# Deloitte.



# ServiceNow als Cloud Service:

Transparente Bewertung von Risiken als erster Schritt

# ServiceNow als Cloud Service: Transparente Bewertung von Risiken als erster Schritt

Die Nutzung von ServiceNow in der Cloud wird zunehmend populärer. Vor der tatsächlichen Einführung von ServiceNow stehen viele unserer Kunden vor einer intensiven Prüfung der Risiken. Typische Fragestellungen sind:

- Ist meine Organisation reif für ServiceNow aus der Cloud?
- Ist ServiceNow professionell organisiert und im Hinblick auf relevante Standards zertifiziert?
- Gibt es Wege unternehmenskritische Daten sicher und im Einklang mit geltenden Gesetzen mit ServiceNow zu verarbeiten?
- Ergreift ServiceNow angemessene Maßnahmen zur Sicherung seiner Infrastruktur?

# Ein Blick hinter die Kulissen

Vor einer endgültigen Entscheidung tragen sich unsere Kunden mit dem Gedanken, ServiceNow als prozessunterstützendes Tool in meist globalen Organisationen einzuführen. Die Lösung soll, wenn aus Risiko-Sicht möglich, in der Cloud betrieben werden. Zumeist haben Kunden bereits Vorarbeit im Hinblick auf Risiko Management und Information Security Management getroffen und orientieren sich an marktgängigen Standards.

# Deloitte hilft die entscheidenden Risiken der ServiceNow Lösung für Sie zu identifizieren

1. Wir greifen auf bestehende ServiceNow Risiko-Assessments zurück.

- 2. Marktgängige Standards und neue Kunden-Spezifika werden mit diesen verknüpft.
- Abschließend dokumentieren wir die ServiceNow Risiken vollständig in einer klaren Entscheidungsvorlage.

Im Ergebnis zeigt die Entscheidungsvorlage auf, welche Risiken zu vernachlässigen sind und welche tatsächlich Einfluss auf die Auswahl von ServiceNow als Cloud Lösung haben.

# Jeder Kunde bewertet Risiken anders – unsere ServiceNow Erfahrung hilft dabei

- Deloitte nutzt die Cloud Computing Intelligence Risk Map, mittels derer ServiceNow-spezifische Risiken angemessen identifiziert werden (siehe Grafik im Innenteil).
- Insgesamt adressiert die Cloud Computing Intelligence Risk Map 130 Risiken, die mit marktgängigen Standards verknüpft sind (siehe Abb. 1).



Sources: Deloitte assessment based on Standardized Information Gathering (SIG) Questionnaire (04.12) and several reports and white papers originating from ServiceNow

# Abb. 1 - Client-specific evaluation of each risk map sub-area in scope

## Abb. 2 – Management summary with 5 core results identified per risk map area



- Deloitte ist globaler Partner von Service-Now und hat tiefgreifende Informationen bezogen auf organisatorische, prozessuale und technische Rahmenbedingungen (siehe Abb. 2).
- Wesentliche Ergebnisse werden im Einklang mit kundenspezifischen Anforderungen klassifiziert und priorisiert (siehe Abb. 3).

# Deloitte unterstützt Sie als globaler ServiceNow System Integrator ganzheitlich

Deloittes Service Line Technology Strategy & Architecture bietet umfangreiche Dienstleistungen in IT Strategy & Innovation, IT Governance & Management, IT Sourcing & Procurement, IT M&A sowie Transformation an und kann somit im gesamten Service Lifecycle beraten. Unsere Dienstleistungen werden zudem regelmäßig von Analysten ausgezeichnet. Deloitte erzielte beispielsweise in der "ALM Intelligence Competitive Landscape Analysis: Cloud Consulting 2016" als führendes Cloud Beratungsunternehmen die Leader-Position.

### Abb. 3 - All core results per risk map area are classified in a heat map



According to a potential negative impact on CLIENT the majority of core results have been classified with a risk of "low" or less (38 of 45). Methodology according to CLIENT Risk Management Process: Vulnerability analysis scenarios and rating applied to findings of ServiceNow assessment and a possible negative impact on CLIENT environment

# Ihre Ansprechpartner

### Jochen Fauser

Partner Technology Strategy & Architecture jfauser@deloitte.de

# **Timm Riesenberg**

Senior Manager Technology Strategy & Architecture triesenberg@deloitte.de

# Per Kall

Manager Technology Strategy & Architecture pkall@deloitte.de



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/de/ UeberUns for a more detailed description of DTTL and its member firms.

Deloitte provides audit, risk advisory, tax, financial advisory and consulting services to public and private clients spanning multiple industries; legal advisory services in Germany are provided by Deloitte Legal. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 244,000 professionals are committed to making an impact that matters.

