Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

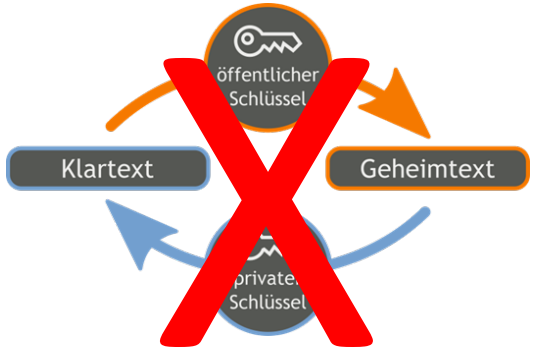
BSIs Leitfaden zu quantensicherer Kryptografie (Don‘t panic!?)

Dr. Heike Hagemeier, BSI, Referat TK 21

Security Forum „Quanten, Qubits und Security“, Brandenburg, 19.01.23

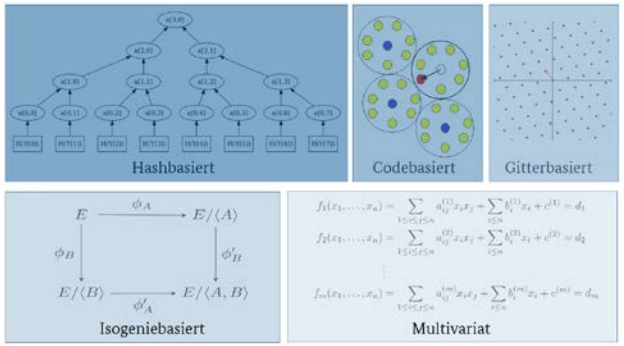
- Motivation
- Das „Theorem“ von Mosca
- X,Y und Z
- Empfehlungen und Aktivitäten des BSI
- Gemeinsame Umfrage „Kryptografie und Quantencomputing“ mit KPMG
- Fazit

Motivation

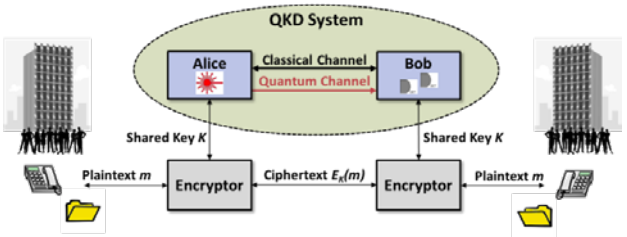


Derzeit eingesetzte Public-Key-Kryptografie

Post-Quanten-Kryptografie

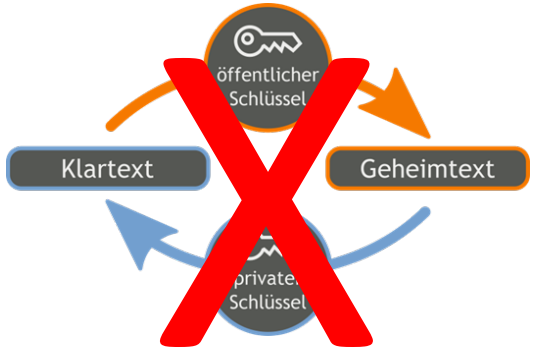


Quantensichere Kryptografie



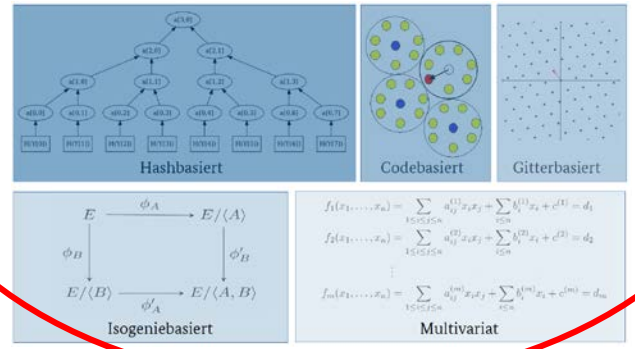
Quantum Key Distribution

Motivation

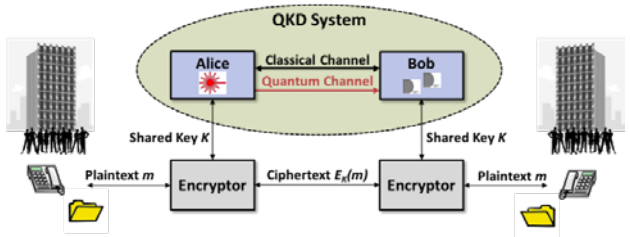


Derzeit eingesetzte Public-Key-Kryptografie

Post-Quanten-Kryptografie



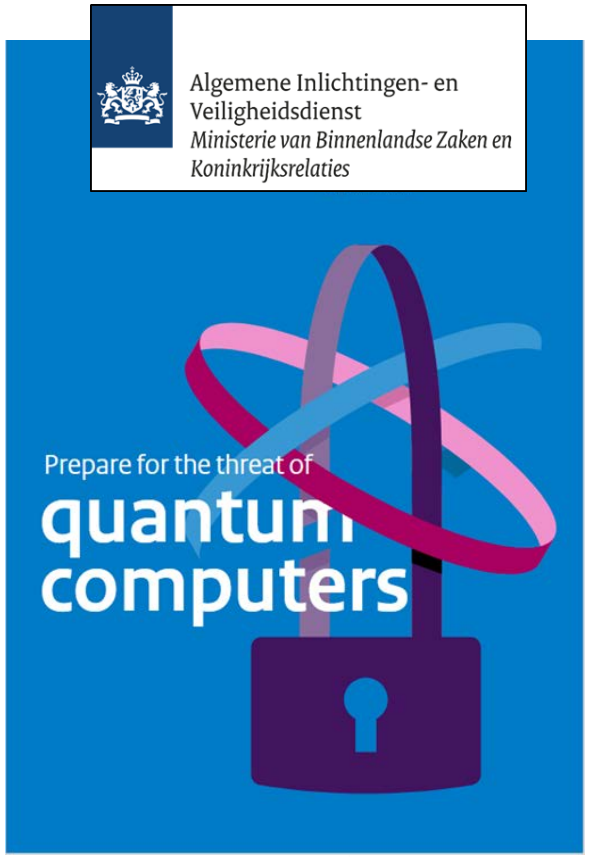
Quantensichere Kryptografie



Quantum Key Distribution

Was passiert in anderen Ländern?

