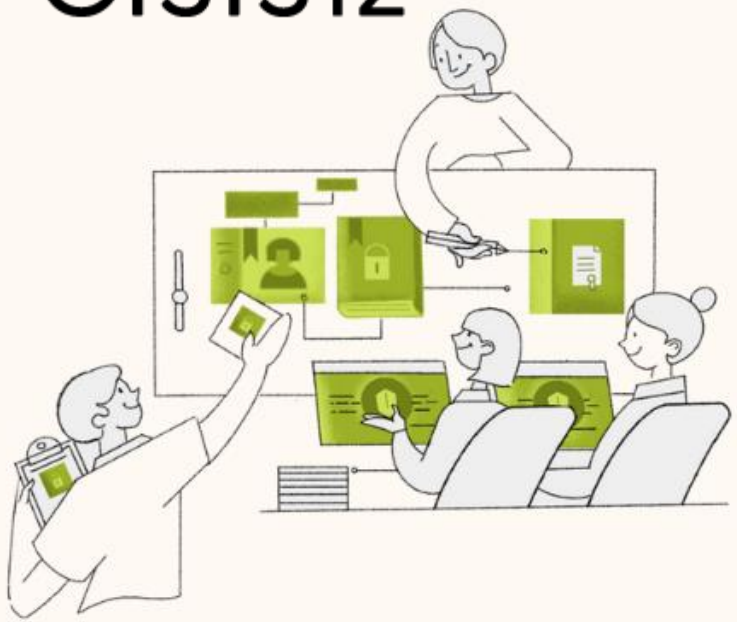
Compliance im Griff

mit

CISIS12



IT-Sicherheitscluster e. V. | Franz-Mayer-Straße 1 | D-93053 Regensburg

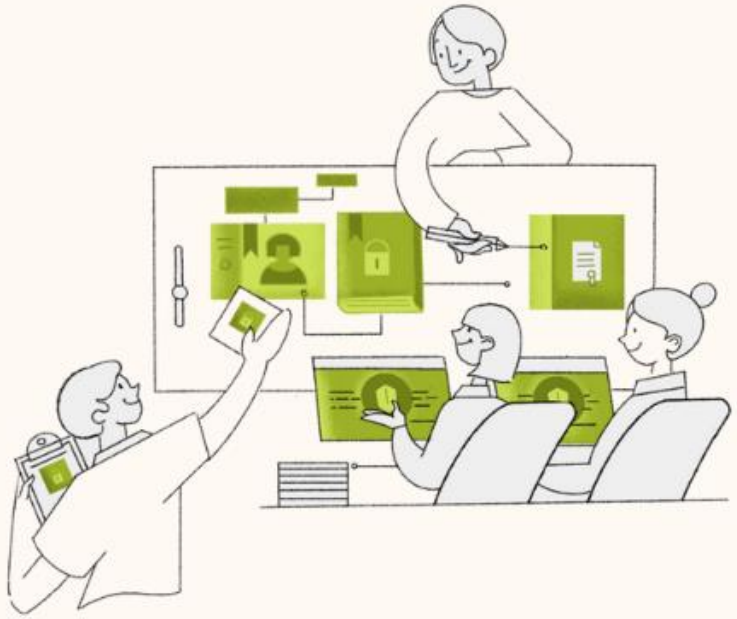
Was ist was?

01 Was ist das IT-Sicherheitscluster?

02 Was ist CISIS12?

03 Welche Rolle spielt Compliance bei CISIS12?

1. Was ist das Cluster?



Der IT-Sicherheitscluster e. V.

ITSECURITY
www.it-sicherheitscluster.de

Zirka 130 Mitglieder, darunter Hochschulen, Beratungsunternehmen, KMU, aber auch größere Organisationen.

Gegründet aus städtischer Cluster-Initiative in Regensburg, seit 2013 Verein.

