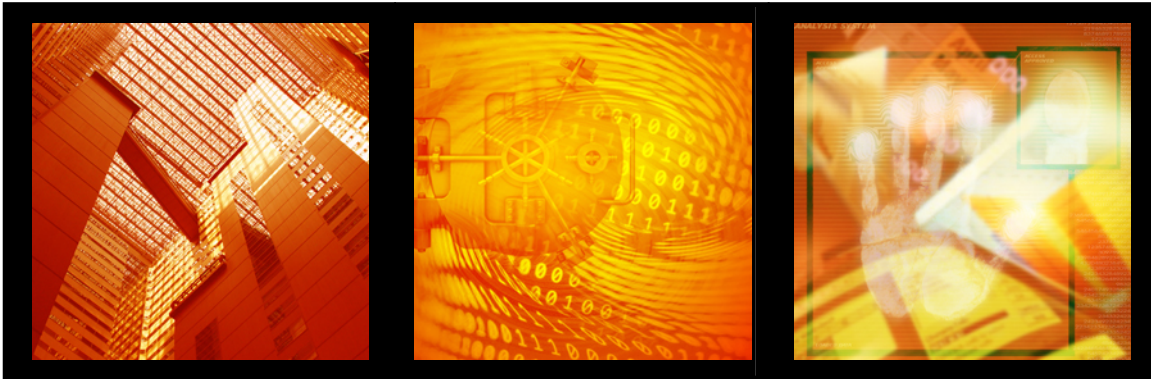


# *AN ENLIGHTENED WHITE PAPER*



## INFORMATION ASSURANCE: ENTERPRISE SECURITY POSTURING FROM GAP ANALYSIS TO REGULATORY COMPLIANCE

JANUARY 2009

---

Copyright © 2009 Enlightened, Inc. All rights reserved.  
This document is provided for the intended recipient's  
informational purposes only and shall not be duplicated,  
otherwise used, or disclosed to a third party—in whole or in  
part—without the express written consent of Enlightened,  
Inc.



**WHITE PAPER CONTENTS**

---

- 1.0 ABSTRACT..... 1**
- 2.0 BUSINESS CHALLENGE ..... 2**
- 3.0 SOLUTION DESCRIPTION..... 3**
  - 3.1 Definition of Information Assurance ..... 3
  - 3.2 Information Assurance Controls ..... 3
  - 3.3 Gap Analysis..... 5
- 5.0 CONCLUSION ..... 6**
- 6.0 COMPANY INFORMATION ..... 7**

## **1.0 ABSTRACT**

---

Over the past decade, Information Assurance (IA) has become a topic which has stimulated debate on secure transmission solutions, formed the construct for new business continuity processes, and raised the importance of safeguarding data to the foreground. The prevalence of IA integration into an enterprise comes as no surprise, since most companies are heavily dependent on computing technology to operate. With the constant need to have information resources readily available coupled with the proliferation of digital espionage, malicious “hacker” attacks, and the threat of cyber terrorism, agencies need to consider IA integration into their enterprise to protect their most important asset, their data.

## **2.0 BUSINESS CHALLENGE**

---

How exactly does an organization establish, design and implement IA into the workplace? Many will find that the transition towards compliance seems daunting and burdensome, however an efficient IA program streamlines IT processes, enforces technological constraints for mission tier systems, and provides the user community as well as management quantifiable metrics to gauge the company's effectiveness, thereby increasing the organization's residual Earned Value Management (EVM) threshold. This document will define Information Assurance (IA), discuss the types of controls leveraged to achieve IA compliance, and demonstrate a typical scenario for assessing an enterprise's inherent security posture.

## **3.0 SOLUTION DESCRIPTION**

---

### **3.1 Definition of Information Assurance**

Information Assurance is essentially a multifaceted approach to protecting data at all levels of an organization. For government agencies, this requirement is defined by the Federal Information Security Management Act (FISMA) and enforced by departmental policies originating from the agency's Office of the Chief Information Officer (OCIO). Information Assurance is broad and hierarchal in nature, with subordinate disciplines such as IT Security, Business Continuity Planning, Auditing, and Regulatory Compliance performing the technical work to build a valid and robust security support structure to support the enterprise.

