

WHITE PAPER



PRESENTED BY:



INFOSEC ARCHITECTURAL SERVICES:

**A PROVEN FIVE-PHASE METHODOLOGY TO DEVELOP A SCALABLE
ENTERPRISE SECURITY ARCHITECTURE**

Carl F. Allen, CISM

May 5, 2006

Introduction

Federal Network Services, Inc., Information Security (INFOSEC) Services practice is pleased to present this summary white paper on a five-phase methodology to develop a scalable Enterprise Security Architecture (ESA). The resulting ESA can enable an organization to integrate business, information technology, and information security, and provides for information protection while facilitating trust in the electronic infrastructure.

Entities and companies, large and small, from both government and commercial sectors are being requested or may be required to provide users, customers, partners, employees, and many others to interconnect in order to exchange, process, and store electronic information almost anywhere, and at anytime. Customers, regulators, and best practices industry standards suggest or may even demand that information be protected so that the public or business trust in electronic information infrastructures can be maintained.

Federal Network Services realizes that organizations must strike a balance between creating an information security (INFOSEC) process that is too rigid and establishing an INFOSEC framework that provides little protection and does not develop trust. The ESA concept of Federal Network Services' INFOSEC practice designs and implements as it strikes that balance. As such, it includes references to industry Information Technology (IT) security and regulatory standards including standards such as the International Standards Organization (ISO) in ISO 17799, the National Institute of Standards and Technology (NIST) in the NIST Special Publication (SP) 800 series and laws such as the Information Technology Management Reform Act (ITMRA) (which is also known as the Clinger-Cohen Act of 1996), the Federal Information Security Management Act (FISMA), the Health Information Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act of 2002 (SARBOX), the Gramm-Leach-Bliley Act (GLB), the National Infrastructure Protection Program (NIPP) and many others.

The ESA model and approach uses a five-phase pragmatic methodology to understand the organization's business, review and verify the enterprise IT infrastructure, perform a business and IT risk analysis, design the appropriate information enterprise security architecture, and develop a phased process for implementation.

The Enterprise Security Architecture Methodology

PHASE 1 – UNDERSTANDING THE BUSINESS

The first step of the ESA methodology is to identify the core business mission, goals and objectives of the organization. This is best accomplished by meeting with senior management and in reviewing either public or other internal company documents. The INFOSEC architects who are designing the ESA should understand the feedback from the meetings with management and the reviews of the documents.

Once understood, and even if unique, the findings should be validated with the general practices and directions within the enterprise's government, industry, or market sector. The validation is an important part of this first step, as the INFOSEC architect needs to determine how to position the ESA model. The ESA model is developed and implemented for the company based on internal business mission, goals and objectives, and the direction of the customer's government, industry, or market sector.

For example, based on this internal and external view, is the enterprise by nature a leader or follower? Reviewing and understanding this one question, can alter the design of the architecture for the organization, but position the company to gain strategic and/or competitive advantage by implementing an INFOSEC business-driven framework.

Finally, while the ESA will be mostly technical in nature, it is important to be able to present the approach to the management sponsor using the language of management, which is rarely in IT or IT security-centric terms. The language is usually in business terms such as reducing costs, increasing productivity, diminishing liability, improving ROI, mitigating risk and enhancing market share. Hence, starting the first step by understanding the business aspects before designing the ESA is important.

PHASE 2 – REVIEW AND VERIFY ENTERPRISE INFORMATION TECHNOLOGY INFRASTRUCTURE

The second step of the ESA methodology is to review and verify the enterprise IT infrastructure. In most organizations, a visit with the network and telecommunications departments is a good place to start (or if there is a functional configuration management service, it may also suffice) to initially obtain a network map or assist in the creation of a current one, if needed. Meetings follow with network and telecommunications managers and staff to discuss and review the IT infrastructure and components that support the enterprise. Questions are asked including if any part of the infrastructure is outsourced, and if the company can identify where the network begins and ends.

This is followed by working with the IT organization, in-house or outsourced, to verify the IT infrastructure, and the IT enterprise architecture technical standards that are defined and whether they are followed. These technical standards may include hardware and software specifications, software development methods and practices, and network protocols.

Additionally, industry reference models, such as the OSI reference model, are used to overlay the organization's IT architecture technical standards. This provides further understanding about how different industry reference models have shaped the current IT infrastructure and components selection, implementation, and future direction.

PHASE 3 – PERFORM BUSINESS AND IT RISK ANALYSIS

The third step of the ESA methodology is to perform a baseline business and IT risk analysis. There are several industry risk assessment models that can be used, but INFOSEC Services uses a comprehensive qualitative and quantitative approach to thoroughly review, understand and measure the business and IT risks. This approach is the one documented by NIST in SP 800-30

The risk assessment method includes reviewing the business, information processes, and assets, and identifying internal and external vulnerability and threats along with real and perceived business and IT risks through the use of the Strengths, Weaknesses, Opportunities, and Threats (SWOT) Analysis. The output from this comprehensive business and IT risk analysis yields Pareto charts that can be presented to business, IT, audit, and information security management functions within the enterprise. These charts can assist in identifying risks that can be prioritized as high, medium, and low.

