CISIS12 ®
Ihr Einstieg in die Informationssicherheit

it-sa 2022
Nürnberg, 26.10.2022

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

Manuela Feese-Zolotnitski

Zertifizierte T.I.S.P. TeleTrust Information Security Professional
Zertifizierte CISIS12 Information Security Officer (IT-Sicherheitscluster e. V.)
Zertifizierte Datenschutzbeauftragte (TÜV, GDD)
Diplom-Ingenieurin (BA) für Technische Informatik, Dipl. sc. pol. Univ.

Telefon 089 2868 5140

Mobil 0176 100 86 5 46
Telefax 089 2868 3155
mfeese-zolotnitski@gv-bayern.de

Genossenschafts-Treuhand Bayern GmbH /
Genossenschaftstreuhand Wirtschaftsprüfungsgesellschaft mbH
Türkenstraße 22-24
80333 München

Unsere Leistungen

Prüfung

Beratung

Bildung

Interessenvertretung

Unser Netzwerk

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

Wer ist die GTB?

- **Tochtergesellschaft des Genossenschaftsverbandes Bayern e.V.**
- erbringt Dienstleistungen für Organisationen der Privatwirtschaft und des öffentlichen Sektors
- Die GTB ist somit **eine der größten Outsourcing-, Beratungs- sowie Prüfungsdienstleisterinnen in Deutschland**.

Ein Auszug unserer Dienstleistungen

Auslagerung des Datenschutz-beauftragten

Auslagerung des Informations-sicherheits-beauftragten

Beratung zum Aufbau von Managementsystemen hinsichtlich Datenschutz, Informationssicherheit, Notfallmanagement

Unterstützung der Innenrevision

Durchführung von Prüfungsaufträgen

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

Wo wirkt die GTB mit?

`

GDD MITGLIED
Gesellschaft für Datenschutz und Datensicherheit e.V.

Allianz für Cyber-Sicherheit
Partner

IDW
INSTITUT DER WIRTSCHAFTSPRÜFER

DATEV
Mitglied

ITSECURITY

IT-Sicherheitscluster e.V.

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

Zweck:
Förderung der Weiterentwicklung und Erforschung von Datenschutz, IT-Sicherheit und Informationssicherheit.

Gründung:

- 2006 als Netzwerk (Cluster) in Regensburg
- 2017 IT-Sicherheitscluster e.V.
- 2022 ca. 140 Mitglieder
  (Unternehmens aus dem Bereich IT-Sicherheit, Hochschulen, Kommunen, ohne Bezug)

Mitglieder:

- Unternehmen der IT-Wirtschaft
- Anwender
- Forschungs- und Weiterbildungseinrichtungen
- Juristen

IT-Sicherheitscluster e.V.

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

Aktivitäten

- Arbeitskreise & Gremien:
  - Arbeitskreis betrieblicher Datenschutzbeauftragter
  - Arbeitskreis der Informationssicherheits-Beauftragten
- Weiterbildung:
  - Zertifikatslehrgang zum Informationssicherheits-Beauftragten
  - Seit 2021 Workshops zu Themen, wie IT-Recht, Projektmanagement, IT-Security
- Regelmäßige Veranstaltungen
  - 2023 2. Regensburger Cybersecurity-Kongress, 4. Regensburger Datenschutz Kongress
  - Mitwirkung bei it-sa und Kommunale
  - Kooperationsveranstaltungen und Austausche
  - Informationsveranstaltungen zu CISIS12

CISIS12

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

Etablierung als Standard:

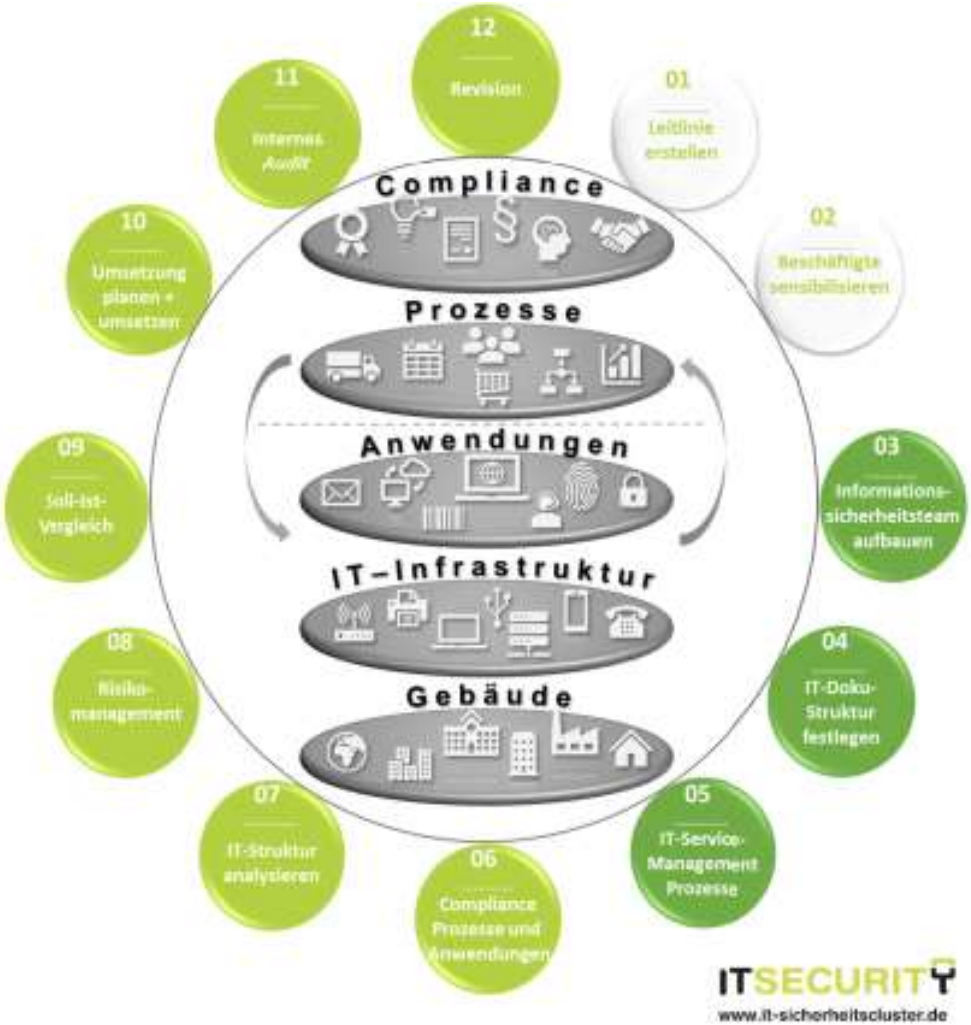
- Über 400 (C)ISIS12-Beratungsprojekte
- Über 300 genehmigte Förderanträge
- 180 Zertifizierungen und Begutachtungen
- 74 zertifizierte Berater

CISIS12 - Überblick

- Nachfolger von ISIS12
- Neuerungen:
  - Einführung Projektmanagement
  - Compliance
  - Risikomanagement
  - Revision
  - Verbesserung der Struktur
    - Norm, Maßnahmen, Audit
    - Verweise zu ISO27001/BSI
  - Software

