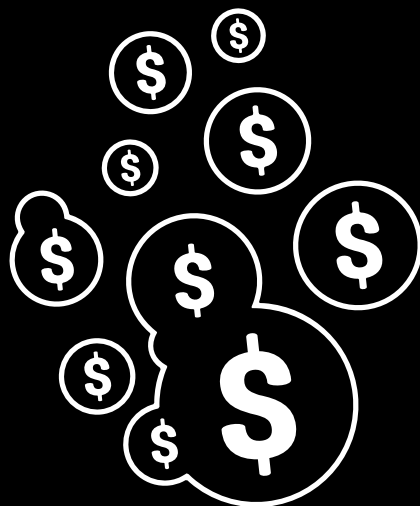


TECHNOLOGY BUDGETING FOR 2027



HEALTHCARE



FINANCIAL



MANUFACTURING



LEGAL



INSURANCE



NONPROFITS

*Six industry-specific
checklists to guide
wiser technology
investments*

Paige Yeater

*Chief Operating Officer &
Chief Information Security Officer*



Technology Budgeting Checklists *by Industry*



A Practical Planning Tool for Leaders Who Want to Fund Wisely, Phase Thoughtfully, and Plan Ahead

Every organization depends on technology, but every industry carries a different kind of risk. A **law firm** needs to protect billable time, document access, and client confidentiality. A **healthcare** organization needs to protect patient access, EHR availability, and care continuity. A **manufacturer** needs to protect uptime, production visibility, and customer commitments. A **nonprofit** needs to protect mission stewardship, donor trust, and staff capacity. **Financial services** and **insurance firms** need to protect client confidence, secure communication, audit readiness, and service consistency.

A useful technology budget starts with the work your organization cannot afford to disrupt. This checklist collection was created to help leaders ask better questions before budget decisions are final. Each industry checklist is designed to surface the technology needs that often stay hidden until they become urgent: aging systems, support gaps, cybersecurity needs, vendor dependencies, lifecycle planning, and the staff time lost to workarounds.

How To Use These Checklists

Start with the checklist that best matches your organization. Then bring the right people into the conversation: leadership, finance, operations, compliance, IT, department owners, and the people closest to the day-to-day work. As you move through each section, check off items that have been reviewed, assign owners where decisions are needed, and mark what should be funded, phased, or revisited later. You do not need every answer right away. The value is in seeing the full picture before the next budget cycle locks in.

What To Look For

- The systems that would disrupt service, care, production, client work, or mission delivery if they failed.
- Security controls that need funding, documentation, or follow-through.
- Aging equipment and software that should be refreshed before they create urgency.
- Vendor relationships, renewals, and integrations that need clearer ownership.
- Support issues that are costing your team more time than your budget currently reflects.

Plan Wisely With Mainstay

We created this checklist collection to give leaders a practical place to begin. We hope it helps your team step back, ask better questions, and see technology budgeting as part of a larger responsibility: protecting the people, promises, and daily work your organization depends on. Use it as a starting point for clearer conversations, wiser trade-offs, and a more confident path into the next budget cycle.



STENZ CON

04 HEALTHCARE

09 FINANCIAL

14 MANUFACTURING

19 LEGAL

24 INSURANCE

29 NONPROFITS

TECHNOLOGY BUDGETING CHECKLIST FOR HEALTHCARE

A Board-Ready Planning Tool for Care Continuity



TECHNOLOGY BUDGETING CHECKLIST FOR HEALTHCARE

Start with Patient-Critical Systems



- ☐ List the systems that support scheduling, EHR access, patient communication, phones, portals, billing, file access, and clinical documentation.
- ☐ Identify which systems would disrupt patient access, care coordination, documentation, or follow-up if unavailable for one business day.
- ☐ Map where ePHI is created, received, maintained, transmitted, backed up, and archived.
- ☐ Assign an owner and support path for each patient-critical system.

Protect EHR Availability



- ☐ Review the infrastructure around the EHR, including internet, Wi-Fi, endpoints, phones, backups, integrations, and vendor access.
- ☐ Identify where EHR downtime would create manual work, delayed documentation, patient follow-up gaps, or staff bottlenecks.
- ☐ Confirm how clinical and administrative teams continue working during an EHR, internet, or phone outage.
- ☐ Budget for improvements that strengthen access to the EHR and the systems that make it usable every day.

Separate Must-Fund Resilience from Optional Improvements



- ☐ Identify technology needs tied to patient access, HIPAA readiness, security controls, recovery, and staff productivity.
- ☐ Mark which items are required for continuity of care versus which are helpful future enhancements.
- ☐ Name the operational impact of delaying each major budget item.
- ☐ Prepare a leadership-ready explanation for why resilience investments should be funded before patient-facing workflows feel the strain.

