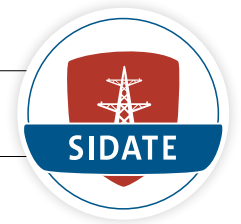


# Stand der IT-Sicherheit bei deutschen Stadtwerken

Julian Dax, Benedikt Ley, Sebastian Pape, Volkmar Pipek, Kai Rannenber, Christopher Schmitz, André Sekulla

Forschungsprojekt:  
SIDATE



## Stand der IT-Sicherheit bei deutschen Stromnetzbetreibern

Im Projekt SIDATE wurde eine Umfrage zum Stand der IT-Sicherheit bei deutschen Stromnetzbetreibern durchgeführt. Dazu wurden alle 881 im August 2016 bei der Bundesnetzagentur gelisteten Betreiber angeschrieben. Im Umfragezeitraum vom 1. September 2016 bis 15. Oktober 2016 antworteten von diesen 61 (6,9%) Betreiber. Der Fragebogen fokussiert auf die Umsetzung der rechtlichen Anforderungen und die Implementierung eines Managementsystems für Informationssicherheit (ISMS). Weiterhin wurden aber auch Fragen zu Leitsystem, Netzaufbau, Prozessen und organisationalen Strukturen und

zur Büro-IT gestellt. Nachfolgend werden einige ausgewählte Ergebnisse der Umfrage präsentiert. Die vollständige Umfrage ist als technischer Bericht verfügbar [1].

## Übersicht der teilnehmenden Stromnetzbetreiber

Zunächst wurde die Größe abhängig von den Zählpunkten der befragten Stromnetzbetreiber ermittelt. Anhand der Ergebnisse, wie in Abbildung 1 dargestellt ist, wurden vier etwa gleich große Gruppierungen festgelegt (kleine (bis 15.000 Zählpunkte), mittlere (15.001 bis 30.000 Zählpunkte), große (30.001 bis 100.000 Zählpunkte) und sehr große (ab 100.000 Zählpunkten) Stromnetzbetreiber).

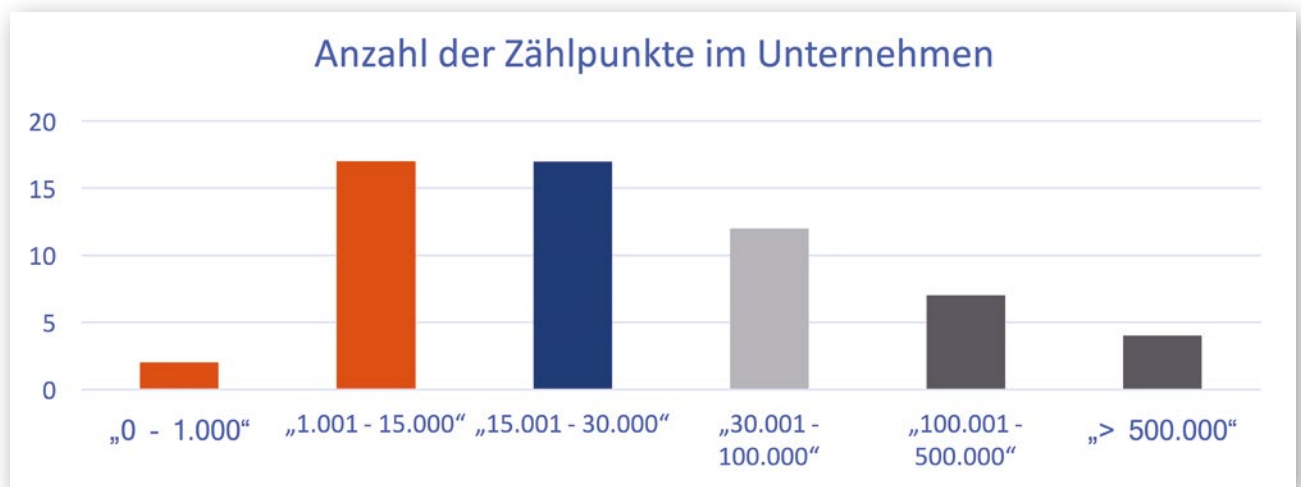


Abb. 1: Anzahl der Zählpunkte im Unternehmen

## IT-Sicherheit als Dienstleistung

Aus zwei weiteren Fragen (Abbildung 2) wird deutlich, dass der Großteil der Netzbetreiber auf externes Informationssicherheits-Know-how zurückgreift, insbesondere bei der Einführung eines ISMS (ohne Abbildung, siehe technischer Bericht [1]).

