IT-Zertifizierungen: Welche darf's denn sein?

Ob Nahrungsmittel, Gefrierschränke oder Autos: Zertifizierungen und Labels sollen uns bescheinigen, dass die Produkte ökologisch, sicher oder «fair» sind. Solche Attribute, insbesondere das der Sicherheit, sind auch für die IT relevant. Was heisst das nun für die Finanzbranche?

Der Autor
Kaspar Geiser, Geschäftsführer, Aspectra

Als oberste Instanz hat in der Schweiz die Eidgenössische Finanzmarktaufsicht Finma das Sagen. Die Finma erlässt Richtlinien, überprüft Institute und deren Prozesse und beurteilt Risiken des Finanzplatzes. Auch in Sachen IT erlässt die Finma Richtlinien, sogenannte Rundschreiben, die mehr oder weniger konkrete Vorgaben an die IT stellen. Ein Standard wie ISAE 3000 stellt sicher, dass diese Richtlinien eingehalten werden.

Doch die Finanzindustrie ist global und sieht sich in jedem Land mit spezifischen Regeln konfrontiert. Bis auf die Berichtsform haben diese Vorgaben nicht immer viele Gemeinsamkeiten. Einzig im Bereich von Kreditkartengeschäften gibt es einen globalen IT-Standard, an den man sich halten kann. Dieser Standard wiederum wird nicht von einer Regierungsorganisation erstellt, sondern im Wesentlichen von den Kreditkartenfirmen Visa, Mastercard und American Express. Neben den eher finanzplatzspezifischen Regulatorien gibt es zudem die ebenfalls global etablierte Zertifizierung nach ISO 27001, die ein IT-Sicherheitsmanagement-System bescheinigt.

Jedes Audit, jede Zertifizierung hat ihre Eigenheiten. Da sich Technologie sehr schnell verändert, sind technisch konkrete Vorgaben mit Vorsicht zu geniessen. Einzig PCI DSS macht hier konkrete Vorgaben, wie etwa ein Netzwerk segmentiert sein muss. Trotzdem sollten Zertifizierungen nicht nur das Risikomanagement eines Dienstleisters unter die Lupe nehmen, sondern die technisch bestmögliche Umsetzung erzwingen.

Doch wozu all die Berichte und Zertifizierungen? Kaum ein Finanzinstitut betreibt heute die komplette IT selbstständig, sondern lagert immer mehr Teile davon aus. Die internen und externen Prüfer haben somit kaum mehr die Möglichkeit, alle Systeme und Prozesse, die das Institut nutzt, zu überprüfen. Daher verlangen die Prüfer von den externen Dienstleistern Zertifizierungen. Im besten Fall genügt ein Zertifikat, nicht selten aber werden komplette Prüfberichte verlangt. Für Outsourcing-Anbieter wiederum bedeutet dies einen erheblichen Aufwand.

IT-Dienstleister

Für die IT-Dienstleister bedeutet das: Wer Schweizer Finanzinstituten Leistungen anbietet, muss sich auditieren und zertifizieren lassen. Dies bringt eine ganze Reihe von Auflagen und Aufwänden mit sich. Sämtliche Prozesse und Verantwortlichkeiten müssen klar geregelt, dokumentiert und kontrolliert werden. Dies wiederum hat zur Folge, dass innerhalb einer Organisation – und sei sie noch so klein – die Rollen klar verteilt werden müssen, um so eine interne Governance beziehungsweise eine klare Unternehmensführung zu garantieren. Sind Prozesse, Aufgaben und interne Vorgaben dokumentiert, folgen als Nächstes die Kontrollen. Es gilt, diese klar zu formulieren. Sowohl die Vorgaben wie auch die Kontrollmechanismen müssen allen Mitarbeitern kommuniziert werden. Dies bringt als Erstes die Ausbildungskontrolle mit sich. All diese Kontrollen werden dann in Form von internen Audits erhoben, bevor die externen Auditoren ins Haus geholt

werden. Deren Besuch verbreitet nicht immer nur Freude. Die Auditoren haben die Pflicht, möglichst viele Unzulänglichkeiten aufzudecken. Zumindest hinterfragen und verifizieren sie die Kontrollmechanismen und verfassen anschliessend einen Bericht. Aus Sicht der Dienstleister sollten diese Berichte möglichst wenige Findings aufweisen. Der Auditor wiederum möchte natürlich nur das bescheinigen, was er auch verantworten kann. Nicht zu unterschätzen ist der Aufwand eines Audits oder einer Zertifizierung. Für Organisationen mit bis zu 50 Mitarbeitern sind mit Gesamtkosten von zirka 50 000 Franken pro Zertifizierung und Jahr zu rechnen. Um eine möglichste hohe Akzeptanz der Testate zu erlangen, empfiehlt es sich, als Prüfer einen der «Big Four» (Deloitte, EY, PwC und KPMG, Anm. d. Red.) ins Boot zu holen.