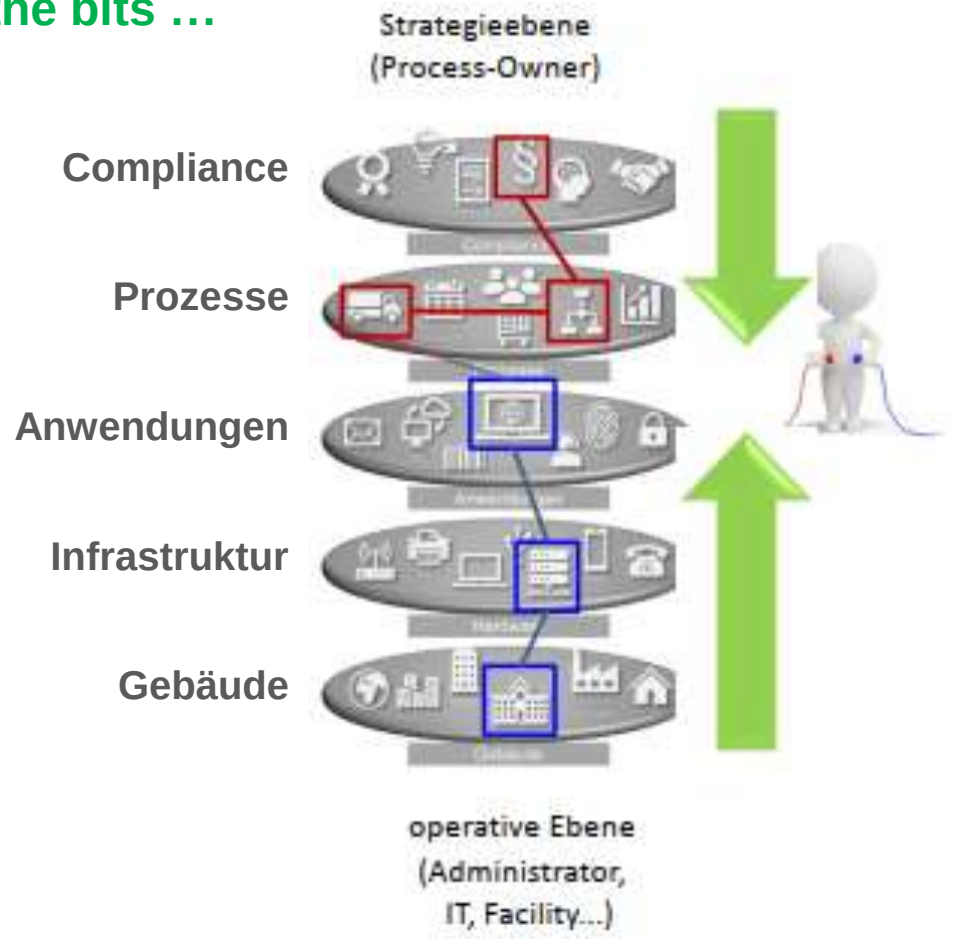
CISIS12 - Compliance

- Compliance-Ebene:
  interne / externe Vorgaben
- Durch die Leitungsebene in Prozessen berücksichtigt
- Umsetzung auf Systemebene (Anwendungen, Infrastruktur, Gebäude)
- Zyklische Verbesserung (PDCA)



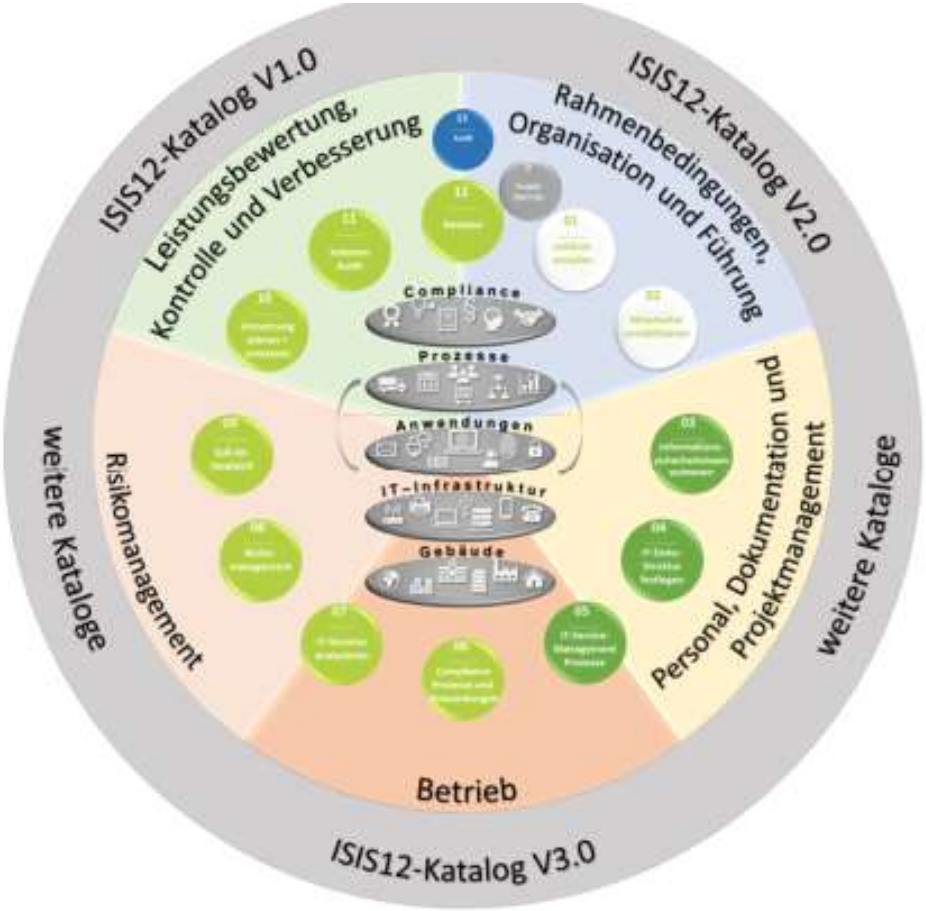
Connecting the bits …

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH



CISIS12 - Compliance

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH



Zielgruppen und Umfang

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

Kriterium	CISIS12	VdS10000	ISO27000x	BSI IT-Grundschutz
Herausgeber	IT Sicherheitscluster e.V.	VdS Schadensverhütungs GmbH	International Standardisation Organisation	Bundesamt für Sicherheit in der Organisationstechnik
Zielgruppen	Kleine und mittlere Organisationen	Kleine und mittlere Organisationen	Organisationen jeder Größenordnung	Bundesamt für Sicherheit in der Organisationstechnik
Dokumentation	Ca. 40 Seiten + (2022)	Ca. 40 Seiten	Ca. 30 Seiten +	Ca. 4.800 Seiten (2016)
Detaillierung	Mittel		abstrakt	Maximal detailliert