Finally, using both qualitative and quantitative measures, over time the ESA baseline risk assessment can be updated regularly. The resulting Pareto charts can be compared with earlier versions in order to show the gains made by developing and implementing the INFOSEC framework.

PHASE 4 – DESIGN THE ENTERPRISE SECURITY ARCHITECTURE

The fourth step of the ESA methodology is to design the security architecture itself. With the first three steps completed, an INFOSEC architect will review many known and publicly available models before designing the architecture for the enterprise. Federal Network Services uses a proven industry method to design INFOSEC architectures for IT infrastructures and components. In addition, the security architects have years of experience and have interacted with hundreds of clients around the world in multiple industries to advise, design, deliver, and implement IT security architectures.

The proven INFOSEC architecture design process includes creating a comprehensive security baseline, with reference to regulatory or industry security standards as necessary. The next part of the process is to identify the essential pieces of the security baseline for the IT infrastructure and components. Referencing the complete network map from Step 2 and other IT architecture standards is an important consideration for this part of the design process.

After the security baseline is established, the INFOSEC architect works with the organization using information gathered and learned in Steps 1 and 3 to identify a set of business critical security elements to include in the ESA implementation roadmap. The elements may include addressing critical business needs of the organization, regulatory mandates, or strategic projects to gain competitive advantage.

Additionally, the business critical security elements may include identifying information technology needs or areas such as single or simplified sign-on, enterprise directory, identify management, or encryption services. Yet, they may be very technology specific such as server or network hardware, operating systems, or application-specific software requirements.

The INFOSEC architecture is shaped using the business critical elements to identify controls and safeguards that will work within the framework of people, business processes, and technology. At this point the INFOSEC architect reviews the need to integrate business, technology, and security at the enterprise level.

Finally, the ESA process must consider up to 10 variables that are used to validate the ESA integration priorities. These variables range from understanding how the security framework impacts the end user, to determining the network performance and business operational impact

of implementing different aspects of the architecture on the overall performance of the enterprise infrastructure.

PHASE 5 – DEVELOP A PHASED PROCESS FOR IMPLEMENTATION

The fifth and final step of the ESA methodology is to develop a phased process for implementation of the architecture. INFOSEC Services uses this final step to validate that the implementation phases are pragmatic and achievable for the culture of the enterprise.

The industry culture of the enterprise can include the market sector adoption of IT security, whether the enterprise is a leader or follower, if the enterprise has a centralized or decentralized business and IT management focus, and whether enterprise management or even the sector or arena views security as a proactive or reactive activity.

In addition, some security architects fail to align the architecture development, design, and implementation with the company culture, which increases the risk of failure for the implementation. INFOSEC architects interact with the enterprise points of contact to understand the users (i.e., employees, partners, customers, etc.) and how each views INFOSEC in relation to their business function. Understanding the users and the enterprise culture assists in phasing the implementation and achieving desired results.

INFOSEC Architecture Methodology

INFOSEC Services can provide security management, architecture, implementation, and lifecycle operational consulting services to achieve delivery of a fully featured, functional, and operable security system documented fully so that when determined to be the most cost-effective method, customer personnel can take over and operate the system.

To implement such a security system for an enterprise, INFOSEC Services provides credentialed and experienced resources to ensure the success of the project. To deliver this type of system that includes INFOSEC architecture, INFOSEC Services will assign a senior project manager and INFOSEC architect certified in many areas of INFOSEC operations to oversee the strategic planning and other efforts. That project manager-architect may be supported by:

- Senior INFOSEC Consultants with extensive INFOSEC architecture, design, engineering, and operational experience
- A senior Security Architect and advisory engineers with extensive experience in government and commerce
- Risk and vulnerability management Senior INFOSEC Consultants
- Senior INFOSEC Consultants with technical engineering expertise (as needed):
 - ✓ Directory Services including LDAP, MSAD, NDS, X.500
 - ✓ Windows 2000, XP, and NetWare
 - ✓ UNIX – Solaris, AIX, HP-UX, Linux, Macintosh OS X
 - ✓ Internet, Web and Secure Operating System-based platforms
 - ✓ Mainframe Systems
- Senior INFOSEC Consultants with INFOSEC and Information Assurance backgrounds and certifications

Consulting and development services are provided as outlined below in a series of steps to achieve delivery of the desired system.

PROPOSED WORK PLAN:

- Step 1. INFOSEC Strategic Planning
 - ✓ The initial effort will be to determine the exact requirements for the IT security system. For this type of effort, people who are familiar with the requirements set forth by Federal mandates can be drawn from diverse parts of the service market. All Federal Network Services' INFOSEC Services personnel are very experienced with working in Federally-regulated security systems.
 - ✓ Once a set of valid requirements is in place, the major applications and general support systems (networks) will be specified based on the needs of the customer. This is the start of a knowledge management system that will be turned over to the customer when the system goes operational. This also is required in order to design the INFOSEC architecture for the enterprise.
 - ✓ If necessary, site surveys or audits of physical infrastructure design will be performed to ensure most effective design of the security system. The earlier security design will be incorporated with both the physical architecture of the facility and the network design for the IT system. Minimal cost will be incurred to ensure the integrity and security of the network and data whether at rest (archived data) or in transit (as used throughout the IT system by various applications). This requires knowledge of the business workflow of the operation.

