



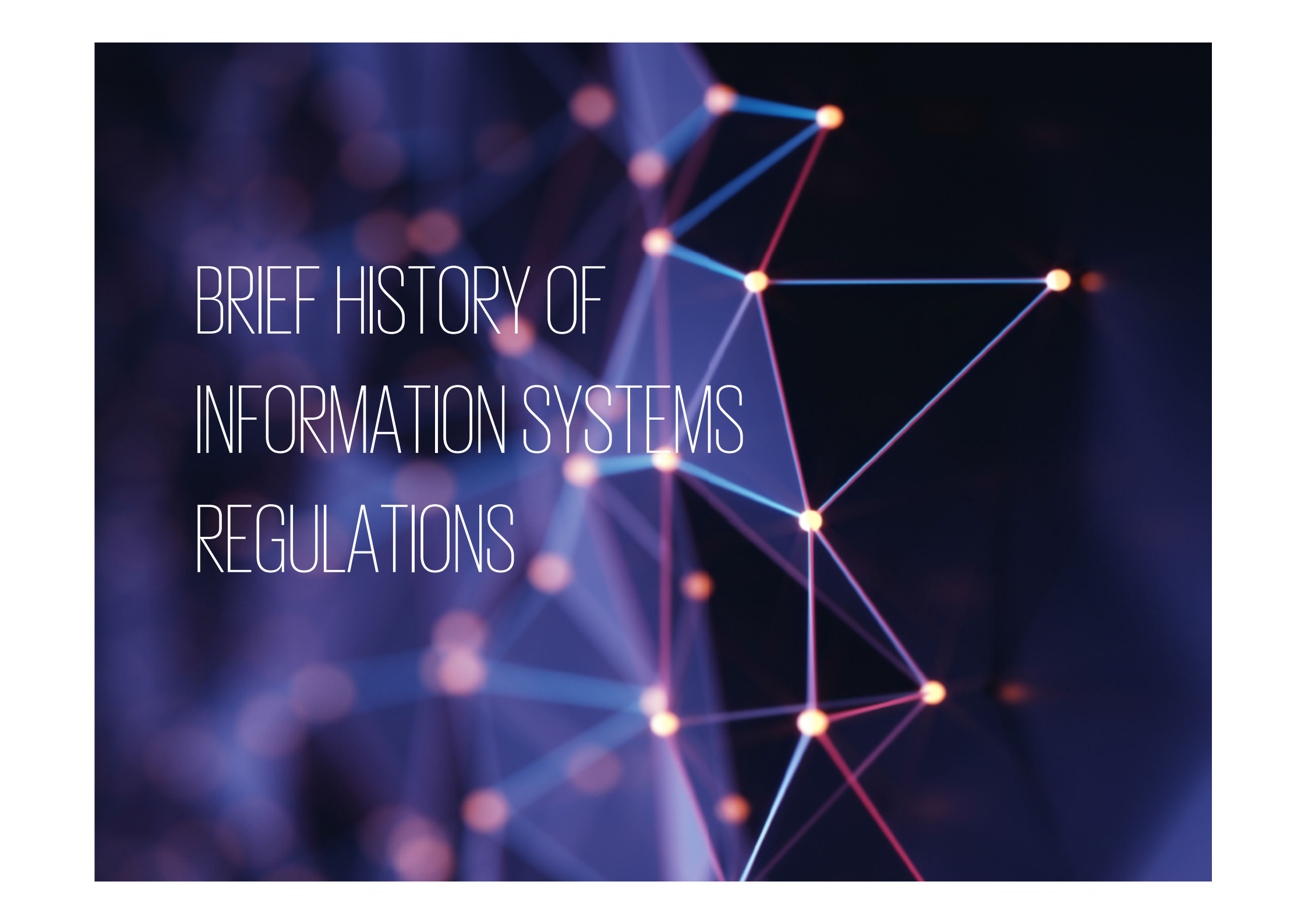
Information Systems Regulations for Banking Industry

