Compliance im Prozessmanagement

Ute Riemann

Das heutige Unternehmensumfeld wird von einer sich immer dynamischer verändernden Entwicklung der Markt- und Wettbewerbssituation geprägt [1]. Erfolgreiche Unternehmen unterliegen damit der Notwendigkeit sich einem kontinuierlichen tief greifenden und grundlegenden Wandel zu stellen [2]. Dies erfordert ein hohes Maß an Flexibilität und Anpassbarkeit für die Unternehmensprozesse sowie für entsprechende IT-Systeme. In diesem Zusammenhang kommt den Konzepten „agiles Prozessmanagement" und „Cloud Services" verstärkt Bedeutung zu, adressieren sie doch aufgrund ihrer Methodik bzw. ihrer Konzeption genau die flexible und schnelle Anpassung auf neue Unternehmensanforderungen [3].

Dipl.-Informatikerin Ute Riemann ist Business Enterprise Consultant bei der SAP mit Expertenwissen im Bereich Projektmanagement und Business Prozess Entwicklung sowie Dozentin für Projekt- und Change Management der FH Villingen-Schwenningen.

Die prozessuale Compliance-Sicherheit muss umfänglich betrachtet werden. Anders als im traditionellen Prozessmanagement ist die Berücksichtigung der technischen Realisierung durch die enge Verzahnung mit der IT im Cloud-Umfeld unabdingbar. Zur Beantwortung dieser Frage, ist es notwendig, sich die verschiedenen Dimensionen, die betrachtet werden müssen, zu vergegenwärtigen:

- Dimension 1: Prozessmodule
- Dimension 2: Cloud Services
- Dimension 3: Compliance-Anforderungen

Diese Dimensionen unterliegen zusätzlich noch einer zeitlichen Dynamik: in unterschiedlichen Phasen des Prozesslebenszyklus kommen unterschiedliche Anforderungen auf die Cloud Services zu und beeinflussen so den Compliance-Lebenszyklus.

In diesem Beitrag lesen Sie:

- wie die Erfüllung der Compliance-Anforderungen sichergestellt werden kann,
- wie ein realistisches Compliance-Versprechen aussieht,
- ob die Nutzung der Cloud Lösungen für alle Prozesse eine Option ist.

Mehrdimensionale Betrachtung der Compliance-Anforderungen

Obwohl Compliance in der Praxis oft als abstrakt, komplex und intransparent angesehen wird, ist es in der heutigen Geschäftswelt ein unausweichliches Thema. Durch die Modularisierung der Prozesse und der Individualisierung der IT, kommen neue Herausforderungen auf die Einhaltung der Compliance zu, bedarf es einer erweiterten Herangehensweise zur ihrer Umsetzung und Sicherstellung.

Prozessmodule

Zur Umsetzung der geforderten Prozessflexibiliät ist die Überwindung der traditionell-hierarchischen Herangehensweise an Prozesse [4] sowie die Zerlegung der Unternehmensprozesse in sogenannte Prozessmodule ein wesentlicher Ansatz. Diese Zerlegung führt zu einer Prozess Inter-Flexibilität (= der Flexibilität und individuellen Kombinierbarkeit der Prozessmodule selbst) und einer Prozess Intra-Flexibilität (= der Flexibilität zwischen den Prozessmodulen). Die Prozessmodule selbst bestehen aus einem Prozesskern, der die wesentlichen Funktionalitäten umfasst und aus den standardisierten Schnittstellen. Diese dynamische Verbindung der Prozessmodule erlaubt die Generierung unterschiedlichster End-to-End Unternehmensprozesse. Was bedeutet es für diese Prozessmodule wenn diese „in der Cloud" stattfinden und welche Konsequenzen hat das für die Erreichung und Einhaltung der Compliance-Anforderungen für ein Unternehmen?

