Österreichischer Städtebund

SAT- Security Assessment Tool

Mag. Roman Breitfuss
Alexander Leitner BSc MSc

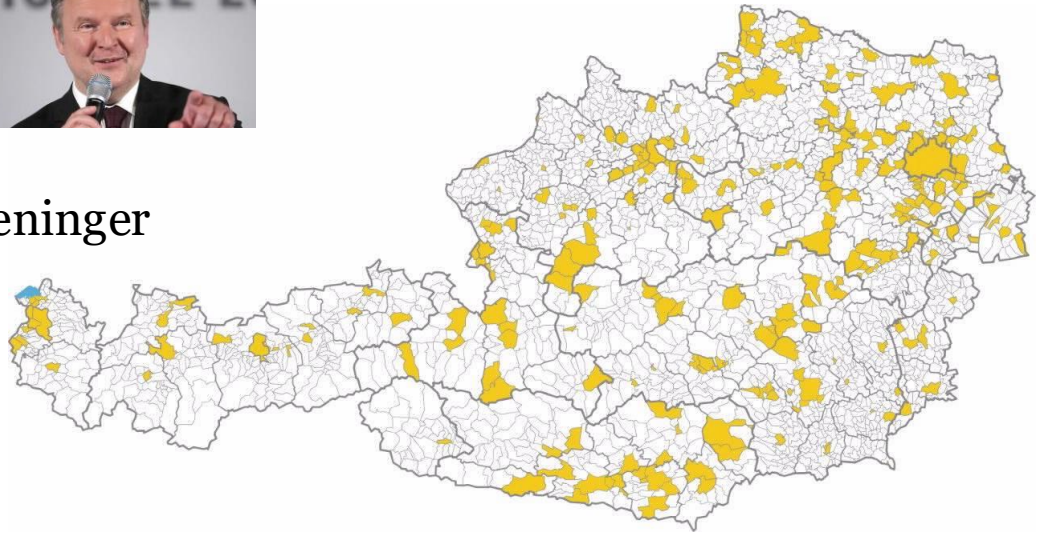
19.6.2024

Österreichischer Städtebund

- 258 Mitgliedsgemeinden,
  ca. 65 % der Bevölkerung

- Präsident Wr. Bürgermeister
  Dr. Michael Ludwig

- Generalsekretär Dr. Thomas Weninger



© Österreichischer Städtebund, Rathaus, A 1082 Wien

Fachausschüsse

- Diskussion über aktuelle Fragen
- Meinungsfindung
- Abgabe von Stellungnahmen zu Gesetzesentwürfen
- Erfahrungsaustausch
- Präsentation erfolgreicher Lösungen

© Österreichischer Städtebund, Rathaus, A 1082 Wien

Fachausschuss IT & Digitalisierung

Österreichischer Städtebund

- Präsidiumssitzungen (4-6 mal jährlich)
- Fachausschüsse mit reger Beteiligung (2 x jährlich)

  Erfahrungsaustausch
  Neuigkeiten aus Österreich und EU
  Berichte zu Spezialthemen (ungeschminkt)
  Umfragen
  Vorlagen (zb Dienstanordnungen)
  etc. etc.
- Schwerpunktprojekte (anlassbezogen)

  Allgemeines Interesse
  Beteiligung besonders interessierter Städte
  (Co-)Finanzierung Städtebund

