

A close-up, low-angle shot of a laptop keyboard and trackpad. A black padlock is placed on the trackpad area, symbolizing security. The background is a soft, out-of-focus blue.

Information Assurance & Security

Due to the increased risk of Information Technology attacks, from leaks of classified data involving the mission-critical activities of our troops in the warzone to blatant credit card and identity theft in the banking and healthcare sectors, the need for advanced information security standards and controls has never been greater.

Our team employs processes and technologies that bring peace of mind to its customers. Whether data is proprietary for financial (banking attacks), medical (health records), or national security reasons, the practices we follow and the sensitivity of our mission is the same. By providing a proactive analysis and response, we are able to allow our customers to minimize disruptions to the organization while mitigating potentially hazardous risks.

Standards Followed

- NIST
 - FISMA
 - FIPS
 - SCAP
 - SP 800 Series
- HIPAA
- PCI DSS
- ISO 27000 Series
- DIACAP
- NSTISSP

The Experts, Inc. is a professional services provider of IT and engineering support services, both within the public and private sector. Incorporated in 1998, we have built a reputation as a go-to solution provider in both the commercial market (Fortune 100 companies, banking/financial institutions, technology manufacturers) and the federal market (civilian, defense and intelligence agencies).

Exceeding Expectations

The Experts, Inc. is an Equal Opportunity/Affirmative Action (M/F/D/V) Employer.

Proactive, Preemptive Approach

The key to managing any information security vulnerabilities is anticipation. Passive information security efforts such as signature-based system patches, firewall protection and active vulnerability scanning, while absolutely necessary, are only a portion of an appropriate Information Assurance strategy. Let The Experts, Inc. guide your efforts by augmenting your existing IT governance strategies with the tools and processes required to preempt and respond to threats.

Integrating the appropriate security controls into a complex environment without adversely affecting your operational standards is not a simple task. Our professionals have the knowledge and experience to assist in aligning your IT security program with your business strategy. By transparently integrating security within your systems development and maintenance operations, our professionals can ensure that all levels of your organization understand your specific security needs and actively participate in securing your enterprise.

Our team will meet with key personnel to discuss goals and timeframes. We will then assess the environment, perform gap analysis, remediation plans, and awareness training, all using proven industry best practices. From this assessment we create a CONOPS from which the security plan can be formulated. If our team is retained to implement the CONOPS, the team would come in with the tools, knowledge, and experience to implement the plan. Once the CONOPS implementation is completed, our team can be retained iteratively to evaluate the environment and re-assess as needed. By re-applying lessons learned to each customer environment for a continuous improvement process, it brings a cross domain of experience to the government when you share best practices/experience from banking and healthcare to their process.

By working in an integrated, collaborative environment with our customers, we are able to get the necessary buy-in from the organization to allow for ongoing protection of company assets. By refining the security processes in place, we can collectively create a plan that appropriately addresses vulnerabilities, prompts collaboration within your organization, prioritizes threats and minimizes vulnerabilities and therefore, information security risks.

Supply Chain / Vendor Risk Management Protection

All companies, large and small, public and private, need to be concerned with the security of their cyber supply chain. Cyber security supply chain is essentially the entirety of an organization's IT systems (software, hardware, and networks) that together allow for the uninterrupted operations of the organization and its customers. Our professionals, in coordination with key personnel within supply chain, are able to assess weaknesses and vulnerabilities within the supply chain to protect confidential, privileged, and classified data.

We are experienced in performing comprehensive threat assessments with a focus on the specific internal and external channels. We will provide recommendations of specific customized supply chain assurance methods that uncover and mitigate threats. Total gap analysis can be completed through our team's understanding of a holistic view of the vulnerabilities in the IT environment as well as supply chain.

The key elements of vendor risk management include:

- Risk Analysis
- Physical Security
- Incident Reporting and Investigations
- Crisis Management and Disaster Recovery
- Information Security
- Procedural Security
- Access Control
- Personnel Security
- Education and Training Awareness
- Documentation Processing Security
- Trading Partner Security
- Conveyance Security

Exceeding Expectations

The Experts, Inc. is an Equal Opportunity/Affirmative Action (M/F/D/V) Employer.

Governance, Risk Management & Compliance Services (GRC)

GRC encompasses activities such as corporate governance, enterprise risk management (ERM), corporate compliance, and statutory and regulatory compliance. It relates to the consistent management and transparency into defined policies, clear and repeatable processes, and decision-rights for the appropriate area of responsibility within an organization.

Services provided under GRC include:

- Information Assurance
- Certification & Accreditation
- Audit & Compliance Validation
- Business Continuity Planning
- IT Architecture Validation (wireless network, infrastructure, application and data center design)
- IT Governance (asset management, security management, data governance)
- Risk Assessments
- Vulnerability Assessment and Penetration Testing
- Awareness Training

Payment Card Industry Security Assessments

- Perform gap assessments within the parameters of the Payment Card Industry Data Security Standards (PCI DSS) and Payment Application Data Security Standard (PA DSS)
- Working within the PCI DSS, we are able to execute a remediation plan – taking the gap analysis results and creating a remediation plan based on a risk-based approach to the work
 - Audit services
 - Penetration testing
 - Application security analysis
 - Gap analysis
 - Remediation plan

Cyber Defense

- 24/7/365 managed network operations
- Security infrastructure design, planning, and implementation
- Email encryption
- Log monitoring and retention
 - IDS
 - IPS
 - HIDS
 - HIPS
- Security Operations Services
 - Strategic network planning
 - Rule set changes and validation
 - Configuration changes
 - Firewall upgrades
 - Patch management
 - Backup and recovery
 - Security event monitoring
 - Performance and availability management
 - Fault analysis
 - On-demand reports
- Enterprise configuration, vulnerability and patch management
- Penetration testing and vulnerability assessments
- Incident response
- Root causal analysis and post mortem alignment