BİLGİSAYAR MÜHENDİSLERİ KURULTAYI
10-11 ŞUBAT 2018, BOĞAZİÇİ ÜNİVERSİTESİ-İSTANBUL

Mesleki Düzenlemeler, Mesleki Denetim ve İmza Yetkisi

Funda ÇETİNTAŞ
ISACA İstanbul Chapter Başkanı

Bilgisayar Mühendisleri Kurultayının değerli katılımcıları, sevgili meslektaşlarım ve saygıdeğer panelistler hepinizi saygıyla selamlıyorum.

BMO'nun emek emek işlenerek oluşumuna tanık olan bir üyesi olarak Kurultay'ın önemli bir sıçrama noktası olduğunu düşünüyorum ve bundan dolayı çok heyecanlıyım. Bu heyecanımı sizlerle paylaşmayı ve sizlerle buluşma fırsatını yarattığı için Kurultay Düzenleme Kuruluna çok teşekkür ederim.

Bu sene, Bilgisayar Mühendisliği bölümlerinin kuruluşunun 40. yılını tamamladık. 1977'de açılan ilk lisans bölümlerinin ilk öğrencilerinden biri olmak benim için ayrı bir öneme sahip. Türkiye'nin ilk bilgisayar mühendislerinden biri olarak yaklaşık 35 yıldır sürdürdüğüm meslek yaşamımda mesleğin çeşitli alanlarında görev yaptım. Yazılım geliştirme uzmanı olarak başlayan meslek hayatım proje yöneticiliği, bilgi işlem müdürlüğü, bilgi sistemleri baş denetçisi gibi birbirini tamamlayan ama farklı alanlarda devam etti.

Görev aldığım çoğu alanı iyi tanıyorsunuz. Sanırım en az bilinen yeni meslek alanlarımızdan biri *bilgi sistemleri denetçiliği*. Bugün sizlerle hem bu alandaki deneyimlerimi paylaşmak hem *denetimde sertifikasyon önemli mi* bunu değerlendirmek hem de bilgi işlem denetimi konusunda bilgi vermek istiyorum.

Biz bilgi teknolojisi uzmanlarının eğitiminde teknik bilgilerle donatılmamız öne çıkmakla birlikte *kontrol* ve *risk* kavramlarıyla eğitimde genelde tanışmayız. Hedef, işimizi teknik anlamda en iyi şekilde yapmak, bu konuda gereken donanımı sağlamaktır. Bu arada yaptığımız işlerin işe yansımaları, BT'deki güvenlik zafiyetlerinin sonuçları, teknik elemanların işi olarak görülmez. Ancak son yıllarda yaşanan bazı olayları ve siber saldırılar sonucu bilgi teknolojileri, riskleri değerlendirmeden ilerlenmesi zor bir alan olmaya başlamıştır.

Bu konuda belki de en vurucu ve tüm denetim ve kontrol mekanizmalarını etkileyen örnek, 2001 yılında yaşanan Enron skandalıdır. Bilmeyenler için küçük bir not: Önceleri bir doğalgaz dağıtım firması olarak başlayan, yıllar içinde çok farklı konulara el atan ve uluslararası boyutlarda büyük bir şirket olan Enron'un borsadaki değerlerinin bir kısmının fiktif olduğu, muhasebe kayıtlarında manipülasyon yapıldığı ortaya çıkmış ve sonrasında firma büyük bir çöküş yaşamıştır. Bu olay sadece Enron firması değil, denetçisi Arthur Andersen firmasının da sonunu getirmiş ve dünyada 85.000 kişi bu olay nedeniyle işsiz kalmıştır.

Türkiye'de de 2003 yılında İmar Bankası skandalı patlak vermiştir. Çift kayıt skandalı olarak da adlandırılan bu skandalda resmi kurumlara, BDDK'ye ve denetim şirketine gösterilen kayıtlarla gerçek kayıtlar arasında ciddi fark olduğu ortaya çıkmış, uzun süre gerçek kayıtların elde edilmesi ve banka müşterilerinin zararlarının en aza indirgenmesi için çalışılmıştır.

Biri dünyayı diğeri Türkiye'yi sarsan her iki olayda da süreç ve bilgi sistemlerindeki kontrol eksiklerinin olmasının, suiistimal tespitini güçleştirmesi ve sisteme güvensizliği artırması nedeniyle ülkeler bir arayışa girmiş ve bu konuda yeni düzenlemeler getirilmiştir.