TECHNOLOGY BUDGETING CHECKLIST FOR HEALTHCARE



Budget For HIPAA Readiness

- ☐ Confirm that the organization has a current HIPAA risk analysis and documented follow-up actions.
- ☐ Review administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of ePHI.
- ☐ Identify gaps in policies, procedures, access controls, documentation, contingency planning, and security training.
- ☐ Budget for the controls and evidence needed before an audit, incident, insurance review, or breach response creates urgency.

Review Access to ePHI



- ☐ Review access for staff, providers, vendors, business associates, contractors, and former employees.
- ☐ Confirm that MFA is enabled for email, remote access, EHR access, administrative accounts, and sensitive systems.
- ☐ Document how access is added, changed, reviewed, and removed when roles or employment status change.
- ☐ Separate privileged administrative accounts from everyday user accounts where appropriate.

Fund Core Cybersecurity Controls



- ☐ Review protections for phishing, ransomware, credential theft, known vulnerabilities, endpoint compromise, and email security. Confirm
- ☐ coverage for patching, endpoint protection, vulnerability management, encryption, logging, backup protection, and staff training. Identify
- ☐ internet-facing systems and remote access tools that need closer monitoring or remediation.
- ☐ Budget for practical testing, security reviews, tabletop exercises, and remediation work.

TECHNOLOGY BUDGETING CHECKLIST FOR HEALTHCARE

Manage Vendor & Business Associate Risk

- ☐ Inventory vendors and business associates that store, transmit, process, support, or access ePHI.
- ☐ Review agreements for security responsibilities, breach notification, access expectations, backup requirements, and data handling.
- ☐ Confirm who tracks vendor contacts, renewal dates, security documentation, and incident escalation steps.
- ☐ Budget for vendor review time and support around EHR, billing, imaging, telehealth, patient portal, and practice management systems.



Strengthen Patient Communication

- ☐ Review how patients access scheduling, portals, forms, reminders, secure messages, billing, and follow-up instructions.
- ☐ Confirm that phones, email, portal messaging, texting tools, and online forms are secure, reliable, and supported.
- ☐ Identify communication gaps that create staff rework, missed follow-up, or patient frustration.
- ☐ Budget for improvements that protect responsiveness, privacy, and continuity across patient communication channels.



Plan Lifecycle Around Care Delivery

- ☐ List aging endpoints, tablets, workstations, scanners, printers, network gear, phones, firewalls, Wi-Fi, backup systems, and peripheral tools.
- ☐ Identify unsupported devices, shared workstations, outdated operating systems, and tools dependent on one internal expert.
- ☐ Review upcoming warranties, renewals, vendor deadlines, platform changes, and equipment replacement needs.
- ☐ Build planned refreshes into the budget before old systems affect care teams or patient-facing workflows.



TECHNOLOGY BUDGETING CHECKLIST FOR HEALTHCARE

Test Backup, Recovery, & Downtime Plans

- ☐ Confirm what systems and data are backed up, how often backups run, and how quickly key systems can be restored.
- ☐ Test recovery for EHR-related files, patient documents, billing data, shared files, email, and critical administrative records.
- ☐ Review downtime procedures for scheduling, documentation, communication, prescriptions, billing, and patient follow-up.
- ☐ Run a tabletop discussion for ransomware, EHR outage, internet outage, vendor incident, and phone system failure.
- ☐ Assign follow-up owners for any gaps found during backup testing or downtime planning.

Decide What to Fund, Phase, & Monitor

- ☐ Mark each technology need as fund this year, phase over time, or monitor for future risk.
- ☐ Prioritize investments that protect patient access, EHR availability, secure communication, HIPAA readiness, and staff capacity.
- ☐ Assign owners, timelines, budget estimates, and success measures to approved items.
- ☐ Review the technology roadmap quarterly with leadership, operations, compliance, finance, and IT.



TECHNOLOGY BUDGETING CHECKLIST FOR **FINANCIAL SERVICES**

*A Board-Ready Planning Tool for Client Trust
& Risk Stewardship*



TECHNOLOGY BUDGETING CHECKLIST FOR FINANCIAL SERVICES



Start With Client Trust Infrastructure

- ☐ List the systems that support client relationships, including CRM, planning platforms, email, portals, phones, file storage, and meeting tools. ¹
- ☐ Identify the systems that affect client response time, account service, document access, reporting, or records if unavailable for one business day.
- ☐ Map where sensitive client information is stored, shared, archived, backed up, and disposed of.
- ☐ Confirm which systems support confidentiality, integrity, and availability of sensitive data.



Protect Advisor Productivity

- ☐ Review whether advisors can reliably access client records, planning tools, communications, and meeting platforms from approved devices and locations.
- ☐ Identify recurring technology issues that slow client follow-up, meeting prep, internal approvals, or account service.
- ☐ Confirm that remote work, branch access, mobile devices, and meeting tools have clear security and support standards.
- ☐ Budget for improvements that reduce friction in client service and strengthen consistency across advisors and staff.



