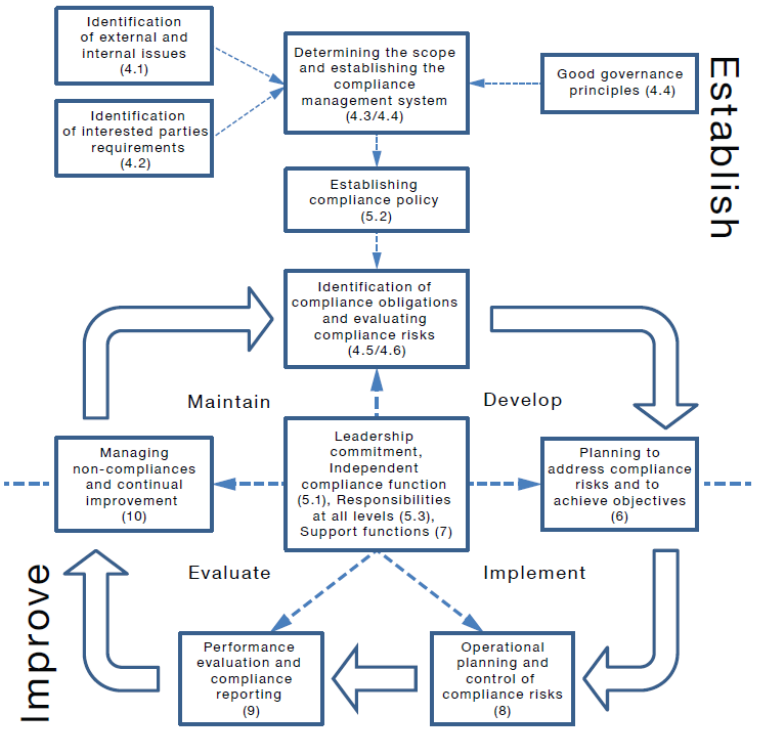
KPMG

Assessment/ Audit of Compliance Management Systems (CMS)

ECS
Zurich, 24 August 2017

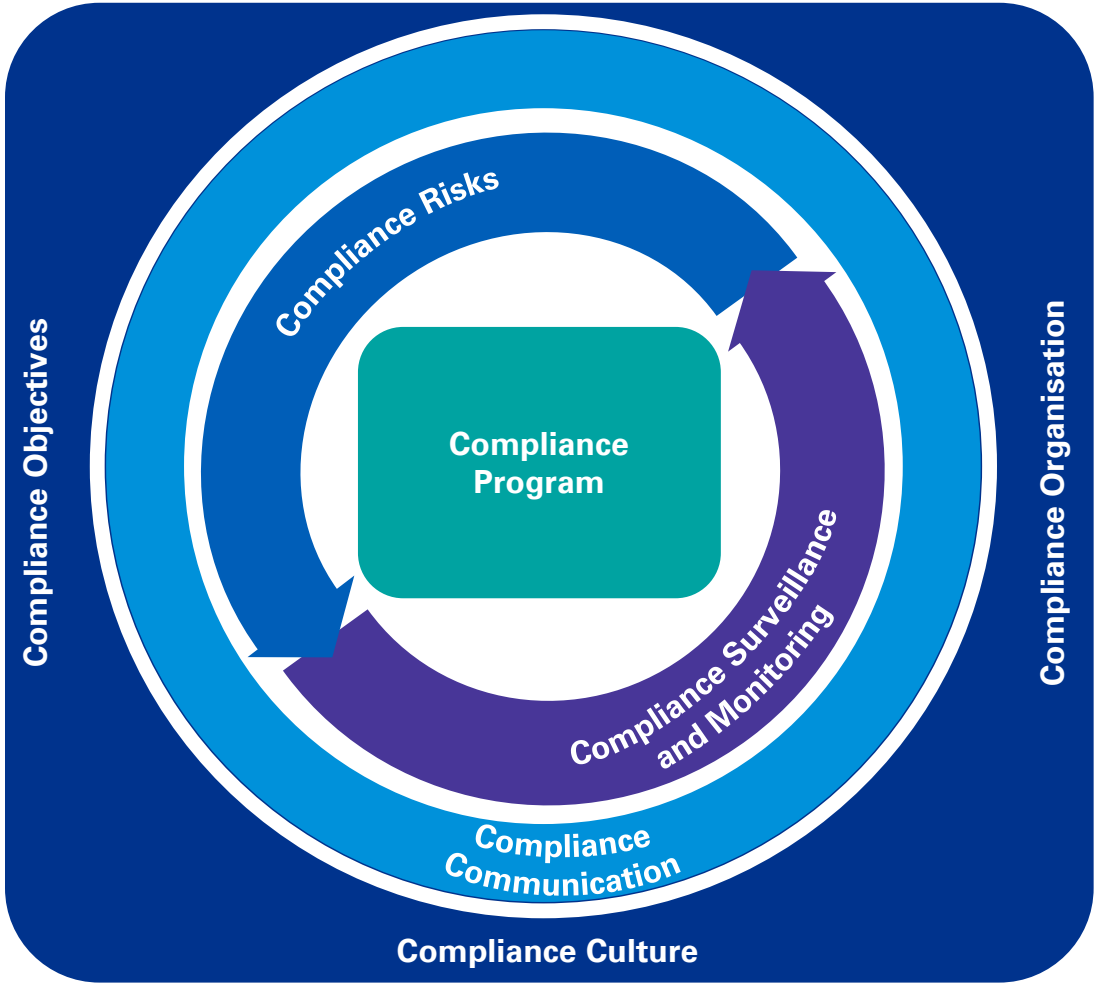
Assessment/ Audit of CMS - Two Standards