This communication contains general information only not suitable for addressing the particular circumstances of any individual case and is not intended to be used as a basis for commercial decisions or decisions of any other kind. None of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

# **Deloitte**

location

# Cloud Computing Risk Intelligence Map



from within the cloud • Lack of controls to prevent cloud provider from accessing encryption keys

environment

• Poorly implemented encryption and key management due to cloud service immaturity

The Cloud Computing Risk Intelligence Map™ provides a unique view on the pervasive, evolving, and interconnected nature of incremental risks associated with cloud computing that executives and managers may find useful in identifying risks that apply to their organizations.

Businesses thrive by taking risks, but falter when risk is managed ineffectively. A Risk Intelligent Enterprise™ recognizes this dual nature of risk and devotes sufficient resources both to risk taking for reward and to the protection of existing assets.

The Risk Intelligence Map is intended to serve as a guide on the journey toward Risk Intelligence by helping personnel in

all functions of an organization broaden their perspective on risk and improve their ability to execute their risk-related responsibilities.

This may be accomplished by using the Risk Intelligence Map to:

- spur discussions about risk management topics, including risk identification, prioritization, measurement, and mitigation
- acilitate the connection of risk management silos
- identify redundant efforts in place to manage risk
- improve efficiency in compliance and risk management efforts
- develop risk event scenarios that require integrated responses The Risk Intelligence Map is not a definitive or comprehensive representation of risks that may be encountered by an organization.

Consider customizing the Risk Intelligence Map based on risks that impact your organization. Areas could include regulatory, geographic, industry, and company-specific issues. For more information on customizing the Risk Intelligence Map to meet the needs of your organization, please contact your Deloitte practitioner.

### 6. Business Resiliency 9. Business 8. Vendor Management 7. IT Operations and Availability Operations Technology Vendor Selection Asset Change Contracting Human Resources Resiliency Management Management • Failure to comply with Cloud service failure • Inadequate cloud mi-• Inadequate due dili-• Inability to customize • Malicious insiders with software licenses due to due to oversubscription administrative access to gration planning gence of cloud security cloud contract and establish cloud provider ease of cloud resource controls cloud components in peak usage periods · Inability to align busiliability provisioning • Inability to verify cloud Lack of sufficient Inadequate IT skills to ness process changes number of viable cloud infrastructure resiliency Insufficient tracking of with standardized cloud • Failure to update cloud manage cloud-based contract over time to revirtual assets providers technologies service options • Single-points-of-failflect operating changes Lack of coordination of • Lack of performance ure due to addition of Failure to retain techtrack record due to nical specialists upon complex technology system maintenance Project components resulting in conflicting cloud service immatucloud migration to over Management Resource changes and difficult see cloud operations rity Provisioning Increased complexity Poorly defined roles troubleshooting of data replication or and responsibilities of · Failure to formally debackup to other clouds Monitoring fine maximum available cloud participants Legal or back in-house Operations cloud resources • Unresponsiveness in cloud provider com-• Lack of performance Inadequate records **Cloud Provider** munications due to Inadequate monitoring monitoring mechanisms management, preser Continuity customer volume of cloud resource utilibeyond cloud provider vation, retention, and zation reports disposal policies Inability to test cloud • Inability to use third • Failure to consider continuity and disaster IT operational pro-Incident digital evidence and recovery plans cesses not updated to parties to assess cloud Management reflect unique cloud provider performance ediscovery issues in • Lack of continuity plan • Delayed data breach computing risks contracts • Gap between provider's for cloud provider notification due to failure, acquisition, Lower availability of nonperformance vs. Unauthorized exposure complex identification or change in service cloud service than business impact of of data at cloud locaof affected customers prescribed by the SLA service disruption tions with unpredictable strategy Ineffective incident due to provider overlegal environment Failure to establish investigation due to imsubscription source code escrow permanence of virtual Vendor Lock-in Inability to provide adagreement for proprie-Finance systems equate level of service tary software Failure to limit incident • High cost of migrating globally Lack of internal controls spill-over to other cloud cloud-resident technol-**Supply Chain** for financial processes tenants ogy due to proprietary Physical and Continuity architecture and transactions in the Inability to troubleshoot

• Interruption of cloud services due to critical subcontractor failure

# Environmental

performance issues due

to continuous environ-

ment changes

- Inadequate physical and environmental safeguards for cloud locations
- Increased data loss for multiple customers from physical machine theft
- Complexity in architecting technical solutions that minimize vendor lock-in
- Failure to plan for cloud portability and interoperability
- Lack of agreed upon exit obligations for both provider and customer

- cloud
- Failure to control cloud expenses due to ease of proliferation of cloud usage
- Economic denial-ofservice by exhausting metered cloud resources

# Тах

• Failure to analyze and plan for tax considerations