

Compliance Standards

ISO 19600 AND ISO 37001

Bratislava, April 5, 2017



SLOVENSKO – RAKÚSKA
OBCHODNÁ KOMORA
SLOWAKISCH – ÖSTERREICHISCHE
HANDELSKAMMER





SCREENING
SOLUTIONS

A leading Czechoslovak consulting firm providing risk management services to clients in CEE.

Services are mainly focused on compliance management, background research, business intelligence, investigations and forensic audit.

A background image showing a business meeting. Several hands are visible, some pointing at documents and others near a smartphone on a desk. The scene is brightly lit, suggesting an office environment.

ATcons

A consultancy cooperating with other experts in areas of Compliance and Contract management, especially with well-known law firms and tax consultants, to provide their customers with a performance spectrum as required.



Dr. Ivan Moroz

- XXX
- XXX
- XXX
- XXX



Dr. Armin Toifl

- Over 30 years of experience
- Consulting and professional services focused on Compliance management systems
- XXX
- XXX

Is your Compliance Program *State-of-the-Art*?

WHO MAY BE INTERESTED TO KNOW?

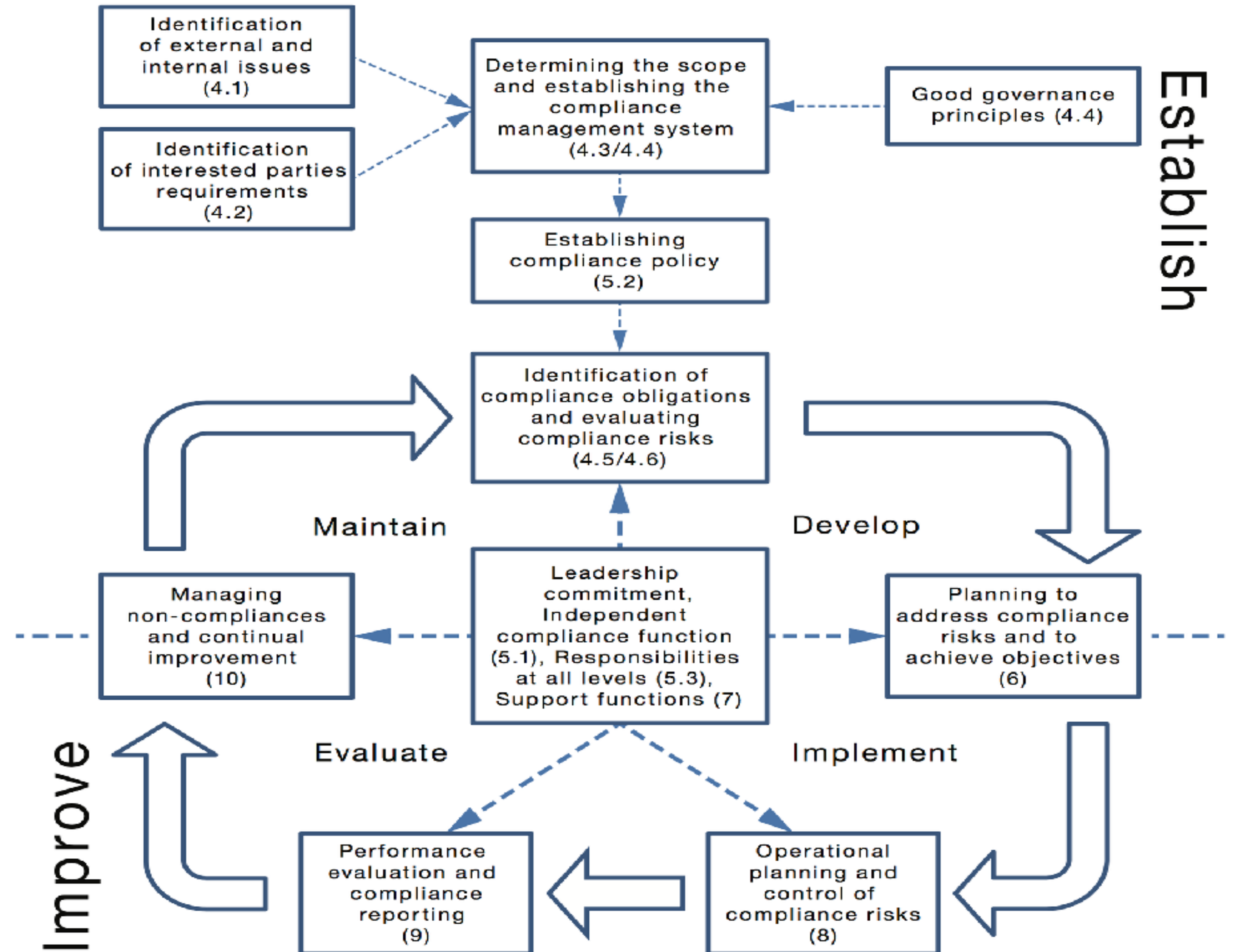
- **You** as the Compliance Manager might be interested to find some guideline for the design, implementation or review of your Compliance Management System (CMS)
- The question may also be asked by
 - your **manager**,
 - the **CEO / CFO**,
 - the chairperson or a member of your **supervisory board**,
 - a shareholder, financing institution or other stakeholder.
- **Battle of Codes** among business partners
- Following a serious offence your public customers may ask for **evidence of self-purification** (e.g. based on public procurement law).
- You may wish to (re-)gain the **trust** of your business partners.
- You might seek defense in a case of **corporate criminal liability**.

