



Standpunkt

CGI Quantum Risk Assessment



Strukturiert zur Quantum Readiness

Viele Unternehmen haben die Relevanz von Quantencomputing und Post-Quanten-Kryptografie bereits erkannt. Um ihre IT auf das Quantenzeitalter vorzubereiten, benötigen sie jedoch einen strukturierten Ansatz.

Mit dem CGI Quantum Risk Assessment unterstützen wir Organisationen dabei, diese Transformation systematisch zu gestalten. Dazu verbinden wir strategische Fragestellungen mit einer fundierten technischen Analyse und begleiten sie von der ersten Standortbestimmung bis zur Umsetzung.

Unser Standpunkt erklärt den Aufbau des Assessments und zeigt, wie Unternehmen den Übergang zur quantensicheren IT wirtschaftlich sinnvoll umsetzen können.



Erst verstehen, dann handeln

Die grundsätzlichen Auswirkungen leistungsfähiger Quantencomputer auf bestehende kryptografische Verfahren haben wir bereits in unserem Standpunkt zur quantensicheren IT erläutert. Für viele Organisationen stellt sich nach der ersten Einordnung jedoch eine ganz praktische Frage: Wie entwickelt man aus dem Wissen um die Risiken einen konkreten und umsetzbaren Handlungsplan?

Genau an diesem Punkt beginnt für die meisten Unternehmen die eigentliche Herausforderung. Sie wissen, dass Handlungsbedarf besteht, überblicken ihre kryptografischen Abhängigkeiten und Risiken jedoch nicht vollständig.

Warum Transparenz entscheidend ist

Moderne IT-Landschaften basieren auf einer Vielzahl von Vertrauensmechanismen: Zertifikate, digitale Identitäten, Signaturen und Authentifizierungsverfahren bilden die Grundlage einer sicheren Kommunikation und vertrauenswürdiger Geschäftsprozesse.

Unternehmen müssen daher erst einmal verstehen, wo in ihrer IT-Landschaft kryptografische Verfahren eingesetzt werden und welche Systeme davon abhängig sind. Dieses Wissen fließt dann in alle weiteren Entscheidungen ein.

In der Praxis ist dies häufig schwieriger als erwartet. Kryptografie ist tief in den Anwendungen, Netzwerken, Cloud-Plattformen, Identitätslösungen, Kommunikationssystemen und industriellen Umgebungen verankert.

Änderungen an einzelnen kryptografischen Komponenten können daher Auswirkungen auf zahlreiche Anwendungen, Schnittstellen und Partnerbeziehungen haben. Die Herausforderung liegt häufig nicht in einzelnen Systemen, sondern in den dahinterliegenden Vertrauensketten und Abhängigkeiten.

Einflüsse von außen erhöhen die Komplexität zusätzlich. Denn Softwarehersteller, Cloud-Anbieter, Lieferanten und Partner verwenden eigene kryptografische Komponenten, die nur eingeschränkt sichtbar sind.

Quantum Readiness – eine gemeinsame Aufgabe

Neben den technischen Fragestellungen spielen auch organisatorische Aspekte eine wichtige Rolle. Quantum Readiness betrifft nicht ausschließlich die IT und die Informationssicherheit. Verantwortliche aus der IT-Architektur, den Fachbereichen, dem Risikomanagement, der Compliance und dem Einkauf müssen gemeinsam mit dem Management Entscheidungen treffen und die weitere Transformation steuern.

Mehr als eine Technologieinitiative

Gerade deshalb ist Quantum Readiness keine isolierte Technologieinitiative und entsteht nicht durch das Einführen einzelner kryptografischer Verfahren. Benötigt wird ein strukturierter Ansatz, der technische, organisatorische und geschäftliche Anforderungen miteinander verbindet.

Gleichzeitig gilt es, den Schutzbedarf der verschiedenen Systeme und Daten realistisch einzuordnen. Während einige Informationen nur für kurze Zeit vertraulich bleiben müssen, erfordern andere einen Schutz über viele Jahre oder sogar Jahrzehnte hinweg.

Auf dieser Grundlage müssen die Risiken konsequent bewertet und die Ressourcen gezielt auf die Bereiche mit dem größten Handlungsbedarf ausgerichtet werden.

