INTELLECT INTEGRATED SERVICES

# Business Technology Health Guide™

## 21 Essential Questions Every Business Owner Should Answer Before Their Next IT Crisis

A practical executive guide for evaluating your organization's technology, cybersecurity, email, backup, cloud, and business continuity readiness.

**VETERAN-OWNED TECHNOLOGY ADVISOR**

Serving businesses throughout the High Desert, Inland Empire, and nationwide

Managed IT • Cybersecurity • Cloud • Compliance • Technology Advisory

START AT /FREEASSESSMENT

INTRODUCTION

# A Welcome From IIS

**Technology should help your business grow.**

It should not become a source of unexpected downtime, cyber threats, lost productivity, or costly surprises.

This guide was created to help business owners evaluate the health of their technology environment using the same practical categories we discuss during client engagements.

You do not need to be an IT expert. Answer each question based on what you know today. A “Not Sure” response is useful because unknown technology risks often become business risks.

This guide does not replace a professional evaluation. It is designed to help you recognize priorities, ask better questions, and decide where a closer review may be valuable.

I hope you find it useful and that it gives you greater clarity about the technology supporting your organization.

**Tolulope A.**

Founder & Technology Advisor

Intellect Integrated Services

10–15 MINUTES

# How to Use This Guide

1

## Answer Every Question

Select Yes, No, Not Sure, or Not Applicable. Choose N/A only when the practice genuinely does not apply.

2

## Score Each Response

Yes = 5 points. Not Sure = 2 points. No = 0 points. Exclude Not Applicable questions from available points.

3

## Review the Business Impact

Read why each control matters and compare the recommended action with your current practice.

4

## Choose Your Priorities

Start with Immediate and Important priority questions marked No or Not Sure. Use the Quick Wins page to begin.

5

## Request a Second Opinion

Use the Complimentary Business Technology Health Review™ if you want an advisor to review your responses.

**IMPORTANT: THIS IS A SELF-CHECK, NOT AN ASSESSMENT**

Your answers are self-reported and directional. Choose Not Applicable only when the technology or practice truly does not exist. If you do not know, choose Not Sure. This guide does not validate controls or inspect systems. Any Complimentary Review Recap is limited to your stated concerns, up to three discussion priorities, and a recommended next step. It is not an assessment, executive report, financial exposure analysis, or roadmap.

AT-A-GLANCE WORKSHEET

# 21-Point Quick Checklist

Use this page for a fast first pass. Mark Y, N, ?, or N/A, then use the detailed pages for business impact, actions, and notes. N/A is excluded from scoring; use ? when you do not know.

| | | | Y | N | ? | N/A |
|---|---|---|---|---|---|---|
| **IDENTITY & ACCOUNT PROTECTION** | | | | | | |
| 01 | Multi-Factor Authentication | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| 02 | Separate Administrator Accounts | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| 03 | Password Management | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| 04 | Access Reviews | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| **EMPLOYEE & DEVICE SECURITY** | | | | | | |
| 05 | Endpoint Detection and Response | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| 06 | Device Encryption | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| 07 | Central Device Management | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| 08 | Supported Systems and Lifecycle | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| **BACKUP & BUSINESS CONTINUITY** | | | | | | |
| 09 | Protected Backups | IMMEDIATE | ☐ | ☐ | ☐ | ☐ |
| 10 | Recovery Testing | IMMEDIATE | ☐ | ☐ | ☐ | ☐ |
| 11 | Recovery Expectations | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| 12 | Alternate Operations | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| **NETWORK & REMOTE WORK SECURITY** | | | | | | |
| 13 | Business-Grade Firewall | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| 14 | Secure Wi-Fi Separation | FOUNDATIONAL | ☐ | ☐ | ☐ | ☐ |
| 15 | Secure Remote and Vendor Access | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| **EMAIL & CLOUD SECURITY** | | | | | | |
| 16 | Cloud Account Security and Access | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| 17 | Email Domain Protection | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| 18 | Independent Cloud Data Backup | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| **GOVERNANCE, TRAINING & INCIDENT READINESS** | | | | | | |
| 19 | Security Awareness | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| 20 | Technology Documentation | IMPORTANT | ☐ | ☐ | ☐ | ☐ |
| 21 | Incident Response Plan | IMMEDIATE | ☐ | ☐ | ☐ | ☐ |

# Identity & Account Protection

Protecting employee identities is the first line of defense against account takeover and business email compromise.

