



FOR CEOS, COOS, CFOS AND IT LEADERS AT REGULATED AND MULTI-SITE ORGANIZATIONS

Cybersecurity Maturity Roadmap

Find your organization's cybersecurity maturity level in 15 minutes, see what to invest in first, and build a 12-month plan aligned with NIST CSF 2.0.

A plain-language roadmap with six maturity levels, a fillable 22-question self-assessment, a 2026-2027 compliance calendar, AI and agentic-AI guardrails, and a 12-month action plan.

INSIDE THIS GUIDE

- Six maturity levels from reactive to AI-governed
- Fillable 22-question self-assessment with score bands
- 2026-2027 calendar: CMMC, HIPAA, PCI DSS, Windows 10 ESU
- Where to invest first, by impact and urgency
- 12-month roadmap and roles

Talk to a BTI business advisor

Review your maturity score with a BTI business advisor and get a prioritized 12-month roadmap.

National
800-435-7284
info@btigroup.com

LOS ANGELES 323-510-8002 CHICAGOLAND 312-432-5300 PHOENIX 602-733-6807
www.btigroup.com/contact • www.btigroup.com/it-services/cybersecurity/

Serving businesses since 1985 • Integrated security since the 2010s • ISO 27001 compliant • GSA, CMAS & TESMA contracts • ACO licensed in CA, AZ & IL

At a glance

SHORT ANSWER

Cybersecurity maturity describes how consistently an organization governs, protects, detects, responds to and recovers from cyber risk, the six functions of NIST CSF 2.0.[1] This roadmap uses six practical levels, from **Level 0 (Reactive)** to **Level 5 (Advanced and AI-Governed)**. Score yourself with the 22-question assessment, then fund the foundational gaps first: identity and MFA, patching, backups, logging and clear ownership.

\$4.44M

Global average cost of a data breach;
US average \$10.22M
IBM Cost of a Data Breach 2025[6]

6

NIST CSF 2.0 functions: Govern,
Identify, Protect, Detect, Respond,
Recover
NIST CSWP 29, Feb 2024[1]

Oct 14, 2026

Windows 10 commercial ESU Year 2
begins (\$122 per device)
Microsoft[9]

Contents

The six maturity levels	3
Self-assessment (fillable)	4
2026-2027 compliance and risk calendar	6
AI and agentic-AI guardrails	7
How BTI helps	8
Frequently asked questions	9
Sources and change log	10

The six maturity levels

Level	Name	Typical posture	Priority investments
0	Unstructured and reactive	No owner, no policies, fixes when things break	Name an owner; MFA; backups; asset list
1	Foundational	Owner and basic policies; MFA rolling out	Endpoint protection, patching cadence, training
2	Managed	Core tools in place but inconsistent	Monitoring, vulnerability management, IR plan
3	Governed	Policies, risk register, evidence for audits and insurers	Vendor management, tested recovery, metrics
4	Integrated and converged	IT, cyber, physical security, VoIP and facilities coordinated	Segmentation of cameras and building systems, unified monitoring
5	Advanced and AI-governed	Continuous improvement; AI use governed	AI risk reviews per use case; agent guardrails

Levels describe dominant operating postures, not rigid gates; most organizations work on several at once.

Self-assessment (fillable)

Score each question: **0** = not in place, **1** = partially, **2** = mostly, **3** = implemented, reviewed and current. Maximum 66.