Make Audit Readiness Budgetable

- ☐ List the policies, reports, logs, access reviews, and vendor records the firm may need during audits, exams, insurance reviews, or client diligence.
- ☐ Confirm who owns evidence for access management, incident response, backups, encryption, data retention, and vendor oversight.
- ☐ Review whether current systems can produce evidence quickly and consistently.
- ☐ Budget for documentation, reporting, log retention, and compliance support where evidence depends on manual follow-up.

TECHNOLOGY BUDGETING CHECKLIST FOR FINANCIAL SERVICES

Review Access Management



- ☐ Review access for staff, advisors, contractors, vendors, and former employees across client systems, email, file storage, portals, and admin tools.
- ☐ Confirm that MFA is active for sensitive systems, remote access, email, and administrative accounts.
- ☐ Document onboarding, role changes, and off-boarding steps for every system that contains client or firm data.
- ☐ Schedule periodic permission reviews with compliance, operations, and system owners.

Budget for Cybersecurity Controls



- ☐ Review protections for phishing, account takeover, ransomware, fraudulent wires, vendor breaches, and data loss.
- ☐ Confirm coverage for endpoint security, patching, email protection, vulnerability management, encryption, backup protection, and staff training.
- ☐ Align budget priorities with the firm's cybersecurity risk assessment and written supervisory or compliance programs.
- ☐ Set funding for tabletop exercises, incident response updates, and remediation items from recent reviews.

Manage Vendor and Service Provider Risk



- ☐ Inventory vendors that store, transmit, process, support, or access customer information.
- ☐ Review service provider contracts for security responsibilities, breach notification, data access, backup, retention, and exit requirements.
- ☐ Confirm who tracks vendor due diligence, insurance, audit reports, and renewal dates.
- ☐ Budget for vendor review time, documentation, and support around critical third-party systems.

TECHNOLOGY BUDGETING CHECKLIST FOR FINANCIAL SERVICES

Strengthen Client Data Protection



- ☐ Identify where customer records, communications, statements, reports, tax documents, and personal information are created and retained.
- ☐ Review disposal, archiving, and retention procedures for electronic files, old devices, shared folders, and legacy systems.
- ☐ Confirm encryption, access controls, and secure transfer methods for sensitive customer information.
- ☐ Budget for data cleanup, secure file structure, record keeping improvements, or migration support where needed.

Plan Lifecycle & Integration Improvements



- ☐ List aging endpoints, file structures, phone systems, network gear, portals, and legacy applications that support client work.
- ☐ Identify systems that coexist with newer CRM, planning, trading, or reporting platforms and create duplicate work.
- ☐ Review upcoming renewals, hardware warranties, support deadlines, and platform changes before the budget is finalized.
- ☐ Budget for lifecycle refreshes that protect client experience, evidence, and support efficiency.

Test Incident Response & Continuity



- ☐ Confirm the firm has written incident response procedures for unauthorized access to or use of customer information.
- ☐ Review customer notification, service provider coordination, and legal or compliance escalation steps with the right internal owners.
- ☐ Test restoration of client records, email, file shares, phones, portals, and critical applications.
- ☐ Run a tabletop discussion for account takeover, ransomware, vendor incident, email compromise, and system outage.

TECHNOLOGY BUDGETING CHECKLIST FOR FINANCIAL SERVICES

Clarify Support Ownership

- ☐ Identify which technology responsibilities belong to operations, compliance, advisors, vendors, internal IT, and outside support.
- ☐ Document recurring exceptions, shared-account practices, unsupported workflows, and one-off workarounds that create risk.
- ☐ Define escalation paths for urgent client-service issues, security events, vendor outages, and after-hours support.
- ☐ Decide where a co-managed support model could improve accountability, response time, and planning discipline.

Decide What to Fund, Phase, & Monitor

- ☐ Mark each technology need as fund this year, phase over time, or monitor for future risk.
 - ☐ Prioritize investments that protect client trust, advisor productivity, audit evidence, secure communications, and resilience.
 - ☐ Assign owners, due dates, budget estimates, and success measures to approved items.
- Review the roadmap quarterly with leadership, operations, compliance, finance, and IT.



TECHNOLOGY BUDGETING CHECKLIST FOR **MANUFACTURING**

*A Leadership-Ready Planning Tool
for Operational Resilience*



TECHNOLOGY BUDGETING CHECKLIST FOR MANUFACTURING

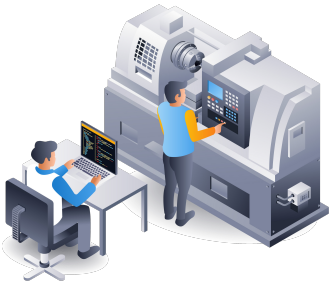
Start with Production-Critical Systems

- ☐ List the systems that keep production moving, including ERP, MRP, inventory, scheduling, quality, shipping, email, file storage, and phones. **1**
- ☐ Identify the shop-floor equipment, control systems, scanners, sensors, and workstations that depend on network connectivity.
- ☐ Name the systems that would affect orders, throughput, quality records, or customer delivery if unavailable for one shift.
- ☐ Assign an internal owner and support contact for each critical system.



