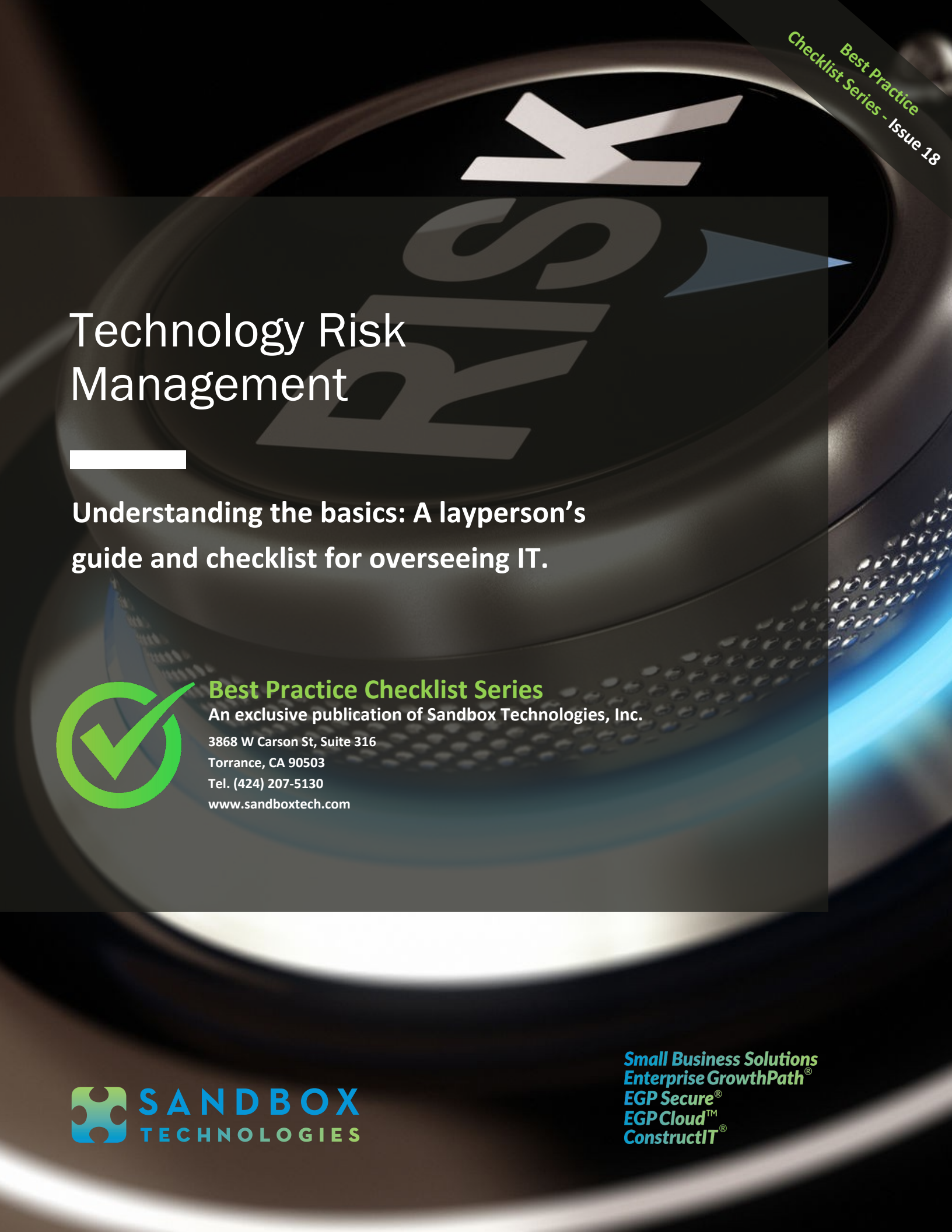


Best Practice Checklist Series - Issue 18

Technology Risk Management

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®

Technology Risk Management

Every organization that relies on technology accepts a measure of risk in doing so. Systems fail, vendors are breached, credentials are stolen, and well-intentioned changes occasionally produce unintended consequences. The objective of a mature technology risk program is not to eliminate this reality, which is not possible, but to understand it, to measure it in terms the business can weigh, and to make deliberate, defensible decisions about what to do in response. Risk is inherent to the use of technology; it is, however, manageable.

A central premise of this publication is that the acceptance of risk is a business decision, and that decision belongs to the client. Sandbox Technologies does not possess complete knowledge of a client's contractual obligations, revenue dependencies, tolerance for disruption, or competitive circumstances. The firm's obligation is to present the relevant facts, variables, likelihoods, and potential outcomes within its area of focus, and to do so even-handedly: the danger of acting and the danger of not acting are both disclosed. Whether a given exposure is remediated, insured, avoided, or simply accepted is for the client to determine on an informed basis. A given exposure may well constitute an acceptable risk once it is understood and agreed upon; what is not defensible is exposure that was never identified, never quantified, and never consciously chosen.

