

# **Governance, Risk & Compliance Management**

Vernetzen Sie mit USU Service Management Business Services, Risiko-Management, Continuity-Verfahren und IT-Prozesse

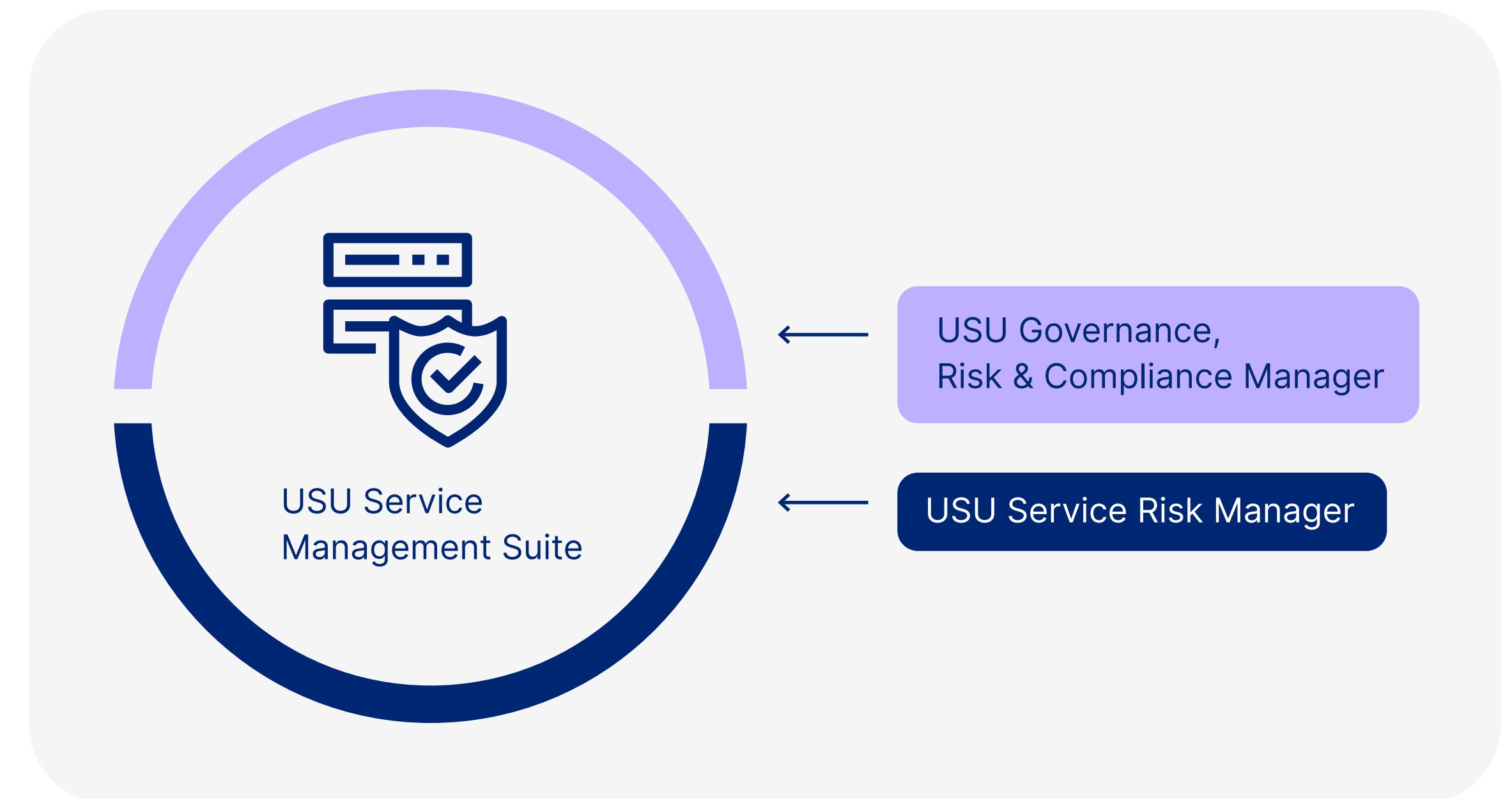


**Das aktive Managen von Risiken wird heute in vielen Unternehmen durch Compliance- und Governance-Vorgaben bzw. durch notwendige Zertifizierungen und zu erfüllenden Normen zwingend vorgeschrieben. Viele Risiken betreffen dabei den Betrieb geschäftskritischer IT-Services, da bei einem Ausfall dieser Services sehr schnell hohe Kosten und möglicherweise auch Umsatzverluste entstehen können.**

Rollen wie der Corporate Risk Manager oder Business Continuity Manager können nun mittels der entsprechenden Module mit ITSM-Unterstützung Risikomanagement im Unternehmen transparenter verwalten und relevante Informationen intelligenter miteinander verknüpfen. So ist auch der Weg zur ISO 27001, zu TISAX oder zu einem BCM mit deutlich weniger Aufwänden verbunden.

Der USU Governance, Risk & Compliance Manager (GRCM) und der USU Service Risk Managers (SERM) decken alle Aspekte von Governance, Risk und

