNTEM

6.1. İşin başlangıcında bir çalışma planı yapılacak ve taraflarca onaylanacaktır.
6.2. Çalışmaların durumu ve gereklerine göre uzaktan bağlantı, telekonferans, yüz yüze çalışma veya saha ziyareti yöntemleri kullanılacaktır.
6.3. Her çalışma için yöntem birlikte kararlaştırılacaktır.
6.4. Danışman; çalışma programına uygun olarak bir proje takip platformu üzerinden (Trello, Asana, Wrike, vb.) bir proje panosu oluşturacak ve projede görev alacak kişiler bu çalışma ortamına, rolleri dahilinde, eklenecektir.
6.5. Görev kartları bu panoda işlenecektir. Projenin ilerlemesi anlık olarak izlenecektir.
6.6. Dosya paylaşımı için bu pano kullanılmayacaktır.
6.7. Her çalışmanın sonunda danışmanlık takip formu oluşturulacak ve karşılıklı (e-)imza altına alınacaktır.
6.8. Proje süresince aylık ilerleme raporları hazırlanacak ve kuruma sunulacaktır.
6.9. Çalışmalarda ihtiyaç duyulduğunda teknik uzmanlar da görevlendirilecektir. Kurum veya danışmanın teknik uzmanları da aynı gizlilik ilkelerine bağlı olarak çalışacaktır.
6.10. Eğer ön görülemeyen şartlardan dolayı planlanmış uzaktan veya yüz yüze çalışmanın yapılamaması söz konusu olursa bu bilgi geç kalınmadan karşı tarafa bildirilecek ve alternatif çalışma zamanı kararlaştırılacaktır.
6.11. Çalışmalar sırasında farkındalık veya diğer eğitim faaliyetleri tercihen online, etkinliğin sağlanması için ihtiyaç duyulması halinde ise yüz yüze yapılacaktır. Eğitim yeri, ortamı ve katılımcıların organizasyonu ve lojistiği kurum tarafından yapılacaktır. Tüm eğitim malzemesi danışman tarafından hazırlanacaktır.
6.12. Panoda takip edilen işlerin durumu ve proje takvimine uyumda sorun veya olası tıkanıklıklar tespit edildiğinde taraflar için uygun olan en kısa sürede değerlendirme

toplantısı yapılacak ve çözüm yöntemi tespit edilecektir. Toplantı kararları karşılıklı ıslak imza veya e-imza ile kayıt altına alınacaktır.

7. DANIŞMAN PERSONEL NİTELİKLERİ

7.1. Projede görev alacak danışman personeli aşağıda listelenen şartlardan en az birini sağlamalıdır.

7.1.1. Danışmanlık görevini yürütecek ekip kümülatif olarak bu şartların tamamını sağlamalıdır.
7.1.2. ISO 27001 BGYS Baş Denetçi belgesine sahip olmak
7.1.3. ISO 27701 KVYS Baş Denetçi belgesine sahip olmak
7.1.4. ISO 22301 İSYS Baş Denetçi belgesine sahip olmak
7.1.5. Bilgi Teknolojileri, Bilgi Güvenliği ve ilgili sektörlerde veya projelerde en az 5 yıl tecrübeye sahip olmak
7.1.6. Kamu veya Kritik altyapı şirketlerinde Bilgi Teknolojileri, Bilgi Güvenliği veya İş Sürekliliği yöneticiliği yapmış olmak
7.1.7. TSE tarafından verilen Bilgi ve İletişim Güvenliği Uyum Denetçisi Eğitim Sertifikasına sahip olmak
7.1.8. TSE onaylı Cumhurbaşkanlığı Dijital Dönüşüm Ofisi "Bilgi ve İletişim Güvenliği D1 ve D2 Denetçisi Eğitimi" Sertifikasına sahip olmak
7.1.9. En az bir üniversitede Bilgi ve İletişim Güvenliği Uyum Danışmanlığı yapmış olmak

8. GENEL HUSUSLAR

8.1. Yüklenici, sözleşme aşamasında projede görevlendireceği personelin bilgilerini İdare ile paylaşacak ve işin sonuna kadar proje personelinin teminini sağlayacaktır.
8.2. Yüklenici, sağladığı personelin uzmanlığının yeterli olmadığı durumlarda, çözüm odaklı uzman personel sağlamakla yükümlüdür. Yüklenici sağlamış olduğu uzman personel ile ilgili özgeçmiş bilgilerini önceden İdare ile paylaşacaktır ve İdarenin onayından sonra uzman personel çalışmaya başlayacaktır. Yüklenici, sözleşme süresince sorunlar giderilene kadar teknik uzman hizmeti verecektir.
8.3. İdare, Yüklenici personelinin yetersiz bulunduğu veya tutum ve davranışları uygun görülmediği takdirde personelin değiştirilmesi talebinde bulunabilir. İdarenin söz konusu personelin değiştirilmesi isteğini yazılı olarak Yükleniciye bildirdiği tarihten itibaren en geç 15 (onbeş) iş günü içerisinde personel, İdare tarafından uygun görülen kişi ile değiştirilecektir.
8.4. Proje ekibinde en az 4 (dört) kişi yer alacaktır. Teknik açıklık testlerini gerçekleştirecek uzman veya uzmanlar ile aynı kişi olmamak üzere yüklenici tarafından; 1 (bir) Proje Koordinatörü görevlendirilecektir. Proje koordinatörü; projenin yönetilmesinden sorumlu olacak, sözleşme süresi boyunca proje ile ilgili olarak İdare tarafından muhatap kabul edilecek, genel olarak projenin takibinden, üretilen çıktıların doğruluğu ve kalitesinin kontrolünden sorumlu olacaktır.

