Bilgi Teknolojileri Yönetişim ve Denetim Konferansı

BTYD 2010

ISACA
Serving IT Governance Professionals

Türkiye Bilişim Derneği 1971

Türkiye İç Denetim Enstitüsü 1995

eDem
TODAİE
eDevlet Merkezi

Etkin BT Yönetişimi ve Uyum

Esra Gönenli Yalçın, CISA, CISM
FİNANSBANK - IBTECH

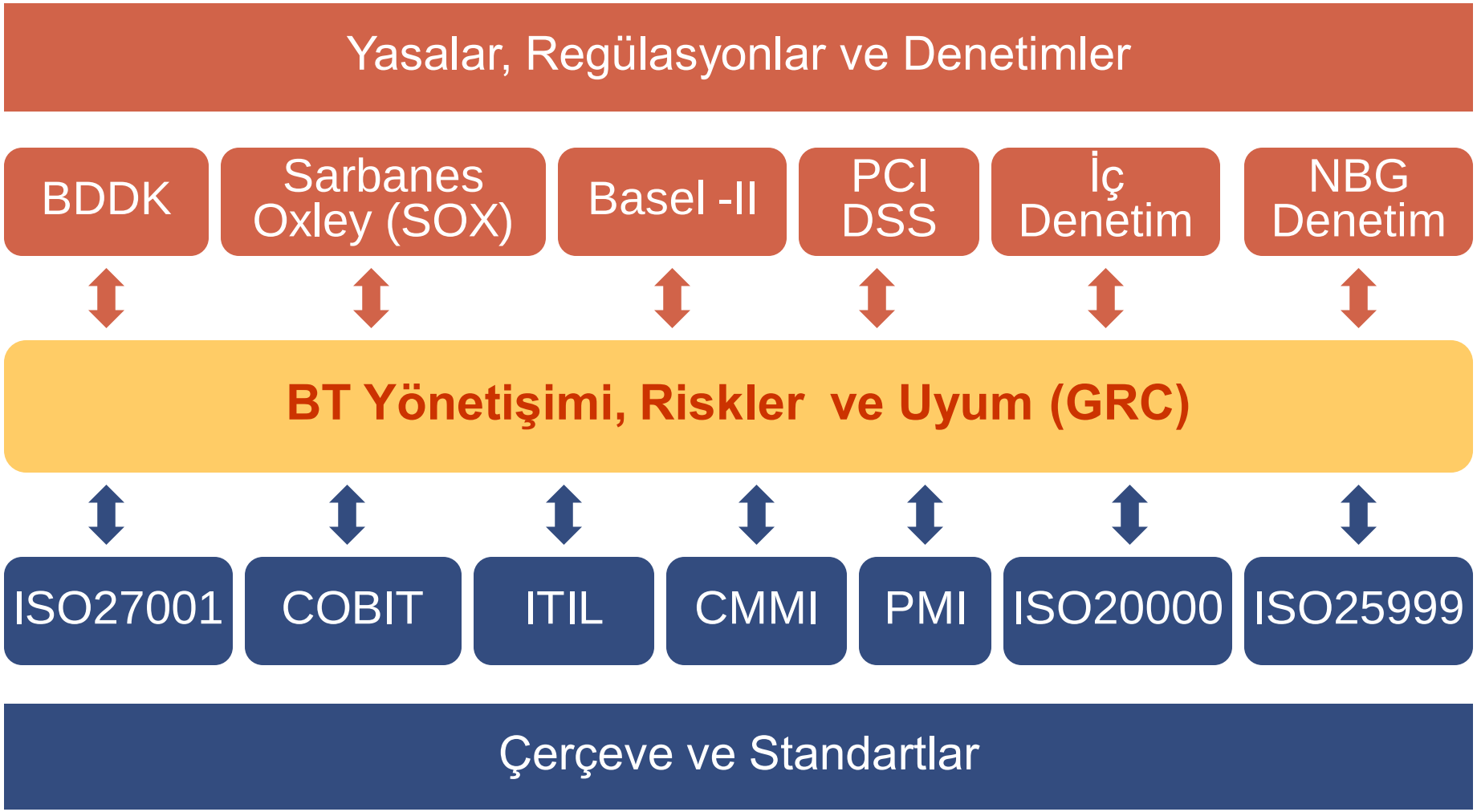
Gündem

- IBTECH Hakkında
- Finansbank – IBTECH Uyum İhtiyaçları
- BT Yönetişimi ve Uyumun Getirdikleri
- Finansbank – IBTECH Yönetişim ve Uyum Modeli
- IBTECH Süreç Modeli ve Süreçlerin Yönetimi
- BT Risklerinin Yönetimi
- Projelerde Güvenlik, Risk ve Uyum Yönetimi
- BT İç Kontrol Uyum Çalışmaları ve Yönetim Beyanı
- BT Denetim Süreçleri
- Performans İzleme ve Ölçme
- Sorularınız

IBTECH Hakkında

- IBTech, NBG Grup şirketlerinden Finansbank'ın bir iştirakidir.
- Finansbank, FEHAŞ, FinansLeasing, FinansInvest, FinansPortföy, FinansFactoring , NBG ve NBG Malta'ya Bilgi Teknolojileri Hizmetleri veriyor.
- Personel olarak 500 kişi çalşıyor.
- Uzmanlık Alanları ve Verilen Hizmetler:
  - Uygulama Yazılım Geliştirme ve Veri Mimari (Temel Bankacılık (Core Finans), Kredi Kartları, İnternet Bankacılığı, Call Center)
  - Altyapı Yönetimi (Enterprise Systems, Database, Distributed Systems, Network, Security, Application Infrastructure)
  - Proje Yönetimi ve İş Analizi
  - BT Hizmet Yönetimi ve Servis Sürekliliği
  - BT Operasyonlarının yürütülmesi ve 7 X24 Destek Hizmetleri
  - BT Güvenlik, Risk, Denetim ve Uyum

