Aufbau eines Compliance Managementsystems

SUHLING TOOLING

Dozent: Peter Suhling

Herausgeber: suhling tooling GmbH

Hauptstraße 128, 69469 Weinheim, www.suhling.biz

Autor: Peter Suhling

Version: 1

Vortrag am 22.12.2022 um 16:30 Uhr

SUHLING TOOLING

Agenda

- Vorstellung
- Prüfgrundlage
- Ziele
- Geltungsbereiche
- Tooling
- Projekt
- Anwendung
- Pflicht und Kür
- Zertifizierung

SUHLING TOOLING

Vorstellung Peter Suhling

- Zertifizierter IT Compliance Manager (TÜV Rheinland)
- Berufener Compliance Officer 2 Jahre
- 2 x zertifizierter Datenschutzbeauftragter
- externer Datenschutzbeauftragter seit 2007 - heute
- Dozent für Datenschutz an der IHK 2018 - 2022
- Technical Reviewer ISO 27001 seit 2017 für unterschiedliche Zertifizierungsgesellschaften
- IT-Sachverständiger für Datenschutz, Informationssicherheit und KRITIS seit 2018-2022
- Berufener Lead Auditor ISO 37301 TÜV Rheinland seit September 2022

SUHLING TOOLING

Prüfgrundlage

Die Prüfgrundlage:

ISO 37301

oder

SOC 1, ITAR, HIPAA, ISO 27001

oder

Eigener Standard

SUHLING TOOLING

Ziele

Was können die Ziele eines CMS sein?

- Compliance – was ist das?
- Nachweis über Compliance – Nachweise vorhalten
- Nachweis eines Dritten - Zertifizierungsgesellschaft
- Unternehmen aufhübschen vor Unternehmensverkauf

SUHLING TOOLING

Geltungsbereiche

Was soll compliant sein?

Unterschied zwischen
Anwendungsbereich
und
Geltungsbereich

SUHLING TOOLING

Tooling

Wie soll das CMS technisch und inhaltlich abgebildet werden?

Ort	Art
On premises / On-site	MS-SharePoint leer
IaaS	Confluence leer
PaaS	Wiki leer
SaaS	Ordnerstruktur Windows Explorer, Vorlagen
Mix	CMS-Anbieter befüllt, Vorlagen
	Mix aus Kollaborationsplattform und Inhalten

Pro und Contra: Sicherheit / Verfügbarkeit

SUHLING TOOLING

Projekt

Wie soll das CMS aufgebaut werden?

- Freigabe GF
- Projektziel
- Zeitrahmen, Meilensteine
- Projektteam
- Aufrechterhaltung des CMS

SUHLING TOOLING

Anwendung

Wie soll der Aufbau und die später Anwendung gestaltet werden?

- ISO-Team bilden
- Aufbau der Inhalte, Verifizierung durch Verantwortliche
- Code of Conduct: Verboten sind Preisabsprachen, Geschenkerichtlinie, Anti-Korruption, Kartellrecht, Datenschutz, Cyber-Security, Geldwäsche, Arbeitszeitüberschreitungen, Arbeitssicherheit, Hinweisgebersystem
- Assetmanagement, Risikomanagement, Kennzahlen
- Aufbau des Rechtskatasters
- Interne Prüfung, Stichproben, interne Audits
- Managementbewertung
- Schulung der Mitarbeiter

SUHLING TOOLING

Pflicht und Kür

Woran muss und kann man sich halten?

- Einhalten von Gesetzen und Vorschriften (Rechts- und Regelkonformität)
- Erweiterte Bedingungen, die erfüllt werden können, z.B. für Konzerne, zukünftige Branchen
- Zertifizierung des CMS durch Zertifizierungsgesellschaft, bisher keine Akkreditierung

SUHLING TOOLING

Zertifizierung in Deutschland

Kann man das CMS zertifizieren lassen?

- Zertifizierung des CMS durch Zertifizierungsgesellschaft, bisher keine Akkreditierung
- Man kann den Standard ISO 37301 nutzen,
- Zertifizierungsgesellschaften nutzen eigenen Standard,
- Audit-Wiederholung jedes Jahr, Voraussetzung internes Audit, Managementbewertung

SUHLING TOOLING

Noch Fragen?

