The Information Assurance Process: Charting a Path Towards Compliance

A white paper on a collaborative approach to the process and activities necessary to attain compliance with information assurance standards.

6605 Business Parkway
Elkridge, MD 21075
Ph.: 410.560.7177
Fax: 410.308.0950

The Information Assurance Process: Charting a Path Towards Compliance

Abstract

Public laws, regulations, directives, and the specific policies, procedures, and guidelines regarding information systems security have resulted in a proliferation of documentation. As cited in audit reports, periodicals, and conference presentations, it is generally understood by the IT security professional community that people are one of the weakest links in attempting to secure systems and networks. Attending to this human factor versus solely focusing on technology is essential to providing an adequate and appropriate level of security. CyberCore Technologies proposes that a collaborative approach to the information assurance process produces the greatest result for the investment. A four-step approach to transforming your technology group and system users relies upon a flexible team approach to assess, coach, collaborate, and implement best practices of the information security field. By customizing your information assurance process through this team-based, collaborative effort your organization is empowered to comply with governing laws, regulations, and directives.

Compliance Mandate

Information technology professionals must assure their information system's compliance with privacy and security laws, regulations, directives, and the secondary policies, procedures, and guidelines. This challenge confronts both public and private organizations. Each organization's information assurance (IA) initiative must include employing measures to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. IA measures include providing for the restoration of information systems by incorporating protection, detection, and reaction capacities**.** Note: Laws and presidential directives for every government agency mandate information assurance. Based upon their information security requirements several agencies have published standards for their information assurance process. Magnifying the impact of the information assurance laws, directives, policies, and agency specific procedures is that each private business that exchanges data with the government must meet all of the applicable standards. CyberCore Technologies' Information Assurance engineers have extensive experience providing security solutions in sensitive networks of all sizes in both the government and commercial arenas. Our professional services facilitate the continuing process of securing networks through a vendor-neutral approach to:

- Policy and Process Development
- Network Design
- Authentication, Authorization, and Accounting (AAA)
- Network Vulnerability and Penetration Assessment
- System Certification and Accreditation
- Information Assurance Training

Within each area, our client engagement process combines expertise and practical experience with the most applicable technologies, policies, and processes for your organization. To foster the organizational change required to ensure ongoing compliance, CyberCore Technologies believes the selection of the most applicable technologies must be a product of a joint, collaborative effort.

Policy and Process Development

Information Assurance engineers understand that a security policy is a custom-created, evolving standard of business conduct that is much more than any single device or software configuration. The best practices and experiences of the information security field provide the basic foundations, but every organization has unique requirements to manage information security. As such, CyberCore Technologies' security specialists develop and refine security policies and processes that not only protect the enterprise from the risks of shared network computing but also account for the key aspect of usability. Together with your network staff and management, CyberCore Technologies' certified security professionals perform a comprehensive assessment of your current policies and processes. This includes reviewing the data processed, stored, and accessed by your information system in conjunction with the applicable governing regulations. From the Gramm-Leach-Bliley Act governing financial information, HIPAA governing medical records, to the Sarbanes-Oxley Act organizations must guarantee that policies and business systems protect the privacy of the records and secure the information stored and processed. For government entities, DITCSAP, NISCAP, DCID 6/3, NSITSSP 11, and other Federal policies and regulations supercede or augment these regulations. In comparing our consultant's role to the traditional apprentice/master craftsperson relationship, taking on the role of apprentice automatically adopts the humility, inquisitiveness and attention to detail needed to collect good data.1 Working as a team, your staff benefits from the breadth of enterprise level experience of our security engineers and efficiencies of technical writers familiar with documenting standard operating procedures in support of secure information technology policies. With careful attention to your IT professional's comprehensive understanding of the enterprise, CyberCore Technologies' staff acts as a collaborative resource for information assurance expertise. From the information gathered during assessment the team educates all stakeholders in your unique information assurance landscape. The team collaborates on developing processes and defining policies that achieve the targeted level of security for your organization's information system. As required by your organization, CyberCore Technologies offers training support for your management, technical, and user populations in the implementation of secure information technology policies and processes. Through this flexible and cooperative client engagement approach your staff is empowered to continue to meet the challenge of information security requirements.