  zum Nutzen aller Mitglieder

© Österreichischer Städtebund, Rathaus, A 1082 Wien

Von der Idee zur Realisierung

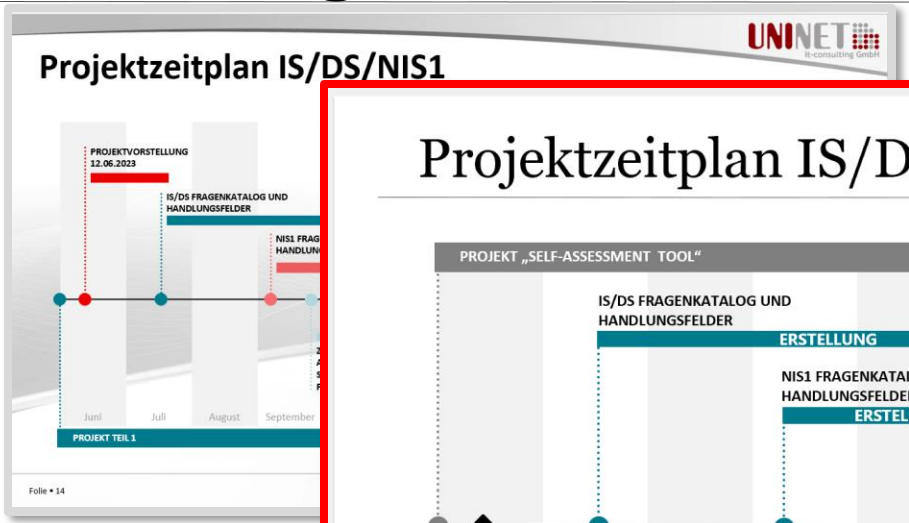
Österreichischer Städtebund

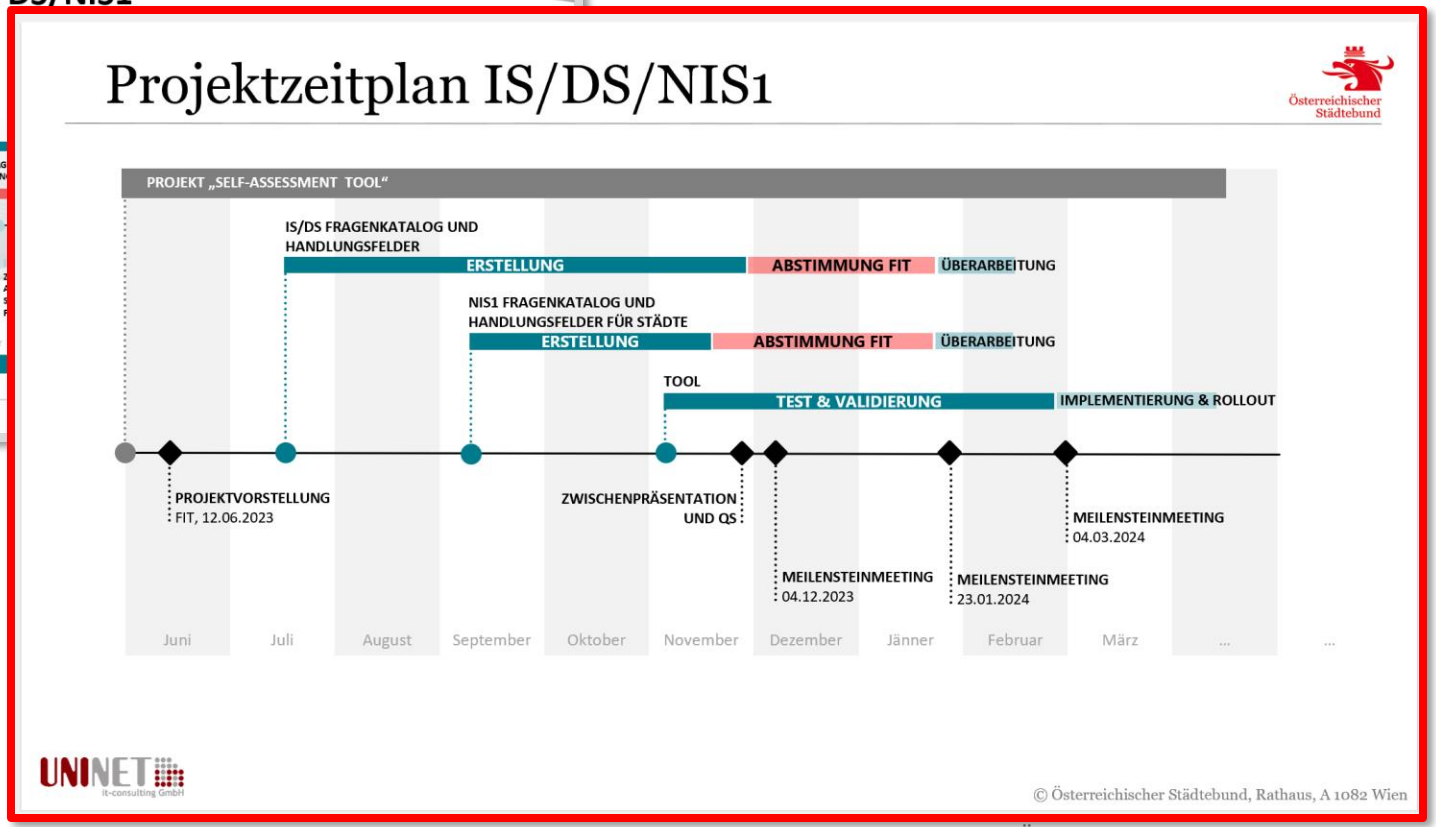
- Cybersecurity-Versicherung
- Check-Liste
- IT-Security
- NIS 2