Auch für die Durchführung von Sicherheitsaudits (Abbildung 3) werden externe Dienstleister herangezogen. Diese sollen Schwachstellenscans oder Penetrationstests für die Systeme zur Steuerung der Netzleittechnik durchführen. Wobei etwa die Hälfte der Befragten angibt keine Sicherheitsaudits durchzuführen.

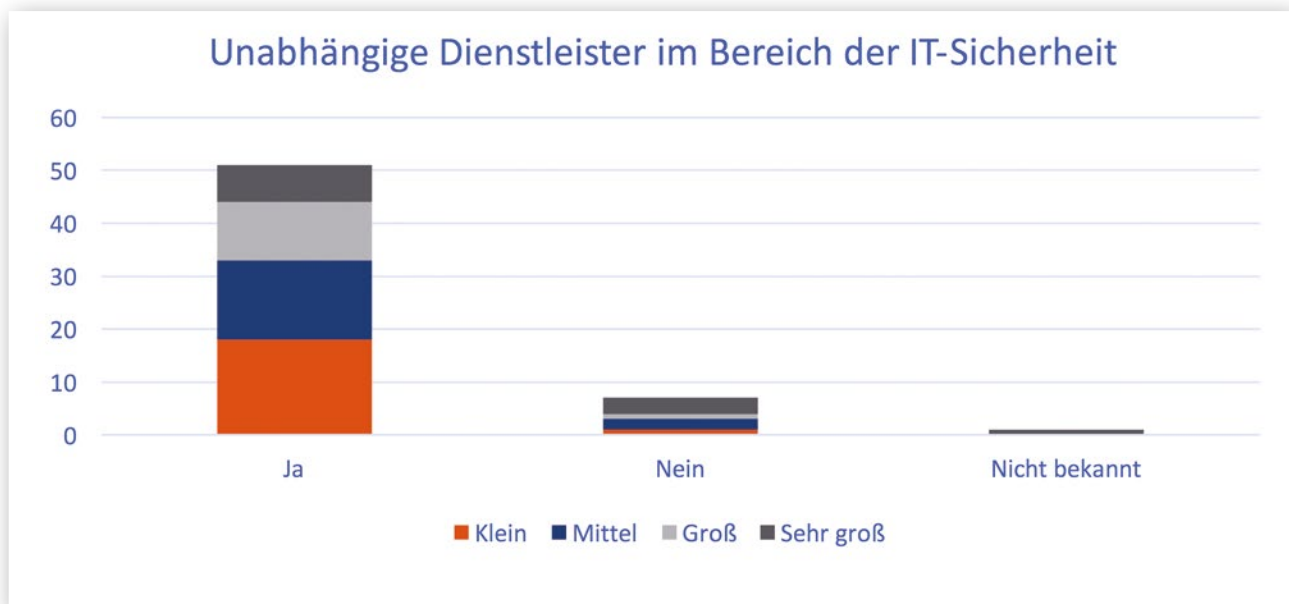


Abb. 2: Unabhängige Dienstleister im Bereich der IT-Sicherheit

## IT-Sicherheitsmanagement

Anhand der aufgeführten Umfrageergebnisse wird ersichtlich, daß ein Großteil der Stromnetzbetreiber ihre IT-Sicherheit an externe Dienstleister ausgelagert haben. Dies kann für eine kurzfristige Lösung, die Einführung des ISMS, sinnvoll sein. Auf längere Sicht gesehen sollten sich die Mitarbeiter des Betreibers dennoch vermehrt um IT-Sicherheit kümmern denn sie ist notwendig und wird immer wichtiger. An dieser Stelle soll das SIDATE Portal anknüpfen und als Wissensaustauschplattform zur Verbreitung von Erfahrungen in Bezug auf IT-Sicherheit und entsprechende Maßnahmen beitragen.