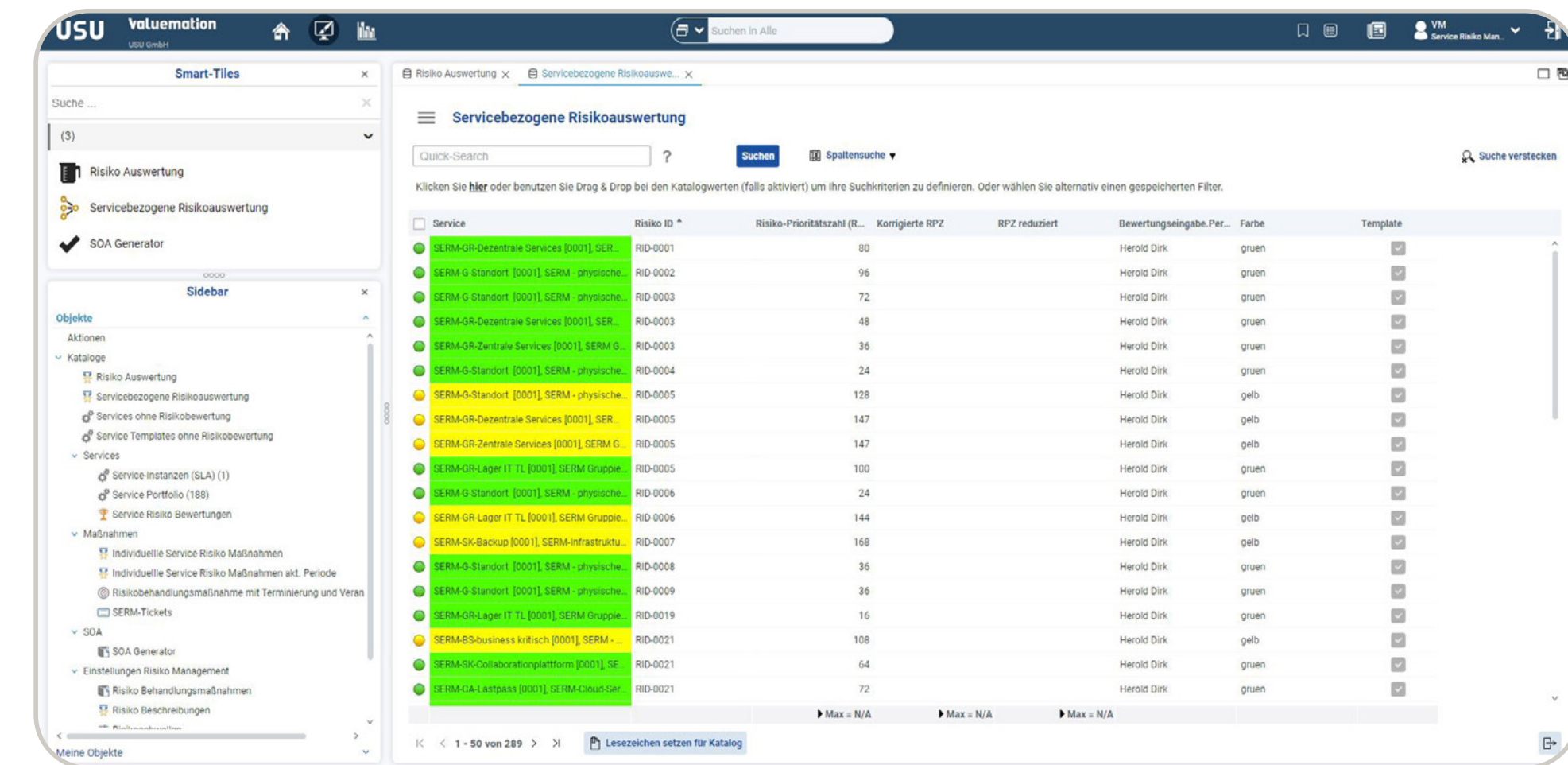
Compliance Prozessen ab. Es lassen sich Compliance Vorgaben erstellen, Service und Prozesse bewerten, Risiken erkennen und Maßnahmen definieren. Beide Module sind mit dem USU Service Management nutzbar:



# USU Service Risk Manager (SERM)

## Managen Sie aktiv die Risiken Ihres IT-Betriebs

Innerhalb der Produktsuite USU Service Management ermöglicht das Modul USU Service Risk Manager die toolgestützte Bearbeitung sämtlicher Aufgaben für das ganzheitliche Managen der Risiken für den Betrieb Ihrer Business Services.



The screenshot displays the USU Service Risk Manager (SERM) interface. On the left, a sidebar contains navigation options like 'Risiko Auswertung', 'Servicebezogene Risikoauswertung', and 'SOA Generator'. The main area shows a table titled 'Servicebezogene Risikoauswertung' with columns for Service, Risiko ID, Risiko-Prioritätszahl, Korrigierte RPZ, RPZ reduziert, Bewertungseingabe, Farbe, and Template. The table lists various services and their associated risks, with some rows highlighted in green and others in yellow. At the bottom, there are pagination controls showing '1 - 90 von 289' and a button to 'Lesezeichen setzen für Katalog'.

Service	Risiko ID	Risiko-Prioritätszahl	Korrigierte RPZ	RPZ reduziert	Bewertungseingabe	Farbe	Template
SERM-GR-Standard Services [0001] SERM	RID-0001	80			Herold Dirk	gruen	✓
SERM-G-Standard [0001] SERM - physisch	RID-0002	96			Herold Dirk	gruen	✓
SERM-G-Standard [0001] SERM - physisch	RID-0003	72			Herold Dirk	gruen	✓
SERM-GR-Standard Services [0001] SERM	RID-0003	48			Herold Dirk	gruen	✓
SERM-GR-Zentrale Services [0001] SERM G	RID-0003	36			Herold Dirk	gruen	✓
SERM-G-Standard [0001] SERM - physisch	RID-0004	24			Herold Dirk	gruen	✓
SERM-G-Standard [0001] SERM - physisch	RID-0005	128			Herold Dirk	gelb	✓
SERM-GR-Standard Services [0001] SERM	RID-0005	147			Herold Dirk	gelb	✓
SERM-GR-Zentrale Services [0001] SERM G	RID-0005	147			Herold Dirk	gelb	✓
SERM-GR-Lager IT TL [0001] SERM Gruppe	RID-0005	100			Herold Dirk	gruen	✓
SERM-G-Standard [0001] SERM - physisch	RID-0006	24			Herold Dirk	gruen	✓
SERM-GR-Lager IT TL [0001] SERM Gruppe	RID-0006	144			Herold Dirk	gelb	✓
SERM-SX-Backup [0001] SERM-Infrastruktur	RID-0007	168			Herold Dirk	gelb	✓
SERM-G-Standard [0001] SERM - physisch	RID-0008	36			Herold Dirk	gruen	✓
SERM-G-Standard [0001] SERM - physisch	RID-0009	36			Herold Dirk	gruen	✓
SERM-GR-Lager IT TL [0001] SERM Gruppe	RID-0019	16			Herold Dirk	gruen	✓
SERM-GR-Business kritisch [0001] SERM	RID-0021	108			Herold Dirk	gelb	✓
SERM-GR-Collaborationssysteme [0001] SERM	RID-0021	64			Herold Dirk	gruen	✓
SERM-GR-Lager IT TL [0001] SERM Gruppe	RID-0021	72			Herold Dirk	gruen	✓

