Best Practice Checklist Series - Issue 14

Compliance

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®

Compliance

Compliance has evolved from a specialized concern of regulated industries into a broad operational reality for organizations of nearly every size and sector. Contractual obligations, industry mandates, statutory privacy requirements, and the tightening conditions attached to cyber-insurance policies increasingly converge on a single expectation: that an organization can demonstrate, with evidence, that it manages information and systems in a disciplined and defensible manner. The stakes are concrete. An organization that cannot substantiate its posture may forfeit contracts, face regulatory exposure, encounter difficulty procuring or renewing insurance, or find a claim contested at the moment it is most needed.

It is essential at the outset to distinguish compliance readiness from certification, because the two are frequently conflated to an organization's detriment. Readiness refers to the state of having implemented, documented, and operationalized the controls a given framework requires, together with the evidence necessary to substantiate them. Certification, attestation, or a formal audit is a separate act performed by an independent third party who examines that evidence and renders a judgment. Readiness is the work of building and maintaining a defensible posture; certification is an external verdict rendered upon it at a point in time.

Sandbox Technologies prepares organizations to be audit-ready and defensible. Assistance is provided in scoping the environment, inventorying data, mapping controls, identifying and remediating gaps, and assembling the documentation and evidence upon which an assessment depends. The firm does not itself perform the certification or the audit. That function is, by design and often by requirement, reserved to an independent assessor engaged separately, so that the party preparing the environment is not the party judging it. This separation is a feature of a credible compliance program, not a limitation of the engagement.

Mandatory legal and contractual obligations must be met; they are not optional business preferences. The client, with qualified legal counsel, should identify applicable duties and decide whether additional voluntary frameworks are worthwhile. Industry, customer and vendor contracts, insurance terms, and risk tolerance inform that assessment. This document supports an informed decision and does not replace legal advice.

The material that follows is intended to serve as a layperson's primer and a practical checklist, written so that a non-technical manager or executive can work alongside their internal or outsourced IT personnel and their counsel to assess the organization's compliance readiness. Consideration should be given to reviewing these items with a Consulting CIO, who can help translate framework requirements into a prioritized, evidence-driven plan of action suited to the organization's specific circumstances.

© 2026 Sandbox Technologies, Inc.

Contents

Key Concepts 4

Scenarios 6

Areas to Discuss 7

Recommended Implementation Practices 10

© 2026 Sandbox Technologies, Inc.

Key Concepts

Compliance Readiness. The state in which an organization has implemented, documented, and operationalized the controls a chosen framework requires, and has assembled the evidence needed to substantiate them, such that it is prepared to withstand an independent assessment. Readiness is an internal condition; it is achieved and maintained by the organization and its advisors.

Certification and Attestation. An independent party examines controls and evidence and issues a credential or opinion within a defined scope. A SOC 2 Type 1 report addresses a specified date; Type 2 also addresses operating effectiveness over a specified period. Neither guarantees future compliance. Sandbox prepares organizations for assessment but does not issue these certifications or reports.

Framework. A structured, published set of security and privacy requirements against which an organization's practices are measured. Frameworks differ in origin and force: some are contractual, some are statutory, and some are voluntary standards adopted to demonstrate diligence. Common examples include the Cybersecurity Maturity Model Certification (CMMC), National Institute of Standards and Technology (NIST) Special Publication 800-171, the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and System and Organization Controls (SOC 2).

Scope. The defined boundary of what a given framework applies to within an organization, encompassing the systems, networks, data, physical locations, personnel, and third parties that fall under its requirements. Accurate scoping is foundational; an overly broad scope inflates cost and effort, while an overly narrow scope leaves obligations unmet and the assessment vulnerable to challenge.

Control. A specific safeguard, whether technical, administrative, or physical, implemented to satisfy a requirement and to mitigate an identified risk. Examples include multifactor authentication, encryption of data at rest, documented access-review procedures, and retention of security logs. A control that is implemented but undocumented is generally difficult to defend.

Gap Assessment. A structured comparison of an organization's current practices against the requirements of a target framework, undertaken to identify where controls are absent, incomplete, or insufficiently evidenced. The gap assessment produces the prioritized remediation plan and is typically the pivotal early deliverable of a readiness engagement.

Evidence and Documentation. The tangible artifacts, including written policies, procedures, configurations, logs, records, screenshots, and attestations, that substantiate the existence and ongoing operation of a control. In an assessment, an unevidenced control is generally treated as an absent control. Documentation is therefore not administrative overhead; it is the currency of a defensible posture.

© 2026 Sandbox Technologies, Inc.

Data Inventory. A catalog of the data an organization creates, receives, stores, and transmits, classified by sensitivity and mapped to where it resides and who may access it. Because most frameworks and privacy laws attach obligations to specific categories of data, the inventory determines what must be protected and, in turn, what falls within scope.