Ziele:

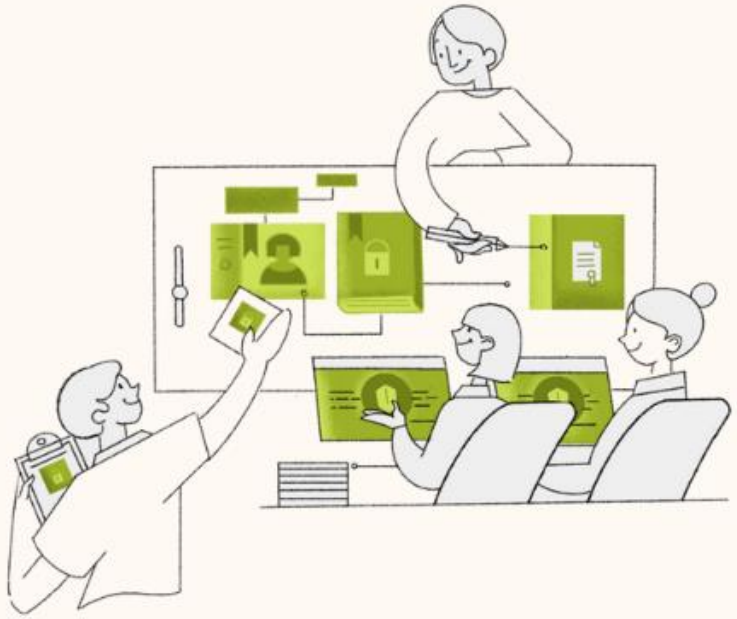
- Bündelung der IT-Sicherheits-Kompetenz,
- Förderung der Erforschung, Entwicklung, Anwendung und Vermarktung von Produkten der IT-Security,
- Unterstützung im Bereich Aus- und Weiterbildung (u. a. Ausbildung zum Informationssicherheits-Beauftragten),
- Initiierung und Begleitung von Kooperationen zwischen Wissenschaft und Wirtschaft im Bereich der IT-Sicherheit,
- Unterstützung der Zusammenarbeit von Einrichtungen und Initiativen zur Förderung der IT-Sicherheit in Unternehmen.

Forschungsförderung: Derzeit drei Projekte, gefördert vom BMBF und ein Projekt im Rahmen von Erasmus+

Veranstalter des jährlichen Regensburger Cybersecurity-Kongresses.
Veranstalter von breitenwirksamen Awareness-Events und Premium-Veranstaltungen für Mitglieder.

