# The Cybersecurity Maturity Roadmap

## How to Invest in the Right Controls Today and Prepare Your Organization for an AI-Driven Future

A practical guide for business leaders, IT teams, operations leaders, and facilities managers

BTI COMMUNICATIONS GROUP

# Table of Contents

This guide is organized as a practical, educational resource for executives, IT leaders, operations managers, facilities directors, and compliance officers. It teaches the fundamentals of cybersecurity maturity, provides a self-assessment, and shows how BTI Communications Group can help at each stage.



This guide is an educational resource. It does not constitute a formal audit, legal determination, compliance certification, or penetration test. Contact BTI Communications Group to discuss a formal assessment of your environment.

# Executive Introduction

Many organizations feel overwhelmed by cybersecurity. The reasons are understandable: long control lists, dozens of competing tools, multiple overlapping frameworks, and a steady stream of warnings from vendors, insurers, regulators, and the news cycle. The result is often either paralysis or fragmented purchasing — acquiring tools without a clear strategy, assigning responsibility to no one in particular, and hoping the situation improves on its own.

The real objective is not to buy everything immediately. Organizations are generally better served by treating cybersecurity as an ongoing operating discipline than by relying on a one-time burst of technology purchasing. The goal is to understand risk, establish accountability, secure the most critical systems and users, create repeatable operations, collect evidence that controls are working, and then improve through an ongoing, prioritized roadmap.

Cybersecurity expectations may come from laws and regulations, contracts, certification standards, government programs, voluntary frameworks, insurance underwriting, and customer requirements. Applicability and required evidence vary by organization.

> Cybersecurity maturity develops through ongoing, risk-based improvement. The right investment depends on your organization's size, risk, regulatory obligations, infrastructure, internal capabilities, and business priorities. There is no single product, platform, or provider that resolves every risk at once.

This guide is organized around a six-level maturity roadmap covering governance, identity, devices, networks, cloud platforms, vulnerability management, monitoring, incident response, backup and recovery, compliance evidence, physical security, communications security, vendor risk, and AI governance. Each level describes what a typical organization looks like at that stage, what the primary risks are, what controls to prioritize, and where BTI Communications Group can help.

Organizations do not need to start at Level 0 and work linearly through every stage. Many begin at Level 1 or 2 and find that governance, compliance readiness, or AI adoption requires them to address gaps that were never properly established. This guide is designed to help leadership teams understand where they are, identify what matters most right now, and make informed decisions about where to invest.

### Understand Risk

Identify what matters most and where exposure is greatest

### Establish Accountability

Assign clear ownership for controls and decisions

### Secure the Basics

Protect identity, devices, email, and critical systems first

### Create Evidence

Demonstrate that controls are operating and effective

### Improve Over Time

Build on a foundation rather than starting over repeatedly

# Why Cybersecurity Decisions Are Becoming Harder

The security environment that most organizations operate in today is meaningfully different from what it was five years ago. Cloud adoption has accelerated. Remote and hybrid work have become common in many organizations, while on-site organizations increasingly depend on cloud services, mobile access, connected facilities, and remote administration. Microsoft 365 and other cloud-based identity platforms now sit at the center of many organizations' business operations. At the same time, the number of connected systems — including cameras, access-control panels, VoIP systems, and IoT devices — has grown steadily, adding infrastructure that carries cybersecurity risk but often receives far less security attention than servers and workstations.

### External Pressures

- Many cyber insurers now ask more detailed questions about controls such as MFA, endpoint protection, backups, vulnerability management, incident response, privileged access, and security awareness.
- Vendor and customer security questionnaires are increasingly common in regulated and business-to-business environments.
- Many organizations face additional cybersecurity obligations through new contracts, customer requirements, regulatory updates, insurer questionnaires, and industry programs.
- Weak or compromised identities — including stolen credentials, stale accounts, inconsistent MFA, and excessive privileges — are a major source of cybersecurity risk.

### Internal Pressures

- Limited internal staffing for dedicated security work
- Tool sprawl with unclear ownership and coverage gaps
- Multiple vendors with overlapping but uncoordinated responsibilities
- Employees already using generative AI tools for work
- Leadership evaluating AI agents and workflow automation

# The AI Factor

Generative AI tools are already being used in many workplaces, sometimes without formal approval, security review, or governance. Employees use AI to write communications, summarize documents, analyze data, generate code, and automate routine tasks. This creates genuine productivity benefits, and it also creates security and governance challenges that did not exist a few years ago.[2,3]

### AI Accelerates Work

Automates routine work, improves analysis, helps users find information, and can support selected IT and security workflows when deployed through appropriate tools and controls.

