

Das ITSCM-Barometer

2026 – Jahresumfrage der Controllit AG

Trends, Zahlen, Daten und Fakten der
Unternehmen im deutschsprachigen Raum zum
Thema IT Service Continuity Management

Vorhang auf zu unserem ersten ITSCM-Barometer! Nachdem es unser BCM-Barometer mittlerweile seit über zehn Jahren gibt, haben wir in diesem Jahr zur ersten Umfrage eingeladen, um zusätzlich den aktuellen Status quo im IT Service Continuity Management zu erfassen, Entwicklungen zu dokumentieren und einen Ausblick auf zukünftige Trends zu geben.



Ansatz und Vorgehen - so war unsere Umfrage zum ITSCM-Barometer aufgebaut

Unsere Umfrage haben wir im Zeitraum vom 23. Februar bis zum 29. Mai 2026 im deutschsprachigen Raum durchgeführt. Im Fokus standen die Trends, Zahlen, Daten und Fakten der Unternehmen zum Thema IT Service Continuity Management für das Jahr 2025 und vorausschauend für 2026.

Alle Teilnehmer konnten sich anonym an der Umfrage beteiligen. Zur Umfrage eingeladen haben wir über

die Netzwerkplattform LinkedIn. Bei unserem Auftakt haben 47 Personen an der Umfrage teilgenommen, von denen uns einige außerdem ihre Ideen und Wünsche bezüglich der nächsten Umfrage mitgeteilt haben.

Herzlich bedanken möchten wir uns bei allen, die an der Umfrage teilgenommen haben, und wir wünschen Ihnen viel Freude beim Lesen unseres ITSCM-Barometers.

Hamburg im Juli 2026

Matthias Rosenberg

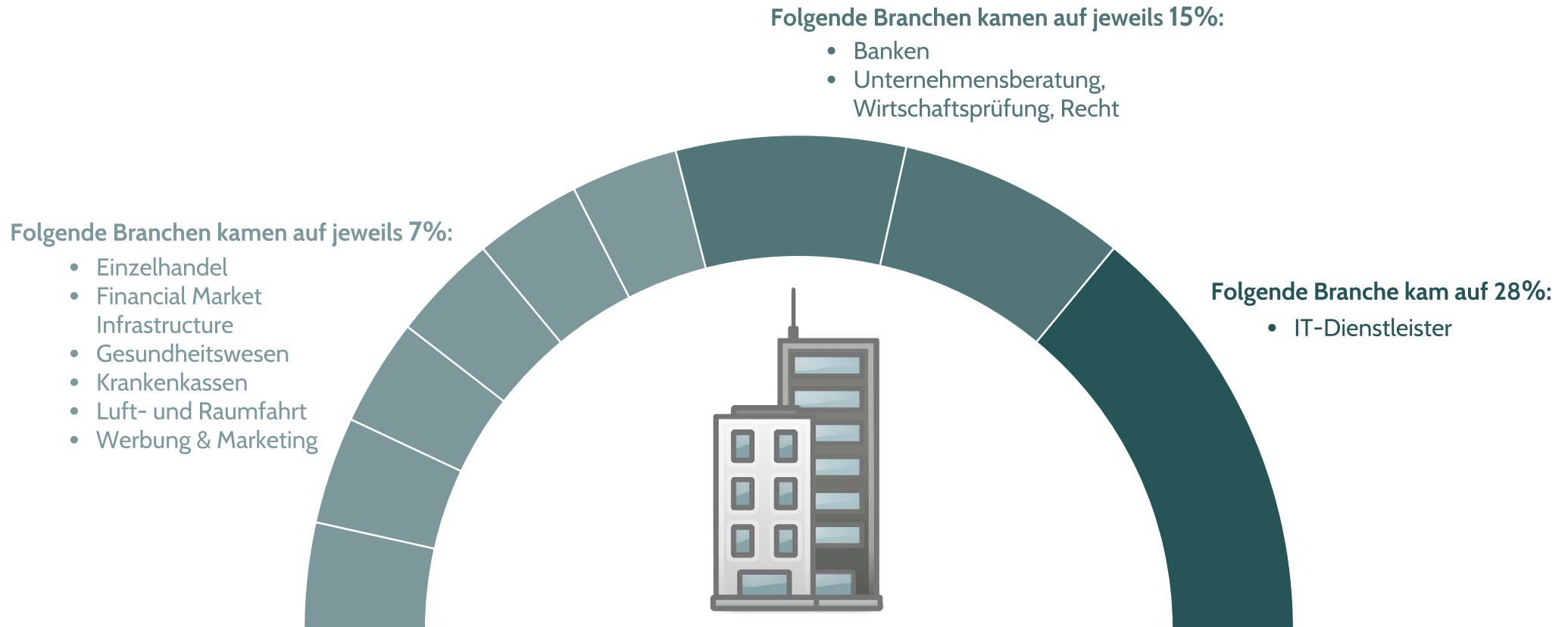
FBCI

Vorstand Controllit AG

Gender-Hinweis: Aus Gründen der besseren Lesbarkeit haben wir bei Personenbezeichnungen und personenbezogenen Hauptwörtern in diesem Bericht die männliche Form verwendet. Selbstverständlich sind immer alle Geschlechter gemeint, auch wenn explizit nur eines angesprochen wird.

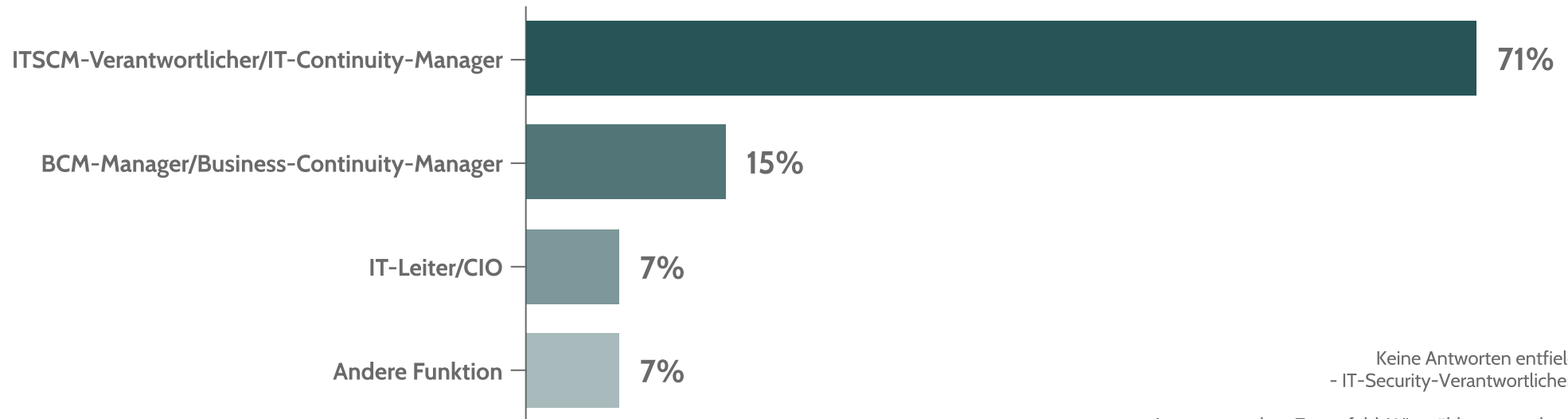
01. Zu welcher Branche lässt sich Ihr Unternehmen zählen?