Continuous Compliance. The ongoing discipline of maintaining controls, refreshing evidence, and adapting to changes in the environment, applicable requirements, and threats between assessments. An audit covers a defined date or period; ongoing review helps maintain a defensible posture after that assessment.

© 2026 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.

The Lost Defense Subcontract. *A manufacturing firm had for several years supplied a component to a larger prime contractor serving a federal agency. At renewal, the prime advised that continued participation would require the subcontractor to demonstrate readiness aligned to the Cybersecurity Maturity Model Certification (CMMC) and the underlying National Institute of Standards and Technology (NIST) Special Publication 800-171 controls, with an independent assessment to follow. The firm had not scoped its environment, inventoried its handling of controlled information, or documented its controls, and it could not achieve readiness within the window the prime allowed. The contract was awarded to a competitor that had prepared in advance. The loss was not attributable to the quality of the firm's product; it was attributable to an inability to demonstrate a defensible posture when the requirement arrived. Had readiness work begun earlier, the outcome may have differed, though no preparation could guarantee the assessment result.*

The Contested Insurance Claim. *A professional-services company carried a cyber-insurance policy and, following a ransomware incident, submitted a claim expecting coverage of its recovery costs and business interruption. During the claim review, the insurer examined the application and the control attestations the company had made at binding, which represented that multifactor authentication was enforced across all remote access and privileged accounts. Investigation indicated that a category of privileged accounts had been excluded from that control. The insurer asserted that the loss fell outside the coverage the company had represented it qualified for, and the claim was substantially disputed. The episode illustrates how insurer control requirements now function as a de facto compliance framework, and how the gap between an attestation and the operational reality can jeopardize recovery at the precise moment coverage is relied upon.*

The Multi-State Privacy Exposure. *A retailer operating primarily online gradually accumulated customers across numerous states without appreciating that several of those states had enacted consumer privacy laws imposing obligations regarding data collection, disclosure, consumer rights requests, and reasonable security. The company had no data inventory, no mechanism to honor deletion or access requests within statutory timeframes, and no documented security program. Following a consumer complaint and inquiry, the company incurred legal expense, remediation cost, and reputational harm disproportionate to its size. The exposure arose not from a deliberate decision to disregard the law, but from the absence of the scoping and inventory work that would have apprised leadership of which laws applied and what they required. Which of these obligations to address, and in what order, remained a business and legal decision for the company and its counsel; the readiness work would have equipped that decision with facts.*

© 2026 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.

Determining Applicable Frameworks and Mandates

Before any control work begins, it is necessary to establish which frameworks and legal mandates actually apply to the organization. This determination is driven by industry, by the specific data the organization handles, by the obligations embedded in customer and vendor contracts, and by applicable law. The decision of which frameworks to pursue is reserved to the client and should be made in consultation with counsel.

- Review customer and vendor contracts for flow-down security and compliance clauses.
- Identify applicable legal duties, such as HIPAA for covered entities and business associates handling protected health information, and contractual or industry duties, such as PCI DSS obligations for cardholder data.
- Consider whether a voluntary attestation such as System and Organization Controls (SOC 2) is expected by customers or advantageous in the market.
- Assess the reach of multi-state consumer privacy laws based on where customers and data subjects reside.

Scoping and Data Inventory

Accurate scope depends upon knowing what data exists, where it resides, how it flows, and who can access it. The data inventory is therefore the foundation upon which scope, and ultimately cost and effort, are determined. This exercise should be conducted with care, as errors here propagate through every subsequent stage.

- Catalog data by category and sensitivity, including regulated data types.
- Map where each category is created, stored, transmitted, and disposed of, including Cloud services and third-party processors.
- Document who and what has access, and by what means.
- Define the boundary of the environment subject to each applicable framework.

Control Mapping and Gap Assessment

Once scope is established, existing practices are compared against the requirements of each target framework to determine where controls exist, where they are incomplete, and where they are absent. The output is a prioritized understanding of the work required to reach readiness, expressed in terms the organization's leadership can weigh against cost, timeline, and risk.

- Map current technical, administrative, and physical controls to framework requirements.

© 2026 Sandbox Technologies, Inc.

- Identify deficiencies and classify them by severity and effort to remediate.
- Prioritize remediation in a manner informed by risk and by contractual or statutory deadlines.

Documentation and Evidence Collection

In an assessment, controls that cannot be evidenced are generally treated as if they do not exist. It is therefore necessary to develop and maintain the written policies, procedures, and operational records that substantiate the organization's posture. Documentation should reflect actual practice; a policy that describes conduct the organization does not follow can be more damaging than no policy at all.

- Develop and maintain written policies and procedures aligned to the framework.
- Collect operational evidence such as configurations, logs, records, and reviews.
- Establish a repository and a cadence for keeping evidence current and retrievable.