ISO 19600: Leadership & Commitment



IDW PS 980 Assessment: Culture and Program

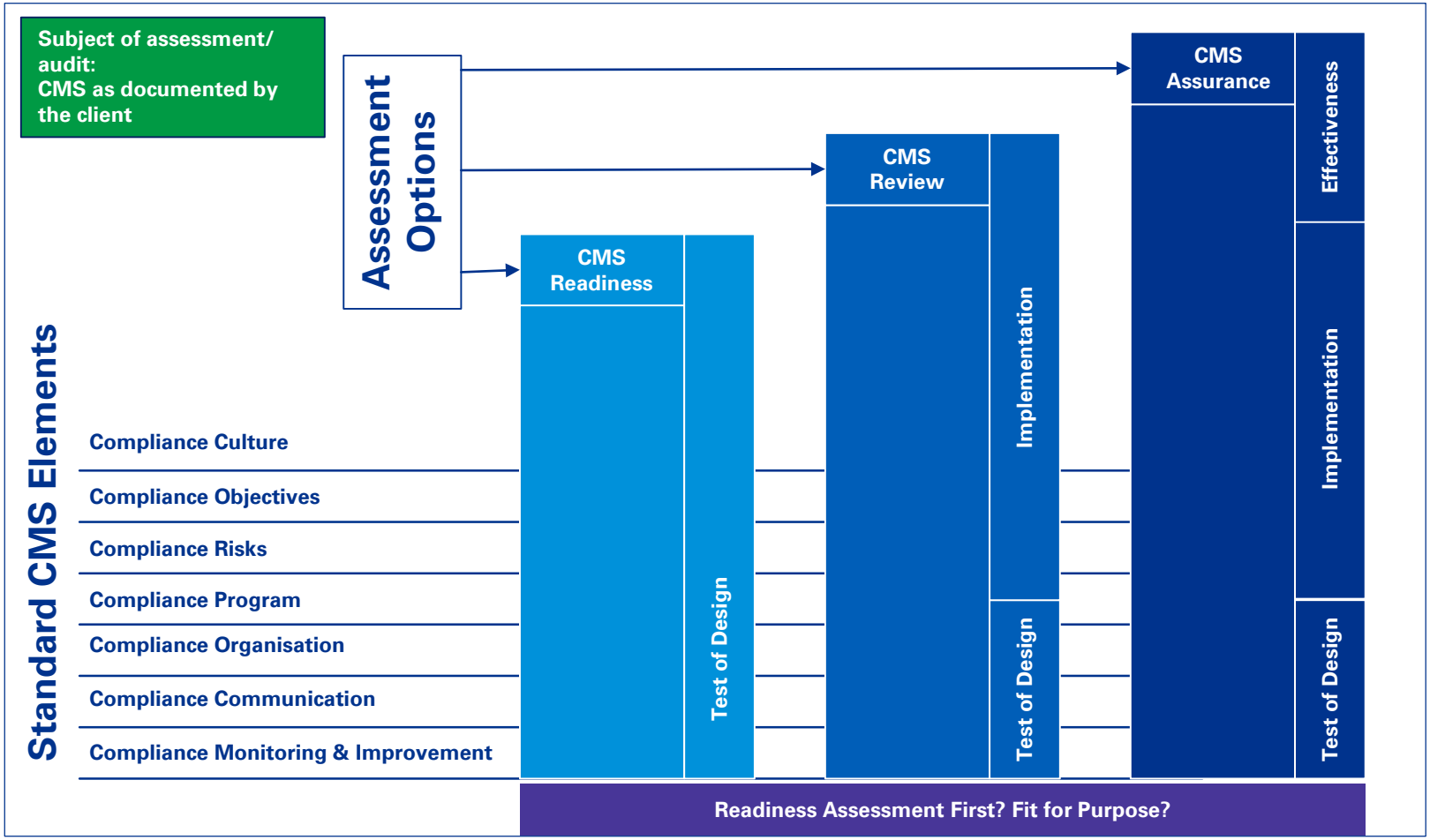
CMS - IDW Prüfungsstandard (PS) 980



COSO Framework

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring activities

Three Assessment Types: Design, Implementation and Effectiveness



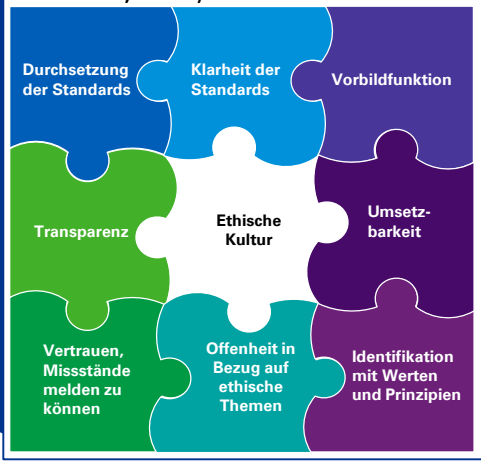
CMS IDW PS 980 – Audit Objectives

Compliance Objectives

- Consideration of general goals corporate/ **business objectives**
- Identification and evaluation of the **rules and regulations relevant to the organisation**
- Definition of **specific compliance topics** associated with respective risks to the organisation

Compliance Culture

- Basis for the appropriateness and the **effectiveness** of the CMS
- **Commitment and actual behaviour** of the executive level / the board (i.e. commitment, compliance culture as top management issue, etc.)



Compliance Organisation

- **Roles and responsibilities**
- Organisational structure
- **Independence**
  - Separate function or integrated with other control functions
  - Collaboration with other functions
  - Centralised vs. decentralised function
- Operational organisation
- Definition of the **ressources**
  - Financial
  - Personnel

CMS IDW PS 980 – Audit Objectives

Compliance Risks

- Systematic **risk assessment** in order to identify risks
- Systematic risk reporting
- Analysis of probability of occurrence and potential consequences (**impact assessment**)
- **Regular** adjustment/ **update**

