ZORLU ENERJİ ENTEGRE RİSK YÖNETİMİ

Zorlu Enerji, tehdit oluşturabilecek riskleri belirlemek amacıyla bütünleşik ve merkezi bir kurumsal risk yönetim sistemini benimsemiştir. Bu sayede, risklerini daha kapsamlı, etkili ve maliyet açısından uygun bir şekilde tanımlayıp değerlendirebilmekte ve yönetebilmektedir. Bu süreçte, COSO'nun İç Kontrol Entegre Çerçevesi ve ISO 31000 Risk Yönetimi Standartları ile uyum sağlayarak risk yönetim sistemi kurmuştur. Bu adımlar çerçevesinde, ISO 31000'e dayalı ISO 9001 ve 14001 Yönetim Sistemleri prosedürlerini de hayata geçirmiştir. Bu sistemle, günlük operasyonlarında sürekli olarak risk ve fırsatlar her yıl gözden geçirilmektedir. Bu yönetim stratejisi, risklerin analiz edilmesi, sıralanması ve takip edilmesini kolaylaştırmaktadır. Ayrıca, Kurumsal Risk Yönetimi ve Finans Departmanları, mali etkileri senaryo bazlı hesaplayıp, bu senaryo sonuçlarını Sürdürülebilirlik Kurulu ile paylaşarak riskleri entegre etmektedir. Kurul, sürdürülebilirlikle ilgili tüm riskleri analiz etmekte ve en önemlilerini yönetim stratejilerini belirlemek üzere üst yönetim kuruluna sunmaktadır. Bu noktada, Yönetim Kurulu risk seviyesini yeniden değerlendirerek, alınacak tedbirleri saptamaktadır. Yönetim Kurulu bu kararları, Yönetim Kurulu ile CEO'yla paylaşmakta ve öneriler, Yönetim Kurulu ve CEO'nun onayıyla hayata geçirilmektedir.

Etkili bir değerlendirme ve yönetim için Kurumsal Risk Yönetimi departmanı bünyesinde Erken Risk Tespit Komitesi kurulmuştur. Komite, risk azaltma stratejilerinin uygulanması ve risk yönetiminden sorumludur. İki bağımsız yönetim kurulu üyesinden oluşan Riskin Erken Saptanması Komitesi çalışmaların etkinliği için gerekli görülen ve çalışma esaslarında açıklanan sıklıkta, yılda en az 3 defa toplanır. Riskin Erken Saptanması Komitesi iş operasyonlarına zarar verebilecek riskleri zamanında ve doğru bir şekilde belirlemek için 2023 yılında 6 defa toplanmış ve hazırladığı 6 adet risk raporunu Yönetim Kurulu'na sunmuştur. Riskin Erken Saptanması Komitesi Tutanakları her yıl dış denetçi tarafından gözden geçirilmektedir. Risk değerlendirme sürecinde; yasal yaptırımlar, olasılık, frekans, alaka düzeyi, etkilenen işletmelerin sayısı, zaman sınırlamaları ve etki yoğunluğu gibi çeşitli faktörler göz önünde bulundurulmaktadır. Risk haritalamasında, daha önceden oluşturulan risk envanterinden yararlanılmaktadır. Ekonomik, çevresel ve sosyal etkiler incelenmekte ve envanterle uyumlu bir SWOT analizi gerçekleştirilmektedir, bu sayede potansiyel fırsatlar belirginleşmektedir. Daha sonra, bu çalışmaların tüm sonuçları Sürdürülebilirlik Kurulu'na sunulmaktadır.

Zorlu Enerji Grubu şirketlerinin varlığını, gelişmesini ve devamını tehlikeye düşürebilecek risklerin erken teşhisi, tespit edilen risklerle ilgili gerekli önlemlerin uygulanması ve risklerin merkezi bir

yapıda yönetilmesi amacıyla, Zorlu Holding Kurumsal Risk Yönetimi Bölümü faaliyetlerine devam etmektedir.

Bu kapsamda Zorlu Holding bünyesinde faaliyet gösteren tüm ilişkili şirketlerde geçerli olmak üzere Zorlu Holding Risk Politika ve Prosedürü ile Kurumsal Risk Yönetimi Çerçevesi hazırlanmıştır.

