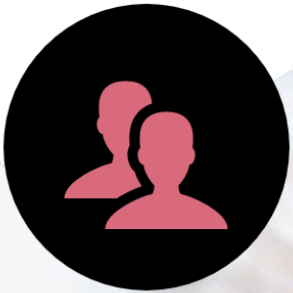


ISMS Implementierung nach ISO 27001

DVT Daten-Verarbeitung-Tirol GmbH
georg.kraler@tirol.gv.at

Über die DVT



- Gründung 1997 durch Auslagerung der IT per Landesgesetz
- Zentraler IT-Dienstleister der Tiroler Landesregierung (<https://www.dvt.at/>)
- 90+ Mitarbeiterinnen

DVT in Zahlen



- Firmenstandort und 2 gleichwertige Rechenzentren
 - 500 virtuelle und physische Server
 - 12.000 PCs, Drucker und Telefone im Netzwerk
- 400+ IT-Services
 - 70 Eigenentwicklungen mit Portaleinbindung (<https://portal.tirol.gv.at>)
 - Tiroler Schulnetz
 - Tiroler Gemeindenetz



ISMS IMPLEMENTIERUNG

Ein Blick zurück...

2011

- Erste Überlegungen / Analysen zur ISO 27001 (Kontrollziele)
- Prozesslandkarte in Anlehnung an ITIL v3

2015

- GAP Analyse wird von externem Consultant durchgeführt.
- Hohe technische Reife – organisatorisch Verbesserungspotenzial

2016

- Risikomanagement mit CRISAM wird eingeführt (BIA relevanter IT-Services & Schwachstellenanalyse der Infrastruktur).

2017

- Kick-Off Besprechung für ISMS Projekt mit Zertifizierungsziel Ende 2017

März

- ISMS Framework ist definiert (notwendige Inhalte) und Zertifizierung durch OCG im Q4/2017 wird beauftragt.

Juli

- Entwürfe für Richtlinien und Prozesse liegen vor. Redaktionssitzungen zur finalen Diskussion und Freigabe sind terminiert.

Aug

- BCM definiert und erster Notfalltest wird durchgeführt: Rechenzentrumsausfall

Sept

- Alle relevanten Richtlinien und Prozesse sind aktuell und freigegeben. ISMS Schulung aller DVT Mitarbeiter werden durchgeführt.

Nov

- Zertifizierungsaudit (Dokumenten & Konformitätsaudit) durch die OCG und Zertifikatsverleihung im Dezember 2017

Argumente für ein zertifiziertes ISMS

- Transparente Arbeitsabläufe und standardisierte Prozesse.
- Awareness hinsichtlich Informationssicherheit steigern.
- Reduktion möglicher Haftungsrisiken.
- EU-DSGVO stützt sich auf ein aktives Risikomanagement.
- Marktsituation (6 von 9 Bundesländer sind bereits zertifiziert)

Überlegungen vor Projektstart

- Definition des Geltungsbereiches (Scope)?
- Welche (Mitarbeiter)Ressourcen werden für die ISMS Implementierung / Betrieb benötigt?
- Wie können die Normanforderungen effizient umgesetzt werden?

DVT ISMS Scope Definition

Der **Geltungsbereich** des ISMS umfasst **alle Organisationsbereiche** der DVT Daten-Verarbeitung-Tirol GmbH inkl.

- dem Bürostandort in Innsbruck,
- den Rechenzentren in Hall und Innsbruck.

Grenzen des ISMS:

- Standorte des Landes Tirol sind nicht Teil des ISMS.
- Dezentrale Standorte und kleine Außenstellen (Bezirkshauptmannschaften, Straßenmeistereien) sind nicht Teil des ISMS.

DVT ISMS - 4 Säulen

ISMS- Dokumentation

DVT Wiki

Leitlinie

Org.
Richtlinien

Technische
Richtlinien

Geschäfts- prozesse

DVT Wiki

Management-
prozesse

Kernprozesse

Unterstützungs-
prozesse

ISMS- Umsetzung

CRISAM

BIA

Risiko Analyse

Risiko
Steuerung

Awareness

IT-Notfall- management

DVT Wiki

Vorsorge

Übungen

Bewältigung

Viele technische Voraussetzungen waren bereits vorhanden:

- Zentrale Rechteverwaltung
- Zentrale Servicedokumentation

Organisatorische Unterstützung (ITIL nahe Prozesslandschaft)

- Change Management
- Service Desk

Projektverlauf

- Bereits bei Projektstart wurde das Zertifizierungsdatum fixiert.
- Gefahr sich in Detail-Diskussionen zu verlieren ...
- Absolute Unterstützung durch die GF

ZERTIFIKAT

für das

Information Security Management System nach ISO/IEC 27001:2013

Die Österreichische Computer Gesellschaft (OCG) bescheinigt hiermit die regelkonforme Anwendung und Weiterentwicklung eines Informationssicherheits-Managementsystems (ISMS) gemäß ISO/IEC 27001:2013 für

zertifizierte Organisation:



DVT-Daten-Verarbeitung-Tirol GmbH
Adamgasse 22, 6020 Innsbruck

zertifizierte Standorte und Geltungsbereiche:

Alle Organisationsbereiche der DVT Daten-Verarbeitung-Tirol GmbH inklusive der kunden- und betriebsrelevanten Geschäftsprozesse, an dem Firmenstandort in Innsbruck sowie den Rechenzentrumstandorten in Innsbruck und Hall in Tirol.

Datum der Erstzertifizierung: 18.12.2017

Gültigkeit bis: 17.12.2020

Zertifikats-Nr.: 004/1_2017

Für die Zertifizierungsstelle der Österreichischen Computer Gesellschaft (OCG)

Wien, 18. Dezember 2017
Ort, Datum



Dipl.-Ing. Wilfried Seyruck
OCG-Präsident

Die OCG ist von der „Akreditation Austria“ seit 5.7.2013 gemäß ISO/IEC 17021-1:2015 und ISO/IEC 27006:2015 als Zertifizierungsstelle für Managementsysteme mit der Identifikationsnummer 0348 für Managementzertifizierungsverfahren nach der Norm ISO/IEC 27001 akkreditiert.



Danke