Technology risk and information-security risk are treated together here because, in practice, they are inseparable. A single point of failure in an aging server is an operational risk and a security risk at once; a vendor that mishandles data is a supply-chain risk and a breach risk at once. The lens of this issue is risk itself: how exposures are identified, assessed, prioritized, and governed over time, and how the common responses to risk, including insurance, are used.

This document is written as a layperson's primer and checklist. It is intended to equip a non-technical manager or executive to work alongside their IT personnel, to ask informed questions, and to recognize when a matter of consequence has been surfaced for a decision. It does not substitute for a formal risk assessment conducted in the context of a specific environment.

As with all matters carrying material business consequence, it is recommended that the topics raised here be reviewed with your Sandbox Technologies Consulting CIO, who can assist in translating the principles below into a risk posture appropriate to your organization.

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

Contents

Key Concepts 4

Scenarios 6

Areas to Discuss 8

Recommended Implementation Practices 10

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

Key Concepts

Risk. The potential for events to harm operations, finances, reputation, or obligations. Risk is commonly assessed by considering likelihood and consequence together. Specific risks may be avoided or removed, while others remain; the practical task is to identify, prioritize, and respond to them deliberately.

Likelihood. An estimate, often expressed on a simple scale such as low, medium, or high, of the probability that a given adverse event will occur within a defined period. Likelihood is informed by threat intelligence, historical incidents, the condition of systems, and the effectiveness of existing safeguards. It is an estimate, not a certainty, and is revisited as conditions change.

Impact. The magnitude of harm the organization would sustain should an event occur, assessed across dimensions such as downtime, financial loss, legal or regulatory exposure, contractual penalties, and reputational damage. A useful discipline is to express impact in business terms, for example hours of downtime or dollars at stake, rather than purely technical terms, so that the business can weigh it meaningfully.

Risk Register. A maintained record, typically a structured document or database, in which identified risks are catalogued along with their assessed likelihood, impact, assigned owner, chosen response, and current status. The Risk Register is the central artifact of a risk program; it converts scattered concerns into a governed, prioritized, and reviewable inventory, and it provides the evidentiary record that a given risk was in fact identified and consciously handled.

Common Responses to Risk. Organizations may mitigate, accept, transfer, share, or avoid risk. Mitigation reduces likelihood or impact through safeguards. Acceptance consciously retains exposure. Transfer and sharing allocate aspects of risk through insurance, contracts, or other arrangements; limits and exclusions remain important. Avoidance ceases or forgoes the activity creating the exposure. Responses may be combined, and their selection is a business decision.

Residual Risk. The risk remaining after responses have been applied. Safeguards often reduce likelihood or impact without removing every exposure. Residual risk should be identified, evaluated, and accepted at an appropriate level of authority. Avoiding an activity may remove a specific risk, although the organization may still face other risks or consequences from that decision.

Third-Party and Supply-Chain Risk. The exposure an organization inherits from the vendors, service providers, software publishers, and Cloud platforms on which it depends. A weakness in a supplier's security, a supplier's own breach, or a supplier's failure can become the organization's incident. Vendor

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

certifications and audit reports, such as a System and Organization Controls (SOC 2) report, are useful indicators of good-faith diligence but do not by themselves establish that a given vendor is suitable or secure for a particular use; a degree of trust in the vendor's representations remains, and that trust is itself a form of accepted risk.

Single Point of Failure (SPOF). A component, system, person, or supplier whose failure would by itself interrupt an essential business function, because no redundant or alternative path exists. Single points of failure may be technical, such as a lone server or a single Internet circuit, or organizational, such as sole reliance on one individual or one vendor. A related concern is concentration risk, in which too many functions depend on a single provider or location.

Business Impact Analysis (BIA). A structured exercise that identifies the organization's essential functions, determines what each depends upon, and establishes how quickly each must be restored and how much data loss can be tolerated. The BIA typically yields two governing measures: the Recovery Time Objective (RTO), the target duration within which a function should be restored, and the Recovery Point Objective (RPO), the maximum acceptable amount of data, measured in time, that may be lost. These objectives translate business priorities into technical requirements for continuity and recovery.

© 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.