Auswertung der Risiken

## Nutzen

### Starten Sie mit dem Service Risk Manager

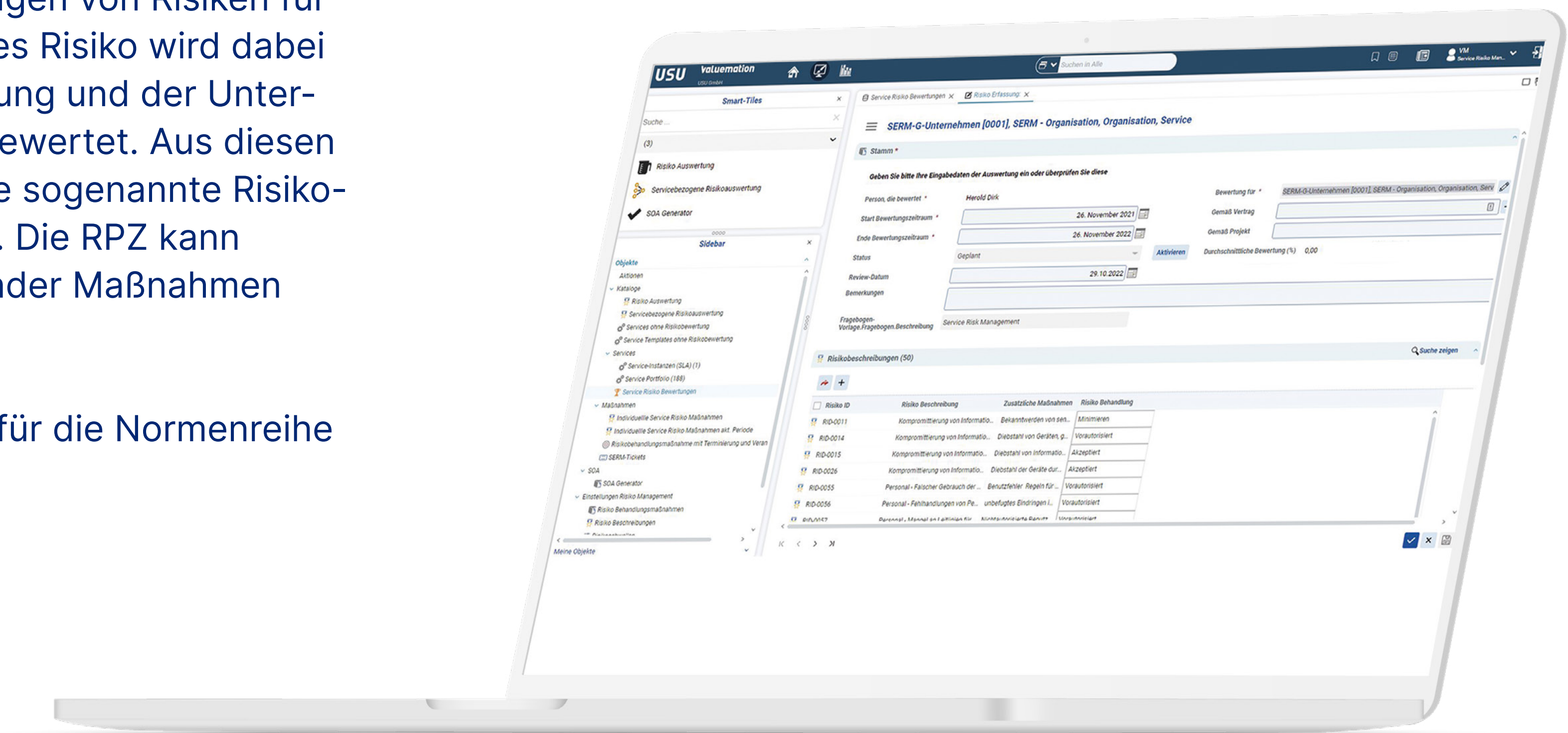
- Risiken werden auf Basis von Services erfasst, verbunden und ausgewertet (ohne Medienbrüche)
- Mehr Transparenz von Risiken bezogen auf Services, Servicekomponenten und Assets
- Risikomanagement by Design not by Control or Accident
- Nutzen der CMDB für die Erfassung und Bewertung von Risiken sowie Maßnahmenverwaltung.



# Einfaches Erfassen und Bewerten von Risiken

Der Service Risk Manager ermöglicht das Managen von Risiken für in der CMDB definierte Business Services. Jedes Risiko wird dabei mittels Eintrittswahrscheinlichkeit, der Auswirkung und der Unterbrechungswahrscheinlichkeit für den Service bewertet. Aus diesen Angaben ermittelt der Service Risk Manager die sogenannte Risiko-Prioritätszahl (RPZ), die das Risiko quantifiziert. Die RPZ kann schließlich durch die Definition risikominimierender Maßnahmen reduziert werden.

Im Auslieferungszustand ist ein Risiko-Katalog für die Normenreihe ISO 27001 bereits enthalten.

