Best Practice Checklist Series - Issue 20

Cloud Solution Vetting, Testing, Implementation and Use

Understanding the basics: A layperson's guide and checklist for overseeing IT.



Best Practice Checklist Series
An exclusive publication of Sandbox Technologies, Inc.

3868 W Carson St, Suite 316
Torrance, CA 90503
Tel. (424) 207-5130
www.sandboxtech.com

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

Cloud Solution Vetting, Testing, Implementation and Use

Cloud computing and Software as a Service (SaaS) have become the default rather than the exception for organizations of every size. The appeal is genuine and well founded: a subscription to a hosted application generally removes the burden of purchasing servers, patching operating systems, and maintaining a data center; it converts a large capital expense into a predictable operating expense; and it offers elasticity, allowing capacity to expand or contract as the business requires. A capable Cloud solution can be provisioned in days rather than months, can be reached from any location with an Internet connection, and can shift the labor of infrastructure maintenance to a specialized provider whose entire business is the reliable operation of that platform. These are substantial and legitimate advantages, and they explain why so much of modern business now runs on services the organization does not itself own or host.

Precisely because adoption is so easy, the discipline surrounding it is often thin. A service that can be signed up for with a corporate credit card in a matter of minutes rarely receives the scrutiny that a comparable on-premises system would have attracted, yet the organization's data, and frequently its regulatory obligations, travel to that service all the same. The convenience that makes Cloud solutions attractive is the same convenience that allows important questions to go unasked: Who owns the data once it resides on the vendor's systems? How is it protected, and by whom? What happens if the relationship ends, if the vendor is acquired, or if the vendor ceases to operate? What is actually promised, and what remedy exists when a promise is not kept?

A recurring source of misplaced confidence deserves particular attention. Many vendors present independent assurance, such as System and Organization Controls (SOC 2) reports or International Organization for Standardization (ISO) 27001 certification, as though they settle the matter of security. These assurance materials are useful; their absence alone does not prove insecurity. They address the design and, in some cases, the operating effectiveness of controls at a specified date or over a period and within a defined scope. SOC 2 is an attestation, not a certification. They do not establish that a given solution is appropriate for a particular organization's environment, data sensitivity, or regulatory posture, and they do not transfer responsibility away from the customer. Reliance on any vendor is, at bottom, a good-faith trust in that vendor's representations, and prudent governance treats it as such.

The purpose of this issue is to serve as a layperson's primer and checklist for overseeing the full lifecycle of a Cloud or SaaS solution: vetting and vendor due diligence; testing and pilot evaluation before commitment; implementation and phased migration; integration, identity, and data protection; ongoing

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

use and governance; and the pervasive problem of unsanctioned Cloud adoption commonly termed shadow IT. It is written so that a non-technical manager or executive can engage substantively with IT personnel, ask the right questions, and understand the answers well enough to weigh them. It is not a substitute for technical implementation, and it is deliberately vendor-neutral.

As with each publication in this series, the material that follows is intended to inform and to structure a conversation, not to dictate an outcome. The selection of a Cloud solution is a business decision that belongs to the client, informed by facts, variables, risks, and costs particular to the organization. Consideration should be given to reviewing any significant Cloud adoption with the Consulting CIO before commitments are made, so that the diligence described here is applied deliberately rather than reconstructed after difficulties arise.

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

Contents

Key Concepts 5

Scenarios 7

Areas to Discuss 9

Recommended Implementation Practices 11

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

Key Concepts

Software as a Service (SaaS). A delivery model in which an application is hosted and operated by a vendor and made available to customers over the Internet, generally on a subscription basis. The customer typically accesses the software through a browser or a lightweight client and does not install, host, or maintain the underlying servers, storage, or application code. The convenience is substantial, but the customer's data and configuration reside on infrastructure the customer does not control, which is the origin of most of the diligence discussed in this document.

Shared Responsibility Model. The principle, common to essentially all Cloud services, that security and operational duties are divided between the provider and the customer, and that the division varies by service. The provider is generally responsible for the security of the platform itself, such as its physical facilities, its infrastructure, and the availability of the service. The customer typically remains responsible for their own data, for who is granted access, for how the service is configured, and often for the retention and recoverability of that data. Misunderstanding where the line falls is one of the most common and most consequential errors in Cloud adoption.

