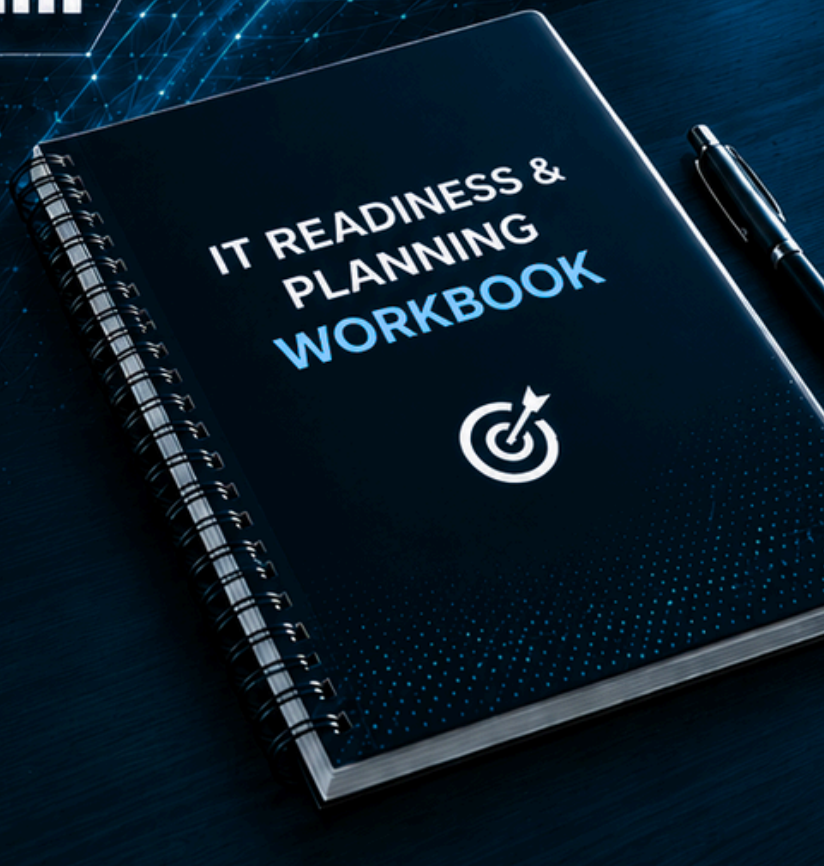
IT READINESS & PLANNING WORKBOOK

BUILD A STRONGER, SMARTER BUSINESS BEFORE NEXT YEAR BEGINS

Help business leaders evaluate their current business readiness, identify hidden operational and technology risks, prioritize improvements, and build a practical roadmap for the next 12 months.

Unlike a traditional IT guide, this workbook focuses on business decisions—not technical decisions.



NEWAVE SOLUTIONS

— CONTENTS

What's Inside This Workbook

01	Welcome	Why IT readiness is a leadership responsibility
02	Executive Readiness	Assess where your business stands today
03	Business Goals	Set direction before evaluating technology
04	Business Risk	Map dependencies beyond cybersecurity
05	Security Culture	Build everyday habits, not just annual training
06	Vendor Evaluation	Judge partners on value, not just price
07	Budget Planning	Invest in outcomes, not just line items
08	Technology Lifecycle	Get ahead of aging systems and technical debt
09	Business Continuity	Prepare for a confident recovery
10	Cyber Readiness	Reduce uncertainty before an incident hits
11	12-Month Roadmap	Turn priorities into a quarterly plan
12	Executive Action Plan	Assign ownership and timelines
13	Readiness Scorecard	Bring every assessment together
14	Next Steps	Make readiness an annual habit

WHAT YOU'LL ACCOMPLISH

- A clear, honest picture of how ready your business is today — across leadership visibility, cybersecurity, continuity, vendors, budget, and technology planning.
- A shared understanding, built with your leadership team, of which business goals should shape your technology decisions over the next 12 months.
- A practical, quarter-by-quarter roadmap with assigned owners, timelines, and the business outcomes each initiative is meant to support.

SECTION 1

Welcome: Why IT Readiness Is a Leadership Responsibility



Is your business ready for what comes next?

To be more specific… *How confident are you that your business could achieve its biggest goals if your technology stayed exactly as it is today?*

I can see how that might sound like an IT question, but I promise it's not. It's actually more focused on leadership.

Every major business objective now depends on technology in one way or another. Whether it's growing revenue, improving customer service, expanding operations, or supporting employees, you'll find some kind of technology right in the middle of it.

Whether you realize it or not, technology now influences nearly every business decision you make.

Technology no longer simply supports the business. It enables it.

That doesn't mean every executive needs to become a tech expert. But it does mean leadership should understand how technology affects business performance, operational resilience, financial planning, and long-term growth.

The strongest organizations don't start with technology. They start with business goals and then make sure they have technology that's ready to support them.



That's exactly why this workbook exists.

This isn't a technical manual or an IT checklist… let's make that very clear. Instead, it's an **executive planning workbook designed to help you ask better business questions,** evaluate where your organization stands today, and build a practical roadmap for the next 12 months.

As you work through each section, focus less on finding the "right" answers and more on having meaningful conversations. Complete the exercises during your annual planning sessions, revisit them during quarterly business reviews, and update your priorities as your business evolves.

By the end of this workbook, you'll have more than a list of technology projects. You'll have a clearer understanding of how your business goals, operational priorities, and technology investments work together to support future success.

Leadership Reflection



But wait, before we dive in, we think you'll find it helpful to sit down with your leadership team and discuss these questions:

1 What are our three biggest business priorities this year?

2 What worries leadership the most?

3 Where do we believe technology helps us the least?

SECTION 2

Executive Business Readiness Assessment



Let’s now go back to our earlier question: How ready is your business, really?

If someone asked you how prepared your business is for the next 12 months, how would you answer?

Most leaders have a general sense of where things stand. But being confident isn't always the same as being ready. You might feel great about how everything is right now as you know it, but what about the risks you’re not yet aware of? That’s where the biggest danger usually lies.

And that’s why this assessment exists.

Let’s be clear that this isn't designed to test your technical knowledge or identify perfect answers. There’s no point in that…you’re a business owner after all, not an IT person.

Instead, it's an opportunity to step back, look at your business from a leadership perspective, and uncover areas that may deserve more attention.

