

How We Approach Your Assessment

The principles behind every Southern Technology Partners security assessment

We assess your organization the way a professional security practitioner would: against recognized principles, with evidence rather than opinion, and with the goal of practical improvement rather than a perfect score. This page explains the thinking you'll see in our questions, findings and recommendations.

What we protect: the CIA triad

Confidentiality

Only the right people can see sensitive information.

Personnel files, payment cards, health records, criminal justice data, residents' personal information.

Integrity

Information is accurate and hasn't been changed without authorization.

Tax bills, utility accounts, court records, payroll and bank details stay correct.

Availability

Systems and information are there when people need them.

911 and dispatch, the tax office, billing and email keep working, and come back quickly if they stop.

Every finding we report ties back to at least one of these three. We also look at accountability: knowing who did what, through unique logins and logs.

How we think about risk

Risk = Likelihood × Impact. We look at what you have (assets), what could go wrong (threats), and the weak spots that would let it happen (vulnerabilities). A weakness on a system that matters most to your residents or customers gets a higher priority than the same weakness somewhere less important.

For each risk, leadership chooses one of four responses. Our job is to make that choice informed and written down, not to make it for you.

Avoid

Stop the risky activity.

Retire an unsupported server; stop storing card numbers.

Reduce

Add controls to lower likelihood or impact.

Turn on MFA; segment the network; test backups.

Transfer

Shift the financial impact to someone else.

Cyber insurance; security terms in vendor contracts.

Accept

Knowingly live with it, in writing.

Signed by leadership, with a reason and a review date.

Principles we apply

Principle	What it means for you
Defense in depth	No single control is trusted alone. Firewall, MFA, patching, backups, cameras and locked doors each cover for the others when one fails.
Least privilege and need to know	People and systems get only the access their job requires, nothing more. Admin rights are the exception, not the default.
Separation of duties	No one person can both make and approve a sensitive change, such as a new vendor bank account or an admin account.
Verify, don't assume (zero trust)	We confirm settings and see evidence. "It should be on" isn't the same as "it is on."

Secure by default	Default passwords changed, unneeded services off, new systems set up safely from day one.
Due care and due diligence	Doing what a reasonable organization would do, and being able to show it. This matters to insurers, auditors and courts.
Fail safe	When something breaks, it should break in the safe direction: doors that let people out in a fire, accounts that lock after repeated failed logins.
Keep it simple	Fewer, well-understood controls beat a complicated setup nobody can maintain.

The eight areas we review

Our review follows the eight domains of the CISSP Common Body of Knowledge, the framework security professionals are trained and certified on, translated into plain terms.

Domain	What we look at in your organization
1 Security and risk management	Policies, who is responsible, risk assessment, laws and rules that apply to you, insurance
2 Asset security	What devices and data you have, where sensitive data lives, how it's kept and destroyed
3 Security architecture and engineering	How systems are built and configured, encryption, physical security of buildings and server rooms
4 Communication and network security	Firewalls, Wi-Fi, network separation, remote access, email security
5 Identity and access management	Logins, MFA, admin rights, adding and removing users, door access and keys
6 Security assessment and testing	Vulnerability scans, configuration checks, re-testing that fixes actually happened
7 Security operations	Patching, monitoring and alerts, backups, incident response, disaster recovery
8 Software development security	The software and cloud services you rely on, vendor updates and settings, websites and payment pages

Resilience, not just protection

No organization can prevent every incident. We measure how well you can handle one, following the six functions of the NIST Cybersecurity Framework 2.0.

GOVERN Leadership, policy and accountability	IDENTIFY Know what you have and what matters most	PROTECT Put safeguards in place	DETECT Notice when something is wrong	RESPOND Act quickly with a plan	RECOVER Get back to normal, and learn
--	---	---	---	---	---

How we work with you

Independent We check the work; we don't replace your IT provider.	Evidence-based Every finding is backed by what we saw, not a guess.	Plain English Leadership gets a clear summary; IT gets a step-by-step fix list.	Practical Fixes are prioritized by risk and budget, not perfection.	Confidential Your findings stay between us, you and the people you choose.
---	---	---	---	--

Southern Technology Partners · 15 Latimer St., Hazlehurst, GA 31539 · (912) 209-4804 · southernpartners.net
 Our approach draws on the CISSP Common Body of Knowledge published by ISC2, NIST Cybersecurity Framework 2.0 and CIS Controls v8.1.
 CISSP is a registered certification mark of ISC2; this page describes the principles we apply and is not an ISC2 publication.