**Bütünlük Politeikası**

* Bütünlük politikaları, **bütünlüğün sağlanmasına** odaklanmalıdır.

**Amaç**

**Lipner** tarafından tanımlanan gereksinimeler

1. Kullanıcılar kendi programlarına yazamalar, ancak mevcut üretim porgramlarına ve veritabanlarını kullanmalıdır.
2. Programcılar, programlarının geliştirimini ve testini üretimin olmadığı bir sistemde gerçekleştirmeldiri. **(Test Ortamında Üretim Olmalıdır)**

* Veriye erişmek istiyrolarsa, very programcılara özel süreçler yardımı ile verilmelidir. Ancak, programcılar bu veriyi kendi geliştirme sistemlerinde kullanmalıdır.

1. Programlar, geliştirme ortamından üretim sistemine yüklenirken özel süreçler takip edilmelidir **(bizim deyimimizle canlıya atılırken)**
2. 3. Adımda özel süreç control edilmeli ve denetlenmelidir. **(Auditing)**
3. Yöneticiler ve denetleyiciler (auditor), oluşturulan system durumuna **(state)** ve günlüklerine **(logs)** erişim yetkilerine sahip olmalıdır.

Bu gereksinimler çeşitli işlem prensiplerini ortaya çıkarmaktadır:

* Görev Ayrılığı **(Seperation of Duty)**
* Işlev Ayrılığı **(Seperation of Function)**
* Denetleme **(Auditing)**

**Görev Ayrılığı (Seperation of Duty)**

Bir işlemi gerçekleştirmek için iki ya da daha fazla adıma ihtiyaç varsa, **en az iki farklı kişi** adımları gerçekleştirmelidir.

Program geliştirilirken;

-Uygulama programıcısı geçersiz bir varsayım **(assumption)** yaptığında

-> Programın yüklenmesi farklı bir kişi tarafından yapıldığında, **hatanın yakalanması ihtimali** data fazladır.

**İşlev Ayrılığı (Speration of Function)**

Uygulama Geliştiriciler;

* Üretim verisini bozmamak için yeni programları üretim sistemlerinde geliştirmemektedir.
* Üretim verisi, geliştirme sisteminde de kullanılmamaktadır.

Verinin duyarlılığına bağlı olarak, uygulama geliştiriciler ve test işlemlerini gerçekleştirenler “**sanitized**” üretim verisi kullanmaktadır.

**Not:** Geliştirme ortamı, mevcut üretim ortamı ile mümkün olduğunda benzer olmalıdır.

**Denetleme (Auditing)**

* Denetleme, **hangi eylemlerin** gerçekleştirildiğini ve bu eylemlerin **kimler tarafından** gerçekleştirildiğini belirlemek için sistemin analiz edilmesi sürecidir.
* Denetlemenin temeli günlüklerdir (logs)
* Programlar, geliştirme sisteminden üretim sistemine taşınırken, günlükler ve denetleme önem kazanmaktadır.

**Biba Modeli**

Yüksek bütünlük seviyesindeki veri, alt bütünlük seviyesinde ki veriden daha güvenilirdir (trustworthy).

**No Read Down** – s<0 ise Özne nesneyi okuyabilir. Yani özne, kendi bütünlük seviyesinden daha alt bir bütünlük seviyesine sahip olan bir nesneyi okuyamaz. (Simple Integrity Axiom)  
**No Wirte Up** - 0<s ise s Özne nesneyi yazabilir. Özne, kendi bütünlük seviyesinden daha yukarı da bir bütünlük seviyesine sahip olan nesneye yazamaz. (\*Star Integirty Axiom)  
S2 <= s1 ise s1, s2 yi yürütebilir.



**Clark-Wilson Modeli**

İşlemler sonucunda tutarlılık (consistency) koşulları sağlanmalıdır. **Amaç ticari ortamda ki verinin bütünlüğü ve veri üzerinde gerçekleştirilen işlemlerin bütünlüğü**

1. **Kısıtlandırılmış Veri Öğeleri** (Constrained Data Items) **CDI – Bütünlük Kontrollerine Maruz Kalır**
2. **Kısıtlandırılmamış Veri Öğleri** (Unconstrained Data Items) **UDI – Bütünlük Kontrollerine Maruz Kalmaz**

