

Umsetzung des Datenschutzes mit Hilfe einer GRC Software

Simon Bislin

Corporate Risk Manager / Betrieblicher Datenschutzbeauftragter





Agenda

- Ivoclar Vivadent AG – Zahlen und Fakten
- Corporate Governance Programm bei Ivoclar Vivadent
- Funktionsweise GRC Software
- Umsetzung OBSERVAR Datenschutzmodul
- Fragen / Diskussion

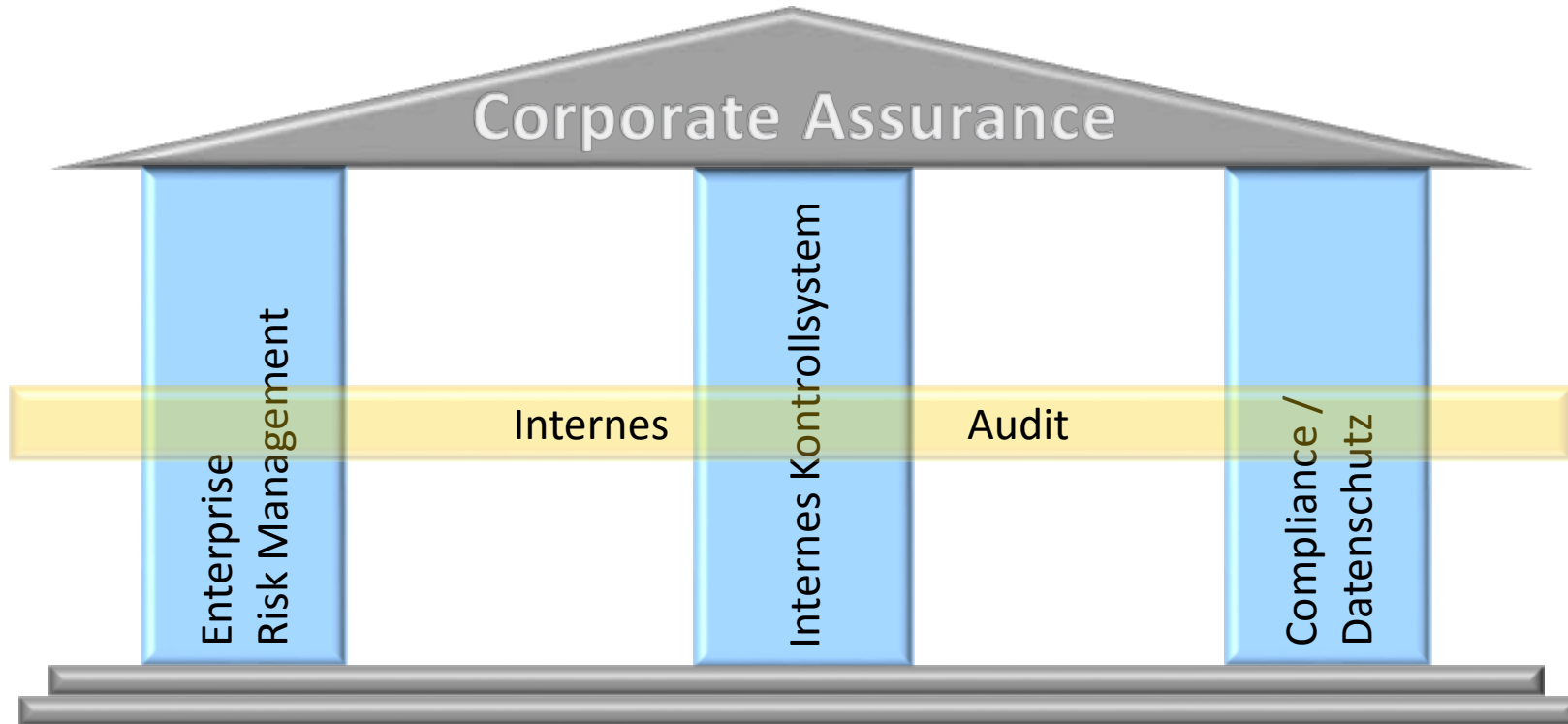
Ivoclar Vivadent

- auf einen Blick

- Herstellung und Vertrieb zahnmedizinischer Produkte
- Umsatz 2013: 747 Mio CHF
- > 3'000 Mitarbeitende weltweit
- Tochtergesellschaften und Marketingbüros in 23 Ländern
- Globales Vertriebsnetz mit unabhängigen Vertriebspartnern und Dentalfachhändlern