Service Level Agreement (SLA). The contractual commitment describing the level of service the vendor undertakes to provide, most often expressed as a percentage of uptime or availability over a period, together with the remedy available if the commitment is not met. It is important to distinguish the promised service level from the remedy: the remedy is frequently limited to a service credit proportional to fees paid, which may bear little relationship to the loss the business actually sustains during an outage.

Data Residency. The physical or geographic location in which data is stored and processed. Residency can carry significant legal and regulatory weight, as certain data is subject to requirements governing where it may be held or across which borders it may be transferred. A vendor's default storage location, and its use of facilities in multiple jurisdictions, should be understood before regulated or sensitive data is entrusted to the service.

Data Portability and Exit. The degree to which an organization can retrieve its data from a service, in a usable and complete form, and migrate it elsewhere if the relationship ends. Portability depends on the availability of export mechanisms, the formats in which data is returned, the inclusion of associated metadata and history, and the terms governing data return and deletion upon termination. A service that is straightforward to enter but difficult to exit constrains the organization's future options.

Single Sign-On (SSO). A capability that allows users to authenticate once through a central identity provider and then access multiple applications without separate credentials for each. Properly implemented, Single Sign-On is intended to strengthen security and simplify administration by centralizing account management, enforcing consistent authentication policy, and enabling prompt removal of access when an individual leaves the organization.

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

Subprocessor. A third party engaged by the vendor to help deliver the service, which may itself store or process the customer's data. A SaaS provider commonly relies on other Cloud providers for hosting, on additional services for functions such as email delivery or analytics, and on support contractors. Each subprocessor represents an extension of the trust the customer places in the primary vendor, and the customer's data is only as protected as the weakest link in that chain.

Vendor Lock-In. The condition in which the cost, difficulty, or risk of moving away from a vendor becomes high enough to constrain the organization's freedom of action. Lock-in can arise from proprietary data formats, from deep integration into business processes, from accumulated history that cannot be exported, or from pricing structures that penalize departure. Its practical effect is to reduce the organization's leverage over time, including at renewal.

Shadow IT. The use of Cloud services, applications, or accounts by employees or departments without the knowledge, review, or sanction of the organization's IT function. Shadow IT is rarely malicious; it typically reflects a genuine attempt to solve a problem quickly. It is nonetheless hazardous, because data placed in unvetted services escapes the organization's security controls, governance, and visibility, often including data subject to regulatory protection.

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

Scenarios

The following scenarios are hypothetical and are provided to illustrate, in general terms, how choices in this area can affect business outcomes. No judgment is offered regarding what caveats are or are not acceptable; the objective is to inform, so that decisions may be made deliberately.

Adoption Without an Exit Path. *An organization selects a specialized operational platform under time pressure, drawn by an attractive introductory price and a rapid onboarding process. Over two years the platform accumulates the organization's records, workflows, and institutional history. When service quality declines and fees rise sharply at renewal, the organization investigates alternatives and discovers that the platform offers only a limited export, returning data in a proprietary format that omits much of the history and structure on which daily operations now depend. The practical cost of leaving, in reconstruction, retraining, and disruption, exceeds the increased fees, and the organization renews on unfavorable terms. The difficulty was not the original selection but the absence of any evaluation of portability and exit before the platform became indispensable.*

The Backup That Was Never There. *A department migrates its core documents and correspondence to a widely used Cloud productivity suite and reasonably assumes that so large and capable a provider must be backing up the data. Some months later an account is compromised, and an attacker deletes a substantial volume of files; in a separate incident, an employee empties folders in error and the deletions are not noticed until the provider's short retention window has lapsed. On inquiry, the organization learns that the provider's responsibility, consistent with the shared responsibility model, extended to the availability and integrity of the platform, not to protecting the customer against the customer's own deletions or against the consequences of a compromised account, and that a separate backup was the customer's responsibility all along. The data is not recoverable.*

Regulated Data in an Unsanctioned Service. *A team, frustrated by a slow internal process, adopts a convenient Cloud application on its own initiative to manage its work, signing up with a corporate card and inviting colleagues. Over time the application comes to hold information subject to regulatory protection. IT is unaware the service exists, so it is excluded from the organization's access controls, monitoring, and backup, and no agreement governing the handling of regulated data is ever put in place with the vendor. When a security questionnaire or an audit later requires the organization to enumerate every system holding protected data, the service surfaces as an unmanaged and undocumented exposure, and the organization must account for a period during which regulated data resided outside its governance entirely.*

A Token Credit Against a Real Loss. *An organization relies on a Cloud service for a revenue-generating function and is assured of high availability, described in marketing materials as effectively guaranteed. The service suffers a multi-hour outage during a critical period, and the business sustains a significant loss in revenue and reputation. On reviewing the contract, the organization finds that the Service Level Agreement's sole remedy is a service credit calculated as a small percentage of the monthly fee, that the*

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

credit must be claimed within a narrow window through a defined process, and that the agreement expressly excludes liability for consequential or business losses. The remedy is honored precisely as written, and it is trivial in relation to the harm. The gap was visible in the contract before signing.