Cloud Services

Reduziert man Cloud Services auf Ihre Kernelemente, dann geht es um eine Form der bedarfsgerechten und

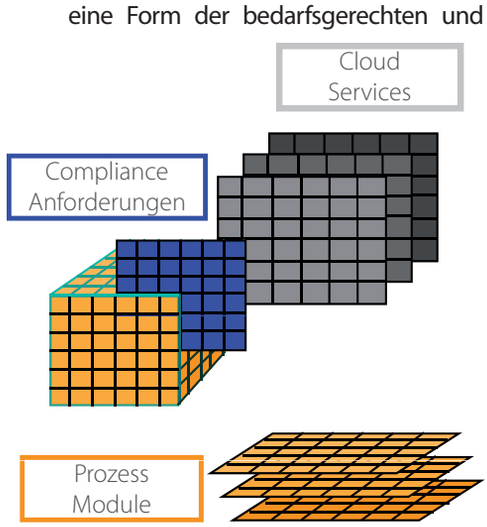

Bild 1: Dimensionen der Compliance im Prozessumfeld.

flexiblen Nutzung von IT-Leistungen. Somit werden die Cloud Services zum idealen Partner zur schnellen und flexiblen Umsetzung von Prozessanforderungen durch die ganzheitliche und effiziente Integration verschiedenster Cloud Services. Aktuell gehen die Meinungen beim Thema Cloud Services spätestens bei der Compliance-Sicherheit weit auseinander. Das Spektrum reicht von hoch risikobehafteter bis hin zu gefeierter neuer Technologie. Wesentlich für diese Einschätzung ist, dass unabhängig von Cloud Services die Verantwortlichkeit für Prozesse und Daten nach wie vor beim Besitzer verbleibt. Insofern ist es zur Erreichung einer adäquaten Cloud Compliance notwendig alle Anforderungen umfänglich zu kennen und hinsichtlich ihrer Bedeutung zu bewerten, sodass

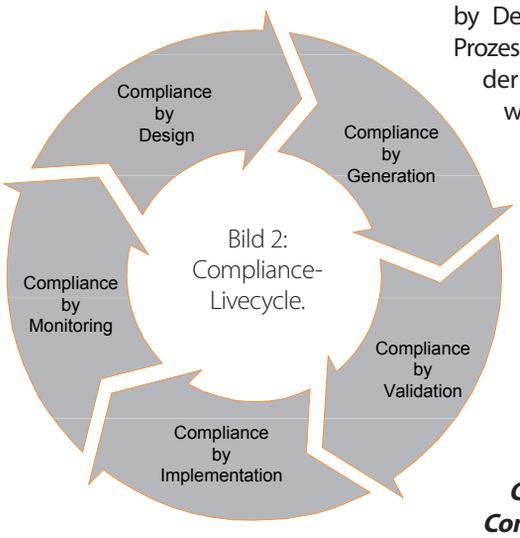

Bild 2: Compliance-Livecycle.

eine sichere Basis geschaffen wird sowie Vorteile der Cloud Services ihr Potenzial entfalten können.

Compliance-Anforderungen

Die grundlegende Annahme dieses Artikels ist, dass den Compliance-Anforderungen ein Compliance-Zyklus der Prozesse und Cloud Services zu Grunde liegt. Auf Basis der genauen Kenntnis von Prozessen und Cloud Services entlang dieses Compliance-Zyklus können so die Compliance-Anforderungen identifiziert und geeignete Maßnahmen ergriffen werden.

Die Identifikation der individuellen Rahmenbedingungen eines Unternehmens, die sowohl den Nutzer von Cloud Services als auch dessen Anbieter betreffen, ist unerlässlich. Von Bedeutung sind hierbei unter anderem die Branche, die Rechtsform, der Ort der Leistungserbringung oder der angebotenen Produkte bzw. Dienstleistungen. Der Compliance-Zyklus bietet hier eine Orientierungshilfe bei der Identifikation der Compliance-Anforderungen und sichert eine gewisse Vollständigkeit, Konsistenz und Qualität der Maßnahmen zu, die zur Erfüllung der Compliance-Anforderungen zu definieren sind.

Compliance by Design

Bei der Prozessdefinition steht die Spezifikation von Regulationen und deren Integration in die Prozesse im Vordergrund. Generell sollte die Compliance by Design durch die Annotation von Prozessmodulen mit Regulationen bei der Dokumentation sichergestellt werden. Anders als bei der traditionellen Prozessmodellierung ist im Hinblick auf agile Prozessmodule davon auszugehen, dass bei der Zusicherung von Compliance in der Prozessdesign-Phase die Granularität der Prozessmodule gegenüber den zu prüfenden Regulationen auf Prozessmodulebene angepasst werden müssen.

Compliance by Generation und Compliance by Validation

Compliance by Generation und Compliance by Validation sind Effekte die erst durch das Konzept der dynamischen Prozessmodule und den Ansatz der Cloud Services zu einem Thema geworden sind. Durch die Anwendung dieser dynamischen Konzepte und die Ausprägung der Prozesse sowie deren Implementierung über verschiedene Cloud Services hinweg wird die notwendige Kontextinformation zur Beantwortung der Compliance-Anforderungen geliefert.