Corporate Governance @ Ivoclar Vivadent





Ausgangslage / Problemstellung

- Unübersichtliche Dokumentation auf Word oder Excel Dateien
- Doppelspurigkeiten infolge verschiedener Zuständigkeiten
- Keine Nachverfolgung, keine Wirksamkeitskontrollen





Vision

Ivoclar Vivadent unterhält eine zentrale Plattform für die Bewertung und Dokumentation von Risiken, Steuerung von Maßnahmen sowie zur Wirksamkeitskontrolle des Corporate Assurance Programms.





Lösung



Bitte wählen Sie die angezeigte Sprache und ein Modul aus. **Deutsch** ▼

Wenn Sie Probleme mit der Bildschirmsicht haben - bitte drücken Sie F5 um die Seite wieder aufzufrischen. Dies kann nach Updates notwendig sein, wenn der Internet Browser noch alte Einstellungen im 'cache' hat. (F5 drücken)

Hier werden alle wesentlichen Grundeinstellungen aller Module sowie die Abbildung der Unternehmung / Benutzer / Kataloge etc. bearbeitet.



Master

Analysieren Sie die eingegangenen Durchführungsmeldungen sowie Versäumnisse. Bearbeiten Sie Änderungsvorschläge. Dokumentieren Sie funktionale und Design Audits.



ICS / Operative
Strategic Processes
Compliance / Data protection

Process Module

Melden und dokumentieren Sie die Durchführung von Prozessschritten / periodischen Kontrollen. Schlagen Sie notwendige Änderungen vor.

Analysieren Sie die eingegangenen Projektmeldungen sowie Versäumnisse. Bearbeiten Sie Änderungsvorschläge. Dokumentieren Sie Projekt Audits.



Risk Management Projects
Internal Audit Follow Up

Project Module

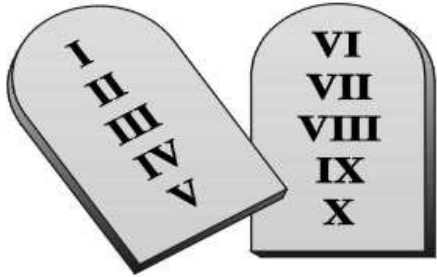
Melden und dokumentieren Sie den Fortschritt von Projekten / Umsetzungsgrad von neuen Massnahmen. Schlagen Sie notwendige Änderungen vor.

Funktionsweise GRC Software

Vorgaben

Umsetzung

Überwachung



- Gesetze
- Richtlinien
- Regularien
- Normen
-

Beschreibung, mit welchen Aktivitäten die Vorgaben umgesetzt werden:

- Prozesse
- Projekte

Werden Aktivitäten auch durchgeführt?

Information bei:

- Überfälligkeiten
- Abweichungen



Umsetzung Datenschutzmodul

Anforderung:

Welche Aufgaben obliegen einem Datenschutzverantwortlichen?

Die Aufgaben des Datenschutzverantwortlichen sind in Art. 13a Abs. 2 DSV geregelt.

Diese sind insbesondere:

- Er prüft die Bearbeitung von Personendaten und empfiehlt Korrekturmaßnahmen,
- Er führt eine Liste der Datensammlungen nach Art. 15 DSG, die vom Inhaber der Datensammlungen geführt werden;





Vorgehen

1

- **Inventur**
- Welche Datensammlungen gibt es im Unternehmen?

2

- **Kategorisierung**
- Erhebung Datenschutzrelevanter Charakteristiken

3

- **Risikobeurteilung**
- Erhebung der technisch / organisatorischen Massnahmen

4

- **Dokumentation**
- Erfassen der Massnahmen im EGRC-System /Bestätigung Massnahme



1 Inventur der Datensammlungen

Kundendaten

- Vertragsdaten
- Kundenstammdaten
- Webshop
- Customer Relationship Management
- Kurs-Mgt ICDE
- Kundenreklamationen
- Messebesucher / Wettbewerbsteilnehmer

Mitarbeiterdaten

- Videüberwachung
- Zutritts- und Zeiterfassungssystem
- Telefonlisten
- Personalstammdaten
- Notfalladressen
- Qualifikationsdatenbank
- Organisationsstammdaten
- Daten zur Leistungsbeurteilung
- Bewerberdatenbank
- Talent Management
- Zeugnisgenerator
- Protokoll System-Zugriffe
- Legal Entity Management