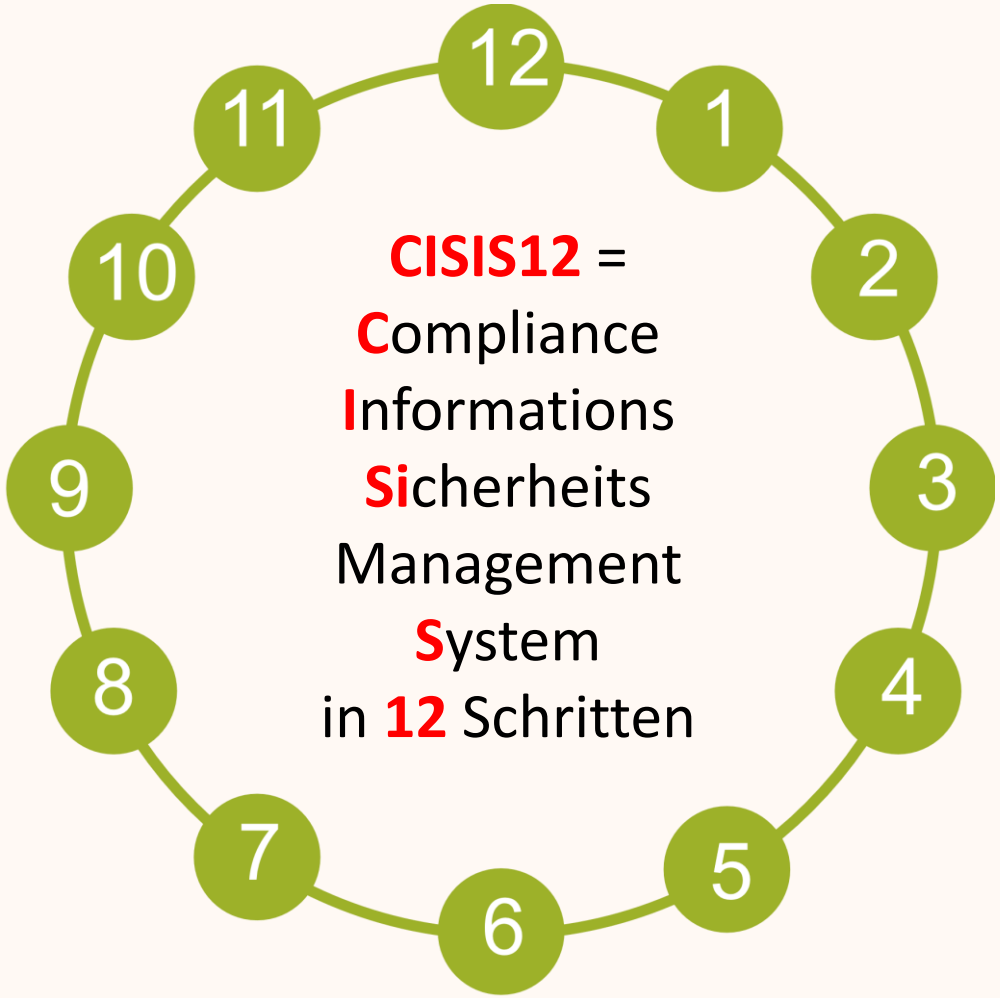
Mitglied im Messebeirat der it-sa, Jurymitglied und Partner des ATHENE up@it-sa Startup Awards. Mitglied im Präsidium des BITMi; Mitarbeit in Fachgremien der European Digital SME-Alliance. Core-Mmitglied in AIR-Regensburg.