In unserem ersten Jahr der Umfrage haben wir bewusst viele Branchen als Antwortmöglichkeit aufgeführt. Und so sieht das Ergebnis aus:



Keine Stimmen entfielen auf: allgemeine Dienstleistungen, Bankdienstleister, Baugewerbe, Baustoffe, Behördenumfeld, Bildung & Training, Börsen, Chemie und Erdöl verarbeitende Industrie, Druck, Papier, Verpackung, E-Commerce, Elektronik, Energie- und Wasserversorgung, Fahrzeugbau/Fahrzeugzulieferer, Freizeit, Touristik, Kultur & Sport, Glas/Keramik, Holz-/Möbelindustrie, Maschinen-/Anlagenbau, Medien, Nahrungsmittel, Pharma-/Medizintechnik, Telekommunikation, Textil, Transport & Logistik, Unternehmensberatung, Versicherungen, Wissenschaft & Forschung, Zahlungsdienstleister, Lebensmitteleinzelhandel, andere Branchen

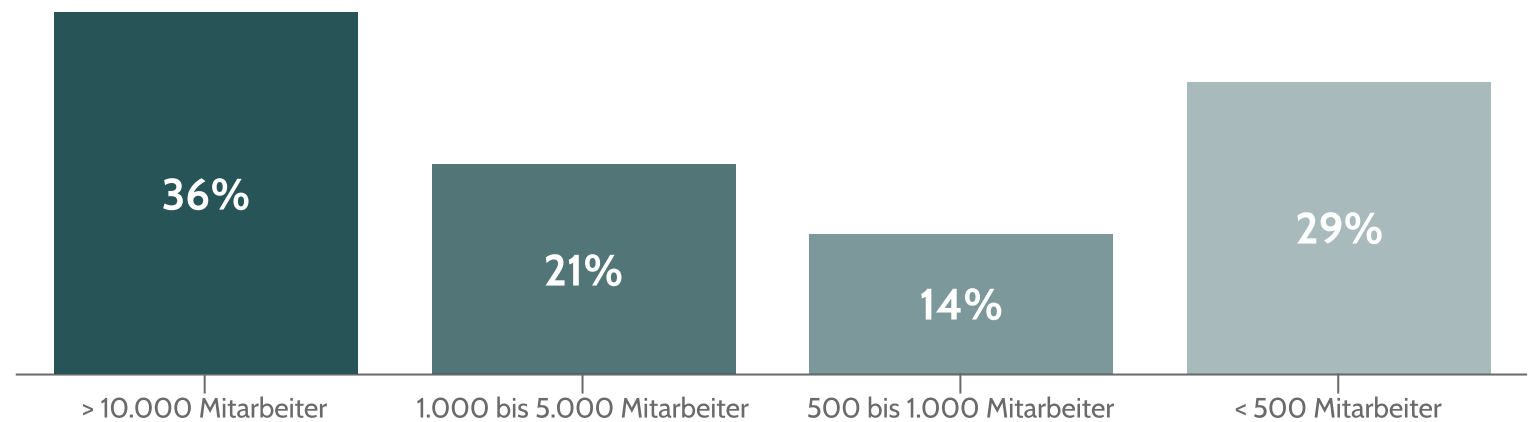
02. Welche Funktion haben Sie in Ihrem Unternehmen?



Keine Antworten entfielen auf:
- IT-Security-Verantwortlicher/CISO

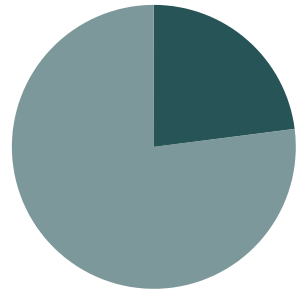
Antwort aus dem Zusatzfeld: Wie wählt man mehrere aus?

03. Wie viele Mitarbeiter sind in Ihrem Unternehmen beschäftigt?

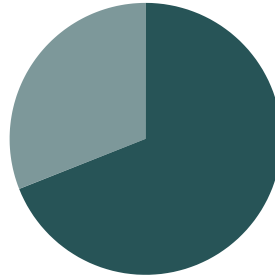


Keine Stimmen entfielen auf: "5.000 bis 10.000 Mitarbeiter".

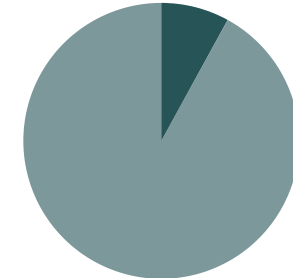
04. Verfügt Ihr Unternehmen über ein formales IT-Service Continuity Management?



23%
Ja, vollständig etabliert



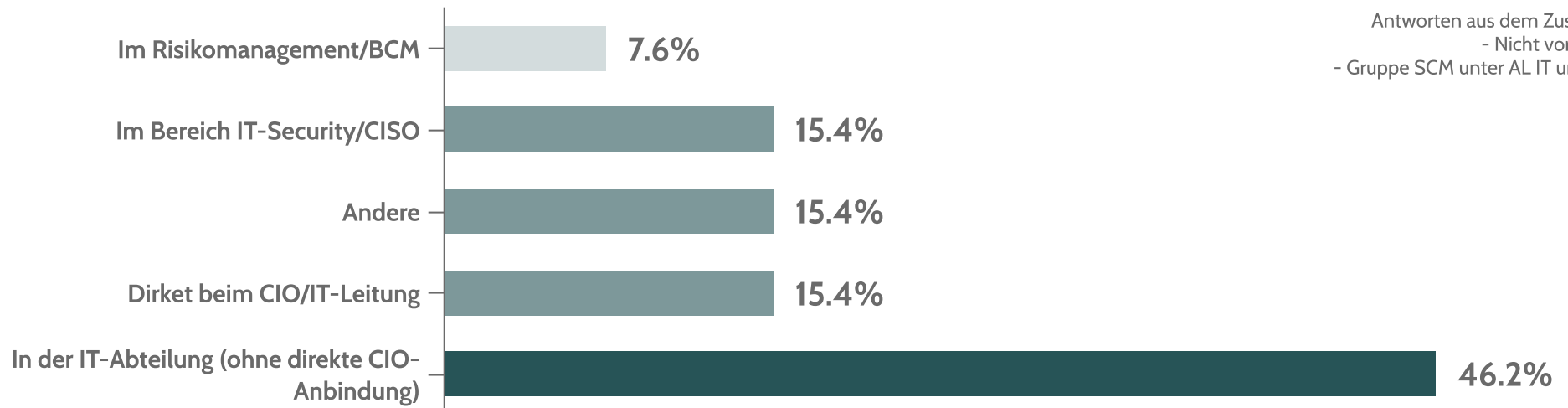
69%
Ja, teilweise etabliert/
im Aufbau



8%
Nein, kein ITSCM vorhanden

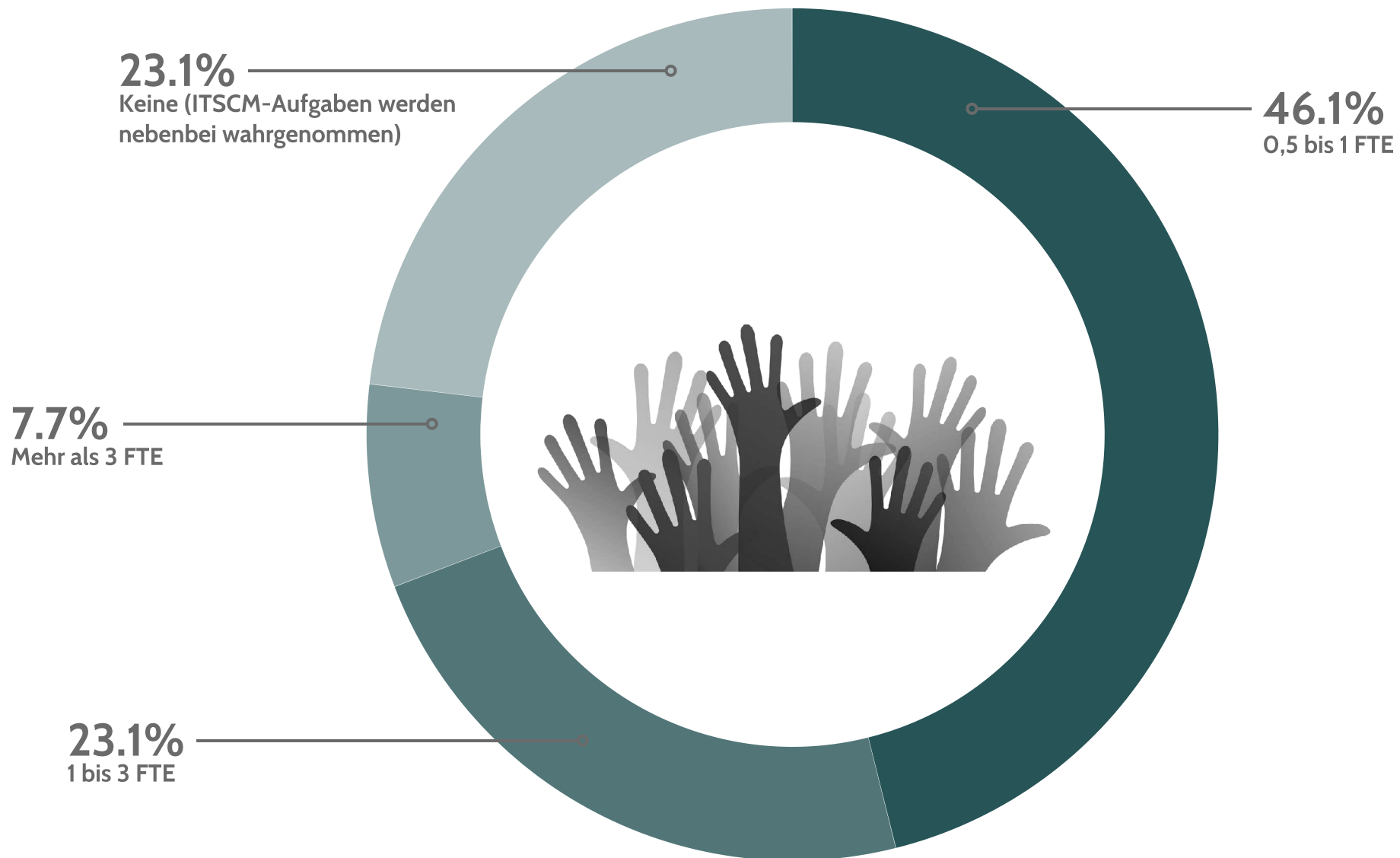
Keine Stimmen
entfielen auf "Nein, aber
geplant".