Bütünlük Dooğrulama – Integrity Verification Procedure – **IVP**

Değişim Yordamı – Transformation Procedure – **TP**

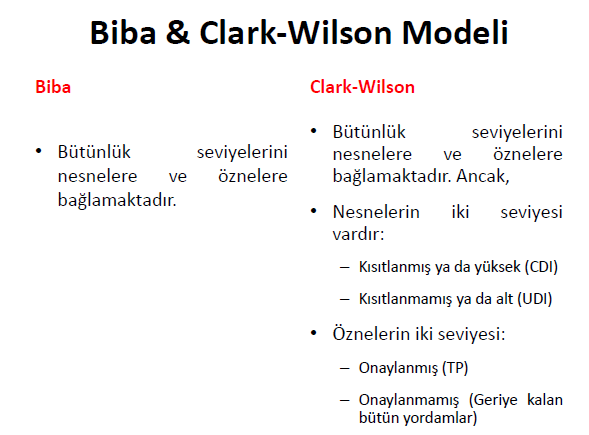
Model , **9 adet** kural kümelerinden oluşur;

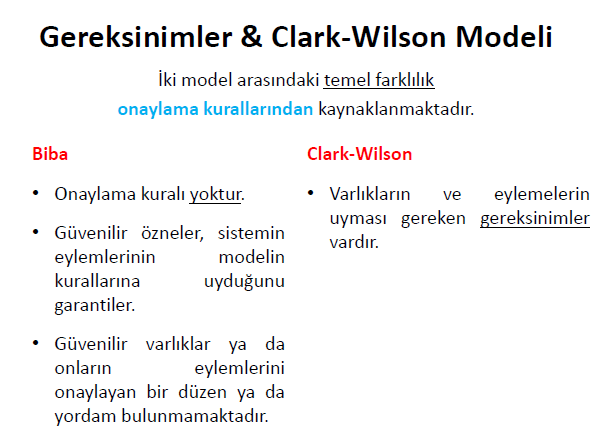
* **Onaylama Kuralları** (Certification Rules, CR) \*5 Adet
* **Uygulama Kuralları** (Enforcement Rules, ER) \*4 Adet

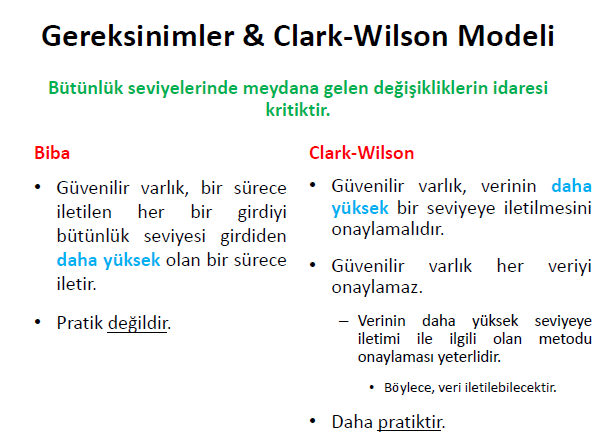
**CR1:** Herhangi bir IVP çalıştığında CDI’ların geçerli bir durumda olduğu garantilenmelidir.  
CR2: TP, birbiri ile ilgili bazı CDI kümeleri için bu CDI’ları bir gerçerli durumdan başka bir geçerli duruma dönüştürmelidir.  
ER1: Sistem onaylanmış ilişkilerin sürekliliğini sağlamalı ve sadece onaylanmış TP’lerin CDI üzerinde değişiklik yapabileceğini garantilemelidir.  
ER2: Sistem, her bir TP ve CDI kümesi ile ilgili bir kullanıcıyı ilişkilendirmelidir. TP, ilişkilendirilmiş kullanıcının yerine, CDI’lara erişebilir.  
CR3: İzin verilen ilişkiler, görev ayrılığı prensibi gereksinimlerini karşılamalıdır.  
ER3: Sistem, TP’ye erişmek istiyen her kullacının kimliğini doğrulamalıdır  
CR4: Bütün TP’ler, işlemle ilgili yeterli blgiyi günlüğe eklemelidir.  
CR5: Herhangi bir TP, bir UDI’yı girdi olarak alıp, UDI’nın bütün geçerli değerleri için sadece **geçerli dönüşümleri/değişimleri gerçekleştirir** ya da **hiçbir dönüşüm/değişim gerçekleştirmez.**  
ER4: ER2 ve ER3’deki ilişkilerin bütünlüğünün sağlanması için görev ayrımını uygular.

**Gereksinimler**

**G1:** Kullanıcılar kendi programlarına yazamazlar ancak mevcut üretim programlarını ve veritabanlarını kullanmalıdır  
**G2:**Programcılar, programlarının geliştirimini ve testini üretimin olmadığı bir sistemde gerçekleşirmelidir. **G3:**Programlar, geliştirme ortamından üretim sistemine yüklenirken özel süreçler takip edilmelidir. **G4:**3. Adımda ki özel süreçler kontrol edilmeli ve denetlenmelidir.







**Chines Wall (CW) Modeli**

Bütünlük ve gizlilik ile eşit olarak ilgilenen bir güvenlik modelidir. İşletmelerde meydana gelen çıkar çatışmasına yönelik politikaları tanımlar.