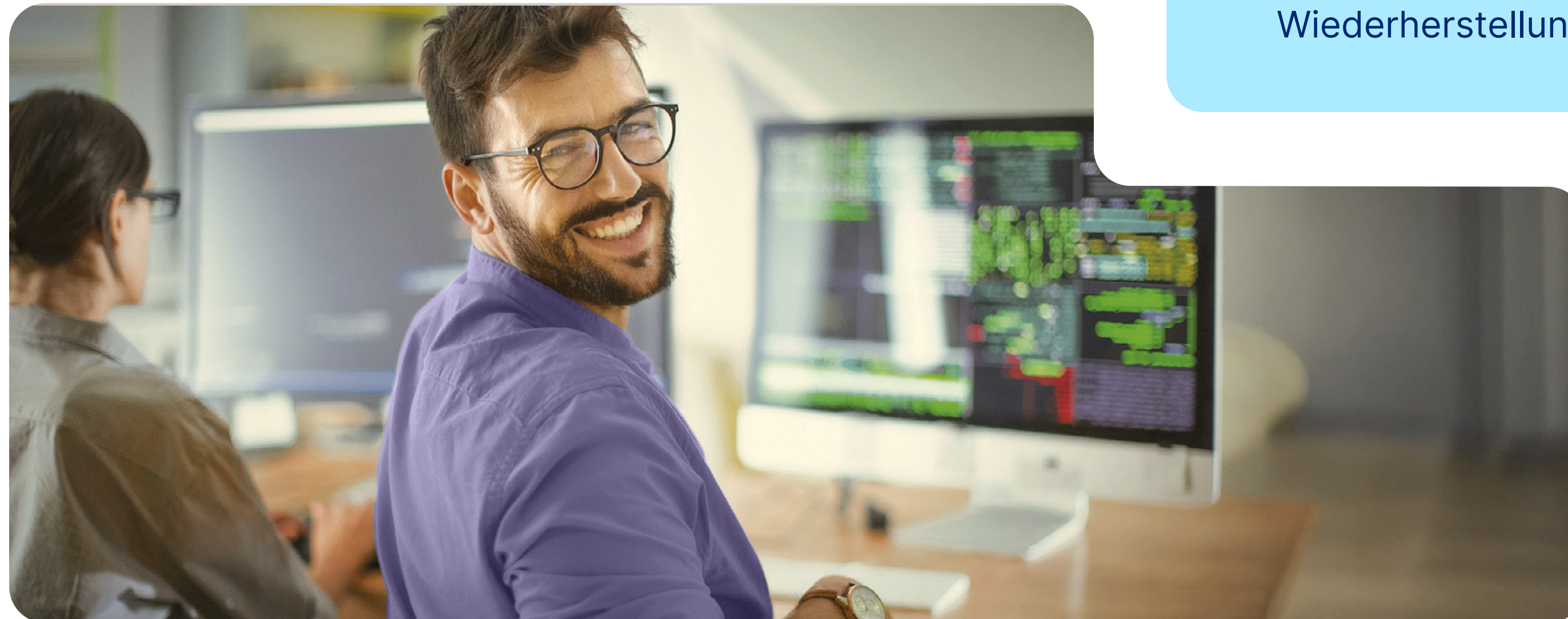


Erfassung von Risiken



# USU Governance, Risk & Compliance Manager (GRCM)

Mit dem USU Governance, Risk & Compliance Manager (GRCM) werden Prozesse & Services in Hinblick auf Risiko, Compliance („Regeltreue“) und Governance („Steuerung“) bewertbar. Für alle drei Bewertungsdimensionen (Governance, Risk & Compliance) kann so mit einem einheitlichen Vorgehensmodell gearbeitet werden.



