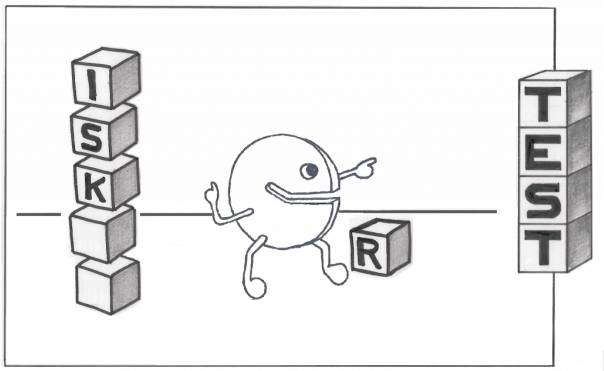
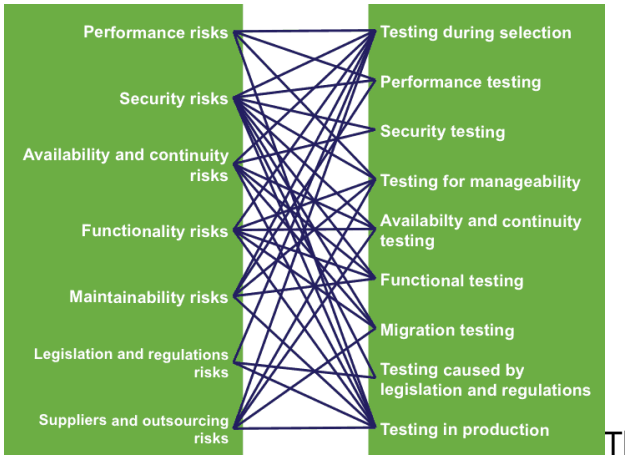


From the essential characteristics of cloud computing, a number of risks can be immediately determined. For example, broad network access means that most services are offered over the Internet, which introduces security risks. A further example is that resource pooling means that devices are shared with other customers, so response times of the service are affected by these other customers. This introduces a performance risk. The chosen implementation model also affects the risks, especially the severity of the risks. The security risk in the private cloud is less than in the public cloud where other customers have access to the same service. To determine which test measures are needed, all risks need to be mapped. For testing of services, this is no different from traditional test processes. By conducting a product risk analysis on the service, the areas that are important enough to test, and how stringent testing needs to be can be determined. This chapter contains a collection of cloud-related risks. We indicate which test measures can be taken to cover every risk. Risks and measures are based on practice and are meant as a source of inspiration; they are not exhaustive, but do provide guidance. This is the basis of *Testing Cloud Services* and, as such, the starting point of the test approach.



The following risk groups are identified:

- Performance risks
- Security risks
- Availability and continuity risks
- Functionality risks
- Maintainability risks
- Legislation and regulations risks

- Suppliers and outsourcing risks

The relationships between risks and test measures are not one to one but vary. For one risk, more than one measure can be deployed, or one measure can cover different risks (see figure).

Terug naar Testing cloud services