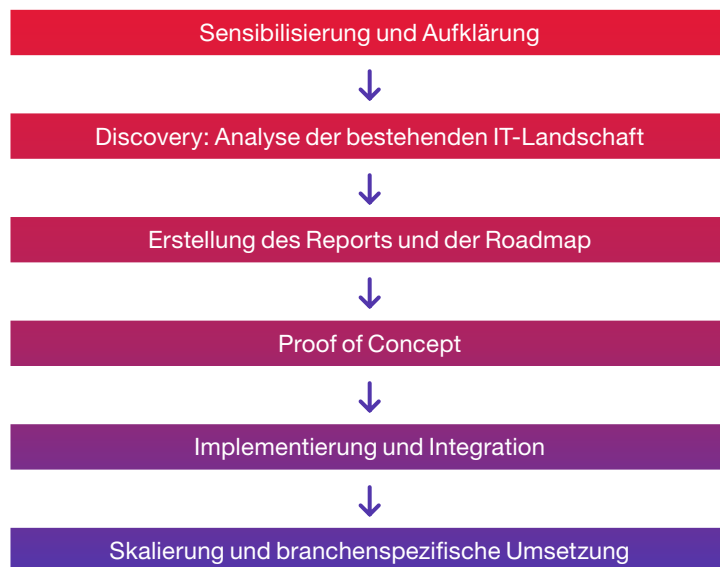
Genau hier setzt unser CGI Quantum Risk Assessment an. Es ermöglicht fundierte Entscheidungen auf Management-, Architektur- und Security-Ebene und schafft die Grundlage für die weitere Transformation.



Das CGI Quantum Risk Assessment im Überblick

Mit dem CGI Quantum Risk Assessment unterstützen wir Unternehmen dabei, den Übergang zur quantensicheren IT strukturiert zu gestalten. Unser ganzheitlicher Ansatz begleitet sie von der ersten Einordnung ihrer Ausgangssituation bis zur schrittweisen Umsetzung konkreter Maßnahmen.

Das Assessment gliedert sich in sechs aufeinander aufbauende Phasen.



Die Phasen des CGI Quantum Risk Assessments

Der erste Schritt zur Quantum Readiness besteht darin, ein gemeinsames Verständnis der Auswirkungen von Quantencomputing auf die eigene Organisation zu schaffen. Diese Sensibilisierungs- und Aufklärungsphase bildet die Grundlage für alle weiteren Aktivitäten.

Phase 1 – Sensibilisierung und Aufklärung

Ziel ist es, relevante Stakeholder auf die Quantenbedrohung und ihre möglichen Folgen aufmerksam zu machen. Dabei werden die grundlegenden Zusammenhänge eingeordnet und die Relevanz für die eigene Organisation wird bewertet.

Im Fokus stehen Fragen wie: Welche Bedeutung haben Quantencomputer für unsere Sicherheitsstrategie? Welche Risiken ergeben sich durch langfristig schutzbedürftige Daten? Und welche Vorbereitungen sollten bereits heute getroffen werden?

Besondere Bedeutung hat dabei das „Harvest now, decrypt later“-Szenario. Daten mit langfristigem Schutzbedarf können bereits heute abgefangen und gespeichert werden, um sie zukünftig zu entschlüsseln. Dadurch entsteht Handlungsbedarf lange vor einem möglichen Q-Day.

Am Ende der Phase eins verfügen das Management, die Security- und Architektur-Verantwortlichen sowie die Expertinnen und Experten aus den Fachbereichen über ein einheitliches Bild der Risiken und ihrer Bedeutung für die Organisation. Erste Handlungsfelder werden sichtbar und die Voraussetzungen für fundierte Entscheidungen geschaffen.

Phase 2 – Discovery: Analyse der bestehenden IT-Landschaft

Nach der Sensibilisierung der relevanten Stakeholder richtet sich der Fokus in der zweiten Phase des Assessments auf die bestehende Unternehmenslandschaft. Bevor Risiken bewertet oder konkrete Maßnahmen geplant werden können, müssen zunächst die eingesetzten kryptografischen Verfahren erfasst werden.