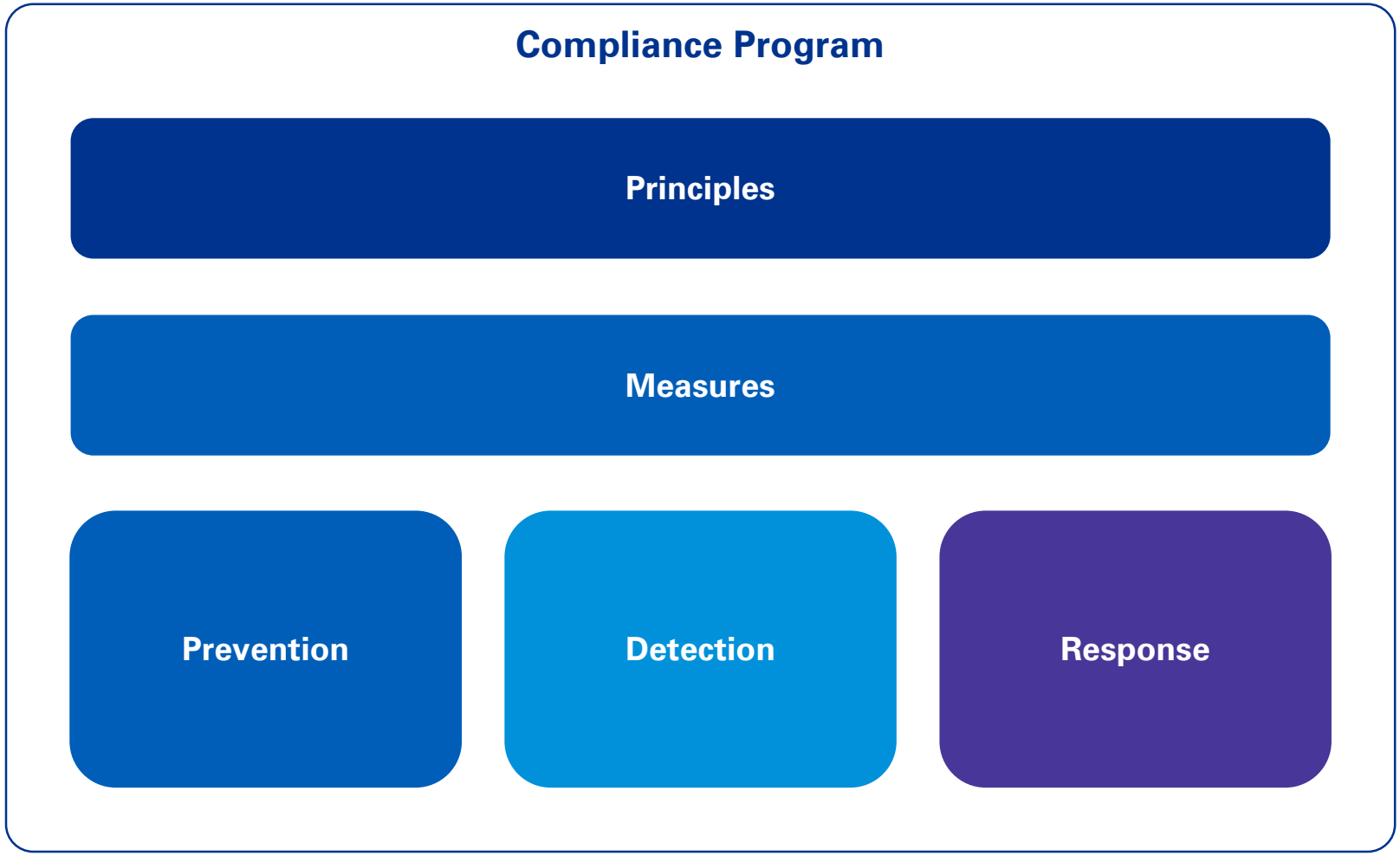
Compliance Communication

- **Communication on the Compliance Program** and associated roles and responsibilities towards employees
- Communication of the **applicable rules and regulations** towards employees
- Communication on the **reporting lines** that are available to employees
- **Training** (classroom and web-based training)
- Concept for the **qualification of employees in compliance** relevant functions

Compliance Monitoring & Improvement

- Regular **assessment** of the **appropriateness** and the **effectiveness** of the Compliance Program
- e.g. **specific audits**, analysis of incoming reports, etc.
- Reporting on the elimination of weaknesses/ gaps and improvement of the Compliance Program

CMS IDW PS 980 – Audit Objectives



CMS IDW PS 980 – Audit Objectives (Program)

Principles

- Definition of the principles, e.g. in the form of a Code of Conduct
- Definition of specific rules and procedures (policies)
- Adjustment and update of rules and procedures (policies)

Measures for Prevention

- Process-specific measures, e.g.
  - — Separation of functions
  - — Management of permissions
  - — Four-eye-principle
- Due diligence on third parties and employees
- Job rotation
- Training

Measures for Detection

- Whistleblowing/ Reporting procedures
- Proactive data analysis on transactions
- Assessments/ Audits

Measures for Response

- Definition of internal reporting
- Definition of external reporting
- Definition of internal investigations protocol
- Definition of a protocol on securing evidence resulting from compliance violations or other misconduct

CMS IDW PS 980 – Audit Work Paper (Example)

[Client] Compliance Audit
[Focus area, e.g. Anti-corruption]

[Client] Compliance Audit

Project Name	*Test of Design and Implementation* ***Monitoring and Improvement***	Reference
Prepared by / Abbreviation	***Monitoring and Improvement Concept***	Reviewer / Abbreviation
Date of Preparation		Date of Review

Understand activities and processes:	WP Ref.