- ✓ With a complete set of requirements, the initial project plan will be developed that will put resources and time required for each stage of the buildup.
- Step 2. Information System Security Architectural Services
 - ✓ Based on the validated requirements and the project plan, architectural services will be provided to design the specific IT functionality that is required and will follow the five steps outlined in the prior paragraphs.
 - ✓ From the design, a mockup will be developed on a test bed network for proof of the design. This may be the installed IT system before operational rollout or a laboratory network built to simulate the operational network.
 - ✓ Initial benchmarking of the security system components will be performed based on the results of vulnerability testing using state-of-the-art vulnerability analysis applications and best practice risk management principles in order to validate the design, determine any inherent weaknesses in the system, and validate the configuration so that configuration management and control can be performed and patch management efforts can be efficiently continued from the initial design.
 - ✓ If not planned, a configuration management system will be designed and put into place.
- Step 3. Information System Security Engineering Services
 - ✓ With completion of the initial vulnerability testing and risk management actions, Information System Security Engineers (ISSEs) will determine how best to remediate any identified vulnerabilities and mitigate any residual risk in order to ensure safe, secure operability of the system.
 - ✓ ISSEs will prepare full infrastructure drawings, design security component policies and rules-based operational parameters, and define the initial operational efforts required for the system.
 - ✓ Any integration and inter-operability testing with other IT components not dedicated to the security system will be designed by the ISSEs along with a full set of interface drawings and documentation.
 - ✓ The results of this step will be reviewed by the INFOSEC architect before presentation to the customer.
- Step 4. Information System Security Officer Services
 - ✓ With the design validated and the operational network being built up with the required components (e.g., firewalls, switches, hubs, etc.) put into place, the Information System Security Officers (ISSOs) will be able to start development of operational policies and procedures required for operational control of the system once it is put into effect. This is part of the management communications efforts that are used to control business workflow processes.
 - ✓ ISSOs develop system development lifecycle documents specific to the INFOSEC system or develop the documentation system that will describe all IT functionality. This includes design of the organization (through business process engineering) that will be responsible for day-to-day operation of the system including the development of charters, design of required hard copy forms, configuration control mechanisms, and any required system certification and accreditation that will be required for governance of the system. This all adds to the organization's management communications efforts.
 - ✓ The results of this step will be reviewed by the INFOSEC architect before presentation to the customer.
- Step 5. Pre-Operational Testing
 - ✓ To ease the move from design to operations, final test and evaluation will be performed with complete documentation of the results.
 - ✓ At this point, the ISSOs will develop the Incident Response Plan, Contingency Plan, and Continuity of Operations Plan for the operational system.

- ✓ The results of this step will be reviewed by the INFOSEC architect before presentation to the customer.
- Step 6. Transition to Operations
 - ✓ ISSOs used during the design and test of the operational system to this point can be transitioned to an outsource IT security team or can develop training for the business' security services IT experts to ensure that operations will function to the efficiency level for which it was designed.
 - ✓ ISSOs will conduct tests of the Incident Response Plan, Contingency Plan, and Continuity of Operations Plan.
- Step 7. Operations
 - ✓ The Information System Security Team will monitor system operations through real-time monitoring, periodic vulnerability testing, periodic risk analyses, policy and procedure update, and system upgrade based on technological and/or operational changes that result from governance or driven by greater IT efficiency.
 - ✓ Regular interface with the system owner, user representatives, and any other required personnel will ensure that the operational capability of the system is maintained as designed and upgraded as necessary for any desired improvements.
 - ✓ Regular review of policies and procedures related to the network (e.g., access management, identity management, live video feeds, business monitoring, etc.) will ensure the level of support for the system is maintained at the highest degree possible.
 - ✓ Regular reports of system performance will be used to determine any necessary changes as technology improves.
 - ✓ Regular research into new technologies will ensure that the system remains as efficient as possible and as cost effective as can be managed.

Summary

The ESA development model consists of a five-phase pragmatic methodology. The resulting INFOSEC architecture can be implemented to enable an organization to integrate business, information technology and information security, and to provide information protection and facilitate trust in the electronic infrastructure. The implemented ESA can achieve measurable Return-on-Investment (ROI) results, allow the enterprise to focus on the highest priorities, be used to identify top-level security risks, be used to establish a comprehensive security baseline, shape the INFOSEC framework using business critical security elements, and be implemented using a phased approach.

The key to a successful IT security program lies in how well systems are documented and evaluated with regard to security issues. Federal Network Systems' INFOSEC Services practice provides a holistic approach to INFOSEC in general and specifically to INFOSEC architectural efforts for Government and Federally mandated programs to ensure IT systems can be operated safely and securely. In addition, INFOSEC Services provides services that offer Return-On-Investment (ROI) features to increase safe, secure operations of IT systems and to provide for better system protection throughout the life cycle of the system.

For more information, refer to the contact information provided on our Website: www.fnsnet.com and a representative will be happy to provide more information.