2. Was ist CISIS12?

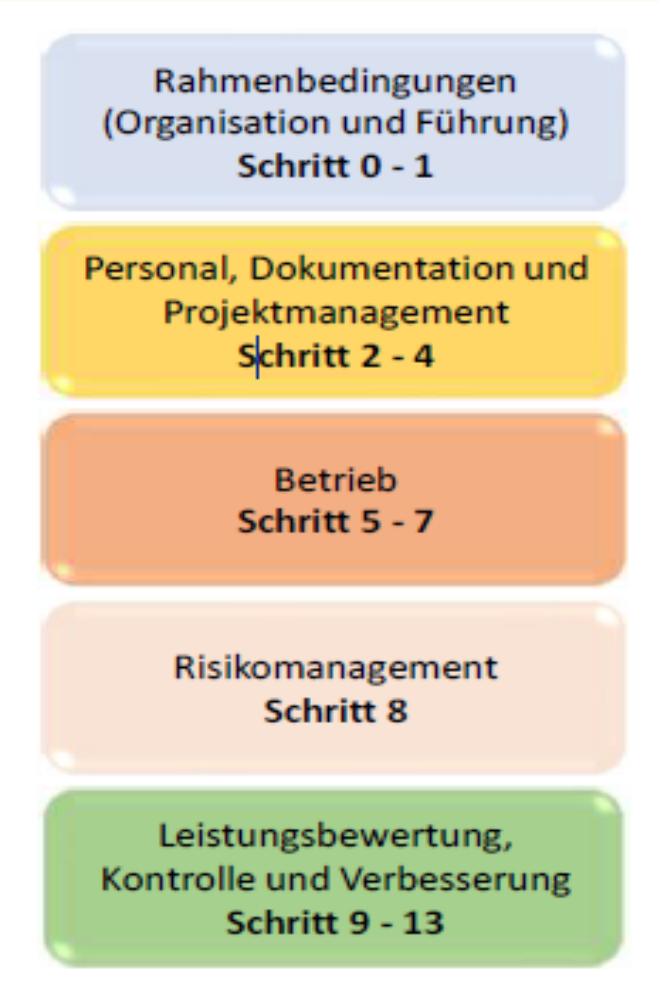


CISIS12 ist…

- ein Informationssicherheitsmanagementsystem in zwölf Schritten,
- branchenunabhängig,
- leichtfüßig,
- besonders gut geeignet für kleine und mittständische Unternehmen (KMU),
- die Weiterentwicklung aus dem bereits gut etablierten Vorgänger ISIS12.
- Folgt dem PDCA-Zyklus,
- ist auditierbar, zertifizierbar.



Zwölf plus zwei Schritte in fünf Phasen



- 00: Startup
- 01: Leitlinie erstellen
- 02: Beschäftigte sensibilisieren
- 03: Informationssicherheitsteam aufbauen
- 04: IT-Dokumentation aufbauen
- 05: IT-Servicemanagement
- 06: Compliance, Prozesse und Anwendungen
- 07: IT-Struktur analysieren
- 08: Risikomanagement
- 09: Soll-Ist-Vergleich
- 10: Umsetzung planen und umsetzen
- 11: Internes Audit
- 12: Revision
- 13: Audit

CISIS12 setzt Schwerpunkte auf:

- Risikomanagement,
- Compliance und zugehörige Prozesse,
- strukturierten Aufbau: Norm, Maßnahmenkatalog, Auditschema,
- liefert Verweise zu relevanten Normen und Maßnahmen-Katalogen aus BSI-IT-Grundschutz und ISO/IEC 27001,
- bietet Integrationsmöglichkeiten von branchenspezifischen Normen und Katalogen, wie TISAX, B3S-KRITIS,
- wird ergänzt durch ein Handbuch, Schulungskonzept,
- umfasst einen Software-Markt mit unterschiedlichen Produkten, darunter Projektmanagement, DSGVO-Modul, Dokumentensteuerung.

Auch das ist CISIS12

- **Über 400** CISIS12-Beratungsprojekte bislang,
- **Über 205** genehmigte Förderanträge (Bayern/Saarland),
- **Über 140** Zertifizierungen und Begutachtungen,
- **Über 70** zertifizierte CISIS12-Berater.

CISIS12 hat sich als Standard etabliert!

Die Ziele von CISIS12

Werte sichern

Vertrauen

Rechtssicherheit schaffen

Akzeptanz

Haftungsrisiko reduzieren

Risiken erkennen

Außenwirkung

Wirtschaftlichkeit

Glaubwürdigkeit

Bedrohungen minimieren

Kompetenz

Wettbewerbsvorteil

Bestandteile von CISIS12

- Norm
- Handbuch
- Maßnahmenkatalog

Ebene:	Relevanz:
Compliance	**MUSS**

Baustein:
B1.010 - Complianceanforderungen

Maßnahmennummer - Maßnahmenbeschreibung:
B1.010-M010 - Complianceanforderungen

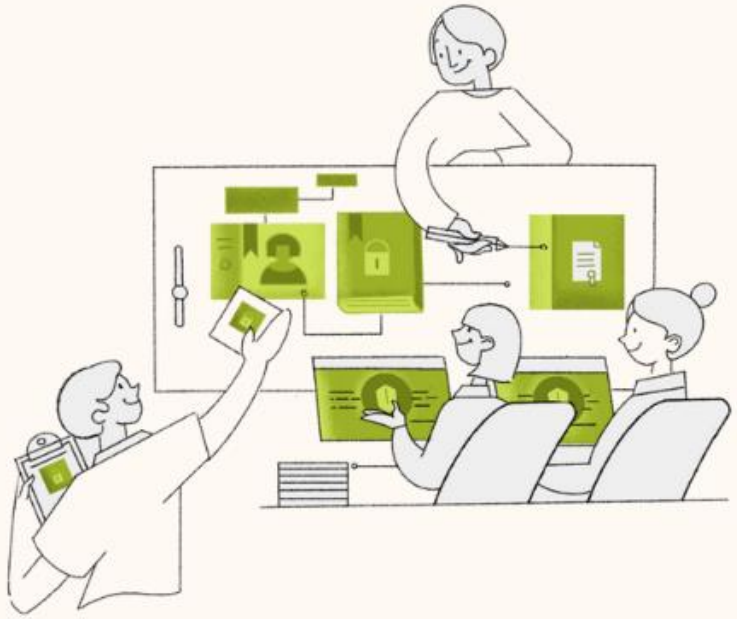
Maßnahmenanforderung:
Die Institution MUSS einen Prozess aufbauen und etablieren, um alle relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben zu identifizieren.

