ID	Risiko	Schadens-potenzial (h)	Eintrittswahr-scheinlichkeit (%)	Schaden gewichtet (h)	Gewichtung	Präventionsmassnahmen	Massnahme bei Eintritt
R01	Regelwerk zwischen Updates und Systemen zu komplex	40	25.00%	10	Sehr schwer	Klare Anforderungen definieren, Erwartungen des Auftraggebers früh abholen.	Schnell reagieren und Auftraggeber kommunizieren, dass der Aufwand zu gross wird. Einschränken der Anforderungen.
R02	Komplexes Permission-System für User	24	25.00%	6	Schwer	In Elaboration-Phase auf Rechtesystem einigen, so dass Machbarkeit gewährleistet ist.	Wenn möglich: Anforderungen einschränken. Andernfalls Anforderung komplett weglassen.
R03	Ruby ist für Umsetzung des Agents resp. Anschluss an apt nicht geeignet	16	25.00%	4	Mittel	So früh wie möglich Eignung von Ruby für Agent überprüfen	Python benutzen, wo es bereits ähnliche Projekte gibt.
R04	apt-Schnittstelle ist nicht so umfangreich wie erwartet, z.B. lässt sich nicht erkennen, welche Updates einen Neustart erfordern	4	50.00%	2	Gering	Frühzeitiges Abklären des Umfangs der apt-Schnittstelle	a) Selbst erstellte Schnittstelle einsetzen b) Anpassung der Aufgabe, falls nicht anders lösbar
R05	Zertifikat-Handling ist komplexer als erwartet	8	10.00%	0.8	Sehr Gering	Machbarkeit früh abklären	Spezialisten (HSR: Steffen; nine.ch) anfragen
R06	Viele gleichzeitige Anfragen bereiten Probleme beim Control-Center (Last)	16	25.00%	4	Gering	Auslastung einplanen, mit erstem stabilem Prototypen Last-Tests fahren	Spezialisten (HSR: Steffen; nine.ch) anfragen
R07	Auftraggeber mit Umsetzung nicht zufrieden	24	25.00%	6	Schwer	Use-Cases, Scope und NFAs früh teilen und bestätigen lassen. Regelmässige Meetings mit Statusbesprechung und Planung der nächsten Wochen.	Meeting mit Betreuer und Auftraggeber einberufen.