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

Areas to Discuss

The following are aspects that should be discussed and addressed with your organization’s IT professional(s). Some points may or may not be applicable depending on the environment.

Vendor Security Posture and the Limits of Certification

The starting point of diligence is the vendor's own security posture, evidenced by independent attestations and by direct inquiry. It should be understood, however, that a certification describes the vendor's controls within a defined scope and period; it does not certify that the solution suits the organization's specific environment, and it does not relieve the customer of responsibility. Marketing language such as bank-grade security or fully compliant carries no defined meaning and should be treated as a claim to be substantiated, not as a finding.

- Request the current SOC 2 report or ISO 27001 certificate, and confirm what is actually within its scope and how recent it is.
- Distinguish a report describing control design from one that also tests operating effectiveness over time.
- Ask how vulnerabilities are identified and remediated, and how customers are notified of relevant issues.

Data Ownership, Residency, and Regulatory Fit

Contracts should be examined to confirm that the organization retains ownership of its data and that the vendor's rights to use that data are appropriately limited. Where data is subject to regulatory obligations, its storage location and cross-border movement, and the availability of any required contractual terms, should be established before adoption rather than assumed.

- Confirm in writing that the customer owns its data and that vendor use is limited to delivering the service.
- Establish where data is stored and processed, including any secondary or backup locations.
- Determine whether the vendor will execute the data-handling terms the organization's regulatory posture requires.

Portability, Exit, and Continuity

Before entry, attention should be given to exit. The organization should understand how it would retrieve its data in a complete and usable form, how the vendor handles data return and deletion at termination, and what would occur if the vendor were acquired, discontinued the product, or ceased operations.

- Identify the available export mechanisms and the formats and completeness of exported data.
- Review the terms governing data return and certified deletion upon termination.
- Consider the continuity risk posed by the vendor's financial condition and ownership.

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

Subprocessors and the Extended Trust Chain

A vendor's assurances extend only as far as the parties it in turn relies upon. The organization should understand which subprocessors handle its data, how the vendor holds them to comparable standards, and how the organization is apprised of changes to that roster.

- Obtain the current list of subprocessors and the functions they perform.
- Confirm how the vendor imposes equivalent obligations on its subprocessors.
- Establish whether and how customers are notified before subprocessors change.

Breach Notification and Incident Handling

The value of a vendor's security depends in part on how it behaves when something goes wrong. The contract should specify a timely and defined breach-notification obligation, and the organization should understand the support it can expect during an incident.

- Establish the timeframe and method for breach notification and what information will be provided.
- Understand the vendor's incident-response commitments and available support during an event.
- Confirm that notification obligations align with the organization's own regulatory reporting duties.

Service Levels and Real Remedies

An availability commitment should be read together with its remedy and its exclusions. Consideration should be given to the difference between the service level promised and the compensation available if it is missed, and to whether that compensation bears any relationship to the loss the business would sustain.

- Identify the committed availability figure, how it is measured, and what is excluded from measurement.
- Read the remedy: whether it is limited to service credits, how it is calculated, and how it must be claimed.
- Note any exclusion of consequential or business losses, and weigh it against the criticality of the function.

Financial Viability and Total Cost

A solution is only as durable as the vendor behind it, and only as affordable as its full cost over time. Consideration should be given to the vendor's stability and to the complete cost of ownership, including growth, add-on modules, integration, and the cost of eventual exit.

- Assess indicators of the vendor's financial stability and longevity.
- Model total cost over the expected term, including likely growth and renewal increases.
- Account for implementation, integration, training, and exit costs, not the subscription fee alone.