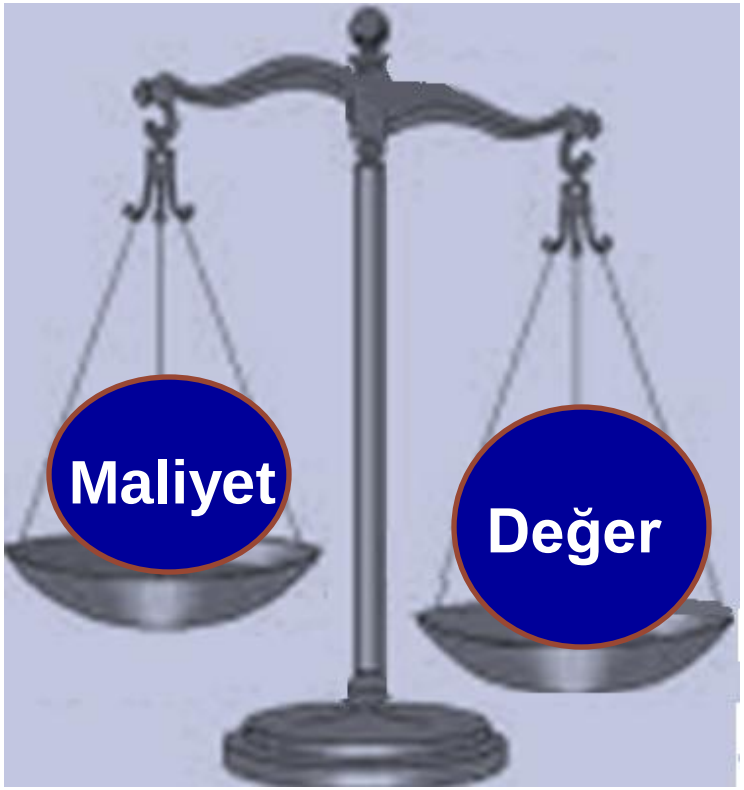
Finansbank – IBTech Uyum İhtiyaçları



BT Yönetişimi ve Uyumun Getirdikleri

İş ve BT Stratejilerinin Uyumluluğu

- Farklı regülasyonlar, çerçeve ve standartlardan gelen uyum ihtiyaçlarını karşılayabilme
- Güvenlik, Denetim, Uyum ve Risk Yönetim çalışmalarının
  - Maliyetlerini azaltma
  - Etkinliğini artırma
- BT Süreçlerinin kurumsallaşması ve olgunlaşmasını sağlama

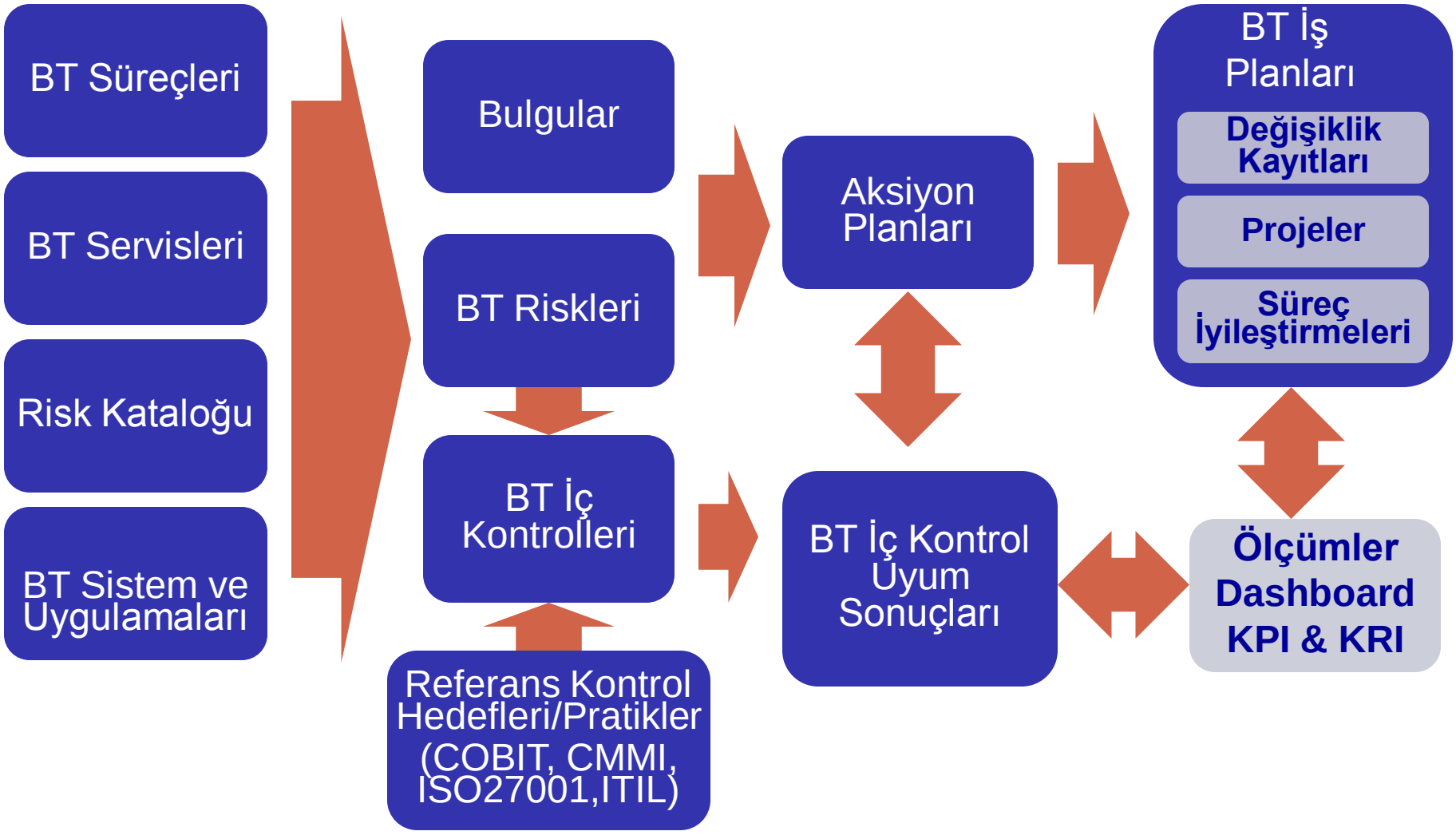


- İş Strateji ve İhtiyaçları doğrultusunda Esnek ve Hızlı Çözümler üretmeyi sağlayan BT Süreçleri
- Verilen BT Hizmet kalitesini sürekli iyileştirme
- Risklerin ve Güvenlik Tehditlerinin EtkinYönetimi
- Kaynakların Etkin Kullanımı
- Müşteri ve Paydaşların Memnuniyeti ve Güvenini sağlama