### AI Expands Risk Surface

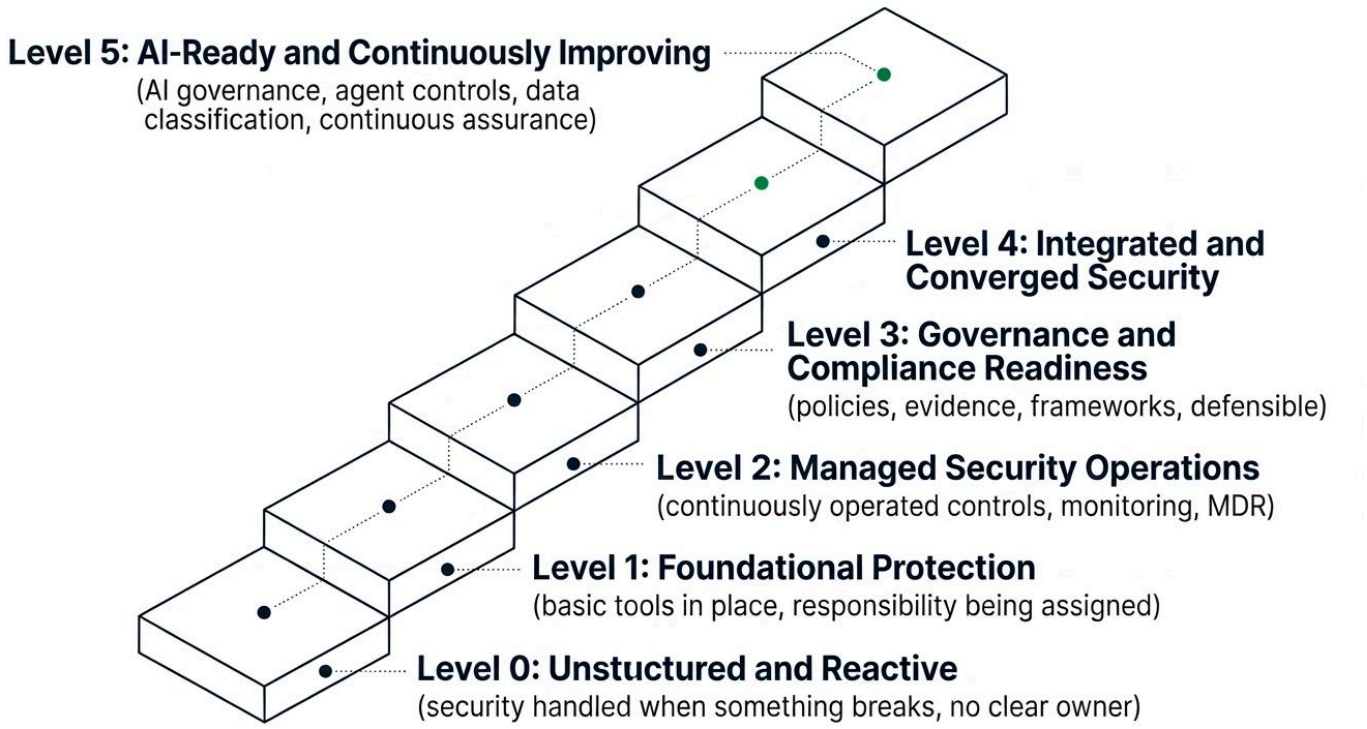
Can expose sensitive information, increase shadow AI and other forms of unmanaged technology use, expand identity and permissions risk, introduce insecure automation, and amplify the consequences of weak access controls

As organizations move toward AI agents — systems that can read data, write records, send messages, create tickets, trigger workflows, access cloud systems, and interact with customers at machine speed — the security foundation becomes more important, not less. Organizations that have strong identity controls, reliable logging, data governance, and documented workflows are far better positioned to adopt AI safely than organizations that are still operating without those fundamentals.

# The BTI Cybersecurity Maturity Roadmap

The six-level roadmap below provides a practical planning framework for understanding where your organization is today and what a logical path forward looks like. Each level describes a **dominant operating posture** — not a rigid sequence of gates that must be fully completed before progress can begin at the next level. Progress is driven by deliberate investment and clear priorities, not by purchasing the most advanced tools available.

The BTI Cybersecurity Maturity Roadmap is an educational planning framework developed to help organizations prioritize cybersecurity, operational resilience, compliance readiness, converged security, and AI governance. It is informed by widely recognized cybersecurity and AI risk-management principles[1,2], but it is not a certification framework, formal audit methodology, or substitute for a framework-specific assessment.




Organizations often work across several maturity levels simultaneously. Urgent risks, incidents, regulatory obligations, acquisitions, customer requirements, and AI adoption may require advanced governance, monitoring, or response capabilities before every foundational gap has been closed. The roadmap helps identify the most important investments at each stage — it does not prescribe a strictly linear progression.

That said, foundational controls matter. Advanced capabilities are significantly less effective when core elements — such as identity management, patching, backup integrity, asset visibility, and clear accountability — are weak or absent. Organizations that invest in those fundamentals first are better positioned to extend their security posture reliably and sustainably over time.

# Levels 0 & 1 — From Reactive to Foundational

The levels below describe **dominant operating postures** — not rigid gates that must be fully completed before progress can begin. Organizations often address risks across multiple levels simultaneously based on urgency, regulatory requirements, or specific vulnerabilities.

LEVEL 0

## Unstructured and Reactive

At this level, security is handled primarily when something breaks. There is no clear security owner, no documented policies, and no consistent approach to patching or backup testing. MFA is inconsistent or absent, devices and software are not fully inventoried, and backups may exist but are rarely validated. Security responsibilities are distributed across several vendors without clear coordination, and there is no formal process for responding to incidents. Employees receive little or no security training, and there are no established rules around AI use.

**Primary objective:** Establish visibility and stop the most preventable risks.

### First Actions

- Basic environment and asset assessment
- Review MFA, privileged accounts, stale accounts, and other immediate identity risks
- Backup validation
- Endpoint protection review
- Microsoft 365 security review
- Basic vulnerability scan
- Identify critical systems and data
- Create acceptable-use policy and AI-use guidance
- Establish who owns security decisions

### BTI Can Help With

- Initial cybersecurity assessment
- Vulnerability and infrastructure review
- Backup and continuity review
- AI governance starter discussion
- Basic remediation roadmap

LEVEL 1

## Foundational Protection

At Level 1, the organization understands its most important systems and has begun assigning security responsibility to specific individuals. Basic tools are being put in place — MFA is being deployed, asset inventory is underway, and backup processes are being established — though consistency and enforcement are still improving.

The primary objective is to make preventive controls repeatable and to close the gaps that create the highest likelihood of a preventable incident. Identity lifecycle management and consistent MFA enforcement are important priorities at this level.

**Primary objective:** Put basic preventive controls in place and make them repeatable.

### Recommended Controls

- MFA across critical applications
- Managed endpoint protection
- Regular OS and third-party patching
- DNS and email security
- Secure firewall and remote-access configuration
- Backup monitoring and testing
- User onboarding and offboarding procedures
- Basic security-awareness training
- Asset inventory
- Secure admin access to cameras, access control, and VoIP
- Approved and prohibited AI-use guidelines

### BTI Can Help With

- Managed or co-managed IT
- Microsoft 365 security configuration and hardening within agreed scope
- Network and firewall management
- Security-awareness training
- Managed support for in-scope physical-security systems
- VoIP and communications security review

# Levels 2 & 3 — Managed Operations to Compliance Readiness

LEVEL 2

## Managed Security Operations

At Level 2, security controls exist but require ongoing management, monitoring, and accountability. Many organizations at this level have purchased tools that are not fully configured, monitored, or maintained. Internal IT may need additional capacity. Leadership typically wants fewer vendors and clearer responsibility for what is actually being done. The defining shift at this level is moving from installed security tools to continuously operated security controls.