Umsetzungshinweise:
Die Organisation muss ein Compliance- und Stakeholdermanagement aufbauen.

Verantwortlicher:
Leitungsebene, Leitung Compliance, ISB,

Referenzen:
ISO/IEC 27001:
A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5, A.18.2.2
BSI Grundschutz 15. Ergänzungslieferung 2016
B 1.16, M 2.340, M 3.2, B 1.16, M 2.217, M 2.10, M 4.99, B 1.16, B 1.5, M 3.2, M 2.10, M 2.205, M 2.199, BSI 100-2
BSI Kompendium
ORP.5

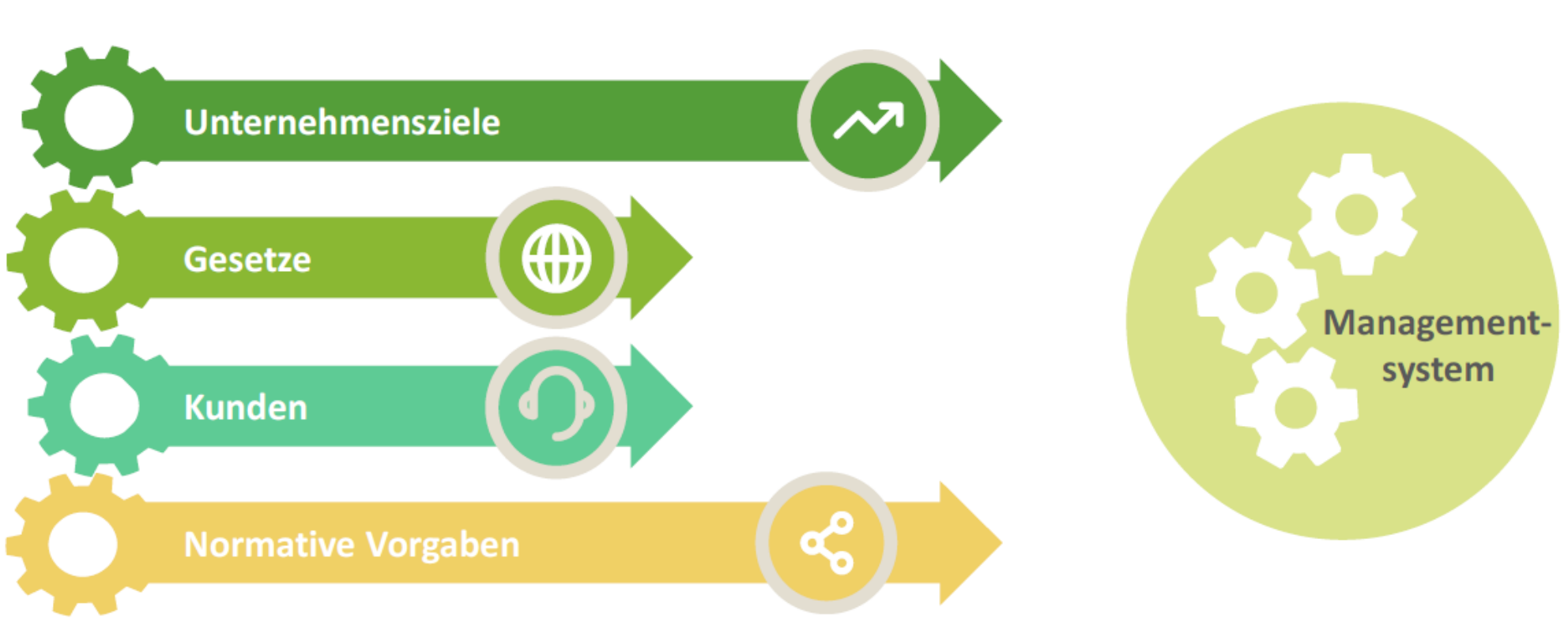
3. Compliance mit CISIS12



Grundlagen Managementsystem

Was ist ein Managementsystem?

