# BİLGİ SİSTEMLERİ DENETÇİLİĞİ SERTİFİKASI

**Hasan ERKEN, CISA**
İç Denetçi
Hazine Müsteşarlığı

**Said Vakkas BOZKURT**
Hazine Kontrolörü

**Kısa Tarihçe**

Sertifikalı Bilgi Sistemleri Denetçiliği (Certified Information Systems Auditor - CISA) sertifika programı ilk olarak 1978 yılında EDP Auditors Foundation[1] tarafından başlatılmıştır. Bu programın başlatılmasında en önemli etken bilgi sistemlerinin kendine özgü hususiyetleri nedeniyle denetçiler arasında bu sistemlerin denetimine yönelik ayrı bir sertifikasyonun gerekli olduğu düşüncesi olmuştur. İlk Sertifikalı Bilgi Sistemleri Denetçiliği sınavı 1981 yılında iki dilde gerçekleştirilmiştir. Bugün itibariyle 60.000'i aşkın denetçinin bu sertifikayı almış bulunmaktadır. Günümüzde denetçilere yönelik olarak bilgi sistemlerinin denetimi, kontrolü ve güvenliği alanlarında önemli bir standardı sağladığı dünya çapında yaygın bir şekilde kabul edilmektedir. CISA sertifikası sağlamış olduğu prestijin yanı sıra CISA sertifikalı bir denetçi yaklaşık olarak yılda 10.000-15.000 ABD Doları arasında normal bir iç denetçiden daha fazla gelir elde etmektedir.

Proviti firması tarafından 450 iç denetim birimi yöneticisi tarafından yapılan İç Denetçi Yetenekleri ve İhtiyaçları Araştırması sonucunda; iç denetçilerin "bilişim teknolojileri" konusunda iç denetçilerin en az tecrübe ve yeteneğe sahip oldukları ve bu nedenle kendilerini en fazla geliştirmesi gerekli alan olduğu anlaşılmıştır. Ayrıca bilişim teknolojilerinin sürekli değişen bir yapısı olması nedeniyle elde edilen bilgi ve tecrübelerin de sürekli korunması gerektiği vurgulanmıştır.

**Sertifika İçin Aranan Şartlar**

CISA sertifikası alabilmek için gerekli şartlar şunlardır:

1) CISA sınavında başarılı olmak
2) Bilgi sistemleri denetçiliği tecrübesine sahip olmak

1 Information Systems Audit and Control Association (ISACA)

3) Meslek ahlak kurallarına bağlı kalmak
4) Sürekli mesleki eğitim politikasına uymak
5) Bilgi sistemleri denetim standartlarına uymak

**CISA Sınavı**

Yukarıdaki beş şarttan ilki ve en önemlisi CISA sınavında başarılı olmaktır. Bu sınav Haziran ve Aralık aylarında olmak üzere yılda iki kez yapılmaktadır. Sınav başvurusu online olarak http://www.isaca.org/examreg adresinden yapılmaktadır. Başvuru ücreti Information Systems Audit and Control Association (ISACA) üyesi olmayanlar için 525,- ABD Dolarıdır. (ISACA'ya üye olduktan sonra sınava başvuru yapmak toplam maliyeti çok değiştirmemekle birlikte internet üzerinden oldukça fazla kaynağa erişim imkânı sağlaması ve düzenli olarak IS Control dergisinin gönderilmesi nedeniyle daha avantajlı olmaktadır.) Sınav yeri ve zamanına ilişkin bilgiler hem normal posta hem de e-posta aracılığıyla gönderilmektedir.

Sınav 200 adet test sorusu içermekte olup bu soruların 4 saat sürelik bir oturum içerisinde cevaplandırılması istenmektedir. Sınav Türkiye'de İngilizce olarak İstanbul'da yapılmaktadır. Bu sınavın amacı adayların bilgi sistemleri denetimi kapsamında yer alan 6 ana konuya ilişkin teorik ve pratik bilgilerini test etmektir. Bu ana konular ve ağırlıkları şunlardır:

1) Bilgi Sistemleri Denetimi Süreci (%10)
2) Bilgi Teknolojileri Yönetimi (%15)
3) Sistem ve Altyapı Yaşam Döngüsü (%16)
4) Bilgi Teknolojileri Hizmet Sunumu ve Destek (%14)
5) Bilgi Varlıklarının Korunması (%31)
6) İş Sürekliliği ve Felaket Kurtarma (%14)

Bu sınavın ana konusunu bilgi teknolojileri oluşturması nedeniyle sınava girecek adayların bu alanda yeterli seviye de bilgi sahibi olması beklenmektedir. Özellikle BT altyapısı, donanımlar, işletim sistemleri, yazılım geliştirme, ağ yapıları, veri tabanı yönetimi, bilgi güvenliği gibi alanlarda temel kavram ve konuları özümsemiş olması sınavdaki başarısını doğrudan etkilemektedir. Yukarıdan da anlaşılacağı üzere sınavın en önemli bölümü bilgi varlıkların korunması bölümüdür. Ayrıca özellikle teknik bölümlerden mezun olmayanların en çok zorlandıkları bölümdür. Bu nedenle özellikle bu bölümde anlaşılmayan konuların ek materyallerle desteklenmesi sınavdaki başarıyı arttırmaktadır.