Ehtiram Ismayilov
Director
Information Risk Management
KPMG Türkiye

Baku, 17 May 2019

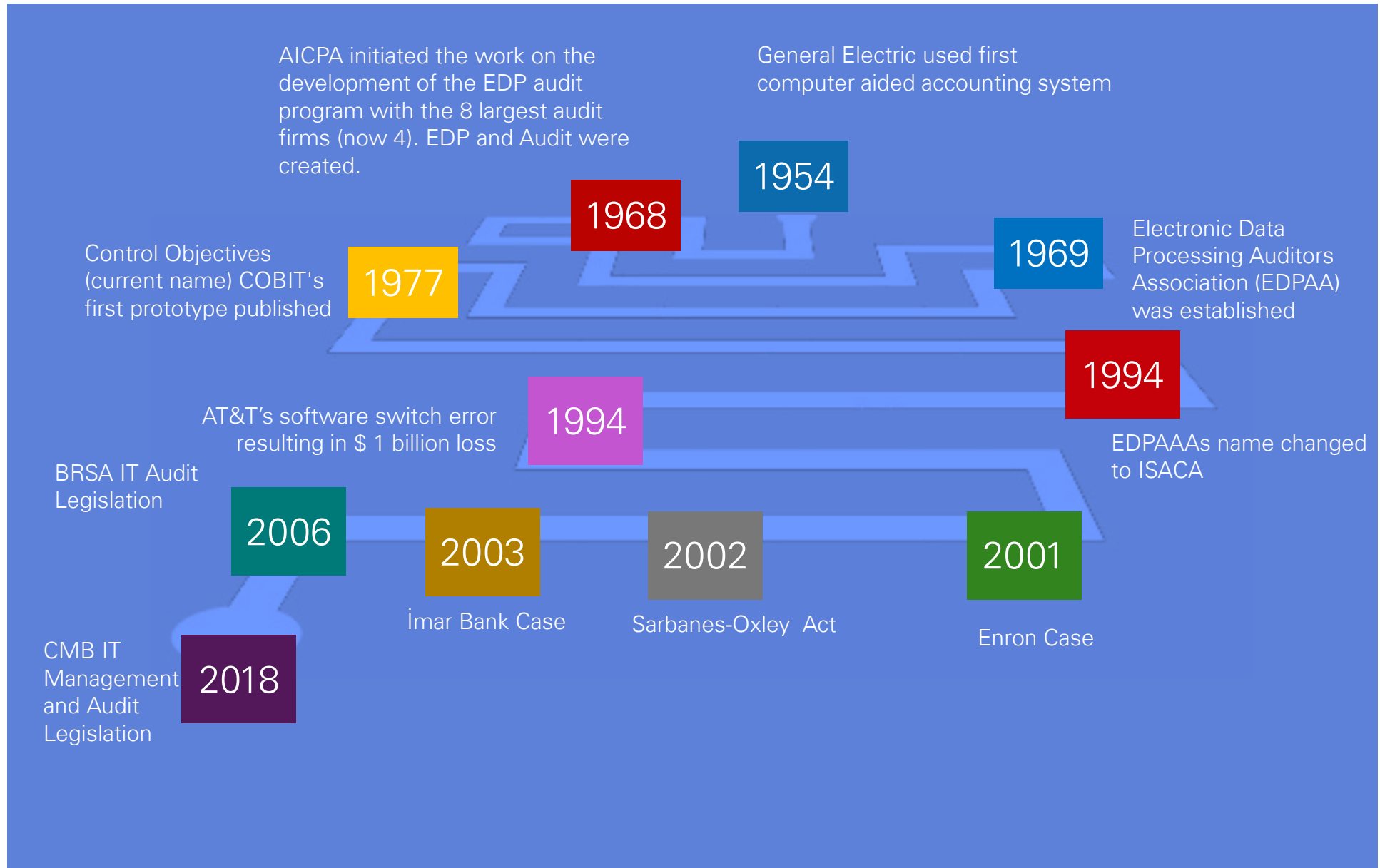
Agenda

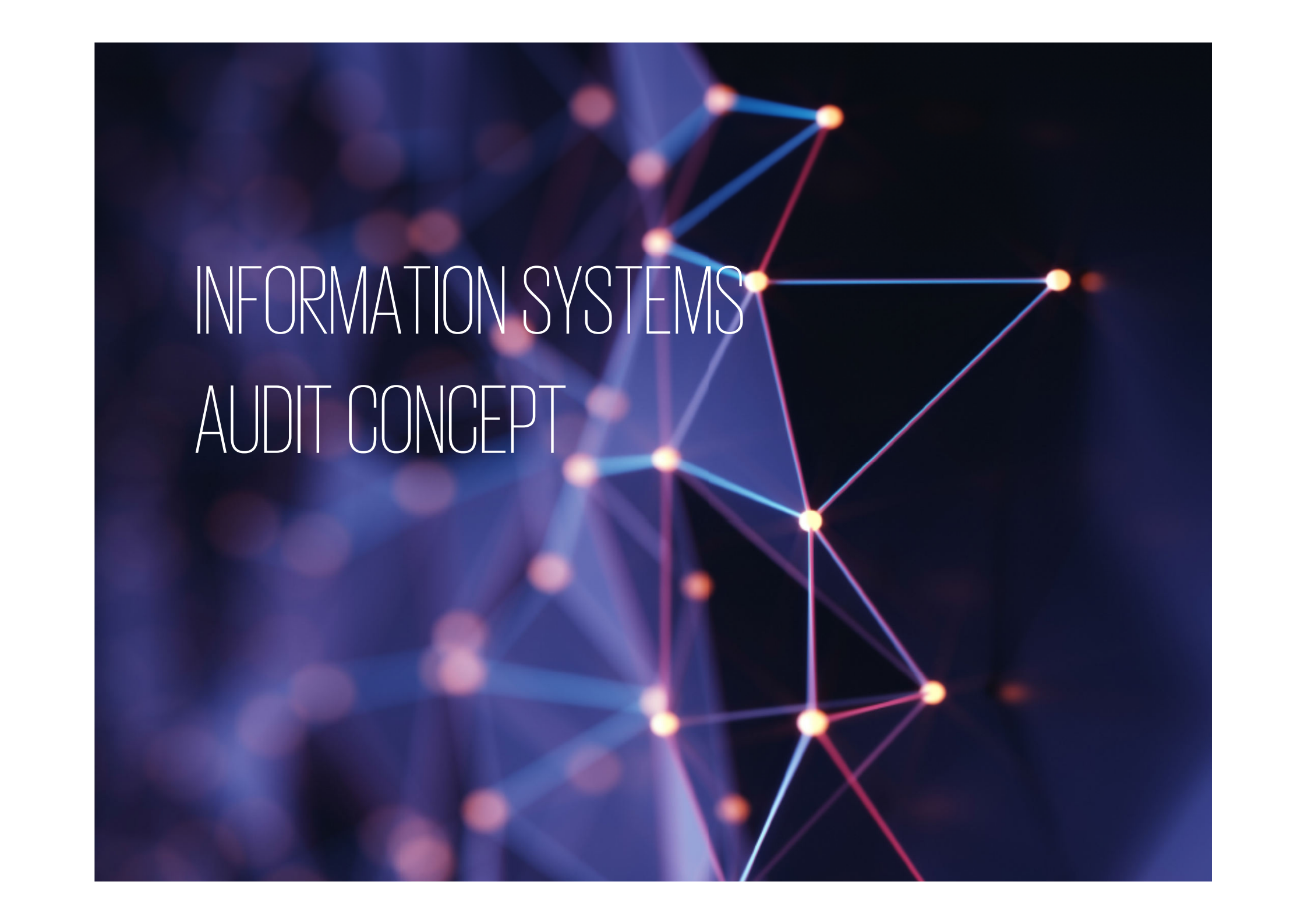
- ❑ Brief History of Information Systems Regulations
- ❑ Information Systems Audit Concept
- ❑ International Information Systems Audit Regulations
- ❑ Information Systems Regulations in Turkey