05. Wo ist das ITSCM in Ihrem Unternehmen angesiedelt?



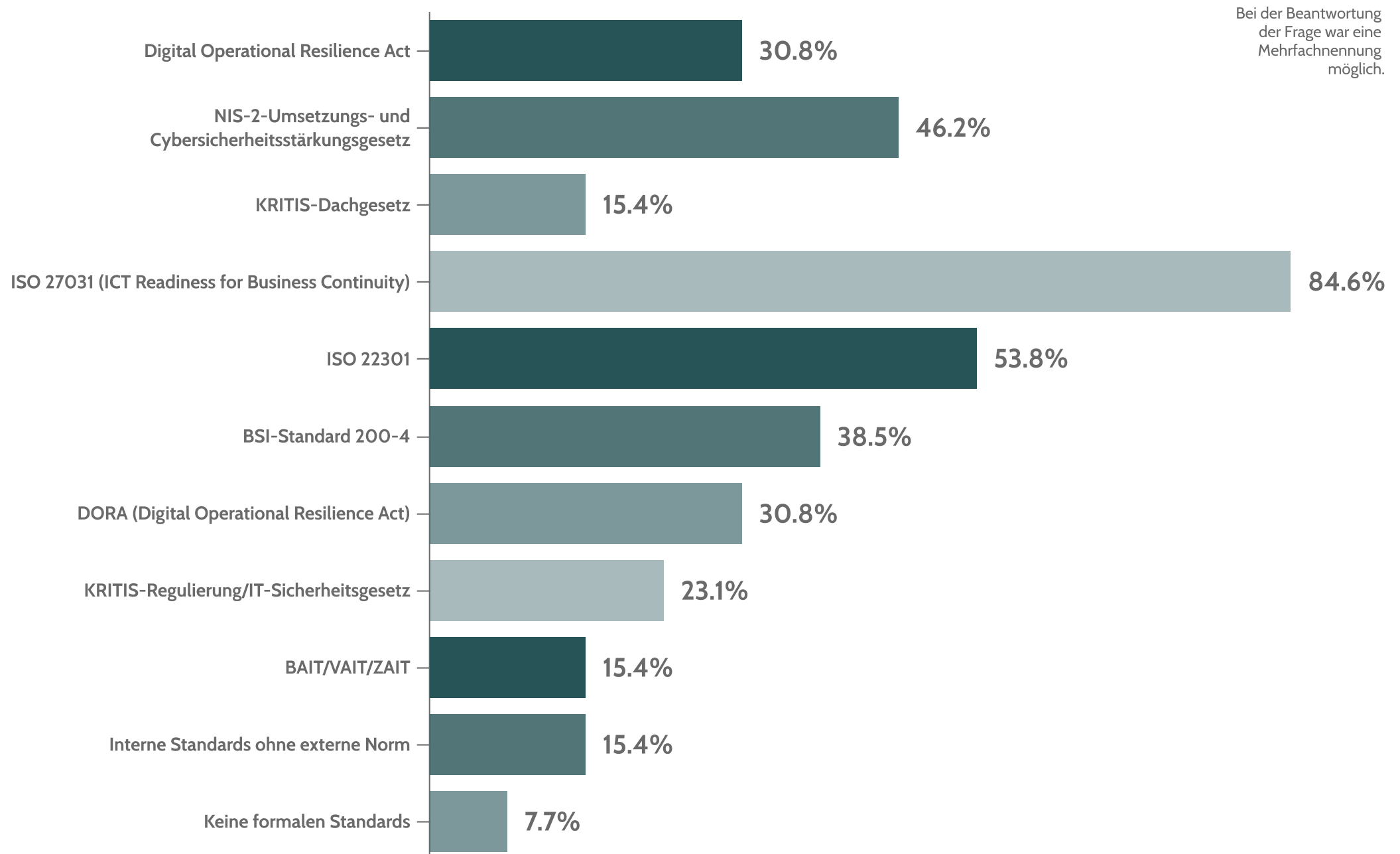
Antworten aus dem Zusatzfeld:
- Nicht vorhanden
- Gruppe SCM unter AL IT und BL IT

06. Wie viele Vollzeitstellen (FTE) sind in Ihrem Unternehmen für ITSCM tätig?



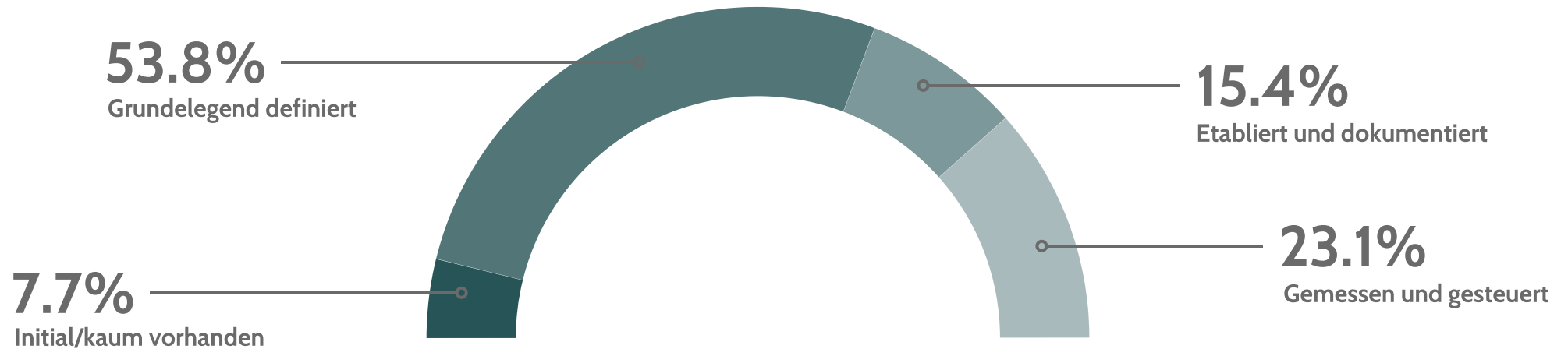
7.

Welche Normen, Standards oder regulatorischen Anforderungen sind für Ihr ITSCM maßgeblich?

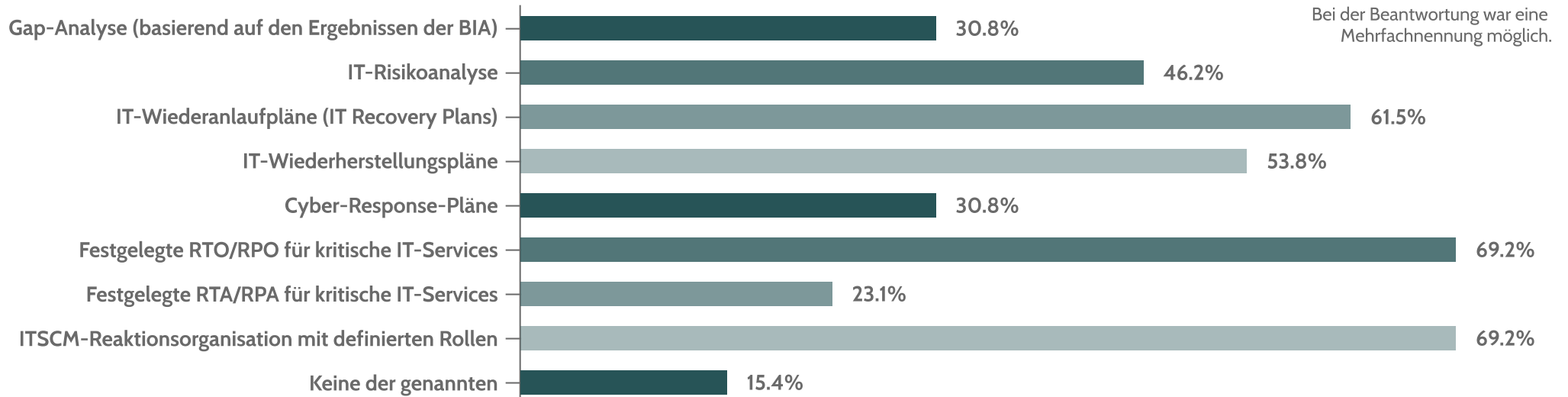


08. Wie schätzen Sie den Reifegrad Ihres ITSCM insgesamt ein?

Keine Stimmen entfielen auf
"Kontinuierlich optimiert".