Auf prozessualer Seite kann durch eine entsprechende logikbasierte Modellierung der Prozessmodule inkl. der entsprechenden Regularien eine ausreichende Visualisierung ermöglicht werden:

1. Generierung und Sicherstellung über die Schnittstellen, dass nur compliance-verträgliche Prozessmodelle erzeugt werden [5, 6].
2. Validierung der Prozessmodelle zur Laufzeit. Damit wird die Compliance-Sicherheit geprüft und transparent gemacht wodurch wiederum die Zusicherung der Compliance-Anforderung zur Modellierzeit sichergestellt wird.

Auf technischer Seite kann durch Pilotieren der Prozesse auf Basis der ausgewählten Services diese Frage beantwortet werden:

1. Pilot-Implementierung der Prozessmodule um die sich in diesem Kontext ergebenden Compliance-Anforderungen zu identifizieren und geeignete Maßnahmen zu definieren.
2. Technische Trennung der Prozess-Guidelines und Content von der Cloud Service Applikationslandschaft, um die Compliance-Anforderungen, sensitive Information und Prozesse vor dem Zugriff unbefugter Dritter zu schützen.

Compliance by Implementation

Im Gegensatz zu den prozessual-definitorischen Phasen kommen in den Laufzeitphasen zur Überprüfung der Verträglichkeit mit Regulationen (Compliance by Implementation und Compliance by Monitoring) größere Herausforderungen an die Zusicherung der Compliance zu. Für Cloud gelten keine neuen Regeln, sodass die bekannten IT-Compliance-Anforderungen Anwendung finden. Grundsätzlich gilt, dass der Datenbesitzer für die Datensicherheit und Ausführung der Sicherheitskontrollen verantwortlich ist – unabhängig von der Umgebung in der die Daten prozessiert werden. Obwohl die Laufzeitüberwachung der Compliance wichtige Kontextinformation einbezieht, bleibt doch die Limitation bestehen, dass keine Aussagen über Prozesse im Detail und der Absicherung der Daten gemacht werden können um Unverträglichkeiten ausschließen zu können. Hinzu kommt, dass die Services aus der Cloud neue Merkmale aufweisen, die in der klassischen Prozessimplementierung nicht oder kaum existierten. Dazu

zählt z.B. der Applikationsbezug über das Internet wie auch der hohe Grad an Virtualisierung. Um in einem solchen Umfeld eine nachweisbare Konformität der Implementierung zu erfüllen, verlangt es eine gesonderte Auseinandersetzung mit den für Cloud Computing spezifischen Risiken und Vorgaben.

Da es für den Daten-/Prozessbesitzer keine direkte Kontrollmöglichkeit gibt, ist es umso wichtiger entsprechende indirekte Kontrollmechanismen hinsichtlich Cloud Services-Anbieter sicher zu stellen:

1. Sicherstellung (z.B. über den Firmensitz), dass datenschutzrechtliche Bestimmungen, Compliance-Regeln (die u.a. in den Rahmenwerken Basel II/III und EuroSox festgelegt sind) erfüllt werden.
2. Nachweis von IT-Sicherheitszertifikaten.
3. Nachweis von Compliance-Zertifikaten (SAS-70-Typ-II-Zertifikat) für den Fall das SOX Auflagen erfüllt werden müssen und z.B. Finanzdaten des Kunden richtig und vollständig verarbeitet werden.

Compliance by Monitoring

Um die Compliance-Anforderungen gerecht zu werden, ist es notwendig ein Compliance Monitoring aufzusetzen. Dieses Monitoring muss einerseits die Überwachung der Prozesse und Services im gesamten Lebenszyklus sowie in der Interaktion mit den beteiligten IT-Systemen umfassen andererseits aber auch die kontinuierliche Berücksichtigung bei Veränderungen der Compliance-Regularien berücksichtigen. Die hier zur Anwendung kommenden Regularien sind technologie-unabhängig – also auch auf Cloud anwendbar. Sogar wenn die Auditkriterien im Zeitalter proprietärer und selbst-geownter Systeme entwickelt wurden.

