Glenfis Customer Experience

Glenfis Cloud Talk

19.05.2021

Sven Ossenberg
Senior Consultant. Agile Coach.

Resilienz und Continuity Management in der Multi-Cloud

Was ist organisatorische Resilienz?

- Die **Fähigkeit** eines Unternehmens, auch in einem **komplexen** und **dynamischen** Umfeld den Wandel vorherzusehen, sich darauf **vorzubereiten**, zu **reagieren** und sich **anzupassen**, um das **Bestehen** des Unternehmens zu sichern

Was ist Continuity Management?

- **BCM: Absicherung** der zeitkritischen **Geschäftsprozesse** gegen **Ausfälle**
- **ITSCM:** Definiertes Ziel, im Falle eines Schadenseintritts den schnellstmöglichen **Wiederanlauf** der Prozesse und **Services** zu ermöglichen und Auswirkungen von Katastrophen **proaktiv** vorzubeugen
- IT-Service Continuity Management (ITSCM) erstellt eine **ITSCM-Strategie**, die in die allgemeine Business Continuity Management **(BCM)-Strategie integriert** wird

Was ist eine Multi-Cloud?

- In einer Multi-Cloud wird **mehr** als **ein Cloud-Service** von **mehr** als **einem Public oder Private Cloud -Anbieter** bereitgestellt

Eine «typische» Unternehmenssituation

Umfeld

- Einer zunehmenden **Nutzung von Cloud- und Sourcing-Anbietern** kann man sich nicht mehr verschliessen
- **Corona-Krise** zeigt Lücken in bestehenden **Multi-Provider** und **Cloud** Strategien auf
- **Best-in-Breed** Sourcing Ansätze haben bereits zu **mehreren Outsourcing Providern** geführt
- Die bereits bestehende Multi-Provider-Umgebung muss **aufwendig gesteuert und verwaltet** werden

Herausforderungen

- Die **Management Prozesse der Partner** sind nicht aufeinander abgestimmt
- Zwischen den Partnern entstehen **Reibungsverluste und Unstimmigkeiten**
- Verschiedene Tools lassen kein **End-to-End Monitoring** zu
- **Hochverfügbare** Infrastruktur **unabhängig** vom Arbeitsplatz als zentrale Anforderung

Bisherige Initiativen und Status

- **Service Management** ist in der internen IT etabliert Die Maturität sollte verbessert werden
- Ein **ITSM Tool** ist vorhanden. Die Lieferanten arbeiten mit eigenen Tools, eine Integration fehlt
- Der bestehende **BCM-, respektive ITSCM-Prozess** hält einer Audit Prüfung hinsichtlich **unvorhergesehener** Ereignisse nicht stand