BRIEF HISTORY OF INFORMATION SYSTEMS REGULATIONS

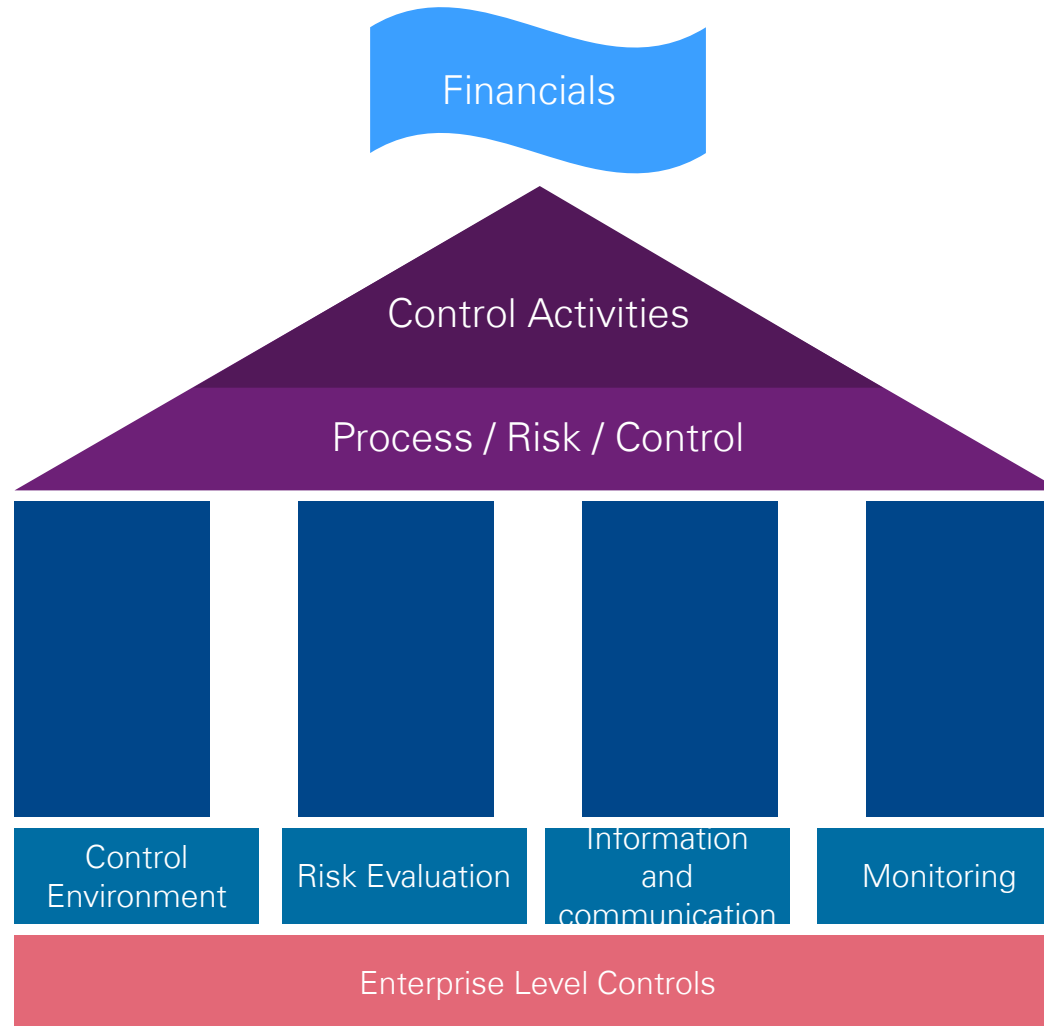
Brief History of Information Systems Regulations