Zorlu Holding Kurumsal Risk Yönetimi çerçevesi aşağıdaki temel unsurlardan oluşmaktadır:

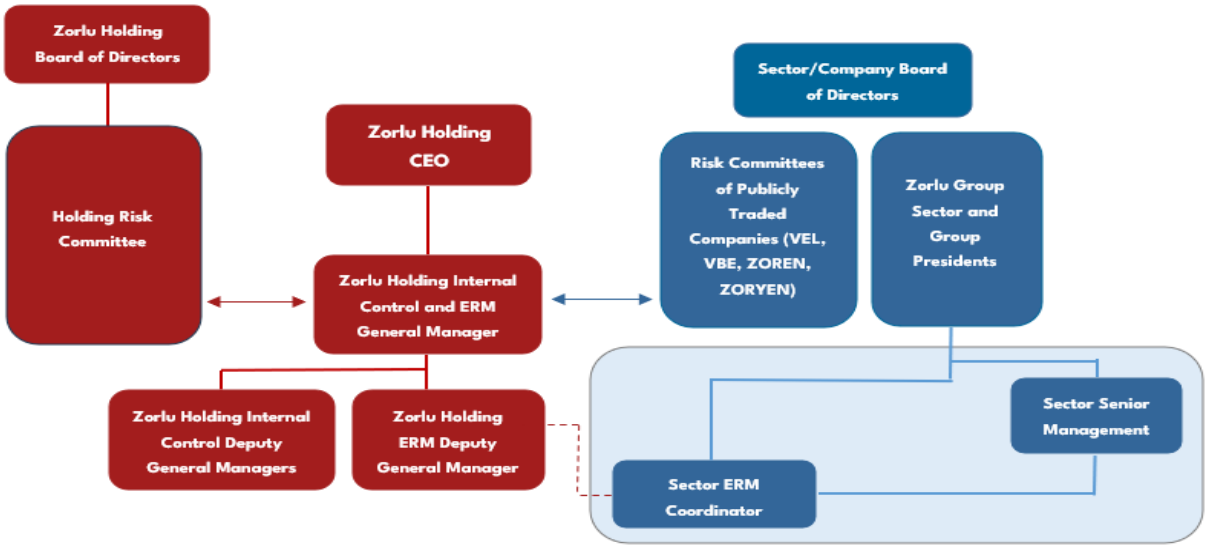
1. Kurumsal Risk Yönetim Modeli
2. Risk Değerlendirmesi
3. Risk Yönetim Stratejileri
4. İletişim ve Danışma
5. İzleme ve Gözden Geçirme
6. Raporlama

Kurumsal Risk Yönetimi (KRY) Departmanı, Holding bünyesinde kurulmuş olup, tüm Gruba merkezi olarak hizmet vermektedir. KRY departmanı, risk yönetim çerçevesini uygun şekilde tasarlamak ve yönetimin bunu etkin bir şekilde işletmesi için rehberlik etmekten sorumludur.

Holding KRY Departmanı, Holding İç Kontrol ve Kurumsal Risk Yönetimi Genel Müdürüne rapor verir, Genel Müdür de Holding CEO'suna rapor verir. Departman, çalışmalarının sonuçlarını Holding CEO'su, Holding ve Grup şirketlerindeki Risk Komiteleri, Sektör Yönetim Kurulları ve Holding ve Grup şirketlerinin ilgili yönetim ekiplerine ileterek görevlerini yerine getirir.

Kurumsal Risk Yönetimi Departmanı, faaliyetlerini yürütürken gizlilik çerçevesinde ihtiyaç duyduğu tüm kayıt, personel, varlık ve operasyonlara erişim yetkisine sahiptir. Grup içindeki Kurumsal Risk Yönetimi faaliyetlerinin çıktıları, önem ve ilgili risk seviyeleri dikkate alınarak çeşitli seviyelere raporlanır.

Aşağıdaki organizasyon şeması, Sektör/Şirket ve Holding yönetsel fonksiyonları ile "İç Kontrol ve Kurumsal Risk Yönetimi Departmanı" arasındaki ilişkileri göstermektedir.



Kurumsal risk yönetiminin son sorumluluğu, ilgili alanlarındaki üst düzey yöneticiler ve işlev yöneticilerine aittir; ancak kurumsal risk yönetimi süreçleri Sektör KRY Koordinatörleri ve Holding KRY Genel Müdür Yardımcısı rehberliğinde ve koordinasyonunda yürütülür.

Kurumsal Risk Yönetimi Departmanı uluslararası standartların prensip ve yönergeleri (IIA, COSO ERM Çerçevesi) doğrultusunda faaliyet gösterir. Birinci hat süreç ve risk taşıyan fonksiyonlarla sürekli iletişim halinde olup, rehberlik ve koordinasyon sağlar. Ayrıca ikinci hat işlevi olan İç Kontrol Departmanı ile yakın işbirliği içinde çalışır, risklere ilişkin mevcut ve arzu edilen iç kontrol tasarımları ile ilgili bilgi paylaşır ve ilgili süreçlerin olgunluk düzeylerini değerlendirir. Tüm detaylar Zorlu Holding KRY Politikası ve Zorlu Holding KRY Prosedürü belgelerinde bulunmaktadır.