Ziel der Infrastruktur-Analyse ist es, ein möglichst vollständiges Verständnis der kryptografischen Landschaft einer Organisation zu gewinnen. Geklärt werden müssen verschiedene Punkte wie: Welche Systeme und Anwendungen nutzen kryptografische Verfahren? Welche Vertrauensketten existieren innerhalb der Organisation und zu externen Partnern? Und welche Komponenten könnten von zukünftigen kryptografischen Veränderungen betroffen sein?

Dazu werden technische Analysen mit der Auswertung bestehender Dokumentationen und Interviews mit Fachbereichen, Infrastruktur- und Security-Teams kombiniert. Ziel ist dabei nicht, jede einzelne Komponente zu erfassen, sondern eine belastbare Grundlage für die nachfolgenden Bewertungs- und Planungsphasen zu bilden.

So entsteht ein umfassender Überblick darüber, wo und in welchem Umfang Kryptografie eingesetzt wird. Kritische Systeme, relevante Abhängigkeiten und potenzielle Risikobereiche werden identifiziert und dokumentiert.



Phase 3 – Erstellung des Reports und der Roadmap

Die dritte Phase bildet den Übergang von der Analyse zur strategischen Planung. Im Mittelpunkt steht die Frage, welche Konsequenzen sich aus den gewonnenen Erkenntnissen für die weitere Transformation ergeben.

Die Ergebnisse der vorangegangenen Analysen werden zusammengeführt, bewertet und in einen unternehmensspezifischen Kontext eingeordnet. Daraus können Prioritäten für die weitere Transformation und konkrete Handlungsempfehlungen für Management, IT-Architektur und Security abgeleitet werden.

Alles dreht sich um Fragen wie: Welche Risiken besitzen die höchste Relevanz für das Unternehmen? Welche Systeme oder Prozesse sollten mit besonderer Priorität betrachtet werden? Welche regulatorischen oder branchenspezifischen Anforderungen müssen berücksichtigt werden? Und welche Maßnahmen können kurz-, mittel- und langfristig zur Verbesserung der Quantum Readiness beitragen?

Ein zentrales Ergebnis dieser Phase ist die Entwicklung einer Quantum-Readiness-Roadmap. Sie beschreibt, welche Maßnahmen in welcher Reihenfolge umgesetzt werden sollten und schafft die Grundlage für die weitere Transformation.

Phase 4 – Proof of Concept

Nach der Entwicklung der Roadmap müssen ausgewählte Lösungsansätze unter realistischen Bedingungen überprüft werden. Die Proof-of-Concept-Phase bildet den Übergang von der strategischen Planung zur praktischen Erprobung.

Beantwortet werden müssen Fragen wie: Welche Auswirkungen haben neue kryptografische Verfahren auf bestehende Anwendungen? Wie verhalten sich die Systeme hinsichtlich Performance, Skalierbarkeit und Kompatibilität? Welche technischen oder organisatorischen Herausforderungen können bei einer späteren Migration auftreten? Und welche Lösungsansätze eignen sich am besten für die Anforderungen der Organisation?

Der Fokus liegt nicht auf einer vollständigen Migration, sondern auf der gezielten Validierung ausgewählter Szenarien. Dazu können beispielsweise Testumgebungen aufgebaut, Pilotanwendungen betrachtet oder einzelne Integrationspfade untersucht werden.

Die Validierung liefert belastbare Erkenntnisse über die praktische Umsetzbarkeit und die möglichen Auswirkungen auf die bestehende IT-Landschaft. Potenzielle Risiken und Optimierungsmöglichkeiten werden sichtbar und können in die weitere Planung einfließen.



Phase 5 – Implementierung und Integration

Nach der Validierung ausgewählter Lösungsansätze beginnt in Phase fünf die schrittweise Realisierung der definierten Maßnahmen. Hierbei gilt es, die bisherigen Ergebnisse des Assessments nachhaltig in der Organisation zu verankern.

Für die praktische Umsetzung sind unter anderem folgende Fragen relevant: Welche Maßnahmen sollten in welcher Reihenfolge umgesetzt werden? Wie lassen sich die Risiken während der Transformation minimieren? Welche organisatorischen Voraussetzungen müssen geschaffen werden? Und wie können die bestehenden Prozesse, Governance-Strukturen und Sicherheitsrichtlinien entsprechend angepasst werden?