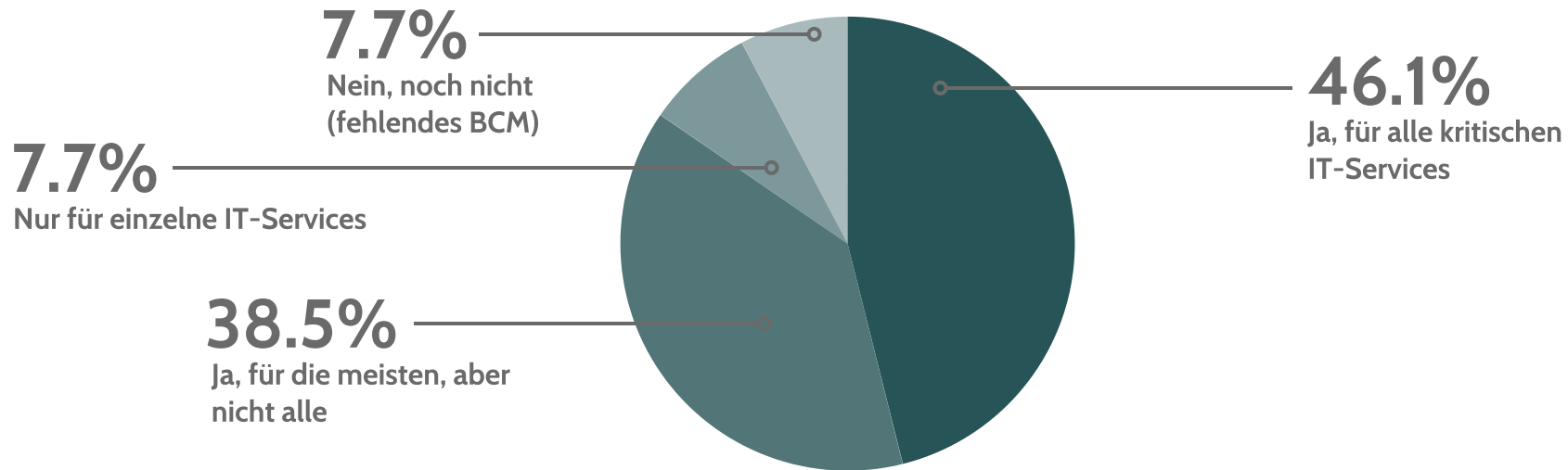


09. Welche ITSCM-Kernelemente sind in Ihrem Unternehmen vollständig umgesetzt?

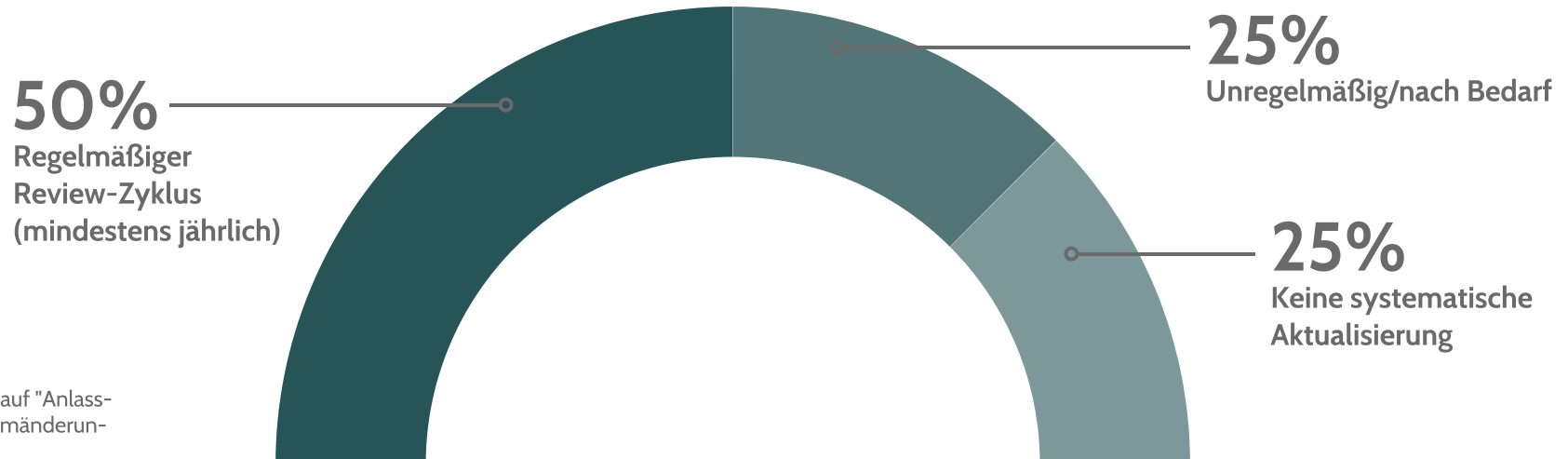


Bei der Beantwortung war eine
Mehrfachnennung möglich.

10. Sind für Ihre kritischen IT-Services konkrete RTO- und RPO-Ziele definiert und dokumentiert?



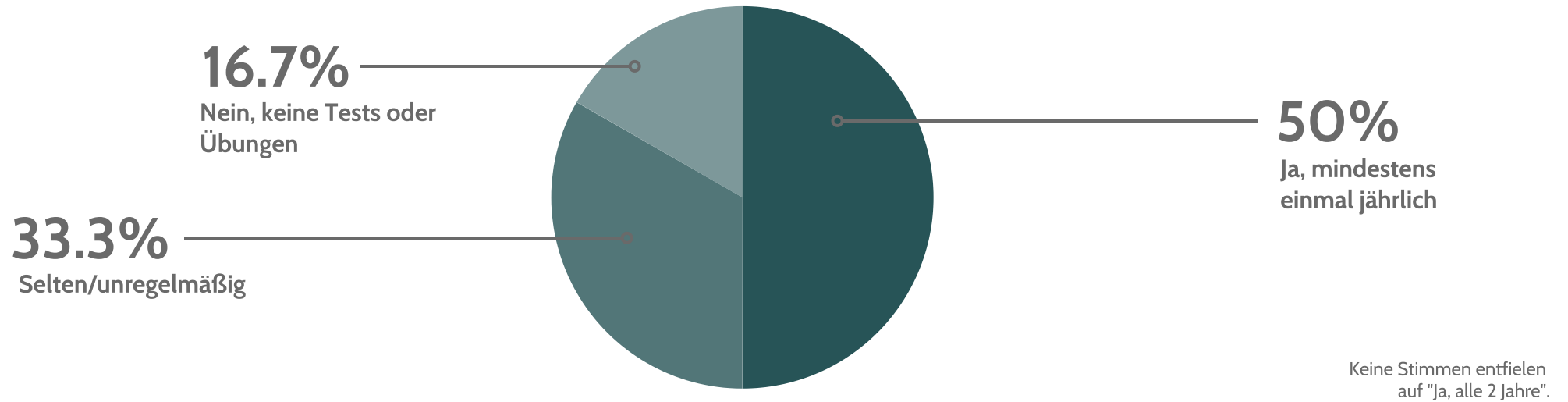
11. Wie werden Ihre ITSCM-Pläne und -Notfalldokumente im Regelbetrieb aktuell gehalten?



Keine Stimmen entfielen auf "Anlassbezogen (z. B. nach Systemänderungen, Reorganisation)".