Performans Ölçüm ve İzleme

BT Yönetişim ve Uyum Modeli

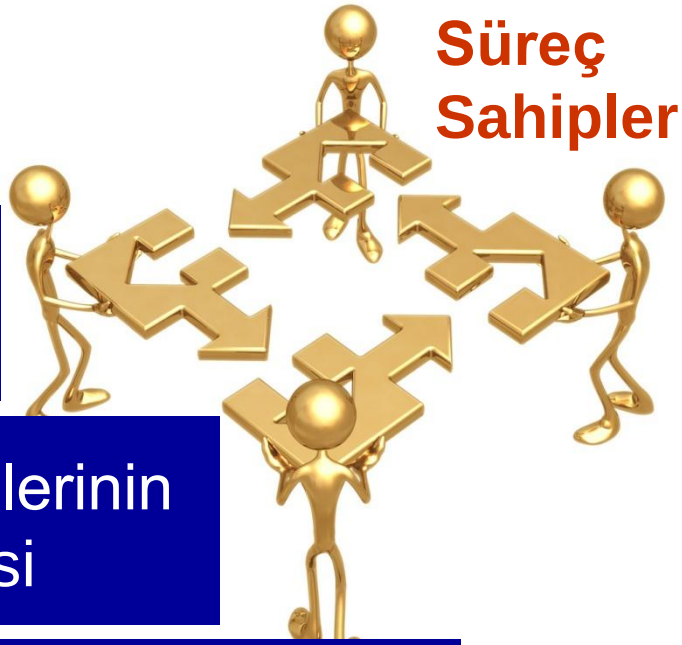
Ibtech Yönetişim ve Uyum Modeli



Ibtech Süreç Modeli ve Süreçlerin Yönetimi

Süreçlerin Modellenmesi ve Tanımlanması

ARIS



Süreç Sahipleri

Kurumsal Doküman Kütüphanesi

Süreç Risklerinin Belirlenmesi

Politikalar, Süreçler ve Prosedürler

Süreç İç Kontrollerinin Belirlenmesi

Süreç Performans Metriklerinin (KPI) Belirlenmesi

Kurumsal Ölçüm Veri Ambarı

Sürekli İyileştirilen ve Değer Katan Süreçler

Enterprise Process Map

Management Processes

- Governance
- Strategy Management
- Risk Management
- Information Architecture
- Internal Audit
- Internal Control
- Compliance Management

Core Processes

Development

- Infrastructure Design & Development
- Software Development
  - Requirements Development &...
  - Technical Solution
  - Product Integration
  - Review
  - Test Management
  - Decision Analysis & Resolution
  - Software Configuration & Change Mng

Service Management

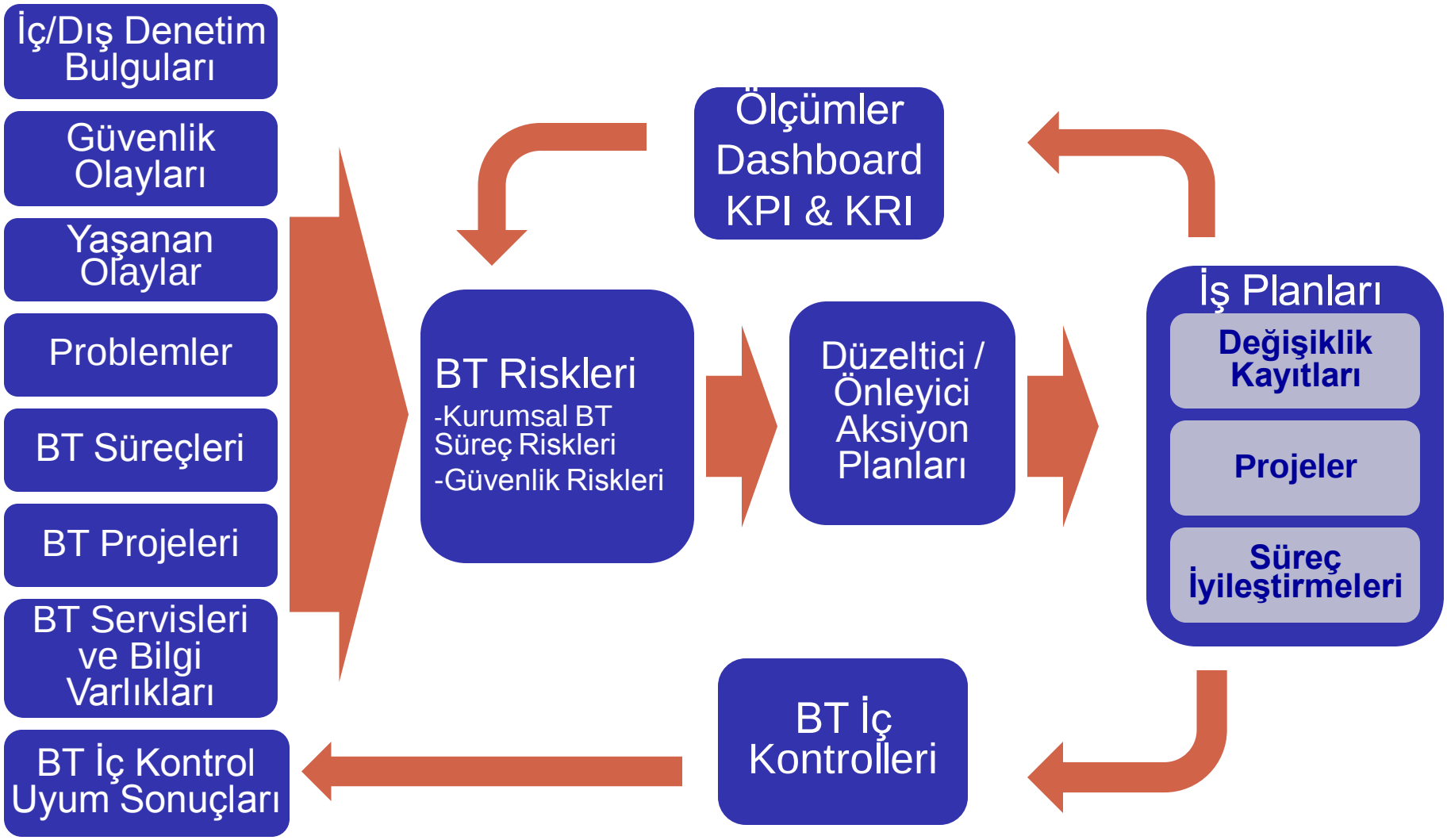
- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Service Improvement

Project Management

Support Processes

- Human Resources
- Supplier Management
- Process Management
- Quality Assurance
- Corporate Financial Managemen...
- Measurement Analysis
- Security Management