## Multi-Factor Authentication

IMPORTANT

Are employees required to use a second verification step when accessing Microsoft 365, email, or other business applications?

**BUSINESS IMPACT**

A stolen password alone may give an attacker access to email, files, and sensitive business information.

**RECOMMENDED ACTION**

Require MFA for every user, especially administrators and finance staff.

**NOTES OR EVIDENCE TO VERIFY**

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

## Separate Administrator Accounts

IMPORTANT

Do people who manage your systems use separate administrator accounts rather than their everyday email accounts?

**BUSINESS IMPACT**

Using one account for daily work and administration increases the damage a stolen password can cause.

**RECOMMENDED ACTION**

Create separate admin accounts and use them only when elevated access is required.

**NOTES OR EVIDENCE TO VERIFY**

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

# Identity & Account Protection

Protecting employee identities is the first line of defense against account takeover and business email compromise.

## Password Management

IMPORTANT

Does your organization use a secure password manager and prohibit shared or reused passwords?

**BUSINESS IMPACT**

Reused and shared passwords make unauthorized access harder to detect and contain.

**RECOMMENDED ACTION**

Adopt an approved password manager and require unique passwords for every service.

**NOTES OR EVIDENCE TO VERIFY**

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

## Access Reviews

IMPORTANT

Do you regularly review who can access business systems, especially after job changes or departures?

**BUSINESS IMPACT**

Old or excessive access can leave confidential information exposed long after it is needed.

**RECOMMENDED ACTION**

Review access quarterly and remove accounts immediately when employment or roles change.

**NOTES OR EVIDENCE TO VERIFY**

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

# Employee & Device Security

Every laptop, desktop, and mobile device that reaches business information can strengthen or weaken your security.

## Endpoint Detection and Response

IMPORTANT

Do all business computers use centrally monitored security software that can detect and contain suspicious behavior, not just basic antivirus?

**BUSINESS IMPACT**

Modern attacks can bypass basic antivirus and spread before anyone notices.

**RECOMMENDED ACTION**

Use centrally monitored endpoint detection and response on every supported business device.

**NOTES OR EVIDENCE TO VERIFY**

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

## Device Encryption

IMPORTANT

Are business laptops protected so stored information remains unreadable if a device is lost or stolen?

**BUSINESS IMPACT**

A lost laptop can become a reportable data incident if its storage is not encrypted.

**RECOMMENDED ACTION**

Enable full-disk encryption such as BitLocker and securely retain recovery keys.

**NOTES OR EVIDENCE TO VERIFY**

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

# Employee & Device Security

Every laptop, desktop, and mobile device that reaches business information can strengthen or weaken your security.

## Central Device Management

IMPORTANT

Are business laptops, desktops, and mobile devices inventoried, updated, and managed through an approved process or management platform?

**BUSINESS IMPACT**

Unmanaged devices may miss critical updates and can become an easy path into the business.

**RECOMMENDED ACTION**

Maintain a current inventory and centrally enforce updates, security settings, and device ownership.

**NOTES OR EVIDENCE TO VERIFY**

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

## Supported Systems and Lifecycle

IMPORTANT

Are operating systems and business devices still supported, with planned replacement dates before support ends?

**BUSINESS IMPACT**

Unsupported systems stop receiving normal security fixes and can create downtime and emergency replacement costs.

**RECOMMENDED ACTION**

Track support dates and maintain a planned replacement lifecycle for every business device.

**NOTES OR EVIDENCE TO VERIFY**

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

# Backup & Business Continuity

Reliable recovery protects revenue, customer commitments, and operations when systems or locations become unavailable.

## Protected Backups

IMMEDIATE

Are critical files and systems backed up automatically to a location attackers cannot easily change or delete?

**BUSINESS IMPACT**

If ransomware can reach the backup, recovery may be impossible when the business needs it most.

**RECOMMENDED ACTION**

Use automated, isolated or immutable backups for critical information.