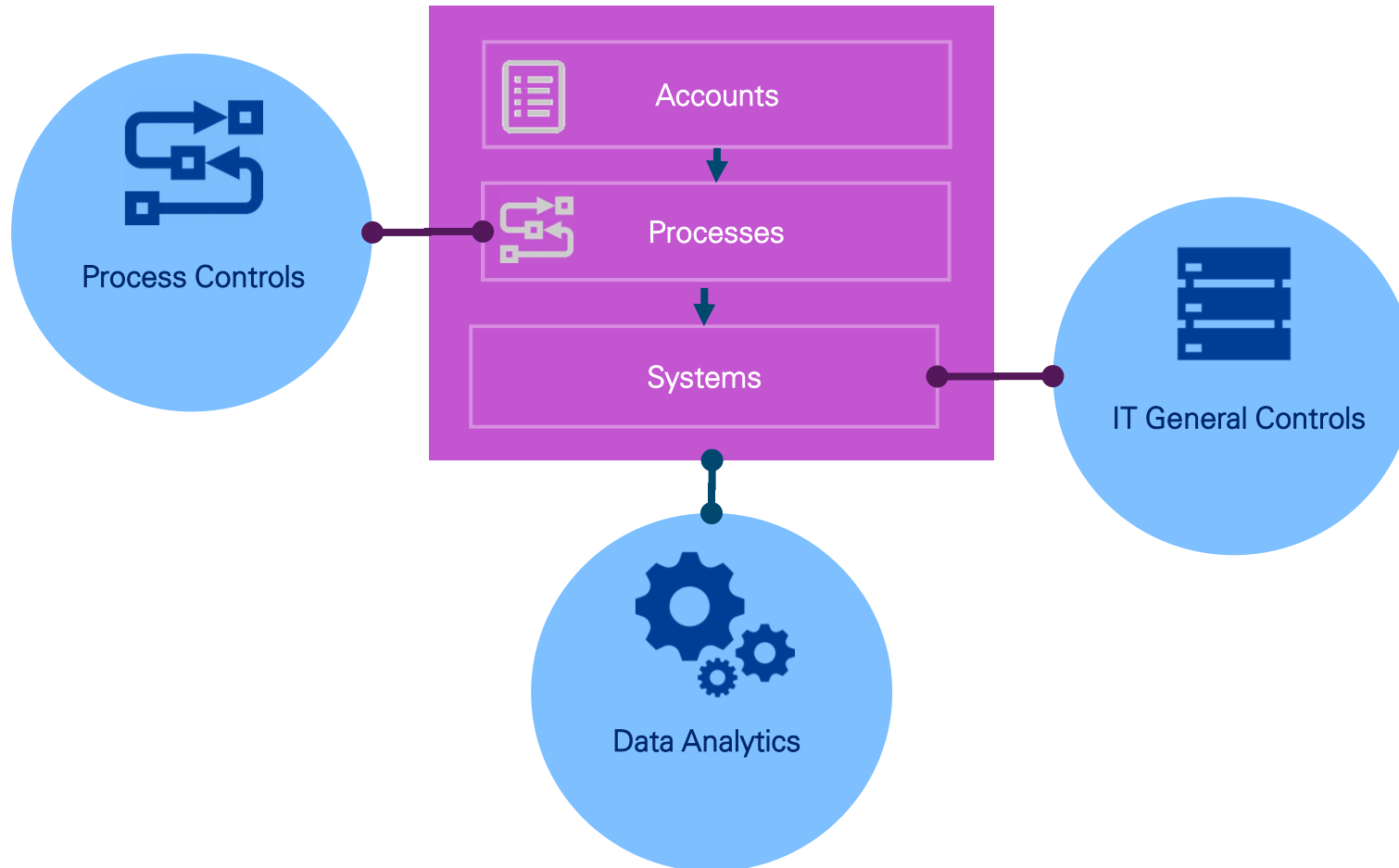


INFORMATION SYSTEMS AUDIT CONCEPT

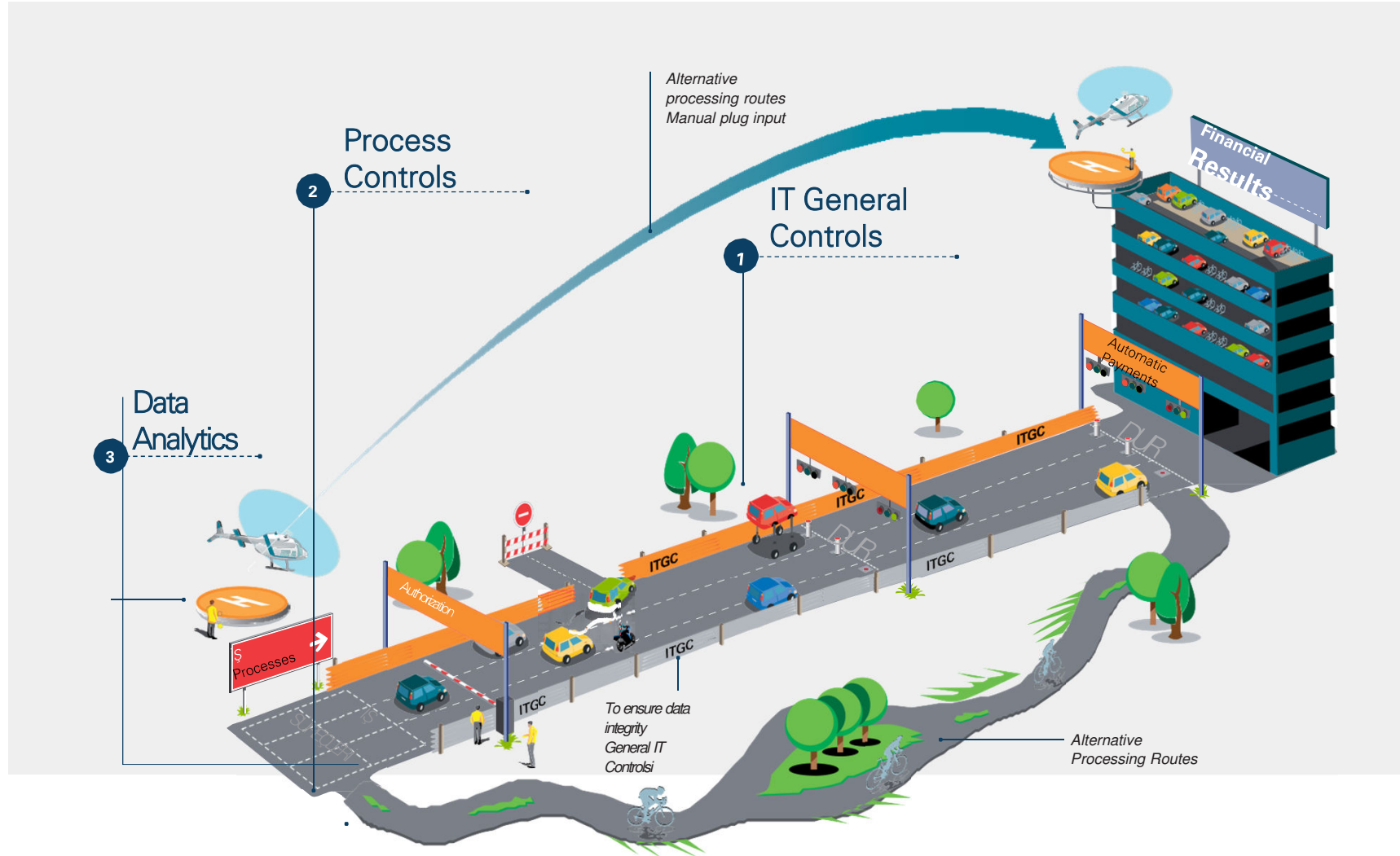
COSO: Internal Control Framework



Information Systems Audit Concept



Information Systems Audit Concept





INTERNATIONAL INFORMATION SYSTEMS AUDIT REGULATIONS

International Information Systems Audit Regulations



Germany

BaFin: German Federal Monitoring Agency

BSI: Federal Information Security Office

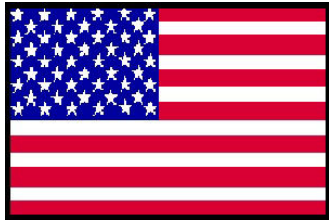
IDW: German Institute of Auditors

MaRisk: Access Rights, Data Integrity, Accessibility, Privacy

Safety Management System and Risk Management Standards of Information Technologies

IDW PS 330: IT environment, IT strategy, IT infrastructure, applications, monitoring systems and outsourcing

International Information Systems Audit Regulations



U.S.A

PCAOB: Accounting Supervisory Board for Public Companies

NIST: National Institute of Standards and Technology

GAO: USA. Court of Auditors

SOX: Internal Control Environment on Financial Reporting Processes, Management Statement, SOX404 IT and Process Audits

GAPP: Generally Accepted Security Principles and Applications

SSAG: Security Self-Assessment Guide

GAGAS: Public Audit Standards, Security Management, Access Management, Configuration Management, Duties Separation, Emergency Planning

FISCAM: Federal IT Audit Guide

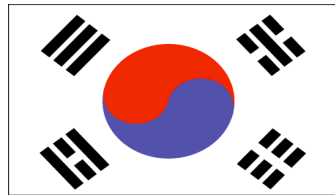
International Information Systems Audit Regulations