Connect IT Spend to Throughput

- ☐ Map each technology request to uptime, production visibility, quality, shipping, supplier response, or customer commitments.
- ☐ Identify technology items that protect revenue-producing work, including ERP access, network reliability, backups, and endpoint support.
- ☐ Document where technology delays create manual work, rework, overtime, WIP visibility gaps, or delivery pressure.
- ☐ Create a budget summary that connects technology spend to operational risk and customer commitments.



Review ERP, MRP, Inventory, Quality, & Shipping

- ☐ Confirm that ERP, MRP, inventory, quality documentation, label printing, EDI, and shipping systems have clear support paths.
- ☐ Test whether teams can access production schedules, BOMs, work orders, customer specs, and shipment data during a system issue.
- ☐ Review integrations between office systems, shop-floor systems, customer portals, and vendor platforms.
- ☐ Budget for upgrades or support where manual entry, duplicate work, or system delays slow operations.



TECHNOLOGY BUDGETING CHECKLIST FOR **MANUFACTURING**



Map IT & OT Connectivity

- ☐ Create a simple map of office networks, production networks, wireless coverage, internet connections, remote access, and vendor connections.
- ☐ Identify where machines, PLCs, HMIs, cameras, sensors, or industrial control systems communicate with business systems.
- ☐ Review which systems should be segmented into security zones based on operational importance and risk.
- ☐ Validate access paths between office IT, production systems, and vendor support connections.

Plan Equipment Lifecycle

- ☐ Create a refresh list for network gear, servers, shop-floor PCs, rugged devices, barcode scanners, Wi-Fi, backups, UPS equipment, and endpoints.
- ☐ Review unsupported operating systems, aging switches, older firewalls, shared workstations, and legacy line-of-business tools.
- ☐ Add technology requirements to capital equipment purchases, including power, network, cybersecurity, vendor access, maintenance, and data ownership.
- ☐ Build planned replacement costs into the budget before operational demand or vendor end-of-support forces a rushed decision.



Strengthen Security Evidence

- ☐ Identify customer, insurance, supply chain, defense-adjacent, or regulatory requirements that require cybersecurity evidence.
- ☐ Review documentation for MFA, backups, endpoint protection, patching, incident response, and access controls.
- ☐ Complete a gap assessment or self-assessment using a recognized manufacturing cybersecurity framework (like **CMMC**).
- ☐ Create a plan of action for controls, documentation, and milestones that support customer confidence and contract readiness.



TECHNOLOGY BUDGETING CHECKLIST FOR MANUFACTURING

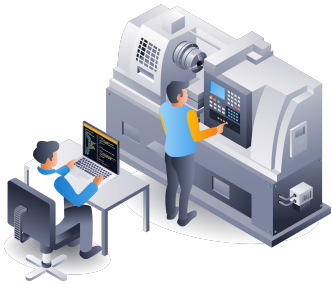


Budget For Ransomware & Vulnerability Resilience

- ☐ Review patch status for internet-facing systems, servers, endpoints, remote access tools, and critical applications.
- ☐ Set maintenance windows for updates that affect production systems, shop-floor workstations, or vendor-managed equipment.
- ☐ Verify that backups are protected, tested, and able to restore ERP, quality records, file shares, and critical production data.
- ☐ Include employee training, MFA, endpoint detection, and incident response practice in the budget.

Clarify Support Ownership

- ☐ Identify who coordinates technology vendors during production issues, system outages, machine connectivity problems, and after-hours events.
- ☐ Define escalation paths for office IT, shop-floor technology, ERP support, automation vendors, and internet providers.
- ☐ Document recurring issues that pull operations, finance, or production leaders into troubleshooting.
- ☐ Decide which support should stay internal, which needs vendor ownership, and which could benefit from a fully managed or co-managed IT partner.



Plan For Industry 4.0

- ☐ Identify planned automation, robotics, sensor, AI, analytics, or connected equipment projects for the next budget cycle.
- ☐ Confirm that each project includes cybersecurity, network capacity, data storage, support, training, and lifecycle costs.
- ☐ Review whether production data can improve quality, forecasting, maintenance, and continuous improvement.
- ☐ Budget for the infrastructure needed to make smart manufacturing investments stable and secure.



TECHNOLOGY BUDGETING CHECKLIST FOR **MANUFACTURING**

Test Continuity & Recovery

- ☐ Define recovery priorities for ERP, MRP, inventory, scheduling, quality, shipping, internet, phones, and file access.
- ☐ Run a tabletop discussion for ransomware, internet outage, ERP outage, vendor failure, and shop-floor network disruption.
- ☐ Confirm who communicates with employees, customers, carriers, suppliers, and leadership during a disruption.
- ☐ Schedule a follow-up review for any gaps found during backup tests or tabletop discussions.