Die Implementierungsphase umfasst also weit mehr als die Einführung neuer kryptografischer Verfahren. Die Unternehmen werden auch bei der Integration der entwickelten Roadmap in bestehende Transformations- und Modernisierungsvorhaben begleitet – unter Berücksichtigung aller organisatorischen und regulatorischen Anforderungen.

Strategische Empfehlungen werden schrittweise in konkrete Maßnahmen überführt. Fortschritte lassen sich nachvollziehbar verfolgen und Risiken kontinuierlich überwachen. Die weitere Transformation kann gezielt gesteuert werden.

Phase 6 – Skalierung und branchenspezifische Umsetzung

Nach der Umsetzung erster Maßnahmen gilt es, Quantum Readiness schrittweise auf weitere Bereiche der Organisation auszuweiten und dauerhaft in bestehende Prozesse, Sicherheitsstrategien und Geschäftsabläufe zu integrieren. Dabei unterscheiden sich die Anforderungen je nach Branche erheblich. Geschäftsmodelle, regulatorische Vorgaben, Schutzbedarfe und technologische Abhängigkeiten erfordern eine individuelle Betrachtung.

Im Mittelpunkt stehen Fragen wie: Welche regulatorischen Anforderungen gelten für unsere Branche? Welche Geschäftsprozesse besitzen einen besonders hohen Schutzbedarf? Welche Daten müssen langfristig geschützt werden? Welche Abhängigkeiten bestehen zu Partnern, Lieferanten oder kritischen Infrastrukturen? Und wie lassen sich die eingeführten Maßnahmen auf weitere Bereiche der Organisation übertragen?

Darüber hinaus müssen die unterschiedlichen Lebenszyklen von Technologien und Systemen berücksichtigt werden. Während moderne Plattformen kontinuierlich aktualisiert werden können, bleiben industrielle Anlagen, medizinische Systeme oder kritische Infrastrukturen häufig über viele Jahre oder sogar Jahrzehnte im Einsatz. Eine nachhaltige Quantum-Readiness-Strategie muss diese Unterschiede berücksichtigen und die Roadmap an die jeweiligen organisatorischen und branchenspezifischen Rahmenbedingungen anpassen.

In der sechsten Phase werden die entwickelten Maßnahmen dauerhaft in den organisatorischen, technischen und regulatorischen Kontext der Organisation eingebettet.

Mehrwerte des CGI Quantum Risk Assessments

Das CGI Quantum Risk Assessment liefert nicht nur technische Erkenntnisse. Es hilft Unternehmen, ihre Risiken besser zu verstehen, Maßnahmen gezielt zu planen und die weitere Transformation kontrolliert und wirtschaftlich sinnvoll zu steuern. Anstelle einer kurzfristigen Komplettmigration wird ein realistischer Transformationspfad erstellt, der sich an den spezifischen Anforderungen und Rahmenbedingungen der Organisation orientiert.

1

Kontrollierte Steuerung von Risiken

Schutzbedarfe, regulatorische Anforderungen und potenzielle Auswirkungen kryptografischer Veränderungen werden sichtbar. Die Risiken lassen sich strukturiert bewerten und in ihrem geschäftlichen Kontext einordnen.

2

Hohe Planungssicherheit

Die gewonnenen Erkenntnisse schaffen eine Informationsbasis für die weitere Transformation. Maßnahmen können frühzeitig geplant und schrittweise umgesetzt werden. So lassen sich die Veränderungen kontrolliert gestalten.

3

Gezielter Ressourceneinsatz

Handlungsfelder lassen sich kurz-, mittel- und langfristig priorisieren. Investitionen und Ressourcen werden dort eingesetzt, wo sie den meisten Nutzen bringen und die wichtigsten Risiken adressieren.

4

Fundierte Entscheidungen

Die Verantwortlichen verfügen über eine belastbare Informationsbasis. Dadurch lassen sich Investitionen und weitere Transformationsmaßnahmen auf einer nachvollziehbaren Grundlage priorisieren.

5

Anforderungsgerechte Transformation

Regulatorische Anforderungen, branchenspezifische Vorgaben und individuelle Rahmenbedingungen werden frühzeitig berücksichtigt. Komplexe Transformationsvorhaben können kontrolliert umgesetzt werden.