Managed security means controls are not only purchased — they are configured, monitored, maintained, tested, documented, reviewed, and improved over time. Vulnerability management at this level is a program, not a one-time scan. Patching is orchestrated rather than ad hoc. Incidents are triaged and escalated through defined workflows rather than discovered by accident.

### Recommended Capabilities

- 24/7 monitoring where appropriate
- EDR, with managed detection and response where appropriate
- Centralized logging, managed detection, SIEM, or another appropriate monitoring approach based on the organization's size, architecture, risk, contractual obligations, and regulatory requirements
- Vulnerability management program
- Patch orchestration
- Identity monitoring
- Email and SaaS security
- Incident triage and escalation workflows
- Network, firewall, and Wi-Fi oversight
- Recurring security reporting and quarterly reviews
- Managed monitoring of security-system servers
- VoIP and SBC hardening

### BTI Engagement Options

- BTI managed or co-managed IT and cybersecurity services
- Endpoint security, managed detection and response, SOC-supported monitoring, and vulnerability management within defined scope
- Managed network services
- Managed backup, recovery support, and continuity planning within defined scope
- Physical-security system support and management within defined scope
- Quarterly security reviews

LEVEL 3

## Governance and Compliance Readiness

At Level 3, technical controls are improving, but the organization is being asked to prove that security is working. Cyber-insurance underwriters, customers, regulators, auditors, and contracts increasingly require evidence — not just assertions. Policies and responsibilities may be incomplete or undocumented, and security work that is genuinely occurring may be difficult to demonstrate because evidence has not been collected or organized.

It is important to distinguish between controls, policies, procedures, and evidence. A control is a technical or operational safeguard. A policy is a documented standard. A procedure describes how the control is carried out. Evidence demonstrates that the control operated as required during a specific period. Compliance readiness requires all four, along with a clear shared-responsibility matrix and a process for managing open items — often called a Plan of Action and Milestones (POA&M).

### Recommended Capabilities

- Formal security policies
- Incident-response plan
- Risk assessment
- Control ownership and shared-responsibility matrix
- Evidence collection and compliance framework mapping
- Vendor-risk management
- Vulnerability-remediation records and patch-compliance reports
- POA&M creation and tracking
- Executive reporting and quarterly evidence review

### Applicable Requirements — Four Categories

- **Laws, regulations, and regulated obligations** — HIPAA-related obligations[6], applicable privacy and security laws, sector-specific regulatory requirements
- **Government or contractual program requirements** — CMMC[7], government contracting security requirements, customer security addenda
- **Standards and voluntary frameworks** — NIST Cybersecurity Framework[1], CIS Controls[5], ISO/IEC 27001[11]
- **Industry, customer, and insurer expectations** — PCI-related obligations[8], cyber-insurance questionnaires, customer security reviews, vendor risk questionnaires

The applicable requirements, scope, evidence expectations, and assessment method depend on the organization, industry, contracts, data, systems, and legal environment. BTI helps clients prepare and organize technical and operational readiness but does not determine legal applicability or provide legal advice.

### BTI Engagement Options

- Compliance-readiness assessment
- GRC platform onboarding and evidence-management support, where included in the approved scope and supported by the selected platform and service agreement
- vCISO advisory or qualified security-leadership support, depending on scope and availability
- Third-party penetration-testing coordination and remediation support
- Audit-preparation and evidence-readiness support for an audit, formal assessment, customer security review, insurer review, or compliance examination

# Level 4 — Integrated and Converged Security

LEVEL 4

## Integrated and Converged Security

At Level 4, IT, cybersecurity, physical security, facilities technology, and communications are highly interconnected. Multiple vendors may manage different parts of the environment, creating coordination gaps that affect visibility, incident response, and accountability. Multi-site consistency is increasingly important, and leadership needs better coordination across domains that previously operated in isolation.

Converged security does not mean placing every system into one tool. It means the organization has shared standards, defined responsibilities, coordinated workflows, consistent documentation, better escalation paths, fewer coordination gaps, clearer accountability between providers, and improved visibility across participating technology domains.

### Recommended Capabilities

- Unified identity and access governance
- Network segmentation for cameras, access control, and IoT
- Secure remote access
- Zero-trust-aligned improvements to identity, access, segmentation, device trust, verification, and monitoring
- Coordinated incident response across IT and physical systems
- Physical access reviews and camera lifecycle management
- Security-system patching, configuration management, and access-log review
- VoIP and communications security
- Multi-site standards and vendor accountability
- Centralized reporting and project change governance

### BTI Engagement Options

- Converged security assessment
- IT and physical-security architecture review
- Access-control and video-surveillance modernization
- PMO-led modernization projects
- Unified QBR and roadmap planning

# Level 5 — Advanced, AI-Governed, and Continuously Improving

LEVEL 5

At Level 5, the organization is actively adopting generative AI and evaluating AI agents for workflow automation. Employees are using AI tools to assist with work. Leadership is considering or already piloting systems that can read data, write records, send messages, create tickets, trigger workflows, access cloud systems, use credentials, and interact with customers at machine speed. This creates a new risk category that requires both governance and technical controls.

The security foundation for AI adoption must include strong identity, strong permissions, reliable logging, data governance, approved workflows, human oversight, and continuous review. Organizations that reach Level 5 with weak foundations in any of these areas will find that AI amplifies existing vulnerabilities rather than simply adding new ones. AI outputs and automated actions require risk-appropriate governance and oversight. High-impact, external-facing, security-sensitive, financial, safety-related, or difficult-to-reverse actions should have stronger testing, approval, monitoring, and rollback controls.[2,3]

A high general cybersecurity score does not by itself prove that an organization is ready for every AI use case. AI readiness also depends on the specific use case, data quality, privacy requirements, legal obligations, vendor risk, application architecture, testing, user competence, and business-process controls.[2,3]