Decide What to Fund, Phase, & Monitor

- ☐ Mark each technology need as: fund this year, phase over time, or monitor for future risk.
- ☐ Prioritize investments that protect uptime, production visibility, customer delivery, cybersecurity evidence, and employee productivity.
- ☐ Assign owners, due dates, and budget estimates to approved items.
- ☐ Review the technology roadmap each quarter so operational changes stay connected to the budget.



TECHNOLOGY BUDGETING CHECKLIST FOR LEGAL FIRMS

*A Partner-Ready Planning Tool for Billable Time
& Client Trust*



TECHNOLOGY BUDGETING CHECKLIST FOR **LEGAL FIRMS**



Start With Matter-Critical Systems

- ☐ List the systems that support matter management, document management, time entry, billing, email, phones, remote access, file sharing, and client communication.
- ☐ Identify which systems would affect attorney productivity, matter deadlines, document access, or client responsiveness if unavailable for one business day.
- ☐ Map where client files, privileged communications, financial records, case materials, and administrative documents are stored and shared.
- ☐ Assign an owner and support path for every system the firm depends on to keep legal work moving.

Protect Billable Productivity

- ☐ Identify recurring technology issues that interrupt time entry, document drafting, calendaring, research, e-signature, or client follow-up.
- ☐ Estimate how much attorney and staff time is lost each month to slow systems, workarounds, password issues, or vendor follow-up.
- ☐ Review whether attorneys can work reliably from approved devices, offices, court, home, and client sites.
- ☐ Budget for improvements that reduce friction in billable work and protect the firm from avoidable emergency spend.



Review Document & Email Reliability

- ☐ Confirm that document management, email, scanning, templates, PDFs, e-signature, and shared files have clear support ownership.
- ☐ Identify where version confusion, duplicate files, slow search, or inconsistent naming creates risk or rework.
- ☐ Review whether attorneys and staff can access the right files securely without relying on personal storage or informal workarounds.
- ☐ Budget for cleanup, migration, permissions review, or training where document workflows slow matter progress.



TECHNOLOGY BUDGETING CHECKLIST FOR **LEGAL FIRMS**



Protect Client Confidentiality

- ☐ Review access controls for client files, privileged communications, financial records, HR files, and administrative systems.
- ☐ Confirm that MFA is enabled for email, remote access, document systems, practice management platforms, and administrative accounts.
- ☐ Document how access is added, changed, reviewed, and removed when attorneys, staff, vendors, or contractors transition.
- ☐ Budget for security controls that protect client trust and support the firm's professional responsibility around technology.

Manage Vendor & Platform Risk

- ☐ Inventory vendors that store, transmit, support, or access client information, firm records, or critical systems.
- ☐ Review contracts and vendor responsibilities for security, breach notification, backup, support, data ownership, and exit planning.
- ☐ Confirm who tracks renewals, platform changes, support contacts, and security documentation for each vendor.
- ☐ Budget for vendor review time around practice management, billing, document management, research, e-discovery, and client portal tools.



Plan Lifecycle Across the Firm

- ☐ List aging laptops, desktops, phones, scanners, printers, network gear, firewalls, Wi-Fi, backup systems, and legacy applications.
- ☐ Identify unsupported systems, shared workstations, outdated operating systems, and tools dependent on one internal expert.
- ☐ Review upcoming warranties, renewals, support deadlines, platform changes, and equipment replacement needs.
- ☐ Build planned refreshes into the budget before outdated technology affects deadlines, client service, or attorney productivity.



TECHNOLOGY BUDGETING CHECKLIST FOR LEGAL FIRMS



Manage Vendor & Business Associate Risk

- ☐ Inventory vendors and business associates that store, transmit, process, support, or access ePHI.
- ☐ Review agreements for security responsibilities, breach notification, access expectations, backup requirements, and data handling.
- ☐ Confirm who tracks vendor contacts, renewal dates, security documentation, and incident escalation steps.
- ☐ Budget for vendor review time and support around EHR, billing, imaging, telehealth, patient portal, and practice management systems.

Plan Lifecycle Across the Firm

- ☐ List aging laptops, desktops, phones, scanners, printers, network gear, firewalls, Wi-Fi, backup systems, and legacy applications.
- ☐ Identify unsupported systems, shared workstations, outdated operating systems, and tools dependent on one internal expert.
- ☐ Review upcoming warranties, renewals, support deadlines, platform changes, and equipment replacement needs.
- ☐ Build planned refreshes into the budget before outdated technology affects deadlines, client service, or attorney productivity.