As you go through each category, don't stress about whether your organization is "doing everything right." Focus on whether you have enough visibility and confidence to make informed business decisions. If you're unsure about an answer, that also says a lot, and it’s considered valuable insight in itself.

Before you go ahead and complete the **Executive Readiness Scorecard,** gather your leadership team and have an honest discussion of the following questions.

Leadership Visibility

- Do we clearly understand the technology-related risks that could affect our business?
- Do we make our tech decisions based on business priorities, or are they mostly reactive?

Cybersecurity

- How confident are we that we could detect and respond to today's most likely cyber threats?
- Do we have real evidence that our security measures are working, or are we just assuming they do?

Business Continuity

- If a major disruption occurred tomorrow, could we continue serving our customers?
- Have we done a full test of our continuity and recovery plans within the past year?

Vendor Management

- Do we know which vendors are critical to our day-to-day operations?
- Are our vendors helping us achieve our business goals, or are they adding unnecessary risk and complexity?

Employee Awareness

- Do our employees understand their role in protecting the business?
- Have we created a culture where people feel confident identifying and reporting potential issues?

Budget Planning

- Does our tech budget support our business strategy, or does it usually go towards surprise fixes and emergencies?
- Are we investing proactively, or simply reacting when something breaks?

Technology Planning

- Do we have a roadmap for future technology investments?
- Are today's technology decisions helping us reach tomorrow's business goals?

Operational Resilience

- Could our business continue operating if a key system or process became unavailable?
- Have we identified our biggest operational dependencies before they become business problems?

Future Readiness

- Are we preparing for where the business is going, not just where it is today?
- Do we regularly review whether our technology can support future growth and changing business needs?

Leadership Exercise

Now, complete the **Executive Readiness Scorecard** by rating each category from **1 (Needs Significant Improvement) to 5 (Highly Confident).**

CATEGORY	1 Needs Significant Improvement	2 Needs Improvement	3 Moderately Confident	4 Confident	5 Highly Confident
Leadership Visibility	○	○	○	○	○
Cybersecurity	○	○	○	○	○
Business Continuity	○	○	○	○	○
Vendor Management	○	○	○	○	○
Employee Awareness	○	○	○	○	○
Budget Planning	○	○	○	○	○
Technology Planning	○	○	○	○	○
Operational Resilience	○	○	○	○	○
Future Readiness	○	○	○	○	○

Don't overthink your answers. Your initial score often highlights where the greatest opportunities for improvement exist. There's no such thing as a perfect score here, so don't aim for one. Your goal is simply to create a clear starting point for meaningful discussions and smarter planning.

SECTION 3

Business Goals Before Technology Goals

Think back to the last time your leadership team discussed technology. Was the conversation about software and hardware, or about the future of your business?

Too often, organizations invest in new technology before clearly defining what they want to achieve. You know how it goes… every time a brand-new tool comes out, you see all the other companies getting it, then FOMO kicks in, so you jump in and get it as well.

The result? You find yourself owning a collection of tools that may solve individual problems but don't always move the business closer to its long-term goals.

The most successful technology strategies don't begin with technology. They begin with a clear understanding of where the business is headed.

And so the real question is: *are you planning your technology, or your business?*

Before considering new systems, upgrades, or investments, ask yourself what success looks like over the next 12 months. Are you focused on increasing revenue? Expanding into new markets? Improving customer service? Hiring more employees? Streamlining operations? These business priorities should guide every technology decision that follows.

Technology is most valuable when it helps solve a specific business challenge or creates a measurable opportunity.

Instead of asking, *"What technology should we buy?"* ask, *"What business outcome are we trying to achieve?"* With that simple shift in perspective, you'll soon be making smarter investments and seeing better long-term results.



Earlier this year, we gave you the **AI Business Playbook,** which explores how emerging technologies like artificial intelligence can help organizations work more efficiently and make better decisions.

But AI, like any technology, isn't a business strategy on its own. If you're evaluating AI initiatives, revisit the **Safe AI Adoption Framework** to ensure those investments support your business objectives, not the other way around.

Your Planning Session

Before evaluating any technology investments, **define the business outcomes that matter most.**

The **Business Goals Worksheet** will help you identify your organization's priorities across revenue, growth, operations, customer experience, and technology. Complete each section, then rank your priorities to create a clear foundation for the planning decisions you'll make throughout the rest of this workbook.

CATEGORY	1 Needs Significant Improvement	2 Needs Improvement	3 Moderately Confident	4 Confident	5 Highly Confident
Revenue Goals	○	○	○	○	○
Growth Goals	○	○	○	○	○
Operational Goals	○	○	○	○	○
Customer Experience Goals	○	○	○	○	○
Technology Goals	○	○	○	○	○

Priority Ranking

Write the goal categories in order of priority, from **1 (highest priority) to 5 (lowest priority).**

1 _____ 2 _____ 3 _____

4 _____ 5 _____

SECTION 4

Business Risk Assessment



The first thing that comes to mind when most leaders think about business risk is cybersecurity. Yes, that's absolutely part of it. But it's not the only part. There are plenty of other risks you should also plan for. What if your biggest disruption had nothing to do with a cyberattack? Think about these scenarios…

A key employee resigns without documenting a critical process.
A software vendor unexpectedly discontinues a service you rely on.
An important business file can't be found when you need it most.

They don't directly relate to technology, right? But for sure, each can quickly escalate into operational and financial challenges.

Business risk comes in many forms. Technology is only one piece of the picture.

Strong organizations understand how different parts of the business depend on one another. One small delay in one area can easily affect customers, employees, vendors, cash flow, and even leadership's ability to make informed decisions.

The more clearly you understand those connections, the easier it becomes to reduce unnecessary risk before it affects the business.

Also, it's very important to **challenge the assumptions** we make every day:

- Do only one or two people know how critical processes work?
- Are important vendor agreements easy to access?
- Could your leadership team continue making decisions if key systems or information suddenly became unavailable?

Asking these questions doesn't automatically mean you're a pessimist always expecting the worst. What it means is that you're working towards building a business that's resilient enough to adapt in case the unexpected does happen.

A few months back, we presented to you the **Business Continuity Blueprint,** which introduced the importance of identifying operational dependencies and preparing for disruption before it occurs.