Motivation II



THE WHITE HOUSE
WASHINGTON

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

BRIEFING ROOM › STATEMENTS AND RELEASES

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

COMPANIES EMERGING TECH FINANCIAL GOVERNMENT & PUBLIC SECTOR

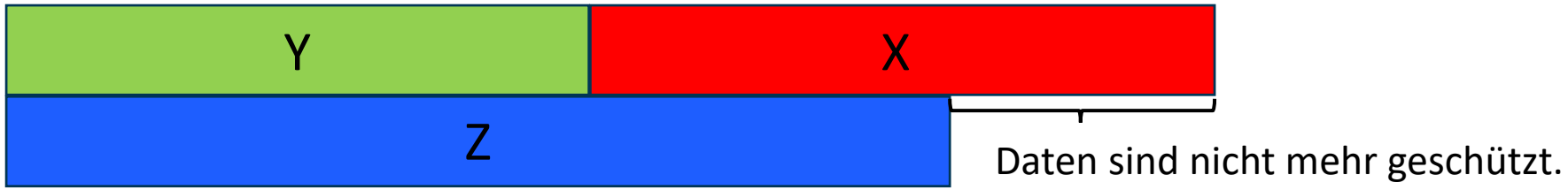
Government of Canada invests $360 million in new National Quantum Strategy

ASHEE PAMMA JANUARY 13, 2023

Wie viel Zeit bleibt für die Migration auf quantensichere Kryptografie?

Das hängt von folgenden Faktoren ab:

- Wie lange sollen Ihre Daten sicher bleiben? (X Jahre)
- Wie lange dauert die Umstellung Ihrer Systeme auf quantensichere Kryptografie? (Y Jahre)
- Wie lange wird es dauern, bis kryptografisch relevante Quantencomputer existieren? (Z Jahre)

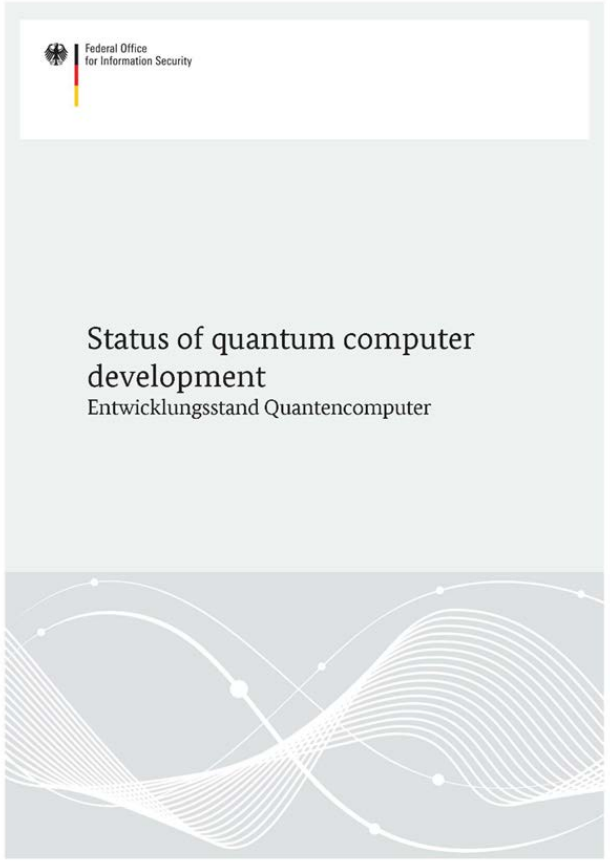


Mosca: Wenn X + Y > Z, dann haben Sie ein Problem!

Wie lange wird es dauern, bis kryptografisch relevante Quantencomputer existieren?

Wie groß ist Z?

BSI-Studie: „Entwicklungsstand Quantencomputer“



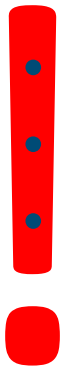
- Durchgeführt 2018 unter Leitung von Prof. Wilhelm-Mauch
- Zwei Revisionen: 2019, 2020
- Aktueller Stand verfügbar unter www.bsi.bund.de/qcstudie
- Aktuelles BSI-Projekt: Erneute Aktualisierung
- Projektleiter wieder Prof. Wilhelm-Mauch (jetzt FZ Jülich)
- Veröffentlichung der erneuten Revision in Q1/2023

„Highlights“ in der neuen Version:

- Bisher viel Rauch und wenig Feuer bei NISQ-Kryptanalyse
- Wir stehen am Übergang zu funktionierender Fehlerkorrektur
- Rydberg-Atome als ernstzunehmende Plattform