Network Design

Network design involves the integration of products, people, and processes to implement the security design. An effective solution uses products within their capabilities to supply defense-in-depth. Constructing and updating networks to take advantage of the best practices in security often requires modifications to the network infrastructure. CyberCore Technologies' approach begins with a joint assessment of your network's ability to protect the privacy of records and provide information security and assurance. Through scanning applications, surveys, physical inspection, and interviews our team documents your information system to isolate vulnerabilities, identify threats, and potential performance limitations. Following upon the assessment, network design activities to assure information security include addressing:

- Network Architecture
- System Integration and Engineering
- Site-to-Site and Remote Access Virtual Private Networks (VPN)
- Firewalls
- Intrusion Detection

Using a proven network design methodology, our engineers work with client staff to deliver the highest level of success with minimum disruption to your company and users. CyberCore

Technologies' Information Assurance engineers specialize in the implementation and integration of VPNs, firewalls, intrusion detection, and prevention systems in conjunction with a complete understanding of the desktop environment. In support of technology modernization to enhance information assurance, our engineers provide technical support in demonstrating appropriate technology, prepare and collaborate in delivering briefings, and produce technical reports highlighting the demonstration details for management review. CyberCore Technologies' engineers have extensive experience participating in Integrated Product Teams (IPTs), including working group meetings, design reviews, and complete meeting minutes to reinforce team decisions.

In this collaborative environment, recommendations, consultations, briefings for specific audiences, and supporting program activities are accomplished through joint team effort. Through this approach to the design process the team's common understanding results in efficiencies in the implementation of the proposed solutions. The solutions need to result from integrated product/process development (IPPD) with key vendors as team members. This is key to achieving an affordable solution. As critical to selecting the correct hardware, firmware, and software is implementation of the most appropriate configuration of the deployed assets to maintain the integrity of the network design. Built upon the knowledge gained during network assessment, CyberCore Technologies collaborates with your IT staff to physically safeguard and protect your network and information assets to optimize results and your return on investment.

Authentication, Authorization, and Accounting

A key requirement for many organizations is the design of an appropriate user authentication, authorization, and accounting (AAA) strategy to secure information system data. CyberCore Technologies' engineers are certified in various authentication and authorization technologies, including products that support two-factor authentication, secure socket layer acceleration, and Public Key Infrastructure (PKI). In addition, our Information Assurance team understands the particular networking protocols and standards that enable this key security service, especially Remote Authentication Dial-In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP). In assessing your system requirements, our background knowledge gained though diverse client exposure allows us to match the most appropriate secure technologies to the needs of your information system. Our security engineers work directly with your staff to develop a successful implementation plan. Partnering with knowledgeable resources to implement your AAA strategies streamlines the information assurance process by delivering the required expertise to achieve your security goals. It must be noted that CyberCore Technologies' extensive AAA expertise places us in a strong position to address your Identity Management requirements. Identity management refers to the process of employing emerging technologies to manage information about the identity of users and control access to organization's resources.3 It refers to the use of a set of technologies and administrative processes intended to manage information about the identity of employees, contractors, customers, partners, and vendors that are distributed among too many systems, and are consequently difficult to manage. The goal of identity management is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials within a given enterprise. Large enterprises are concluding that an identity management solution, alongside an enterprise-wide security strategy, is necessary to ensure the confidentiality, integrity, and availability of critical resources.

Network Vulnerability and Penetration Assessment

With extensive knowledge and expertise in conducting network vulnerability and penetration assessments utilizing the best-of-breed products CyberCore Technologies' engineers have practical experience conducting in-depth hands-on assessments. The requirement for conducting a security audit is fundamentally the same as any other periodic accounting process. Our Information Assurance professionals maintain that the hallmark of a secure environment is the unending adherence to the elements of sound security processes. There is no beginning or end to a security audit; rather, it is a required element of the ongoing information assurance process. In certain environments network control is de-centralized, while the organizational responsibility for establishing and maintaining security remains centralized. CyberCore Technologies' Information Assurance specialists understand that vulnerability scanning is a favorable approach in those network environments where the standard security methodology and processes are not capable of base lining and consistently sustaining the security posture of the network. Jointly with your staff, CyberCore Technologies' security engineers employ both proprietary and commercials applications to identify and isolate network vulnerabilities. Working in a mentoring approach to configure the testing applications, conduct the testing, and analyze the results our security staff empowers your organization to complete future audits as part of the ongoing information assurance process.