- Vorbild Datenschutz
  Muster Verfahrenverzeichnisse

© Österreichischer Städtebund, Rathaus, A 1082 Wien

Umsetzung





© Österreichischer Städtebund, Rathaus, A 1082 Wien

SAT – Security Assessment Tool

Österreichischer Städtebund

Elektronisches Self-Assessment Tool zur Bewertung von Maßnahmen im Informationssicherheits- und NIS(2)-Umfeld zur automatisierten Ableitung von Handlungsfeldern

- Tool-Umsetzung in Excel mit Fragen-/Auswertelogik und Berichterstellung

Fragenset

- **Informationssicherheit** | 50 Haupt- und 110 Detailfragen
  - Aufteilung in organisatorische und technische Aspekte
  - Berücksichtigung von anerkannten Normen/Standards
- **NIS** | 53 Haupt- und 146 Detailfragen
  - Aufteilung in 29 Themenbereiche in 11 Kategorien
  - Kategorien entsprechend NISG/NISV und NIS Fact Sheet 9/2022
  - Fragenkaskade für Anwendung des NIS-Fragenkatalogs mit Berücksichtigung von NIS2 nach aktuell verfügbaren Informationen der betroffenen Sektoren/Bereiche

© Österreichischer Städtebund, Rathaus, A 1082 Wien

Informationssicherheit-Fragenkatalog

Österreichischer Städtebund

- Aufteilung in organisatorische und technische Aspekte
- Berücksichtigung von anerkannten Normen/Standards (z.B. ISO/IEC 27001, Österreichisches Informationssicherheitshandbuch, BSI IT-Grundschutz)

1. Organisatorische Aspekte

- 1.1 Informationssicherheitsrichtlinie / -regelungen
- 1.2 Sicherheitsorganisation & Systemlandschaft
- 1.3 Verantwortungsbereiche
- 1.4 Informationssicherheit im Projektmanagement
- 1.5 Asset-Management
- 1.6 IT-Risikomanagement
- 1.7 Mitarbeiter und Mitarbeiterinnen
- 1.8 Zutritts- / Zugangs- / Zugriffsmanagement, Datenträger und Schutzmaßnahmen
- 1.9 Physische Sicherheit
- 1.10 Schulungen
- 1.11 IT-Dokumentation und Informationsklassifizierung
- 1.12 Change Management
- 1.13 Externe Dienstleister und Lieferanten
- 1.14 Incident Management
- 1.15 Business Continuity Management
- 1.16 Audits
- 1.17 Compliance

2. Technik

- 2.1 Netzwerk
- 2.2 WLAN
- 2.3 Applikations- und Systemlandschaft
- 2.4 Endpoint Security
- 2.5 Schadsoftwareschutzkonzept
- 2.6 Software und Patch Management
- 2.7 Datensicherung
- 2.8 Fernzugriff
- 2.9 Cloud-Dienste

© Österreichischer Städtebund, Rathaus, A 1082 Wien

NIS-Fragenkatalog

Österreichischer Städtebund

- Kategorien entsprechend NISG/NISV und NIS Fact Sheet 9/2022
- Aufteilung in 29 Themenbereiche in 11 Kategorien

1. Governance und Risikomanagement
- 1.1 Risikoanalyse
- 1.2 Sicherheitsrichtlinie
- 1.3 Überprüfungsplan der Netz- und Informationssysteme
- 1.4 Ressourcenmanagement
- 1.5 Informationssicherheitsmanagementsystemprüfung
- 1.6 Personalwesen

2. Umgang mit Dienstleistern, Lieferanten und Dritten
- 2.1 Beziehungen mit Dienstleistern, Lieferanten und Dritten
- 2.2 Leistungsvereinbarungen mit Dienstleistern und Lieferanten

3. Sicherheitsarchitektur
- 3.1 Systemkonfiguration
- 3.2 Vermögenswerte
- 3.3 Netzwerksegmentierung
- 3.4 Netzwerksicherheit
- 3.5 Kryptographie