Quelle:
Deutscher Landkreistag, Handreichung zur Ausgestaltung der Informationssicherheitsrichtlinie in Kommunalverwaltungen (2015); eigene Anpassungen (2022)

CISIS12 --- konkretisiert Begriffe aus der Norm

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

CISIS12	ISO27001
4.7.2 Leitlinie / Formalien	--
Ferner **MUSS** die Leitlinie	Die Informationssicherheitspolitik muss:
in entsprechender Form (schriftlich oder digital) verfügbar sein,	e) als dokumentierte Information verfügbar sein;
von der Leitungsebene unterschrieben werden,	
bei Bedarf für weitere Zielgruppen verfügbar gemacht werden.	g) für interessierte Parteien verfügbar sein, soweit angemessen.

CISIS12 --- ergänzt Textteile zum erleichterten Verständnis

GTB Wirtschaftsprüfungsgesellschaft Wissenschafts-Treuhand Bayern GmbH

CISIS12	ISO27001
4.8 Aufgaben, Rechte und Pflichten von Rollen	**5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation**
Die Leitungsebene MUSS nachstehende Rollen mit entsprechenden Aufgaben, Rechten und Pflichten benennen. Hierzu gehören: • Informationssicherheitsbeauftragter (ISB); • IT-Verantwortliche; • Administratoren; • Benutzer.	Die oberste Leitung muss sicherstellen, dass die Verantwortlichkeiten und Befugnisse für Rollen mit Bezug zur Informationssicherheit zugewiesen und bekannt gemacht werden. Die oberste Leitung muss die Verantwortlichkeit und Befugnis zuweisen für:
Die Leitungsebene **MUSS** für eine entsprechende Aufgabentrennung der einzelnen Rollen sorgen. In kleineren Organisationen **KANN** eine Personalunion durch entsprechende Argumentation gerechtfertigt werden.	a) das Sicherstellen, dass das Informationssicherheitsmanagementsystem die Anforderungen dieser Internationalen Norm erfüllt; und

CISIS 12 --- ergänzt Textteile aus Praxiserfahrung heraus

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

CISIS12	ISO27001
4.7.2 Leitlinie / Formalien	--
Ferner **MUSS** die Leitlinie	Die Informationssicherheitspolitik muss:
in entsprechender Form (schriftlich oder digital) verfügbar sein,	e) als dokumentierte Information verfügbar sein;
von der Leitungsebene unterschrieben werden,	--

Umsetzung der Maßnahmen

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

Kriterium	CISIS12	VdS10000	ISO270001	BSI IT-Grundschutz
Aufbau	Selektierte Bausteine und Maßnahmenkataloge		Maßnahmenempfehlungen	Umfassende Bausteine
Maßnahmen	ca. 400		ca. 150	ca. 1.500
Umsetzung	Konkret formulierte Maßnahmen umsetzen		allgemein gültig formulierte Maßnahmen umsetzen	Konkret formulierte Maßnahmen umsetzen

Quelle:
Deutscher Landkreistag, Handreichung zur Ausgestaltung der Informationssicherheitsrichtlinie in Kommunalverwaltungen (2015); eigene Anpassungen (2022)

Beispiel: CISIS12 Maßnahme (I)

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

Ebene: **ISMS-Prozess**	Relevanz: **MUSS**
Baustein: B2.060 - Aufbau einer Sicherheitsorganisation	
Maßnahmennummer - Maßnahmenbeschreibung: **B2.060-M020 - Rollendefinition innerhalb der ISMS-Organisation**	
Maßnahmenanforderung: **Innerhalb dieser Organisationssktruktur MÜSSEN die entsprechenden Rollen definiert werden.**	
Umsetzungshinweise: Diese Rollen sind für den Aufbau, die Etablierung des Informationssicherheitsmanagementsystems und die Erreichung der Sicherheitsziele verantwortlich. - Informationssicherheitsbeauftragter - ggf. Datenschutzbeauftragter - IT-Verantwortlicher	
Verantwortlicher: **Leitungsebene**	

Beispiel: CISIS12 Maßnahme (II) vs. ISO27001-Maßnahme

GTB Wirtschaftsprüfungsgesellschaft
enossenschafts-Treuhand Bayern GmbH

Referenzen:

ISO/IEC 27001:

A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.5, A.8.1.1, A.8.2.1, A.8.2.2, A.18.2.1

BSI Grundschutz 15. Ergänzungslieferung 2016

BSI 100-2, M 2.335, M 2.338, M 2.199, M 2.237, M 2.250, M 2.226, M 3.5, M 3.96, M 2.139, M 2.195, M 2.217

BSI Kompendium

ISMS.1

ISO27001 Maßnahme (Auswahl)

A.8 Verwaltung der Werte

A.8.1 Verantwortlichkeit für Werte

Ziel: Die Werte der Organisation sind identifiziert und angemessene Verantwortlichkeiten zu ihrem Schutz sind festgelegt.