**Sınava İlişkin Materyaller**

Doğrudan sınava yönelik Türkçe herhangi bir kaynak bulunmamaktadır. Sınava yönelik temel kaynaklar şunlardır:

- CISA Review Manual 2008
- Certified Informations Systems Auditor Study Guide
- Exam Cram 2 – CISA
- Exam Prep – CISA
- The CISA Prep Guide
- CBT Nuggets CISA Certification Package
- CISA Review Questions, Answers & Explanations Manual 2009
- CISA Practice Question Database v8

Bunların dışında CISA sınavının içeriğini oluşturan 6 ana konuyu ele alan oldukça fazla sayıda kitap bulunmaktadır.

CISA sınavına yönelik en önemli kaynak **CISA Review Manual'dir**. CISA Review Manual (CRM), yukarıda değinilen 6 ana konunun her biri için çeşitli görevler (tasks) ve bilgi açıklamaları (knowledge statement) belirlemiştir.

Görevler denetçiye denetiminde yapması gerekli olduğu faaliyeti ve amacını belirlerken bilgi açıklamaları bu görevin yerine getirilebilmesi için denetçinin bilgi sahibi olması gerektiği konuları işaret etmektedir.

Bu ana çerçeve içerisinde her bir konu ele alınmaktadır. Ancak CRM'nin asıl amacının bu konuları denetçi perspektifinde değerlendirmek olduğu ve BT konularına ilişkin teknik kavramları öğretmek olmadığı unutulmamalıdır. Sınava girecek kişilerin eksiklik hissettiği CRM'den anlayamadığı konuları mutlaka destekleyici materyallerden araştırıp öğrenmesi gerekmektedir.
Bu anlamda internet üzerinden oldukça fazla kaynak bulabilirsiniz. Ancak konuların ne kadar derinlikte öğrenilmesi gerektiği sürekli akılda tutulmalıdır. Aksi halde enerjinizin çoğunu ayrıntılarda kaybetmeniz söz konusudur. Bu doğrultuda özellikle www.hows-

tuffworks.com sitesinde yer alan içerikler çoğu konu için yeterli olmaktadır.

**Sınava Yönelik Öneriler**

- CISA sınavına girme kararını mümkün olduğunca erken vermek çok önemlidir. Bu karar ücretinin hem daha düşük sınav ücreti ödemeyi sağladığı gibi sınava hazırlanmak için daha uzun bir süre ayırmanız mümkün olacaktır.
- ISACA web sitesinde bulunan "CISA Exam Bulletin of Information" ve Candidates guide to CISA exam" dokümanları incelenmelidir. (http://www.isaca.org/cisa)
- CISA Review Manual temel doküman olarak kabul edilmeli, çok iyi çalışılmalı ve gerektiğinde daha ayrıntılı ve belirli bir konuya özgü diğer materyaller ile desteklenmelidir.
- Sınava hazırlık açısından CISA Review Questions, Answers & Explanations Manual 2009 ve CISA Practice Question Database v8'den örnek soruların çözülmesi oldukça faydalı olacaktır.
- Soruların belirli bir teknoloji veya platforma özgü olarak gelmediği hatırda tutulmalıdır.
- COBIT v. 4.1, ISO 27001 ve ITIL v.3 dokümanlarının okunması faydalı olacaktır.
- BT konularının çok geniş bir alanı içermesi nedeniyle sınava yönelik öncelikli konularınız çok iyi belirlenmeli ve zaman planına bağlanmalıdır.
- Sınav soruları arasında salt bilgiye dayalı sorular olduğu gibi belirli bir değerlendirme yapılmasını gerektiren sorular da bulunmaktadır. Birçok soruda "en yakın cevap hangisi", "en doğru hangisi" gibi ifadeler yer aldığından bu soruları çözebilmek için konuların özümsenmiş olması gerekmektedir.
- Soruların basit olmasına özen gösterildiği unutulmamalıdır. Adayı yanıltmaya, dikkatini ölçmeye veya gizli bir ifadeyi fark etmesine yönelik sorular bulunmamaktadır.
- Sınav 200 sorudan oluşmaktadır ve Türkiye'de İngilizce olarak İstanbul'da yapılmaktadır. Sorular, yukarıda belirtilmiş olan konu başlıkları itibariyle sınav kitapçığında yer almamaktadır. Sınav soruları gelişigüzel dağıtılmış bulunmaktadır. Sınav tek bir 4 saat
- Sınav sonuçları 200 – 800 puan arasında değerlendirilmektedir. Sınavda başarılı olabilmek için en az 450 puan alınması gerekmektedir. Bu puan için gerekli olan doğru sayısı CISA Sertikasyon Kurulu tarafından belirlenmektedir.
- Sınav yerinin fiziki imkânlarının yetersiz olabileceği durumuna hazırlıklı olarak gelinmesinde fayda var. Genellikle kolçaklı sıralar ile karşılaşılması muhtemeldir.
- Yanlışların doğruları götürmesi gibi bir durum olmadığından doğru olduğuna inanılan en yakın seçenek mutlaka işaretlenmelidir.
- Sınava giderken başvuru yazısı, kimlik kartı, kurşun kalem ve silgi mutlaka adayın yanında olmalıdır.