2 Kategorisierung

Erhebung Datenschutzrelevanter Parameter zu den Datenbanken als Grundlager zur Risikobewertung

| Parameter | Ausprägung (Auswahl) |
|-----------------------------|---|
| Bezeichnung der Datenbank | |
| Verantwortliche Person | |
| Standort Datenträger | |
| Bezeichnung der Applikation | |
| Datenkategorie | |
| Zweck | Gesetzliche Vorgaben; vertragliche Beziehung (Arbeitsvertrag); Geschäftsinteresse; Werbung / Kundenaquisition |
| Rechtfertigungsgrund | Einwilligung; überwiegendes Interesse; Kenntnis der Erhebung |





2 Kategorisierung

Erhebung Datenschutzrelevanter Parameter zu den Datenbanken als Grundlager zur Risikobewertung

| Parameter | Ausprägung (Auswahl) |
|-------------------------------|--|
| Datenempfänger | Intern; externe Auftragsdatenbearbeiter; Dritte |
| Information Betroffene | |
| Geltendmachung der Rechte | Recht auf Auskunft, Berichtigung; Sperrung; Löschung Wer ist intern verantwortlich Wer nimmt nach aussen hin die Kontaktstelle wahr? |
| Aufbewahrungsdauer | |
| Melde-/Bewilligungspflicht | |
| Datenübermittlung ins Ausland | |



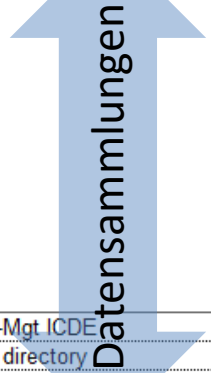


3 Dokumentation Massnahmen

Basierend auf der Risikoeinschätzung werden die technisch / organisatorischen Massnahmen zur Gewährleistung des Datenschutz beschrieben.



| | A | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | AA | AB | AC | |
|----|---------------------------|---------------------|-------------------------------|----------------------------|-------------------------------|---------------------------------------|---------------------|--|------------------------|----------------|-----------------|--------------------------------------|-----------------|-----------------------|----------------|------------------|--------------------------|-----------------------|----------------|----------|----------------------------------|---------------------------|-----------------|----------------|--------------------------------|----------------|------------------------------|----------------------------------|
| 1 | Ta | Ta01 | Ta02 | Ta03 | Ta04 | Ta05 | Ta06 | Tb | Tb01 | Tb02 | Tb03 | Tb04 | Tb05 | Tb06 | Tb07 | Tb08 | Tb09 | Tc | Tc01 | Tc02 | Tc03 | Tc04 | Tc05 | Td | Td01 | Td02 | | |
| 2 | | Zugang zu den Daten | Sicherheit der Räumlichkeiten | Sicherheit der Serverräume | Sicherheit des Arbeitsplatzes | Identifizierung und Authentifizierung | Zugang zu den Daten | Zugang von aussenhalb der Organisation | Lebenszyklus von Daten | Datenerfassung | Protokollierung | Pseudonymisierung und Anonymisierung | Verschlüsselung | Datenträgersicherheit | Datensicherung | Datenvormittlung | Auslagerung von Arbeiten | Sicherheit und Schutz | Datenaustausch | Netzwerk | Verschlüsselung von Mitteilungen | Übergabe von Datenträgern | Protokollierung | Datenaustausch | Unterzeichnen von Mitteilungen | Auskunftsrecht | Recht der betroffenen Person | Reproduzierbarkeit der Verfahren |
| 22 | Kurs-Mgt ICDE | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 23 | User directory | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 24 | Protokoll System-Zugriffe | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 25 | Legal entity management | | | | | | | | | | | | | | | | | | | | | | | | | | | |



4 Dokumentation einer Massnahme (Kontrolle)

Hinzufügen/Bearbeiten Compliance Themen

Assessments **Katalog** Verantwortlich Beendet Pendente

Bitte Unit und Katalog wählen:

T IV Test Datensammlungen

Anzeigen

T IV Test / Datensammlungen

- U Liste Datensammlungen
 - Ua Mitarbeiterdaten
 - Ua01 Personalstammdaten
 - Ua02 Organisationsstammdaten
 - Ua03 Mitarbeiter Leistungsbeurteilu...
 - [3] Löschung Arbeitsze...