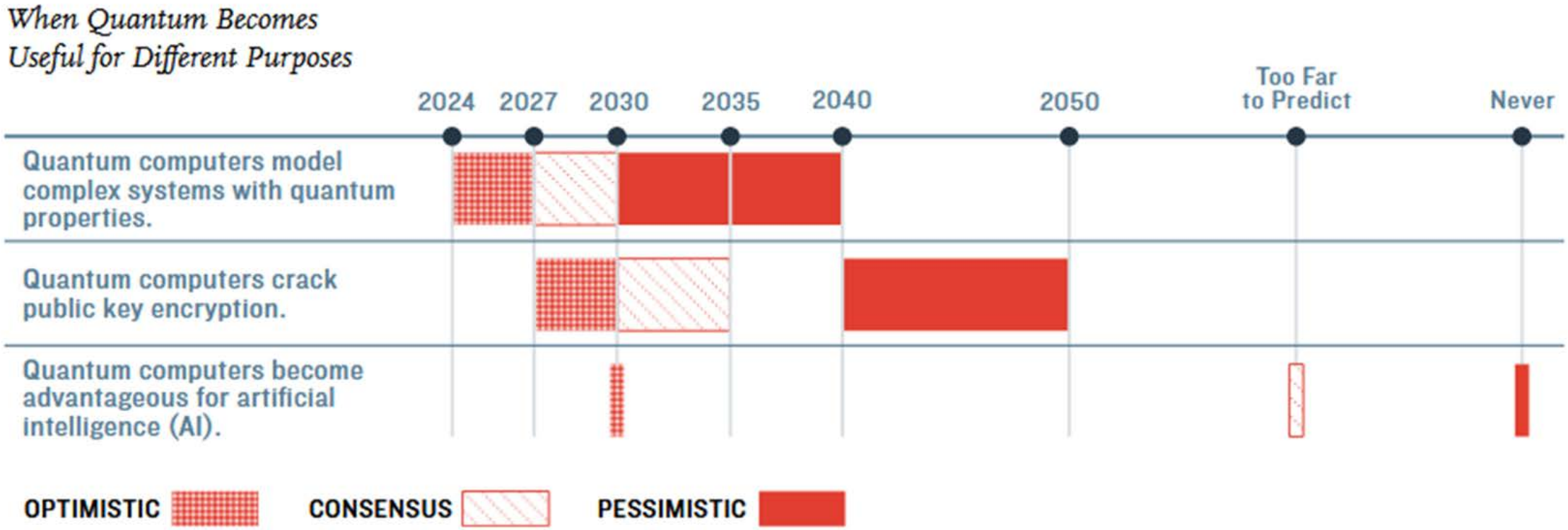
Arbeitshypothese des BSI für den Hochsicherheitsbereich

Mit signifikanter Wahrscheinlichkeit gibt es Anfang der 2030er Jahre einen kryptografisch relevanten Quantencomputer



- **Keine** Prognose
- „kryptografisch relevant“ ist nicht wohldefiniert
- Detaillierte Analyse in der QC-Studie

Report von Booz Allen Hamilton (Januar 2022)



Wie groß ist X?

Unterschiedliche Bedrohungsszenarien

Vertraulichkeit

- „Store now, decrypt later“ **Bedrohung**

➢ Verschlüsselung und Schlüsseleinigung(!) muss so lange sicher sein, wie die zu schützenden Daten vertraulich bleiben sollen.

Authentizität

- Signaturen müssen meist nur kurzfristig sicher sein, Problem bei langen Laufzeiten von Zertifikaten
- Migration der Systeme voraussichtlich sehr aufwändig

➢ rechtzeitiger Umstieg notwendig

Wie groß ist Y?

NIST-Prozess („A long and winding road“)

Weitere Schritte notwendig für…

… **die Migration zu Post-Quanten-Kryptografie**:

- Erweiterung kryptografischer Protokolle
- Anpassung digitaler Zertifikate und von PKIen
- Implementierung in Kryptobibliotheken
- Implementierung in Produkten
- ….

… **die Einsatzreife von Quantum Key Distribution**:

- Sicherheitsuntersuchungen
- Standardisierung von Protokollen
- Erarbeitung zugehöriger Sicherheitsbeweise
- Zertifizierung von Produkten
- ….

Empfehlungen und Aktivitäten des BSI

BSIs Leitfaden zu quantensicherer Kryptografie

Empfehlungen u.a.

- Rechtzeitige Risikoanalyse
- Kryptoagilität
- Hybride Lösungen
- FrodoKEM und Classic McEliece für Schlüsseleinigung
- Hashbasierte Signaturen für bestimmte Anwendungen, z.B. Firmware-Updates
- Quantum Key Distribution ist bzgl. Sicherheit noch nicht einsatzreif
- Migration zu Post-Quanten-Kryptografie hat Vorrang vor Quantum Key Distribution
- Weitere Forschung und Dialog notwendig!

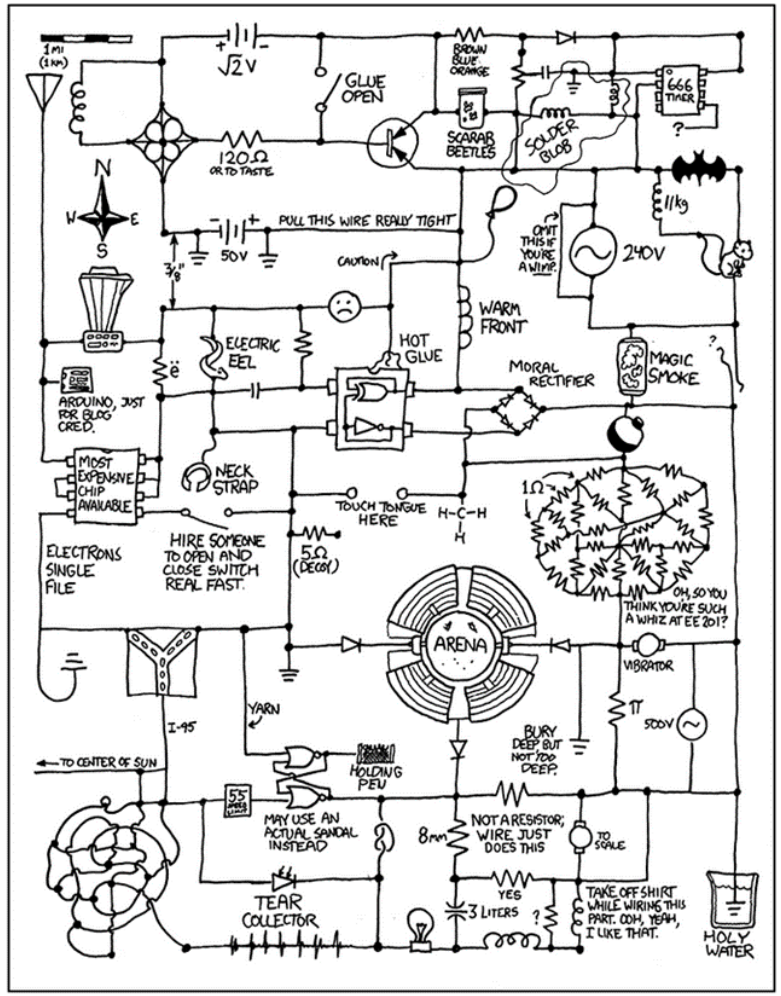
Verfügbar unter www.bsi.bund.de/PQ-Migration