Finanzinstitute

Wer IT-Dienstleistungen auslagert, tut gut daran, die gewünschten Berichte bereits bei einer Ausschreibung zu verlangen. Bei deren Sichtung ist als Erstes der Scope (Geltungsbereich) zu prüfen. Der Scope definiert, was beim IT-Partner effektiv geprüft wird. Er sollte möglichst genau definiert sein und gleichzeitig alle vom Finanzinstitut bezogenen Dienstleistungen abdecken – auch alle potenziellen. Wichtig ist, dass man sich neben der Einsicht in die Berichte auch ein möglichst umfangreiches Auditrecht bei den Dienstleistern ausbedingt. Das bietet den internen wie externen Auditoren Einsicht in die kompletten Berichte des Dienstleisters oder sogar in Berichte von dessen Subakkordanten. Doch das Einfordern der Berichte allein genügt nicht. Sie müssen gelesen und hinterfragt werden. Oftmals wird diese Aufgabe ebenfalls ausgelagert, was dazu führt, dass sich Auditoren gegenseitig auditieren. Selbstredend nützt das dem eigenen Institut wenig.

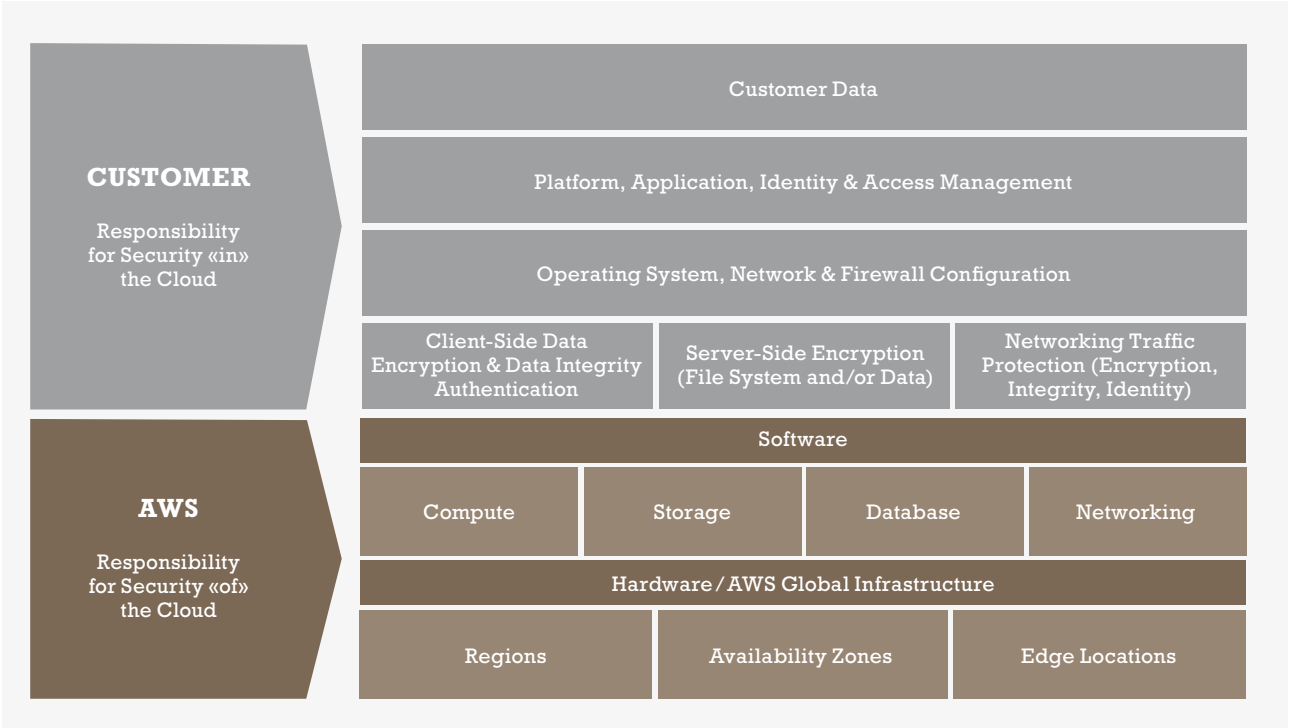
Und was ist mit der Cloud?

Das Berichtswesen ist mit der Auslagerung von Dienstleistungen an die Public-Cloud-Provider Amazon, Microsoft und Google nicht einfacher geworden. Diese globalen Anbieter decken heute bis zu 25 Standards ab. Doch der Scope und die damit verbundenen Kontrollen sind nur schwer zu verstehen beziehungsweise einzusehen. Microsoft stellt für zirka 50 Azure-Services eine Zertifizierungstabelle zur Verfügung, wobei aber nicht jeder Dienst die dieselben Standards erfüllt. Amazon wiederum bedient sich des «Shared Responsibility»-Modells, bei dem etwa das Firewall-Management in der Verantwortung des Dienstleistungsbezügers, also des Finanzdienstleisters ist.

> Im besten Fall genügt ein Zertifikat, oft aber werden komplette Prüfberichte verlangt.

Fazit

Finma, ISO 27001 und PCI DSS sind etablierte Standards und sowohl für Finanz- wie IT-Dienstleister zwingend. Doch eine Zertifizierung ist an sich noch kein Garant für maximale Sicherheit. Es ist allen Parteien zu empfehlen, bei der Auslegung des Geltungsbereichs und dessen Kontrollen zusammenzuarbeiten. Finanzinstitute müssen sich bewusst sein, dass eine Auslagerung von Dienstleistungen zu Public-Cloud-Anbietern ein hoher Aufwand verursacht: Ein Auditrecht kann kaum eingefordert werden und die effektiv zertifizierten Dienste müssen identifiziert werden.



Shared Responsibilty Model von AWS. Quelle: AWS