Risk	Test measure (section number/s)
Buildings insufficiently protected against break-in	5.1.3, 5.3.2
Authentication is insufficient: – Other customers (possibly competitors) gain access. – Unauthorized people gain access. – Authorized people cannot gain access. – Customer gains access to other customers' data.	5.1.3, 5.3.5
Authorization is insufficient: – Too few roles and functions can be defined on the customer side. – Too few functions are assigned different access rights. – Administrators on the supplier's side are not sufficiently restricted from accessing client data.	5.1.3, 5.3.6, 5.6.13, 5.9.2
There are too many people that can access everything (on the supplier side).	5.1.3, 5.2.9
Data is accessible through insufficient encryption: – By customer – On network – By supplier	5.1.3, 5.3.4
Service is insufficiently robust against attacks by hackers.	5.3.7, 5.3.10
Data is lost: – Storage device error – Errors in encryption – Loss of encryption key – Scaling (including elasticity) – Procedural errors – Software errors	5.5 5.3.4 5.3.4 5.2.4 5.4.6, 5.4.7 5.6
No access to data because of a business incident on the supplier side.	5.1.3, 5.5.5
Unauthorized people have access to data because of unsafe user behavior.	5.3.3
(Un)authorized access is not traceable.	5.1.3, 5.3.8
Security is not up to date: – On supplier side – On connected systems (customer) – On user devices (customer)	5.4.7, 5.9
It is unknown if user's own devices are safe.	5.3.3
Data is unintentionally not (fully) deleted.	5.6.13, 5.7.6
Disruption of the (virtual) environment by others occurs.	5.9
Third parties obtain access due to summons or investigation (jurisdiction, for example, the US Patriot Act): – Company data – Logging data	5.8

Terug naar Testing cloud services | Terug naar From risk to test