ABD'de de çıkarılan Sarbane's Oxly yasasıyla kurumların iç kontrol ve iç denetim mekanizmalarının, sistem üzerindeki tehditleri, olası riskleri önceden görüp gerekli kontrol noktalarıyla donatması amacını gütmektedir ve bilgi sistemleri de bu yapı içerisinde önemli bir yer tutmaktadır.

Aynı şekilde finans dünyasında da BDDK bankaların iç kontrol ve iç denetim mekanizmalarını geliştiren mevzuatları hayata geçirirken çok ilerici bir yaklaşımla 2006 yılında sadece finansal süreçlerin değil, bu süreçlerin gerçekleşmesi için kullanılan uygulamalar ve sistemler de değerlendirilmeden gerçek bir kontrol mekanizması kurulamayacağı kararına varılmış ve bilgi sistemleri denetimini Türkiye'de ilk kez yasal düzenlemelere sokmuştur.

BDDK, düzenlemelerinde ISACA'nın COBIT çerçevesini, BT yönetişim ve tüm BT süreçlerindeki kontrol hedeflerini kapsaması nedeniyle referans noktası olarak değerlendirmiş ve mevzuatta yer vermiştir.

Bu tarihten sonra daha önce çok kısıtlı alanlarda uygulanan yeni bir mesleki disiplin "bilgi sistemleri denetimi" hayatımıza girmiştir.

Biraz önce açıkladığım örneklerden görüleceği gibi BT denetiminin zorunlu hale gelmesinde kurumların muhasebe sistemleri ve bu sistemler üzerindeki risk faktörlerinin ortaya çıkarılıp risklerin minimize edilmesi temel alınmıştır.

BT denetimi tabii ki bununla kısıtla değildir. Korumak istediğiniz bilgi varlıklarını merkez alan bir risk yaklaşımı söz konusudur. Örneğin bir seçim sisteminde "seçim sonuçları güvenli midir" sorusunun yanıtı, bu süreçteki manuel ve otomatik kontrol noktalarının hangi riskleri ortadan kaldırdığıyla ya da riski azalttığıyla oranlı olarak değişkenlik gösterir.

Denetim, hiçbir zaman kesin bir güvence veremez. Çünkü denetimi yaptığınız ortam ve şartlar bir dakika sonra farklılaşabilir. Bazen bilinen riskleri tamamen ortadan kaldırmak mümkün değildir, bazen oluşmasına engel olamadığınız risklerin gerçekleştiğini tespit edip sonuçlarını düzeltmek zorunda kalabilirsiniz. En gelişkin sistemlerde bile otomatik olarak yapılan kontroller güvence seviyesini arttırsa bile "0"lamak mümkün değildir.

Örneğin çok gizli bir alana giriş için el tanıma, yüz tanıma vb. biyometrik tanıma yöntemleriyle giriş izni verildiğini düşünün. Sonuçta o kişiyi tanımlama işinin arkasında yine bir dizi otomatik kontroller vardır; ama sonuçta o kişiyi sisteme tanıtan bir görevlidir. Başka bir kişinin biyometrik verisini alsa ve sisteme kaydetse ne olacak? Sonuçta biyometrik veri de sistemde tutuluyor, yetkili birinin biyometrik verisini kendime tanımlasam ne olacak?

Bu nedenle denetim sadece belirli bir koruma noktası gözetilerek değil, süreci anlamak ve bu sürecin BT'ye yansımalarını gözlemlemek ve oluşan büyük resimdeki süreç ve BT'nin kendine ait risklerini ortaya koymakla olur.

Denetimin bu yapısı teknik bilgiyle birlikte süreç analizi ve süreç yaklaşımını da birlikte getirdiği için bilgisayar mühendisleri için çok cazip görünmemektedir. Aynı zamanda eğitim süreçleri denetim algısına yönelik unsurları genel olarak müfredatta barındırmadığı, BT denetimi genellikle yüksek lisans konusu olduğu için de bu konudaki bilgi eksikliği de mühendislerin bu konuya yaklaşımını kısıtlamaktadır.