If you'd like to explore those concepts in greater depth, it's a valuable companion resource to this workbook.

Business Continuity Blueprint

Leadership Scenario

Here's a common real-life scenario that clearly illustrates the importance of addressing all business risks, not just cybersecurity.

Let's say your operations manager is unexpectedly unavailable for several weeks. Customer orders continue to arrive, but no one else knows the approval process, where key documents are stored, or which vendor to contact when issues arise.

Your business slows, but it's not because technology failed. It's because critical knowledge wasn't shared. The business somehow became dependent on a single person. And this kind of oversight can create significant business challenges over time.

Executive Exercise

Complete the **Business Risk Assessment** below by looking beyond technology alone. As you work through the exercise, consider the people, processes, vendors, documentation, and assumptions your business depends on every day. Identifying these dependencies now is the first step toward building a more resilient organization.



Mapping What Actually Keeps Your Business Running

1. Map Your Critical Systems

Why This Matters

Most business disruptions become serious because leadership doesn't realize what depends on what until something changes or fails. This exercise helps you identify the systems your business relies on to operate, serve customers, get paid, and remain compliant.

- **Identify Your Critical Systems** - Include software, platforms, outsourced services, and shared tools. Examples may include accounting and payroll, CRM, email and collaboration, scheduling, payment processing, remote access, file storage, and industry-specific applications.

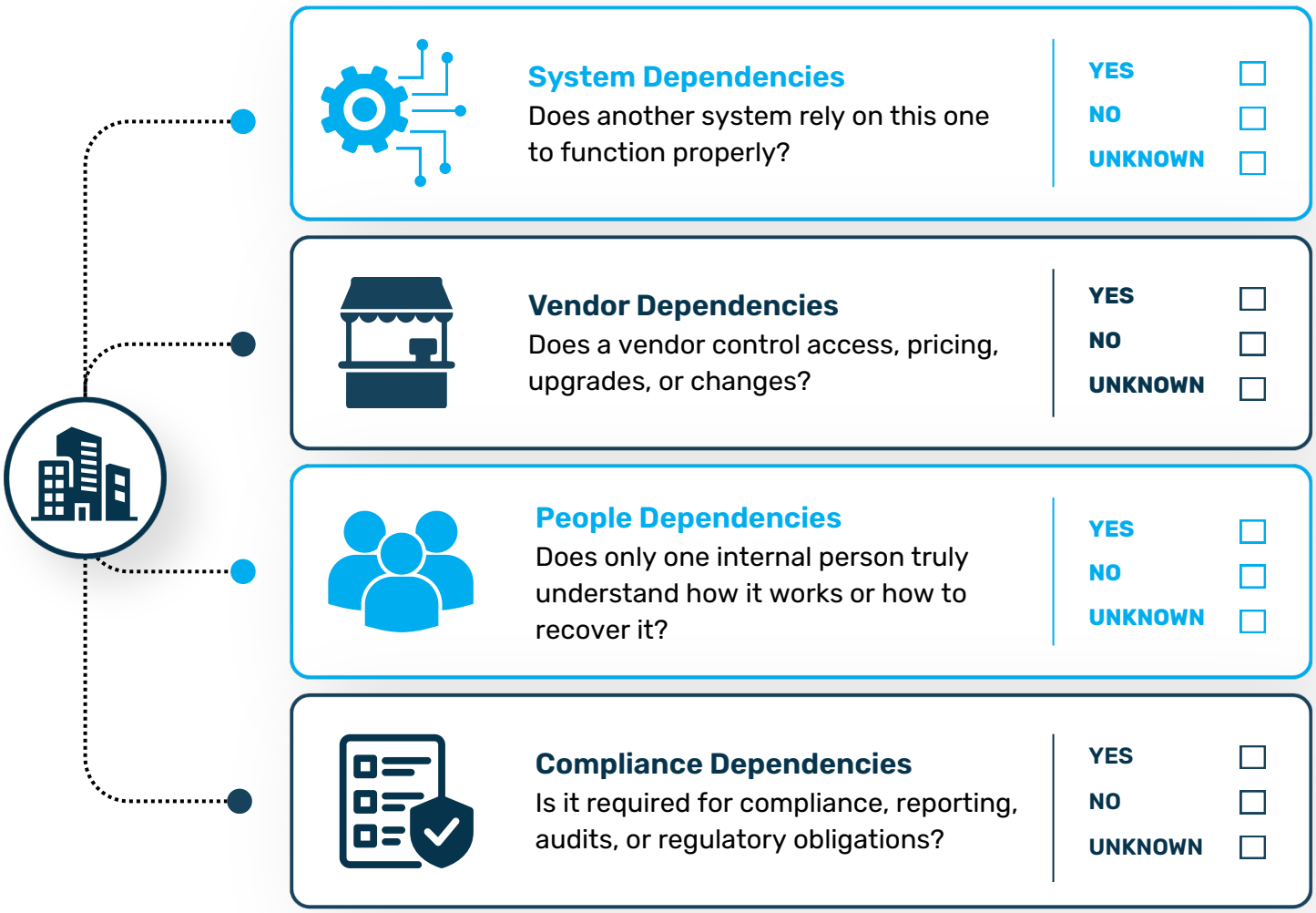
SYSTEMS	What Business Function Does IT Support?	What Stops Working If It's Down?	Who Notices First?	How Long before Impact?
Ex. Accounting Software	*Billing, Payroll, Reporting*	*Invoicing, Payroll*	*Finance Team*	*Same Day*



If you don't know the time to impact, write **"UNKNOWN."** That's a signal, not a failure.

2. Find What Your Systems Depend On

For each critical system, ask:



If you answered “yes” to any of these questions, circle or mark that system. These are not problems yet, but they are points of dependency. And dependency is where continuity risk lives.

What This Map Gives You

By the end of this exercise, you should have:

- A shared understanding of what systems are truly critical
- Visibility into where knowledge, vendors, or integrations create exposure
- Fewer assumptions about what would happen if something changed or failed

This map isn’t about fixing anything yet. It’s about replacing confidence based on habit with confidence based on understanding.

SECTION 5

Security Culture & Employee Readiness



Is security part of your company culture?

Let's say a security incident happened tomorrow. Would it be caused by technology, or by an everyday decision that someone made?