SUHLING TOOLING

Vielen Dank.

Peter Suhling - suhling tooling GmbH

Telefon: 06201 8725124

E-Mail: info@suhling.biz

Website: https://suhlingtooling.com

Urheberrechtshinweise

Diese Unterlagen sind als Begleitmaterial zum Vortrag “Aufbau eines Compliance Managementsystems“ von suhling tooling GmbH, Peter Suhling gedacht und nicht zum Selbststudium geeignet.

SUHLING TOOLING

Backup

Links:

https://www.redhat.com/de/topics/cloud-computing/iaas-vs-paas-vs-saas

https://www.omt.de/online-marketing-tools/compliance-software/

https://intex.software/de/intex-solution-center/hinweisgebersystem/

https://www.compliance.com/resources/what-are-compliance-best-practice-standards/

https://www.austrian-standards.at/de/themengebiete/management-qualitaet-risiko/compliance

https://envoy.com/blog/compliance-standards/

🇬🇧 English
Establishment of a compliance management system

Lecturer: Peter Suhling

Publisher: suhling tooling GmbH

Hauptstraße 128, 69469 Weinheim, Germany, www.suhling.biz

Author: Peter Suhling

Version: 1

Lecture on 22.12.2022 at 4:30 pm

SUHLING TOOLING

Agenda

- Introduction
- Test basis
- Objectives
- Scope
- Tooling
- Project
- Application
- Compulsory and optional
- Certification

Introduction Peter Suhling

- Certified IT Compliance Manager
- appointed Compliance Officer 2 years
- 2 x certified data protection officer
- Data Protection Officer since 2007 - today
- Lecturer for data protection at IHK since 2018 - 2022
- Technical Reviewer ISO 27001 since 2017 for different certification bodies
- IT expert for data protection, information security and KRITIS since 2018-2022
- Appointed Lead Auditor ISO 37301 TÜV Rheinland since September 2022

SUHLING TOOLING

Test basis

The test basis:

ISO 37301

or

SOC 1, ITAR, HIPAA, ISO 27001

or

House standard

SUHLING TOOLING

Goals

What can be the goals of a CMS?

- Compliance - what is it?
- Evidence of compliance - keep evidence
- Evidence from a third party - certification company
- Make the company look good before selling it

Scope

What should be compliant?

Difference between

Scope

and

Technical Scope

SUHLING TOOLING

Tooling

How should the CMS be mapped technically and in terms of content?

Location	Types
On premises / On-site	MS-SharePoint empty
IaaS	Confluence empty
PaaS	Wiki empty
SaaS	Folder structure Windows Explorer, Templates
Mix	CMS provider filled, Templates
	Mix of collaboration platform and content

Pros and cons: Security / Availability

SUHLING TOOLING

Project

How should the CMS be structured?

- Release Management
- Project goal
- Time frame, milestones
- Project team
- Maintenance of the CMS

SUHLING TOOLING

Usage

How should the structure and later application be designed?

- Form ISO team
- Structure of content, verification by responsible persons
- Code of Conduct: Prohibited are price-fixing, gift policy, anti-corruption, antitrust law, data protection, cyber security, money laundering, working time violations, occupational safety, whistleblower system.
- Asset management, risk management, key figures
- Structure of the legal register
- Internal audit, spot checks, internal audits
- Management assessment
- Staff training

Compulsory and freestyle

What must and can be complied with?

- Compliance with laws and regulations (legal and regulatory compliance).
- Extended conditions that can be met, e.g. for corporate groups, future industries
- Certification of CMS by certification body, no accreditation so far

SUHLING TOOLING

Certification in Germany

Can the CMS be certified?

- Certification of the CMS by a certification body, no accreditation yet.
- One can use the ISO 37301 standard,
- Certification companies use their own standard,
- Audit repeat every year, prerequisite internal audit, management assessment

SUHLING TOOLING

Any questions?

SUHLING TOOLING

Thank you very much.

Peter Suhling - suhling tooling GmbH

Phone: 06201 8725124

Mail: info@suhling.biz

Website: https://suhlingtooling.com

SUHLING TOOLING

Copyright notice

These documents are intended to accompany the lecture "Establishing a Compliance Management System" by suhling tooling GmbH, Peter Suhling and are not suitable for self-study.