Ben BT denetiminin BT'nin bütünsel sürecin bir parçası olduğunu algılamak, BT tabanlı çalışmaları yaparken risk algısını göz önünde tutmak gibi özel farkındalıklar geliştirdiği için değerli bir disiplin olduğunu düşünüyorum. BT denetimi, "network"ten sisteme, sistemden veritabanına, veritabanından iş uygulamalarına varan çok geniş bir alanda gerçekleştirilen ve belirli bir aşamadan sonra vizyoner bir bakış açısıyla tüm BT süreçlerine genel bakabilen bir profil geliştirilmesine de yardımcı olduğu için sadece teknik alanda kalmayıp ileride bir BT biriminin yöneticisi olmak isteyen gençler için de çok değerli bir birikim yaratmaktadır.

Tabii ki bu yeni disiplini uygulamak için ek bilgilendirmeye ve gözetim altında kontrollü uygulama çalışmalarına gereksinim vardır. Sertifikasyon tam da bu noktada devreye girmektedir. BT denetimi, mevcut uygulanışıyla iş süreçlerden özellikle de finansal raporlamadan ayrı düşünülemeyecek bir kavram.

Bu nedenle "Sürecin analizi nasıl yapılır? Bu süreçteki kritik bilgi varlıkları nelerdir? Bu bilgiler hangi ortamlarda saklanıyor? Kimler erişebilir? Bilgi sistemleri ve süreç üzerinde bu kritik varlıkları üzerindeki riskler nedir? Bu varlıkları nasıl koruyabiliriz? Korumak için yeterli önlemler alınmış mı? Alınan önlemler kontrol ediliyor mu? Süreçte bir değişiklik var mı? Bu değişikliğin riskler üzerindeki etkisi nedir? Riski azaltabiliyor ya da yok edebiliyor muyuz? Eğer yapamıyoruz bu riskten kaçınmamız mümkün mü?" gibi sorulara yanıt vermek için izlenmesi gereken adımların bir bölümü standartlarda tarif edilmiş olsa bile bu kapsamda bütünlükçü yaklaşım ve farkındalığı, sertifikasyonlarla ortaya konuyor.

2006'dan bu yana Türkiye'de önce BDDK, geçtiğimiz günlerde SPK tarafından yayımlanan bilgi sistemleri yönetim ve denetim yönetmelik ve tebliğleri, BT denetiminde CISA sertifikasını işaret etmektedir.

CISA sertifikası, Uluslararası Bilgi Sistemleri denetçisi unvanı veren ve tüm dünyada geçerli bir sertifikadır. Sertifika şu anda başkanı olduğum ISACA Istanbul Chapter'ının merkez örgütü ISACA tarafından verilmektedir. Sertifikasyon sınavları için gerekli Türkçeleştirme çalışmaları yapılmış ve merkez organizasyonumuz tarafından yönetilen sertifikasyon sürecinde "Türkçe" kabul edilen diller arasına girmiştir. Bu zor çalışmayı yürüten tüm ISACA'lılara bir teşekkür borçluyuz.

CISA sertifikasyon programı, The American National Standards Institute (ANSI) tarafından ISO 17024 olarak akredite edilmiştir.

Şu ana kadar anlattıklarım genel BT denetimiyle ilgiliydi. Belki de hepimizin daha tanıdık olduğu ve göz önünde olan konu *siber saldırılar*. Bu nedenle siber güvenlik, siber güvenlik uzmanlığı da BT teknolojisi eğitimi alan gençlerimizin ilgisini çok çeken konulardan biri.

Çoğu *beyaz yakalı "hacker"* denilen bu gençler de bu konudaki farkındalıklarının seviyesini çeşitli sertifikalarla ortaya koyuyorlar. Yine ISACA tarafından yürütülen "Cyber Security NExsus" çalışması ve bağlı sertifikasyon programları bu yapının bir parçası.

Sertifika konusunu kapamadan önce vurgulamak istediğim önemli bir konu, sertifikasyon sürecinin sadece teorik bir farkındalıktan ibaret olmadığı, deneyimle desteklenmeyen pratiklerin çok da başarılı olmadığı hususudur. Bu nedenle sertifika almak için sınav geçmek yeterli değildir, bunu deneyimle desteklemeniz gerekir; ancak ondan sonra *sınav geçmiş* değil, *sertifika sahibi* biri olarak çalışabilirsiniz.

Bugün dünya genelinde tarihi 1970'lere dayanan ama yasalara girişi ve gelişmesi göreli yeni bir alt disiplinle sizi tanıştırmaya çalıştım. Umarım bir fikir verebilmişimdir.

Hepinizi saygıyla selamlıyorum.