Auditing Software as a Service (SaaS): Balancing Security with Performance
Goals for Today

- Defining SaaS (Software as a Service) and its importance
- Identify your company's process for managing SaaS solutions and evaluate the selection methodology
- Assess the process to analyze the security of SaaS solutions
- Review the contract management process for SaaS providers
- Evaluate the process for managing logical access to the SaaS solutions
- Measure the effectiveness of SaaS tools to monitor performance
What is Software-as-a-Service (SaaS)?

- Software deployment via the Internet “Web Software”
- “On-demand” Service Model
- Per-user pricing (pay-as-you-go) or flat monthly fee
- Very little customization (Multi-tenant)

*All trademarks, service marks, images, products, and brands remain the sole property of their respective holders.*
Growth of SaaS Providers

*All trademarks, service marks, images, products, and brands remain the sole property of their respective holders.
Growth of SaaS

Public Cloud Services Market by Segment, 2010-2016

Billions of Dollars

250

200

150

100

50

0


Cloud Management and Security Services
Cloud System Infrastructure Services (IaaS)
Cloud Application Infrastructure Services (PaaS)
Cloud Application Services (SaaS)
Cloud Business Process Services (BPaaS)
Cloud Advertising

“Companies are saving up to 90% in time and expenses compared to traditional on-premises software solutions.” – Salesforce.com

“While SaaS can typically be the best financial bet, there could be reasons not to use it. ROI goes away quickly if you’re busted for some violation of the law by placing data somewhere it should not be.” – Forbes

“Now that computing power has become dirt cheap and Internet usage ubiquitous, software developers are racing to put cutting-edge business apps into the hands of small firms in ways that could give a lift to the economic recovery.” – USA Today

“A risk of SaaS is that your data is on someone else’s servers.” – IT World

“SaaS is becoming a key word in the IT world.” – OPRO Japan Co., Ltd.

“SaaS is one of the fastest growing segments in the IT sector.” – Gartner and Forrester
Benefits of SaaS

- Scalability
- Reduction of Acquisition Costs
- Simple Deployment
- Global Accessibility
- Easy Administration
- Compatibility
Risks related to SaaS

• Security
• Operational Reliability
• Professional & Business Competence
• Vendor Viability
• Legal
• Compliance
**SaaS Benefits**

• Groupon’s use of SaaS provider Zendesk
  – Explosive growth created the need for a robust ticketing solution

• Benefits Received
  – Online support solution provided scalability
  – Flexible solution delivered value
  – Groupon service agents can easily tweak the system without calling a consultant

*All trademarks, service marks, images, products, and brands remain the sole property of their respective holders.*
Audit Approach

• What SaaS tools are in use at your company?
  – How are they managed (centralized, decentralized)
  – Who are the primary users?

• Is the process for engaging SaaS providers standardized or informal?
  – Identification
  – Evaluation
  – On-boarding
Audit Approach cont.

- Obtain a population of SaaS tools in use

- Test for Completeness
  - Speak with employees
  - Review credit card and A/P payments
  - Legal Department

- Test for Accuracy
  - Verify listed items meet definition of SaaS

Get comfortable with the population!
Evaluation of the Selection Process

- Is the process defined and established?
  - If not, how are the risks mitigated?
- Business case evaluation
- Vendor scorecard
- Security assessment
- Review of contract terms
- System integration and evaluation by IT
- Final vendor approval
Security Assessment

• Why is an assessment important?
  – Ensure compliance with regulatory requirements
  – Identify possible security vulnerabilities
  – Ensure compliance with corporate security policies
Security Assessment cont.

• If a formal assessment was performed...
  – Were the issues properly communicated?
  – Was the assessment signed off by someone with the appropriate authority?
  – Was the residual risk acceptable?
Security Assessment cont.

• If a formal assessment was NOT performed…
  – Are security policies documented?
  – Are SLAs (Service Level Agreements) documented?
  – Does a disaster recovery policy exist?
  – What are the data encryption / storage requirements?
  – Does the tool support your password requirements?
  – Does the vendor have any 3rd party assessments?
• ISO 27001
• SSAE 16 (SOC 1, 2, or 3)
Evaluation of Contract Terms

• Importance of contract terms
  – Reduce liability risks
  – Ensure performance

• Approval process
  – Review legal and business terms
  – Approval by appropriate parties
  – Execution prior to use of services
  – Periodic review and update
Evaluation of Contract Terms cont.

• Contract testing considerations
  – Service Level Agreements (SLAs)
  – Right-to-audit clauses
  – Renewal and termination clauses
  – Relevant governing laws for multi-national agreements
  – Notice of material adverse impacts
  – Record retention / ownership of data or source code
Access Management

• Why is this important?
  – Data integrity
  – Loss of data
  – Confidentiality
Access Management - Important Questions

• Who is able to authorize access?
• Who is responsible for managing employee access?
• Is Single Sign-on or Same Sign-on utilized?
• Are periodic access reviews performed?
Performance Monitoring

• How does monitoring add value?
  – Ensures compliance with the contract
  – Timely identification allows for mitigation
  – Reduction of operating expenses
  – Reduction of legal liability expenses
Performance Monitoring cont.

• Evaluate the monitoring process
  – Who is responsible for monitoring activities?
  – What metrics are tracked?
  – How are SLA terms tracked?
  – What is the process for following-up on SLA breaches?
  – Is billing monitored for accuracy?
  – How are results communicated?
Final Thoughts

- Identify your company’s appetite for SaaS solutions.
- Formal or informal, a security evaluation is an essential part of the SaaS selection process.
- Proper contract terms are vital to supporting the successful utilization of SaaS tools.
- Robust access management processes will help support a secure environment.
- Monitoring performance is important to ensure your company can meet their goals and objectives.
Final Thoughts cont.

• Risks do exist but the value that SaaS solutions can provide is too great to ignore.

• Internal Audit can assist Management in identifying the right controls and processes needed to allow them to realize the value that SaaS tools can bring.
Q & A

Remi Nel
Global IT Audit Manager
Rackspace
remi.nel@rackspace.com