#	Question	Area	0	1	2	3
1	Is there a named individual or team responsible for cybersecurity decisions?	Governance	☐	☐	☐	☐
2	Does a formal security policy exist, reviewed in the past 12 months?	Governance	☐	☐	☐	☐
3	Is MFA enforced for all users on email, remote access, admin accounts and critical cloud apps?	Identity	☐	☐	☐	☐
4	Are user accounts reviewed and promptly disabled when employees leave?	Identity	☐	☐	☐	☐
5	Do employees receive security-awareness training at onboarding and periodically after?	Users	☐	☐	☐	☐
6	Is there a written policy on acceptable and prohibited use of AI tools?	Users	☐	☐	☐	☐
7	Is managed endpoint protection deployed and actively monitored on all in-scope endpoints?	Devices	☐	☐	☐	☐
8	Are OS and third-party patches applied on a consistent, documented schedule?	Devices	☐	☐	☐	☐
9	Is the network segmented to separate critical systems, IoT and guest traffic?	Networks	☐	☐	☐	☐
10	Are firewall and remote-access configurations documented and regularly reviewed?	Networks	☐	☐	☐	☐
11	Is Microsoft 365 or your primary cloud identity platform configured to an approved security baseline and monitored?	Cloud	☐	☐	☐	☐
12	Are SaaS application access and permissions reviewed on a recurring basis?	Cloud	☐	☐	☐	☐
13	Is vulnerability scanning performed on a schedule with results tracked?	Vulnerabilities	☐	☐	☐	☐
14	Are vulnerabilities prioritized (including CISA KEV) and remediated on defined timelines?	Vulnerabilities	☐	☐	☐	☐
15	Are security logs collected centrally with alerting, review and response?	Monitoring	☐	☐	☐	☐
16	Is there a documented incident-response plan with named contacts and escalation steps, tested in the past year?	Incident response	☐	☐	☐	☐
17	Are backups and restores tested on a schedule, with results reported to leadership?	Backup	☐	☐	☐	☐

#	Question	Area	0	1	2	3
18	Is evidence of controls organized for audits, customers, contracts and cyber insurance?	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 and maintained?	Communications	☐	☐	☐	☐
21	Are vendor security responsibilities documented and reviewed?	Vendors	☐	☐	☐	☐
22	Is there an approved AI-tool list and a review process (with human approval) for AI agent deployments?	AI governance	☐	☐	☐	☐

Total score: out of 66 · Percent: %

Percent of 66	Result	Focus
0-25%	Reactive	Ownership, visibility and immediate risk reduction
26-45%	Foundational	Consistent preventive controls and documentation
46-65%	Managed	Continuous monitoring, remediation and response
66-80%	Governed	Integrated policy, evidence and risk management
81-90%	Integrated	Coordinated IT, cyber, physical and vendor security
91-100%	Advanced and AI-governed	Use-case-specific AI risk reviews and automation

Directional and educational only; not an audit, certification or compliance determination. A low score on identity, backups or incident response needs attention even if the total is high.

Talk to a BTI business advisor about your cybersecurity maturity results

A BTI business advisor will review your sites, current systems and requirements, then outline options, timelines and budget ranges. No obligation.

[Contact a BTI business advisor](#)

[Cybersecurity services](#)

Call **800-435-7284** (national) · Los Angeles **323-510-8002** · Chicagoland **312-432-5300** · Phoenix **602-733-6807** · info@btigroup.com

2026-2027 compliance and risk calendar

Date	Item
Mar 31, 2025	PCI DSS v4.0.1 future-dated requirements mandatory[7]
June 3, 2026	SEC Reg S-P amendments apply to smaller covered institutions[10]
July 13, 2026	DoD memo suspends CMMC Phase 2; L1/L2 self-assessments continue; DFARS 7012 still applies[8]
Oct 14, 2026	Windows 10 ESU Year 2 starts (\$122 per device; enrolling late means paying for Year 1 too)[9]
July 2027	Projected final action on the HIPAA Security Rule update; current rule enforceable[11]

Where to invest first

Category	Examples	When
Foundational	MFA everywhere, offboarding, patching, tested backups, asset inventory	Now (0-90 days)
Detect and respond	Managed endpoint detection, central logging and alerting, IR plan and tabletop	3-6 months
Govern	Policies, risk register, vendor reviews, evidence for insurers and auditors, vCISO	6-12 months
Converge and advance	Segment cameras and building systems, unify monitoring, AI governance	9-18 months

Prioritize by exploitation, not just severity: use the CISA Known Exploited Vulnerabilities catalog to set remediation order.[4] CIS Controls v8.1 Implementation Group 1 is a practical baseline for smaller teams.[5]

AI and agentic-AI guardrails

- Approved AI-tool list and data rules (what may and may not be entered).
- Use-case risk reviews aligned with the NIST AI RMF and its Generative AI Profile.[2][3]
- For AI agents: least-privilege access, human approval for changes, logging of agent actions, and a kill switch.
- Vendor contracts that address data retention and model training on your data.