System Certification and Accreditation

The information certification and accreditation (C&A) process identifies an organization's security vulnerabilities, potential threats, risks, and defines the appropriate protection measures to mitigate the risks. CyberCore Technologies' team has numerous years of experience with various Governmental agencies and industry-standard security C&A processes that enables them to provide a best of breed Information Technology (IT) security verification program. The team of engineers, analysts, and technicians combine approved IT security checklist methodologies with organization-specific security evaluations to define, verify, and validate entire systems. Performing vulnerability scans utilizing a variety of tools and techniques and analyzing the results, our team can develop security test cases for system hardware and software. In evaluating non-technical IT security aspects such as personnel security awareness, user training, physical security practices, along with data and system backup procedures, we collaborate to develop continuity of operation strategies. CyberCore Technologies' team also has extensive experience in developing the policy and technical requirements associated with the C&A process in addition to conducting automated site tests and engineering analyses to verify that security features are properly implemented. Our team's capabilities encompass compiling and composing the documentation required to support the C&A process. This includes Systems Security Authorization Agreements, System Security Plans, System Requirements Traceability Matrix, System Design Documents, Certification Test and Evaluation Plans, Contingency Plans, and required training programs. Building upon our knowledge and expertise, your organization benefits this firm foundation to launch or operate an accredited information system.

Information Assurance Training

Federal agencies and organizations cannot protect the confidentiality, integrity, and availability of information in today's highly networked systems environment without ensuring that all people involved in using and managing information technology (IT):

- Understand their roles and responsibilities related to the organizational mission
- Understand the organization's IT security policy, procedures, and practices
- Possess adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible

As people are the key, but are also a weak link, more and better attention must be paid to the human resource. A robust and enterprise-wide awareness and training program is essential to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them. Regulations and policies direct that all authorized users must attend training on how to fulfill their security responsibilities. The users must also participate in periodic training in information system security awareness and accepted information system security practices, as appropriate to their job functions and responsibilities. CyberCore Technologies' team of security professionals offers both the knowledge and years of experience in developing and presenting in-depth information assurance training. Our team has designed and can deliver role specific types of training such as system administration and general user training.

Summary

There are building blocks to achieving information assurance for your information system. From instituting appropriate policies and processes to modernizing your technology infrastructure, how you approach information assurance produces maximum results for your investment.

Assess - Through our client engagement process our account and program managers deliver the right team at the appropriate time to assess your organizational requirements for information security. Using surveys, interviews, scanning applications, and physical evaluations, the CyberCore Technologies' engineers work with your staff to develop an accurate assessment of your current system and required information security technologies and strategies.

Coach - In this time of meeting regulations, mitigating threats, and negotiating audits our security professionals offer comprehensive knowledge of both design and remediation approaches to managing information assurance. Building upon the outcome of the information security assessment, our engineers will brief your technical and management staff on potential approaches to mitigate system vulnerabilities and together review the associated implementation and evaluate maintenance expenses.

Collaborate - Familiar with the best of breed products CyberCore Technologies' staff works with your technical and management personnel to develop a consensus on potential solutions to mitigate your information system vulnerabilities. Built out of a collaborative process with vendors, security engineers, system administration, and your management team, the proposed solutions are planned and budgeted for implementation.

Implement - CyberCore Technologies' security professionals are skilled at strategically deploying technology solutions to minimize any disruptions to your system uptime. Based on their experience integrating applications and configuring hardware, our staff coordinates their efforts with your team to streamline the implementation and minimize ongoing system maintenance. There is not a single application or device that magically delivers information assurance compliance. The solution is developed through teaming with a flexible partner with the background and expertise to effectively fulfill the information assurance requirements of your organization.

About Us:

Exemplified through our client engagements and demonstrated by our range of project competencies, CyberCore Technologies delivers a full spectrum of information assurance services. With a staff of certified security specialists serving clients, we provide expertise in remediation of procedures, hardware, software, and network connections. Our clients rely upon our technical competence and practical experience to collaborate and effectively manage each information system’s risks, reduce system vulnerabilities and proactively address security threats.