Einführung von ibo netProject mit der Cloud-Lösung

in der Sparkasse zu Lübeck AG

Sparkasse
zu Lübeck

Inhalt

1. Persönliche Vorstellung
2. Ausgangssituation
3. Vorgehen
4. Umsetzung
5. Verlauf
6. BAIT und ibo Cloud-Hosting

Inhalt

1. Persönliche Vorstellung

Joanna Warszawski

Werdegang in der Sparkasse zu Lübeck AG

08.2007 - 01.2010	Ausbildung zur Bankkauffrau
01.2010 - 06.2012	Sachbearbeiterin Betriebsorganisation
07.2012 - 02.2019	Multiprojektmanagerin
seit 03.2019	Teamleiterin Passivsteuerung

Inhalt

2. Ausgangs-situation

in der Sparkasse zu Lübeck AG

Projektmanagement in der Sparkasse zu Lübeck AG

- 2005 führten wir das **klassische Projektmanagement** ein.
- In dem Zuge stellten wir eine **Software** zur Verfügung, die einfache Funktionen abbilden konnte (Notes-basiert).
- Wir schulten die Rolle und Aufgaben eines Projektleiters und händigten **Projektleiter-Zertifikate** aus.
- 2006 implementierten wir die Stelle „**Multiprojektmanager/in**“.
- 2011 wickelten wir über einen Zeitraum von drei Jahren erstmalig ein großes **Strategieprojekt** ab, das mehr als 50 (Klein)Projekte umfasste, die teilweise in Abhängigkeiten zueinander standen.
- 2014 stießen wir mit der vorhandenen Software an **Funktionsgrenzen** und suchten nach einer Möglichkeit, das klassische Projektmanagement weiter zu professionalisieren.
- 2015 entwickelten wir die **Projektmanagement Konzeption** weiter.

Inhalt

3. Vorgehen

Voraussetzungen und Anforderungen

Voraussetzungen:

- Wir sind eine **IT-konsolidierte** Sparkasse.
- Unsere **IT-Strategie** sieht vor, dass wir in erster Linie die angebotenen Produkte der Finanz Informatik nutzen.
- Das klassische **Projektmanagement** wird seit Jahren in der Sparkasse **gelebt** und kontinuierlich **weiterentwickelt**.
- Projektleiter werden im Rahmen einer Projektmanagement **Schulung** zum Projektleiter befähigt.
- Es gibt eine monatliche **Projektekommission** mit dem Gesamtvorstand.
- Jährlich wird eine strategische **Projektplanung** durchgeführt, die dynamisch an veränderte Rahmenbedingungen angepasst wird.

3. Vorgehen

Voraussetzungen und Anforderungen

Anforderungen:

- Software zur **Unterstützung** des Projektleiters (→ schneller Soll-/Ist-Abgleich, schneller Status-Überblick)
- **Intuitive** Software mit einem guten **Preis-Leistungs-Verhältnis**
- Elektronische **Workflows**
- Komfortables **Rollen- und Rechtesystem**
- Automatische **E-Mail-Erinnerungen** für Abgabetermine
- **Berichte** auf Knopfdruck (MPM)
- Individuelle **Gestaltungsmöglichkeiten** der Inhalte (Anträge, Formulare, Berichte, etc.)
- Nutzung über **mobile Endgeräte** (IPad/IPhone)
- **Perspektivisch**:
  - Möglichkeit komplexere „Linienmaßnahmen“ getrennt vom Projektportfolio darzustellen
  - Abbildung der Projektplanung
  - Abbildung der Projektreview-Phase

Inhalt

1. Persönliche Vorstellung
2. Ausgangssituation
3. Vorgehen
4. Umsetzung
5. Verlauf
6. BAIT und ibo Cloud-Hosting

4. Umsetzung

Phase Softwareanforderung 2015

Softwareanforderung:

- IT-Strategie: Es gibt **kein FI-Produkt** → freie Wahl bei Software
- ibo netProject in der **Mietvariante mit Cloud-Hosting**, da hohe Serverkosten für Drittanwendungen bei der FI
- Herausforderung: Anmerkungen vom DSB bzgl. Cloud-Hosting zur Bewertung des **Datenschutzes** und der **Datensicherheit**:
  - Auftragnehmer-Konstrukt Cloud-Server inkl. Server-Standort
  - Fehlende Service-Level
  - Hohe Aufwände bei Kontroll- und Überwachungsfunktion der Daten auf den Cloud-Servern (Server-Standort „Karibik“)

