Cybersecurity Services

Every Good Cybersecurity Program Begins With Questions.

- Do we know where our key cyber risks exist?
- Are we addressing these risks? Can we demonstrate how?
- What gaps do we have in compliance (either with security best practices or regulatory frameworks)?
- Do we have a cybersecurity program in place? Does it encompass the whole organization?
- Do we have emergency response and recovery plans? Have they been practiced and tested?
- Are we addressing risks related to vendors and third parties?

How Can Weaver Help You?

To be effective, your organization's cybersecurity program must provide an ongoing process that assesses risks, identifies threats, creates protections, monitors systems, and enables quick response and recovery. And that cybersecurity process must be embedded into the organization's governance, not just relegated to a corner of the IT department.

Weaver's IT Advisory Services team understands that cybersecurity has to be built into your organization from the ground up.

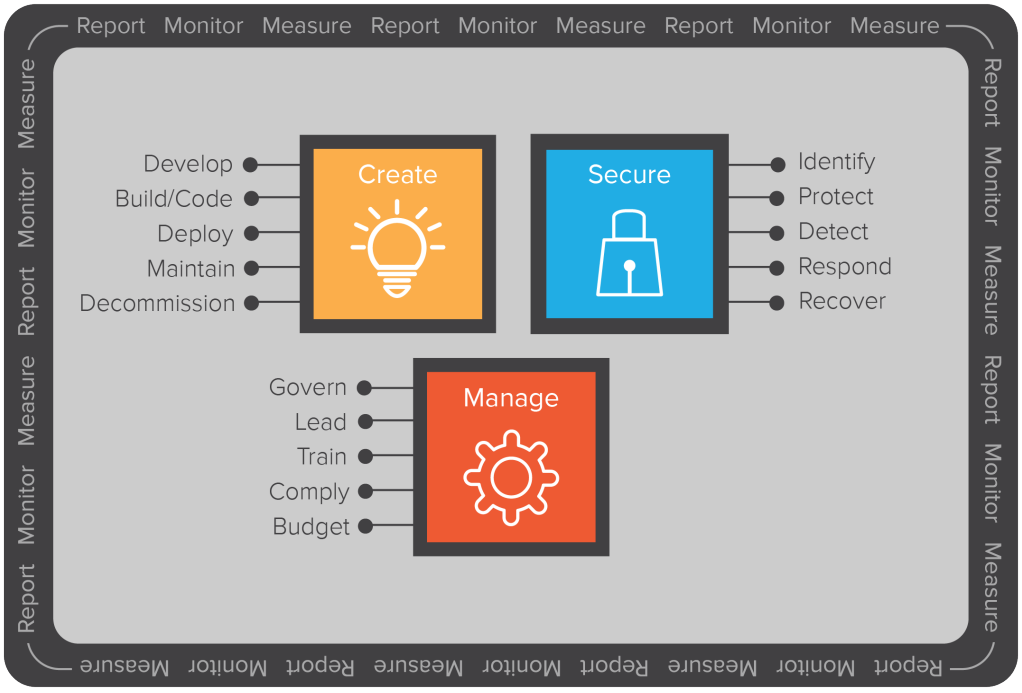
We regularly assess systems and processes against a variety of technical and regulatory requirements, including PCI, Red Flags, Sarbanes-Oxley, HIPAA, FDICIA and GLBA, and we are well-versed in the standards and control frameworks used by leading organizations to manage compliance with these regulations, including:

- NIST-CSF
- COBIT 2019
- ISO 27001/27002
- SOC 1, 2 and 3
- SOC for Cybersecurity
- PCI DSS
- 23 NYCRR 500
- FISMA
- NIST SP 800-53
- FFIEC
- ITIL
- HIPAA

weaver
Assurance • Tax • Advisory

The Cybersecurity Landscape

Weaver looks at your IT environment based on organizational practices to go beyond standards and address cybersecurity at the root of what you do.



Weaver's Cybersecurity Services

CYBER RISK MANAGEMENT	CYBER COMPLIANCE	CYBER OPERATIONS

▶ Build/assess cybersecurity programs
▶ Conduct cyber risk assessments
▶ Define strategic roadmaps
▶ Evaluate KPIs for cybersecurity skills and tools
	▶ Measure your readiness for achieving compliance
	▶ Identify the current compliance state and goal
	▶ Outline a path towards goals
	▶ Verify to others
	▶ Communicate the competitive advantage
	▶ Develop a maintenance program and maturity plan
		▶ Vulnerability assessments
		▶ Penetration tests
		  ▶ Network services
		  ▶ Web applications
		  ▶ Wireless networks
		▶ Social engineering & security awareness
		  ▶ E-mail phishing
		  ▶ USB media drops/ baiting

For more information visit weaver.com.

weaver
Assurance • Tax • Advisory