Prepare For Continuity & Recovery

- ☐ Confirm what systems and files are backed up, how often backups run, and how quickly key systems can be restored.
- ☐ Test recovery for client files, email, billing records, matter data, shared folders, and administrative documents.
- ☐ Review how the firm would continue working during a ransomware event, internet outage, email outage, vendor failure, or office closure.
- ☐ Assign communication owners for attorneys, staff, clients, courts, vendors, and firm leadership during a disruption.



TECHNOLOGY BUDGETING CHECKLIST FOR **LEGAL FIRMS**

Budget For Adoption & Training

- ☐ Identify where attorneys and staff need training to use existing systems more consistently.
- ☐ Include staff feedback when evaluating tools that affect daily legal work, client communication, or document workflows.
- ☐ Budget time for onboarding, documentation, role-specific training, and process updates when tools change.
- ☐ Review whether new technology is actually reducing work, improving visibility, or creating another layer of complexity.

Decide What to Fund, Phase, & Monitor

- ☐ Mark each technology need as fund this year, phase over time, or monitor for future risk.
- ☐ Prioritize investments that protect billable time, client confidentiality, matter continuity, document access, and firm resilience.
- ☐ Assign owners, timelines, budget estimates, and success measures to approved items.
- ☐ Review the technology roadmap quarterly with firm leadership, finance, operations, practice leaders, and IT.



TECHNOLOGY BUDGETING CHECKLIST FOR INSURANCE

*A Board-Ready Planning Tool for Client Trust
& Service Continuity*

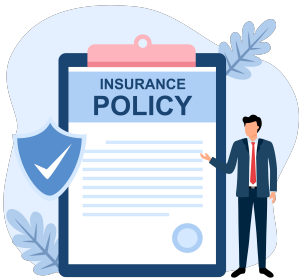


TECHNOLOGY BUDGETING CHECKLIST FOR **INSURANCE**



Start with Client Service Systems

- ☐ List the systems that support quoting, policy servicing, claims support, renewals, document access, payments, email, phones, and client communication. ¹
- ☐ Identify which systems would affect client response time, producer productivity, or carrier follow-up if unavailable for one business day.
- ☐ Map where client, policy, claims, payment, health, and commercial information is stored, shared, archived, and backed up.
- ☐ Assign an owner and support path for every client-service system the agency depends on.



Protect Quoting & Policy Servicing

- ☐ Review whether producers and service teams can reliably access rating tools, agency management systems, carrier portals, files, and client notes.
- ☐ Identify recurring technology issues that slow quotes, policy changes, claims support, certificates, renewals, or client follow-up.
- ☐ Confirm that remote work, branch access, mobile devices, and meeting tools have clear security and support standards.
- ☐ Budget for improvements that reduce duplicate entry, service bottlenecks, and delays across the client service chain.

Review Carrier Access & Integrations

- ☐ List carrier portals, comparative raters, downloads, scanning workflows, e-signature tools, document systems, and data integrations.
- ☐ Confirm who owns credentials, MFA, portal access, vendor contacts, and support requests for each carrier or platform connection.
- ☐ Identify where fragmented systems create manual work, missed updates, duplicate records, or inconsistent client service.
- ☐ Budget for integration cleanup, vendor support, automation, or workflow improvements where service teams lose time.

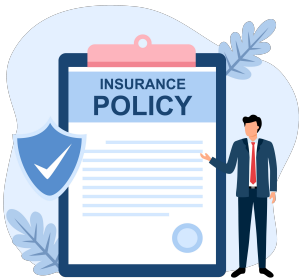


TECHNOLOGY BUDGETING CHECKLIST FOR **INSURANCE**



Protect Client & Business Data

- ☐ Identify sensitive personal, commercial, financial, health, and claims information across agency systems and shared files.
- ☐ Review access controls for producers, service teams, operations, vendors, former employees, and shared accounts.
- ☐ Confirm MFA, encryption, secure file transfer, and backup protection for systems that contain client information.
- ☐ Review retention and disposal practices for old files, archived records, retired devices, shared folders, and legacy systems.



Budget for Security Program Needs

- ☐ Confirm the agency has written cybersecurity or information security policies appropriate to its size, systems, and data sensitivity.
- ☐ Review risk assessment findings and identify which safeguards need budget support this year.
- ☐ Assign a named owner for security program oversight, vendor coordination, documentation, and follow-through.
- ☐ Budget for monitoring, testing, vulnerability review, employee training, access reviews, and incident response practice.



Manage Vendor Accountability

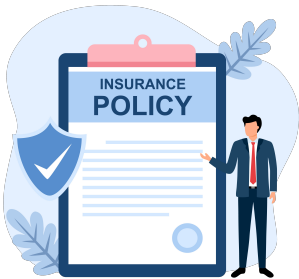
- ☐ Inventory vendors that store, transmit, process, support, or access client and agency information.
- ☐ Review vendor agreements for security responsibilities, breach notification, data handling, backups, access, and exit requirements.
- ☐ Confirm who tracks vendor renewals, insurance, support contacts, security documentation, and platform changes.
- ☐ Budget for vendor review time and support around critical systems, carrier tools, and service platforms.