4. Umsetzung

Phase Softwareeinführung 2016

Softwareeinführung:

- Start mit **50 Lizenzen**
- **ibo-Einführungstage** mit einem Trainer
- Zunächst Abbildung des **Projektportfolios** mit den Phasen Projektantrag, Projektdurchführung und Projektabschluss
- **Schulungen** mit Theorie-Teil Projektmanagement („Auffrischung“) und Übungsaufgaben durchgeführt:
  - für Projektleiter Tagesschulung
  - für Projektmitarbeiter Halbtagesschulung
  - für Vorstand wegen techn. Workflow-Freigabe und Management-Cockpit

Inhalt

1. Persönliche Vorstellung
2. Ausgangssituation
3. Vorgehen
4. Umsetzung
5. Verlauf
6. BAIT und ibo Cloud-Hosting

5. Verlauf

Ausbau ibo netProject

Ausbau der Funktionen in ibo netProject:

- **Berichtswesen** für monatliche Projektekommission
- **Projektreview** und **Projektumsetzungscontrolling**
- **Projektjahresplanung**
- Ausbau der **Mandanten** für:
  - Schulungen
  - Innerbetrieblicher Unterricht für Azubis
  - Abteilungsinterne Maßnahmen

→ 2017: Erhöhung der Lizenzen auf 75

→ 2019: Erhöhung der Lizenzen auf 110

5. Verlauf

Revisionsprüfung 2017

Revisionsprüfung:

- **Externes Server-Hosting** wurde unter den verschärften Anforderungen der BAIT* in Bezug auf IT-Risiken bewertet.
- **Feststellung**:
  Bei der Softwareanforderung wurden für das Server-Hosting die Themen Auslagerung und Risikoanalyse nicht betrachtet (vgl. Anforderungen gem. AT 7.2 Tz. 2* i.V.m. AT 9** MaRisk).
- Diskussion um die Einstufung des externen Server-Hostings als **Auslagerung** oder **IT-Fremdbezug**.
- Im Rahmen der Umsetzung der 5. MaRisk Novelle bis Oktober 2018 wurde AT 9 Outsourcing neu bewertet und aufgestellt, hierzu gab es eine neu erarbeitete **Risikobetrachtung**.

*) BAIT: Bankaufsichtliche Anforderungen an die IT

**) AT 7.2: Technisch-organisatorische Ausstattung; Tz. 2: IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen.[…]

***) AT 9: Outsourcing

Inhalt

1. Persönliche Vorstellung
2. Ausgangssituation
3. Vorgehen
4. Umsetzung
5. Verlauf
6. BAIT und ibo Cloud-Hosting

6. BAIT und Cloud-Hosting

Grundsätzliches zum Cloud-Computing in der Sparkasse

Cloud-Hosting:

- Sparkassenverband spricht interne Empfehlungen zur IT-Strategie aus, um die aufsichtsrechtlichen Anforderungen zu erfüllen:
  → Erste Wahl grds. FI-Produkte
- Gemäß der Anforderungen aus der BAIT 8* ist Cloud-Computing grundsätzlich OK, sofern technische und organisatorische Maßnahmen sicherstellen, dass die **Ordnungsmäßigkeit der Geschäftsorganisation** beachtet wird und Risiken angemessen bewertet werden.
- In Bezug auf ein externes Server-Hosting stellen sich die Fragen:
  - Wo stehen die Server?
  - Wer hat Zutritt zu den Server-Räumen?
  - Wie sind die Server-Räume abgesichert (u.a. Brandschutz u.ä.)?
  - Wir sehen die (Unter-)Auftragnehmer-Verhältnisse konkret aus?
  - Bekommen wir Dienstleisterwechsel mit?

*) BAIT 8 Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

6. BAIT und Cloud-Hosting

Risikoanalyse des externen Server-Hostings in der Sparkasse

Risikoanalyse externes Server-Hosting:

- Neue Risikoanalyse resultierend aus der 5. MaRisk Novelle

  Ergebnis:
  Externes Server-Hosting stellt keine Auslagerung im Sinne der AT 9 MaRisk dar, sondern einen **Fremdbezug von IT-Dienstleistungen gem. BAIT 8**.