4. Systemadministration
- 4.1 Administrative Zugangsrechte
- 4.2 Systeme und Anwendungen zur Systemadministration

5. Identitäts- und Zugriffsmanagement
- 5.1 Identifikation und Authentifikation
- 5.2 Autorisierung

6. Systemwartung und Betrieb
- 6.1 Systemwartung und Betrieb
- 6.2 Fernzugriff

7. Physische Sicherheit
- 7.1 Physische Sicherheit

8. Erkennung von Vorfällen
- 8.1 Erkennung
- 8.2 Protokollierung und Monitoring
- 8.3 Korrelation und Analyse

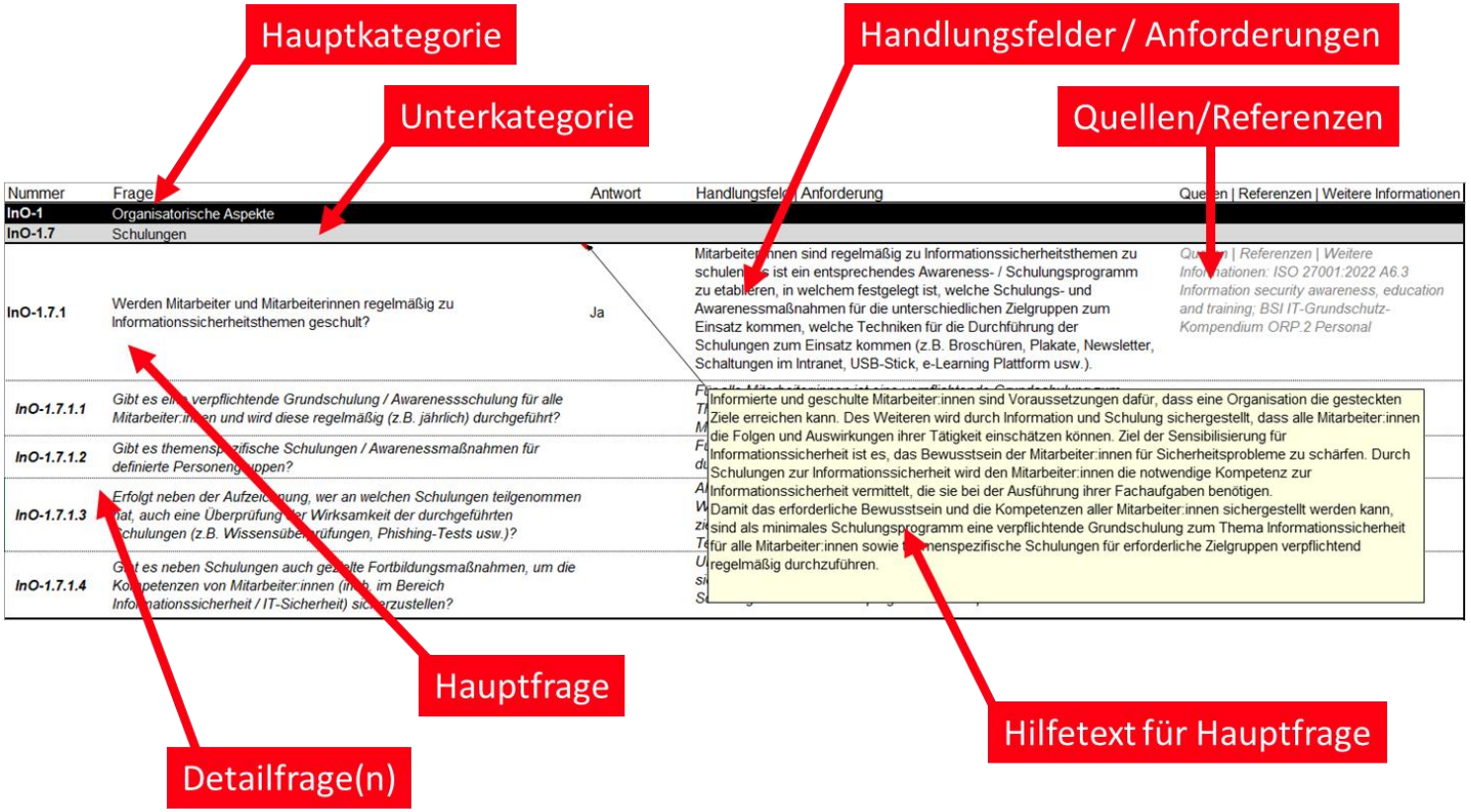
9. Bewältigung von Vorfällen
- 9.1 Vorfallsreaktion
- 9.2 Vorfallsmeldung
- 9.3 Vorfallsanalyse