Ein Managementsystem ist ein System von Richtlinien, Verfahren, Anleitungen und zugehörigen Betriebsmitteln (inkl. Personal), die zur Erreichung der Ziele einer Organisation erforderlich sind!



Schwerpunkte Governance, Compliance

Governance bedeutet so viel wie „Organisationsverfassung“ und Compliance hingegen bedeutet in etwa „Einhaltung, Befolgung, Übereinstimmung, Einhaltung der Vorgaben“.

Wenn von Governance und Compliance die Rede ist, verschwimmen inhaltlich oftmals die Grenzen, weil es bisher keine einheitlichen Definitionen gibt.

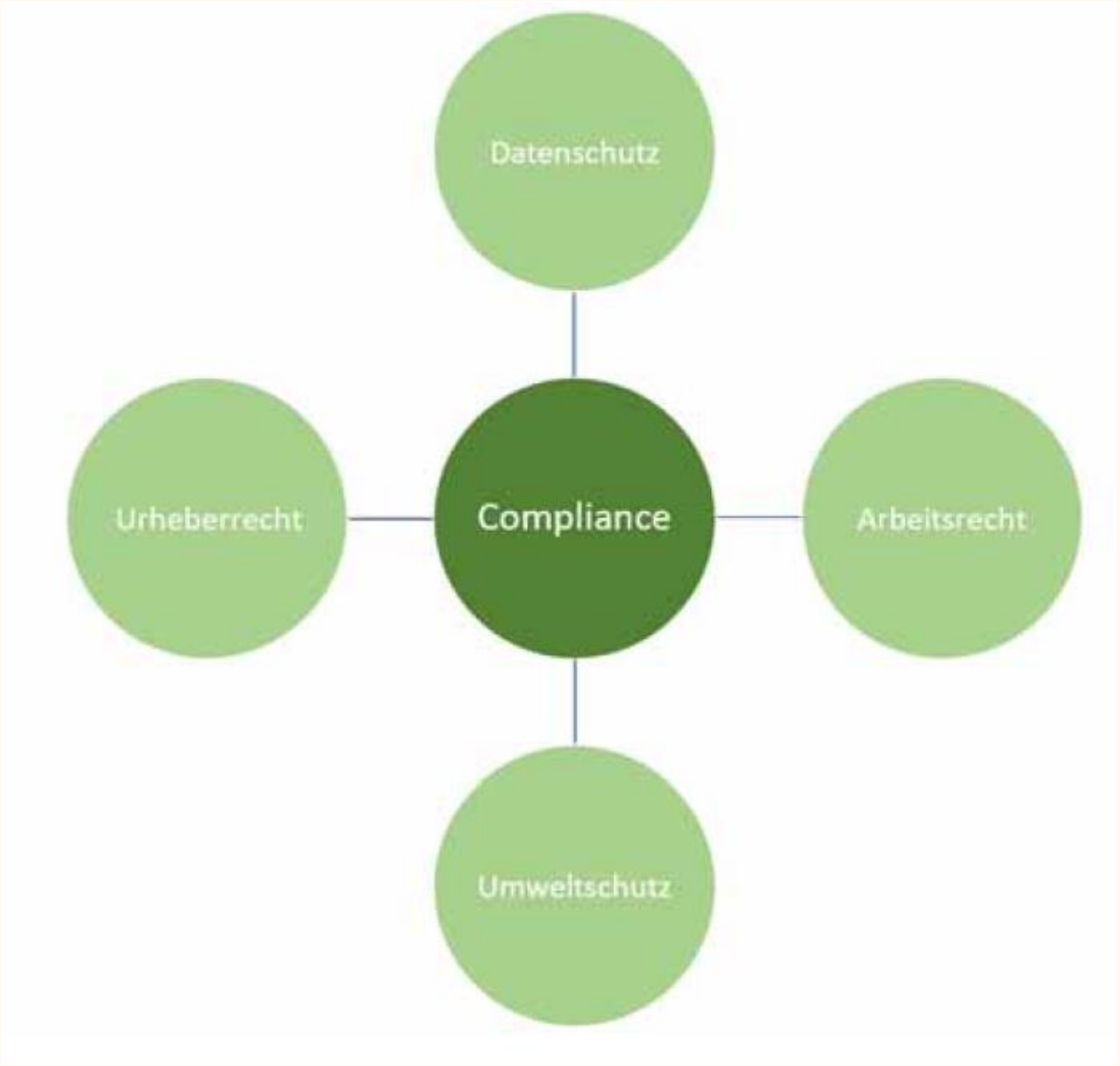
Auch der Bereich Compliance beschäftigt sich mit Gesetzen und Vorschriften, die den Ablauf sämtlicher Organisationsprozesse regeln.