Hochsicherheitsbereich

- Zeitplan für Migration entsprechend Arbeitshypothese
- Priorität: Schutz von GEHEIM; Schlüsseleinigung
- Erstes für GEHEIM-zugelassenes Produkt mit hybrider Schlüsseleinigung seit Juli 2021

Informationssicherheit im Wandel

Migration zu Post-Quanten-Kryptografie



Quelle: https://xkcd.com/730/

BSI Projekte zu Post-Quanten-Kryptografie

"Pflege und Weiterentwicklung der Kryptobibliothek Botan"	"Integration von Post-Quanten-Kryptografie in den E-Mail Client Thunderbird"
• Aktualisierung des BSI-Zweigs von Botan • Implementierung von Post-Quanten-Kryptografie in Botan • Hybride Schlüsseleinigung für TLS 1.3 • Start 01/22, Laufzeit 3 Jahre • Ansprechpartner: Dr. Stephan Ehlen	• Quantencomputerresistente E-Mail-Verschlüsselung und Signatur • Standardisierungsentwurf OpenPGP • Beteiligung an Arbeitsgruppen „lamps“ und „openpgp“ der IETF • Start 01/22, Laufzeit 3 Jahre • Ansprechpartner: Dr. Stavros Kousidis

BSI-Projekte und Aktivitäten zu Quantum Key Distribution

- BSI-ETSI Common Criteria Protection Profile für Prepare-and-Measure QKD
  - PP soll Mitte 2023 zertifiziert sein
  - Es müssen noch Hintergrunddokumente und Standards entwickelt werden

- Studie zu Seitenkanalangriffen auf QKD Systeme
  - Wird Mitte 2023 zur Kommentierung verteilt werden
  - Veröffentlichung voraussichtlich Ende 2023

- Schirmprojekt Quantenkommunikation Deutschland (SQuaD)
  - Koordination in Zusammenarbeit mit PTB
  - Input zu Aspekten der IT-Sicherheit

Wie schätzen Unternehmen X, Y und Z ein?

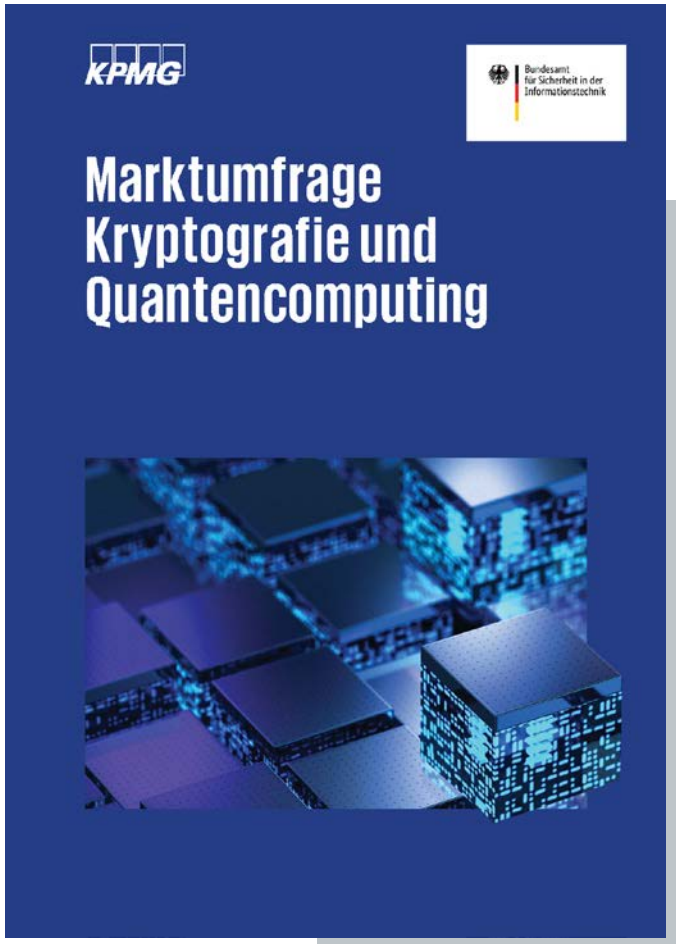
Umfrage „Kryptografie und Quantencomputing“