Ibtech Risk Yönetimi



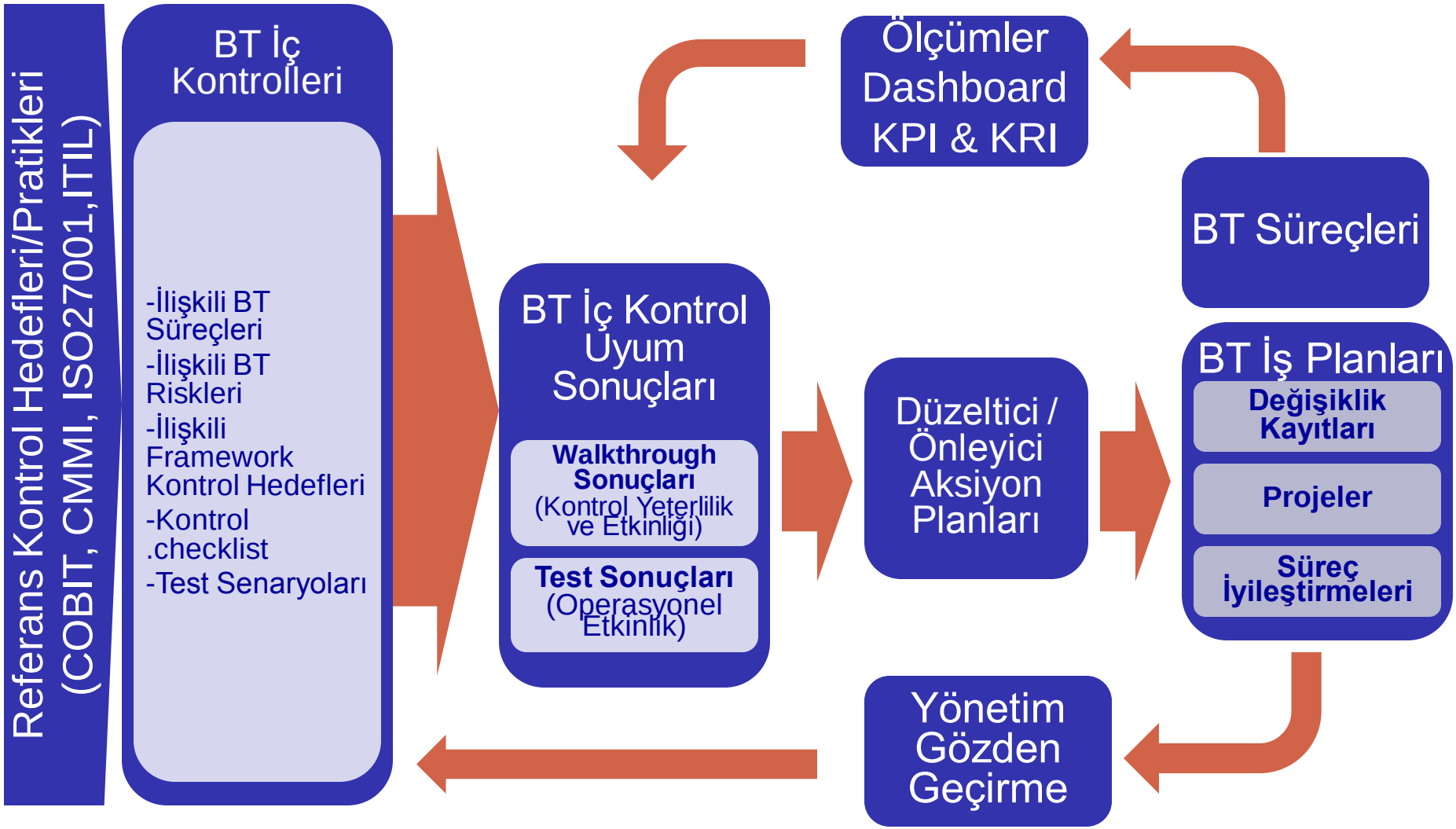
Ibtech Risk Yönetim Süreci

- Risklerin NBG ve Finansbank Operasyonel Risk yönetimine paralel yönetilmektedir.
- Riskler belirlenmesinde bulgular, problemler, yaşanan olaylar ve risk izleme sürecinden gelen riskler (projeler, süreçler, servisler) dikkate alınır.
- Her bir risk değerlendirilir.
- Önem derecesi orta ve yüksek olan riskler için aksiyon planları belirlenir.
- Risk aksiyon planının uygulanması için risk sorumlusu atanır.
- Önem derecesi yüksek olan riskleri indirgemek için aksiyon planı uygulanır.
- Gerektikçe ve belirli dönemlerde riskler gözden geçirilerek güncellenir.
- Riskler periyodik olarak Üst Yönetim, Finansbank Operasyonel Risk Yönetimi ve NBG ile paylaşılır.

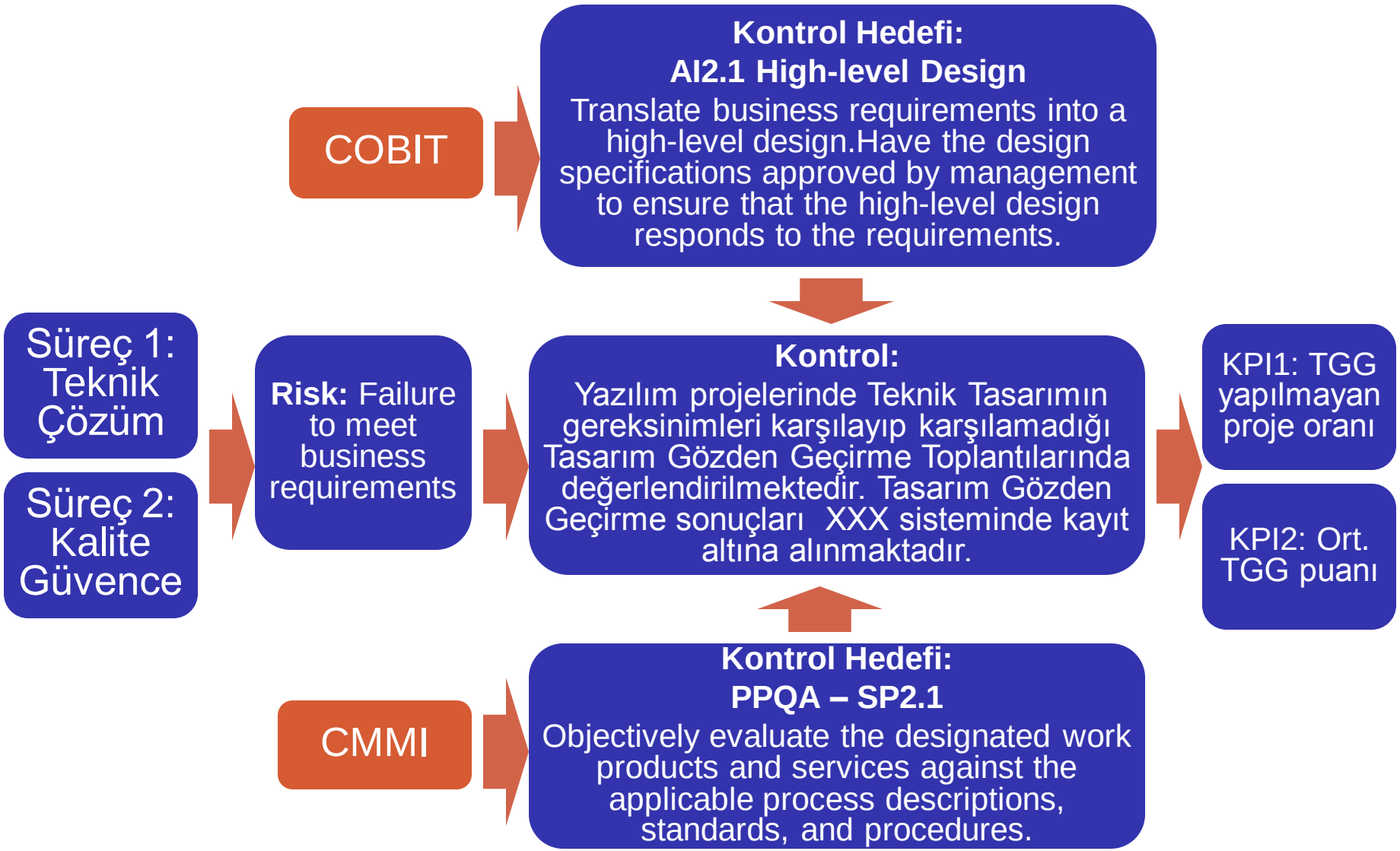
Projelerde Güvenlik, Risk ve Uyum Yönetimi