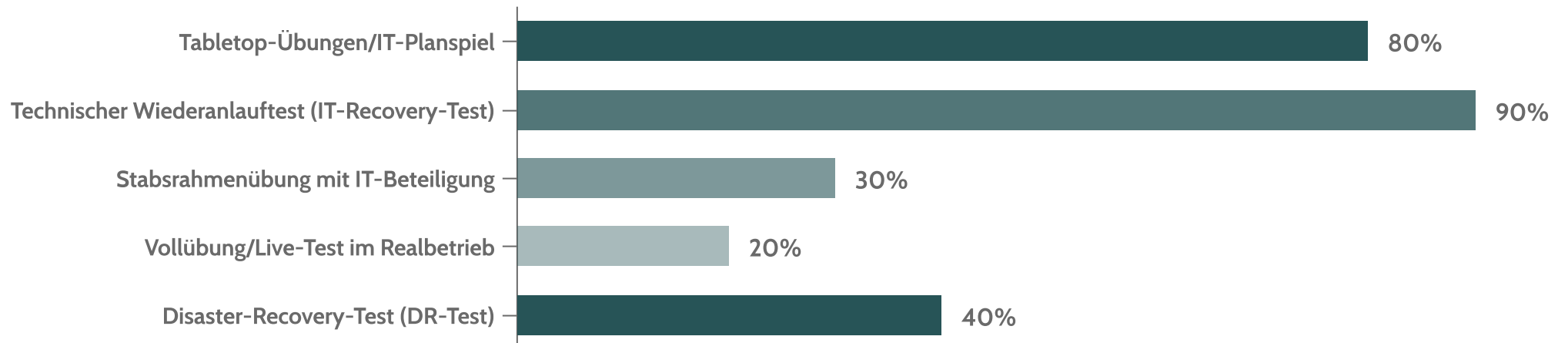
12.

Führen Sie regelmäßige ITSCM-Tests oder IT-Notfallübungen durch?



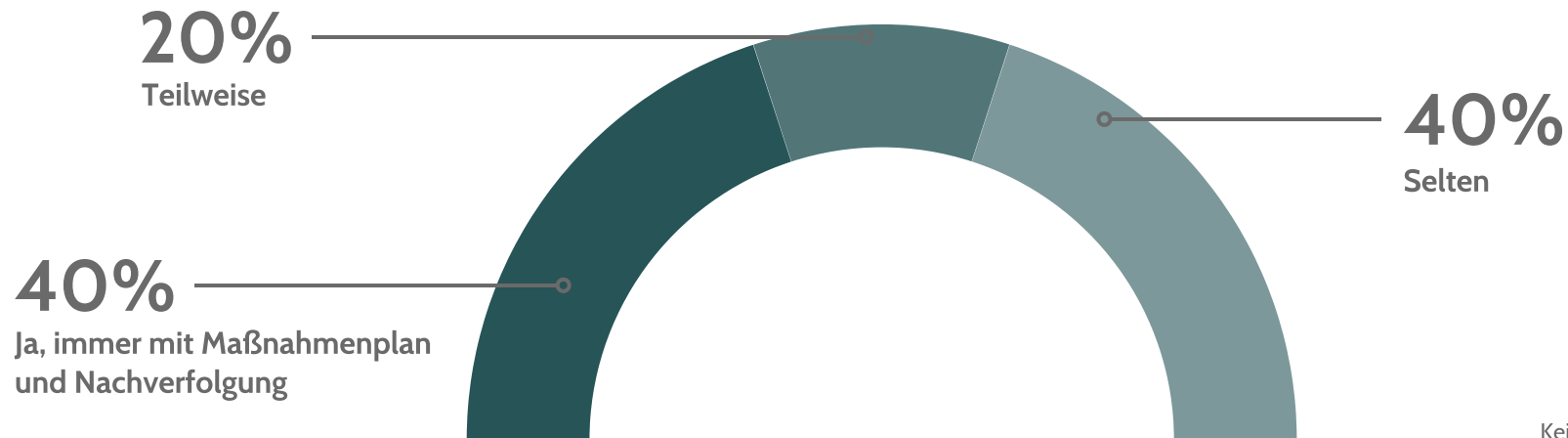
13.

Welche Arten von ITSCM-Tests führen Sie durch?



Bei der Beantwortung der Frage war eine Mehrfachnennung möglich.

14. Werden die Ergebnisse Ihrer ITSCM-Tests systematisch ausgewertet und Maßnahmen abgeleitet?



Keine Stimmen entfielen auf "Nein".

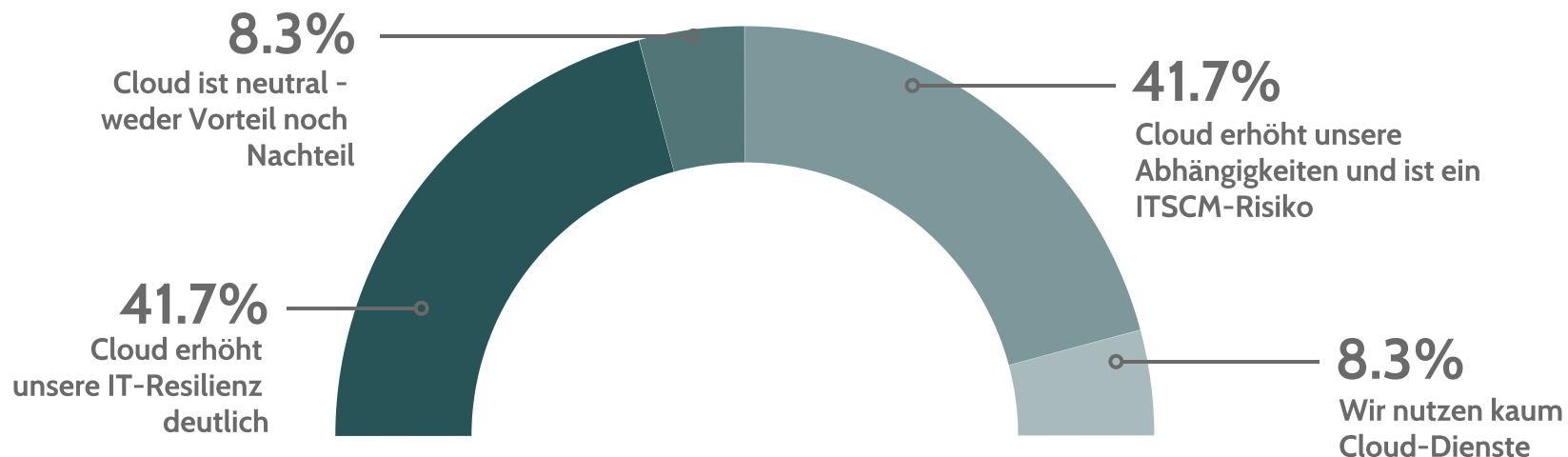
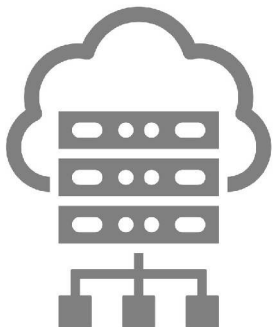
15. Welche Wiederherstellungsstrategien setzen Sie für kritische IT-Services ein?



Bei der Beantwortung war eine Mehrfachnennung möglich.
Keine Stimmen entfielen auf "Keine formale Wiederherstellungsstrategie".

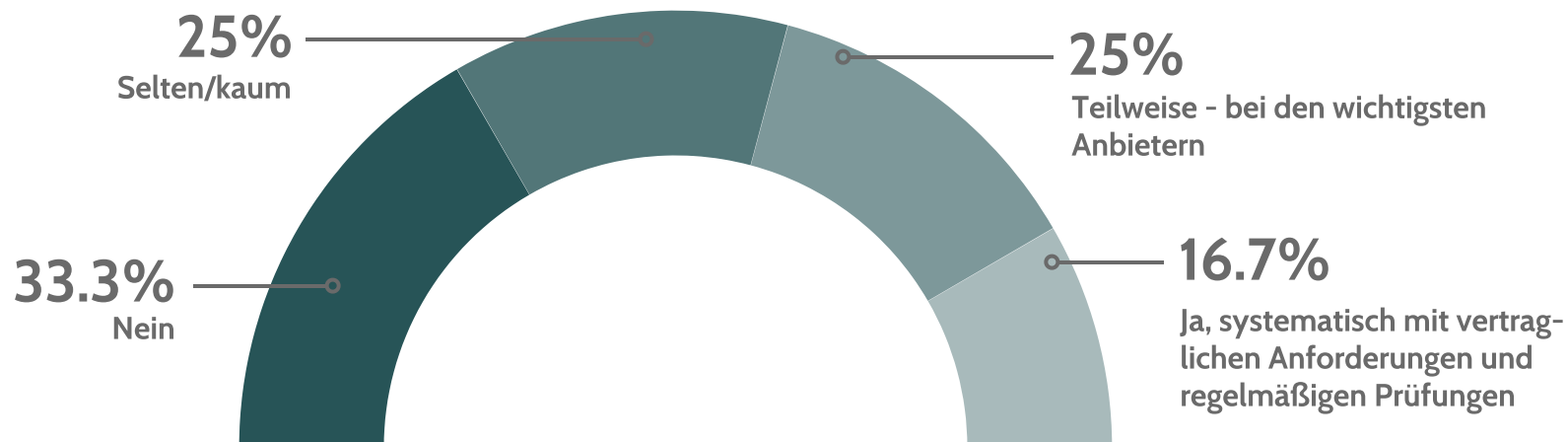
16.