• Conduct interviews with [responsible person/s]
  • to understand in how far the monitoring and improvement concept is linked to the CMS elements and risks
  • to understand how the program is provided to the entities
  • to understand what data-sources are used for the assessment
  • to understand if there are central data analyses performed to detect compliance breaches at an early stage and an adequate tool is available
  • to understand procedures regarding continuous improvement and remediation of identified deficiencies	

KPMG

Draft SAS 980 (PS 980)

Draft SAS 980

SAS 980 (Draft Version 31.12.2016)

- Provides guidance for a **voluntary** audit of Compliance Management Systems (CMS)
- Effective date **not yet** determined
- Audit objectives:
  - **Appropriateness** (Test of Design/ Implementation)

    Is the CMS-related documentation adequately described to ensure that potential instances of non-compliance are identified early enough to prevent non-compliance? Were adequate principles and measures **implemented at a certain point in time**?
  - **Effectiveness**

    Were the implemented principles and measures **effective** over a certain time period?
- Additional element in IDW PS 980: "**Konzeptionsprüfung**" (audit objectives: statements regarding the concept of the CMS)
- **Elements** of the CMS
  - Compliance Culture / Objectives / Risks / Program / Organisation / Communication / Monitoring

Draft SAS 980

SAS 980 (Draft Version 31.12.2016)

- Reporting

a) Überschrift: Angabe, dass es sich um den Bericht eines unabhängigen Wirtschaftsprüfers handelt;
b) Berichtsadressaten;
c) Prüfungsauftrag (vgl. Tz. 18 ff.); Aussage, ob eine Angemessenheits- (begrenzte oder hinreichende Sicherheit) oder Wirksamkeitsprüfung durchgeführt worden ist
d) Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche;
e) Darstellung der oder Bezugnahme auf die vom Unternehmen angewandten CMS-Grundsätze;
f) Gegenstand, Art und Umfang der Prüfung;
g) Abgrenzung der Verantwortlichkeiten der gesetzlichen Vertreter und des CMS-Prüfers;
h) Aussage, dass die Prüfung in Übereinstimmung mit diesem PS durchgeführt wurde;
i) Aussage, dass die Prüfungsgesellschaft des Prüfers und der Prüfer die Richtlinie zur Unabhängigkeit von EXPERTsuisse einhalten. Dieser Richtlinie basiert auf den Prinzipien der Integrität, Objektivität, professionellen Kompetenz und Verhalten, Vertraulichkeit sowie der Sorgfaltspflicht.
j) Aussage, dass die Prüfungsgesellschaft des Prüfers den Qualitätsstandard QS 1 oder ISQC 1 Im Prüfungsbericht des Prüfers anwendet.
k) Falls relevant:

- Beschreibung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstands.
- Aussage, dass der Auftrag für einen bestimmten Zweck bzw. Adressatenkreis durchgeführt wurde und deshalb die Verwendung der Ergebnisse für andere Zwecke ausgeschlossen ist.

Some discussion points …

… relative to IDW PS 980 and SAS 980 respectively

- Readiness Assessment first?
- Art. 102 Abs. 2 SCC (AB&C)?
- Importance of Documentation!
- Experience of (statutory) auditors?
- In-house availability of specific skills? Accreditation? Team?
- Approaches to audit soft factors (e.g. reputation risks/ “tone at the top”) –> example Swiss Post
- How to determine materiality?
- Liability for Auditors (e.g. “clean” audit opinion on CMS vs. corruption payment post audit)
- Audit Opinion (short-form/ long-form)?
- etc.

KPMG

Your Contact

Contact Details

Matthias Kiener
Partner Forensic
KPMG AG
Forensic
Badenerstrasse 172
8026 Zürich
T: +41 58 249 21 35
M: +41 79 667 36 94
E: mkiener@kpmg.com

kpmg.ch/socialmedia

kpmg.com/app