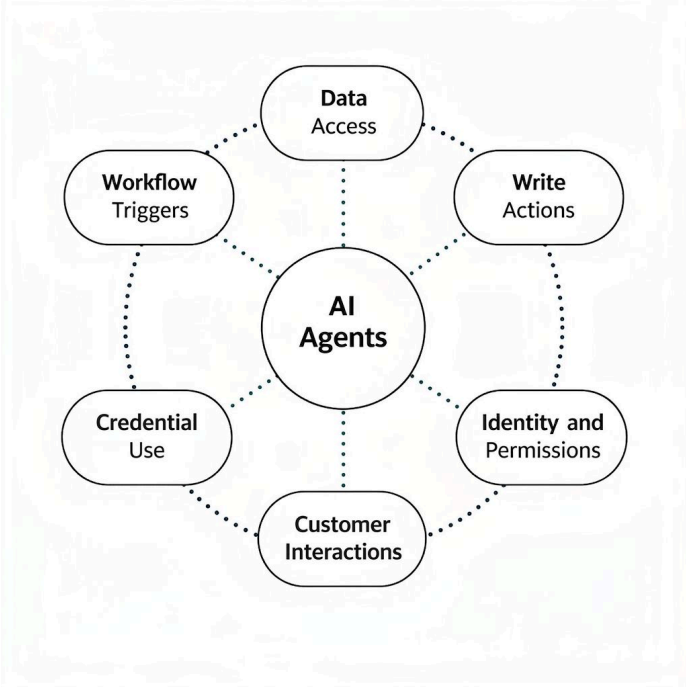
### Recommended Capabilities

- AI governance policy and approved-tool list
- Data-classification rules and prohibited-use standards
- AI-agent approval workflows and sandbox environments
- Identity, role-based access, and least privilege
- Application and API inventory with logging
- Data-loss prevention
- Vendor and model risk review[2]
- Output validation and procedures to pause, disable, isolate, or roll back AI-enabled workflows
- Incident-response procedures for AI events
- Periodic access reviews and user training
- Clear ownership for AI systems

### Potential BTI Advisory and Security Engagements — Subject to Scope and Current Availability

- AI governance and acceptable-use workshop
- Approved-tool and prohibited-use policy guidance
- Identity and permissions review for proposed AI workflows
- Microsoft 365 and cloud-security review within agreed scope
- AI application and vendor inventory planning
- Shadow AI risk discussion or scoped discovery planning
- AI-agent risk and control planning
- Managed cybersecurity and compliance operations supporting the underlying environment
- Executive roadmap and recurring review support

AI-related services are subject to scope, available tooling, client architecture, risk level, third-party dependencies, and current BTI service availability. Some engagements may require coordination with qualified legal, privacy, compliance, application-security, software-development, or other specialist providers.




AI agents can execute consequential actions — reading data, writing records, triggering workflows, and interacting with customers — faster than human review processes. Least-privilege access, defined authorization boundaries, logging, testing, monitoring, and rollback procedures should be treated as foundational controls before deploying AI agents that can take consequential actions.

# Maturity Self-Assessment — Part 1 of 2

Use this self-assessment to gauge your organization's current cybersecurity maturity. For each item, select the number that most accurately reflects your current state. This is an educational tool — it is not a formal audit, compliance certification, penetration test, or legal determination.

| | |
|---|---|
| **0**<br>Not in place | **1**<br>Partially in place |
| **2**<br>Mostly in place | **3**<br>Implemented, reviewed, and current |

**Maximum possible score: 66**

| Question | Category | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| 1. Is there a named individual or team responsible for cybersecurity decisions? | Governance | | | | |
| 2. Does a formal security policy exist and has it been reviewed in the past 12 months? | Governance | | | | |
| 3. Is MFA enforced for all users on email, remote access, administrative accounts, and supported critical cloud applications? | Identity | | | | |
| 4. Are user accounts reviewed and promptly disabled when employees leave? | Identity | | | | |
| 5. Do employees receive security-awareness training during onboarding and periodically thereafter, with additional training based on role or risk where appropriate? | Users | | | | |
| 6. Is there a written policy governing acceptable and prohibited use of AI tools? | Users | | | | |
| 7. Is managed endpoint protection deployed and actively monitored on all supported and in-scope endpoints? | Devices | | | | |
| 8. Are OS and third-party software patches applied on a consistent, documented schedule? | Devices | | | | |
| 9. Is the network segmented to separate critical systems, IoT devices, and guest traffic? | Networks | | | | |
| 10. Are firewall and remote-access configurations documented and regularly reviewed? | Networks | | | | |
| 11. Is Microsoft 365 or the organization's primary cloud identity platform configured, monitored, and reviewed according to an approved security baseline? | Cloud | | | | |

*Continued on Part 2 of 2 — Questions 12–22, Scoring Guide, and Results Summary.*

# Maturity Self-Assessment — Part 2 of 2

0 = Not in place | 1 = Partially in place | 2 = Mostly in place | 3 = Implemented, reviewed, and current

| Question | Category | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| 12. Are SaaS application access and permissions reviewed on a recurring basis? | Cloud | | | | |
| 13. Is vulnerability scanning performed on a regular schedule with results tracked? | Vulnerability Mgmt | | | | |
| 14. Is there a process to prioritize and remediate identified vulnerabilities? | Vulnerability Mgmt | | | | |
| 15. Are relevant security logs collected centrally and supported by appropriate alerting, analytics, review, and response processes? | Monitoring | | | | |
| 16. Is there a documented incident-response plan with named contacts and escalation steps? | Incident Response | | | | |
| 17. Are backups and restoration procedures tested on a documented schedule, with results reviewed by responsible personnel and significant issues reported to leadership? | Backup & Continuity | | | | |
| 18. Is evidence of security controls collected and organized for applicable audits, assessments, customer reviews, contractual obligations, or insurance requirements? | Compliance Evidence | | | | |
| 19. Are cameras and access-control systems securely configured, segmented, patched, and access-controlled? | Physical Security | | | | |
| 20. Is VoIP and communications infrastructure securely configured, maintained, and access-controlled? | VoIP Security | | | | |
| 21. Are vendor responsibilities for security clearly documented and reviewed? | Vendor Management | | | | |
| 22. Is there an approved AI-tool list and a review process for AI agent deployments? | AI Governance | | | | |

Your score: _____ out of 66

Percentage: total score ÷ 66 × 100 = _____ %

## Scoring Bands

### 0–25% — Reactive

Foundational visibility, ownership, and immediate risk reduction are the priorities.

### 26–45% — Foundational

Preventive controls are developing but need greater consistency, coverage, documentation, and ownership.

### 46–65% — Managed

Core tools and processes exist, but the organization should strengthen continuous operation, monitoring, vulnerability remediation, response, and reporting.

### 66–80% — Governed

Policies, responsibilities, evidence, risk management, and compliance readiness are becoming integrated into operations.

### 81–90% — Integrated

IT, cyber, physical security, communications, facilities technology, and vendor responsibilities are increasingly coordinated.