A.8.1.2	Zuständigkeit für Werte	*Maßnahme* Für alle Werte, die im Inventar geführt werden, gibt es Zuständige.

A.8.2 Informationsklassifizierung

Ziel: Es ist sichergestellt, dass Information ein angemessenes Schutzniveau entsprechend ihrer Bedeutung für die Organisation erhält.

A.8.2.1	Klassifizierung von Information	*Maßnahme* Information ist anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert.

Beispiel: CISIS12 Maßnahme (III) vs. BSI-Maßnahme

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

BSI Maßnahme (Auswahl)

ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit [Institutionsleitung] (B)

Eine geeignete übergreifende Organisationsstruktur für Informationssicherheit MUSS vorhanden sein. Dafür MÜSSEN Rollen definiert sein, die konkrete Aufgaben übernehmen, um die Sicherheitsziele zu erreichen. Außerdem MÜSSEN qualifizierte Personen benannt werden, denen ausreichend Ressourcen zur Verfügung stehen, um diese Rollen zu übernehmen. Die Aufgaben, Rollen, Verantwortungen und Kompetenzen im Sicherheitsmanagement MÜSSEN nachvollziehbar definiert und zugewiesen sein. Für alle wichtigen Funktionen der Organisation für Informationssicherheit MUSS es wirksame Vertretungsregelungen geben.

Kommunikationswege MÜSSEN geplant, beschrieben, eingerichtet und bekannt gemacht werden. Es MUSS für alle Aufgaben und Rollen festgelegt sein, wer wen informiert und wer bei welchen Aktionen in welchem Umfang informiert werden muss.

Es MUSS regelmäßig geprüft werden, ob die Organisationsstruktur für Informationssicherheit noch angemessen ist oder ob sie an neue Rahmenbedingungen angepasst werden muss.

Risikoanalyse

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

Kriterium	CISIS12	VdS10000	ISO270001	BSI IT-Grundschutz
Risikoanalyse	grundsätzlich		grundsätzlich	ergänzend

Quelle:
Deutscher Landkreistag, Handreichung zur Ausgestaltung der Informationssicherheitsrichtlinie in Kommunalverwaltungen (2015); eigene Anpassungen (2022)

Zertifizierung, Akkreditierung

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

- Teil einer **Konformitätsbewertung**
- Vergabe durch Zertifizierungsstellen, evtl. akkreditiert:
  - Akkreditierung: **Bestätigung der Fachkompetenz**, bestimmte Konformitätsbewertungsaufgaben durchzuführen

Zertifizierung

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

Kriterium	CISIS12	VdS10000	ISO270001	BSI IT-Grundschutz
Name der Zertifizierung	CISIS12	VdS10000	ISO27001 (2013)	ISO27001 auf Basis von IT-Grundschutz
Durchführend	ISO27001-zertifizierter Auditor	VdS-Auditor	Zertifizierter ISO27001-Auditor,	Zertifizierter ISO27001-Auditor, zertifiziert vom BSI
Zertifizierungs-stellen	datenschutzCert DQS TÜV Rheinland	VdS Schadensverhütungs GmbH	… und viele mehr	… und viele mehr

Zertifizierung Nutzen

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH

- Intern: Verbesserung der Informationssicherheit
- Externe Kontrolle durch einen Dritten
- Nachweis methodischen Herangehens an Informationssicherheit

- Vertrauensbildend für Geschäftspartner und Kunden
- Voraussetzung für Cyber-Versicherungen
- Entlastung im Ernstfall (persönliche Haftung)


ZERTIFIKAT

Verwaltungsgemeinschaft Neumarkt i.d.OPf.

CISIS12

DQS GmbH

GTB - Genossenschafts-Treuhand Bayern GmbH
Wirtschaftsprüfungsgesellschaft
Türkenstrasse 22 - 24
80333 München

gtb@gv-bayern.de
www.genossenschafts-treuhand.de

GTB Wirtschaftsprüfungsgesellschaft
Genossenschafts-Treuhand Bayern GmbH