The Unassessed Single Point of Failure. *An organization operated a critical line-of-business application on a single aging server that had performed reliably for years. Because it had never failed, its condition was not treated as a pressing concern, and no formal assessment of the exposure was recorded. The server's storage failed during a routine week, and the most recent usable backup was several days old and had not been tested for restoration. Recovery required the procurement of replacement hardware, the rebuilding of the operating environment, and the reconstruction of lost data from manual records. The function was unavailable for the better part of a week. The failure was foreseeable, and the underlying exposure was, in hindsight, a small yet very real possibility that had never been surfaced for a decision. Had the single point of failure been entered in a Risk Register and its impact expressed in hours of downtime, the organization might have chosen to fund redundancy, to validate its backups, or to formally accept the exposure with open eyes. It did none of these, because the question was never asked.*

The Vendor Breach That Cascaded. *An organization engaged a third-party provider to handle a routine back-office function and, in the ordinary course, granted that provider access to certain systems and data. The provider had furnished a current audit report, and its assurances were accepted in good faith. The provider was later compromised, and the credentials and connectivity it held became the path through which the organization itself was reached. Sensitive information was exposed, and notification obligations followed. The audit report had been a reasonable indicator of diligence, but it did not, and could not, guarantee the provider's security at every moment thereafter. The residual risk of extending trust and access to an outside party had always been present; it had simply not been assessed, limited by contract, or constrained by the principle of least privilege. The exposure was real, it was inherited, and it was governable, but it had not been governed.*

The Denied Cyber-Insurance Claim. *An organization carried a cyber-insurance policy and regarded itself as protected. In applying for the policy, it had attested to a set of security controls, including Multifactor Authentication (MFA) on all remote and administrative access. Over time, an exception was made for a category of accounts, and MFA lapsed there without the change being reconciled against the policy's requirements. A compromise occurred through precisely such an account. Upon review of the claim, the insurer determined that a warranted control had not been in place as attested, and coverage was contested. The organization had believed the risk was transferred; in practice, a substantial portion of it had quietly reverted, because the conditions of transfer had not been maintained. Insurance transfers financial consequence only to the extent its control requirements are genuinely and continuously satisfied.*

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

The Accepted Risk That Was Never Agreed. *During a technical review, IT personnel identified an exposure and, judging it minor, elected to defer remediation. No entry was made in a Risk Register, no owner was assigned, and the matter was never presented to management for a decision. When the exposure was later realized and questioned, there was no record of who had accepted the risk, on what basis, or with what authority. What might have been a perfectly defensible acceptance of a minor risk instead became an accountability gap. Acceptance is a legitimate and often correct response, but only when it is a conscious decision made at the appropriate level, documented, and agreed upon. An acceptance that exists only by default is indistinguishable from an oversight.*

© 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.

Establishing and Maintaining a Risk Register

A risk program begins with a single, authoritative inventory of identified risks. Each entry should record the exposure in plain terms, its assessed likelihood and business impact, the individual accountable for it, the chosen response, and its current status. The register is not a one-time deliverable; it is a living record reviewed on a defined cadence and updated as systems, vendors, threats, and business priorities change.

- Describe each risk in business terms a non-technical reader can weigh.
- Assign a named owner to every risk, not merely to the register as a whole.
- Record the chosen response and the residual risk that remains after it.

Assessing Likelihood and Business Impact

Prioritization depends on a consistent method for rating how likely an event is and how much harm it would cause. Simple, defensible scales are generally preferable to elaborate ones that are not maintained. Impact should be expressed where possible in terms the business already understands, such as hours of downtime, records exposed, or dollars at risk, so that limited resources are directed to the exposures that matter most.

- Rate likelihood and impact separately, then consider them together.
- Prioritize high-impact exposures even where likelihood is assessed as low.

Selecting Among the Four Responses

For each material risk, consideration should be given to whether it is best mitigated, accepted, transferred, or avoided, recognizing that a combination is common. The selection is a business decision informed by the cost of each option relative to the exposure it addresses. It is recommended that the reasoning behind each selection be recorded, so that the decision is defensible and can be revisited as circumstances evolve.

- Mitigation reduces likelihood or impact but leaves residual risk.
- Insurance may cover specified financial losses, including some interruption costs, subject to policy terms.
- Acceptance is valid only when conscious, documented, and authorized.

Governing Third-Party and Supply-Chain Risk

Dependence on outside providers is unavoidable and often beneficial, but the exposure it creates must be assessed rather than assumed away. Vendor certifications and audit reports are useful indicators of diligence and should be requested and reviewed; they do not, however, establish suitability for a specific

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

environment on their own. Access granted to vendors should be limited to what is necessary, and contractual terms addressing security, breach notification, and liability should be examined before reliance is placed on a provider.

- Maintain an inventory of vendors and the data and access each holds.
- Apply the principle of least privilege to all third-party access.
- Treat a certification as evidence of good-faith diligence, not as a guarantee.

Identifying Single Points of Failure and Concentration

Essential functions should be examined to determine where a single component, individual, location, or supplier could, by itself, cause an interruption. This examination extends beyond hardware to connectivity, key personnel, and the concentration of multiple functions within one provider. Where a single point of failure is identified, the options of introducing redundancy, arranging an alternative, or formally accepting the exposure should be presented for a decision.