- BT'ye gelen Stratejik İş İhtiyaçları ve BT Yatırımları proje olarak yönetilmektedir.
- Tüm BT Projeleri proje ekibi tarafından "Güvenlik, Risk ve Uyum Etki" Formu ile değerlendirilir. İhtiyaç varsa:
  - Projeye Güvenlik, Risk ve Uyum'dan sorumlu kaynak atanır.
  - Projeyle ilgili güvenlik ve uyum gereksinimleri ve ilişkili riskleri azaltmak için alınması gereken aksiyonlar belirlenir, maliyetlendirilir ve önceliklendirilir.
  - Proje tamamlanmadan belirlenen güvenlik ve uyum gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.
  - Gerekiyorsa sızma testleri ve güvenlik testleri uygulanır.
  - Karşılanmayan güvenlik ve uyum gereksinimleri "Risk Yaklaşımı" ile değerlendirilir (Accept, Avoid, Mitigate,Transfer) ve proje hayata geçtikten sonra "BT Riski" olarak yönetilerek ve izlenir.

Ibtech İç Kontrol Uyum Çalışmaları



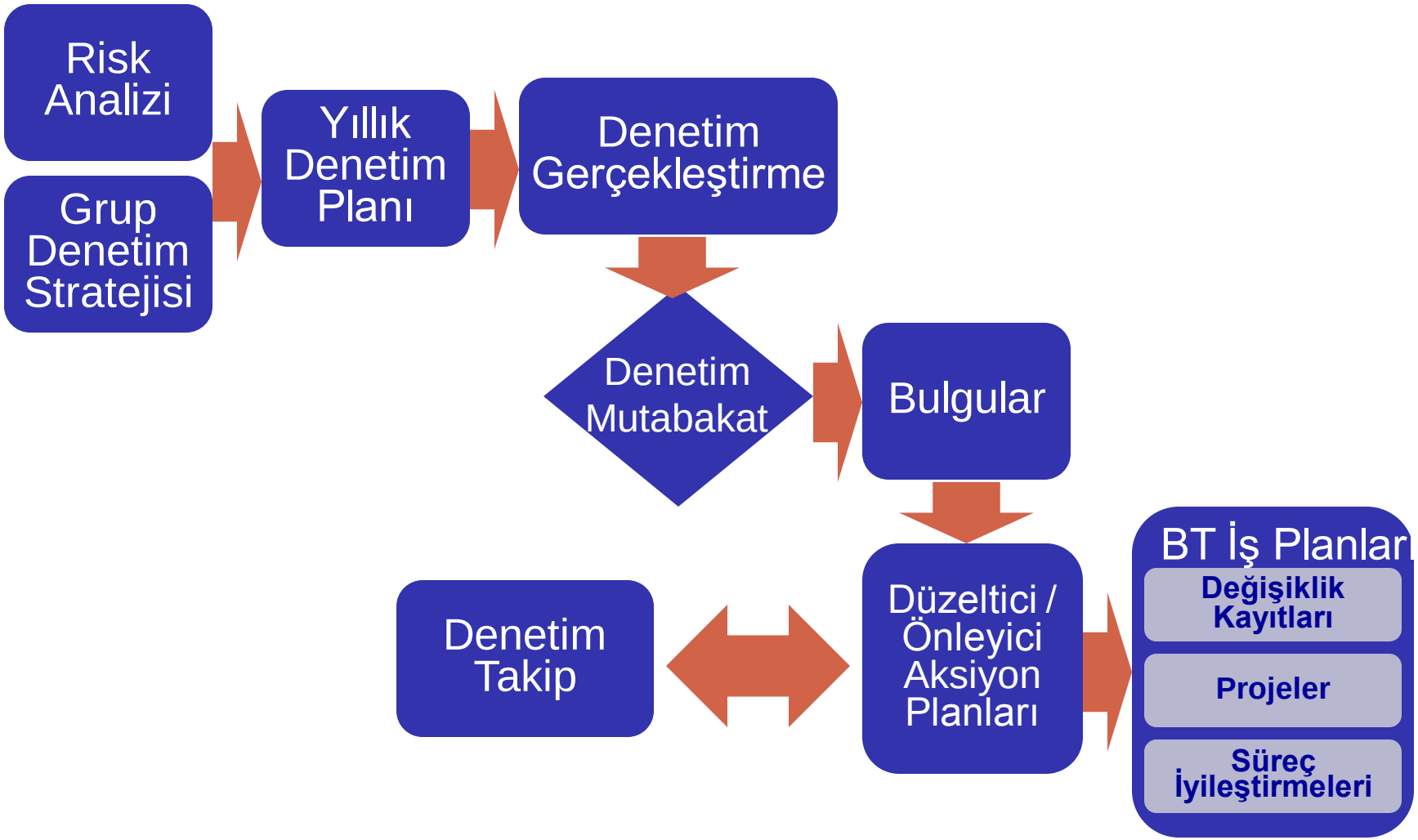
Örnek


COBIT
Kontrol Hedefi:
AI2.1 High-level Design
Translate business requirements into a high-level design.Have the design specifications approved by management to ensure that the high-level design responds to the requirements.
Süreç 1: Teknik Çözüm
Süreç 2: Kalite Güvence
Risk: Failure to meet business requirements
Kontrol:
Yazılım projelerinde Teknik Tasarımın gereksinimleri karşılayıp karşılamadığı Tasarım Gözden Geçirme Toplantılarında değerlendirilmektedir. Tasarım Gözden Geçirme sonuçları XXX sisteminde kayıt altına alınmaktadır.
KPI1: TGG yapılmayan proje oranı
KPI2: Ort. TGG puanı
CMMI
Kontrol Hedefi:
PPQA – SP2.1
Objectively evaluate the designated work products and services against the applicable process descriptions, standards, and procedures.

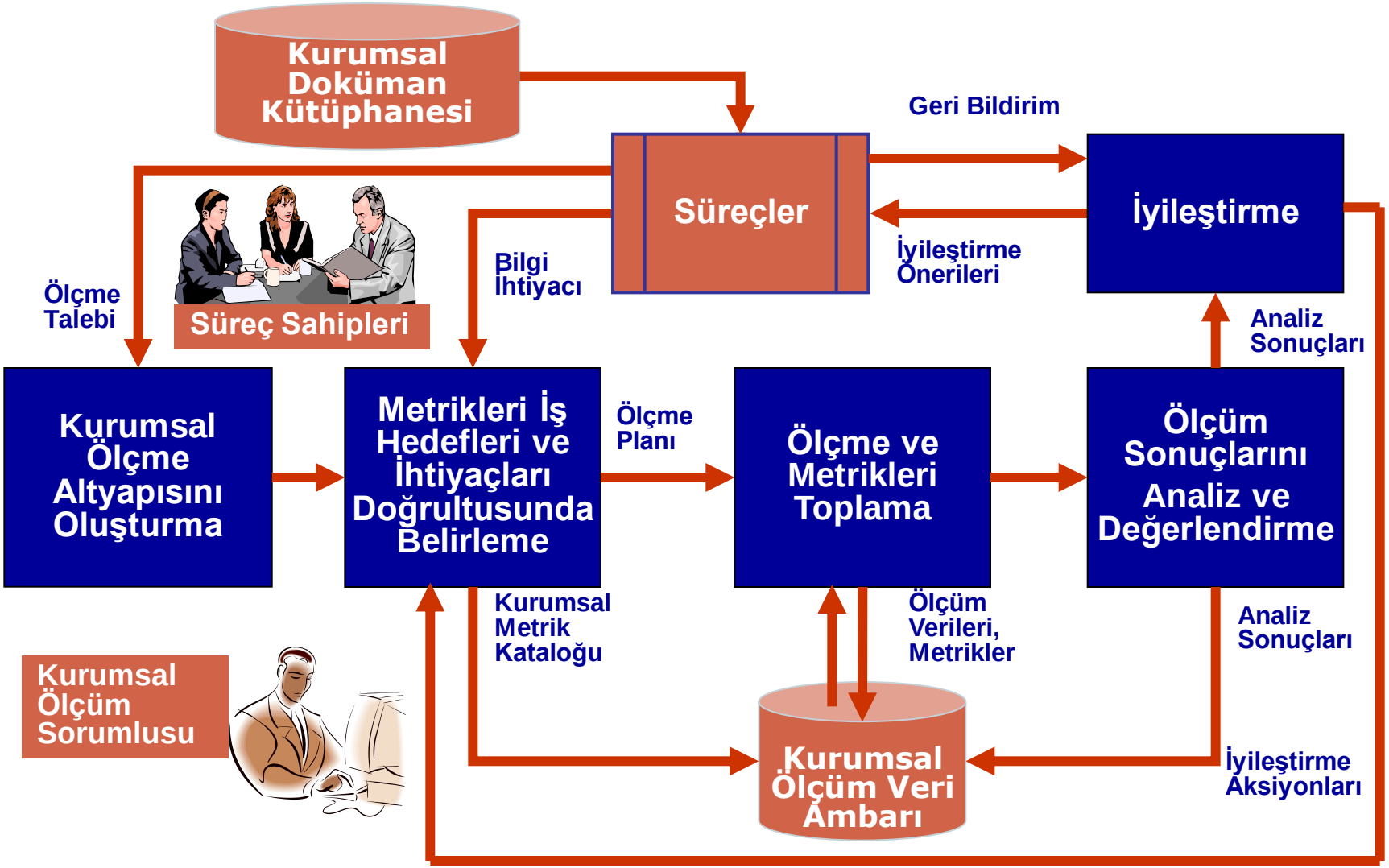
Ibtech İç Kontrol Uyum Süreci

- Referans Kontrol Hedefleri ve Ibtech BT Süreçlerine göre İç Kontroller tanımlanır.
- İç Kontrollerin işleyişinden sorumlu kontrol sahipleri (yönetici ve üzeri) belirlenir. Kontroller kontrol sahipleriyle periyodik olarak gözden geçirilir.
- İç Kontrollere Uyum:
  - Walkthrough çalışmaları ile kontrolün yeterliliği ve etkinliği denetlenir.
  - Test Çalışmalarında kontrolün çalışma sıklığına göre popülasyon ve örneklem seçilerek kontrollerin operasyonel olarak işlediği güvence altına alınır.
  - İç Kontroller Uyumla ilgili ölçümler ve KPI'lar toplanır.
- Süreç bazlı İç Kontrollere Uyum dokümante edilerek Üst Yönetime ve Teftiş Kurulu'na raporlanır.
- İç Kontrol Uyum Sonuçları ve hesaplanan Süreç Olgunluk Seviyelerinin BDDK'nın BSD.2010/3 nolu genelgesi gereği Yönetim Beyanında kullanılması planlanmaktadır.

