

Enstitüsü : Lisansüstü Eğitim Enstitüsü

Dalı : İşletme

Programı : İşletme Uzaktan Öğretim Tezli Yüksek Lisans

Tez Danışman : Dr. Öğr. Üyesi Özgür ATILGAN

Tez Türü : Yüksek Lisans

ÖZET

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN OLUŞTURULMASI, IEC/ISO 27001 STANDARTININ BİR SİVİL HAVACILIK KURUMUNDA HAYATA GEÇİRİLMESİ

SEYDA EMİR ERDOĞAN

Günümüz gelişen teknolojisinde ve rekabetçi pazar koşullarında kuruluşların en değerli varlıklarından bir tanesi şüphesiz sahip olduğu bilgilerdir. Bu bilgilerin kötücül amaçlar besleyen kişilerin eline geçmesi veya çeşitli tehditlerin meydana gelmesi durumunda kuruluşlar maddi anlamda zarara uğrayacaktır. Dijital veya basılı olarak işlenen, saklanan bilginin uygun güvenlik süreçleri tanımlanarak koruma altına alınması oluşabilecek zararları en aza indirmektedir. Özellikle havayolu firmaları gibi ülkelerin stratejik öneme sahip kuruluşları kötü niyetli kişiler tarafından sıklıkla hedef alınmaktadır. Hassas bilgilere sahip olan sivil havacılık kuruluşlarının, bilgi güvenliği unsurlarını dikkate alarak, etkinliği sürekli denetlenen bir bilgi güvenliği yönetim sistemi oluşturması gerekmektedir.

Bilgi güvenliği yönetim sisteminin oluşturulması konusunda gereken tüm maddeleri içeren IEC/ISO 27001 standardı kuruluşlara bir çerçeve sunmaktadır. IEC/ISO 27001 standardı Sivil Havacılık Genel Müdürlüğü'nün yayınlamış olduğu bir genelge ile tüm kurumlara zorunlu hale gelmiştir. Bu nedenle, sivil havacılık kuruluşları IEC/ISO 27001 standartına sadece bilgi güvenliği'ne uygun bir yapının oluşturulması için değil SHGM tarafından yayınlanan genelgeye uygunluk sağlanabilmesi için uyumlu hale gelmelidir.

Kuruluşlar, IEC/ISO 27001 standartını uygulayarak bilgi güvenliği yönetim sisteminin hedeflenen çıktılarını tüm personele ve paydaşlara duyurmalı ve kurum genelinde bilgi güvenliği farkındalığı oluşturmalıdır. Kapsam içerisinde bulunan birimlerin risk ve fırsatları ele alarak değerlendirmeli, ve uygun risk işleme seçenekleri uygulanmalıdır. BGYS'nin hedeflenen çıktıları denetlenerek sürekli iyileştirme yapılmalıdır. IEC/ISO 27001 standartının maddeleri uygulanarak bir bilgi güvenliği yönetim sisteminin sivil havacılık kuruluşunda nasıl uygulanacağı araştırılmıştır. Bu amaçla, IEC/ISO 27001 standartına sahip olan Türkiye'nin bayrak taşıyıcısı Türk Hava Yolları A.O esas alınarak bilgi güvenliği müdürlüğü yönetim ekibi ile mülakat çalışması gerçekleştirilmiştir. Yapılan mülakat sonucunda bilgi güvenliği yönetim sisteminin oluşturulması için önemli noktalar tespit edilmiştir.

Anahtar Kelimeler: BGYS, SHGM, Bilgi Güvenliği, IEC/ISO 27001 Standartı

Institute : Institute of Graduate Education

Department : Business Administration

Programme : Master of Business Administration

Supervisor : Asst. Prof. Dr. Özgür Atılgan

Degree Awarded : Master Thesis

ABSTRACT
**BUILDING AN INFORMATION SECURITY MANAGEMENT SYSTEM,
IMPLEMENTATION OF IEC / ISO 27001 STANDARD IN A CIVIL
AVIATION ORGANIZATION**

SEYDA EMİR ERDOĞAN

In this technological era and competitive market conditions, information is undoubtedly one of the most valuable assets of the institutions. In the event that malicious people capture information of the institutions, or if various threats are occurred, will cause negative effects on these institutions, like damaging their economies. However, identifying appropriate security processes for stored information, processed digitally or wirelessly, minimizes damages that need to be managed with protection. The organizations that have strategical importance for nation-states are especially targeted by cyber attackers around the world. Therefore, civil aviation organizations, which have sensitive information, should establish an information security management system that is continuously monitored by taking into consideration the information security elements.

IEC / ISO 27001 standard, which includes all the necessary elements for the establishment of an information security management system, provides a framework for organizations. The IEC / ISO 27001 standard has become mandatory for all institutions with a circular issued by the General Directorate of Civil Aviation in Turkey. Therefore, civil aviation organizations should comply with the IEC / ISO 27001 standard not only for the creation of a structure that complies with information security, but also for compliance with the circular issued by the SHGM.

By implementing the IEC / ISO 27001 standard, organizations should communicate the targeted outputs of the information security management system to all staff and stakeholders and raise information security awareness throughout the organization. The units within the scope should be evaluated by considering risks and opportunities, and some appropriate risk processing options should be applied. Continuous improvement should be made by monitoring the targeted outputs of ISMS. The provisions of the IEC / ISO 27001 standard were applied, and how an information security management system is implemented in a civil aviation organization was investigated. For this purpose, IEC / ISO 27001 standard with Turkey's flag carrier Turkish Airlines A.O director of information security governance based on interviews with team work was carried out. As a result of the interview, important points were determined for the establishment of information security management system.

Keywords: ISMS, SHGM, Information Security, IEC/ISO 27001 Standart