Wie beurteilen Sie den Einfluss von Cloud-Diensten auf Ihre ITSCM-Fähigkeit?



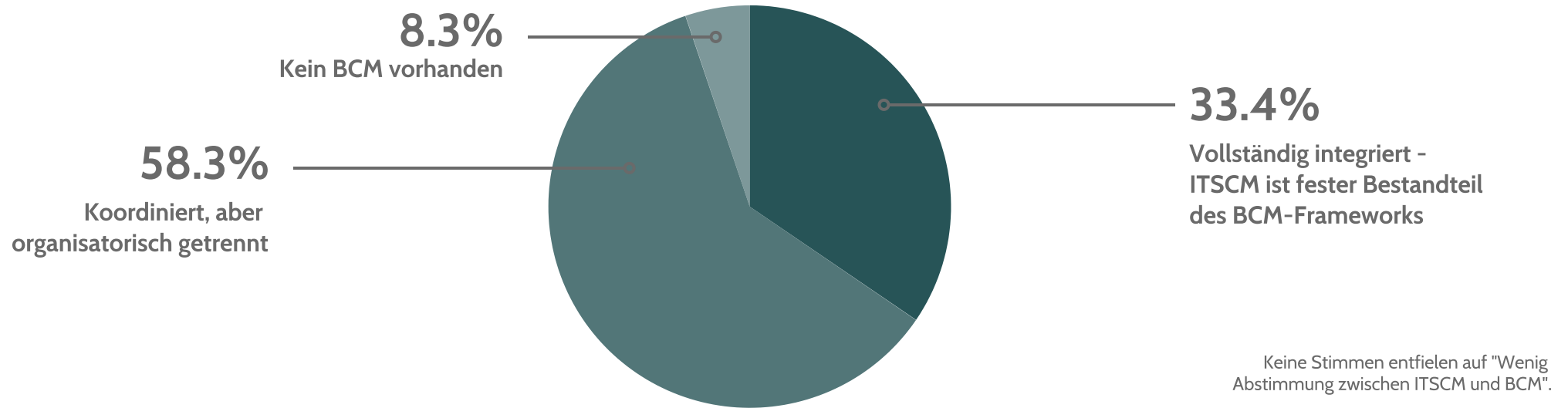
17.

Werden IT-Drittanbieter und kritische IT-Lieferketten systematisch in Ihr ITSCM einbezogen?



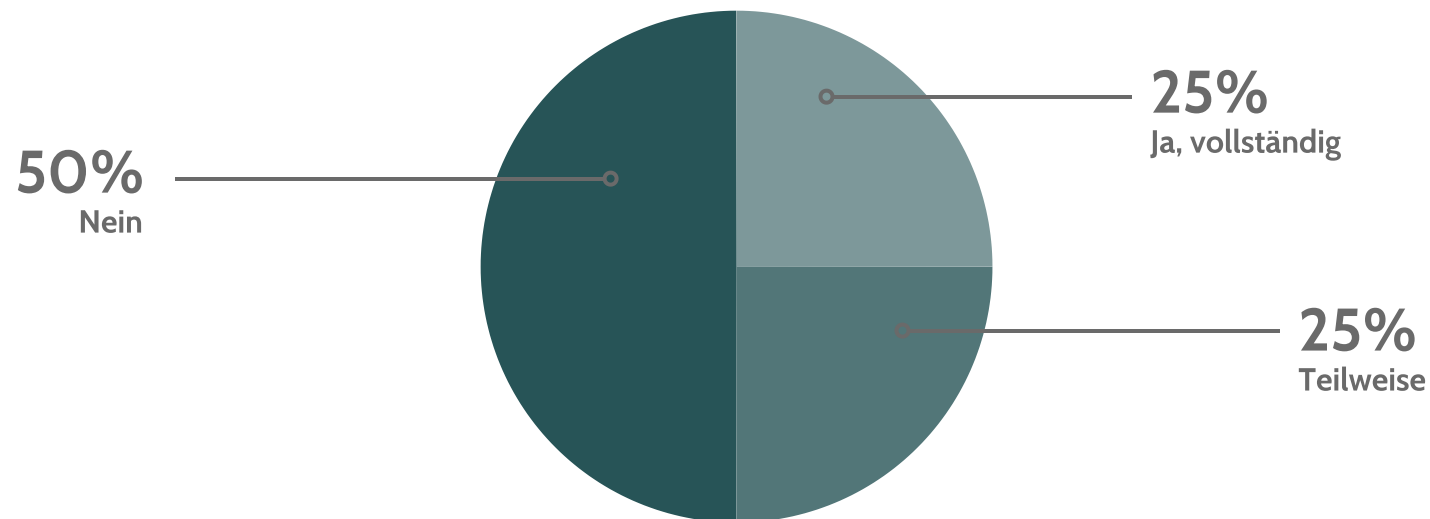
18.

Wie eng ist Ihr ITSCM mit dem Business Continuity Management (BCM) verzahnt?

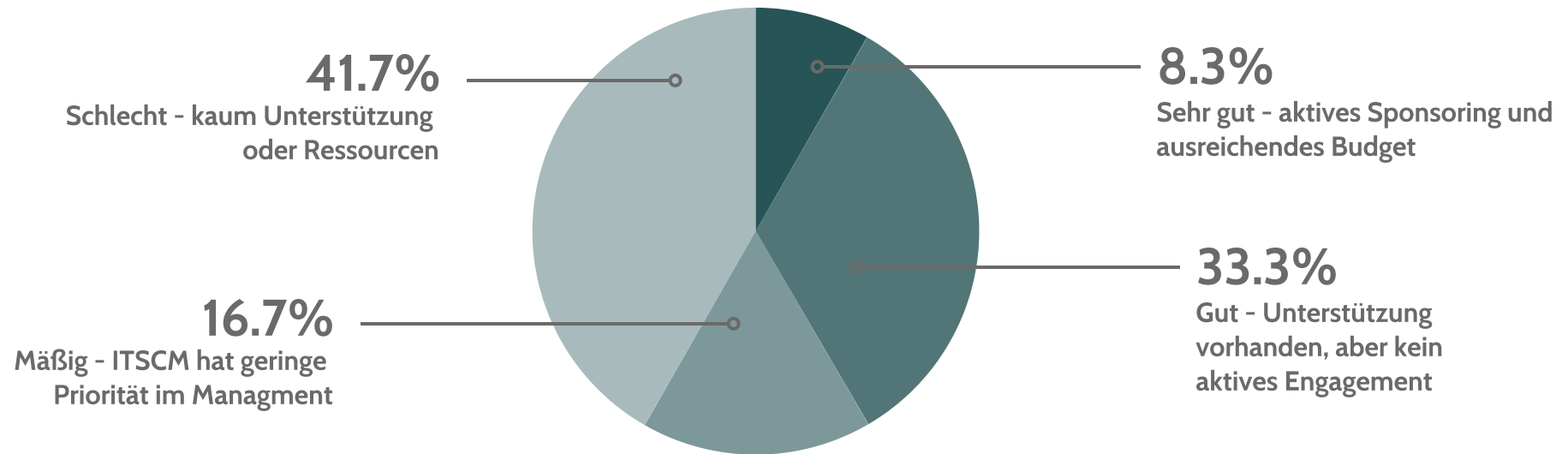


19.