Umfrage „Kryptografie und Quantencomputing“

Umfrage von KPMG, Deutschland und BSI zu Kryptografie und Quantencomputing

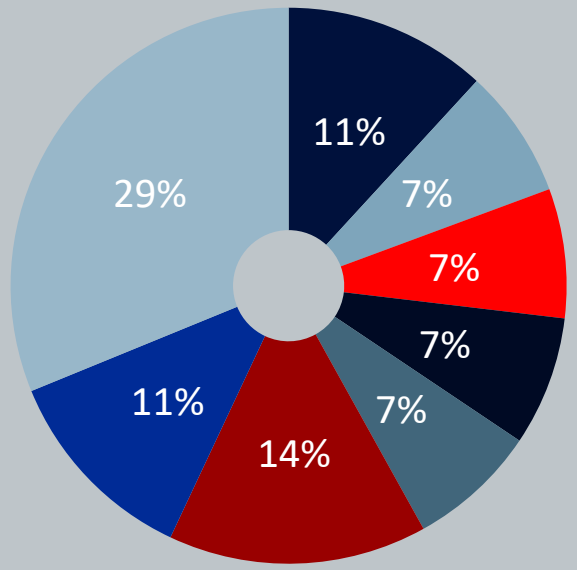
- Basiert auf dem BSI-Leitfaden "Kryptografie quantensicher gestalten".
- Richtet sich an alle interessierten Unternehmen und Organisationen (insb. an das Produktmanagement für Sicherheitsfunktionen, CISO's oder CIO's).
- Jede teilnehmende Organisation erhält einen individualisierten Ergebnisbericht.
- **Ziel: Erhöhung der Awareness zum Thema quantensichere Kryptografie und einen Überblick über die Lage in Deutschland erhalten.**

Allianz für Cyber-Sicherheit



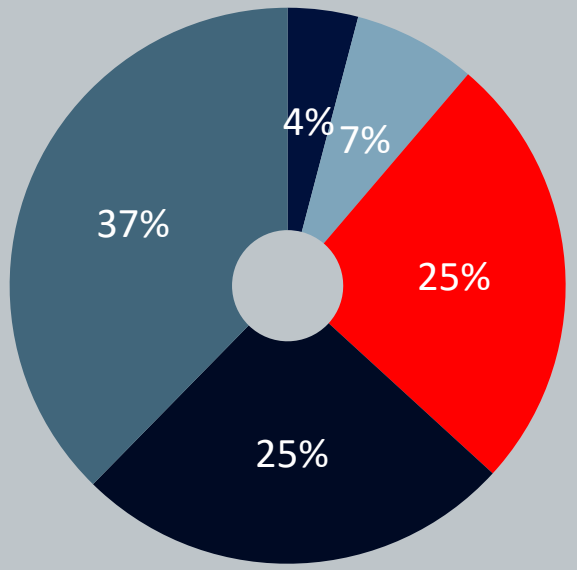
Übersicht – Demografische Daten

Branche



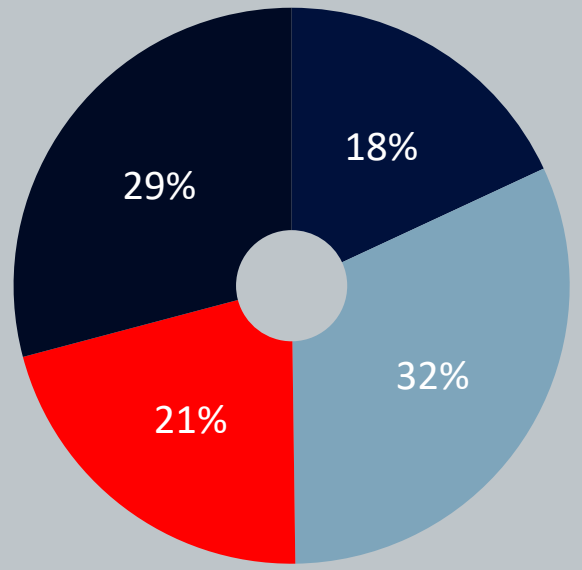
- Chemicals & Pharmaceuticals
- Technology
- Energy & Natural Resources
- Telecommunications
- Government
- Industrial Manufacturing
- Transport & Logistics/Leisure
- Banking

Anzahl Mitarbeiter



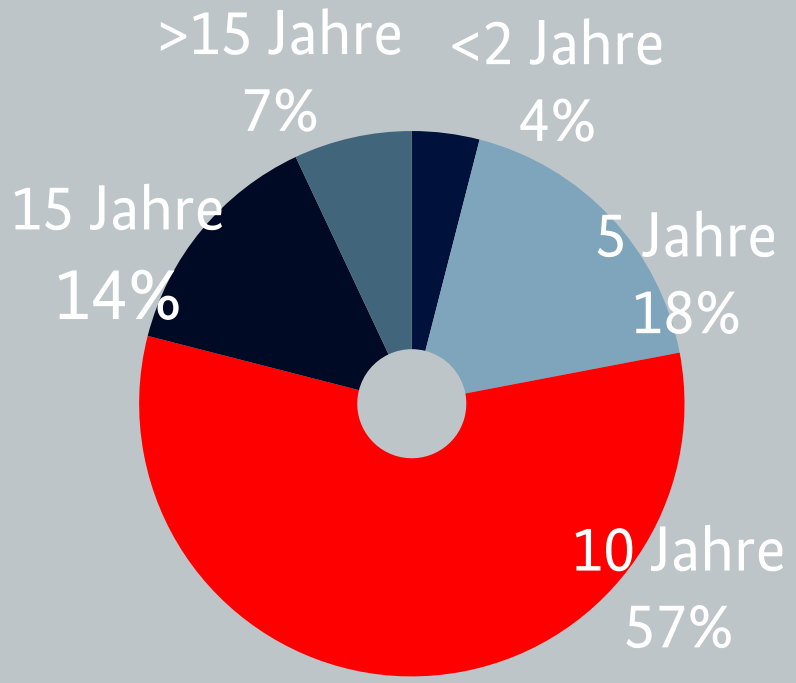
- Weniger als 100
- Zwischen 100 und 1000
- Zwischen 1000 und 10000
- Zwischen 10000 und 50000
- Mehr als 50000