10. Betriebskontinuität
- 10.1 Betriebskontinuitätsmanagement
- 10.2 Notfallmanagement

11. Krisenmanagement
- 11.1 Krisenmanagement

© Österreichischer Städtebund, Rathaus, A 1082 Wien

Aufbau Fragenkatalog



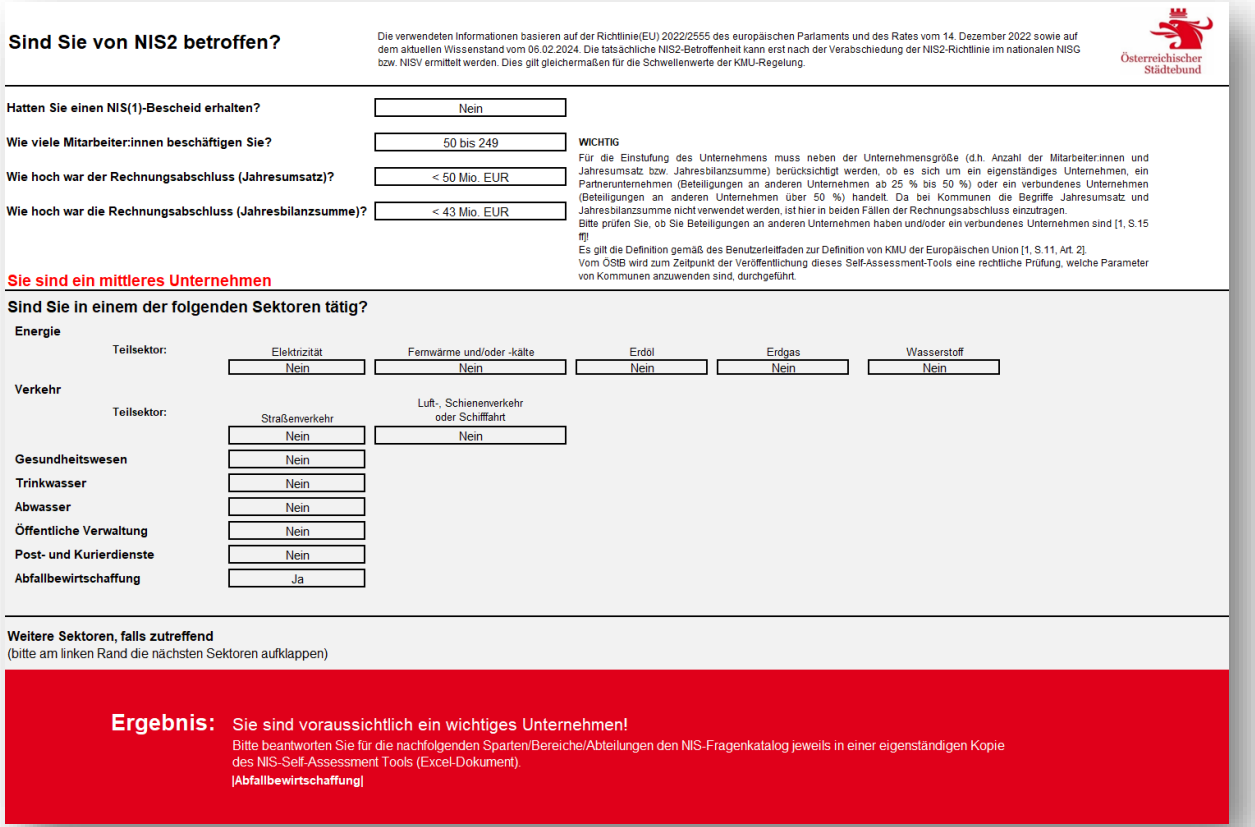
Nummer	Frage	Antwort	Handlungsfeld / Anforderung	Quellen | Referenzen | Weitere Informationen
InO-1	Organisatorische Aspekte			
InO-1.7	Schulungen			
InO-1.7.1	Werden Mitarbeiter und Mitarbeiterinnen regelmäßig zu Informationssicherheitsthemen geschult?	Ja	Mitarbeiterinnen sind regelmäßig zu Informationssicherheitsthemen zu schulen. Es ist ein entsprechendes Awareness- / Schulungsprogramm zu etablieren, in welchem festgelegt ist, welche Schulungs- und Awarenessmaßnahmen für die unterschiedlichen Zielgruppen zum Einsatz kommen, welche Techniken für die Durchführung der Schulungen zum Einsatz kommen (z.B. Broschüren, Plakate, Newsletter, Schaltungen im Intranet, USB-Stick, e-Learning Plattform usw.).	*Quellen | Referenzen | Weitere Informationen: ISO 27001:2022 A6.3 Information security awareness, education and training; BSI IT-Grundschutz-Kompendium ORP.2 Personal*
InO-1.7.1.1	*Gibt es eine verpflichtende Grundschulung / Awarenessschulung für alle Mitarbeiter:innen und wird diese regelmäßig (z.B. jährlich) durchgeführt?*			
InO-1.7.1.2	*Gibt es themenspezifische Schulungen / Awarenessmaßnahmen für definierte Personengruppen?*			
InO-1.7.1.3	*Erfolgt neben der Aufzeichnung, wer an welchen Schulungen teilgenommen hat, auch eine Überprüfung der Wirksamkeit der durchgeführten Schulungen (z.B. Wissensüberprüfungen, Phishing-Tests usw.)?*			
InO-1.7.1.4	*Gibt es neben Schulungen auch gezielte Fortbildungsmaßnahmen, um die Kompetenzen von Mitarbeiter:innen (insb. im Bereich Informationssicherheit / IT-Sicherheit) sicherzustellen?*			