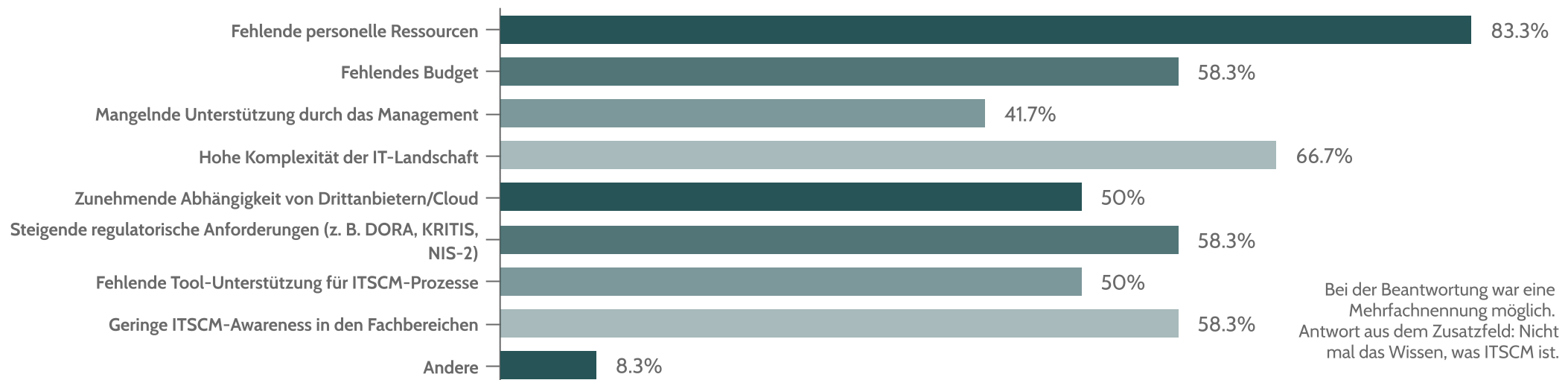
Ist das ITSCM in das unternehmensweite Risikomanagement eingebunden?



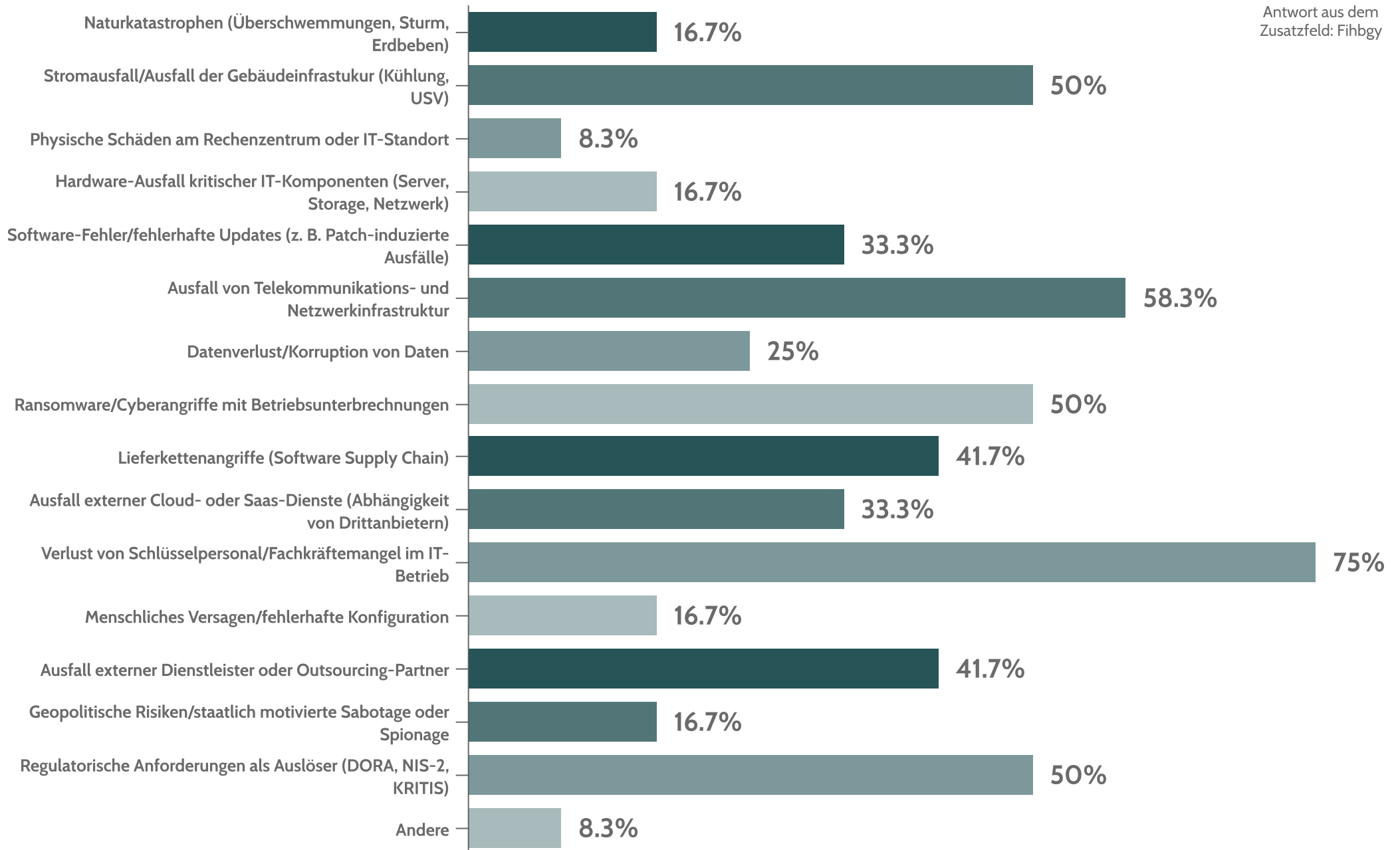
20. Wie bewerten Sie die Unterstützung des Top-Managements für das ITSCM?



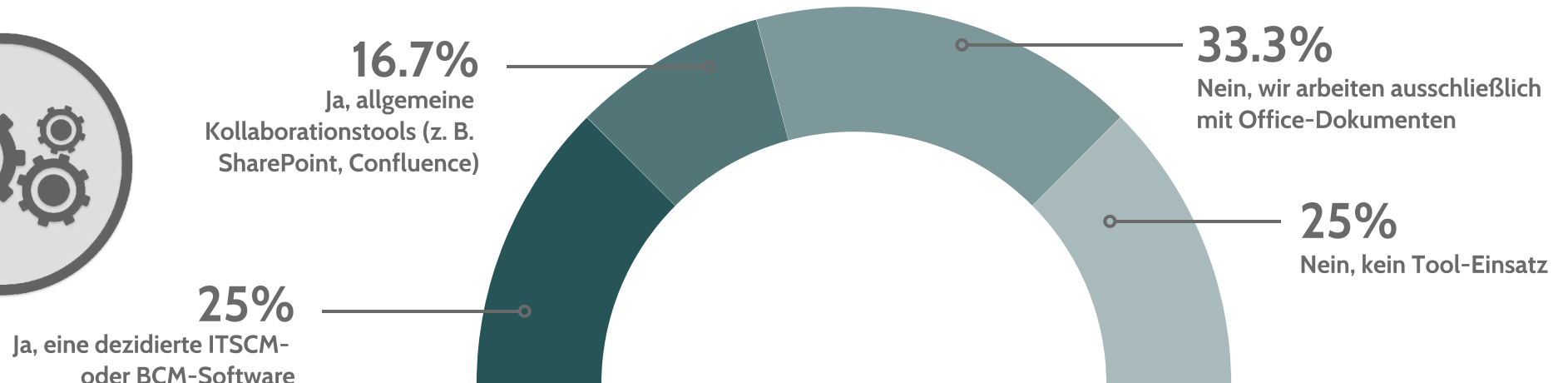
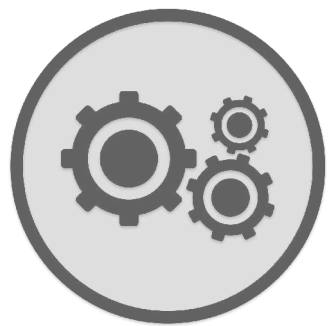
21. Was sind die größten Herausforderungen für Ihr ITSCM?