Gesamtumsatz

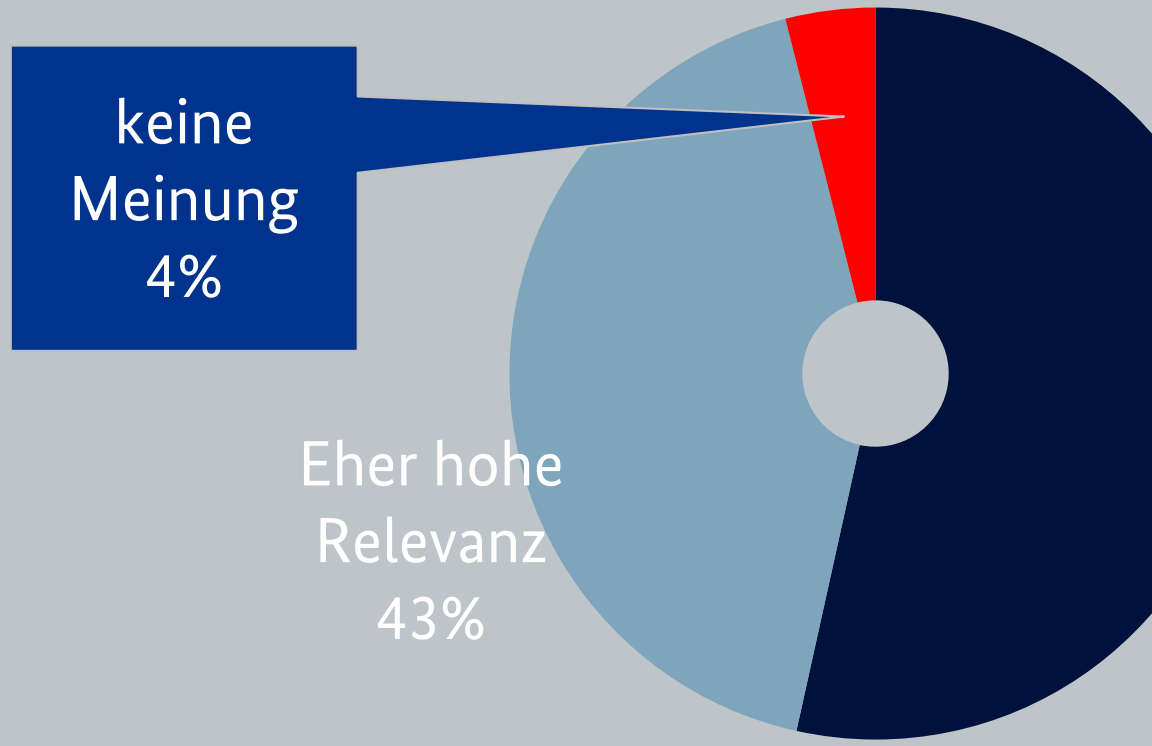


- Bis 1 Mrd. Euro
- Zwischen 1 und 10 Mrd. Euro
- Zwischen 10 und 50 Mrd. Euro
- Mehr als 50 Mrd. Euro

Wann schätzen Sie werden Quantencomputer in der Lage sein, bestimmte, heute eingesetzte kryptographische Verfahren zu brechen?

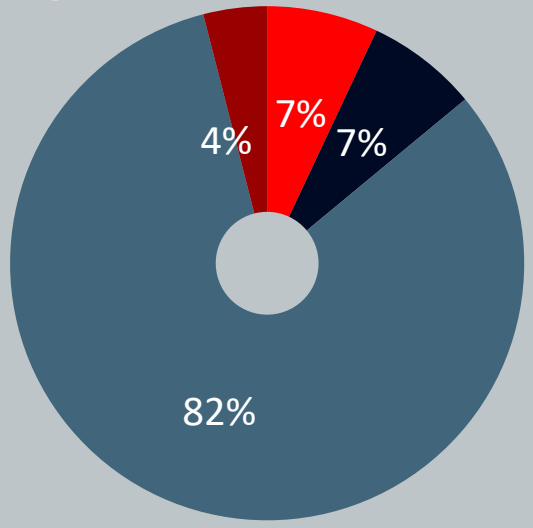


Welche Relevanz von Quantencomputing für die Sicherheit von kryptographischen Verfahren erwarten Sie generell?



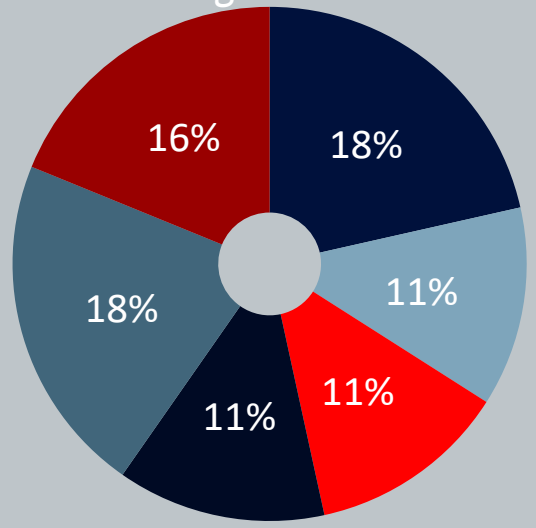
Bitte geben Sie uns Ihre Einschätzung zur zeitlichen Entwicklung

Maximale Dauer, für die Informationen durch Ihre Organisation vertraulich gehalten werden müssen?



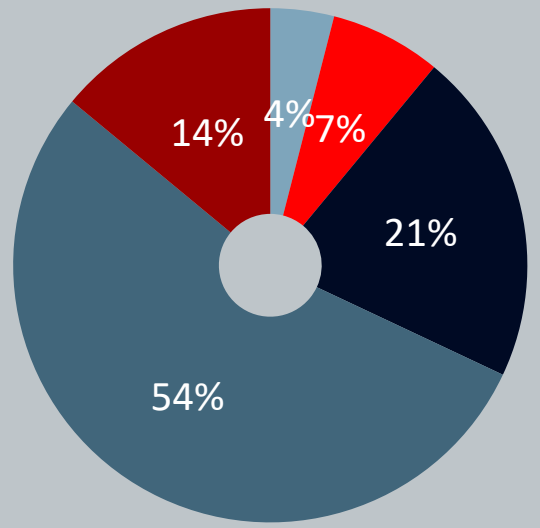
- <1 Jahr
- 1 Jahr
- 3 Jahre
- 5 Jahre
- >5 Jahre
- nicht anwendbar/relevant

Wann plant Ihre Organisation mit der Umstellung auf quantensichere Kryptographie zu beginnen?



