

## 1.1 Audience

This document is intended as a supplement document for Task Order # 4, Deliverable # 4.1.3. Although deliverable # 4.1.3 addresses some specific points of this document, the rest of this document is included to provide SFA with an outline of all the security issues that need to be addressed when designing the security infrastructure to support the organization's operations as they are transitioned to an Internet based environment.

This document provides a comprehensive and complete view of information security and offers an excellent starting point for understanding and designing a secure solution.

## 1.2 Scope and Assumptions

This comprehensive and complete view of information security is intended as a thought trigger and completeness check while designing or implementing a security architecture. The model offers an excellent starting point for understanding and designing a secure solution. It describes the security components that must be incorporated into the plan, design, build and operation of a business capability and how those components fit together.

### Scope

A thorough understanding of a framework's scope is crucial to its use during the design phase of a project. The scope of the SFA *Security Framework* is such that it provides a starting point for designing a security architecture consisting of many security components. It may also be used as a completeness check to verify that all security components have been considered and none forgotten. These components include both technical and non-technical components.

The SFA *Security Framework* may be used as a tool to introduce a security architecture into a general and wider technical architecture.

### Assumptions

This *Security Framework* is not vendor specific, but will contain references to technologies and products supplied by vendors. Not all vendors and products will be represented. Therefore, prior to any product selection, a proper evaluation cycle should be performed to ensure that requirements are met most appropriately.

To summarize, this is an open *Security Framework* for which products and technologies from numerous vendors may be implemented and integrated into a complete security architecture.

### 1.3 Purpose

Designing the complex security architecture required to satisfy the needs of today's distributed, mission-critical applications is a major challenge. As such, it is helpful to have an inventory of the components that may be required for the design, build, installation and operation of systems. It is also helpful to have an understanding of how the components fit together conceptually.

This *Security Framework* should be thought of as a conceptual structure used to frame the security related work to be designed and implemented. It may be used as a thought trigger, starting point, or as a completeness check.

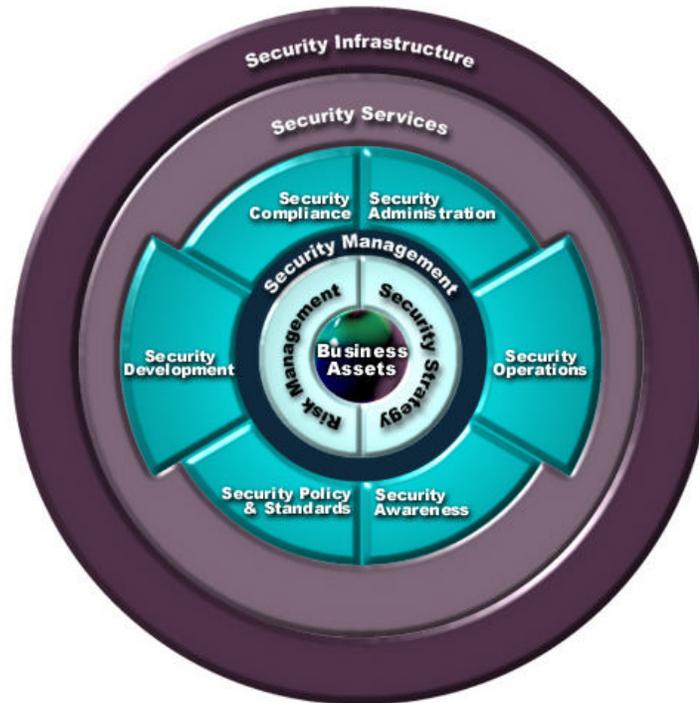
This *Security Framework* can be used to help SFA understand what security components may be required and how the components fit together. Based on the inventory of components and the description of their relationships, practitioners will select the necessary security components for their design.

## 2 Security Framework

A security architecture can be organized into many different areas (for example, tools, processes, policies and standards) that together enable a secure architecture to be deployed and operated. To ensure information security and to protect the *Business Assets*, all these areas should work together as part of the security solution. This model is not intended to be an organizational model. How and in which department each of these components is implemented will vary.

The framework model approaches enterprise security in a way that will address SFA's major concerns such as privacy on many different levels.

The figure below shows the different areas in the *Security Framework*. Each area is described in detail along with its sub-areas.



*Security Framework*

## 2.1 Main Areas of Security Framework

The *Security Framework* can be viewed as consisting of three high-level areas, each of which is equally important for information security and none of which can be excluded. The areas are:

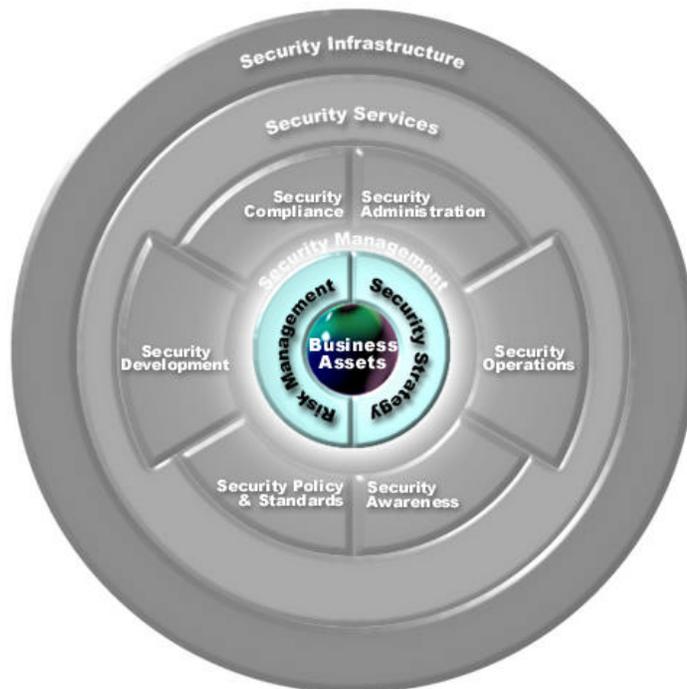
1. Business Assets and key processes – identifies level of effort required to protect assets.
2. The core capabilities – defines security functions performed by people.
3. Technology architecture – describes protective tools and services that help achieve the *Security Strategy*