**NOTES OR EVIDENCE TO VERIFY**

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

## Recovery Testing

IMMEDIATE

Has your organization successfully restored files or systems from backup within the last six months?

**BUSINESS IMPACT**

A backup is only useful if it can restore the right information within an acceptable time.

**RECOMMENDED ACTION**

Perform documented restore tests at least twice a year and correct failures promptly.

**NOTES OR EVIDENCE TO VERIFY**

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

# Backup & Business Continuity

Reliable recovery protects revenue, customer commitments, and operations when systems or locations become unavailable.

## Recovery Expectations

IMPORTANT

Have leaders defined how quickly critical operations must resume and how much recent data the business could afford to lose?

**BUSINESS IMPACT**

Without clear recovery targets, backup spending and recovery plans may not match business needs.

**RECOMMENDED ACTION**

Define recovery time and recovery point expectations for each critical process.

**NOTES OR EVIDENCE TO VERIFY**

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

## Alternate Operations

IMPORTANT

Could your business continue operating if the office, primary server, or main internet connection became unavailable tomorrow?

**BUSINESS IMPACT**

A localized outage can stop revenue-producing work even when no data is lost.

**RECOMMENDED ACTION**

Document alternate work locations, communications, system access, and key responsibilities.

**NOTES OR EVIDENCE TO VERIFY**

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

SECTION 4 OF 6

# Network & Remote Work Security

Your network and remote connections should limit unnecessary access while supporting productive work.

## Business-Grade Firewall

IMPORTANT

If your organization manages an office, store, or facility network, is its internet connection protected by a monitored and current business firewall?

**BUSINESS IMPACT**

Consumer equipment may not provide the visibility or controls needed to protect business operations.

**RECOMMENDED ACTION**

Use a supported business firewall with secure configuration, updates, and monitoring.

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

## Secure Wi-Fi Separation

FOUNDATIONAL

If your location provides guest or personal-device Wi-Fi, is it separated from employee devices, servers, printers, and other business systems?

**BUSINESS IMPACT**

A compromised guest or personal device should not have a direct path to sensitive systems.

**RECOMMENDED ACTION**

Create separate guest and business networks with access controls between them.

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

## Secure Remote and Vendor Access

IMPORTANT

If employees or outside vendors connect remotely, is that access approved, protected by MFA, and removed when no longer needed?

**BUSINESS IMPACT**

Unmonitored remote access can become a hidden entry point into the business.

**RECOMMENDED ACTION**

Use approved secure access, require MFA, log activity, and review vendor access regularly.

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

SECTION 5 OF 6

# Email & Cloud Security

Cloud platforms require active governance; default settings alone may not match your business risk.

## Cloud Account Security and Access

IMPORTANT

If you use Microsoft 365, Google Workspace, or another cloud service, are security defaults or equivalent protections enabled and are user access and sharing reviewed regularly?

**BUSINESS IMPACT**

Stolen accounts, former-user access, and uncontrolled sharing can expose email, files, and customer information.

**RECOMMENDED ACTION**

Enable appropriate sign-in protections and review users, administrators, sharing links, and risky activity regularly.

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

## Email Domain Protection

IMPORTANT

If your organization uses a custom email domain, is it configured to help prevent criminals from impersonating your company?

**BUSINESS IMPACT**

Email impersonation can expose customers, employees, and vendors to fraud.

**RECOMMENDED ACTION**

Configure and monitor SPF, DKIM, and DMARC for every sending service.

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

## Independent Cloud Data Backup

IMPORTANT

If your organization stores email or files in a cloud service, is that information backed up through a separate recovery solution?

**BUSINESS IMPACT**

Built-in retention and deleted-item recovery may not protect against every mistake, account compromise, or ransomware event.

**RECOMMENDED ACTION**

Use an independent backup for critical cloud email and files, and test that information can be restored.

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

SECTION 6 OF 6

# Governance, Training & Incident Readiness

Clear ownership, training, documentation, and preparation reduce confusion when a serious event occurs.

## Security Awareness

IMPORTANT

Do employees receive recurring training and realistic guidance on phishing, payment fraud, and safe information handling?