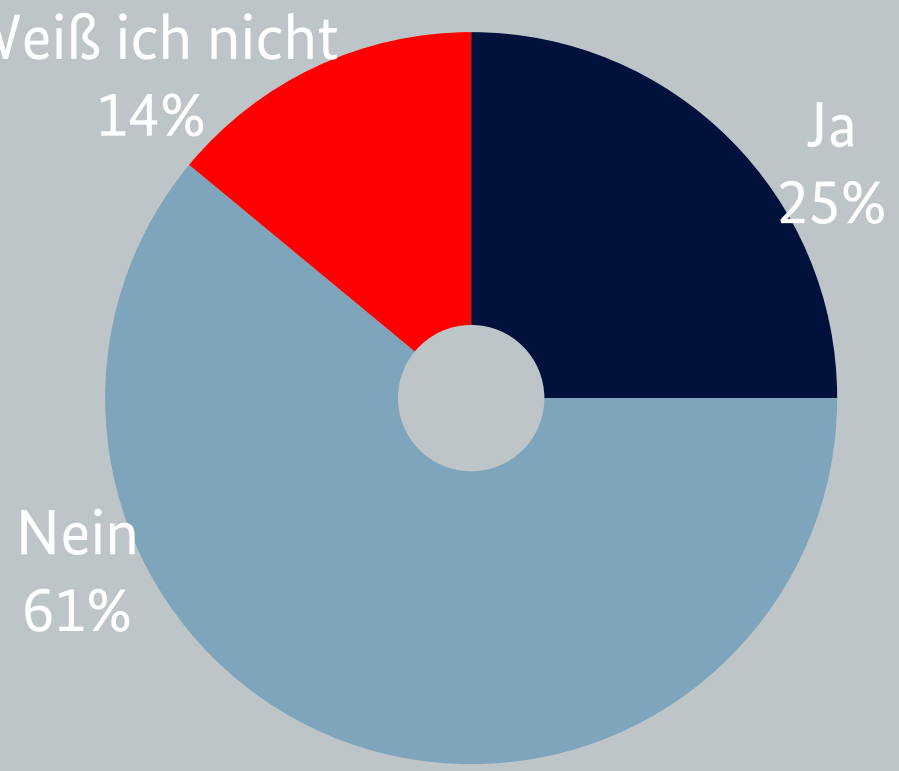
- <1 Jahr
- 1 Jahr
- 3 Jahre
- 5 Jahre
- >5 Jahre
- nicht anwendbar/relevant

Wie lange wird Ihrer Meinung nach Ihre Organisation für die Realisierung der Quantenresistenz benötigen?