United Kingdom

FSA: Financial Services Authority [FCA & PRA]

Senior Management Arrangements, Systems and Controls (SYSC13): Technology strategies, requirements, system acquisition, development, ISO27002



South Korea

KICPA: Institute of Certified Public Accountants of Korea

Audit in Information Systems Environments: Risk assessment and audit procedures sub-headings contain regulations on IT audit.

Log records, separation of tasks, computer aided audit techniques, data accessibility, integrity etc.

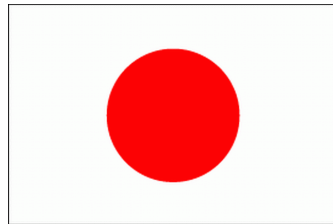


Holland

NOREA: IT Auditors Association

Registered EDP-Auditor: It is the only country where a nationally registered IT auditor certificate is available.

International Information Systems Audit Regulations



Japan

FSA: Financial Services Authority

- Control Environment for IT Risk Management
- IT Risk Management System
- J-SOX: Financial Instruments and Exchange Law



Canada

CICA: Canadian Chamber of Certified Public Accountants

COCO: Internal Control Model
ITCG: IT Control Guide

Summary: Common Themes

GOVERNANCE



- ❑ IT Strategy and Policy
- ❑ Information Systems Risk Management
- ❑ Data Integrity, Privacy and Accessibility
- ❑ IT External Service Management

SECURITY



- ❑ Information Security Awareness and Training
- ❑ Access Management
- ❑ Separation of Tasks
- ❑ Inspection Traces
- ❑ Physical and Environmental Security



