21 Point Checklist for SELECTING AN ENTERPRISE-READY CLOUD SERVICE

skyhigh

Introduction

The journey to the cloud is well underway, and it's easy to see why when 84% of CIOs report cutting application costs by moving to the cloud.[1] But if your company does not manage its journey to the cloud deliberately by selecting the lowest-risk cloud services, it could be putting its data at risk. In fact, 2013 saw a 38% annual increase in incidents of loss, theft, and exposure of personally identifiable information (PII) in the cloud. In order to reap the benefits of the cloud while minimizing risk, organizations must employ a methodology to identify and select enterprise-ready services.

Some services, such as Salesforce and Office 365, are extensively vetted during a formal procurement process. However, the average company now uses 626 different cloud services[2] and many of these services are free or low-cost services employees find and purchase on their own like Dropbox and Evernote, which haven't been vetted by IT.

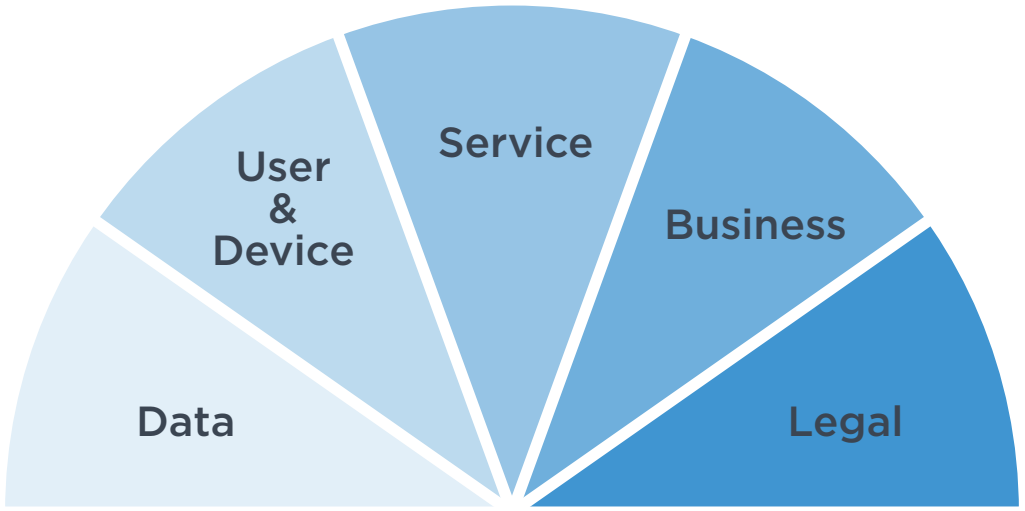
> "Ralph Loura, the CIO of Clorox, riffing off the antagonistic concept of 'shadow IT', has implemented an approach he calls 'Shallow IT.' This allows for the wide testing and nurturing of consumer-grade and adopted solutions in the enterprise, done in a calculated but flexible way, proving out all new enterprise apps to help power the $5.5B company."
>
> Harvard Business Review

[1] Enterprise CIO forum
[2] Skyhigh Cloud Adoption and Risk Report Q1 2014

The good news is that the risk of every cloud service can be measured by performing an audit of the cloud provider. To do this, IT and security teams need a standardized way to assess these services. Based on the Cloud Security Alliance (CSA) Cloud Controls Matrix, there are five categories of attributes to evaluate: data, user and device, service, business, and legal risk. This checklist summarizes those recommendations and offers a standardized way to identify enterprise-ready cloud services. By following this checklist you'll be able to enable utilization of the cloud for your organization while also mitigating risk.

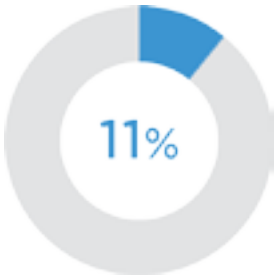
626 **The number of different cloud services used by the average organization**

Cloud Evaluation Criteria



Data Attributes

There are several aspects of how cloud providers manage data that can bolster security and reduce the exposure of your data to security breaches. Encryption is one of the most effective steps to reduce the risk of third parties gaining access to your information, whether via a security breach in which the cloud provider is compromised or if the cloud provider is served with a subpoena and gag order by a government. Security teams should also look for cloud providers that maintain strict separation of data between tenants who use the service. Finally, data retention is a requirement that can be seen both ways: you may need to ensure data is retained for a minimum amount of time to meet regulatory requirements, but if you decide to discontinue using the service you want your data deleted by the provider in a timely way.



Cloud providers encrypt data at rest

Enterprise-Ready Checklist:

- [ ] **1. ENCRYPTION IN TRANSIT**
  Data is encrypted in transit using SSL/TLS protocol to reduce the risk of a third party intercepting data as it moves to and from the cloud.

- [ ] **2. ENCRYPTION AT REST**
  Data stored using strong AES 256-bit encryption. Ideally, you can maintain control of encryption keys so that even cloud provider cannot decrypt your data.

- [ ] **3. DATA MULTI-TENANCY**
  Data for one tenant is separated from other tenants.

- [ ] **4. DATA RETENTION ON TERMINATION**
  The terms and conditions specify an acceptable amount of time data is retained by the service after you terminate your account.

Enterprise-Ready Checklist:

- [ ] **5. ANONYMOUS USE POLICY**
  The service only permits usage by authenticated users with valid accounts, not anonymous users who don't have an account.