## Sicherheitsaudits und -leitlinien

Fast die Hälfte der befragten Stromnetzbetreiber führt keine regelmäßigen Sicherheitsaudits durch (siehe Abbildung 3). Die Stromnetzbetreiber, die Audits durchführen, greifen überwiegend entweder nur oder auch auf externe Dienstleister zurück, was den unter IT-Sicherheit als Dienstleistung beschriebenen Eindruck verstärkt. Ebenso verfügt fast die Hälfte der befragten Stromnetzbetreiber über keine Sicherheitsleitlinien (siehe Abbildung 4), die auch in regelmäßigen Zeitabständen überprüft und gegebenenfalls angepasst werden (ohne Abbildung, siehe technischer Bericht [1]).

Bei beiden Punkten ist der Trend zu sehen, daß der Anteil von Stromnetzbetreibern, die Sicherheitsaudits durchführen bzw. Leitlinien haben von kleinen zu mittleren zu (sehr) großen Betreibern zunimmt.

## ISMS-Einführung

Zur Zeit der Befragung haben die meisten Stromnetzbetreiber mit der Einführung eines Managementsystems für Informationssicherheit (ISMS) begonnen (siehe Abbildung 5). Im 2. Halbjahr 2017 planen über 85% die Einführung abgeschlossen zu haben. Abbildung 6 gibt einen detaillierten Einblick in den Stand der Einführung von ISMS bei den Betreibern. Hier wird z.B. deutlich das 36 der befragten Unternehmen mit der Erstellung der geforderten Dokumentationen begonnen haben und 24 bereits die Phase der Zielsetzung und des Scopings, d.h. der Frage welche Unternehmensbereiche vom ISMS abgedeckt werden sollen, beendet haben. Mit den Vorbereitungen auf das Zertifizierungsaudit hatten hingegen noch die wenigsten Energieversorger begonnen. Als Hauptgründe für die Einführung eines ISMS wurden rechtliche Anforderungen und die gestiegene

Bedrohungslage genannt (ohne Abbildung, siehe technischer Bericht [1]). Erwartungen an die Einführung des ISMS waren konsequenterweise dann auch die Erfüllung rechtlicher Anforderungen sowie die Verbesserung der Informationssicherheit im Unternehmen (ohne Abbildung, siehe technischer Bericht [1]).

## Risikoanalysen

Einer der komplexeren Teile des ISMS sind Risikoanalysen, bei denen das Risiko möglicher Sicherheitsvorfälle bewertet wird. Leider war etwas der Hälfte der Befragten nicht bekannt wie häufig Risikoanalysen im Unternehmen durchgeführt werden (siehe Abbildung 7). Positiv stimmt aber, dass bei der verbleibenden Hälfte die Mehrzahl Risikoanalysen mindestens einmal im Jahr durchgeführt.

