		Score BEFORE mitigation				Score AFTER mitigation			
Item	Risk description	Probability	Impact	Rating	Mitigation	Probability	Impact	Rating	Comments
1	A relying party doesn't understand the relationship between the OU and the certificate	3	2	5	The OU may only be included when the certificate includes an validated organization and the existence of and affiliation of the organizational unit with the subscriber is verified. Self-reported values shall be preceded or followed by a whitespace and the word "department", "division", "unit" or the equivalent in a language other than English.	1	1	2	
2	A self-reported value is used to reference a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity and the CA has not identified the value as such. Example: O="ACME Company Inc.", OU="{trademark} division", …	3	3	6	See item 1; Affiliation must be verified and pre/suffix emphasizes this relationship further. According to the subscriber agreement the subscriber must provide accurate information and should be liable for any IP conflicts as result of included information.	2	2	4	
3	A commonly recognized organizational unit name where the existence of and affiliation with the Applicant is not verified; a certificate listing the "Procurement" department in the OU field is obtained by the "Information Technology" department.	2	1	3	When pre-approving values the risk of the department name can be taken into consideration, e.g. a CA might not want to allow aything related to a financial department to be on this list.	1	1	2	
4	A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable can easily be modified or contain a freefrom data field.	3	3	6		3	3	6	Should we remove this option? This option could make sense for governmental divisions.
5	Abbreviated values can be misinterpreted.	3	2	5	The value SHALL not be abbreviated unless this would exceed the maximum length of the `subject:organizationalUnitName` field, in which case it SHALL only use locally accepted abbreviation. The pre/suffix emphasizes this relationship with the organization and should reduce the impact.	1	1	2	
6	When using a connection to the applicants directory system (e.g. Adctive Directory) any unit can be created.	2	1	3	See item 1 and 2; Affiliation is verified by establishing the connection and because these values are self-reported a pre/suffix emphasizes the relationship further is still required.	1	1	2	
7	An Organizational Chart can be created or modified by anyone with the only purpose to pass the validation.	2	1	3	According to the subscriber agreement the subscriber (listed as organization in the certificate) must provide accurate information and should be liable for any IP conflicts as result of included information.	1	1	2	
8	A sequence refers to a specific natural person or Legal Entity	2	2	4	By using a minimal length of 5 numbers in the sequence this should become unlikely.	1	2	3	
9	A Government, standard, or regulatory body had no clear definition of what values are allowed.	1	3	4	The CA MAY allow values or series as defined by a Government, standard, or regulatory body. Undefined values are not allow.	1	1	2	Should we make it more clear that there needs to be a specific definition of what is allowed/required?