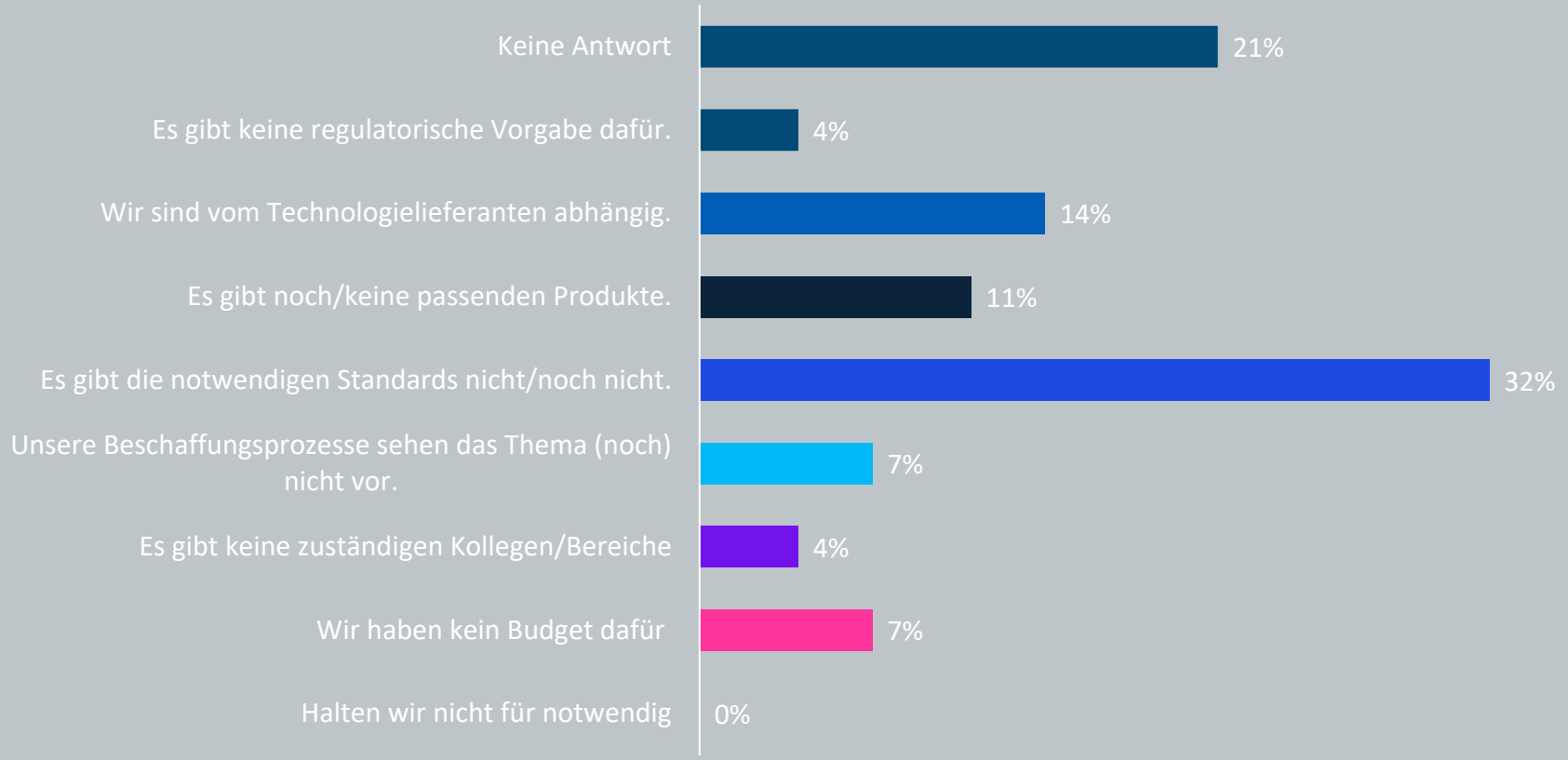


- <1 Jahr
- 1 Jahr
- 3 Jahre
- 5 Jahre
- >5 Jahre
- nicht anwendbar/relevant

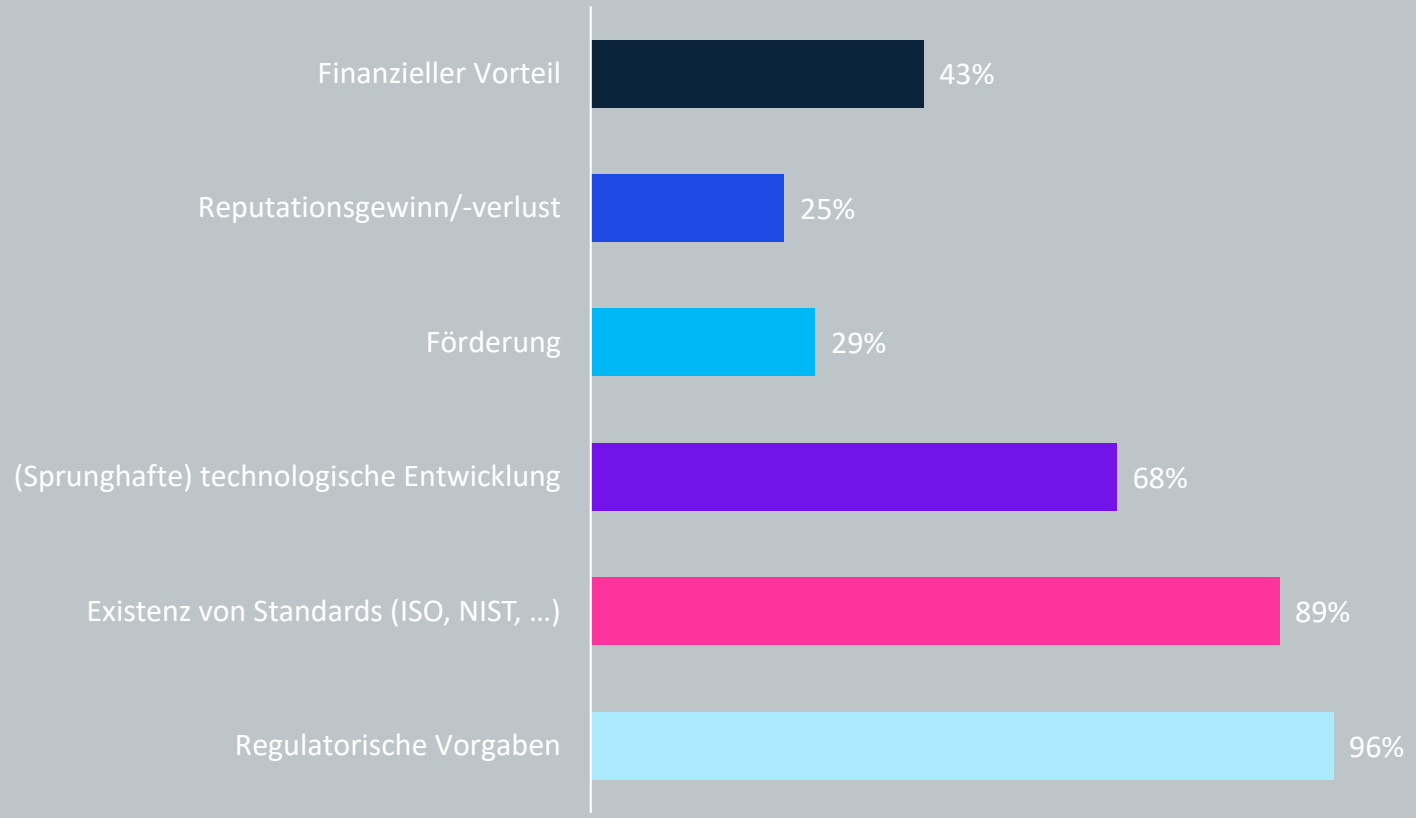
Wird das Thema „Gefährdung der Kryptographie durch Quantencomputing“ im Risikomanagement berücksichtigt?



Falls in Ihrer Organisation keine Initiativen/Vorhaben zu diesem Thema existieren – warum nicht?



Was würde Investitionsentscheidungen begünstigen?



Fazit

Deutschland
Digital•Sicher•BSI•

- Kryptografischer Umbruch muss und wird kommen.
- Migration zu quantensicherer Kryptografie ist voraussichtlich langwierig.
- Inventur und Risikobewertung bereits jetzt möglich.
- Es können sich jederzeit sprunghafte Entwicklungen in der Kryptanalyse ergeben. (Gilt auch unabhängig von Quantencomputern.)
- Kryptoagilität sollte ein Designkriterium sein!

Weitere Informationen: https://bsi.bund.de/Quanten