Ibtech İç Denetim Süreci



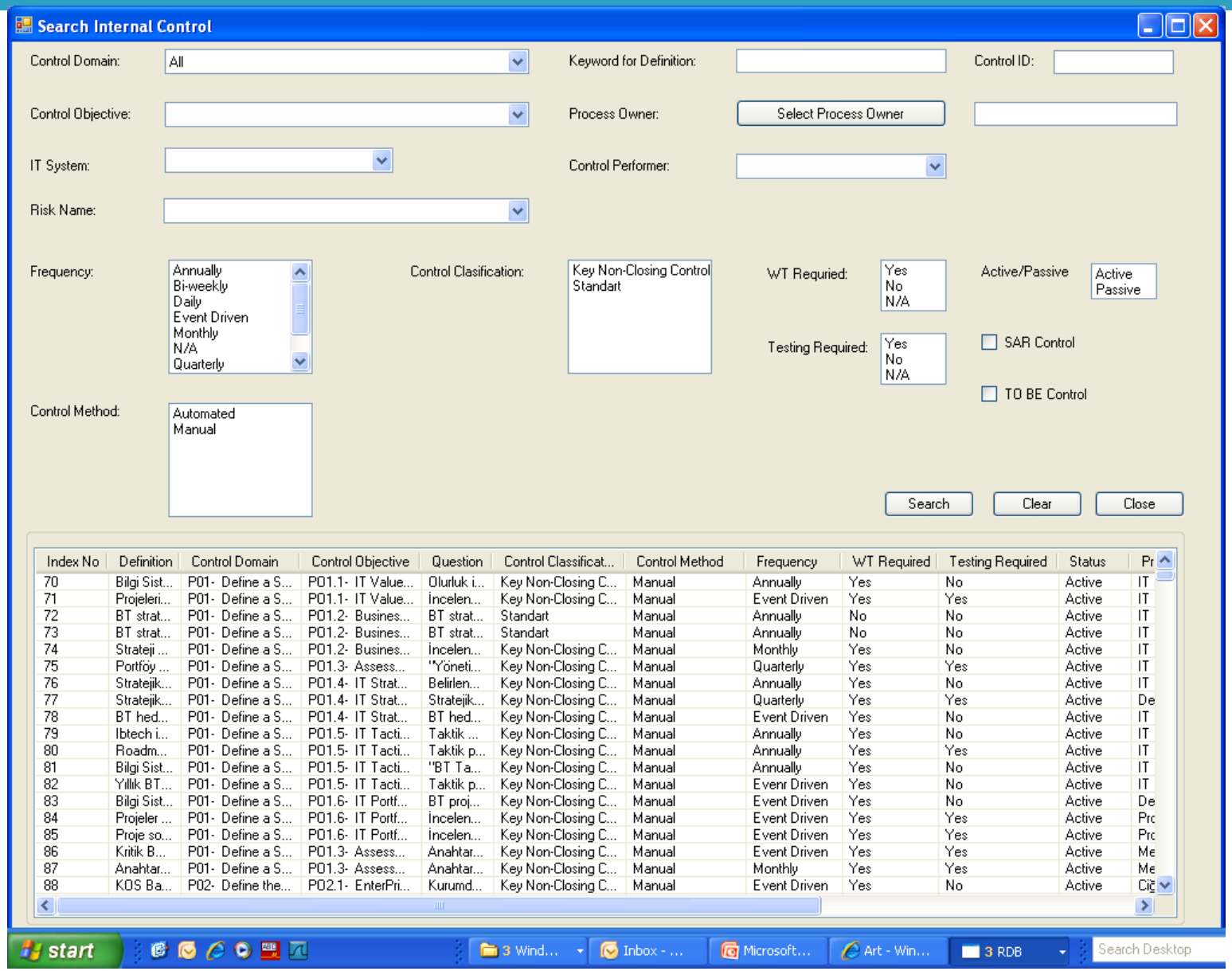
Performans İzleme ve Ölçme



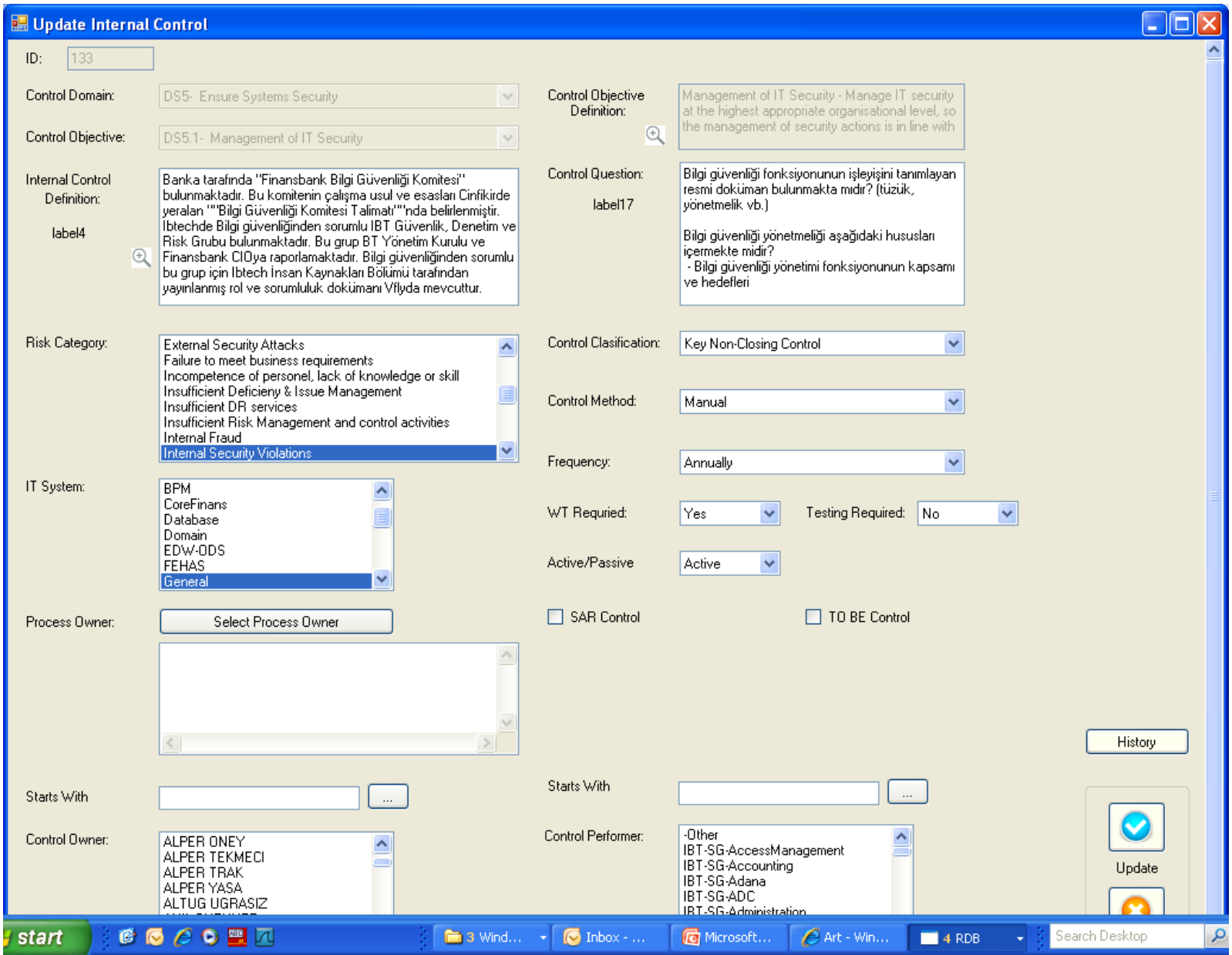
Sorularınız

Teşekkürler ...