Ua03 Mitarbeiter Leistungsbeurteilung - [Aktiv]

ID: Nummer: 1601 Unit: T IV Test

ID: Fortlaufende Nummer: 3

Kurzname: Löschung Arbeitszeugnisse

Beschreibung/Detailtext:

Arbeitszeugnisse, die älter als 10 Jahre sind, werden jährlich durch den Superuser im Zeugnisgenerator gelöscht.

pdf,doc,docx,jpg,jpeg,txt,ppt,pptx,pps,xls,xlsx,xtx,msg

+ Add

Gesamt Verantwortlicher*:

Simon Bislin

Assessor Compliance Einhaltung*:

Simon Bislin

Stv. Assessor Compliance Einhaltung*:

Kein Stellvertreter

Erfassung Meldeeinstellungen

Meldeeinstellungen

Begutachter:

Zusätzliche Referenzierung:

Zus. Referenzierung - max. Anzahl Zeichen: 80

Gültig seit*:

05. Oktober 2011

Gültig bis:

Meldestartdatum*:

05. Oktober 2012

Advance notice verwenden

Meldezyklus*:



jährlich

Kontrollhäufigkeit*:



jährlich

Compliance-Kategorie*:



Datenschutz

Risikobeschreibung:



Hortung von Personendaten

Datenschutzziel*:



Bestandeskontrolle (Life cycle mgt)

Referenz-Dokumentation:



keine

Nachweis Massnahme / Kontrolle:



Keine Arbeitszeugnisse im System, die älter als 11 Jahre sind.

Massnahmentyp*:



Technische Massnahme (Systemeinstellung)



Automatische System-Meldungen

| | Fälligkeitsanzeige | Mahnung | Abweichungsmeldung | Änderungsanträge |
|--------------|---|---|---|--|
| Empfänger | Verantwortlicher und Stellvertretung | Verantwortlicher und Stellvertretung / Vorgesetzter | Vorgesetzter / Prozessverantwortlicher | Vorgesetzter / Moduladministrator |
| Beschreibung | Informiert Verantwortliche über eine fällige Durchführungsmeldung | Informiert Verantwortliche über eine überfällige Durchführungsmeldung. Ab einer definierten Mahnstufe geht die Information auch an den Vorgesetzten / Prozessverantwortlichen | Bei Abweichungen (Vorgabe nicht oder nur teilweise eingehalten) wird der Vorgesetzte automatisch informiert | Änderungen im Prozess können durch den Verantwortlichen oder die Stellvertretung initiiert werden. |

Fälligkeitsanzeige

Beispiel einer automatischen Email (Fälligkeitsanzeige) an Verantwortlichen:



IV Corporate Assurance - Notification

Compliance Notification Responsible

This is a notification email for compliance reports which are due shortly.

| Module | Process ID | Ongoing number | Name | Unit | Responsible | Substitute |
|------------------------------|------------|----------------|---------------------------|-----------|--------------|------------|
| Compliance / Data protection | Ua03 | [3] | Löschung Arbeitszeugnisse | T IV Test | Simon Bislin | |

Please use the link below to submit the data.



Systemdemo

- Erfassen einer Durchführungsmeldung



Process Control (Compliance /
Data protection)



Abweichungsmeldung

Beispiel einer automatischen Email (Abweichungsmeldung) an Verantwortlichen:

IV Corporate Assurance - Notification

Message needs attention (Module Trigger)

The following answer went below the trigger point (points):

Corrective action taken:

Deviation reported to responsible person (10)

The following answer exceeded the trigger point (points):

Compliance with standards:

mainly compliant (90)

The user *Simon Bislin* entered data which needs special attention.

| | |
|----------------------|---|
| Module: | Compliance / Data protection |
| Unit: | T IV Test |
| ID: Number: | 1601 |
| Process ID: | Ua03 Employee performance |
| Name: | Löschung Arbeitszeugnisse |
| Ongoing number: | 3 |
| Creator: | Simon Bislin |
| Assessor Compliance: | Simon Bislin |
| Overall Responsible: | Simon Bislin |
| Period: | October 2012 - September 2013 |
| Reporter: | Simon Bislin |
| Comment: | Arbeitszeugnisse werden nach Abschluss der Verfahren nach Rücksprache mit der Rechtsabteilung gelöscht. |

Reporting I

Mit der Reportingfunktion lassen sich Auswertungen erstellen z.B. über aktuell aktive technische und organisatorische Massnahmen oder auch über die Rückmeldungen, ob die Vorgaben eingehalten worden sind (self assessment).

