TOM

Zutrittskontrolle
Der physische Zutritt zu Rechenzentren (Serverräumen) muss durch Zutrittskontrolle verhindert werden. Dies ist durch elektrische Zugangssysteme oder mithilfe von Kontrolleuren möglich

Zugangskontrolle
Nur berechtigte Personen dürfen digitalen Zugriff auf die Datenverarbeitungsanlagen erhalten. Dies kann durch Verschlüsselungen, Mehr-Faktor-Authentifizierungen oder strenge Passwortverfahren erfolgen.

Zugriffskontrolle
Durch strenge Berechtigungskonzepte wird sichergestellt, dass unbefugte Dritte keinen Schreib- oder Lesezugang zu sensiblen Daten erhalten. Es muss nachvollziehbar sein, wer welche daten geändert hat.

Weitergabekontrolle
Auch bei der Übertragung muss mithilfe von Verschlüsselung sichergestellt werden, dass Dritte keinen Einblick bekommen können. Hier dürfen unberechtigte Dritte ebenfalls weder die Möglichkeit zum Lesen, Verändern, Kopieren oder zum Löschen der Daten erhalten.

Eingabekontrolle
Durch Protokollierung wird jede Änderung oder Löschung von Daten erfasst und ist so nachvollziehbar

Verfügbarkeitskontrolle
Durch Firewalls und Backups muss Verfügbarkeit sichergestellt werden.
Zudem muss gewährleistet werden, dass die Daten im Verlustfall wiederhergestellt werden können.

Trennungsgebot: Der Einsatz separater Systeme soll gewährleisten, dass für unterschiedliche Zwecke erhobene Daten nur für den jeweiligen Erhebungszweck verwendet werden.

TOM	Datenquellen
Zutrittskontrolle	Cloud, Rechner, interne Systeme, Fileserver
Zugangskontrolle	Grundrisse, Cloud, Datenbestand, Raumplan, Gesamtnetzwerkplan
Zugriffskontrolle	Grundrisse, Cloud, Datenbestand, Raumplan, Gesamtnetzwerkplan
Weitergabekontrolle	Cloud, Datenbestand,
Eingabekontrolle	Grundrisse, Datenbestand, Raumplan, Gesamtnetzwerkplan
Verfügbarkeitskontrolle	Cloud, Datenbestand, Raumplan, Gesamtnetzwerkplan
Trennungsgebot	Backup, Cloud, Datenbestand