A large majority of security incidents don't really stem from sophisticated attacks. Instead, they start with ordinary moments:

- Clicking an unexpected email
- Reusing a password too many times
- Sharing sensitive information with the wrong person
- Using a new AI tool without understanding how company data is being handled

These things seem small and unremarkable. But they can be the start of a major disaster.

That's why cybersecurity doesn't just fall on the company's IT team. It's also a leadership responsibility.

If you want to build a secure business, you must **create a culture where employees understand that security is part of their everyday work.**

Sure, the company has policies, tools, and technology in place that play an important role. But they're really just effective when people know what to do, and if they feel comfortable speaking up when something doesn't seem right.

A strong security culture goes way beyond annual awareness training. It includes:

- Onboarding new employees with clear security expectations
- Removing access as soon as someone leaves the organization
- Encouraging employees to report suspicious activity without fear of blame
- Regularly reinforcing good habits

These small but consistent actions usually have a greater impact than one-time training events.

Also, leaders play a critical role by setting expectations and leading by example. When executives follow the same security protocols as everyone else, it sends a clear message that nobody's above the rules, and that protecting the business is a shared responsibility by all, not just the IT department.

Now, as artificial intelligence quickly becomes part of everyday work, companies should also set clear expectations for how AI tools can and cannot be used.

Earlier this year, we created the **AI Business Playbook** to discuss the importance of AI governance and acceptable use policies. If your organization is adopting AI, it's worth revisiting that resource to help ensure innovation supports your business while protecting sensitive information.

Leadership Scenario

A new employee joins your organization and, on their very first day, immediately receives basic login credentials. They aren't given guidance on recognizing phishing emails, using AI tools responsibly, or reporting suspicious activity. Months later, they unknowingly share sensitive information through an unapproved application.

No one intended to create a security risk. You can't really blame them either, as they weren't properly trained. In this case, the issue certainly wasn't a lack of technology. It was a lack of clear expectations and ongoing communication.

Your Next Step

As you complete the **Security Culture & Employee Readiness** worksheet, think beyond technical controls. Consider how your organization trains employees, communicates expectations, manages onboarding and offboarding, encourages reporting, and builds security into everyday business decisions.

Keep in mind that a strong security culture isn't created by a single training session. It's built through consistent leadership and everyday habits.

Security Culture & Employee Readiness Worksheet

CYBER RESILIENCE CHECKLIST

Essential security controls that reduce risk and strengthen your ability to respond when incidents occur.

- [ ] **1. MFA (Multi-Factor Authentication)**

  MFA is required for all users on email, remote access, and critical business applications.

- [ ] **2. Password Policies**

  Strong password requirements are enforced, including length, complexity, and regular updates.

- [ ] **3. Employee Awareness**

  Employees receive regular security awareness training on threats and safe practices.

- [ ] **4. Phishing Simulations**

  Phishing simulations are conducted regularly, and results are used to drive improvement.

- [ ] **5. User Access Reviews**

  User access is reviewed regularly and updated based on role changes or business needs.

- [ ] **6. Incident Reporting**

  Employees know how to report suspicious activity, and incidents are escalated quickly.

AI USAGE POLICY CHECKLIST

Use AI safely, responsibly, and with clear boundaries across your organization.

- [ ] **1. Business Goals**

  We have defined clear business goals for where AI should create value.

- [ ] **2. Low-Risk Use Cases**

  We start with safe, practical, non-critical AI use cases before expanding adoption.

- [ ] **3. AI Usage Policy**

  We have clear rules defining what employees can and cannot enter into AI tools.

- [ ] **4. Sensitive Data**

  Employees know not to enter client data, personal details, or financial records into unapproved AI tools.

- [ ] **5. Employee Training**

  Our team is trained on what is safe, what is risky, and how to recognize AI-related red flags.

- [ ] **6. Oversight & Review**

  Our AI use is reviewed for governance, compliance, security, and vendor risk before we scale further.



Take Action Today

Use these checklists to assess your current state, identify gaps, and take action to strengthen your organization.

SECTION 6

Vendor & Technology Evaluation



In this section, you'll learn how to tell whether your vendors are actually helping…or holding you back.

First, try to think about the last time you evaluated your technology vendors. I'm not talking about during the contract renewal period, or before an impending price increase. Those times are pretty standard.

But have you ever evaluated them specifically for the purpose of seeing whether they were still helping your business succeed?

Over time, businesses tend to keep working with the same providers for the sake of familiarity. After all, it's always easier to stick with what you already know…we get that.

But as your business grows, your goals also change. Your operations evolve. Your technology needs become more complex. A vendor that was the perfect fit three years ago may no longer be ideal today.

You know how to spot an excellent vendor relationship? It's if they deliver more than just products or services. The best vendors provide guidance, reliability, responsiveness, and confidence that your business is prepared for what's ahead. Whether it's your MSP, internet provider, telecoms partner, cloud provider, cybersecurity vendor, or software vendor, each should contribute to your organization's success.

For most businesses, price is an important consideration, as it should be. But it shouldn't be the sole criterion. It doesn't make sense to choose a lower monthly cost, then end up paying more in the long run, as if poor support leads to downtime, unresolved issues, missed opportunities, or frustrated employees.

In other words, you shouldn't be asking, *"Are we paying too much?"*

Instead, you should ask, *"Are we receiving the value our business needs?"*

A Leadership Conversation

As you go through your vendors one by one, discuss questions like these with your leadership team:

- Which vendors are truly helping us achieve our business goals?
- Are there services we're paying for but rarely use?
- Which vendors act as trusted advisors rather than simply responding when something goes wrong?
- Are there recurring issues that affect employee productivity or customer experience?
- If we were choosing vendors today, would we make the same decisions?

After your discussions, you might end up not replacing anyone. And that's fine. As long as you're able to have a better conversation about what your business expects from the partnerships that support it.

Putting It into Practice

The next worksheet will help you evaluate your key business and technology vendors based on the value they provide, not just the price you pay. As you complete it, consider how each relationship supports your organization's goals today and whether it will continue to support where your business is headed tomorrow.





Vendor Reliance & Third-Party Risk Checklist

Understand Where External Decisions Could Disrupt Your Business

Why This Matters

Your business runs on vendors, whether you like it or not. And while they do bring solutions, they also bring risk.