Although having a full IA solution is ideal, budgeting constraints and lack of knowledge may preclude organizations from reaching their highest security posture available. In these instances, it is imperative for the government to include IA funding into their Office of Management and Budget (OMB) submissions in order to demonstrate their willingness to adhere to FISMA mandates. It should be noted that it is more cost effective to design and implement security into solutions from the beginning, rather than to construct a posture after the fact.

### **3.2 Information Assurance Controls**

To assist the government in establishing a secure, robust architecture, the National Institute of Science and Technology (NIST) has created a library of best-practices, procedures, and technical guidelines for the design, hardening, and Certification and Accreditation (C&A) of federal information systems. When looking at these recommendations, realize that there are three primary areas of control that are focused on, especially during the initial construct of the IA program; Technical Controls, Operational Controls, and Management Controls.

Technical Controls are what most managers think of when visualizing information assurance. These controls are the granular settings and configurations which govern the digital protections afforded to IT resources. Examples of Technical Controls include: Antivirus update settings, password complexity settings, router configuration, and patch implementation. These tasks are usually performed by a Network Administrator or Database Administrator with the knowledge and experience to apply such settings.

Operational Controls are, in certain aspects, supportive to the Technical Controls. While Technical Controls perform the granular work of enforcing security, Operational Controls govern the business processes inherent in performing administrative duties for the organization. Typical areas of concern which rely on Operational Controls include new account access procedures, physical security controls, user training, and maintenance and media retention.

Management Controls govern the implementation of the others through policy development and enforcement, auditing, and records management. Management

controls primarily focus on enterprise sustainment and continuity by requiring documentation which supports the enterprise. System Security Plans, Disaster Recovery Plans, and Incident Response Plans fall under this control.

### 3.2.1 The Confidentiality, Integrity, and Availability (CIA) Triad

The primary purpose of the three controls previously mentioned is to enforce data protection by concentrating on three tenets: Confidentiality, Integrity, and Availability, which is collectively known as the CIA triad, shown in Figure 1 below.

The following paragraphs briefly describe each tenet:

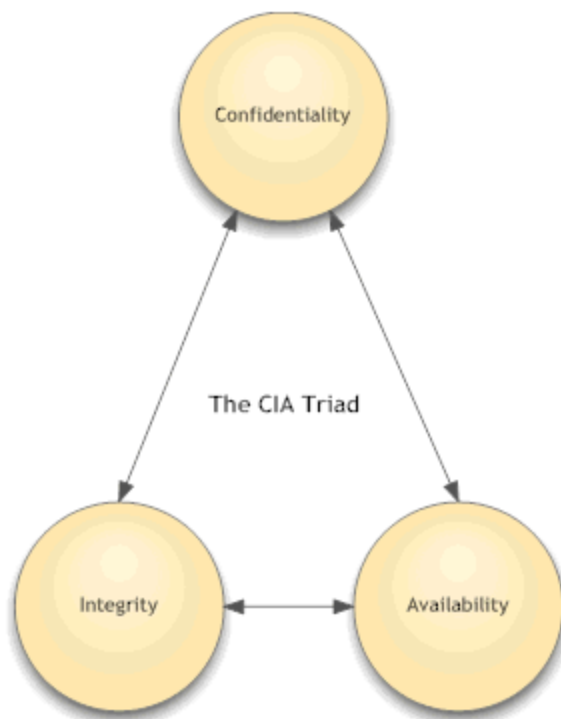


Figure 1: CIA Triad

- **Confidentiality:** Ensures that only the appropriate personnel can access different resources across the platform. This is achieved through the implementation of Dynamic Access Control Lists (DBAC), Lattice-based permission settings, and the “axiom of least” principle which states that users are entitled to all the permissions necessary to perform their duties and nothing else.
- **Integrity:** assures the recipient of a transaction that the data has not been accessed, modified, corrupted, or otherwise compromised in any fashion. The use of MD5 hashes, encryption protocols, and tunneling protocols accomplish this feat. Availability is the ability to retrieve data at any time.