TECHNOLOGY BUDGETING CHECKLIST FOR INSURANCE



Clarify Support Ownership

- ☐ Identify who currently handles password resets, carrier portal issues, device problems, software questions, and vendor follow-up.
- ☐ Estimate how much time service teams, operations leaders, and producers spend coordinating technology support.
- ☐ Define escalation paths for urgent client service issues, system outages, vendor incidents, and after-hours support.
- ☐ Decide where a co-managed support model could improve accountability, response time, and planning discipline.



Plan Lifecycle Across the Agency

- ☐ List aging endpoints, phones, scanners, printers, network gear, firewalls, Wi-Fi, backup systems, and legacy applications.
- ☐ Review unsupported systems, shared workstations, outdated file structures, and tools that depend on one internal expert.
- ☐ Compare renewal dates, warranties, support deadlines, and platform changes before the budget is finalized.
- ☐ Budget for lifecycle refreshes that protect client service, security evidence, and staff productivity.

Test Continuity & Incident Response

- ☐ Define recovery priorities for agency management systems, files, email, phones, carrier access, payment tools, and client records.
- ☐ Test whether backups can restore critical files, policy documents, client records, and service workflows.
- ☐ Run a tabletop discussion for ransomware, email compromise, vendor outage, carrier portal disruption, and system failure.
- ☐ Confirm who communicates with employees, clients, carriers, vendors, and leadership during a disruption.



TECHNOLOGY BUDGETING CHECKLIST FOR **INSURANCE**



Decide What to Fund, Phase, & Monitor

- ☐ Mark each technology need as fund this year, phase over time, or monitor for future risk.
- ☐ Prioritize investments that protect client responsiveness, carrier access, data protection, producer productivity, and service consistency.
- ☐ Assign owners, due dates, budget estimates, and success measures to approved items.
- ☐ Review the technology roadmap quarterly with leadership, operations, service, finance, and IT.



TECHNOLOGY BUDGETING CHECKLIST FOR NONPROFITS

A Board-Ready Planning Tool for Mission Stewardship



TECHNOLOGY BUDGETING CHECKLIST FOR NONPROFITS

Start with Mission-Critical Systems



- ☐ List the systems your team relies on to deliver programs, raise funds, communicate with constituents, manage finances, and report outcomes.
- ☐ Identify which systems would disrupt services, donations, payroll, reporting, or board communication if they became unavailable for one business day.
- ☐ Name the staff, vendors, and volunteers who know how each critical system works.
- ☐ Confirm where key organizational data lives, including donor records, program records, financial files, HR data, and board materials.
- ☐ Decide which systems need funding this year to protect day-to-day mission continuity.

Connect Technology Spend to Outcomes



- ☐ Translate each major technology need into the mission function it supports.
- ☐ Identify which budget requests support program delivery, donor trust, reporting accuracy, staff capacity, cybersecurity, or community access.
- ☐ Prepare a simple board explanation for why each technology investment is stewardship of mission resources.
- ☐ Document how better systems could help staff serve more people, report faster, reduce manual work, or improve donor engagement.
- ☐ Separate essential resilience investments from future improvements, so decision-makers can prioritize clearly.

Plan For Equipment & System Lifecycle



- ☐ Create a refresh list for laptops, desktops, tablets, servers, firewalls, Wi-Fi equipment, phones, printers, and backup hardware.
- ☐ Identify devices that are past warranty, unsupported, donated without a support path, or shared by multiple staff members.
- ☐ Decide which equipment should be replaced this year and which can be responsibly planned for a future budget cycle.
- ☐ Build a recurring lifecycle line item instead of relying on emergency purchases when equipment fails.
- ☐ Confirm whether grant-funded equipment has replacement, support, and ownership requirements after the grant period ends.

TECHNOLOGY BUDGETING CHECKLIST FOR **NONPROFITS**

Surface Hidden Staff Time

- ☐ List the people who currently handle password resets, vendor follow-up, software questions, onboarding, troubleshooting, and device issues.
- ☐ Estimate how many staff hours per month are spent on technology coordination outside formal job responsibilities.
- ☐ Identify recurring issues that pull finance, operations, development, or program leaders away from higher-value work.
- ☐ Decide which support tasks should stay internal, which should be documented, and which need outside support.
- ☐ Budget for the support model that gives staff reliable help and gives leadership visibility into recurring problems.



Protect Donor & Constituent Trust

- ☐ Confirm that donor records, payment information, HR files, program records, and board documents have appropriate access controls.
- ☐ Review who has access to fundraising, finance, payroll, email marketing, file storage, and donation platforms.
- ☐ Enable multi-factor authentication for staff, board members, vendors, and volunteers who access sensitive systems.
- ☐ Document how access is added, changed, and removed when staff, board members, volunteers, or vendors transition.
- ☐ Budget for security improvements that protect donor confidence and support board accountability.