Change Pricing | Change Access | Change Terms | Get Acquired | Shut Down Services

And none of those changes ask for your permission.

Most of the time, businesses adapt. But adaptation under pressure is very different from adaptation by design.

Continuity risk arises when a vendor change necessitates urgent decisions rather than planned ones.

VENDOR	Yes	No	Unsure
Vendor has access to business-critical data			
Vendor controls authentication or access			
Contract has not been reviewed by leadership recently			
No documented exit or replacement plan exists			
Business would stop if vendor access was removed			
Support response times are unclear			

How to Read This Checklist

- “Unsure” should feel like a signal, not a failure
- If you checked “Unsure” more than twice for any vendor, flag it
- Flagging doesn’t mean replacing; it just means understanding

You don’t need to reduce vendor count or renegotiate everything. Just know where continuity depends on decisions made outside your organization, and whether you’re comfortable with that level of exposure.

VENDOR	**Annual Cost**	**Business Value** (High/Medium/Low)	**Renew?** (Yes/No/Unsure)	**Would We Hire Them Again?** (Yes/No/Unsure)	**Action Required** (Notes/Next Step)

Notes

SECTION 7

IT Budget Planning Worksheet



Are you budgeting for costs…or investing in results?

When company budgets are tight, technology spending is often one of the first areas to be cut. That's possibly a smart business practice…as long as the goal is to make better investments, not simply smaller ones.

Reducing costs and reducing value aren't the same thing.

Some technology investments bring immense value to the business by:

- Helping employees work more efficiently
- Strengthening customer relationships
- Reducing operational risk
- Preventing expensive disruptions

Cutting those investments may lower this year's expenses, which is good. But it could also increase next year's costs in ways that aren't immediately visible… and that's not so good.

Business executives tend to evaluate individual products or subscriptions. This time, try evaluating the business outcomes that those products or services support.

Does an investment help your organization grow or improve efficiency? Does it reduce risk, or create a better experience for employees and customers? If it does none of that, it may be time to reconsider its place in the budget.

The strongest technology budgets aren't built around the newest tools. They're built around the organization's strategic priorities. Every investment should have a clear purpose and a measurable benefit that leadership understands.

A Different Way to Think About It

Imagine two organizations each reduce their technology budget by 15%.

The first cancels security monitoring, delays equipment replacements, and eliminates employee training. The budget is smaller, but the business is now exposed to greater operational and financial risk.

The second removes duplicate software subscriptions, retires tools that are rarely used, and invests the savings in projects that improve productivity and support future growth.

Both organizations spent less. But only one increased the value of its technology investments.

Budget Planner	Current Spend	Future Spend	Areas to Cut	Areas to Increase	Potential Savings	Unexpected Expenses	Technology Priorities
TOTAL	$	$			$	$	

Putting Your Budget to Work

Use the **IT Budget Planning Worksheet** to review your current technology spending through the lens of business value.

As you complete the worksheet, consider these questions:

- Which investments directly support our business goals?
- Which expenses reduce risk or improve operational efficiency?
- Are we paying for services or subscriptions that no longer provide meaningful value?
- Where could a strategic investment create a stronger return than another budget cut?
- Which investments will help us achieve our priorities over the next 12 months?

A thoughtful technology budget isn't measured by how little you spend, but by how effectively your investments help the business succeed.

SECTION 8

Technology Lifecycle & Technical Debt Review



When was the last time you looked at your technology, not because something broke, but because you wanted to know whether it was still supporting your business?

Technology rarely fails overnight. It's a gradual change that happens over months, even years. You'll have time to prepare, but only if you're paying attention.

You see, every piece of technology has a lifecycle. Computers age. Software eventually loses vendor support. Hardware becomes less reliable. Applications that once met your needs may no longer keep pace with the way your business operates today.

You may also hear the term **technical debt.** Simply put, it's the cost of delaying technology improvements. Postponing upgrades or replacing outdated systems may reduce expenses in the short term, but those decisions often create greater operational and financial challenges later.

What Should Leadership Be Looking For?

Rather than focusing on technical specifications, consider whether your technology is creating unnecessary business challenges.

Ask questions such as:

- Are we relying on software that is no longer supported or regularly updated?
- Which computers, servers, or network equipment are approaching the end of their useful life?
- Have we postponed upgrades because "everything still works"?
- Are outdated systems slowing employees down or increasing support costs?
- Could aging technology affect our ability to serve customers or support future growth?

Small issues rarely stay small forever. Addressing them early is often less disruptive – and less expensive – than waiting until they become urgent.

The **Business Continuity Blueprint** that we have prepared for you earlier this year explored how aging infrastructure can create hidden operational dependencies and increase business risk. If you'd like to take a deeper look at those connections, it's a valuable companion resource to this workbook.

Looking Ahead

The following worksheet will help you identify technology that may be approaching the end of its useful life and highlight areas where technical debt could affect your business.

Remember, the goal isn't to replace technology simply because it's old. The goal is to understand whether your current technology can continue supporting your business safely, efficiently, and reliably over the next several years.

Aging Technology Assessment

Use the table below to evaluate systems from your dependency map. Don't aim for precision – just be completely honest.

System / Device	Risk Category (Choose One)	Why This Feels Risky	What Would Force a Change	Estimated Replacement Budget

How to Use This Table:

- Choose one risk category per system, even if it feels imperfect.
- "Why this feels risky" should describe business impact, not technical flaws.
- "What would force a change?" often reveals whether the business is proactive or reactive

If a system lands in the Unknown category, resist the urge to rush past it. Lack of clarity is itself a form of exposure. You can't plan around what you don't understand.

SECTION 9

Business Continuity & Recovery Readiness



Every business experiences disruptions. Some are minor and hardly noticeable. Others have the potential to interrupt operations, delay customer service, or affect revenue.

The real question isn't whether disruptions will happen, because they definitely will. It's whether your organization is prepared for a confident recovery.

Business continuity depends largely, but not entirely, on IT. Leadership also plays a huge role because every recovery decision affects people, customers, operations, and the financial health of the business.

Technology is part of the solution, but **continuity begins with understanding what the business needs to keep operating.**

Recovery starts by identifying your most critical business functions:

Which systems are essential?
Which processes must continue?
Who makes key decisions during a disruption?
And what information does your team need to restore normal operations as quickly as possible?