8.5. Projede görev alacak danışman personeli aşağıda listelenen şartları sağlamalıdır.

8.5.1. ISO 27001 BGYS Baş Denetçi belgesine sahip olmak
8.5.2. ISO 27701 KVYS Baş Denetçi belgesine sahip olmak
8.5.3. ISO 22301 İSYS Baş Denetçi belgesine sahip olmak
8.5.4. Bilgi Teknolojileri, Bilgi Güvenliği ve ilgili sektörlerde veya projelerde en az 5 yıl tecrübeye sahip olmak
8.5.5. Kamu veya Kritik altyapı şirketlerinde Bilgi Teknolojileri, Bilgi Güvenliği veya İş Sürekliliği yöneticiliği yapmış olmak
8.5.6. TSE tarafından verilen Bilgi ve İletişim Güvenliği Uyum Denetçisi Eğitim Sertifikasına sahip olmak
8.5.7. TSE onaylı Cumhurbaşkanlığı Dijital Dönüşüm Ofisi "Bilgi ve İletişim Güvenliği D1 ve D2 Denetçisi Eğitimi" Sertifikasına sahip olmak
8.5.8. En az bir üniversitede Bilgi ve İletişim Güvenliği Uyum Danışmanlığı yapmış olmak

8.6. Proje Koordinatörünün sahip olması ve sözleşme aşamasında belgelendirmesi gereken özellikler şunlardır.

8.6.1. Proje koordinatörü Yüklenici firmanın çalışanı olmalıdır.

8.7. Sızma testi personeli Firmanın Kendi Personeli olmalı ve Bilgi güvenliği alanında CISA, LPT, CISSP, OSCP, CCEE, TSE Kıdemli Sızına Test Uzmanı sertifikası veya TSE Sızma Testi Uzmanı sertifikalarından en az ikisine sahip olmalıdır.
8.8. Danışman, daha önce bilgi güvenliği alanında en az 2 (iki) tanesi kamu kurumu projesi olmak üzere IS027001 belgesi ile sonuçlandırılmış en az 2 (iki) projede görev almış olmalıdır.
8.9. Yüklenici firmada ve personelde aranan ve teklif aşamasında belgelendirmesi gereken nitelikler aşağıda verilmiştir.
8.9.1. ISO 9001:2015 Belgesine sahip olmak
8.9.2. ISO27001:2013 Belgesine sahip olmak
8.9.3. ISO20000 -1:2008 ISO/IEC Sertifikasına sahip olmak
8.9.4. TSE onaylı A veya B Sızma Testi belgesine sahip olmak
8.9.5. TSE onaylı Cumhurbaşkanlığı Dijital Dönüşüm Ofisi "Bilgi ve İletişim Güvenliği D1 ve D2 Denetçisi Eğitimi" Sertifikasına sahip olmak

8.10. Yüklenici, bu teknik şartname kapsamındaki Projenin eksiksiz olarak tamamlanmasından sorumlu olacaktır.
8.11. Yüklenici, projede görev alacak personelin nüfus cüzdanı fotokopilerini, adli sicil kayıtlarını, iş deneyimlerini ve sertifikalarım sözleşme dosyasına ekleyecektir.
8.12. Yüklenici, şartnamede tanımlanan aşamalara ait işlerle ilgili hiçbir bilgiyi İstanbul Ticaret Üniversitesi Bilgi İşlem Daire Başkanlığı personelinden saklamayacak, belirlenen güvenlik seviyesine sahip personele tüm bilgileri istenildiği zaman verecektir. Yüklenici, ve projede görev alacak personel, İstanbul Ticaret Üniversitesi ile ilgili veya işin kapsamına giren öğrendiği hiçbir bilgiyi üçüncü şahıslar ile paylaşmayacağını taahhüt edecek İstanbul Ticaret Üniversitesi Bilgi İşlem Dairesi Başkanlığı ile gizlilik sözleşmesi imzalayacaktır.
8.13. Yüklenici, bu teknik şartname maddeleri aşamalarına uygun şekilde, sözleşmenin imzalandığı tarihten en geç 10 (on) iş günü içerisinde proje

süresince kullanacağı kaynakları, iş kalemlerini ve bu iş kalemleri için öngördüğü süreleri içeren detaylı bir "Proje Planı" ile birlikte konfigürasyon ve değişiklik yönetim planı içeren "Proje Başlangıç Raporunu" İdare'nin onayına sunacaktır.

8.14. Proje Planı ile Proje Başlangıç Raporu, İDARE tarafından en geç 5 (beş) takvim günü içerisinden onaylanacaktır

8.15. Yüklenici, bu şartname kapsamında yürüttüğü iş ve işlemler sırasında, BİDB bilişim sistemlerine bilerek veya bilmeyerek vereceği tüm zararı karşılayacaktır.