Aus diesem Grund fällt die Abgrenzung zur Corporate Governance schwer bzw. werden beide Begriffe oft synonym verwendet.

Compliance, Prozesse und Anwendungen

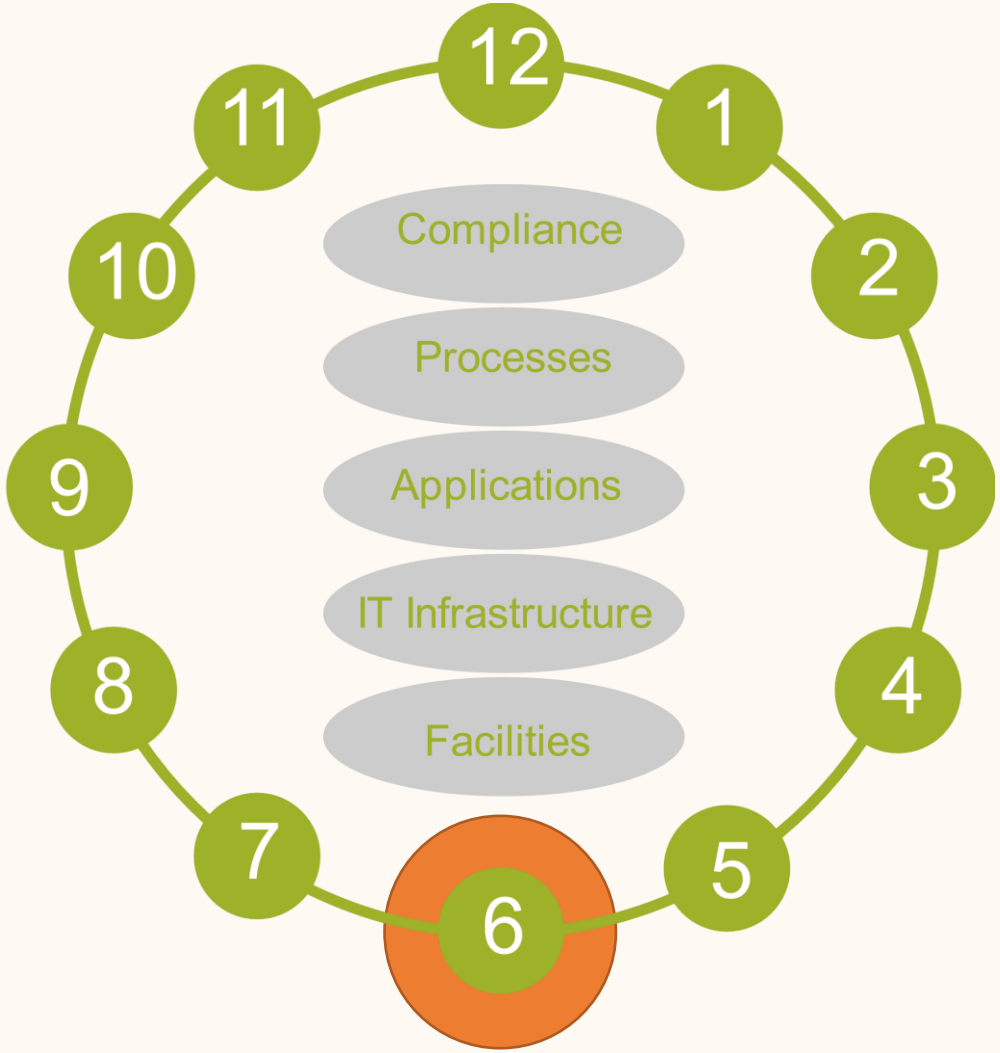
Bestandteile, die in Schritt 6 bearbeitet werden.