## Nutzen

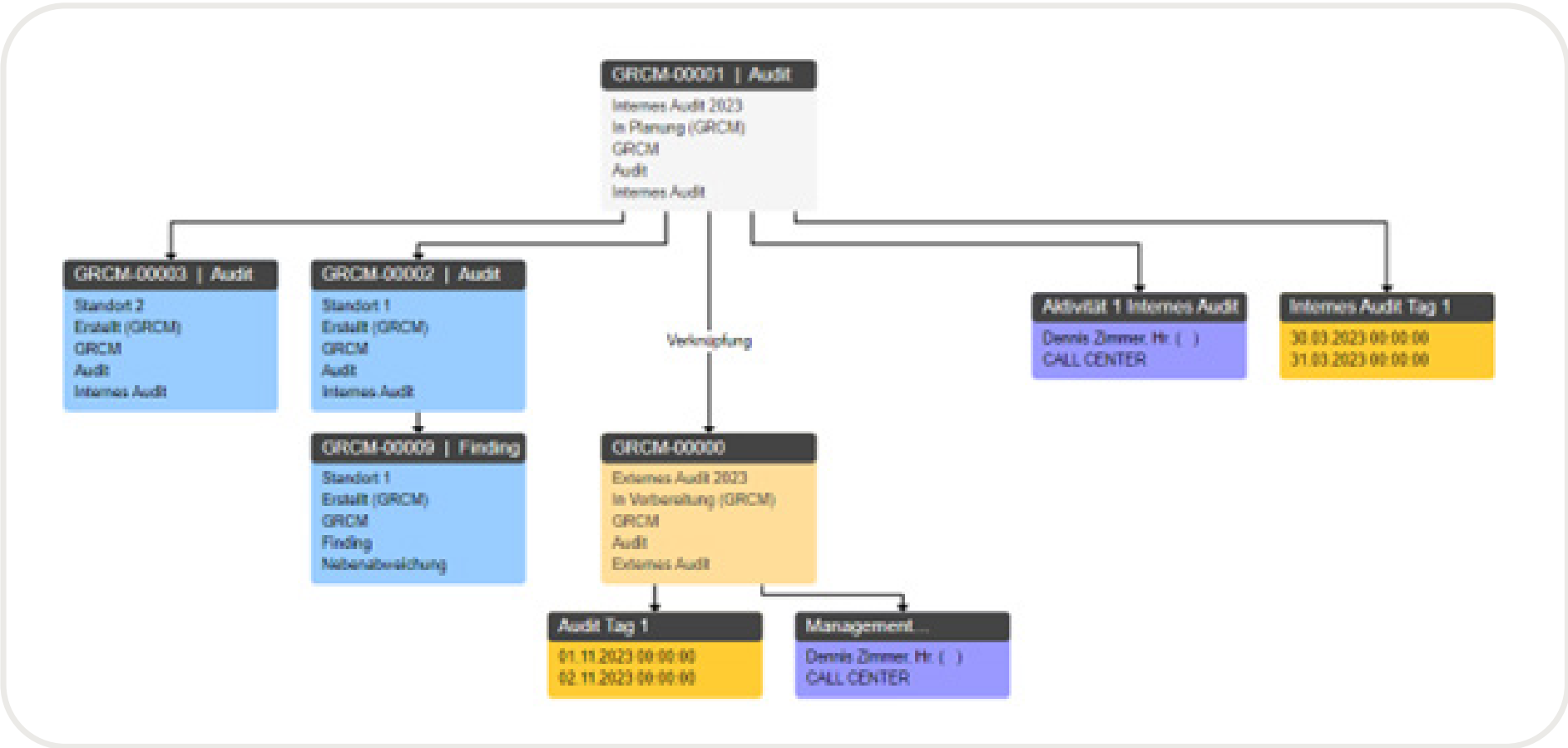
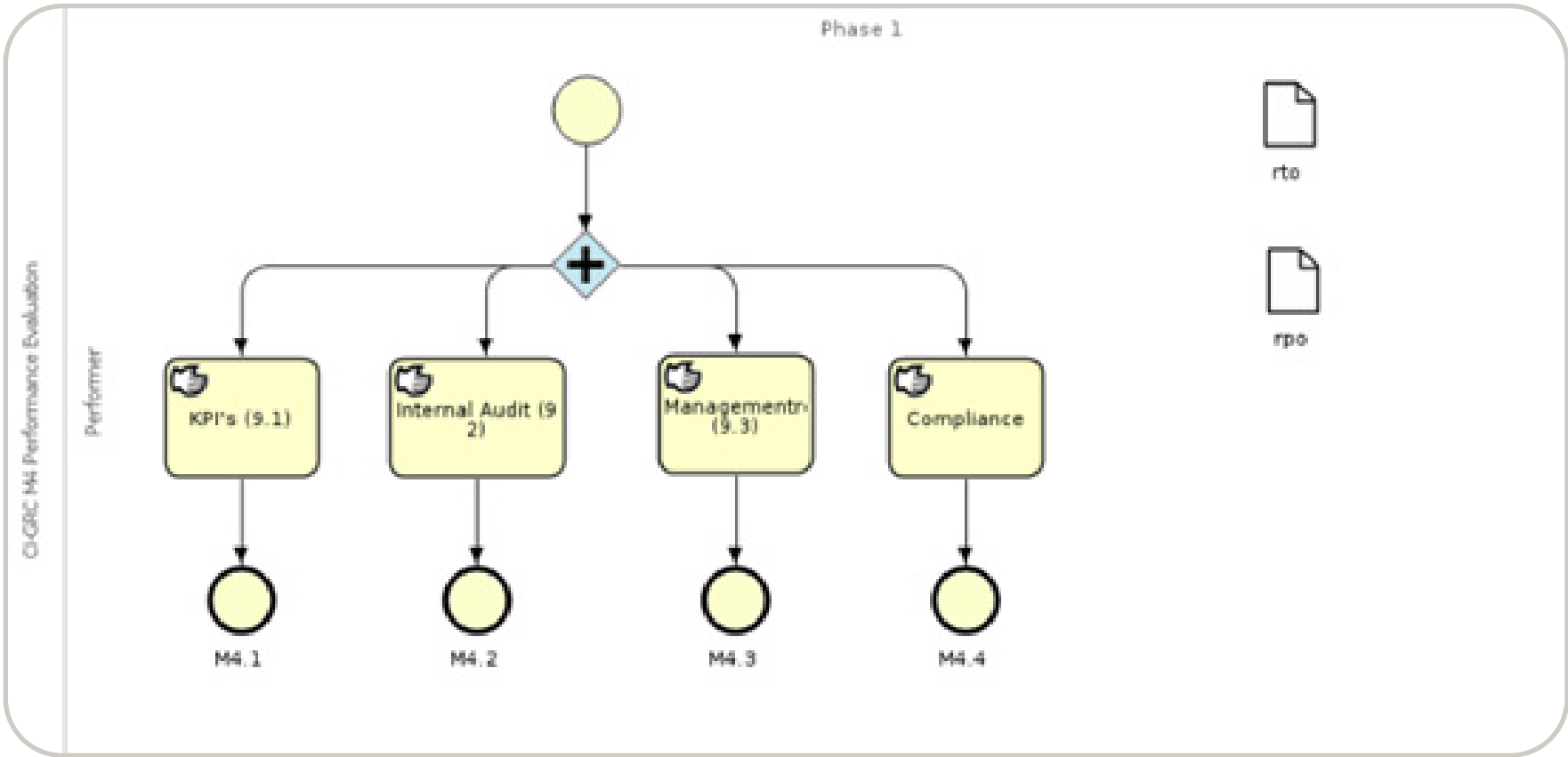
Stützen Sie mit dem USU GRC-Manager Ihr IT Service Management:

- Transparente Audit-Planung
- Business Impact Analysen
- Automatischer Import von Schwachstellen-Meldungen mittels eines automatischen GRCM-Prozesses
- Einfache Berechnung und Prüfung der erreichbaren Compliance-Werte aus der Service Hierarchie (z. B. Wiederherstellungszeit) und Vergleich mit den Vorgaben

# Governance-Funktionen im Überblick:

## Reagieren Sie direkt auf Geschäftsrisiken – auch in Prozessen

Mit dem USU Governance, Risk & Compliance Manager (GRCM) befähigen Sie Ihre IT, auch für Business-Prozesse Störungen zu melden, Changes zu erstellen oder Risiken zu analysieren. Dafür werden BPM-Prozesse in die Servicehierarchie integriert.