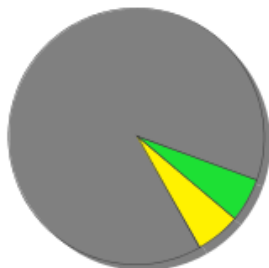
Total Meldungen: 18  Drei Grafiken pro Seite ▼

Einhaltung der Vorgaben



■ voll erfüllt 88.9%
■ überwiegend erfüllt 5.6%
■ nur teilweise erfüllt 5.6%

Potentielle Kosten bei Nicht-Einhaltung



■ N/A 88.9%
■ Wesentliche Kosten auf Unit beschränkt 5.6%
■ Unwesentliche Kosten nur bei der Unit 5.6%

Getroffene Massnahme




■ N/A 88.9%
■ nichts gemacht 5.6%
■ Meldung an die verantwortliche Person 5.6%

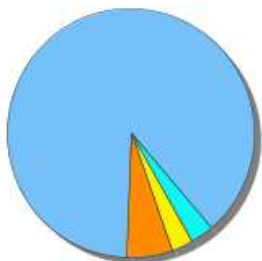


Reporting II

Beispielbericht über alle Datenschutz-Massnahmen in einer Geschäftseinheit.

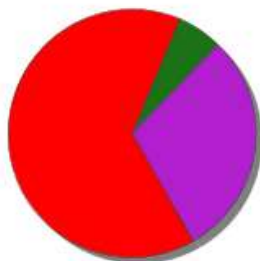
Total Compliance Themen: 34  Drei Grafiken pro Seite




Meldezyklus



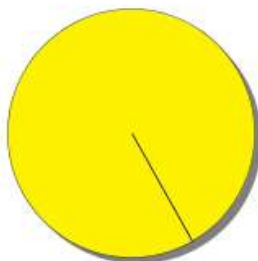
| | | |
|---|---------------|-------|
|  | quartalsweise | 2.9% |
|  | halbjährlich | 5.9% |
|  | jährlich | 88.2% |
|  | alle 2 Jahre | 2.9% |

Kontrollhäufigkeit



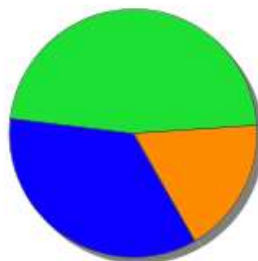
| | | |
|---|---------------|-------|
|  | transaktional | 64.7% |
|  | halbjährlich | 5.9% |
|  | jährlich | 29.4% |

Compliance-Kategorie



| | | |
|---|-------------|--------|
|  | Datenschutz | 100.0% |
|---|-------------|--------|

Datenschutzziel



| | | |
|---|-------------------------------------|-------|
|  | Zugriffskontrolle | 35.3% |
|  | Bestandeskontrolle (Life cycle mgt) | 47.1% |
|  | Auskunftsrecht gewährleisten | 17.6% |

Massnahmentyp



| | | |
|---|--|-------|
|  | Information | 5.9% |
|  | Schulung | 2.9% |
|  | Kontrolle | 8.8% |
|  | Technische Massnahme (Systemeinstellung) | 47.1% |
|  | Org Massnahme (4-A-P) | 23.5% |
|  | Dokumentation | 11.8% |

Fazit

- Einmaliger Aufwand für Inventur der Datensammlungen und Dokumentation der technischen und Organisatorischen Massnahmen
- Die Einführung der GRC Software im Datenschutz hat die Datenbankverantwortlichen auf Risiken sensibilisiert und das Verantwortungsbewusstsein für die technischen und organisatorischen Schutzmassnahmen gestärkt.
- Benutzerfreundlich, hohe Akzeptanz bei den Mitarbeitern
- Auch bei personellen Wechsln ist sichergestellt, dass Datenschutzvorgaben eingehalten werden.
- Durch integriertes Change Management ist sichergestellt, dass das System laufend an die aktuellen Gegebenheiten angepasst wird





Vielen Dank.

Simon Bislin

Ivoclar Vivadent AG

Corporate Risk Manager

simon.bislin@ivoclarvivadent.com

www.ivoclarvivadent.com