Rechtsräume, die von der Informationssicherheit berührt werden:



Schwerpunkt Compliance

- Einführung einer prozessualen Sichtweise zur Compliance-Erfüllung:
  - Die Compliance-Ebene berücksichtigt alle internen und externen Vorgaben.
  - Diese werden verantwortet durch die Leitungsebene und mit entsprechenden Prozessen geplant und entschieden.
  - Die Umsetzung erfolgt in der Systemebene, bestehend aus den Anwendungen, der IT-Infrastruktur und den Gebäuden.
  - Die Schnittstelle zwischen Prozess- und Systemebene bildet die Grundlage eines integrierten Gesamtsystems.
  - Alle Anforderungen werden in übergeordneten PDCA-Zyklen geplant, umgesetzt, kontrolliert und sich daraus ergebende weiter Verbesserungen vorgeschlagen und dokumentiert (Plan-Do-Check-Act).



Schutzbedarfskategorien/-erhebung

CISIS12 definiert A, B, C
A: Begrenzte/überschaubare Schadensauswirkung,
B: Beträchtliche Schadensauswirkung,
C: Existenzielle, bedrohliche oder katastrophale Schadensauswirkung

Konkretisierung der Schadensauswirkung in Schutzbedarfsszenarien:

- Verstoß gegen geltendes Recht und geschlossene Verträge.
- Datenschutz: Beeinträchtigung des informationellen Selbstbestimmungsrechts.
- Finanzielle Auswirkungen.
- Negative Innen- und Außenwirkungen.
- Einschränkung des Handlungsspielraums, Beeinträchtigung der Aufgabenerfüllung.

Schutzbedarfe werden ermittelt (Interviews), dokumentiert, formalisiert (Templates), bestimmt dann durch die Organisationsleitung. Beispiel: Wie hoch ist der Schutzbedarf einer E-Mail-Anwendung in einem Landwirtschaftsbetrieb im Verhältnis zu einem Helpdesk?
Wie hoch darf der MTD (maximal tolerierbare Datenverlust sein)? Oder MTA (maximal tolerierbare Ausfallzeit)? Backup-/Notfallmanagement!

Vielen Dank für Ihre Aufmerksamkeit

Ihr Team des IT-Sicherheitsclusters e. V.

Kontakt
IT-Sicherheitscluster e. V.
Dr. Matthias Kampmann
Franz-Mayer-Straße 1
D-93053 Regensburg
matthias.kampmann@it-sicherheitscluster.de

CISIS12-Kontakt
IT-Sicherheitscluster e. V.
Sandra Wiesbeck
Franz-Mayer-Straße 1
D-93053 Regensburg
sandra.wiesbeck@it-sicherheitscluster.de

Informationen
https://cisis12.de
https://www.it-sicherheitscluster.de