Just as important is documenting those answers before they're needed. Recovery plans, contact information, vendor details, critical procedures, and leadership responsibilities should be accessible, current, and understood by the people who will rely on them. A plan that exists only in one person's memory isn't really a plan.

What Recovery Really Means

Being prepared will not exempt your business from disruption. But it ensures you understand what matters most, how long critical operations can be interrupted, and what steps are needed to resume business with as little impact as possible.

Organizations that think through these questions ahead of time are often able to make calmer, faster, and more informed decisions when unexpected events occur.

Our **Business Continuity Blueprint** explored these topics in great depth, including dependency mapping, recovery planning, and recovery confidence. If your leadership team hasn't completed those exercises, the blueprint is certainly worth checking out.

Putting Readiness into Action

The next worksheet is designed to help you evaluate your current level of business continuity and recovery readiness.

As you work through it, focus less on the technology itself and more on your organization's ability to continue serving customers, support employees, and make informed decisions during a disruption. The stronger your operational resilience, the more confidently your business can respond when the unexpected occurs.



Recovery
Confidence Checklist

Backups Are Not the Same as Recovery

If something breaks tomorrow, how confident are you that you'd recover cleanly and quickly?

That is the question we aim to answer with this checklist.

Recovery confidence is not whether you have backups, documentation, or plans somewhere. It's about whether those things would actually work under pressure, with imperfect information, and without the ideal people available.

Recovery Readiness Questions

For each question below, rate your current state as High / Medium / Low / Unsure.

Questions	High	Medium	Low	Unsure
Do we know **who decides** when to declare an incident?				
Do we know **who communicates** internally and externally?				
Have backups been tested for actual recovery, not just existence?				
Do we know realistic recovery time expectations?				
Are recovery steps documented, or mostly tribal knowledge?				
Would leadership get clear, accurate answers in the first hour?				
Have we tested recovery without the "right" person available?				

Why This Hits Differently

Downtime isn't just "lost revenue."

It's lost trust, wasted payroll, delayed decisions, and recovery chaos that distracts leadership from running the business.

This worksheet is meant to break that pattern of false confidence.

Downtime Impact Assessment

Imagine the impact of a critical system going down, not only hypothetically, but operationally. Be honest. If something hasn't been discussed before, that's important to acknowledge. To get you started, we've entered some possible answers for the Hour 1 row.

Timeframe	Operational Impact	Financial Impact	Customer Impact	Leadership Impact
Hour 1 (The First Hour)	Staff Idle	Payroll Waste	Delays	Confusion
Day 1 (The First Day)				
Week 1 (The First Week)				

How to Use This Worksheet

- Don't overthink precision. This isn't a forecasting exercise.
- Describe what actually happens, not what you hope would happen.
- If leadership has never discussed these scenarios, say that plainly.
- Avoid math-heavy estimates. Use plain, everyday language instead.

SECTION 10

Cyber Readiness & Incident Preparedness



Even if you think you have an idea of what to do during a cyber incident, it hits differently once it's actually unfolding before your eyes. It's when "expectation vs. reality" goes into full gear.

The first few hours after an incident are often the most challenging. Questions come quickly…

Is customer data affected?
Should employees continue working?
Who needs to be notified?
What does our cyber insurance require?

Without a clear plan, even experienced leadership teams can find themselves reacting instead of leading.

Cyber readiness begins long before an incident occurs. It starts with defining roles and responsibilities, establishing communication procedures, and making sure everyone understands what to do if suspicious activity is discovered.

When employees know how to report concerns and leadership knows how decisions will be made, the organization can respond with greater confidence and less confusion.

Preparation also means **understanding your cyber insurance requirements** before you need them. Many policies include specific expectations around incident reporting, documentation, and approved response procedures. Knowing those requirements in advance can help leadership make informed decisions when time matters most.

Leading with Confidence

An effective incident response plan isn't designed to eliminate every challenge. It's designed to reduce uncertainty.

When leadership understands who is responsible for key decisions, how information will be communicated, and what actions need to happen first, the organization is better positioned to protect its people, maintain customer trust, and recover more efficiently.

If you've seen the **Cyber Incident Survival Guide** that we've prepared for you, it explores these topics in greater detail. The **First 60 Minutes Response Plan** and the **Executive Decision Map** would be of particular help in this regard.

If your leadership team hasn't reviewed those resources recently, it's not too late. Check them out…they're excellent companions to this workbook.

A Moment for Reflection

Before moving on, take a few minutes and mull over these questions with your leadership team:

- Who leads the business response if a cyber incident occurs?
- Would employees know how to report suspicious activity quickly and confidently?
- Are our communication procedures documented for employees, customers, vendors, and other stakeholders?
- Do we understand our cyber insurance obligations before an incident happens?
- How confident are we that our leadership team could make timely, informed decisions during the first few hours of a cyber incident?

Then, use the following worksheet to evaluate your organization's current level of cyber readiness and identify opportunities to strengthen your incident preparedness before they're needed.

Incident Response Roles

During a cyber incident, it's not just one person or team that handles response efforts.
Usually, it's a coordinated effort between technical specialists, leadership, and other parts of the organization.

IT teams typically take the lead in identifying and containing the threat. But there are plenty of non-technical jobs to do as well. Clearly defining and assigning these roles in advance helps organizations respond faster and avoid confusion.

Role	Key Responsibilities
Executive Leadership	Makes strategic decisions about operations, business continuity, and resource allocation
IT Team/Managed Service Provider	Investigates the incident, isolates affected systems, analyzes the attack, and works to contain and remove threats.
Legal or Compliance Advisor	Evaluates regulatory obligations, data breach notification requirements, and legal risk associated with the incident.
Communications or Public Relations	Manages internal updates to employees and prepares external messaging if customers, partners, or the public must be informed.
Cyber Insurance Provider	Provides guidance on incident response procedures and may coordinate forensic investigators, legal support, or recovery specialists.
External Security Specialists	Assist with forensic investigation, threat analysis, and recovery when additional expertise is required.

Even in smaller organizations, clearly assigning these responsibilities ahead of time can significantly improve response speed and coordination when an incident occurs.

It's also possible for additional stakeholders to be involved. For example, if employee accounts are compromised, Human Resources may need to assist. Finance teams may be called upon if fraudulent transactions need to be investigated. In some cases, even third-party vendors may need to participate if their platforms support critical business systems.