## Neue Funktion zur Audit-Planung

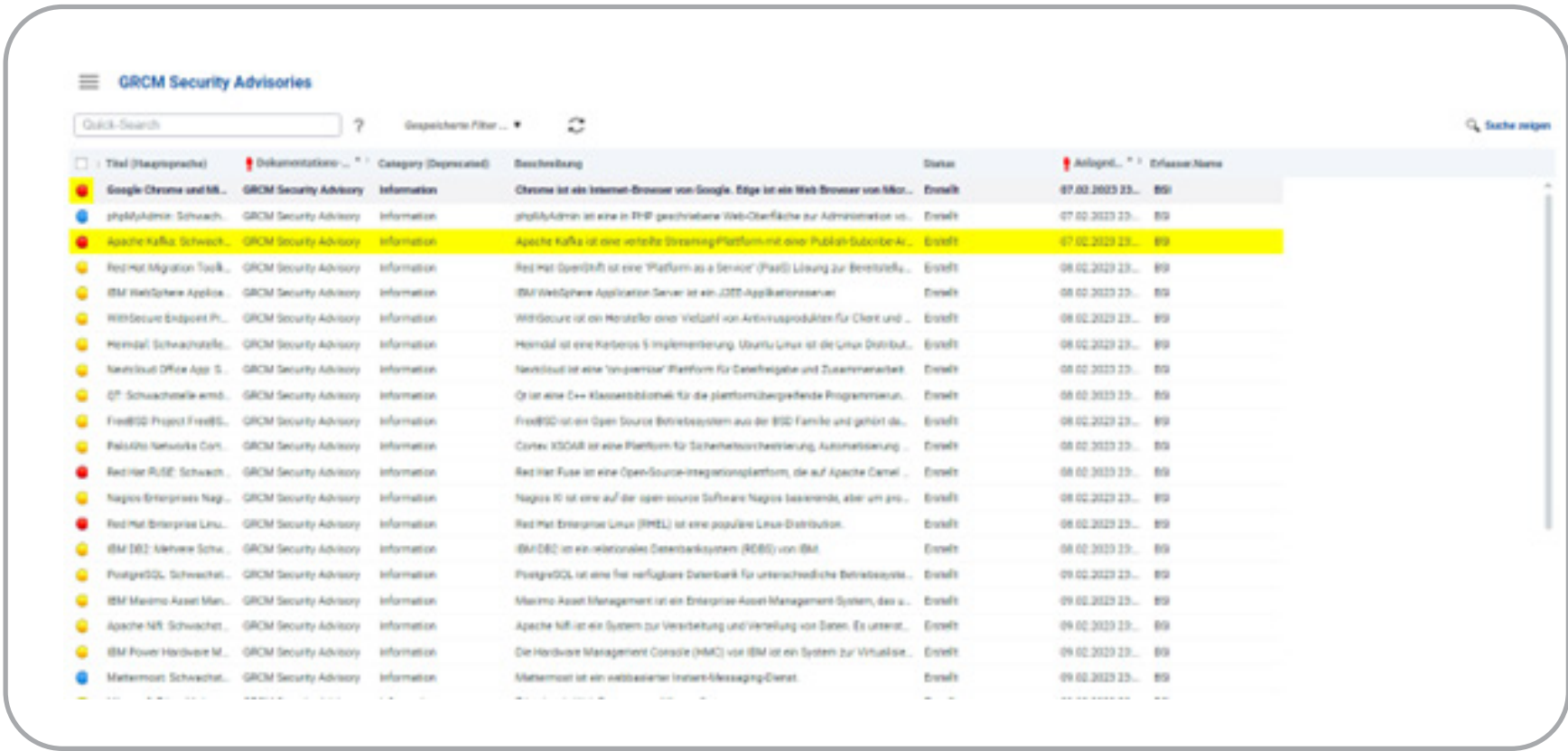
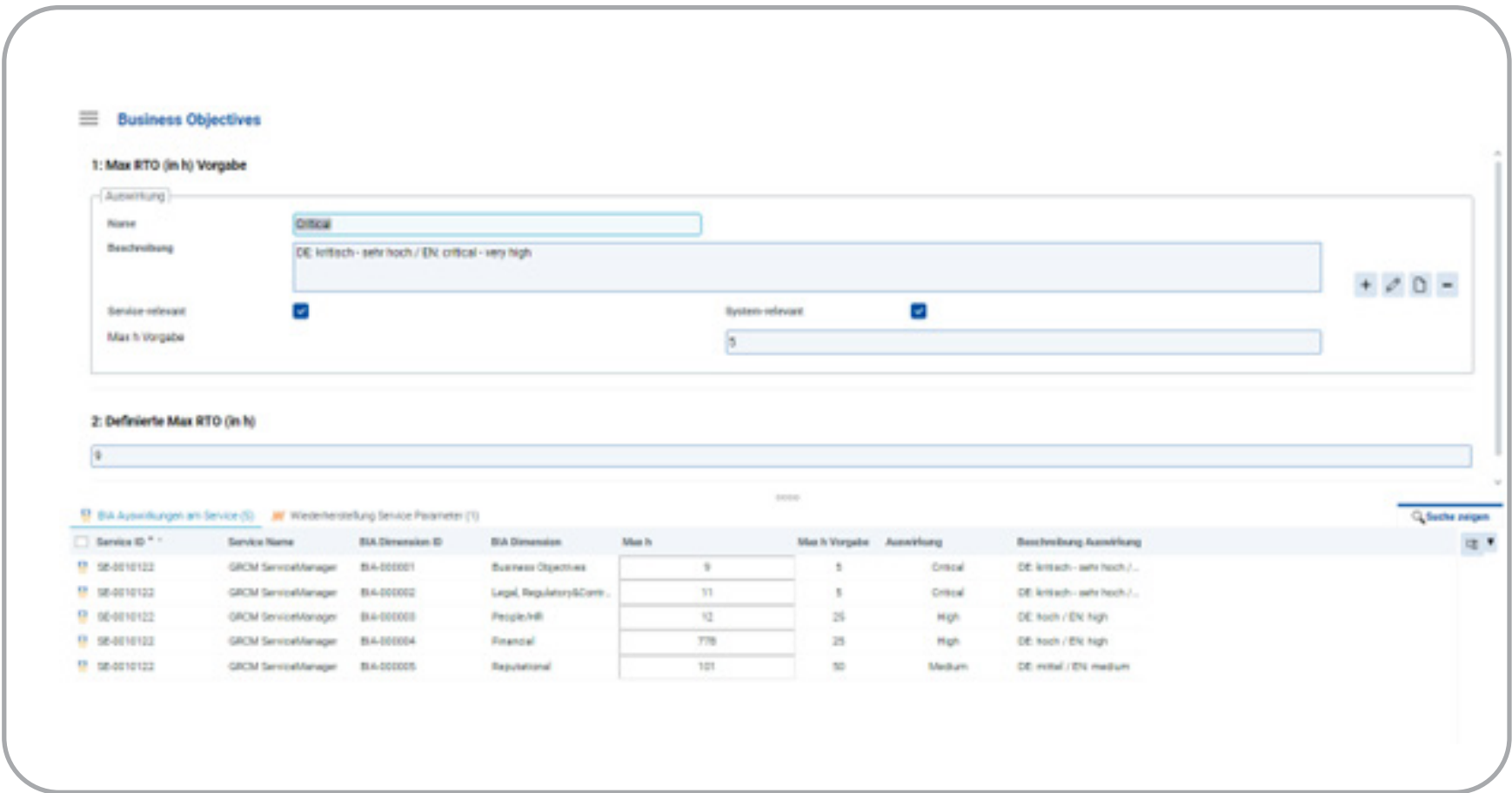
Starten Sie in eine transparente Auditplanung. Der neue Ticket-Typ „GRCM-Audit“ erlaubt es, die ganze Hierarchie eines internen Audits darzustellen und zu verwalten.