- Cloud-Computing ist in der **Risikobetrachtung** grds. als Auslagerung einzustufen, sofern der IT-Fremdbezug im Zusammenhang mit Bankgeschäftsprozessen steht oder mit Prozessen von wesentlicher Bedeutung (bspw. hier: Dokumentation von wichtigen (strategischen) Entscheidungen).

- D.h. dass der IT-Fremdbezug nach BAIT 8 quasi wie eine wesentliche Auslagerung gem. AT 9 MaRisk zu behandeln ist, weil alles im Zusammenhang mit der IT-Dienstleistung wesentlicher (bankfachlicher) Prozesse steht.

- Der **Fokus** liegt bei der Bewertung der Auslagerung aber auf **IT-Risiken**.

6. BAIT und Cloud-Hosting

Maßnahmen aus der Risikoanalyse des externen Server-Hostings in der Sparkasse

Maßnahmen aus der Risikoanalyse:

- **Risikobewertung** gem. BAIT 8:
  Der IT-Fremdbezug wird behandelt wie eine Auslagerung nach AT 9 MaRisk, aber mit **zielgerichteten Fragestellungen** in der Risikobewertung hinsichtlich der IT-Dienstleistung

- Beispielsweise:
  - Wer ist Dienstleister?
  - Welche Prozesse werden ausgeführt?
  - Welche SLA sind vereinbart?
  - Wie sieht das Notfallkonzept aus?
  - Kann die Dienstleistung weiterverlagert werden?
  - Welche Maßnahmen ergreifen wir, um das Risiko zu minimieren?
  - In welchem Turnus wird der Dienstleister kontrolliert? Wie?
  - …

6. BAIT und Cloud-Hosting

Vorstandsbeschluss zum externen Server-Hosting in der Sparkasse 2018

Umsetzungsvarianten:

1. **Installation Drittanwendung auf FI-Server**

   Wir kennen die Risiken und
   wählen das teurere Produkt,
   zu einem schlechteren Preis-/Leistungsverhältnis,
   sind aber aufsichtsrechtlich sicher aufgestellt.

2. **Mietvariante auf ibo-Servern (Cloud-Hosting)**

   Wir sind bereit, die Risiken zu übernehmen,
   folgen dem besseren Preis-/Leistungsverhältnis und
   nehmen den Mehraufwand für die jährliche Überprüfung der Risikoanalyse zum SITB bei der Anwendungsbetreuung in Kauf.

6. BAIT und Cloud-Hosting

Maßnahmen zur Risikominimierung beim externen Server-Hosting in der Sparkasse

Maßnahmen zur Risikominimierung:
(Ein Rest-Risiko wird immer bestehen!)

- Jährliche **Zertifizierung** nach gängigen, internationalen Standards der PCI DSS-Zertifizierung*
  → Spielte in der Entscheidungsfindung eine erhebliche Rolle!
- Jährliche **Risikoanalyse** zu den Informationssicherheits-Risiken (Risikoübernahme durch den Vorstand)
- **Schutzbedarf** der Anwendung ist „hoch“ eingestuft
- Stringentes **Zugriffs-** und **Zugangskonzept** (Hinterlegung von IP-Adressen; restriktive Zugriffsregelungen, Protokollierung Fehlzugriffe, Verschlüsselung der Daten (im Mailversand), etc.)
- **IT-Sicherheitskonzept** ibo netProject im Cloudbetrieb

*) Als offiziell vom PCI Security Standards Council akkreditierter Auditor (QSA) und Approved Scanning Vendor (ASV) berät und zertifiziert die usd AG europaweit nach dem internationalen Sicherheitsstandard der Kreditkartenindustrie (PCI DSS, PCI-PA DSS). Payment Card Industry Data Security Standard kurz PCI DSS **gilt für Banken (Issuer und Acquirer)**, Payment Service Provider, **Hosting Provider**, Händler und Payment Application Provider gleichermaßen.
Quelle: https://www.tuev-sued.de/fokus-themen/it-security/pci-zertifizierung

Fragen?

Vielen Dank.

Ansprechpartner:
Joanna Warszawski
Sparkasse zu Lübeck AG

Telefonnummer: 0451/147-166
E-Mail-Adresse: joanna.warszawski@spk-luebeck.de

Sparkasse
zu Lübeck