Fazit

Der Wettbewerb fordert eine schnellere und flexiblere Antwort auf die sich dynamisch verändernden Rahmenbedingungen. Dieser Herausforderung wird mit agilem Prozessmanagement und Cloud Computing begegnet. Auch wenn das Thema Compliance durch die Sicherstellung einer gleichbleibenden Ausführung und Qualität der Prozesse im Einklang mit den relevanten Normen einen positiven Effekt auf das Prozessmanagement ausübt [7], sind die Herausforderungen, die insbesondere die Nutzung von Cloud Services an die Einhaltung der Compliance-Anforderungen stellen, nicht zu unterschätzen. Die Analyse bezüglich der Sicherstellung einer durchgängigen, transparenten und nachvollziehbaren Compliance über die verschiedenen Phasen hinweg hat gezeigt, dass es verschiedenste Problemstellungen und Herausforderungen gibt.

Es gilt das agile Prozessmanagement und Cloud Services gleichermaßen zu beobachten, um zu wissen, wohin sie sich entwickeln, was sie bewirken und was sie bedrohen. Auch wenn sich Unternehmen heute gegen die die Nutzung von Cloud Services um Zusammenhang mit der Entwicklung und Implementierung von Prozessmodulen entscheiden, sollten sie ihre Rezeption in der neuen „Agilen Cloud-Prozessarena " beobachten. Aktuell ist aufgrund der teilweise noch nicht geklärten Fragestellung hinsichtlich der Absicherung der Compliance-Fähigkeit der Einsatzbereich von Cloud Service begrenzt, verspricht aber durch die in Entwicklung befindlichen Regularien und Services ein enormes Wachstumspotenzial.

Checkliste zur Erreichung der Compliance-Anforderungen

- ❒ Sicherstellen der Prozessschnittstellen und Validierung der Prozessmodelle durch entsprechende Schnittstellendefinition und Tests.
- ❒ Pilotieren kritischer und ausgewählter Prozessmodelle auf Basis identifizierter Compliance-Anforderungen.
- ❒ Aufsetzen entsprechender vertraglicher Dokumentationen um Maßnahmen im Rahmen der Implementierung und des Betriebes abzusichern.
- ❒ Trennung der Prozess-Guidelines und Content von der Cloud Service Applikationslandschaft um sensitive Information und Prozesse vor dem Zugriff unbefugter Dritter zu schützen. ■

Literatur

[1] Knyphausen, D. zu (1993): Überleben in turbulenten Umwelten: Zur Behandlung der Zeitproblematik im Strategischen Management. In: Zeitschrift für Planung 4 (1993), 2, S. 143-162.

[2] Zahn, E.; Schmid, U. (1997): Produktionswirtschaft im Wandel. In: Wirtschaftswissenschaftliches Studium 26 (1997), 9, S. 455-460.

[3] Gareis, R. (1989): „Management by Projects" - Der zukunftsorientierte Managementansatz. In: Reschke, H., Schelle, H. (1989, Hrsg.): Beiträge zum Projektmanagmentforum 89. München, 1989, S. 95-104.

[4] Aier, S., Schönherr, M.: Enterprise Application Integration als Enabler flexibler Unternehmensarchitekturen. In (Hasselbring, W., Reichert M., Hrsg.): EAI 2004 – Enterprise Application Integration. Tagungsband des GI-/GMDS-Workshops EAI'04, OFFIS, Oldenburg, 12. – 13.Februar 2002.

[5] Goedertier, S., Vanthienen, J.: Designing compliant business processes with obligations and permissions. In: BPM 2006 Workshops. (2006), S. 5–14.

[6] Küster, J., Ryndina, K., Gall, H.: Generation of business process models for object life cycle compliance. In: Proc. BPM '07. Volume 4714 of LNCS., Springer (2007), S. 165–181.

[7] Sadiq, S., Governatori, G., Naimiri, K.: Modeling control objectives for business process compliance. In: Proc. BPM '07. (2007).

Schlüsselwörter:
Prozessmodularisierung, Prozess Inter-Flexibilität, Prozess Intra-Flexibilität, Compliance-Livecycle

Compliance between the priorities of agile process management and cloud services

The article provides an insight how to identify the compliance specific requirements across the various phases, and-how to address the phase-specific level of compliance requirements in the best possible way.

Keywords:
process modularisation, process inter-flexibility, process intra-flexibility, compliance lifecycle

Kontakt:

Ute Riemann
Business Enterprise Principal Consultant
Business Transformation Services
SAP Deutschland AG & Co. KG
E-Mail: ute.riemann@sap.com