Das **Biba-Modell** ist ein Zugriffskontrollmodell in der Informationssicherheit, das sich auf die Integrität von Daten konzentriert. Es wurde in den 1970er Jahren von Kenneth J. Biba entwickelt und ist nach ihm benannt. Das Biba-Modell basiert auf der Idee, dass die Integrität von Daten genauso wichtig ist wie die Vertraulichkeit.

Die Grundprinzipien des Biba-Modells sind:

- **Integritätsvertraulichkeit**: Es darf keine Modifikation von Daten durch Benutzer erfolgen, die über niedrigere Integritätsstufen verfügen als die Daten selbst. Dies bedeutet, dass Daten nur von Benutzern mit gleichwertiger oder höherer Integritätsstufe geändert werden können.
- **Integritätsunveränderlichkeit**: Ein Benutzer mit hoher Integritätsstufe darf nicht von Daten geändert werden, die von einem Benutzer mit niedrigerer Integritätsstufe erstellt wurden. Dies verhindert, dass Benutzer mit niedrigeren Integritätsstufen die Integrität von Daten gefährden, die von vertrauenswürdigen Quellen stammen.
- Das Biba-Modell definiert drei Integritätsstufen für Daten und Benutzer:
- **Hohe Integrität (H)**: Benutzer mit hoher Integritätsstufe haben die Berechtigung, Daten mit hoher Integrität zu erstellen oder zu ändern. Diese Benutzer werden als vertrauenswürdig angesehen und ihre Aktionen werden als verlässlich betrachtet.
- **Mittlere Integrität (M)**: Benutzer mit mittlerer Integritätsstufe haben eingeschränkte Berechtigungen und dürfen keine Daten mit höherer Integrität ändern. Ihr Hauptzweck besteht darin, Daten mit niedrigerer Integrität zu erstellen oder zu ändern.
- **Niedrige Integrität (L)**: Benutzer mit niedriger Integritätsstufe haben die geringsten Berechtigungen und dürfen keine Daten mit höherer oder mittlerer Integrität ändern. Sie können jedoch auf Daten mit gleicher oder niedrigerer Integrität zugreifen und diese ändern.

Das Biba-Modell soll sicherstellen, dass die Integrität von Daten in einem System gewahrt bleibt und nicht durch unbefugte oder fehlerhafte Änderungen gefährdet wird. Es ist besonders nützlich in Umgebungen, in denen die Integrität von Daten von entscheidender Bedeutung ist, wie beispielsweise in kritischen Infrastrukturen, Finanzsystemen oder medizinischen Einrichtungen.

Das **Clark-Wilson-Modell** ist ein Sicherheitsmodell in der Informationssicherheit, das sich auf die Gewährleistung der Integrität von Daten konzentriert. Es wurde von David D. Clark und David Wilson in den 1980er Jahren entwickelt und ist nach ihnen benannt. Das Clark-Wilson-Modell legt Wert darauf, dass Daten korrekt und zuverlässig sind, unabhängig davon, wer auf sie zugreift oder sie manipuliert.

Die Grundprinzipien des Clark-Wilson-Modells sind:

- **Well-Formed Transactions (WFT)**: Das Modell verwendet gut geformte Transaktionen, um sicherzustellen, dass Daten nur auf legale Weise modifiziert werden können. Jede Transaktion muss bestimmte Integritätsregeln einhalten, um als gültig betrachtet zu werden. Dies schützt vor inkorrekten oder unsachgemäßen Änderungen an den Daten.
- **Separation of Duties (SoD)**: Das Modell basiert auf dem Prinzip der Aufgabentrennung, bei dem verschiedene Personen oder Prozesse für unterschiedliche Aspekte der Datenverwaltung verantwortlich sind. Dadurch wird sichergestellt, dass keine Einzelperson oder Entität die Kontrolle über alle Aspekte eines Systems hat, was das Risiko von Fehlverhalten oder Missbrauch verringert.

- **Certification and Enforcement of Constraints (CEC)**: Das Modell verwendet Zertifizierungsmechanismen und Durchsetzungsmechanismen, um sicherzustellen, dass die Integritätsregeln eingehalten werden. Daten werden in einem bestimmten Zustand zertifiziert, und alle Änderungen müssen die vorgegebenen Integritätsregeln erfüllen, um gültig zu sein.
- Das Clark-Wilson-Modell verwendet auch Konzepte wie Zugriffskontrolllisten (ACLs) und Trusted Subjects, um den Zugriff auf Daten zu kontrollieren und sicherzustellen, dass nur autorisierte Benutzer Änderungen vornehmen können. Es ist besonders nützlich in Umgebungen, in denen die Integrität von Daten von entscheidender Bedeutung ist, wie beispielsweise in Regierungsbehörden, Finanzinstitutionen oder Gesundheitseinrichtungen.

Die "**Chinesische Mauer**" (auch bekannt als "Chinese Wall") ist ein Sicherheitsmodell in der Informationssicherheit, das dazu dient, Interessenkonflikte zu verhindern, indem es den Zugriff auf sensible Informationen in bestimmten geschäftlichen Situationen beschränkt. Das Konzept wurde erstmals von Brewer und Nash im Jahr 1989 vorgeschlagen.
Die Chinesische Mauer besteht aus einer Reihe von Regeln, die den Zugriff auf Informationen basierend auf den aktuellen Aktivitäten einer Person kontrollieren. Diese Regeln dienen dazu, sicherzustellen, dass Personen, die in sensiblen Geschäftsbereichen tätig sind, nicht unbefugt auf vertrauliche Informationen zugreifen können, die einen Interessenkonflikt darstellen könnten.

Die Grundprinzipien der Chinesischen Mauer sind:

- **Abtrennung von Sektoren**: Das Modell definiert verschiedene Sektoren oder Kategorien von Informationen basierend auf den Interessen der Geschäftsbereiche. Jeder Sektor enthält sensible Informationen, die für eine bestimmte Gruppe von Personen relevant sind.
- **Interessenkonflikte**: Personen, die in einem Sektor arbeiten, dürfen nicht auf Informationen aus anderen Sektoren zugreifen, die potenzielle Interessenkonflikte darstellen könnten. Dies dient dazu, den Austausch sensibler Informationen zwischen konkurrierenden Geschäftsbereichen zu verhindern.
- **Dynamische Zugriffssteuerung**: Die Regeln der Chinesischen Mauer werden dynamisch angepasst, basierend auf den aktuellen Aktivitäten einer Person. Wenn beispielsweise eine Person an einem Projekt arbeitet, das einen Interessenkonflikt mit einem anderen Projekt hat, wird ihr der Zugriff auf Informationen aus diesem anderen Projekt verweigert.

Das Modell der Chinesischen Mauer wird oft in regulierten Branchen wie Finanzdienstleistungen und Rechtswesen eingesetzt, um sicherzustellen, dass sensible Informationen vor potenziellen Interessenkonflikten geschützt sind. Es hilft auch dabei, Compliance-Anforderungen zu erfüllen und das Risiko von Insider-Bedrohungen zu minimieren.