### 91–100% — Advanced and AI-Governed

The organization has a strong general security foundation and may be positioned to evaluate advanced automation and AI use cases through separate, use-case-specific risk reviews.

⚠ A high overall score does not eliminate the importance of individual control gaps. A low score in a critical area—such as identity, backups, incident response, vulnerability remediation, or privileged access—may require immediate attention even when the aggregate score is relatively high.

This score is directional and educational. It is not a formal maturity certification, security audit, compliance assessment, penetration test, or determination that an organization is ready for a particular AI system.

# Where Should We Invest First?

One of the most practical questions any leadership team can ask is where to direct the next dollar and the next 90 days of security effort. The answer depends on your organization's current risk level, regulatory environment, internal capabilities, and budget. The matrix below organizes investment options into four categories ordered from most foundational to most forward-looking. Organizations should generally invest first in controls that are high impact, broadly applicable, foundational to other controls, required by insurance or regulation, and needed to reduce immediate operational risk.

Vulnerability prioritization should consider exploitability, exposure, asset criticality, business impact, available mitigations, and evidence of active exploitation—not severity score alone.[4]

### 🔴 Immediate Risk Reduction

- Multi-factor authentication (MFA)
- Managed endpoint protection
- OS and third-party patching
- Backup validation and testing
- Email security (filtering, anti-phishing)
- Critical vulnerability remediation
- Secure remote access
- Administrative-account cleanup

### 🟡 Operational Consistency

- Managed monitoring, centralized logging, or SIEM where appropriate
- Asset inventory and documentation
- Identity lifecycle management
- Firewall and network standards
- Security-awareness training
- Vendor accountability documentation
- Ticket and escalation workflows
- Recurring reporting and QBRs

### 🟢 Governance and Defensibility

- Formal security policies
- Risk assessment and POA&M
- Incident-response plan
- Evidence collection and, where appropriate, GRC platform support
- Compliance framework mapping
- Conduct or coordinate an appropriately scoped penetration test through a qualified provider when justified by risk, contractual requirements, customer expectations, or compliance obligations
- Cyber-insurance control and evidence readiness
- Shared-responsibility documentation

### 🔵 Future Readiness

- AI governance policy and tool list
- AI-agent approval and monitoring controls
- Data classification framework
- API and application inventory
- Zero-trust-aligned improvements to identity, access, segmentation, device trust, verification, and monitoring.
- Network segmentation expansion
- Converged physical and cyber security
- Automated evidence collection

Vulnerability scanning identifies potential weaknesses, missing patches, insecure configurations, and known exposures that require review and prioritization. Penetration testing uses authorized and controlled attack techniques to test whether selected weaknesses can be exploited within an agreed scope and period. These are distinct services that serve different purposes and should not be treated as interchangeable. No provider can guarantee that an organization will never experience a security incident.

# Ways to Engage BTI — Starting and Operating Engagements

BTI Communications Group's engagement model is designed to meet organizations where they are. There is no required starting point and no single path that every customer follows.

Services shown are examples of potential engagement components. Availability, scope, included features, licensing, geographic coverage, third-party dependencies, and delivery responsibility vary by client and agreement.

### Path 1 — Security Maturity and Risk Review

**Examples:** Cybersecurity maturity discussion · Infrastructure assessment · Microsoft 365 security review (within the scope of the client's BTI agreement, licensing, environment, and approved project plan) · Network and firewall review · Backup and continuity review · Vulnerability assessment · Physical-security cybersecurity review · AI governance starter discussion

**Outcome:** A clearer view of current conditions, priority gaps, shared responsibilities, and practical next steps.

### Path 2 — Priority Remediation Project

**Examples:** MFA and identity improvements · Microsoft 365 security configuration · Firewall and network modernization · Network segmentation · Endpoint protection deployment · Patch-management improvement · Backup modernization · Vulnerability remediation · Camera and access-control modernization · Security-system server hardening · VoIP and SBC security improvement

**Outcome:** A focused project addressing a defined technical, operational, or security priority.

### Path 3 — Managed or Co-Managed Security Operations

**Examples:** Managed IT · Co-managed IT · Endpoint security · MDR · Centralized logging or SIEM · SOC support · Vulnerability management · Patch management · Managed network services · Managed backup · Managed physical-security services for supported systems, where included in the approved agreement · Managed VoIP · Recurring reporting and QBRs

**Outcome:** Ongoing operation, monitoring, maintenance, documentation, escalation, and improvement of agreed controls.

Physical-security service scope depends on supported manufacturers, system architecture, monitoring and maintenance responsibilities, remote and onsite requirements, patching responsibilities, exclusions, geographic coverage, and the approved client agreement.

*Continued — Paths 4 and 5 on the next page.*

# Ways to Engage BTI — Governance and Strategic Engagements

*Continued from previous page — Paths 1–3 cover assessments, remediation, and managed operations.*

### PATH 4 — Compliance and Evidence Readiness

**Examples:** Compliance-readiness assessment · GRC platform onboarding and evidence-management support, where included in the approved scope and supported by the selected platform and service agreement · Policy coordination · Shared-responsibility mapping · Risk assessment · POA&M tracking · Audit-preparation support · vCISO advisory or qualified security-leadership support, depending on scope and availability · Penetration-testing coordination · Cyber-insurance control and evidence readiness

**Outcome:** Better organized controls, evidence, responsibilities, remediation tracking, and preparation for external reviews.

### PATH 5 — Converged Security and AI-Governance Roadmap

**Examples:** Multi-site standards · IT and physical-security convergence · Vendor coordination · Lifecycle planning · Identity and physical-access alignment · Facilities and technology integration · Executive security roadmap · AI governance · AI-agent risk and control planning · Quarterly maturity reviews

**Outcome:** A coordinated roadmap spanning IT, cybersecurity, physical security, communications, facilities technology, compliance, and emerging AI use.

The exact scope, pricing, deliverables, and responsibilities are defined through an approved proposal, statement of work, or managed-services agreement.

# Role-Specific Guidance

Cybersecurity maturity affects every leadership role differently. The following guidance is organized by role to help each leader understand where their priorities and responsibilities intersect with the organization's security posture. Security is not only an IT concern — it is a governance, operations, finance, and compliance responsibility shared across leadership.