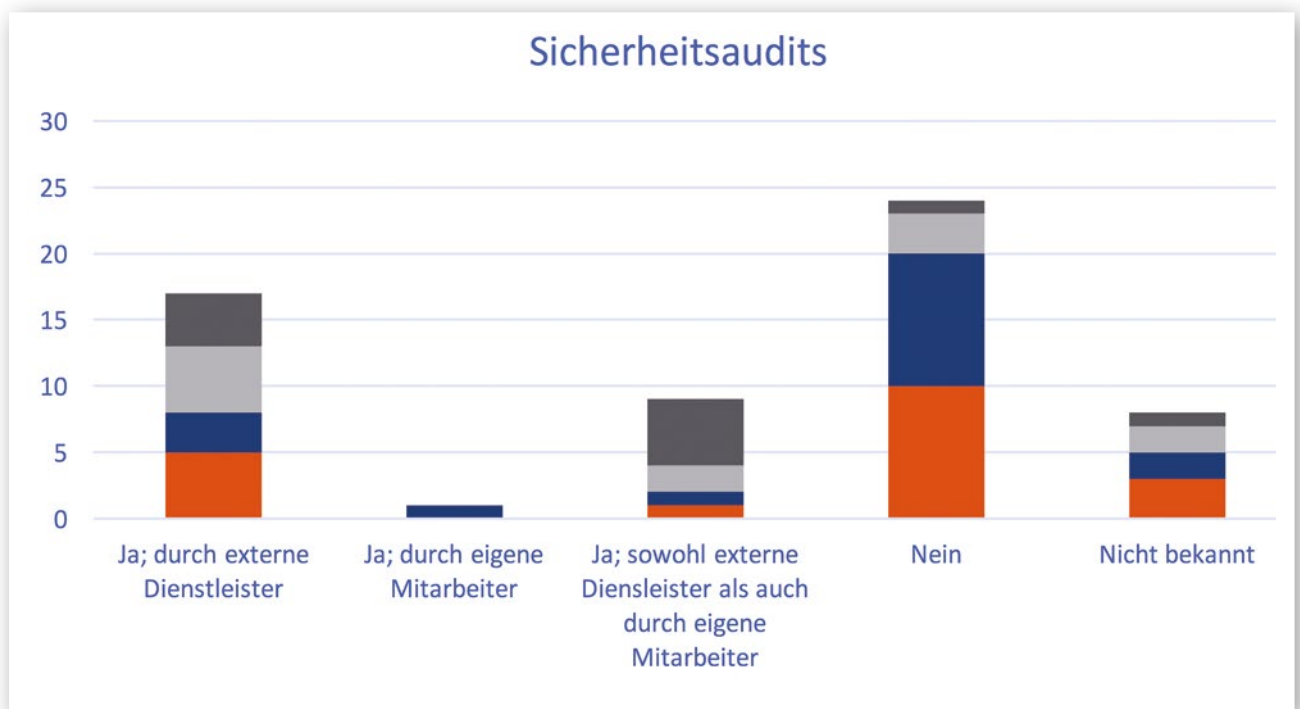


Abb. 3: Sicherheitsaudits

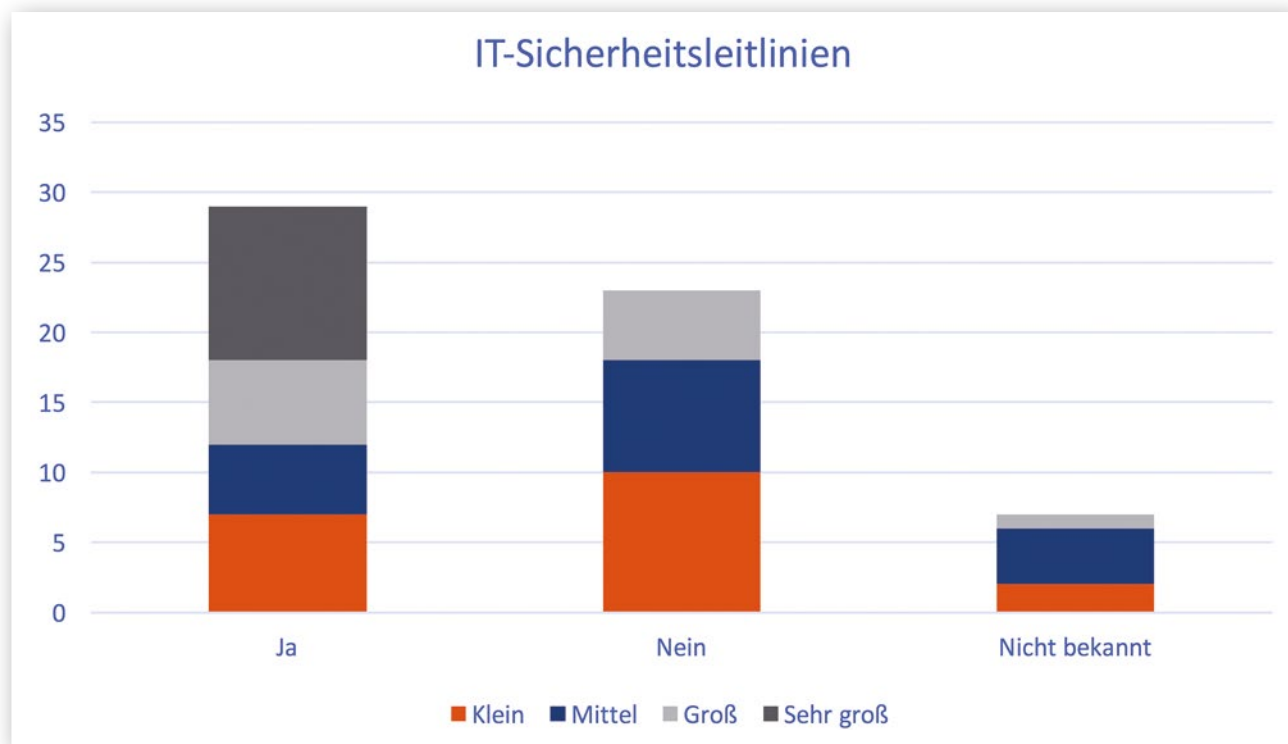


Abb. 4: IT-Sicherheitsleitlinien

Quelle

- [1] Dax, J.; Ley, B.; Pape, S.; Pipek, V.; Rannenber, K.; Schmitz, C. und Sekulla, A.: Stand zur IT-Sicherheit deutscher Stromnetzbetreiber: technischer Bericht, Universität Siegen, 2017. URL: <http://dokumentix.ub.uni-siegen.de/opus/volltexte/2017/1185/>.