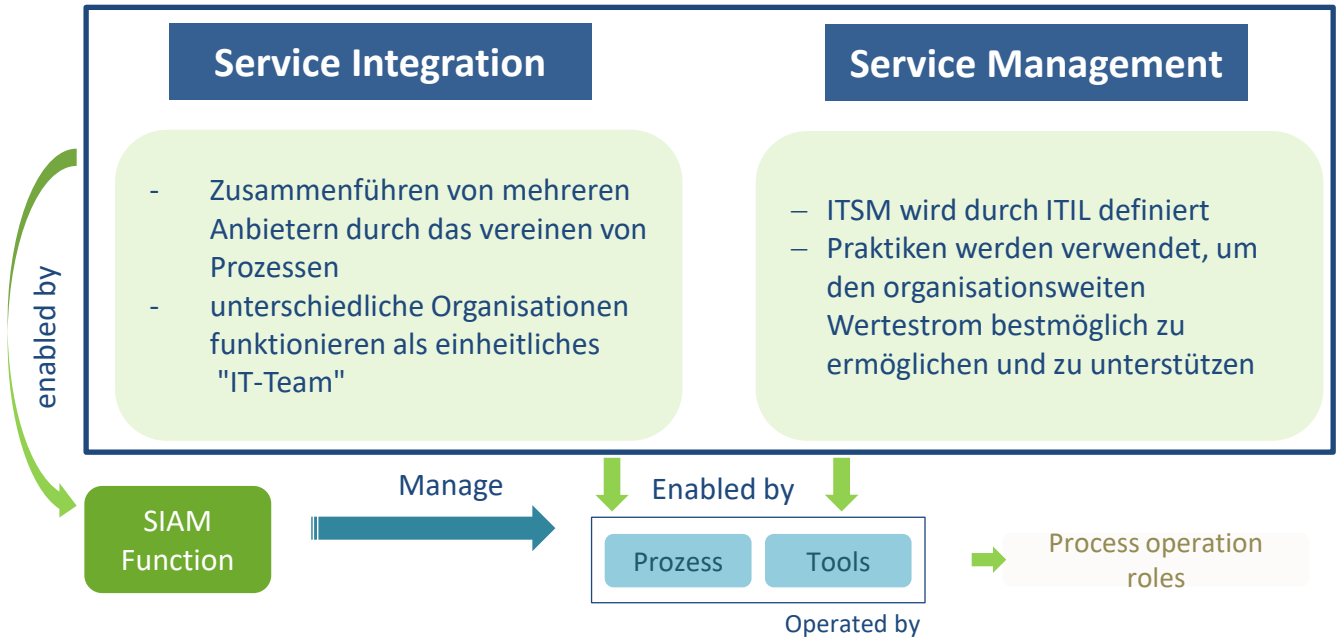
Lösungsansatz Glenfis

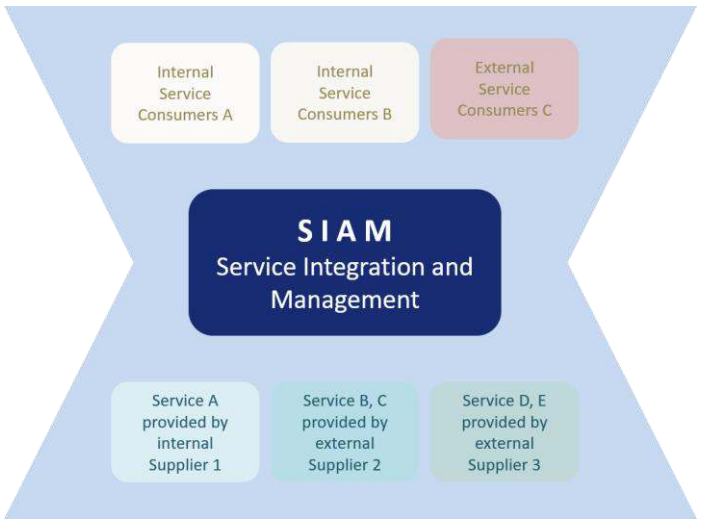
- **SIAM Ansatz** wird sicher stellen, dass ein gemeinsam funktionierendes Ökosystem entsteht
- Erhöhung der organisatorischen **Resilienz** durch Beurteilung **externen** Service-Partner und deren Integration
- Kontinuierliche **Prozessoptimierung** steigert die Resilienz
- Einführung **neuer** Rollenmodelle wie z.B. des **SRE**
- Regelmässige **Disaster-Recovery-Meetings zwischen Site Reliability Engineers** und **Risiko- und Compliance Team**
- **Testing** und Incident-Management-Übungen als **Erfolgsgaranten**

Was verstehen wir unter «SIAM»?