**BUSINESS IMPACT**

Employees are frequently targeted because a convincing message can bypass technical safeguards.

**RECOMMENDED ACTION**

Provide practical training at onboarding and throughout the year.

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

## Technology Documentation

IMPORTANT

Does your organization maintain a current inventory of devices, systems, vendors, owners, key contacts, and recovery information?

**BUSINESS IMPACT**

Missing or outdated documentation delays troubleshooting, recovery, vendor coordination, and leadership decisions.

**RECOMMENDED ACTION**

Maintain a practical technology inventory and review it after major changes and at least annually.

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

## Incident Response Plan

IMMEDIATE

Does your team have a written, accessible plan for the first actions to take during ransomware, a data breach, or a major technology outage?

**BUSINESS IMPACT**

Confusion during an incident increases downtime, cost, data loss, and communication risk.

**RECOMMENDED ACTION**

Document roles, contacts, escalation steps, communication procedures, and recovery priorities, then test the plan annually.

☐ YES ☐ NO ☐ NOT SURE ☐ NOT APPLICABLE

DIRECTIONAL SCORECARD

# Your Preliminary Self-Check Indicator

**Yes = 5 points | Not Sure = 2 points | No = 0 points | Not Applicable = excluded. Score only the questions that apply to your organization.**

**Identity & Account Protection**
4 questions | Applicable questions: ____ × 5 _____ **available**

**Employee & Device Security**
4 questions | Applicable questions: ____ × 5 _____ **available**

**Backup & Business Continuity**
4 questions | Applicable questions: ____ × 5 _____ **available**

**Network & Remote Work Security**
3 questions | Applicable questions: ____ × 5 _____ **available**

**Email & Cloud Security**
3 questions | Applicable questions: ____ × 5 _____ **available**

**Governance, Training & Incident Readiness**
3 questions | Applicable questions: ____ × 5 _____ **available**

**TOTAL POINTS** _____ earned **SELF-CHECK SCORE** _____ %

Formula: Points earned ÷ maximum points from applicable questions × 100

DIRECTIONAL GUIDANCE

# Interpret Your Self-Check

| | |
|---|---|
| **90–100** WELL PREPARED | Your answers suggest many foundational practices may be in place. A professional review can still confirm what the worksheet cannot. |
| **75–89** PROGRESSING | Your answers suggest a solid starting point with several practices worth confirming or improving. |
| **60–74** NEEDS ATTENTION | Several answers deserve a closer conversation and clearer ownership. |
| **40–59** EARLY STAGE | Your worksheet shows multiple gaps or unknowns that should be organized and discussed. |
| **BELOW 40** START HERE | Begin with the Immediate priority items and request professional guidance to establish a practical starting point. |

## 10 Technology Health Quick Wins

1. Require MFA for every account
2. Remove unused administrator access
3. Test one critical backup restore
4. Confirm laptop encryption is enabled
5. Update or replace unsupported systems
6. Review Microsoft 365 licenses and sharing
7. Strengthen email impersonation protection
8. Document vendor and remote access
9. Refresh employee security awareness
10. Review cyber insurance control requirements

# Ready for a Professional Review?

Completing this guide is an excellent first step. If you would like a certified technology advisor to review your responses, schedule a:

## Complimentary Business Technology Health Review™

**During this 30-minute conversation, we will:**

- Review your guide responses
- Discuss your technology goals and concerns
- Answer your questions in plain English
- Clarify up to three discussion priorities
- Provide a limited Complimentary Review Recap

**BONUS CHECK — CYBER INSURANCE ALIGNMENT**

If you carry cyber insurance, can you verify that the security controls listed in your application are still in place? Bring the questionnaire to your review if you are unsure.

### Request My Complimentary Review

Book online:

**outlook.office.com/book/IISTechnologyAdvisory@intellectintegratedservices.com**

Or call (888) 569-0883 | Info@intellectintegratedservices.com

**SCAN TO VISIT /FREEASSESSMENT**

No obligation. No pressure. Clear guidance for smarter technology decisions.

**INTELLECT INTEGRATED SERVICES**

Veteran-Owned Technology Advisor | High Desert & Inland Empire | Nationwide Remote Support