Once response roles are clearly defined, organizations should also understand how cyber insurance may factor into incident response and recovery.

The following section explains how cyber insurance works and why preparation before an incident occurs can make a significant difference during recovery.

[See the Cyber Incident Survival Guide for the complete response framework.]

CYBER INSURANCE READINESS



Cyber insurance is now a standard part of business risk management. Many organizations rely on it as a financial safety net in the event of a cyber incident that disrupts operations or exposes sensitive data.

But hear this – just because you have a policy doesn't mean you're fully protected. Most cyber insurance companies now have very strict requirements before releasing claims. Security practices, incident reporting timelines, documentation, and other requirements must be followed to help avoid claim complications or denial.

For this reason, cyber insurance should be viewed as part of a broader preparation strategy rather than a standalone solution.

BEFORE AN INCIDENT EVER HAPPENS

To find out if you're truly protected under your policy, ask these questions:

1. Do we clearly understand what our policy covers?

Coverage may include items such as ransomware response, forensic investigation, legal costs, customer notification, and business interruption. The exact scope can vary significantly between policies.

2. Do we know the reporting requirements?

Many policies require incidents to be reported within a specific timeframe. In some cases, this window may be as short as 24–72 hours after discovery.

3. Are our required security controls in place?

Some policies require organizations to maintain certain security practices such as multi-factor authentication, backups, or monitoring tools.

4. Do we know who contacts the insurer during an incident?

Assigning this responsibility in advance helps ensure reporting deadlines are not missed during a crisis.

Cyber insurance can play an important role in reducing financial exposure. However, its value depends on preparation, clear procedures, and a strong understanding of the policy before an incident occurs.

SECTION 11

Your 12-Month Technology Roadmap



By now, you've identified your priorities, sorted through potential risks, and reflected on the areas that need the most attention. You're getting quite a lot on your plate but don't panic…you don't need to do all of them all at once. However, you do need to decide what matters most.

A successful technology roadmap isn't measured by the number of projects you've lined up to complete. It's measured by how well each initiative supports your priorities.

The most effective organizations focus on steady, meaningful progress rather than chasing every new technology or solving every challenge at the same time.

As you build your roadmap, think about the year ahead.

Which initiatives will have the greatest impact on your business?
Where should you invest first?
Which improvements can wait until later?

If you can properly prioritize your efforts, you'll also find it easier to allocate resources, manage budgets, and maintain momentum throughout the year.

Your roadmap will likely include, but isn't limited to, the following:

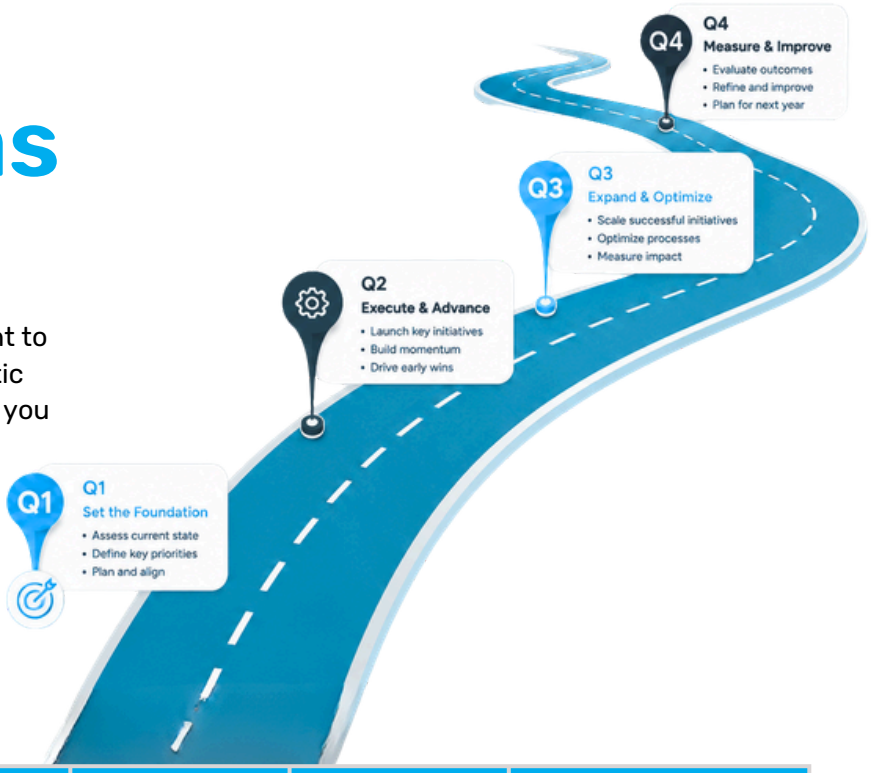
- Strengthening Cybersecurity
- Modernizing Aging Technology
- Reviewing Key Vendors
- Improving Business Continuity
- Planning AI Initiatives
- Supporting Compliance Requirements

It also includes investing in projects that improve operational efficiency and prepare the business for future growth. Again, not every initiative needs to happen this quarter, so there's no need to rush through them. But every initiative should have a purpose.

Turning Ideas into Action

The **12-Month Technology Roadmap** is meant to help you organize your priorities, assign realistic timelines, and identify the business outcomes you expect each initiative to support.

Remember, this isn't about building the perfect plan. It's about creating a practical one that your leadership team can review, adjust, and build upon throughout the year as your business continues to evolve.



Q1

Goals	Projects	Budget	Owner	Status

Q2

Goals	Projects	Budget	Owner	Status

Q3

Goals	Projects	Budget	Owner	Status

Q4

Goals	Projects	Budget	Owner	Status

SECTION 12

Executive Action Plan



A well-designed plan only creates value when it's put into action. Now that you've got the plan, what remains to be answered is: how will you turn today's decisions into tomorrow's results?

We've said it before, and we'll say it again – the goal isn't to complete each initiative right away. The important thing is to make steady progress toward the outcomes that matter most.

While reviewing your roadmap, focus on the actions that will have the greatest impact on your business. Some projects may require significant planning, while others can begin with a simple conversation, a policy update, or a scheduled review. Small, consistent steps often create more lasting results than ambitious plans that never move forward.