**Sınav Sonrasında Yapılması Gerekenler**

Sınavda başarılı olan adaylardan sertifika başvuru belgesini doldurması istenmektedir. Bu belgede denetim tecrübenize ve eğitim durumunuza ilişkin bilgiler istenmektedir. CISA sertifikası alabilmek için en az 5 yıllık bilgi teknolojileri denetim tecrübesi gerekmektedir. Bununla ilgili olarak sertifika başvuru belgesinde CISA Review Manuel'de belirtilmiş olan her bir görevde çalışıp çalışmadığı işaretlenmektedir. Sınavda başarılı olan adayların geçmiş tecrübesi yoksa sınav sonrasındaki 10 yıl içerisinde bu tecrübe şartını yerine getirmesi halinde ilgili adaya sertifika verilebilmektedir. Belirli alanlarda yapılan lisans eğitimi, denetim ve akademik çalışmalar bu beş yıl içerisinde değerlendirilebilmektedir.

Sertifika başvuru belgesinin belli kısımları birim başkanı / işveren tarafından doldurulmaktadır. Burada söz konusu tecrübeye sahip olduğunuza yönelik teyit yapılmaktadır. Bu belgede ayrıca meslek ahlak kurallarına ve denetim standartlarına uygun görev yapacağınıza dair beyan verilmektedir.

Bu başvuru formuyla birlikte tecrübe bilgilerini destekleyici belgeler ISACA'ya gönderilmektedir. CISA Sertifikasyon Kurulu tarafından yapılan değerlendirmeler sonucunda uygun görülmeniz halinde CISA sertifikası ilgiliye gönderilmektedir.

**Sertifika Sonrası Yapılması Gerekenler**

Sertifika verildikten sonra sertifikanın güncel tutulabilmesi için 3 yılda 120 sürekli eğitim puanı top-

lanması gerekmektedir. Bu puanlar katılım sağlanan eğitim ve konferanslardan elde edilebildiği gibi ISACA tarafından yürütülen çeşitli proje, çalıştay vb. faaliyetlere katılmak suretiyle de toplanabilmektedir. Sürekli eğitim puanı alma zorunluluğu sertifikanın alındığı yıl için geçerli değildir. Örneğin 2006 Haziranında alınmış bir sertifika için 2007, 2008 ve 2009 yılları için 120 puanı toplamanız gerekmektedir. Bu şekilde 3'er yıllık periyotlar halinde devam etmektedir.

Sertifikanın güncel tutulması için gerekli diğer bir şartta yıllık olarak 40,- ABD Doları tutarındaki sertifika ücretini ödemeniz gerekmektedir. Ayrıca ISACA üyeliğinizin de devam etmesi için 130,- ABD Doları üyelik ücretini de ödemeniz gerekmektedir.

" Gerek dünyada gerekse ülkemizde denetim alanında eksikliği önemli bir şekilde hissedilen BT denetçiliği konusunda denetim elemanlarının kendilerini geliştirmeleri büyük önem arz etmektedir. Bu açıdan temel bilgi ve tecrübe seviyesinin bulunduğunu tescil anlamına gelen Bilgi Sistemleri Denetçiliği Sertifikasının alınmasının bu alandaki eksikliğin doldurulması açısından önemli bir başlangıç noktası olduğu rahatlıkla söylenebilir. "

**Sonuç**

Gerek dünyada gerekse ülkemizde denetim alanında eksikliği önemli bir şekilde hissedilen BT denetçiliği konusunda denetim elemanlarının kendilerini geliştirmeleri büyük önem arz etmektedir. Bu açıdan temel bilgi ve tecrübe seviyesinin bulunduğunu tescil anlamına gelen Bilgi Sistemleri Denetçiliği Sertifikasının alınmasının bu alandaki eksikliğin doldurulması açısından önemli bir başlangıç noktası olduğu rahatlıkla söylenebilir. Ancak bu sınava girecek meslektaşlarımızın hem sınavın özellikle teknik bölümlerden mezun olmamış kişiler için bir ölçüde zor olduğunu hem de ciddi bir maliyetinin olduğunu baştan bilmeleri yerinde olacaktır. Henüz bu zorluk ve maliyetlerin üstlenilmesini teşvik eden bir sistemin kamu sektörü açısından bulunmadığı da dikkate alındığında yakın dönemde BT denetçi açığının kapanmasının mümkün olmadığı aşikârdır.

**KAYNAKLAR**

1. A. Rafeq, Shirish S. Deshpande, "Effective Approach and Practical Tips For CISA Exam".
2. "IT Audit Skills Found Lacking", Internal Auditor June 2007.