Nr.	Risks	Remarks	Analysis	Chance	Impact	Risk	Risk mitigation adjustments	Residual risk
	Organizational risks							
1	Lock-in	Risk of not being able to migrate easily from one provider to another						
2	Loss of Governance	Control and influence on the cloud providers, and conflicts between customer hardening procedures and the cloud environment.						
3	Compliance challenges (i.e. right to examine, exit clause, privacy acy etc.)	The risk of Cloud Providers which cannot provide evidence of compliancy to all relevant requirements, policies, laws etc.						
4	Loss of business reputation due to co-tenant activities	Risk of malicious activities carried out by one tenant affecting the reputation of another tenant.						
5	Cloud service termination or failure	Ths risk of providers going out of business. The risk of unclear data ownership.						
6	Cloud provider acquisition	Acquisition of the cloud provider could increase the likelihood of a strategic shift and may put non-binding agreements at risk.						
7	Supply chain failure	A cloud provider can outsource certain specialized tasks of its ‘production’ chain to third parties. The risk of non-compliancy of those subcontractors.						
8	Changing regulations	The risk of changes in laws and regulations could impact the requirements for both the financial institution and the cloud provider. Changes in regulations could aslo impact the risks for the Otso.						
	Insufficient skills and knowledge to identify risks related to Outsourcing / Cloud computing	If the financial institution has insufficient knowledge to identify the risks involved or to assess the operational effectiveness of the controls at the Cloud SP outsourcing is not allowed. Monitoring outsourcing requires specific skills and knowlegde.						
	Technical risks							
10	Resource exhaustion; under or over provisioning	There is a level of calculated risk in allocating all the resources of a cloud service, because resources are allocated according to statistical projections.						

Nr.	Risks	Remarks	Analysis	Chance	Impact	Risk	Risk mitigation adjustments	Residual risk
11	Isolation failure	This class of risks includes the failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure.						
12	Cloud provider malicious insider – abuse of high privilege roles	The malicious activities of an insider could potentially have an impact on: the confidentiality, integrity and availability of all kind of data, IP, all kind of services and therefore indirectly on the organization's reputation, customer trust and the experiences of employees.						
13	Management interface compromise	The customer management interfaces of public cloud providers are Internet accessible and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk especially when combined with remote access and web browser vulnerabilities.						
14	Intercepting data in transit	Sniffing, spoofing, man-in–the-middle attacks, side channel and replay attacks should be con-sidered as possible threat sources.						
15	Data leakage on up/download, intra-cloud	Data leakage from inside or outside the cloud provider is a major reputational risk for the financial institution. The contract must contain a section in which the financial institution is informed by the cloud provider in case of any relevant data leakage.						
16	Insecure or ineffective deletion of data	The risk of data being available beyond the lifetime specified in the security policy. (i.e. not wiped/deleted securely enough).						
17	DDOS	Distributed denial of service attacks could lead to: unavailability, identity theft, integrity failures etc. Contract should contain a section in which the financial institution is informed in case of a DDOS						
18	EDOS	as 17, but with the effect of Cloud customer going bankrupt or stolen from.						

Nr.	Risks	Remarks	Analysis	Chance	Impact	Risk	Risk mitigation adjustments	Residual risk
19	Loss of encryption keys	Loss or disclosure of secret keys (SSL, file encryption, customer private keys, etc) or passwords to malicious parties, the loss or corruption of those keys, or their unauthorised use for authentication and non-repudiation (digital signature).						
20	Undertaking of malicious probes or scans	Collect information in the context of a hacking attempt. A possible impact could be a loss of confidentiality, integrity and availability of service and data.						
21	Compromise service engine	Risk of compromise the highly specialized platform, the service engine located above the physical hardware resources and manages customer resources.						
22	Conflicts between customer hardening procedures and cloud environment	Risk of not being able to comply to the hardening procedures of the client, as well as differences between or unclear segregation of responsibilities.						
	Compliance risks							
23	Right to audit for supervisors	Risk of not being compliant to regulation; In the contract the right to examine/audit for DNB must be granted without any limitations to this right. The right also applies for sub- contractors in the chain. If there is an adjustment (new sub contractor) in the chain, the institution needs to be informed.						
24	Subpoena and e-Discovery	The risk of disclosure of centralized storage as well as shared physical hardware, to unwanted parties.						
25	Where is the data	It should be clear where data is stored. This applies also for backup data in a vault locaction and replicated data in a secundary or third datacenter. Also an financial institution needs to know whether the data is traveling between data centers or if the data stays in one datacenter.						
26	Risk from changes of jurisdiction	Change in location of data could lead to different jurisdiction, laws and regulations.						
27	Data protection risks	The risk of not being able to validate if data is handled in a lawfull way. Compliant to regulations like privacy laws, as well as encryption standards apply.						

Nr.	Risks	Remarks	Analysis	Chance	Impact	Risk	Risk mitigation adjustments	Residual risk
28	Specific local data privacy	The risk that other law and regulations apply at the location where the datacenter is situated compared to where the contract party is situated; http://www.cbpweb.nl/Pages/med_20120703_europese-opinie-cloudcomputing.aspx						
29	Risk of conflicting regulations	Laws and regulations due change on a regular basis. The risks exist the cloud provider cannot to comply to both regulations.						
30	Exit clausule in contract	The contract must contain an exit-clause. The exit clause should contain f.i. the way data is threated, time lines, etc.						
31	Licensing risks	Licensing conditions, such as per-seat agreements, and online licensing checks may become unworkable in a cloud environment.						
	Other not cloud specific risks							
32	Network breaks	Due to misconfiguration, system or OS vulnerabilities, lack of resource isolation or lack of, or a poor and untested, business continuity and disaster recovery plan.						
33	Network management	This could dramatically effect network uptime, experience, up-time and service delivery.						
34	Modifying network traffic	This could affect data integrity, loss and alteration of sensitive information. Eventually this will evolve as a reputational risk.						
35	Privilege escalation	This could lead to access to information or parts of the system normally not accessible to these users.						
36	Social engineering attacks	Due to lack of security awareness, user provisioning vulnerabilities, lack of resource isolation, communication encryption vulnerabilities, inadequate physical security procedures.						
37	Loss or compromise of operational logs	Due to lack of policy or poor procedures for logs collection and retention, vulnerabilities, lack of forensic readiness, system or OS vulnerabilities.						
38	Loss or compromise of security logs	Due to lack of policy or poor procedures for logs collection and retention, vulnerabili-ties, user provisioning vulnerabilities, user de-provisioning vulnerabilities, lack of forensic readiness, system or OS vulnerabilities.						

Nr.	Risks	Remarks	Analysis	Chance	Impact	Risk	Risk mitigation adjustments	Residual risk
39	Backups lost, stolen	Due to inadequate physical security procedures, vulnerabilities, user provisioning vul-nerabilities, user de-provisioning vulnerabilities.						
40	Unauthorized access to premises	Due to inadequate physical security procedures. Since cloud providers concentrate resources in large data centres, and although the physical perimeter controls are likely to be stronger, the impact of a breach of those controls is higher.						
41	Theft of computer equipment	Due to inadequate physical security procedures.						
42	Natural disasters	Generally speaking, this risk from natural disasters is lower compared to traditional infrastructures because cloud providers usually offer multiple redundant sites and network paths by default.						
43	Conflict of interest	Large cloud providers could use their resources as well as all the data stored on centralized storage, for other purposes.						
44	Bandwidth limitations	The number of intercontinental data lines is limited. A break in one or more of these lines could impact the availability and the performance.						