# Compliance-Funktionen im Überblick:

## Business Impact Analyse

Welche Auswirkungen hat ein Ausfall auf einen Service?  
Welche Downtime wäre kritisch? Mit der Business Impact Analyse können Sie Ihre Services mit Vorgabe-Informationen anreichern und diese Vorgaben dann auch gegen die Wiederherstellungseigenschaften prüfen.



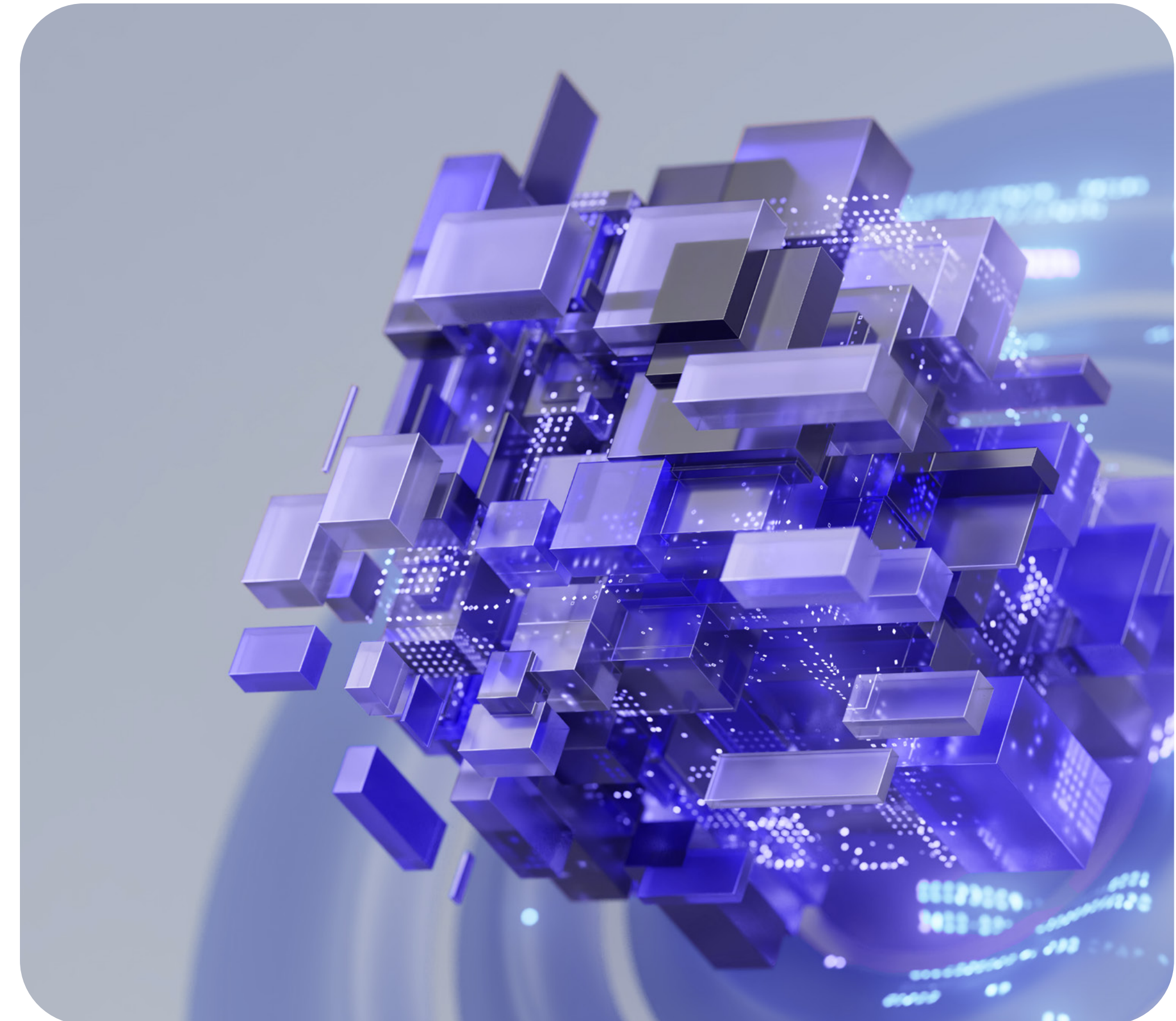
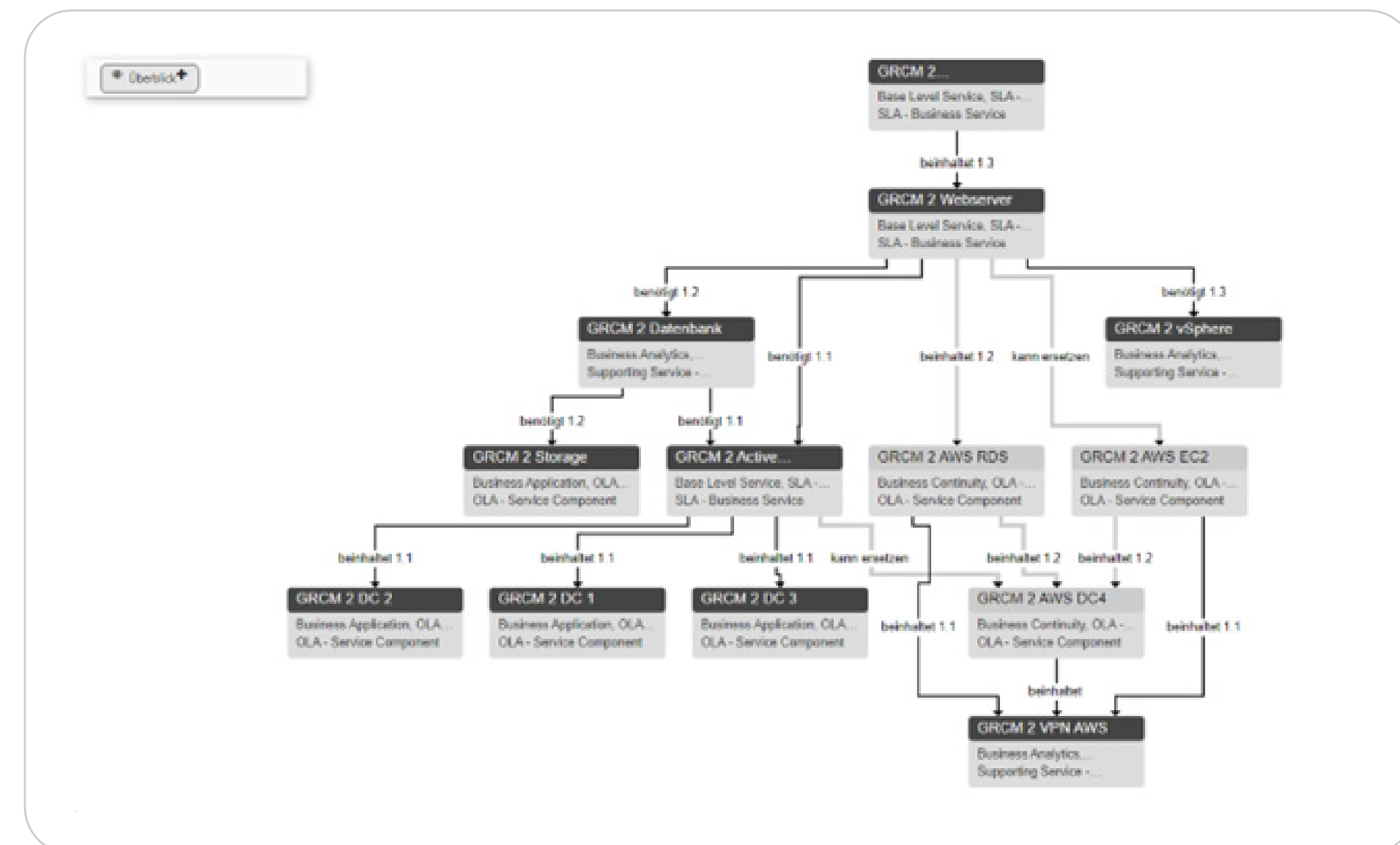
## Import neuester CERT-Meldungen

Integrieren Sie Meldungen aus digitalen Schwachstellen-Quellen vollautomatisch mittels eines GRCM-Prozesses. Die Meldungen können dann direkt mit einem Business Service als Service-Dokumentation verlinkt werden.



## Compliance und Kontinuität

Erstellen Sie für den eine Ausfallsituation eine duale Servicestruktur, die Sie zusammen mit der Hauptstruktur bewerten und visualisieren können. Diese alternative Servicestruktur können Sie nicht nur anlegen, sondern auch auf erzielbare Wiederherstellungsparameter (z.B. Wiederherstellungszeit) prüfen. So stellen Sie sicher, dass auch diese Servicestruktur den Vorgabe-Parametern der Business Impact Analyse (BIA) entspricht.







Entdecken Sie mehr  
auf unserer Website:

[www.usu.com](http://www.usu.com)  
[info@usu.com](mailto:info@usu.com)