

Umsetzung einer Schadensdatenbank bei der LGT Gruppe



LGT

Die LGT ist seit über 80 Jahren im Besitz der Fürstenfamilie von Liechtenstein und verfügt über große Erfahrung in der Verwaltung von Familienvermögen. Sowohl was die Unternehmens- als auch die Anlagestrategie anbelangt, verfolgt LGT eine langfristige Perspektive. Durch die Eigentumsverhältnisse verfügt LGT über eine klare und effiziente Organisationsstruktur. Diese ermöglicht es, schnelle und unabhängige Entscheidungen zu treffen.

Eckdaten*

- 22 Standorte weltweit
- 3544 Mitarbeitende
- CHF 215 Mrd. an verwaltetem Vermögen
- CHF 155.6 Mio. Konzerngewinn

* Stand per 30.06.2019

Die LGT hat als langjähriger Kunde von avedos risk2value für verschiedene GRC-Prozesse im Einsatz. Eine der Anwendungen, welche sich im Einsatz befinden, umfasst eine konzernweite Schadensdatenbank, in der Ereignisse aus operationellen Risiken (sog. „Operational Risk Events“) mit finanziellen und nicht-finanziellen Effekten erfasst werden. Die Idee, die dem Projekt zugrunde lag, war die Harmonisierung mit dem bereits vorhandenen Risikomanagement und dem Internen Kontrollsystem sowie das Zusammenführen von lokalen Insellösungen. Des Weiteren spielte die Perspektive, die Forderungen durch die Regulatorik mit größtmöglichem Nutzen für die Geschäftsabläufe umzusetzen, eine entscheidende Rolle.

Kerntreiber für die Schadensdatenbank (Operational Risk Events Database - ORED)

- Erfüllung von regulatorischen Anforderungen (periodische Meldung von Verlustinformationen aus operationellen Ereignissen, veränderte Eigenmittelanforderungen für operationelle Risiken, Anforderung an das Risikodatenreporting und die -aggregation)
- Konzernweit einheitliche und konsistente Lösung zur Sammlung von Daten zu Verlustereignissen

Anforderungen an ORED:

- Abbildung der regulatorischen sowie der LGT-internen Anforderungen an die Sammlung von Daten im Zusammenhang mit Verlustereignissen (Strukturen, Informationen, Aggregation, etc.)
- Einfache und zielorientierte Lösung zur Einmeldung/Erfassung von Verlustereignissen durch jeden Mitarbeiter des Konzerns zwecks Vermeidung von Ineffizienzen und Medienbrüchen.

Gute Vorarbeit legte die Basis für eine erfolgreiche Implementierung

- **Vorarbeit** - sorgfältige Vorbereitung der inhaltlichen/konzeptbezogenen Arbeit und Entwicklung eines klaren Zielbilds, bevor das Implementierungsprojekt gestartet wurde
- **Zeitraumen** - die sehr knappe Zeitleiste (finale regulatorische Vorgaben: März 2017, Go-live: Januar 2018) ist nur durch ausreichend Vorarbeit und ein eingespieltes Team leistbar
- **Power-User** - Einbindung der Power-User in die Sondierung des gesamten Rahmenwerkes und starkes Engagement im Testing als wesentliche Faktoren für Akzeptanz
- **Schulungen** - Training und Befähigung zum Konzept, Prozess und Tool; teilweise Vor-Ort-Betreuung
- **Awareness** - Verantwortungsübernahme der Mitarbeiter durch Einbindung der Power-User

Fazit

Auch wenn der primäre Treiber des Projektes die regulatorischen Anforderungen waren, so konnte doch ein zusätzlicher Nutzen für das Unternehmen geschaffen werden. Informationen zu vorgefallenen Ereignissen aus operationellen Risiken sind konzernweit zentral, einheitlich und zeitnah verfügbar. Dies bietet die Grundlage, die Informationen mit anderen Anwendungen sinnvoll verknüpfen zu können und so eine integrierte und konsistente Sicht auf operationelle Risiken zu gewährleisten. Der gewählte Ansatz hat aber durchaus auch Widerstände hervorgerufen. Die Änderungen führen zu einem kulturellen Wandel, der kontinuierlich begleitet werden muss.

Mehrwert

Aus der bisherigen Nutzung von ORED konnten folgende Vorteile gezogen werden:

- konzernweit eine zentrale Datenbank („single point-of-truth“) im Zusammenhang mit Informationen zu operativen Schadensfällen (mit oder ohne finanzielle Effekte)
- Informationen zu Vorfällen sind zeitnah verfügbar und in ihrer Ausprägung vergleichbar über identisches Vorgehen
- einfache Einbindung/Erweiterung mit thematisch verwandten Aufgabenstellungen (z.B. Einmeldung von potentiellen Verstößen gegen die DSGVO)
- Verknüpfung von historischen Verlustereignissen mit anderen Themengebieten (z.B. Risk Assessments im Rahmen des IKS) durch identische Strukturen und Taxonomien

Ausblick

- Fokus: Stärkung des Vertrauens in das System, begleitet von weiteren Change Management-Maßnahmen (z.B. Vereinfachung des Datenmodells)
- Entwicklung von (interaktiven) Reporting-Funktionalitäten
- Prüfung der Ausweitung auf weitere/verwandte Themengebiete