- ❑ Information Systems Acquisition, Development and Maintenance
- ❑ Change Management
- ❑ Configuration Management



- ❑ Emergency Management
- ❑ Business Continuity Plan
- ❑ Event Management
- ❑ IT Operations

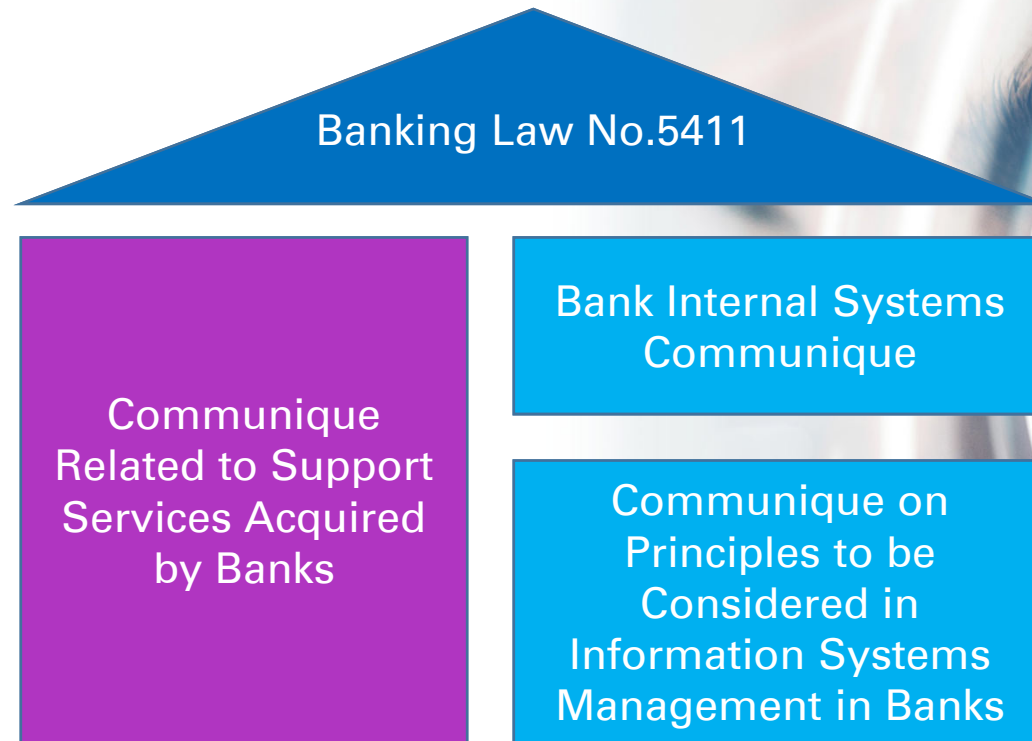
DEVELOPMENT & CHANGE

OPERATIONS

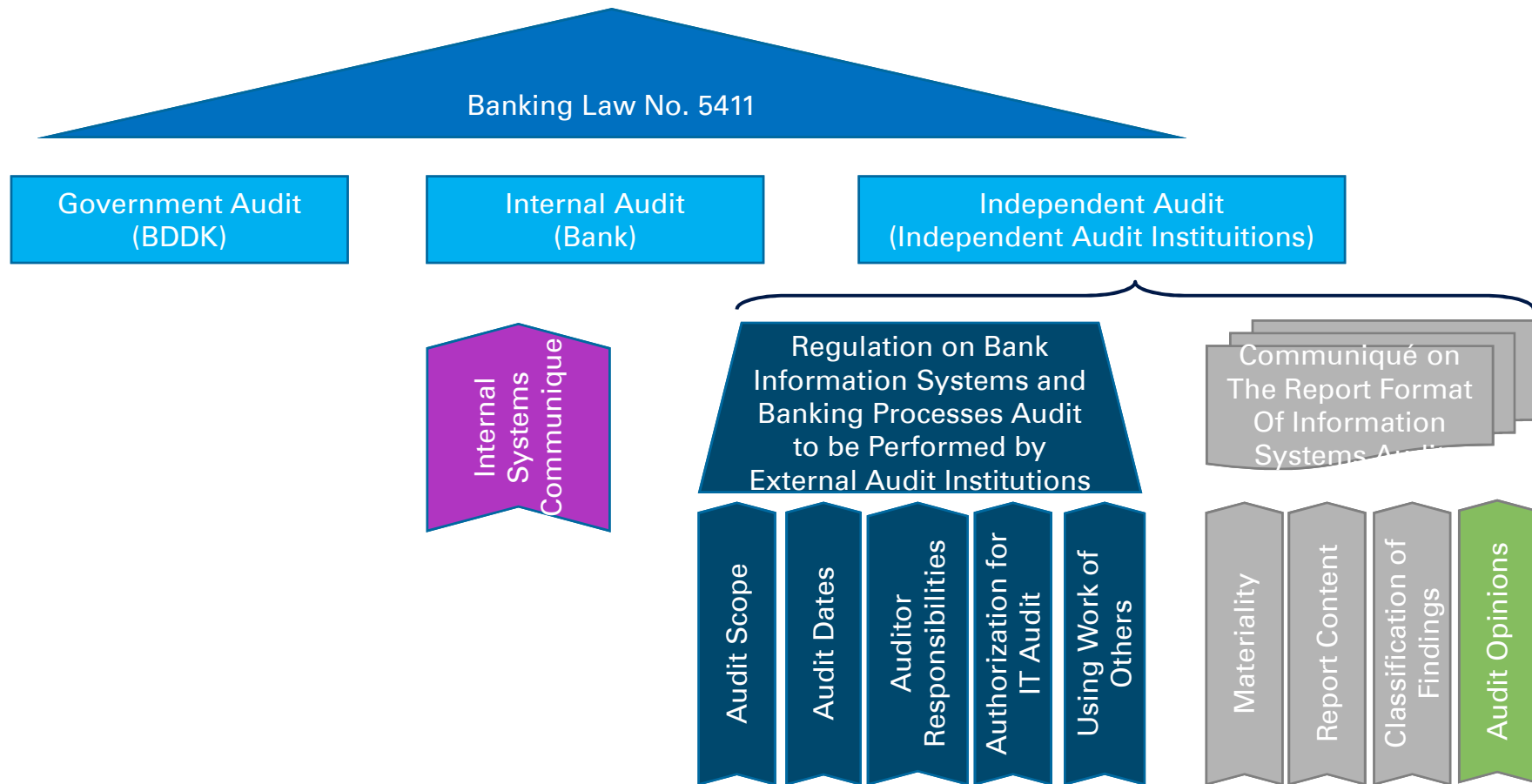


INFORMATION SYSTEMS REGULATIONS IN TURKEY









Information Systems Regulations in Turkey



Information Systems Regulations in Turkey Banking Industry



Other Information Systems Regulations In Turkey

2013		Information Systems Audit Guide
2013		Obligation of Authorized Economic Operator (AEO) Status - ISO27001
2013		Principles Regarding Internal Audit System of Intermediary Institutions
2014		Payment and Electronic Money Institutions Information Systems Audit Legislation
2015		Information Systems Supervision Regulations of TSM Centers belonging to New Generation ÖKC's (payment recorder device)
2016		Risk Center Member Audit Circular
2016		ISO27001 Certificate Obligation
2018		SPK (Capital Market Board) Information Systems Audit and Management Legislation



Ehtiram Ismayilov

Director