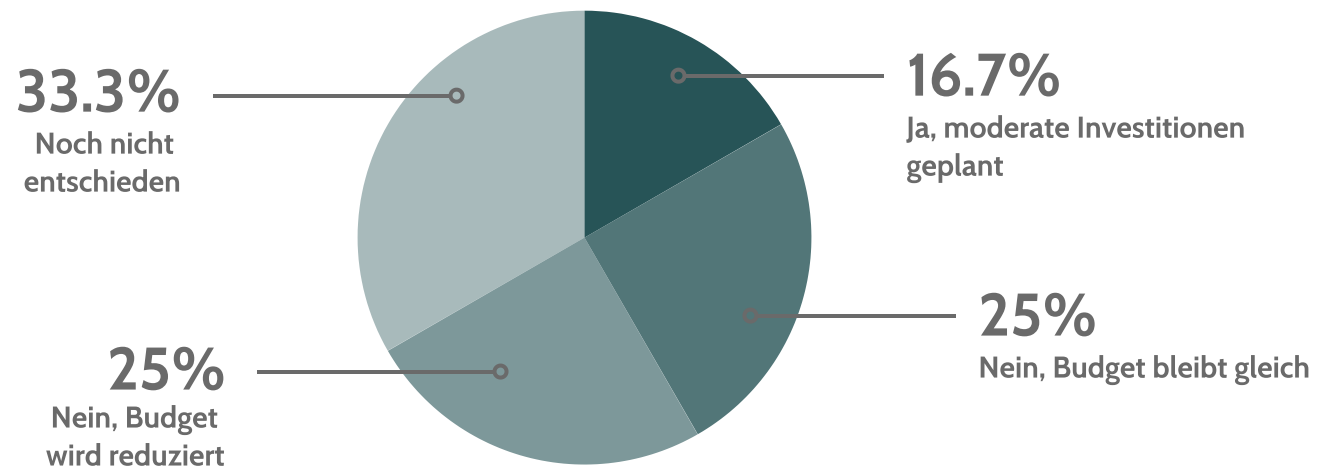
22. Welche Bedrohungsszenarien haben in Ihrem ITSCM in den letzten zwei Jahren an Bedeutung gewonnen?



23. Nutzen Sie spezifische Software-Tools zur Unterstützung Ihrer ITSCM-Prozesse?



24. Plant Ihr Unternehmen in den nächsten zwölf Monaten Investitionen in das ITSCM?



Keine Antworten entfielen auf "Ja, deutliche Investitionen geplant".

25. Wie hat sich der Stellenwert von ITSCM in Ihrem Unternehmen in den letzten zwölf Monaten verändert?



26. Was beschäftigt Sie in Ihrem ITSCM derzeit am meisten - und was wünschen Sie sich für die Weiterentwicklung der Disziplin?

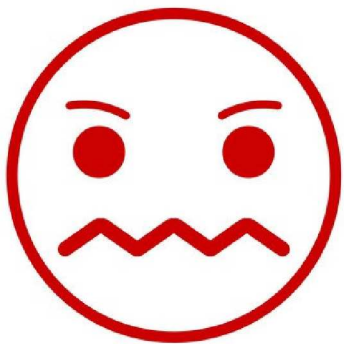


- Die Integration von NIS-2- und KRITIS-Anforderungen an ein ITSCM
- mehr ITSCMler
- Verpflichtende Erstellung von WAP/WHP-Plänen für die kritischen IT-Services und zeitkritischen Geschäftsprozesse
- CMDB-Anpassung an das ITSCM. Dort müssen IT-Services definiert sein.
- Erstellung von Abhängigkeitsbäumen
- Engere Verzahnung mit dem Cyber-Security-Bereich
- Zertifizierung nach ISO 27001, DORA-Anforderungen erfüllen. Dritt-Dienstleister-Management. Wunsch: mehr Austausch unter ITSCM-Managern
- Die kritischen IT-Services für die zeitkritischen Geschäftsprozesse sauber zu definieren, da bei uns die vorhandene CMDB dafür leider nicht nutzbar ist. Übersetzt heißt das, dass wir weder eine nutzbare CMDB noch definierte OLAs haben, um uns als ITSCM tiefer mit den IT-Services beschäftigen zu können
- Umzug Rechenzentrum
- Einführung KI und Cloudanbindung für Office Tools
- Bessere Kommunikation mit Dienstleistern

27. Wie fanden Sie die Befragung?

Ihr Feedback ist uns wichtig!

Wir freuen uns sehr, dass 91% der Teilnehmer mit unserer Umfrage sehr beziehungsweise eher zufrieden sind! Doch ausruhen wollen wir uns auf diesem Zuspruch nicht. Ihre Anregungen und Verbesserungsvorschläge sind für uns von großem Wert und werden in unserer Arbeitsgruppe zur Umsetzung diskutiert werden.



0%

Unzufrieden



0%

Eher unzufrieden



9%

Mittelmäßig



18%

Eher zufrieden



73%

Sehr zufrieden

Herzlichen Dank für Ihre Teilnahme und Ihren konstruktiven Input!

Wir hoffen auf ein Wiedersehen, wenn wir zum nächsten ITSCM-Barometer einladen!

Business Continuity Management seit 2000

Aus der Idee, das Thema "Notfallplanung" interdisziplinär zu erweitern und die Vorgehensweisen anders als bisher zu strukturieren, wurde die Controll-IT GmbH im Jahr 2000 gegründet. Wir hatten schon damals das Ziel, eine der ersten Adressen für Business Continuity Management in Deutschland zu werden.

In den mittlerweile 26 Jahren seit unserer Gründung wurde aus der Controll-IT GmbH die Controllit AG und eines der führenden Unternehmen für dieses Thema. Unsere Kunden – Konzerne, mittelständische und kleine Unternehmen aus nahezu allen Branchen in Deutschland, Europa und der ganzen Welt – profitieren von unseren Konzepten und unserer Erfahrung, um sich auf mögliche kritische Vorfälle und Krisen vorzubereiten.

Wir entwickeln integrative Konzepte und Produkte für das Business Continuity Management, IT Service Continuity Management, Krisen- und Resilience Management. Mit unseren strategischen, organisatorischen und technischen Konzepten helfen wir unseren Kunden, ihre Geschäftsprozesse gegen Bedrohungen abzusichern und für Notfälle vorzusorgen.

Unser Team setzt sich aus erfahrenen Beratern und Praktikern zusammen, die über Qualifikationen und ausgeprägte Berufserfahrung auf diesem Gebiet verfügen.

Unsere Software [alive-IT]

Die Software [alive-IT] wurde für die Planung und Bewältigung von Notfallsituationen entwickelt und ist eines der innovativsten Business-Continuity- und IT-Service-Continuity-Systeme auf dem Markt. Von der Analyse bis zur Erstellung der BC-Pläne unterstützt die Notfallplanungssoftware [alive-IT] den BC-Manager bei seiner Arbeit. Dazu zählt auch die Möglichkeit der Orchestrierung des Wiederanlaufs, die die Planung, Durchführung und Dokumentation von Tests erheblich vereinfacht.

Die Auszeichnungen, die [alive-IT] von SoftwareReviews erhielt, bestätigen eine äußerst hohe Kundenzufriedenheit: 2020, 2021 und 2022 wurde der Software eine Goldmedaille verliehen, im Jahr 2021, 2022, 2023 und 2024 kam außerdem der „Emotional Footprint Diamond“-Award dazu. Die von SoftwareReviews herangezogenen Bewertungen beruhen zu 100 Prozent auf Daten, die von Anwendern der Software geliefert wurden.

Weitere Informationen zu unseren Beratungsleistungen und unserer Software finden Sie auf unserer Homepage www.controll-it.de



Management System
ISO 9001:2015
ISO/IEC 27001:2022
ISO 22301:2019
www.tuv.com
ID 9000017255

Wir sind gemäß ISO
9001:2015, ISO
27001:2022 und ISO
22301:2019 zertifiziert.



Unsere Software [alive-IT] wurde mehrfach ausgezeichnet!

© Urheberrecht und Copyright: 2026 Controllit AG

Alle Rechte vorbehalten. / All rights reserved.

Die durch die Controllit AG erstellten Inhalte, Grafiken und Werke in diesem Dokument unterliegen dem deutschen Urheberrecht. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechtes bedürfen der schriftlichen Zustimmung des jeweiligen Autors bzw. Erstellers. Der Download dieses Dokuments sowie die Nutzung in Teilen oder in Gänze ist nicht für den kommerziellen Gebrauch gestattet. Die anderweitige Nutzung ist lediglich unter Nennung der Quellenangabe und der Urheber gestattet.

Soweit die Inhalte in diesem Dokument nicht von der der Controllit AG erstellt wurden, werden die Urheberrechte Dritter beachtet. Sollten Sie trotzdem auf eine Urheberrechtsverletzung aufmerksam werden, bitten wir um einen entsprechenden Hinweis.

Credits: Titel: iStock/yucelyilmaz; Seite 1: iStock/ClaudioVentrella; Seite 2: iStock/sabelskaya; Seite 4: iStock/undrey; Seite 6: iStock/yellowdesign; Seite 12: iStock/Hiranmay Baidya; Seite 19: iStock/Pavlo Stavnichuk