Elfsec LLC
3743 Jocelyn St NW
Washington, DC 20015
202-237-7280

Services and Capabilities

CUI Protection

The protection of Controlled Unclassified Information (CUI), regardless of where it resides, is a lead goal of the U.S. Federal Government. While all agencies protect this information, the safeguards implemented are not uniform and that can sometimes create reluctance to sharing this information. Both federal and non-federal organizations are subject to requirements to protect CUI under 32 Code of Federal Regulations (CFR) Part 2002. Elfsec has experience assisting non-federal organizations conduct compliance gap assessments against the requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. We can assess your compliance posture with a quick gap assessment, or provide a more in-depth assessment exploring compliance needs and proposing a plan of action. We also provide full life-cycle and maintenance support depending on your needs.

Risk Management and Cybersecurity Frameworks

The Federal IT Risk Management Framework (RMF), defined in NIST SP 800-37 is a robust program for the implementation and maintenance of cyber security controls. Elfsec LLC provides full support for RMF implementation and compliance assessments as required by the Federal Information Security Modernization Act (FISMA) and related Government-wide policies.

The Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) was developed in support of Executive Order 13636 (EO), "Improving Critical Infrastructure Cybersecurity," on February 12, 2013. The Framework is technology neutral and relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience. Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

1. Describe their current cybersecurity posture;
2. Describe their target state for cybersecurity;
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4. Assess progress toward the target state;
5. Communicate among internal and external stakeholders about cybersecurity risk.

Elfsec assesses organizational cybersecurity posture and implements the Framework according to all the applicable regulatory requirements related to their industries and client-base.

For additional information on the Trust Frameworks we support, please visit https://elfsec.com/frameworks.

Elfsec LLC
3743 Jocelyn St NW
Washington, DC 20015
202-237-7280

Cloud Technology

Elfsec can facilitate your transition to "the Cloud." We assist organizations in the selection of Cloud Service Providers (CSPs); planning and implementation of cloud migration strategies; and on-going monitoring of cloud-based system controls. Adoption of cloud strategies requires a shift in operations and maintenance from in-house hosting and Elfsec can assist in updating relevant policies and procedures to help realize their full potential.

Elfsec has assisted commercial organizations providing cloud based services to Federal agencies and supported two Third Party Assessment Organizations (3PAOs) under the Federal Risk and Authorization Management Program (FedRAMP).

Contingency Planning and Incident Response

Elfsec has developed a methodology for developing and testing Contingency Plans in support of continuity of operations to minimize the impact of unexpected events. Contingency Plans can make the difference between a fairly routine event and a mission interrupting situation. Training personnel on their contingency responsibilities and testing the Contingency Plan's effectiveness are critical to avoiding major service interruptions. Our methodology allows various levels of testing, including exercises that challenge readiness without threatening actual operations.

Policies and Procedures

Elfsec works with executive leaders and operational stakeholders to identify mission, regulatory, and business requirements and formulate policies that are consistent with those priorities. The availability of adequate and actionable policies and procedures are critical to demonstrating the proper design and implementation of security controls. As most organizations are subject to financial audits, service attestations, and security compliance assessments, development of the appropriate policies and procedures is critical. IT policies and procedures can also be critical in demonstrating due care during legal challenges and inspections. Elfsec has experience assessing IT and cyber security policies and procedures and have also helped develop IT and related risk management policies and procedures to help reduce service interruptions.

Cyber Risk Management

Elfsec provides risk management services based on risk management tools and techniques that include:

- Strategic planning;
- Uniformly implemented and applied IT, cyber security, and privacy policies and procedures;
- Continuous security monitoring;
- Documentation and tracking of control weakness remediation activities;
- Implementation of government and industry defined cyber security frameworks and guidance;
- Training including security awareness, contingency plan, incident response, etc.