- Examine technical, human, and vendor concentration alike.
- Weigh the cost of redundancy against the assessed impact of an outage.

Aligning Cyber-Insurance With Actual Controls

Cyber-insurance may cover specified losses, subject to the actual policy, limits, exclusions, and conditions. Control representations should be accurate and reconciled against practice throughout the policy period. Whether a discrepancy affects a claim depends on the policy and applicable law; it is not an automatic reversion of all transferred risk. Review material changes and coverage questions with the insurer, broker, and counsel.

- Confirm that attested controls, such as MFA and tested backups, are actually deployed and maintained.
- Reconcile the environment against policy requirements after any significant change.

Incident Preparedness and Business Continuity

Because no set of safeguards eliminates the possibility of an incident, the capacity to respond and recover is itself a risk control. A Business Impact Analysis (BIA) should establish which functions matter most and define the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each. An incident response plan and a continuity plan should be documented, assigned to owners, and, importantly, exercised, since an untested plan offers uncertain assurance.

- Define RTO and RPO for each essential function through a BIA.
- Test backups and recovery procedures rather than presuming they work.
- Rehearse incident response so roles are understood before an event occurs.

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

Recommended Implementation Practices

Maintain a Current Risk Register

Does the organization maintain a single, authoritative inventory of identified technology and information-security risks, with likelihood, impact, an assigned owner, and a chosen response recorded for each? A register that is current and reviewed is the foundation on which every other practice depends.

NOTES

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

Express Impact in Business Terms

Are the consequences of each risk stated in terms the business can weigh, such as hours of downtime, records exposed, or financial loss, rather than in purely technical language? Prioritization is only meaningful when impact is understood by those who must decide.

NOTES

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

Assign Ownership for Every Risk

Has a named individual been made accountable for each risk in the register, including those the organization has chosen to accept? Risk without an owner tends to be risk without attention.

NOTES

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

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

Decide and Document the Response

For each material risk, has a deliberate choice been made among mitigation, acceptance, transfer, and avoidance, and has the reasoning been recorded? The response, and the residual risk that remains after it, should be a matter of record rather than of memory.

NOTES

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

Document and Authorize Accepted Risk

Where a risk has been accepted, has that acceptance been made consciously, at an appropriate level of authority, and recorded as an agreed business decision? An acceptance that exists only by default is indistinguishable from an oversight.

NOTES

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

Inventory and Constrain Vendor Access

Does the organization maintain a current inventory of its vendors, the data and systems each can reach, and the access each holds, with that access limited to what is necessary? Exposure that is inherited from a supplier cannot be governed until it is first understood.

NOTES

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

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

Scrutinize Vendor Assurances

Are vendor certifications and audit reports requested, reviewed, and understood as indicators of good-faith diligence rather than as guarantees of suitability or security? Reliance on a provider is a form of accepted risk and should be recognized as such.

NOTES

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

Identify Single Points of Failure

Have the organization's essential functions been examined to identify any single component, circuit, location, individual, or supplier whose failure would by itself cause an interruption? Where such a point is found, the choice among redundancy, an alternative, and formal acceptance should be presented for a decision.

NOTES

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

Reconcile Insurance With Reality

Do the controls in place match representations made in the cyber-insurance application, and are they reconciled after significant changes? Check policy conditions, exclusions, and notification duties with the broker or insurer; a mismatch can affect coverage.

NOTES

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

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

Conduct a Business Impact Analysis

Has a Business Impact Analysis (BIA) been performed to identify essential functions and to establish a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each? Continuity requirements should be derived from business priorities, not assumed.

NOTES

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

Verify Backups by Testing Them

Are backups not only performed but periodically tested by actually restoring from them? A backup that has never been restored is an assumption, not a safeguard.

NOTES

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

Prepare and Rehearse Incident Response

Does a documented incident response plan exist, with assigned roles, and has it been exercised before it is needed? The capacity to respond and recover is itself a control against the impact of events that safeguards did not prevent.

NOTES

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

Review Risk on a Defined Cadence

Is the risk program treated as an ongoing, cyclical discipline, with the register and assessments revisited on a regular schedule and after material changes to systems, vendors, or threats? Risk is not static, and a program that is not maintained gradually ceases to reflect reality.

NOTES

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

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

Engage Leadership in Risk Decisions

Are matters of material consequence surfaced to the appropriate level of management for an informed decision, with both the danger of acting and the danger of not acting presented even-handedly? It is recommended that these reviews be conducted with your Sandbox Technologies Consulting CIO, so that the organization's risk posture remains a matter of conscious, documented choice.

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.