Information Risk Management

KPMG Türkiye

T: +90 216 681 90 00 – 6061

M: +90 533 294 6113

E: eismayilov@kpmg.com

W: www.kpmg.com.tr



© 2019 KPMG Bağımsız Denetim ve Serbest Muhasebeci Mali Müşavirlik A.Ş., KPMG International Cooperative'in üyesi bir Türk şirkettir. KPMG adı ve KPMG logosu KPMG International Cooperative'in tescilli ticari markalarıdır. Türkiye'de basılmıştır.

Bu dökümanda yer alan bilgiler genel içeriklidir ve herhangi bir gerçek veya tüzel kişinin özel durumuna hitap etmemektedir. Sürekli güncel ve doğru bilgi sunumuna özen gösterilmesine karşın bu bilgiler her zaman her durumda doğru olmayabilir. Hiç kimse özel durumuna uygun bir uzman görüşü almaksızın , bu dökümanda yer alan bilgilere dayanarak hareket etmemelidir. KPMG International Cooperative bir İsviçre kuruluşudur. KPMG bağımsız şirketler ağıının üye firmaları KPMG International Cooperative'e bağlıdır. KPMG International Cooperative müşterilerine herhangi bir hizmet sunmamaktadır. Hiç bir üye firmanın KPMG International Cooperative'e veya bir başka üye firmayı üçüncü şahıslar ile karşı karşıya getirecek zorlayıcı yada bağlayıcı hiçbir yetkisi yoktur.