### CEO & Board

Focus on business risk, leadership accountability, financial exposure from incidents, operational continuity, and reputational implications. Security investment should be framed as risk management and business continuity, not solely as an IT cost. Ask for regular executive reporting that connects security posture to business outcomes and insurance obligations.

### CFO

Focus on predictable spending, cyber-insurance requirements, avoiding fragmented and overlapping purchases, risk-based prioritization of investment, lifecycle budgeting for technology refresh, and understanding the cost of compliance operations. Managed and co-managed relationships can improve cost predictability when scope, responsibilities, service levels, exclusions, licensing, and project work are clearly defined.

### CIO & IT Director

Focus on architecture decisions, internal team capacity, tool consolidation, end-to-end visibility, co-managed service relationships that extend internal capability, identity and access management, vulnerability management programs, and preparing the infrastructure for AI adoption. The goal is a rationalized technology environment with clear ownership and accountability for every control.

### COO & Facilities Leadership

Focus on operational uptime, physical security systems (cameras, access control), network infrastructure supporting facilities, communications systems including VoIP, multi-site consistency, vendor coordination, and the intersection of physical and cyber security. Physical systems that connect to networks carry cybersecurity risk and require the same deliberate governance as IT systems.

### Compliance & Risk Leaders

Focus on the distinction between controls, policies, procedures, and evidence. Risk officers need POA&M processes, shared-responsibility documentation, audit-readiness support, and recurring evidence collection. Compliance is an ongoing operating process, not a one-time documentation project. The frameworks most relevant to your industry — HIPAA, CMMC, NIST, PCI, or CIS Controls — require consistent operation and regular review, not just policy creation.

# 12-Month Sample Roadmap

The roadmap below illustrates a realistic improvement trajectory for a moderately mature organization — one that has basic tools in place but lacks consistency, documentation, ongoing monitoring, and governance. This is provided as an illustrative example. Your organization's specific roadmap should be based on a formal assessment of your current environment, risk profile, internal capabilities, and business priorities.

## 1 Days 1–30

- Identify security owners
- Inventory systems, users, devices, and critical data
- Verify MFA across critical systems
- Review critical vulnerabilities
- Validate backups and restoration readiness
- Review Microsoft 365 identity and security configuration within agreed scope
- Establish incident contacts
- Create basic AI-use guidance

## 2 Days 31–90

- Deploy or validate managed endpoint protection
- Standardize operating-system and third-party patching
- Improve email and DNS security
- Review firewall and remote-access configurations
- Begin security-awareness training
- Complete priority vulnerability remediation
- Document critical systems
- Review camera, access-control, VoIP, and connected-device security

## 3 Months 4–6

- Implement an appropriate managed monitoring, MDR, centralized logging, or SIEM approach
- Improve identity governance
- Formalize incident-response procedures
- Begin evidence collection
- Conduct a risk assessment
- Create priority policies
- Build or update the POA&M
- Review vendor and shared responsibilities

## 4 Months 7–9

- Coordinate scoped penetration testing where justified
- Improve network segmentation
- Map applicable compliance or contractual requirements
- Conduct an incident-response tabletop exercise
- Improve backup and recovery testing
- Standardize multi-site controls
- Review cloud and SaaS exposure

## 5 Months 10–12

- Complete an executive security review
- Close or reduce high-priority POA&M items
- Organize evidence for applicable external reviews
- Establish approval requirements for higher-risk AI-agent use cases
- Create the next-year security roadmap
- Establish a recurring QBR or security-review cadence

This roadmap is illustrative. Specific sequencing depends on risk, business priorities, regulatory and contractual obligations, current architecture, available resources, and the results of a formal assessment. Microsoft, penetration-testing, compliance, and AI-related activities are subject to defined scope and current service availability.

# Common Cybersecurity Investment Mistakes

Understanding where organizations commonly go wrong is as useful as understanding what to do right. The following patterns appear repeatedly across organizations of every size and industry. Recognizing them early can prevent significant wasted investment and avoidable risk exposure.

### Buying Tools Without Assigning Ownership

Technology that no one is responsible for monitoring, maintaining, or reviewing provides limited protection. Every control needs a named owner and a defined operating process.

### Treating Compliance as Documentation Only

Compliance requires controls, policies, procedures, evidence, and defined responsibility. Creating policies without implementing and documenting the associated practices generally provides insufficient evidence for an audit, assessment, insurer review, or customer security examination.

### Ignoring Identity and Permissions

Weak or compromised identities—including stolen credentials, stale accounts, inconsistent MFA, and excessive privileges—are a major source of cybersecurity risk regardless of how strong other controls are.

### Failing to Test Backups

A backup that has not been tested provides limited assurance that data and systems can be restored when needed. Organizations should test restoration procedures on a documented schedule appropriate to system criticality, recovery objectives, and risk.

### Scanning for Vulnerabilities Without Fixing Them

Vulnerability scanning identifies potential weaknesses. Without a remediation process, prioritization criteria, and tracking, scanning produces reports that accumulate without improving security posture.

### Assuming an MSP or Vendor Handles Everything

Organizations should not assume that any provider handles every aspect of security unless the responsibilities are explicitly included in the agreement. Shared responsibility must be documented. Gaps between vendor scopes are a common source of unaddressed risk.

### Securing Servers While Ignoring Cameras, VoIP, and IoT

Physical-security systems, VoIP infrastructure, and connected devices are part of the network attack surface. Leaving them unpatched, on default credentials, or on the same network segment as critical systems creates exploitable pathways that traditional security programs often miss.

### Deploying AI Before Establishing Data Governance

AI tools that access organizational data without data-classification standards, access controls, or approved workflows create significant data-exposure risk. Governance must precede broad AI deployment, not follow it.

### Allowing AI Agents to Use Broad Privileges

AI agents that operate with excessive permissions can execute consequential actions — modifying records, sending communications, triggering workflows — without human review. Least-privilege access, defined authorization boundaries, logging, testing, monitoring, and rollback procedures should be treated as foundational controls before deploying AI agents that can take consequential actions.

### Collecting Logs Without Reviewing Them

Log collection alone may support investigation and retention requirements, but timely detection requires appropriate analytics, alerting, review, and response processes. SIEM and managed monitoring services add detection and response capability that log collection alone does not provide.