Where is State-of-the-Art defined ?

- **Transparency International:** Business Principles for Countering Bribery
- 13 Good Practices by **OECD** on Internal Controls, Ethics and Compliance
- **US Sentencing Guidelines:** 7 Elements of an Effective Compliance Program
- **German IDW** Prüfungsstandard 980 (Principles of proper review of Compliance Management Systems)
- **UK's 6 Principles** for "Adequate Procedures" and BSI 10500 (Specification for an anti-bribery management system)
- **Austrian ONR 192050** Compliance Management Systems
- **ISO 19600** Guideline for Compliance Management Systems
- **ISO 37001** Anti-Bribery Management Systems

Compliance ISO 19600

PLAN-DO-CHECK-ACT



Compliance ISO 19600

SPECIFICS 1/2

ISO 19600 describes the general requirements for Compliance Management Systems. This includes inter alia:

- **Context of the Organization:**
 - Operational environment
 - Identification of compliance obligations
 - Scope of the Compliance Management System
 - Assessment and prioritization of compliance risks
- **Leadership:**
 - Tone from the top, tone from the middle
 - Top Management and Supervising Body's responsibility and commitment
 - Compliance Management: resources, independence
- **Planning:**
 - Establishing compliance policies
 - Planning of measures to manage compliance risks

Compliance ISO 19600

SPECIFICS 2/2

ISO 19600 describes the general requirements for Compliance Management Systems. This includes inter alia:

- **Support:**
 - Training, behaviour and culture
 - Communication and documentation
- **Operation:**
 - Implementation of guidelines, instructions and procedures directing the attitude and behaviour of personnel (incl. management)
- **Performance evaluation:**
 - Monitoring of compliance, application of indicators
 - Evaluation, reporting, whistleblowing
 - Internal audit and management review
- **Improvement:**
 - Action on non-compliance, sanctions, remediation (correction, improvement)

Compliance ISO 37001

SPECIFICS 1/2

The general CMS requirement are here applied more specifically to fighting bribery.
This includes inter alia:

- **Due diligence** on projects and business associates
- **Business associates** shall commit to prevent bribery and in case of failure the relationship shall be discontinued (business associates are to be included in CMS).
- Implementation of **financial** and **commercial controls** (the latter refers to procurement, operational, sales, commercial, HR, legal and regulatory activities)
- Attention to both **active** and **passive bribery** (outbound / inbound)
- Attention to **gifts, hospitality, donations** and similar **benefits**
- Dealing with **public officials**
- Unbiased **investigation** of suspicious circumstances

Compliance ISO 37001

SPECIFICS 2/2

Annex A to ISO 37001 gives useful informative guidance on additional bribery-related issues such as:

- Facilitation and extortion payments
- Reasonable and proportionate CMS
- Bribery risk assessment (low, medium, high bribery risks)
- Employment aspects, in particular:
 - due diligence in recruiting,
 - performance bonuses,
 - conflict of interest,
 - temporary staff or workers.
- Practical suggestions on the bribery-related issues mentioned on previous slide

Certification of your Compliance Management System

- Which organization (part) shall be certified?
- Which standard shall be applied?
- Which risk areas shall be included?
- Who shall certify?
- Certificates are valid for 3 years after the initial audit and thereafter subject to annual surveillance checks
(based on ISO 17021)

Any Questions?
Thank you for your attention!

Dr. Ivan Moroz

Screening Solutions, Slovakia

Dr. Armin Toifl

ATcons Business Consulting, Austria