Informierte und geschulte Mitarbeiter:innen sind Voraussetzungen dafür, dass eine Organisation die gesteckten Ziele erreichen kann. Des Weiteren wird durch Information und Schulung sichergestellt, dass alle Mitarbeiter:innen die Folgen und Auswirkungen ihrer Tätigkeit einschätzen können. Ziel der Sensibilisierung für Informationssicherheit ist es, das Bewusstsein der Mitarbeiter:innen für Sicherheitsprobleme zu schärfen. Durch Schulungen zur Informationssicherheit wird den Mitarbeiter:innen die notwendige Kompetenz zur Informationssicherheit vermittelt, die sie bei der Ausführung ihrer Fachaufgaben benötigen.
Damit das erforderliche Bewusstsein und die Kompetenzen aller Mitarbeiter:innen sichergestellt werden kann, sind als minimales Schulungsprogramm eine verpflichtende Grundschulung zum Thema Informationssicherheit für alle Mitarbeiter:innen sowie themenspezifische Schulungen für erforderliche Zielgruppen verpflichtend regelmäßig durchzuführen.

© Österreichischer Städtebund, Rathaus, A 1082 Wien

NIS(2)-Bewertung

Österreichischer Städtebund



Sind Sie von NIS2 betroffen?

Die verwendeten Informationen basieren auf der Richtlinie(EU) 2022/2555 des europäischen Parlaments und des Rates vom 14. Dezember 2022 sowie auf dem aktuellen Wissenstand vom 06.02.2024. Die tatsächliche NIS2-Betroffenheit kann erst nach der Verabschiedung der NIS2-Richtlinie im nationalen NISG bzw. NISV ermittelt werden. Dies gilt gleichermaßen für die Schwellenwerte der KMU-Regelung.

Österreichischer Städtebund

Hatten Sie einen NIS(1)-Bescheid erhalten?	Nein
Wie viele Mitarbeiter:innen beschäftigen Sie?	50 bis 249
Wie hoch war der Rechnungsabschluss (Jahresumsatz)?	< 50 Mio. EUR
Wie hoch war die Rechnungsabschluss (Jahresbilanzsumme)?	< 43 Mio. EUR

WICHTIG
Für die Einstufung des Unternehmens muss neben der Unternehmensgröße (d.h. Anzahl der Mitarbeiter:innen und Jahresumsatz bzw. Jahresbilanzsumme) berücksichtigt werden, ob es sich um ein eigenständiges Unternehmen, ein Partnerunternehmen (Beteiligungen an anderen Unternehmen ab 25 % bis 50 %) oder ein verbundenes Unternehmen (Beteiligungen an anderen Unternehmen über 50 %) handelt. Da bei Kommunen die Begriffe Jahresumsatz und Jahresbilanzsumme nicht verwendet werden, ist hier in beiden Fällen der Rechnungsabschluss einzutragen.
Bitte prüfen Sie, ob Sie Beteiligungen an anderen Unternehmen haben und/oder ein verbundenes Unternehmen sind [1, S.15 ff]!
Es gilt die Definition gemäß des Benutzerleitfaden zur Definition von KMU der Europäischen Union [1, S.11, Art. 2].
Vom ÖStB wird zum Zeitpunkt der Veröffentlichung dieses Self-Assessment-Tools eine rechtliche Prüfung, welche Parameter von Kommunen anzuwenden sind, durchgeführt.