Strengthen Data Governance & Reporting

- ☐ Identify duplicate, outdated, inconsistent, or hard-to-report data across donor, program, finance, and communication systems.
- ☐ Assign clear ownership for the data each department collects and uses.
- ☐ Decide what data should be retained, archived, deleted, or restricted.
- ☐ Review whether current systems can produce the reports needed for grants, board meetings, audits, fundraising, and program decisions.
- ☐ Budget for data cleanup, system integration, documentation, or reporting improvements where staff currently rely on manual workarounds.



TECHNOLOGY BUDGETING CHECKLIST FOR **NONPROFITS**



Review Software Renewals & Tool Sprawl

- ☐ Build a renewal calendar for every software subscription, platform, domain, security tool, and vendor agreement.
- ☐ Identify tools purchased by individual departments, funded through grants, added during urgent projects, or used by only a few people.
- ☐ Compare license counts with actual usage before renewing.
- ☐ Decide which tools should be renewed, consolidated, replaced, or retired.
- ☐ Confirm who owns each vendor relationship and who receives renewal, billing, and security notices.



Test Backup, Recovery, & Continuity Plans

- ☐ Confirm what systems and files are backed up, how often backups run, and where backups are stored.
- ☐ Test whether key files, email, donor data, financial data, and program records can be restored.
- ☐ Define who leads technology decisions during an outage, cyber incident, vendor failure, or office closure.
- ☐ Prepare a short communication plan for staff, board members, donors, funders, and constituents during a technology disruption.
- ☐ Budget for backup testing, documentation, recovery planning, and support before an urgent event forces rapid decisions.



Include Website, Email, & Donation Experience

- ☐ Test the online donation process from start to finish on desktop and mobile.
- ☐ Confirm that donation forms, event registrations, volunteer forms, and contact forms route to the right staff members.
- ☐ Review website accessibility, mobile usability, page speed, domain security, and form reliability.
- ☐ Check email deliverability settings so donor, funder, and constituent communications reach inboxes consistently.
- ☐ Budget for website maintenance, donation flow improvements, accessibility updates, and digital communication support.

TECHNOLOGY BUDGETING CHECKLIST FOR NONPROFITS



Plan For Grants, Restrictions, & Funder Conversations

- ☐ Identify technology needs that can be included directly in program, capacity-building, infrastructure, or evaluation grants.
- ☐ Prepare language that connects technology funding to service delivery, reporting, equity, and organizational resilience.
- ☐ Review whether restricted grants create technology costs that will continue after the funding period.
- ☐ Ask whether funders will support implementation, training, data cleanup, maintenance, security, or staff capacity around new tools.
- ☐ Create a list of technology needs that require unrestricted funding, board-designated reserves, or phased investment.



Support Staff Adoption & Training

- ☐ Identify where staff need training to use existing systems more confidently.
- ☐ Budget time and funding for onboarding, documentation, refreshers, and role-specific training.
- ☐ Assign owners for keeping technology procedures current.
- ☐ Review whether staff have the devices, access, connectivity, and support they need for remote, field, hybrid, or community-based work.
- ☐ Include change management time when budgeting for any new platform, migration, or major workflow update.



Prepare For AI, Automation, & New Tools

- ☐ Decide which AI and automation uses are appropriate for your organization's mission, data, and staff roles.
- ☐ Create basic guidance for what organizational, donor, HR, financial, and constituent data can be entered into AI tools.
- ☐ Assign an owner to review new technology requests before teams add disconnected tools.
- ☐ Budget for governance, training, and review before adopting tools that affect communications, data, decision-making, or service delivery.
- ☐ Track where automation could reduce repetitive work while keeping staff oversight in place.

TECHNOLOGY BUDGETING CHECKLIST FOR **NONPROFITS**

Give The Board a Clear Decision Framework

- ☐ Sort technology needs into three categories: fund this year, phase over time, and monitor for future risk.
- ☐ Name the risk of delaying each major item in practical terms, such as staff time, service disruption, donor confidence, reporting burden, or replacement cost.
- ☐ Identify which decisions need board approval, finance approval, staff input, or vendor review.
- ☐ Create a one-page technology budget summary for board discussion.
- ☐ End the budgeting conversation with owners, timelines, next steps, and a review date.



Plan Wisely with **Mainstay**

Technology budgeting can feel complex when your expertise is leading the organization, serving clients, supporting staff, or protecting the people who depend on you.

Mainstay helps New England business leaders turn all those moving pieces into a practical and right-sized plan. Our service agreements include IT strategic planning and consulting, with recommendations for scheduled equipment replacement, security optimization, technology improvements, and smarter use of the tools your team already depends on.

If you're ready to build a more strategic technology budget, let's talk about what to fund, what to phase, and what your organization should plan for next!

Scan the QR code,
or visit mstech.com