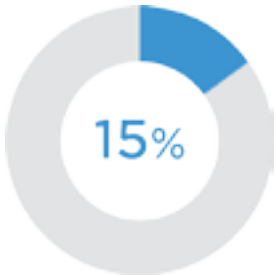
- [ ] **6. IDENTITY FEDERATION METHOD**
  Supports one or both of these common authentication methods for identity federation: SAML and OAUTH.

- [ ] **7. MULTI-FACTOR AUTHENTICATION**
  In addition to a username and password, the service supports additional authentication factors such as a smart phone token or biometric characteristic.

- [ ] **8. DEVICE ACCESS CONTROL**
  Supports the ability to control access to the service based on approved device operating systems or registered devices, limiting exposure to unsecure devices.

User and Device Attributes

Another important step to securing data in the cloud is ensuring that the proper controls are in place for authorized users to access the data. Encrypting data stored in the cloud doesn't mean much if one of your users' accounts can be compromised and the company's data stolen by a third party. Enterprise-ready cloud services provide a range of options to securely authenticate users including federating with identity management solutions via standards-based protocols. They also support multi-factor authentication using a hardware token or mobile app. Finally, security teams should look for services that provide the ability to control access to approved devices, either by device OS or version or to devices registered with an mobile device management (MDM) solution such as AirWatch or MobileIron.



Cloud providers offer multi-factor authentication

Service Attributes

One crucial area to consider is whether a cloud provider performs testing to measure how hardened its service is against attacks. Cloud providers that perform regular testing across Cloud Security Alliance (CSA) and Open Web Application Security Project (OWASP) recommendations generally have more robust security controls in place. Of course, you should also look at whether the service has been compromised, specifically if it's been compromised within the last 12 months. Even the most secure provider can be compromised, so look for ones that give you tools to identify a potential problem. Audit logging not only can allow you to detect anomalous usage activity early, these logs can also support a forensic investigation should data be compromised.

165 The number of cloud services that publicly disclosed a security breach in 2013

Enterprise-Ready Checklist:

- [ ] **9. PENETRATION TESTING**
  Service performs regular penetration testing according to guidance from CSA and OWASP recommendations.
- [ ] **10. NOT COMPROMISED IN LAST TWELVE MONTHS**
  The service has not experienced a security breach in the last 12 months, across all production tenants.
- [ ] **11. IP FILTERING**
  Service supports filtering access to IP ranges associated with your company's Internet providers.
- [ ] **12. AUDIT TRAILS**
  All actions including logins, uploads, downloads, and views are tracked in a full audit trail to identify suspicious activity indicative of a security breach.

Enterprise-Ready Checklist:

- [ ] **13. DATACENTER HOSTING LOCATIONS**
  The cloud provider's datacenter locations are in alignment with your data privacy obligations, or offer options to restrict data movement to meet obligations.

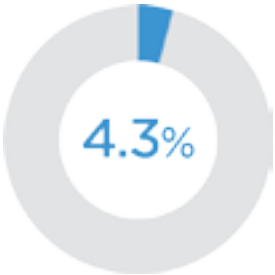
- [ ] **14. THIRD-PARTY CERTIFICATIONS**
  Cloud provider has gone through rigorous third-party certifications including ISO 27001 and SAS 70 certifications.

- [ ] **15. BUSINESS CONTINUITY PLAN**
  A business continuity plan has been created, is accessible to customers, and includes detailed recovery procedures and manual workarounds in the event of a disaster.

- [ ] **16. AUDITS PERFORMED AT LEAST ANNUALLY**
  Third-party assessments ensure the organization follows its policies and meets statutory and regulatory requirements.

Business Attributes

The physical infrastructure and business practices your cloud provider uses to deliver a service can have a significant impact on your company. When cloud providers host data in other countries, cross-border data privacy laws can come into effect. Your provider's datacenters are also important when you consider how a natural disaster or even a power disruption can impact your business critical operations or even lead to data loss. Security and audit teams should look for providers with robust failover procedures and disaster recovery plans. Certifications and audits are important signals of enterprise-readiness as they show that providers have invested in controls to protect their customers' data, but they should not be viewed as the only steps needed to ensure the security of your data in the cloud.



Cloud providers are ISO 27001 certified

Legal Attributes

Most companies find it preferable to audit the legal risks of a cloud provider before they adopt it than deal with legal headaches after a security incident. The first thing to look for is the legal jurisdiction where any dispute would be resolved, and whether the terms of use or contract include provisions for alternate settlement methods like arbitration which limit your legal options. In the event of a breach, you may want the ability to participate in a forensic investigation with the cloud provider. Companies should look for providers that work cooperatively with clients to investigate anomalous activities and close any holes. Finally, to prepare for the worst, ensure your cloud provider maintains chain of custody and preservation of evidence to facilitate legal discovery (e-discovery) as part of a lawsuit.

Enterprise-Ready Checklist:

- [ ] **17. JURISDICTIONAL LOCATION**
  The cloud provider is located in a favorable jurisdictional location in the event of any legal dispute with the provider.

- [ ] **18. DISPUTE RESOLUTION**
  Terms of service or contracts do not contain clauses that limit legal remedies such as arbitration or other alternate settlement methods.

- [ ] **19. PROHIBITED FROM 3RD PARTY DISCLOSURE**
  The cloud provider does not share data in response to subpoena without notifying the tenant their data has been shared.

- [ ] **20. COPYRIGHT CONTROLS**
  Service meets requirements governing intellectual property including the Digital Millennium Copyright Act (DMCA).

- [ ] **21. IP OWNERSHIP**
  The terms and conditions explicitly state that all information uploaded to the service is owned by the customer, not the CSP.