Cyber-Insurance Control Requirements

Insurers increasingly condition coverage, pricing, and claim payment upon the presence of specific controls, and the application and attestation process now functions as a de facto compliance framework in its own right. It is important that representations made to an insurer accurately reflect the operational reality, because a discrepancy discovered at claim time can imperil recovery.

- Reconcile every attestation on an insurance application against actual, evidenced practice.
- Give particular attention to commonly required controls such as multifactor authentication, endpoint protection, backup and recovery, and access management.
- Re-verify representations at each renewal, as requirements typically tighten over time.

Remediation

Where the gap assessment identifies deficiencies, a structured remediation effort closes them in a prioritized, documented manner. Remediation is intended to bring controls into conformity and to generate the evidence of that conformity; it is not complete until the corrected control is both operating and substantiated.

- Assign ownership, timelines, and success criteria to each remediation item.
- Validate that each remediated control operates as intended and is evidenced.
- Retain records of what was changed, when, and by whom.

Ongoing Maintenance of a Defensible Posture

A framework assessment reflects a single point in time. Environments change, personnel change, threats evolve, and frameworks are revised. Sustaining readiness requires an ongoing program of review, evidence

© 2026 Sandbox Technologies, Inc.

refresh, and adaptation, so that the organization remains defensible in the interval between assessments and prepared for the next.

- Establish a recurring schedule for control review and evidence refresh.
- Reassess scope and inventory when systems, vendors, or data flows change.
- Monitor for changes to applicable frameworks, mandates, and insurer requirements.

© 2026 Sandbox Technologies, Inc.

Recommended Implementation Practices

Confirm Applicable Obligations

Has the organization, in consultation with counsel, identified every framework, mandate, contractual clause, and privacy law that applies to it, and documented the basis for each determination? An accurate list of obligations is the prerequisite for all readiness work.

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

Distinguish Readiness from Certification

Does leadership understand that preparing a defensible posture and obtaining an independent certification are separate acts, and has an independent assessor been identified or contemplated for the certification when one is required?

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

Maintain a Current Data Inventory

Does the organization possess a current inventory of the data it creates, receives, stores, and transmits, classified by sensitivity and mapped to its locations, flows, and access? Compliance obligations attach to data, and the inventory is what makes them visible.

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

© 2026 Sandbox Technologies, Inc.

Define and Document Scope

Has the boundary of the environment subject to each applicable framework been deliberately defined and documented, rather than assumed? An undefined or inaccurate scope undermines the defensibility of any subsequent assessment.

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

Complete a Gap Assessment

Has a structured comparison of current practices against each target framework been performed, with deficiencies classified by severity and effort? A documented gap assessment converts a broad obligation into a concrete, prioritized plan.

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

Reconcile Cyber-Insurance Attestations

Do the control representations made on the organization's cyber-insurance application accurately reflect evidenced operational practice, and are they re-verified at each renewal? A discrepancy discovered at claim time can jeopardize coverage when it is most needed.

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

Implement Core Technical Controls

Are foundational controls, such as multifactor authentication across remote and privileged access, encryption of sensitive data, endpoint protection, and tested backups, implemented across the full scope without unmanaged exceptions?

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

© 2026 Sandbox Technologies, Inc.

Document Policies and Procedures

Does written documentation exist for the policies and procedures each framework requires, and does that documentation describe what the organization actually does rather than an aspiration? Documentation that diverges from practice is a liability in an assessment.

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

Collect and Organize Evidence

Is operational evidence, including configurations, logs, records, and reviews, being collected, retained, and organized in a manner that can be produced on request? Unevidenced controls are generally treated as absent controls.

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

Prioritize and Track Remediation

For each identified deficiency, has an owner, a timeline, and a success criterion been assigned, and is remediation tracked to closure with validation and records? Remediation is complete only when the corrected control operates and is substantiated.

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

Manage Third Parties and Vendors

Have vendors and service providers within scope been assessed for their own compliance, and are their obligations reflected in contracts and, where applicable, in business associate or data processing agreements? An organization's posture generally extends to the third parties that handle its data.

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

© 2026 Sandbox Technologies, Inc.

Establish a Continuous Compliance Cadence

Is there a recurring schedule for reviewing controls, refreshing evidence, and reassessing scope when the environment changes? A passed audit reflects a point in time; ongoing discipline is what helps to preserve a defensible posture between assessments.

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

Assign Accountability

Has clear internal ownership of the compliance program been established, so that responsibility does not lapse between projects, personnel changes, or renewal cycles? A program without an accountable owner tends to erode.

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

Review Readiness with a Consulting CIO

Has the organization arranged for periodic review of its compliance readiness with a Consulting CIO or comparable advisor, so that framework changes, new obligations, and emerging risks are apprised to leadership in time to act?

- **Compliant**
- **Needs Attention**
- **N/A**

NOTES:

© 2026 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.

© 2026 Sandbox Technologies, Inc.