- **Availability:** means that businesses can serve their customers in a timely fashion without issue. Creating network redundancy, increasing bandwidth, and performing file server backups are part of a High Availability posture.

### 3.3 Gap Analysis

As the organization develops, it may periodically want to assess the effectiveness of their IA program. The most efficient and comprehensive way to accomplish this is by performing a gap analysis. A gap analysis is a three stage audit of the organization's information security posture, to include an assessment of the supporting controls which constitute the pillars of the organizations IT Security posture.

The first stage is known as the organizational discovery phase. The purpose of organizational discovery is to glean a system "snapshot" to show the current state of the architecture, business processes, and governing policy. The analysts will examine all records, settings, and practices to establish a system baseline.

The second phase is the criterion analysis and vulnerability assessment phase. This phase takes the operational baseline completed in phase one and tests it against federal standards such as NIST SP800-53, Recommended Security Controls for Federal Information Systems. This comprehensive assessment evaluates all Operational, Technical, and Management controls, and is usually considered complete at the conclusion of an enterprise wide "white hat" vulnerability assessment or "red hat" penetration test. All test cases in this phase are clearly noted as pass or fail. A Security Control Group consisting of 9 subordinate tasks is considered a fail if even one task is not compliant with regulatory standards.

The last phase is the risk assessment and reduction phase. This phase takes a closer look at all items noted as a fail and performs a risk evaluation against each. Depending on the severity of the deficiency, along with the cost associated with rectifying it, risk can either be accepted and placed in the Risk Management Matrix (RMM) or marked for correction and placed into the Plan of Action and Milestones (POA&M). It is important to note that all items listed in the POA&M are subject to additional scrutiny for FISMA compliance, and may have an adverse impact against an organization's IT budget if deemed to be out of scope or not implemented.

Once items have been included into the RMM or POA&M as appropriate, the gap analysis is considered to be complete. From here, the organization should strive to enforce good security practices and preserve the integrity of the enterprise. A strong Configuration Management Board (CMB), Auditing, and periodic network scans will greatly help. A full scan of the enterprise should either be conducted at least annually, or to coincide with a new Certification and Accreditation (C&A) initiative, whichever is more frequent.

## 5.0 CONCLUSION

---

As heterogeneous networks begin to converge into dynamic enterprise clusters, the agency's point of presence on the Public Internet expands, and the need for real time transactional asynchronous data processing and storage arises, having a robust IA program is vital to the organization's success. Enlightened's Security Assessment and Analysis Team (SAAT) is an ideal vehicle to develop, supplement, or assess the agency's IA posture. Each SAAT's staff is tailored to the organization's current needs, as there is no "cookie cutter" solution for security. SAAT members are hand-picked Information Assurance Professionals who are versed in security management throughout the System Development Life Cycle (SDLC), and can provide greater EVM to the organization through industry best practice processes and best-of-breed implementation solutions, resulting in satisfaction knowing that the organization's most valuable resource, its data, is protected.

## **6.0 COMPANY INFORMATION**

---

Enlightened, Inc. is a full-service Information Technology (IT) consulting firm that helps our clients solve complex business problems by leveraging technology.

Contact Enlightened, Inc., to learn more about our Information Assurance services:

Name: Antwanye Ford, Co-Founder & President

Address: 666 11<sup>th</sup> Street, NW  
Suite 520  
Washington, D.C. 20001

Email: [marketing@enlightened.com](mailto:marketing@enlightened.com)

Website: [www.enlightened.com](http://www.enlightened.com)

Tel: 202-783-4655

Fax: 202-783-7266