İç Kontrol İç kontrol çerçevesi, Zorlu Grubu içinde yöneticilere, Yönetim Kurullarına, ilgili Komitelere ve paydaşlara iç kontrol sistemlerini kurma, değerlendirme ve güçlendirme konusunda yardımcı olacak şekilde tasarlanmıştır. Çerçeve, hedeflere yönelik genel prensipleri içerir ve Zorlu Grubu paydaşları, iç kontrol sistemine ilişkin değerlendirme yaparken başvurabilecekleri bir referans olarak kullanabilirler. Çerçeve oluşturulurken uluslararası standartlarda en çok kullanılan iç kontrol çerçevesi olan "COSO İç Kontrol - Entegre Çerçeve" esas alınmış olup, Zorlu Grubu için uygun düzenlemeler yapılmıştır.

Zorlu Grubu İç Kontrol Çerçevesi, kurumsal (varlık düzeyi), iş süreçleri (süreç düzeyi) ve bilgi teknolojisi (BT genel kontrolleri) düzeylerinde iç kontroller kurulurken takip edilmesi gereken genel prensipleri içeren bir referans politika belgesidir. İç kontrol çerçevesinin ana amacı, Zorlu Grubu şirketlerinin çalışanlarına süreç bazında risklerini değerlendirme ve iç kontrol sistemlerini ve faaliyetlerini geliştirme konusunda yardımcı olmaktır.

Çerçeve, stratejik, operasyonel, finansal ve raporlama ve uyumluluk alanlarında hedeflere başarılı bir şekilde ulaşma konusunda makul güvence sağlamak için gerekli olan iç kontrol prensiplerini belirler. Bu çerçeve içinde, İç Kontrol Departmanı tüm Grup şirketlerinde ve temel süreçlerinde iç kontrol değerlendirmeleri ve güçlendirme projeleri yürütür. Bu çabalar, Kurumsal Risk Yönetimi (KRY) fonksiyonu ile yakın bir şekilde paylaşılır, böylece risk yönetimi prensipleri entegre edilir ve uyumlu hale getirilir. İç kontrol ve KRY ekipleri arasındaki işbirliği, genel risk azaltma stratejilerini güçlendirir ve iç kontrol etkinliğini artırır.

Kurumsal Risk Yönetimi Eğitimleri

Zorlu Holding, **Kurumsal Risk Yönetimi** (KRY) yaklaşımında tehdit ve fırsatları değerlendirirken her zaman stratejik hedeflerini ve değerlerini, tüm yönetim kadrolarının karar aşamalarında dikkate almalarını önemsemektedir. Bu çerçevede, kurumsal risk yönetiminin Holding'in ve Grup şirketlerinin stratejilerine ve kurum kültürüne entegre edilerek, stratejik yönetim kararlarından günlük operasyonların yürütülmesine kadar her aşamada dikkate alınması, tüm çalışanların risklere, tehdit ve fırsatlar bakış açısıyla yaklaşması ve bu yolla sürdürülebilir büyümeye katkıda bulunulması hedeflenmektedir.

Zorlu Grubu bünyesindeki tüm çalışanlar, yürüttükleri faaliyetler, süreçler ve sistemlerle ilgili; risklerin erken belirlenmesinde, ölçülmesinde ve Grubumuzun risk prensiplerine uygun şekilde etkin olarak yönetilmesinde, ana sorumluluk sahibidir. Çalışanlar, kurumsal risk yönetimi konularında soruları ve görüşleri olduğunda, bunları öncelikle ilgili yöneticileri ve gerekli olduğu durumlarda Sektör KRY faaliyetlerinden sorumlu çalışma arkadaşlarımız veya Holding Kurumsal Risk Yönetimi Bölümü'ne iletmeli ve danışmalıdır. Bu kapsamda hem çalışanlara hem de belirli Yönetim Kurulu üyelerine Kurumsal Risk Yönetimi eğitimleri verilmektedir.

Ortaya Çıkan Riskler

Aşağıda Zorlu Enerji ortaya çıkan risklerinden örnekler sunulmuştur. Tüm risklere 2023 Entegre Faaliyet Raporu sayfa 76'dan ulaşabilirsiniz.