12-month roadmap

Quarter	Focus	Owner
Q1	MFA gaps, offboarding, backup test, asset inventory, IR contacts	IT lead and security owner
Q2	Endpoint detection and logging, vulnerability program, training	IT lead or MSP
Q3	Policies and evidence, vendor reviews, tabletop exercise	Security owner or vCISO
Q4	Segmentation of IoT and security devices, AI governance, reassessment	Leadership and IT

How BTI helps

BTI provides cybersecurity assessments, vCISO and governance support, managed and co-managed IT, network security and security-system integration, so one partner can coordinate IT, cyber and physical security. BTI is ISO 27001 compliant.

Related BTI pages: [Cybersecurity](#) · [Cybersecurity assessment](#) · [vCISO](#) · [Governance, risk and compliance](#) · [Incident response plan guide](#) · [Cybersecurity 2026 guide](#)

About BTI Communications Group

BTI Communications Group (BTI Group) has served businesses since 1985 (40 years) and has delivered integrated security systems since the 2010s, alongside managed IT, cybersecurity services, networking and business communications. BTI focuses on high-security, regulated and multi-site organizations in healthcare, financial services, logistics, manufacturing, education and the public sector.

Credential	Detail
Security management	ISO 27001 compliant information security practices
Public-sector contracts	GSA, CMAS and TESMA contract vehicles
Licensing	Alarm Company Operator (ACO) licenses in California, Arizona and Illinois
Offices	Los Angeles 323-510-8002 · Chicagoland 312-432-5300 · Phoenix 602-733-6807 · National 800-435-7284

Frequently asked questions

What is a cybersecurity maturity model?

A staged description of how consistently an organization manages cyber risk. This roadmap uses six levels aligned with NIST CSF 2.0 functions.[1]

How long does the self-assessment take?

About 15 minutes for a leader who knows the environment; involve IT for accuracy.

What should a small or mid-size organization fix first?

MFA, offboarding, patching, tested backups, an asset inventory and a named security owner.

Is CMMC still required in 2026?

CMMC Phase 2 was suspended by a July 13, 2026 DoD memo; Level 1 and Level 2 self-assessments continue and DFARS 7012 applies. Check the DoD CIO site for updates.[8]

What do cyber insurers usually ask for?

Typical questions cover MFA, endpoint detection, backups, patching, incident response and training; requirements vary by carrier.

Ready to scope your cybersecurity maturity results?

A BTI business advisor will review your sites, current systems and requirements, then outline options, timelines and budget ranges. No obligation.

[Contact a BTI business advisor](#)[Cybersecurity services](#)

Call **800-435-7284** (national) · Los Angeles **323-510-8002** · Chicagoland **312-432-5300** · Phoenix **602-733-6807** · info@btigroup.com

Sources and change log

1. NIST, Cybersecurity Framework 2.0 (CSWP 29), Feb 26, 2024. <https://doi.org/10.6028/NIST.CSWP.29>
2. NIST, AI Risk Management Framework 1.0 (AI 100-1), Jan 2023. <https://doi.org/10.6028/NIST.AI.100-1>
3. NIST, AI RMF Generative AI Profile (AI 600-1), July 2024. <https://doi.org/10.6028/NIST.AI.600-1>
4. CISA, Known Exploited Vulnerabilities Catalog. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
5. Center for Internet Security, CIS Critical Security Controls v8.1. <https://www.cisecurity.org/controls>
6. IBM, "Cost of a Data Breach Report 2025." <https://www.ibm.com/reports/data-breach>
7. PCI Security Standards Council, PCI DSS v4.x. <https://www.pcisecuritystandards.org/standards/pci-dss/>
8. DoD CIO, "Implementing Suspension of CMMC Phase II," memo dated July 13, 2026. <https://dodcio.defense.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf>
9. Microsoft Learn, "Extended Security Updates for Windows 10." <https://learn.microsoft.com/windows/whats-new/extended-security-updates>
10. SEC, "Regulation S-P" amendments (compliance Dec 3, 2025 and June 3, 2026). <https://www.sec.gov/rules-regulations/2024/06/s7-05-23>
11. Unified Agenda, RIN 0945-AA22 (HIPAA Security Rule NPRM; final action 07/2027). <https://www.reginfo.gov/public/do/eAgendaViewRule?RIN=0945-AA22&pubId=202510>

Change log. 2027 edition proof v1 (Oct 11, 2026): refreshed and condensed from 22 pages. Kept the six-level model and 22-question assessment (now fillable); added the 2026-2027 calendar (CMMC suspension, HIPAA timing, Windows 10 ESU, Reg S-P), agentic-AI guardrails, clickable links and metadata.