### Treating Penetration Testing as Ongoing Security

Penetration testing tests security using controlled attack methods at a point in time. It is a valuable input to risk management and compliance programs, but it is not a substitute for continuous vulnerability management, patching, and monitoring.

### Trying to Reach Maximum Maturity Immediately

Organizations that attempt to implement every control simultaneously typically end up with an inconsistent, poorly managed environment. Prioritizing by risk and building in stages produces more durable improvement than attempting to shortcut the maturity progression.

# Questions to Ask a Security Provider

When evaluating a security partner, managed service provider, or technology vendor, the quality of their answers to the following questions will tell you a great deal about the depth and consistency of what they actually deliver. Strong partners answer these questions clearly and in writing. Vague or avoidant answers warrant follow-up.

## Operations and Accountability

- Who owns each control, and how is that documented?
- What is monitored continuously, and what is reviewed periodically?
- What evidence will we receive that controls are operating?
- How are vulnerabilities prioritized and remediated?
- How are patches managed across different device types?
- How is Microsoft 365 specifically secured and monitored?
- What Microsoft 365 security features and configurations are included in your engagement, and what depends on client licensing, architecture, or separate project scope?
- How are physical-security systems protected against cyber threats?
- How are backups tested, and how often?
- Who performs penetration testing — internal staff or a qualified third-party provider? How is scope defined and agreed upon?

## Incidents, AI, and Reviews

- What happens during a security incident — who does what and in what order?
- Who coordinates responsibilities across multiple vendors?
- How are vendor responsibilities documented, and what is explicitly excluded from your scope?
- How is employee use of AI governed and monitored?
- How are AI agents approved before deployment and monitored afterward?
- Which AI-related services are fully productized with defined methodology, deliverables, and pricing — and which are advisory or scoped per engagement?
- What is included in the base agreement versus separately billable?
- How are results reviewed on a quarterly basis?
- How does your engagement model evolve as our organization matures?

A capable security partner will have documented answers to all of these questions. If a provider cannot explain how they handle incident response, evidence collection, vulnerability remediation, penetration testing scope, or AI governance, that is important information before signing an agreement.

# Why Organizations Engage BTI

BTI Communications Group is a converged technology partner that helps organizations coordinate managed IT, cybersecurity, networking, cloud services, physical security, VoIP, compliance operations, and supporting infrastructure. BTI is not a software manufacturer, a cloud-platform operator, a regulator, a compliance certifier, an independent auditor, a law firm, or an insurer. BTI may use, resell, integrate, administer, coordinate, or support third-party platforms and qualified specialist partners depending on the engagement. Exact responsibilities must be defined in the client agreement.

Many organizations find that security and infrastructure responsibilities are fragmented across several vendors — each managing a portion of the environment without meaningful coordination. This creates gaps in coverage, unclear escalation paths, inconsistent documentation, and situations where no single party takes ownership of an issue that spans multiple domains. BTI's converged approach is designed to reduce these gaps.

### Integrated Capabilities

Managed IT, co-managed IT, cybersecurity, network infrastructure, Microsoft and cloud security, physical security, access control, video surveillance, VoIP, compliance operations, PMO and project delivery, and AI governance and governed AI adoption planning — coordinated rather than siloed.

### Fewer Handoff Gaps

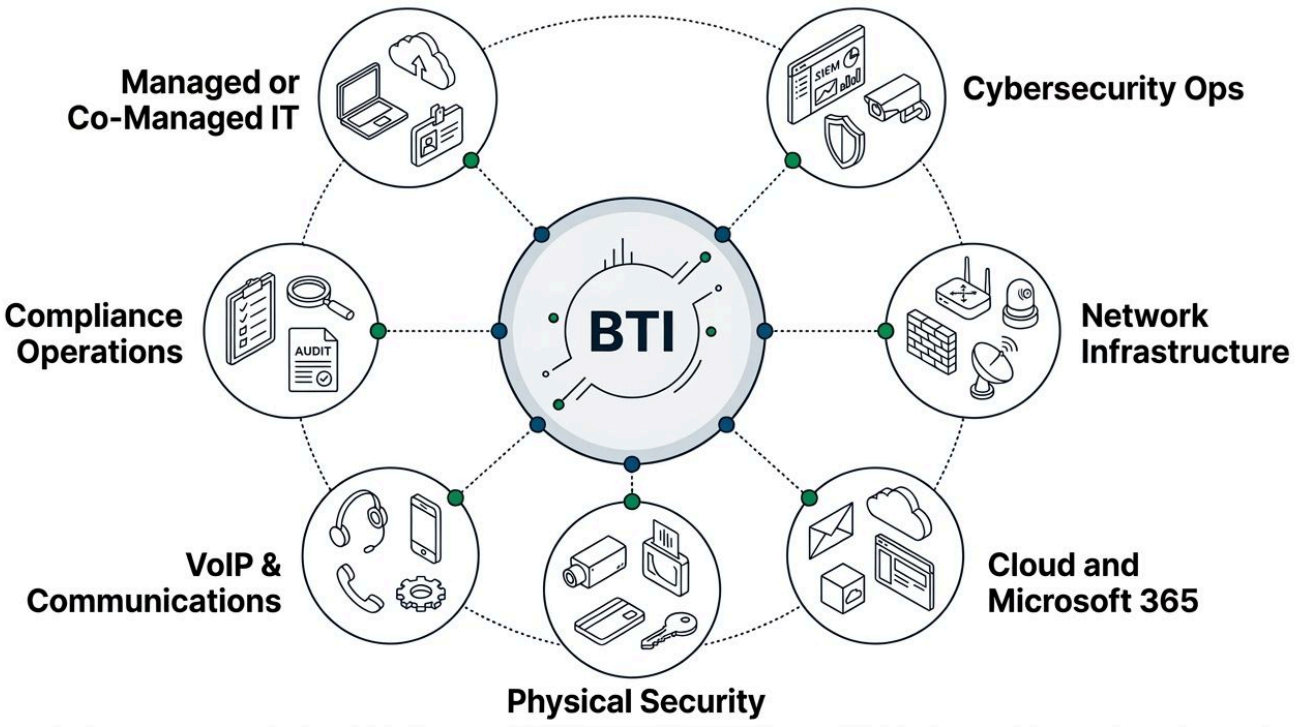
When IT, cybersecurity, physical security, and communications are managed through coordinated relationships, the gaps between vendor scopes shrink. BTI designs engagements with shared standards, defined escalation paths, and clear accountability across domains.