Ortaya Çıkan Risk 1: Siber Risk

Kategori: Stratejik Risk

Tanım:

Bilgi teknolojileri ve dijital sistemlerle ilgili güvenlik açıkları, tehditler ve tehlikelerle ilgili riskleri ifade eder. Bu riskler, bir kuruluşun bilgi varlıklarına, sistemlerine ve veri bütünlüğüne zarar verme potansiyeline sahip çeşitli faktörlerden kaynaklanabilir.

Etki:

Siber riskler, şirketlerin operasyonlarını, itibarlarını ve finansal durumlarını çeşitli şekillerde etkileyebilir:

- Finansal Kayıplar
- İtibar Zararları
- Operasyonel Aksamalar
- Veri Kaybı ve Hırsızlığı
- Yasal ve Düzenleyici Sonuçlar
- Yüksek Güvenlik Maliyetleri
- Rekabet Avantajı Kaybı

Aksiyonlar:

Zorlu Enerji, müşteri verilerinin korunması ve siber güvenlik konularında yüksek standartlara sahip politika ve uygulamalara sahiptir. Şirketimiz, müşteri ve genel halkın gizliliğini ve bütünlüğünü korumak için ISO 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasına sahiptir. Bu sertifika, Zorlu Enerji'nin siber saldırılara, yetkisiz erişime ve veri ihlallerine karşı koruma sağlamak için gerekli politika ve güvenlik önlemlerini uyguladığını göstermektedir.

Siber güvenlik tehditlerinin dinamik ve sürekli evrim geçirdiğini kabul eden şirketimiz, sistemlerimizi, uygulamalarımızı ve bilgi depolarımızı korumak için kapsamlı güvenlik girişimlerine yatırım yapmaktadır. Bu çabalar, teknoloji, süreçler, kaynaklar, eğitim, felaket kurtarma planları ve en iyi

uygulamalara karşı sürekli test ve değerlendirmeyi içermektedir. ISO 27001 sertifikası, şirketimizin bilgi güvenliği yönetim sistemimizdeki riskleri belirleme, değerlendirme ve hafifletme konusunda sürekli bir süreç izlediğini ve bu nedenle siber saldırılara karşı koruma sağladığını belgelemektedir. (IAR, sayfa 182)

- **Ağ Segmentasyonu Projesi:** Tesisin siber güvenliğini artırmak amacıyla bir ağ segmentasyonu projesi uygulanmıştır. (IAR, sayfa 177)

Ortaya Çıkan Risk 2: Küresel Isınma ve İklim Değişikliği Riski

Kategori: İklimle İlgili Riskler

Tanım:

İklimle İlgili Riskler, iklim değişikliği ve iklimle ilgili olayların (aşırı hava koşulları, sıcaklık artışları ve deniz seviyesinin yükselmesi gibi) bir kuruluşun operasyonları, varlıkları veya iş modeli üzerindeki etkileri olarak tanımlanır. Bu riskler iki ana kategoriye ayrılabilir:

1. **Fiziksel Riskler:** İklim değişikliğinin doğrudan etkileri, doğal afetler, sel ve kuraklık gibi.
2. **Geçiş Riskleri:** İklim değişikliği ile ilgili politikalar, teknolojiler ve pazar değişikliklerinden kaynaklanan riskler; örneğin, karbon düzenlemeleri veya yenilenebilir enerjiye geçiş.

Bu riskler, işletmelerin finansal performansını, itibarını ve uzun vadeli sürdürülebilirliğini etkileyebilir.

Etki:

İklimle ilgili riskler, şirketlerin operasyonlarını, itibarını ve finansal durumlarını çeşitli şekillerde etkileyebilir:

- Finansal Etkiler
- Düzenleyici ve Politik Değişiklikler
- Pazar Değişiklikleri
- Operasyonel Aksamalar
- İtibar Yönetimi
- Yatırım ve Finansman Zorlukları
- Fiziksel Altyapı Etkileri

Bu etkiler, enerji şirketlerinin stratejilerini ve iş modellerini yeniden değerlendirmesini gerektirebilir.

Aksiyonlar:

TCFD raporlamasında ele alındığı gibi, iklim değişikliği ve su kıtlığı ile ilgili riskler konusunda bir risk değerlendirmesi yapılmıştır. Bu risklerin etkileri, özellikle su kaynaklarına bağımlı olan yenilenebilir enerji santrallerinde detaylı bir şekilde analiz edilmiştir. Bu enerji kaynaklarının verimsiz çalışması, yerel topluluklarla olası çatışmalar ve su paylaşımı gibi konular da değerlendirme sürecine dahil edilmiştir. Detaylı bilgiye Zorlu Enerji TCFD Raporunun 16-26 arası sayfalarından ulaşılabilir.