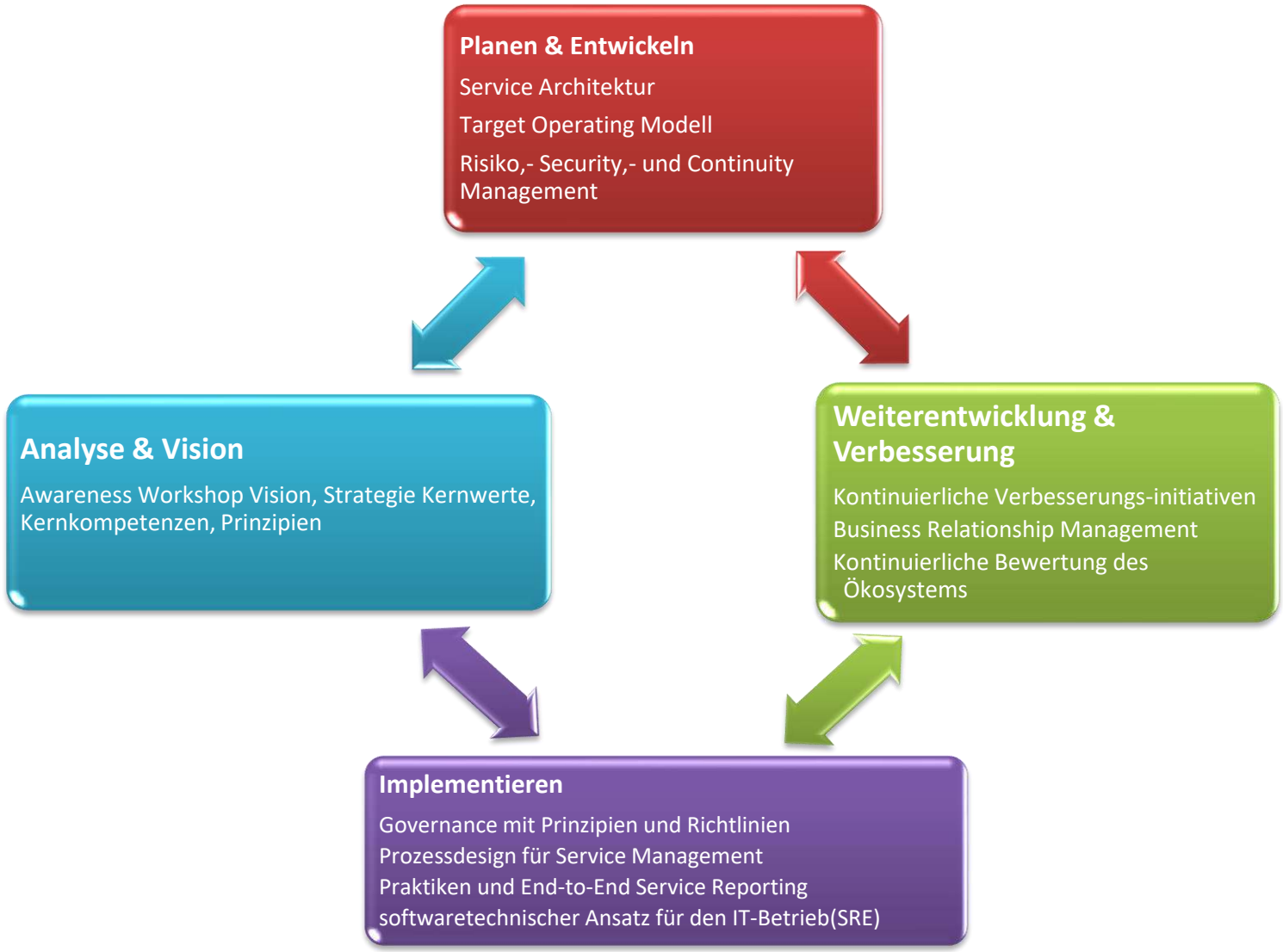
Service-Integration und -Management

- ermöglicht es einer Organisation, mehrere Service-Anbieter auf konsistente und effiziente Weise zu verwalten
- Stellt sicher, dass die Leistung über ein Portfolio von Waren und Dienstleistungen aus mehreren Quellen als nahtloser Service erbracht werden





Aufbau organisatorischer Resilienz



SIAM Sicht: Risiko,- Security,- und Continuity Management

Risk Management

- Kontinuierliche Identifizierung, Beurteilung und Kontrolle von Risiken innerhalb des Ökosystems
- Erfordert genaue Kenntnis des gesamten Risikoprofils des aller beteiligten Partner und Lieferanten
- Beachtung der Compliance Rahmenbedingungen in der Planungsphase
- Geographische und regulatorische Anforderungen frühzeitig bewerten

Information Security Management

- Klare Definition von Verantwortlichkeiten und Zuständigkeiten
- Verwendung von konsistenten Klassifizierungen und Definitionen für die Informationssicherheit
- Kommunizieren von Sicherheitsverletzungen und Schwachstellen im gesamten Ökosystem
- Aufnahme von Sicherheitsvorgaben in Verträge mit Service-Providern
- Steigende Sicherheitsrisiken, wenn Risiken auf niedrigerer Ebene über mehrere Parteien hinweg aggregiert werden

Business Continuity Management (BSI-200-4)

Zahlen, Daten, Fakten:

- BSI-Standard 200-4 löst den BSI-Standard 100-4 ab
- Änderung des Begriffs „Notfallmanagement“ in „Business Continuity Management (BCM)“
- Einführung eines neues Stufenmodells:
  - Reaktiv-BCMS
  - Aufbau-BCMS
  - Standard-BCMS
- Aufbau, Betrieb und die kontinuierliche Weiterentwicklung eines BCMS
  - Umsetzung ohne Zusatzwerk oder Vorhandensein eines ISMS möglich
- Anpassung an ISO-Standard 22301:2019
- Ganzheitliche Betrachtung des BCM im Fokus der **Resilienz**

Resilienz im BCM

- kontinuierlich verbessertes BCMS
- Schaffung eines Prozess, um organisatorische ***Resilienz*** (Widerstandsfähigkeit) aufzubauen
- ISO 22316:2017: Resilienz einer Institution wird auch von Prozessen beeinflusst, die keinen direkten Bezug auf die Themen Security und Business Continuity haben