### Better Documentation

Consistent documentation of configurations, assets, vendor responsibilities, evidence records, and security posture supports both operational continuity and compliance readiness. BTI's managed relationships emphasize configuration management and evidence collection as ongoing operations.

### Realistic Roadmaps

BTI's strategic model is based on helping customers modernize in stages, beginning with an assessment or project and building toward broader managed relationships as the organization's maturity and requirements grow. Organizations can start with a single engagement and expand over time.




**AI Governance and Governed AI Adoption Advisory Options**

Possible engagements may include, subject to scope and current BTI service availability:

- AI-use governance and policy guidance
- Approved and prohibited AI-tool guidance
- Identity and permissions review for proposed AI workflows
- AI application and vendor inventory planning
- Shadow AI risk discussion or discovery planning
- AI-agent risk and control planning
- Microsoft 365 and cloud-security review within agreed scope
- Coordination with qualified legal, privacy, compliance, application-security, software-development, or other specialist providers where required

AI-related services are subject to scope, available tooling, client architecture, risk level, third-party dependencies, and current BTI service availability.

BTI helps, supports, designs, assesses, integrates, implements, administers, manages, coordinates, monitors, advises, prepares, and improves — but does not guarantee prevention of all incidents, certify compliance, eliminate all risk, cover every platform, or replace legal counsel. BTI's value is in coordination, consistency, and the ability to grow with your organization over time.

# Selected Authoritative References — Cybersecurity and AI Frameworks

The following numbered references support key concepts in this guide and provide additional authoritative resources. Standards, regulations, government guidance, vendor platforms, and insurance expectations change over time. Organizations should confirm current requirements with the appropriate regulator, standards body, legal counsel, insurer, auditor, customer, or qualified specialist.

**[1] NIST Cybersecurity Framework 2.0** — National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, published February 26, 2024. Organizes cybersecurity outcomes into six functions: Govern, Identify, Protect, Detect, Respond, and Recover. **doi.org/10.6028/NIST.CSWP.29** — **nist.gov/cyberframework**

**[2] NIST AI Risk Management Framework 1.0** — National Institute of Standards and Technology. AI Risk Management Framework (AI RMF 1.0), published January 2023. Provides a voluntary framework for managing risks associated with AI systems across four functions: Govern, Map, Measure, and Manage. **doi.org/10.6028/NIST.AI.100-1**

**[3] NIST AI 600-1 Generative AI Profile** — National Institute of Standards and Technology. AI RMF Generative AI Profile (NIST AI 600-1), published July 2024. Addresses risks specific to generative AI systems including data privacy, hallucination, harmful content, and misuse. **doi.org/10.6028/NIST.AI.600-1**

**[4] CISA Known Exploited Vulnerabilities Catalog** — Cybersecurity and Infrastructure Security Agency. Maintained continuously. Lists vulnerabilities with confirmed evidence of active exploitation. Used to inform remediation prioritization beyond severity score alone. **cisa.gov/known-exploited-vulnerabilities-catalog**

**[5] CIS Critical Security Controls v8.1** — Center for Internet Security. A prioritized set of cybersecurity safeguards organized into Implementation Groups, designed to help organizations reduce common and significant cybersecurity risks. **cisecurity.org/controls**

**[6] HIPAA Security Rule** — U.S. Department of Health and Human Services. Establishes administrative, physical, and technical safeguard requirements for protecting electronic protected health information. **hhs.gov/hipaa/for-professionals/security**

*Continued — References [7]–[11] on the next page.*

# Selected Authoritative References — Programs, Standards, and Vendor Guidance

Most references are cited directly in the guide. CISA Secure by Design is included as an additional authoritative resource on secure-default and design-accountability principles.

**[7] CMMC Program** — U.S. Department of Defense. Cybersecurity Maturity Model Certification (CMMC) Program. Applies to organizations in the Defense Industrial Base. **dodcio.defense.gov/CMMC**

**[8] PCI DSS v4.0.1** — PCI Security Standards Council. Payment Card Industry Data Security Standard. Applies to entities that store, process, or transmit cardholder data and to certain systems, environments, or service providers that can affect the security of the cardholder data environment. **pcisecuritystandards.org**

**[9] Microsoft Security Documentation** — Microsoft Corporation. Official Microsoft security, identity, and compliance documentation covering Microsoft 365 Defender, Microsoft Entra ID, Microsoft Purview, Azure security, and related products. **learn.microsoft.com/en-us/security** — **microsoft.com/en-us/security**

**[10] CISA Secure by Design** — Cybersecurity and Infrastructure Security Agency. Guidance on reducing security risk through design, default configurations, and accountability. **cisa.gov/securebydesign**

**[11] ISO/IEC 27001:2022** — International Organization for Standardization. Information Security Management Systems — Requirements. Describes requirements for establishing, implementing, maintaining, and continually improving an information security management system. **iso.org/standard/27001**

# Start With Clarity

You do not need to solve every cybersecurity, compliance, infrastructure, and AI risk at once. Organizations improve most effectively when they understand their current position, prioritize deliberately, assign clear ownership, and build on a practical roadmap.

> BTI Communications Group can help you assess your current maturity, prioritize investment, and build a practical roadmap for stronger cybersecurity, infrastructure, compliance readiness, and governed AI adoption.

### Schedule a Cybersecurity Maturity Discussion

Begin with a focused conversation about your organization's current posture, business priorities, internal capabilities, and practical next steps.

Call 800-435-7284 or visit **btigroup.com/contact**

---

### Phone

**800-435-7284**

### Contact BTI Online

**btigroup.com/contact**

### What to Expect

A focused discussion of current conditions, priority gaps, shared responsibilities, and practical next steps.

*Already know what you need? Ask about managed IT, co-managed IT, cybersecurity, compliance readiness, remediation, physical security, VoIP, or converged-security planning.*

---

**BTI Communications Group** helps businesses integrate managed IT, cybersecurity, networking, cloud communications, video surveillance, access control, and physical security into a secure, scalable technology ecosystem.

Proudly serving businesses throughout **Los Angeles, Chicago, and Phoenix**.

BTI COMMUNICATIONS GROUP | MANAGED IT & CYBERSECURITY | PHYSICAL SECURITY | VOIP & CLOUD COMMUNICATIONS