Ekler


Search Internal Control
Control Domain:
All
Keyword for Definition:
Control ID:
Control Objective:
Process Owner:
Select Process Owner
IT System:
Control Performer:
Risk Name:
Frequency:
Annually
Bi-weekly
Daily
Event Driven
Monthly
N/A
Quarterly
Control Clasification:
Key Non-Closing Control
Standart
WT Requried:
Yes
No
N/A
Active/Passive
Active
Passive
Testing Required:
Yes
No
N/A
SAR Control
TO BE Control
Control Method:
Automated
Manual
Search
Clear
Close
Index No
Definition
Control Domain
Control Objective
Question
Control Classificat...
Control Method
Frequency
WT Required
Testing Required
Status
70 Bilgi Sist... P01- Define a S... P01.1- IT Value... Olurluk i... Key Non-Closing C... Manual Annually Yes No Active IT
71 Projeleri... P01- Define a S... P01.1- IT Value... İncelen... Key Non-Closing C... Manual Event Driven Yes Yes Active IT
72 BT strat... P01- Define a S... P01.2- Busines... BT strat... Standart Manual Annually No No Active IT
73 BT strat... P01- Define a S... P01.2- Busines... BT strat... Standart Manual Annually No No Active IT
74 Strateji ... P01- Define a S... P01.2- Busines... İncelen... Key Non-Closing C... Manual Monthly Yes No Active IT
75 Portföy ... P01- Define a S... P01.3- Assess... "Yöneti... Key Non-Closing C... Manual Quarterly Yes Yes Active IT
76 Stratejik... P01- Define a S... P01.4- IT Strat... Belirlen... Key Non-Closing C... Manual Annually Yes No Active IT
77 Stratejik... P01- Define a S... P01.4- IT Strat... Stratejik... Key Non-Closing C... Manual Quarterly Yes Yes Active De
78 BT hed... P01- Define a S... P01.4- IT Strat... BT hed... Key Non-Closing C... Manual Event Driven Yes No Active IT
79 Ibtech i... P01- Define a S... P01.5- IT Tacti... Taktik ... Key Non-Closing C... Manual Annually Yes No Active IT
80 Roadm... P01- Define a S... P01.5- IT Tacti... Taktik p... Key Non-Closing C... Manual Annually Yes Yes Active IT
81 Bilgi Sist... P01- Define a S... P01.5- IT Tacti... "BT Ta... Key Non-Closing C... Manual Annually Yes No Active IT
82 Yıllık BT... P01- Define a S... P01.5- IT Tacti... Taktik p... Key Non-Closing C... Manual Evenr Driven Yes No Active IT
83 Bilgi Sist... P01- Define a S... P01.6- IT Portf... BT proj... Key Non-Closing C... Manual Event Driven Yes No Active De
84 Projeler ... P01- Define a S... P01.6- IT Portf... İncelen... Key Non-Closing C... Manual Event Driven Yes Yes Active Pro
85 Proje so... P01- Define a S... P01.6- IT Portf... İncelen... Key Non-Closing C... Manual Event Driven Yes Yes Active Pro
86 Kritik B... P01- Define a S... P01.3- Assess... Anahtar... Key Non-Closing C... Manual Event Driven Yes Yes Active Me
87 Anahtar... P01- Define a S... P01.3- Assess... Anahtar... Key Non-Closing C... Manual Monthly Yes Yes Active Me
88 KOS Ba... P02- Define the... P02.1- EnterPri... Kurumd... Key Non-Closing C... Manual Event Driven Yes No Active Cİ
start
3 Wind...
Inbox - ...
Microsoft...
Art - Win...
3 RDB
Search Desktop

Ekler


Update Internal Control
ID:
133
Control Domain:
DS5- Ensure Systems Security
Control Objective:
DS5.1- Management of IT Security
Internal Control Definition:
label4
Banka tarafında "Finansbank Bilgi Güvenliği Komitesi" bulunmaktadır. Bu komitenin çalışma usul ve esasları Cinfikirde yeralan ""Bilgi Güvenliği Komitesi Talimatı""nda belirlenmiştir. Ibtechde Bilgi güvenliğinden sorumlu IBT Güvenlik, Denetim ve Risk Grubu bulunmaktadır. Bu grup BT Yönetim Kurulu ve Finansbank CIOya raporlamaktadır. Bilgi güvenliğinden sorumlu bu grup için Ibtech İnsan Kaynakları Bölümü tarafından yayınlanmış rol ve sorumluluk dokümanı Vflyda mevcuttur.
Risk Category:
External Security Attacks
Failure to meet business requirements
Incompetence of personel, lack of knowledge or skill
Insufficient Deficieny & Issue Management
Insufficient DR services
Insufficient Risk Management and control activities
Internal Fraud
Internal Security Violations
IT System:
BPM
CoreFinans
Database
Domain
EDW-ODS
FEHAS
General
Process Owner:
Select Process Owner
Starts With
Control Owner:
ALPER ONEY
ALPER TEKMECI
ALPER TRAK
ALPER YASA
ALTUG UGRASIZ
Control Objective Definition:
Management of IT Security - Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with
Control Question:
label17
Bilgi güvenliği fonksiyonunun işleyişini tanımlayan resmi doküman bulunmakta mıdır? (tüzük, yönetmelik vb.)
Bilgi güvenliği yönetmeliği aşağıdaki hususları içermekte midir?
- Bilgi güvenliği yönetimi fonksiyonunun kapsamı ve hedefleri
Control Clasification:
Key Non-Closing Control
Control Method:
Manual
Frequency:
Annually
WT Requried:
Yes
Testing Required:
No
Active/Passive
Active
SAR Control
TO BE Control
History
Starts With
Control Performer:
-Other
IBT-SG-AccessManagement
IBT-SG-Accounting
IBT-SG-Adana
IBT-SG-ADC
Update
start
3 Wind...
Inbox - ...
Microsoft...
Art - Win...
4 RDB
Search Desktop