6

Gestärkte Resilienz und Zukunftsfähigkeit

Die schrittweise Umsetzung der Roadmap stärkt die Widerstandsfähigkeit der Organisation gegenüber technologischen und regulatorischen Veränderungen und unterstützt eine langfristig zukunftsfähige IT.





Unsere Handlungsempfehlungen für CIOs und CISOs

Die Vorbereitung auf das Quantenzeitalter beginnt nicht mit der technischen Migration, sondern mit den richtigen Entscheidungen. Für CIOs und CISOs stellt sich daher vor allem die Frage, welche Maßnahmen bereits heute sinnvoll sind und wie sich zukünftige Investitionen optimal planen lassen.

Den richtigen Einstieg wählen

Der erste Schritt besteht darin, die eigene Ausgangssituation zu verstehen. Viele Organisationen verfügen heute noch nicht über einen vollständigen Überblick darüber, welche kryptografischen Verfahren eingesetzt werden oder welche Systeme von Vertrauensketten abhängen. Doch erst auf dieser Grundlage lassen sich Risiken bewerten und Maßnahmen sinnvoll priorisieren.

Zukünftige Entwicklungen berücksichtigen

Besonders relevant sind Informationen mit langfristigem Schutzbedarf und Systeme mit langen Lebenszyklen oder eingeschränkter Updatefähigkeit. Diese Bereiche sollten bei der Konzeption besonders früh berücksichtigt werden. Dazu empfiehlt es sich, die regulatorischen Entwicklungen und technologischen Standards kontinuierlich zu beobachten. Unternehmen, die sich rechtzeitig mit neuen Anforderungen auseinandersetzen, können spätere Anpassungen deutlich besser planen.

Kryptografische Agilität fördern

Die Fähigkeit, kryptografische Verfahren flexibel austauschen oder anpassen zu können, wird zu einem wichtigen Architekturprinzip moderner IT-Landschaften.

Unternehmen, die bereits die Voraussetzungen für kryptografische Agilität schaffen, reduzieren spätere Migrationsaufwände und stärken ihre Anpassungsfähigkeit gegenüber späteren technologischen Veränderungen.

Schrittweise vorgehen

Quantum Readiness bedeutet nicht, heute sämtliche Systeme auf neue kryptografische Verfahren umzustellen. Entscheidend ist, frühzeitig mit der Vorbereitung zu beginnen und die Transformation kontrolliert und priorisiert zu gestalten.

Langfristig planen, gezielt umsetzen

Die Diskussion über Quantencomputing konzentriert sich häufig auf neue kryptografische Verfahren und den möglichen Zeitpunkt eines Q-Days. Für Unternehmen liegt die eigentliche Herausforderung jedoch nicht in der Technologie selbst, sondern in der damit verbundenen Transformation.

Diese beginnt nicht mit der Einführung neuer Technologien, sondern mit langfristiger Planung. Davon betroffen sind Sicherheitsarchitekturen, Geschäftsprozesse, Investitionsentscheidungen und der Umgang mit regulatorischen Anforderungen.



Schritt für Schritt in eine quantensichere Zukunft

Die erfolgreiche Vorbereitung auf das Quantenzeitalter beginnt damit, die Ausgangssituation realistisch einzuschätzen. Wer die Auswirkungen der neuen Technologie auf die eigene Organisation frühzeitig einordnet, kann Risiken gezielt adressieren und den Übergang zu einer quantensicheren IT vorausschauend planen.



Über CGI

Insights you can act on

Wir sind ein globales Dienstleistungsunternehmen für IT- und Geschäftsprozesse mit insgesamt 94.000 Mitarbeitenden. An 400 Standorten bieten wir für mehr als 20 Branchen ganzheitliche, skalierbare und nachhaltige Services, durch die unsere Kunden greifbare Ergebnisse erzielen; unser Portfolio umfasst IT- und Business-Beratung, Systemintegration, Managed IT, Business Process Services und Intellectual Property auf Topniveau. Ein Schwerpunkt unserer strategischen Beratung liegt in der Verbesserung der geschäftlichen Agilität und des Change Managements; unsere IP-basierten Lösungen dienen einer beschleunigten Innovation und nutzen dazu Verfahren wie KI.

Mehr Informationen erhalten Sie auf
www.cgi.com/de oder info.de@cgi.com