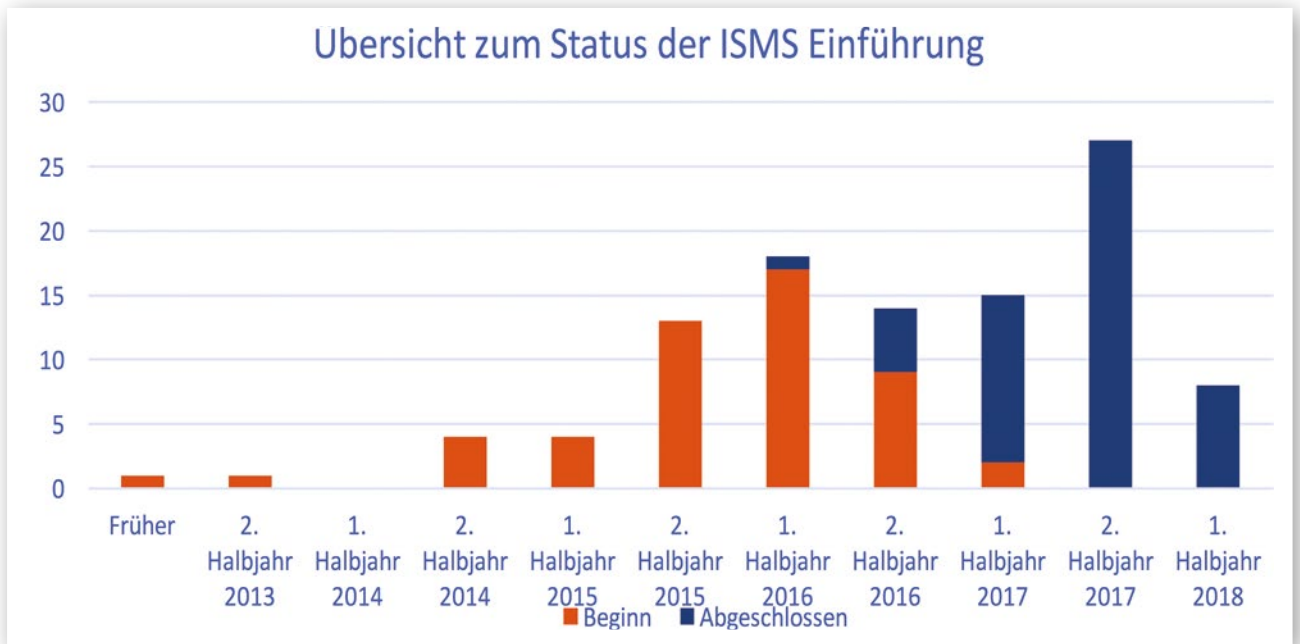


Abb. 5: Übersicht zum Status der ISMS Einführung

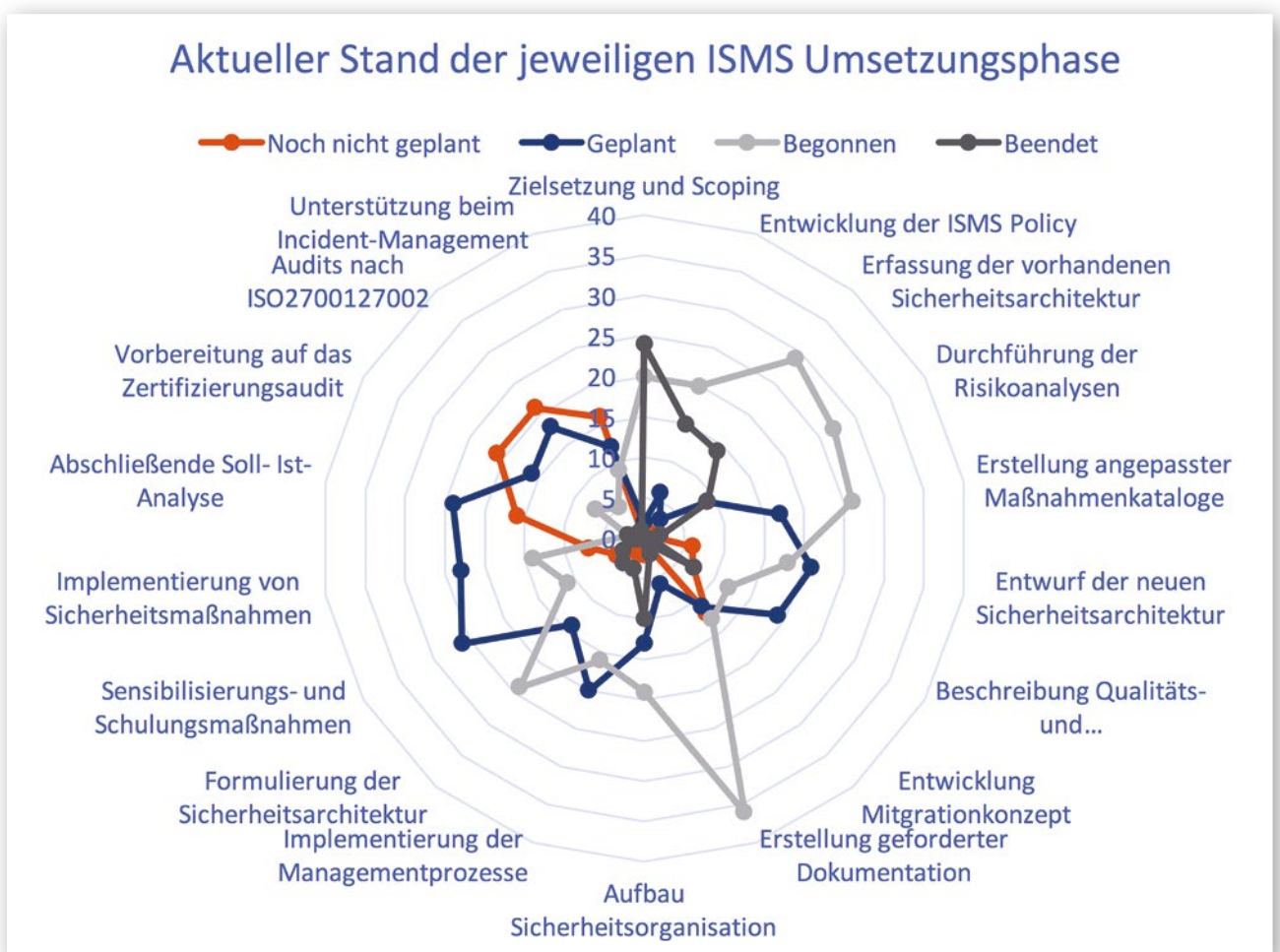


