BROTHERLY
TECHNOLOGY

INDUSTRY PLANNING CHECKLIST

The Industry IT Requirements Checklist

The compliance and uptime requirements that differ by sector - and what they mean for your systems.

01	**Requirements that change by industry**
02	**The software support questions to ask any provider**
03	**How to scope IT around how your business runs**

Use this guide to assess where you are, identify the evidence you need, and turn the biggest gaps into a practical action plan.

Prepared by Brotherly Technology
Owner-led IT, security, and compliance support.

15-MINUTE ASSESSMENT

Start with the current state

Mark each item Yes, Partial, or No. A written policy only counts as Yes when the process is operating and you can show evidence.

[ ] Business-critical workflows and their maximum tolerable downtime are documented.	[ ] Yes [ ] Partial [ ] No
[ ] Sensitive data types and applicable contractual, legal, regulatory, and insurer obligations are identified.	[ ] Yes [ ] Partial [ ] No
[ ] Line-of-business applications have owners, supported versions, vendors, and recovery requirements.	[ ] Yes [ ] Partial [ ] No
[ ] Access roles match job duties, segregation needs, and high-risk approvals.	[ ] Yes [ ] Partial [ ] No
[ ] Retention, legal hold, export, and defensible disposal needs are mapped by record type.	[ ] Yes [ ] Partial [ ] No
[ ] Third parties are classified by data, access, operational criticality, and replacement difficulty.	[ ] Yes [ ] Partial [ ] No
[ ] Endpoint, network, cloud, email, and physical controls reflect the actual work environment.	[ ] Yes [ ] Partial [ ] No
[ ] Backup and recovery cover the application, data, identity, configuration, and dependent vendors.	[ ] Yes [ ] Partial [ ] No
[ ] Logging and incident plans address the events leadership may need to investigate or report.	[ ] Yes [ ] Partial [ ] No
[ ] Remote work, field work, production, clinical, or client-site conditions are included.	[ ] Yes [ ] Partial [ ] No
[ ] IT service scope names the owner for every critical system and vendor relationship.	[ ] Yes [ ] Partial [ ] No
[ ] The plan is reviewed after material business, system, location, or regulatory change.	[ ] Yes [ ] Partial [ ] No

Quick score: Yes = 2, Partial = 1, No = 0. Start with any No that could stop work, expose sensitive data, or create an avoidable contract cost.

SECTOR MAP

Start with the work and data, then select controls

Industry labels are only a starting point. Contracts, state law, customers, insurers, data, and operating conditions can create additional requirements.

Sector	Distinctive concern	IT implication
Dental / healthcare	ePHI, clinical continuity, medical devices	HIPAA risk analysis, BAAs, auditability, tested downtime
Financial services	Customer information and regulated safeguards	Written program, MFA, encryption, vendor oversight, reporting
Legal	Privilege, confidentiality, e-discovery, client terms	Matter access, secure sharing, legal hold, retention
Engineering	Large files, version integrity, client restrictions	Performance, locking/worksharing, project recovery
Manufacturing	Production uptime, safety, legacy OT	Segmentation, controlled access, offline recovery, spares
Nonprofit	Donor/beneficiary data and constrained budget	Eligible licensing, least privilege, payment controls, continuity
Small business	Limited staff and concentration of knowledge	Simple baseline, managed ownership, documented recovery

Use qualified counsel and compliance professionals to confirm obligations; use IT evidence to show how the organization implements them.

PROVIDER FIT

Ask software-support questions that expose gaps

A provider may support the network but exclude the application your team depends on. Name the coordination work before the first outage.

1	List every critical application, version, vendor, contract, support contact, dependency, and business owner.
2	Ask whether the provider supports the application, coordinates the vendor, or excludes it - and who owns each handoff.
3	Confirm supported operating systems, network/storage requirements, backup method, logging, remote access, and upgrade process.
4	Walk through an application outage and a failed upgrade, including severity, escalation, onsite work, rollback, and communications.
5	Put the responsibility matrix, documentation, and recurring review into the service scope.

What to watch for

WATCH: The provider says 'we support everything' but will not name boundaries.

WATCH: The application is unsupported on the current operating system.

WATCH: The software vendor and IT provider each assume the other owns backup.

WATCH: No one has tested a full application restore.

WATCH: Vendor remote access bypasses MFA or logging.

BROTHERLY
TECHNOLOGY

MAKE IT ACTIONABLE

Turn the worksheet into a 30-day plan

Do not try to solve everything at once. Assign one owner, one next action, and one date for each priority.

NOW	Name the owner and confirm the current state.	____________________
NEXT 7 DAYS	Fix the highest-risk gap or gather the missing evidence.	____________________
NEXT 30 DAYS	Complete the remaining quick wins and set review dates.	____________________
NEXT QUARTER	Test the process, document results, and assign improvements.	____________________

Notes / decisions / questions for your provider

____

____

____

____

____

Want a second set of eyes? Book a free consultation at brotherlytechnology.com/contact/ or call 404-907-1005.