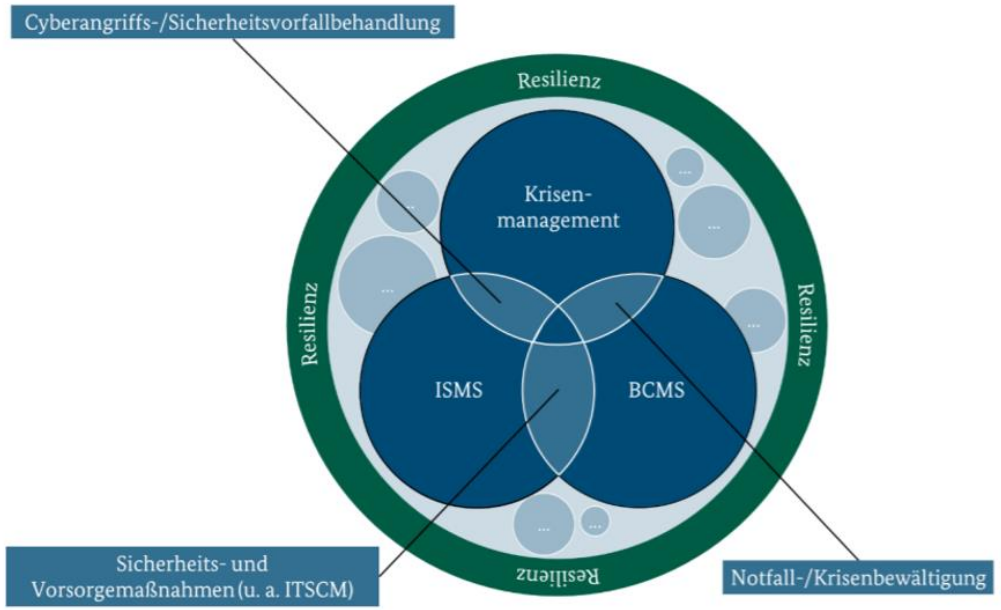
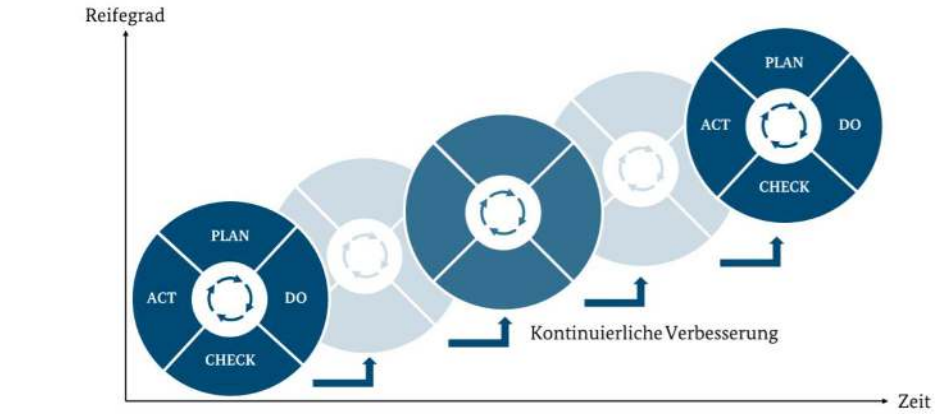
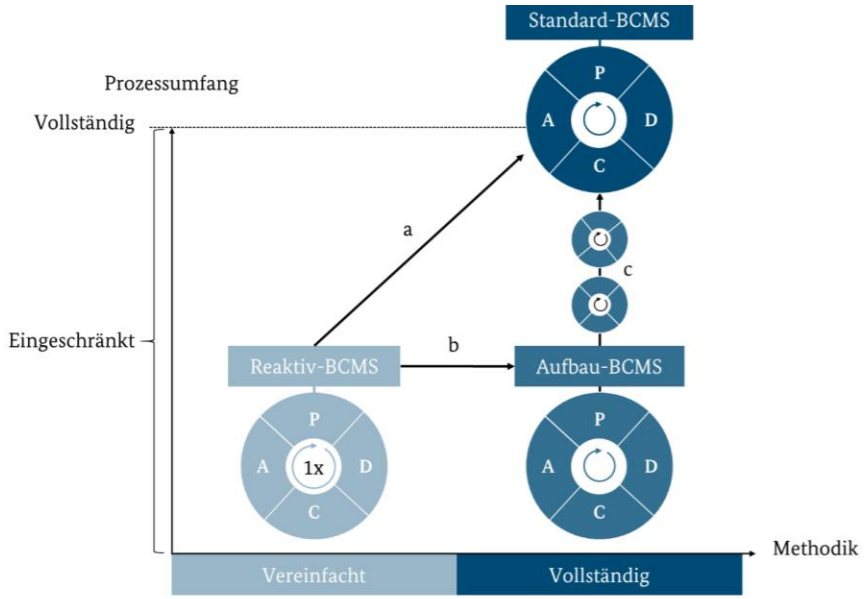