Abb. 6: Aktueller Stand der jeweiligen ISMS Umsetzungsphase

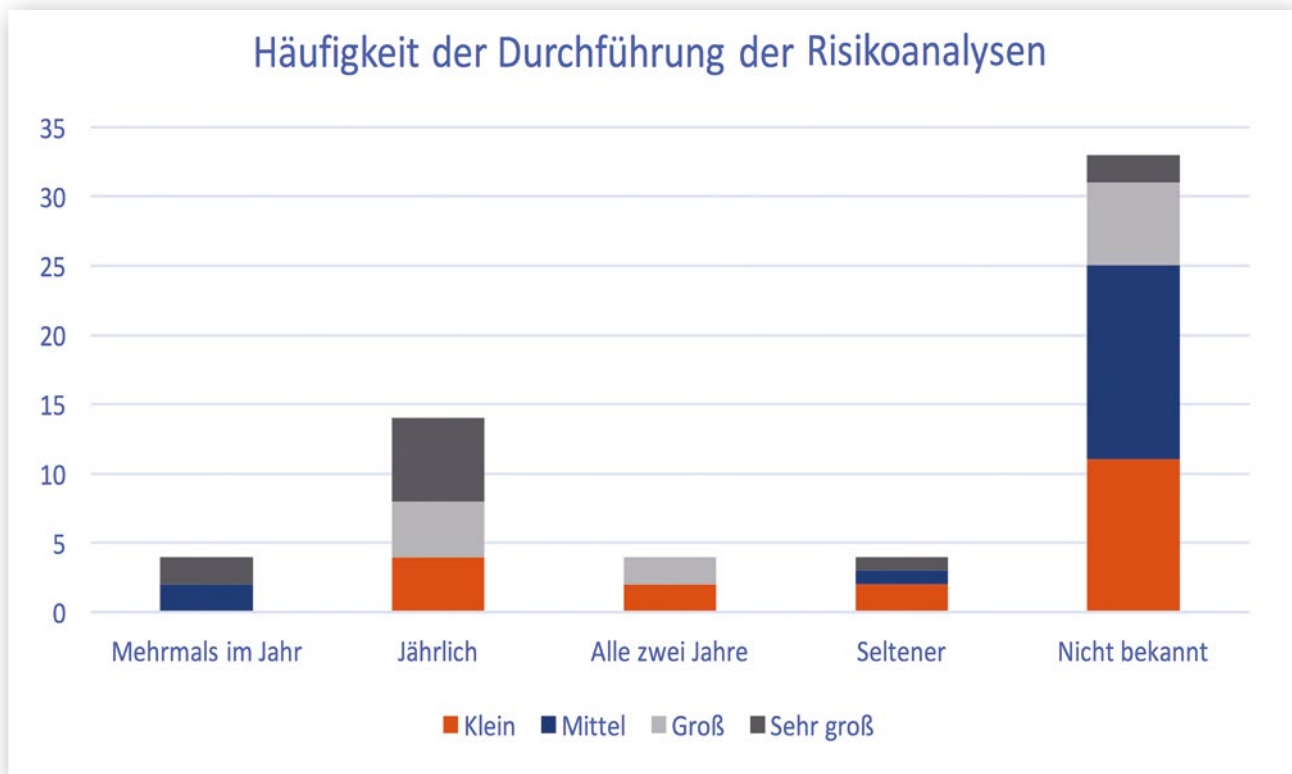


Abb. 7: Häufigkeit der Durchführung der Risikoanalysen