Sie sind ein mittleres Unternehmen

Sind Sie in einem der folgenden Sektoren tätig?

Energie

Teilsektor:	Elektrizität	Fernwärme und/oder -kälte	Erdöl	Erdgas	Wasserstoff
	Nein	Nein	Nein	Nein	Nein

Verkehr

Teilsektor:	Straßenverkehr	Luft-, Schienenverkehr oder Schifffahrt
	Nein	Nein

Gesundheitswesen	Nein
Trinkwasser	Nein
Abwasser	Nein
Öffentliche Verwaltung	Nein
Post- und Kurierdienste	Nein
Abfallbewirtschaffung	Ja

Weitere Sektoren, falls zutreffend
(bitte am linken Rand die nächsten Sektoren aufklappen)

Ergebnis: Sie sind voraussichtlich ein wichtiges Unternehmen!
Bitte beantworten Sie für die nachfolgenden Sparten/Bereiche/Abteilungen den NIS-Fragenkatalog jeweils in einer eigenständigen Kopie des NIS-Self-Assessment Tools (Excel-Dokument).
|Abfallbewirtschaffung|

© Österreichischer Städtebund, Rathaus, A 1082 Wien

Auswertung / Bericht / Ergebnis

Österreichischer Städtebund

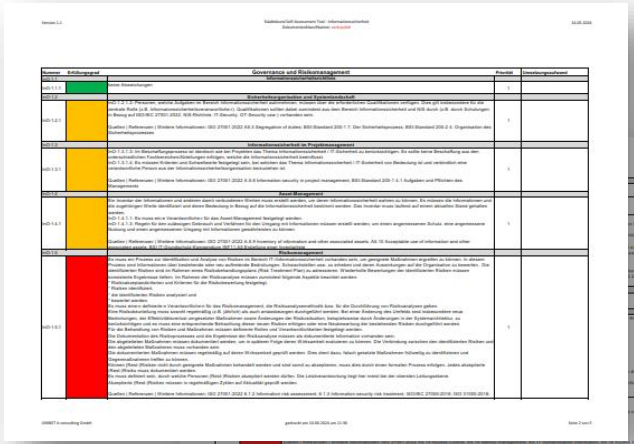
Self-Assessment des österreichischen Städtebunds

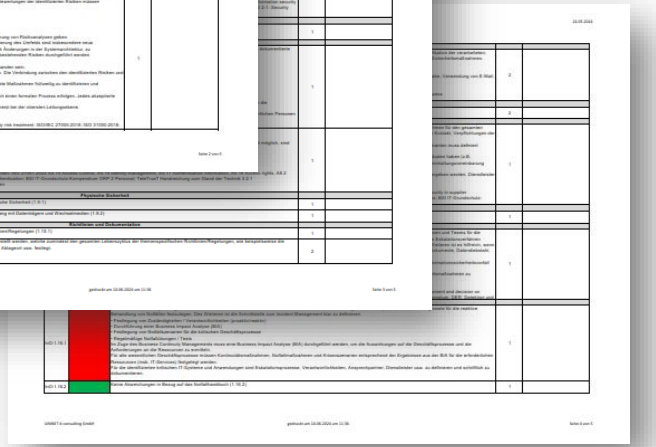
Auswertungsergebnisse der organisatorischen Informationssicherheit

Stadt/Gemeinde:	Musterstadt
Verwaltungsadresse:	Musterstraße 1 1234 Musterstadt
Durchführungsdatum:	19.06.2024
Kontaktperson:	Musterperson
Position:	Verantwortlicher
Telefonnummer:	+43 123 45678910
E-Mail-Adresse:	musterperson@must

Österreichischer Städtebund

gedruckt am 10.06.2024 um 11:56





© Österreichischer Städtebund, Rathaus, A 1082 Wien