Abbildung 1: Resilient schaffen durch verschiedene Sicherheitsthemen

Stufenauswahl für Use Case

Eigenschaft	Reaktiv-BCMS	Aufbau-BCMS	Standard-BCMS
Vorteile	Schnelle Fähigkeit zur Notfall-bewältigung	Schrittweiser und damit ressourcen-schonender Aufbau des BCMS	Vollständige Absicherung und damit **Resilienz** der Institution
Nachteile	Lücken in der Absicherung und Bereiche, die nicht betrachtet werden	Bereiche, die in der Absicherung der Institution nicht betrachtet werden	Erhöhter Ressourcen-bedarf gegenüber den Einstiegsstufen





SRE, Chaos Engineering, Simian Army

Site Reliability Engineering (SRE)

- Site Reliability Engineering (SRE) ist ein Software-Engineering-Ansatz für IT-Operations
- SRE-Teams verwenden Software als Tool zur Verwaltung von Systemen, Behebung von Problemen und Automatisierung von Operations-Aufgaben
- SRE ist eine Praktik bei der Erstellung skalierbarer und hochzuverlässiger Softwaresysteme mit besonderem Fokus auf Resilienz

Chaos Engineering

- Disziplin des Experimentieren mit einem Software-System in Produktion
- Ständige Weiterentwicklung und Aufbau in sichere Systeme und Infrastrukturen durch Herbeiführen von unerwarteten Ereignissen

Simian Army

- "The Simian Army" ist eine von Netflix entwickelte Suite von Tools zum Testen der Zuverlässigkeit, Sicherheit und Resilienz der Infrastruktur
- Es besteht aus Chaos Monkey, die Produktionsinstanzen nach dem Zufallsprinzip deaktivieren
- Es gibt den **Latency Gorilla**, der Netzwerkverzögerungen simuliert oder den **Chaos Gorilla,** der ganze Rechenzentren lahmlegt

“So next time an instance fails at 3 am on a Sunday, we won't even notice.”

Rezept aus der „Chaos-Kitchen“

- ✓ Trennen der Systeme in zentrale Schlüsselkomponenten
- ✓ Testen des Systems, ohne dass die Schlüsselkomponenten verfügbar sind
- ✓ Das System zum Absturz bringen (zuerst in Nicht-Produktionsumgebungen) ☺
- ✓ Fehler der zentralen Schlüsselkomponenten im Produktivsystem einführen
- ✓ Einführen eines Datenbank Fehlers in der Produktionsumgebung
- ✓ Provoziere einen systemweiten Absturz auf der Produktionsumgebung
- ✓ Betrachte das "ganzheitliche" Logging (z.B. was hält den vollen Service noch aufrecht?)
- ✓ Identifiziere Abhängigkeiten zu anderen Systemen, Komponenten, Schnittstellen
- ✓ Verbessere die Fehlerbehandlung und Wiederherstellung (manuell-automatisiert)

*Aus **"echten"** Fehlern **lernen!***

Fazit

Eine der grössten **Schwächen** der meisten Disaster-Recovery-Pläne ist, dass sie nie in die **Praxis** umgesetzt werden

Für das Unternehmen ist das natürlich eine gute Nachricht. Niemand will sich mit einer Katastrophe auseinandersetzen!

Es ist jedoch nur so lange eine gute Nachricht, wie es nie zu einer **Katastrophe** kommt

SRE Ansatz für das Continuity Management:

- regelmässige Disaster-Recovery-Meetings zwischen Site Reliability Engineers und Risiko / Compliance-Team
- Identifizieren von Lücken in der Disaster Recovery
- Entwickeln von zusätzlichen Plänen zur Verbesserung, Bewertung oder Veränderung
- Chaos Engineering zur Simulierung des Ernstfalls

"Hoffnung ist keine Strategie."

Traditioneller SRE-Spruch

„Du lernts nicht, wie man Ausfälle behebt, indem Du Folien liest und Videos schaust….“

„Wir lernen es, indem wir es tun!“

sven.ossenberg@glenfis.ch

Vielen Dank für Dein Interesse!

Glenfis AG

Badenerstrasse 623
8048 Zürich
Schweiz
+41 44 202 81 10

glenfis.ch
pontine.ch
devops.ch