As you build your Executive Action Plan, consider these questions:

- Which initiatives should be addressed first?
- Who will be responsible for each priority?
- What is a realistic timeline for completion?
- How will we measure success?
- When will leadership review our progress?

Assigning ownership is just as important as identifying priorities. When responsibilities are clear and expectations are defined, initiatives are far more likely to stay on track. Accountability turns good intentions into measurable results.

Moving Forward with Confidence

Use the **Executive Action Plan** to capture your highest priorities, assign owners, establish timelines, and define the business outcomes you want to achieve.

The strength of your plan won't be measured by how detailed it is, but by whether it inspires action. Choose a few meaningful priorities, assign clear ownership, and begin moving forward. Real progress starts with the first step, not the perfect plan.

Top Five Priorities

Priority	Owner	Due Date	Expected Outcome	Completed

Notes

SECTION 13

Final Business Readiness Scorecard



Congratulations!

You've reached the end of the workbook. More importantly, you were able to take a close look at your business from a leadership perspective, rather than simply a technology perspective.

Your final score isn't meant to be a grade. There's no passing or failing mark, so don't sweat it. It's simply a snapshot of where your organization stands today. Some areas may reflect strong confidence, while others highlight opportunities for improvement. Both are valuable because they help shape your priorities for the months ahead.

Also, take note that business readiness isn't something you achieve once and then forget. As your organization grows, your goals, risks, technology, and operations will continue to evolve. Your readiness should evolve with them.

Measuring Progress, Not Perfection

The **Final Business Readiness Scorecard** brings together the results from each assessment you've completed and creates an executive view of your organization's overall readiness.

Use this scorecard to track progress, identify new priorities, and keep technology aligned with your business strategy. It will help you a lot in building a more adaptable and future-ready organization one step at a time.

Final Business Readiness Scorecard

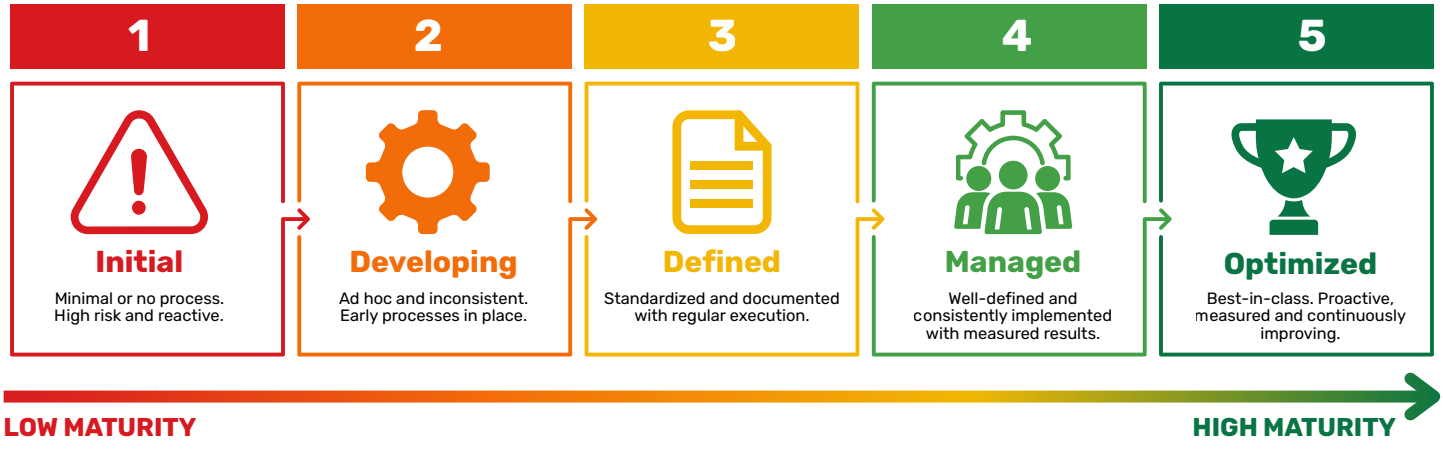
Readiness Areas	Maturity Score (1-5)	Current State Snapshot (What's Working Well / Key Gaps)
Executive Dashboard		
Business Readiness		
Security Culture		
Vendor Management		
Budget Planning		
Technology Planning		
Business Continuity		
Cyber Readiness		

Maturity Scale
(How we measure maturity across all areas)

- **5 — Optimized**: Best-in-class. Proactive, measured and continuously improving.
- **4 — Managed**: Well-defined and consistently implemented with measured results.
- **3 — Defined**: Standardized and documented with regular execution.
- **2 — Developing**: Ad hoc and inconsistent. Early processes in place.
- **1 — Initial**: Minimal or no process. High risk and reactive.

Maturity Scale

Use this scale to assess each area.



SECTION 14

Next Steps



Completing this workbook is an important milestone, but it's by no means the finish line.

Every organization has opportunities to strengthen its operations, reduce risk, and better prepare for the future. So you must continue asking the right questions, making thoughtful decisions, and building a business that's ready for whatever comes next.

As your business grows, your priorities will change. New opportunities will emerge, technology will continue to evolve, and new challenges will require fresh conversations. That's why we've designed this workbook to be a living planning tool, not a one-time exercise.

Review your **Executive Action Plan** during your quarterly leadership meetings to measure progress, adjust priorities, and keep your initiatives aligned with your business goals. Then revisit this workbook each year as part of your annual planning process to establish a new baseline and identify the next opportunities for improvement.

Business readiness is a journey of continuous improvement, and you don't have to navigate it alone.

To continue building your leadership strategy, visit the **Newave Solutions Business Resources page.**There, you'll find the **AI Business Playbook, Business Continuity Blueprint, Cyber Incident Survival Guide,** and future executive resources designed to help your organization make smarter business decisions and build long-term resilience.

Thank you for investing the time to strengthen your business. The conversations you've started today can surely help shape a more sustainable, more confident, and more successful organization for years to come.

Annual Leadership Commitment

Our priorities. Our Owners. Our commitment to progress.

First Priority We'll Complete	Owner	Budget Approved	Quarterly Review Dates	Leadership Signatures



Our Commitment

We will prioritize these initiatives, provide the necessary resources, and review progress quarterly to ensure success.


NEWAVE
SOLUTIONS