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

Recommended Implementation Practices

Define the Requirement Before the Product

Has the organization documented the problem to be solved, the data involved, and the regulatory and integration requirements before evaluating any specific vendor? Selecting a product before defining the need generally leads to solutions chosen for their marketing rather than their fit.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

Conduct Documented Vendor Due Diligence

Has a consistent set of security, contractual, and viability questions been put to the vendor, and have the answers been recorded? Diligence that is not documented is difficult to compare across vendors and difficult to revisit later, and it should be treated as a standard step rather than an occasional one.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

Verify Certifications Rather Than Accept Claims

Have independent attestations been requested and their scope, recency, and relevance actually reviewed, rather than accepted as marketing statements? A certificate is a starting point for inquiry, not a conclusion, and the task of ensuring security does not end where the certificate begins.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

Establish Data Ownership, Residency, and Regulatory Fit

Has it been confirmed in writing that the organization owns its data, that the vendor's use is limited, and that storage locations and available terms satisfy applicable regulatory obligations? These points are far easier to secure before signing than to renegotiate afterward.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

Map the Shared Responsibility Model in Writing

Has the division of responsibility between vendor and customer been made explicit, particularly for data protection, access, and configuration? Where the customer's responsibilities fall should be understood before adoption, so that no critical duty is left to an assumption.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

Arrange Independent Backup Where the Customer Bears the Risk

Has it been determined whether the vendor's retention constitutes a true backup, and, where it does not, has independent backup of the organization's data been arranged? Assuming that a large provider backs up customer data against the customer's own errors or a compromised account is a common and costly mistake.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

Pilot Before Committing

Has the solution been evaluated through a structured pilot with representative data and users before a full commitment is made? A limited, time-boxed evaluation is intended to surface fit, performance, and integration issues while the organization retains the freedom to choose otherwise.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

Plan a Phased Implementation and Migration

Has migration been planned in defined phases, with validation of data integrity and a documented ability to revert, rather than executed as a single irreversible cutover? A phased approach helps to reduce the likelihood that a problem discovered late affects the entire organization at once.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

Enforce Single Sign-On and Multifactor Authentication

Has the service been integrated with the organization's central identity provider, and is Multifactor Authentication (MFA) required for access? Centralized identity and strong authentication are intended to strengthen security and to ensure that access can be granted and, importantly, promptly revoked.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

Configure Access on the Principle of Least Privilege

Have permissions been set so that individuals hold only the access their roles require, and is there a process to remove access when roles change or personnel depart? Default configurations are frequently more permissive than necessary and warrant deliberate review.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

Confirm Breach Notification and Incident Terms

Does the agreement obligate the vendor to notify the organization of a breach within a defined and timely period, and does that obligation align with the organization's own reporting duties? The organization's ability to respond depends on being informed promptly and completely.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

Read the SLA for Its Remedy, Not Only Its Promise

Has the availability commitment been evaluated together with its actual remedy and its exclusions, and weighed against the business impact of an outage? A commitment whose only remedy is a token credit should be understood as such before reliance is placed upon the service.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

Manage Licenses, Costs, and Usage on an Ongoing Basis

Is there a process to review active licenses, actual usage, and cost against value on a periodic basis? Unmonitored subscriptions tend to accumulate unused seats, redundant tools, and unnoticed price increases over time.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

Detect and Govern Shadow IT

Are there measures to identify unsanctioned Cloud services in use across the organization, and a practical, non-punitive path for bringing legitimate needs into the sanctioned process? Addressing the underlying demand helps to reduce the likelihood that employees place organizational data, including regulated data, into unvetted services.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

Re-Review Adopted Solutions Periodically

Are adopted Cloud solutions reassessed at defined intervals and at renewal for continued security, fit, cost, and vendor viability? A solution appropriate at adoption may cease to be so as the organization, the vendor, and the regulatory landscape change, and periodic re-review is intended to catch such drift before it becomes a liability.

NOTES

STATUS ☐ In place ☐ Not in place / N/A ☐ To be discussed

© 2026, All Rights Reserved. Sandbox Technologies, Inc.

The variables, risks, and potential outcomes above are presented so that the business decision may remain where it properly belongs, with the client. Should you wish to review your current environment or discuss any item in this checklist, it is recommended that you consult your **Sandbox Technologies Engineer, Consulting CIO, or Account Manager**.

Not a client yet? Contact Sandbox Technologies to get started.

This document is protected by US and International copyright laws. Reproduction or distribution of this document for commercial advantage and without written permission from Sandbox Technologies, Inc. is strictly prohibited. Any distribution must retain attributions and this notice. © 2026, All Rights Reserved. Sandbox Technologies, Inc.