Below you will see an explanation of these three high-level areas:

### 1. Business Assets and key processes

Three interdependent areas form the core of the model:

- **Business Assets** - represents what needs protection, and is the target of all information security efforts.
- **Risk Management** - analyzes the Business Assets' value and the cost to protect the assets, identifies the level of protection required, and discovers the threats and vulnerabilities that must be addressed through the Security Strategy
- **Security Strategy** - defines the approach and direction SFA is taking to secure the *Business Assets in line with the Risk Management approach*.

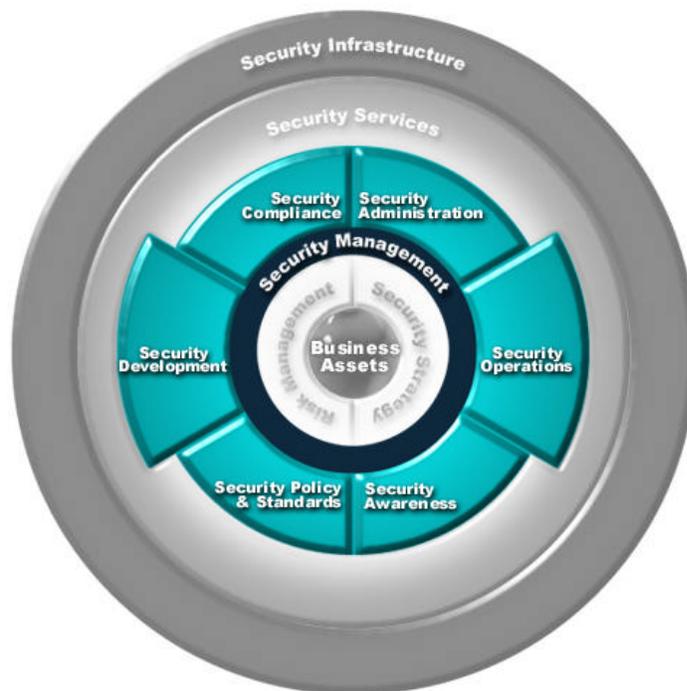


*Business Assets and key processes of the Security Framework*

## 2. Core Capabilities

The core capabilities comprise the security functions necessary to provide complete information security. They include:

- Security Management
- Security Policy and Standards
- Security Awareness
- Security Compliance
- Security Administration
- Security Development
- Security Operations



*Core Capabilities of the Security Framework*

### 3. Technology Architecture

Together with the security functions (Core Capabilities) the technology architecture layer helps secure the *Business Assets*.

The technology architecture comprises:

- Security Services
- Security Infrastructure



*Technology Architecture of the Security Framework*

## 2.2 Business Assets



*Business Assets*

### Component Description

*Business Assets* at the core of the *Security Framework* are the valuables that must be secured and protected. These assets can be tangible (such as systems, networks, facilities, people and customer data) or intangible (for example, the reputation of the business). The *Business Assets* should be identified as the initial step in risk assessment. Business asset identification involves interviewing information owners and recording their perceptions about the following items:

- Assets
- Undesirable events
- Event history
- Potential damage
- Value

Any security practitioner can acquire a good understanding of the *Business Assets* by asking the information owners and business contacts what assets they think need the most protection.

Each asset must be given a value, which can be either intrinsic or related to the cost of restoration if the asset were to be lost or compromised. Both the intrinsic and the business value are taken into consideration when evaluating the assets to be secured.

The value of intangible assets, such as reputation and trust, that do not have any intrinsic or business value must be evaluated. One way to perform this evaluation is to list all assets evaluated so far, ranked in terms of value. Based on this list, the assets with intangible and subjective value will be inserted, according to best judgement, between two assets already evaluated.

All assets will be assigned a security ranking: that way an overall and objective view of the assets is available.

Based on this comprehensive list, business and security executives can make the appropriate decisions when required, and not rely only on subjective judgement.

This list of assets will also be used in other areas, not only as a checklist to verify that all assets have been taken into consideration but also as a ranking list that will support choices and decisions on other parts of the enterprise.

It is important that the owner of the asset as well as the asset itself be identified. A key to achieving success is that the asset owner is held responsible and accountable for the process of securing the business asset. This means that the owner of a sensitive database containing customer data also should be accountable for its safekeeping. The business units should cooperate with the office of the CIO to achieve this.

The business impact loss or damage to *Business Assets* should be evaluated and could include:

- Loss of reputation and client confidence
- Legal penalties against SFA
- Cost of security failure recovery
- Cost of the inability of the system

### **Implementation Considerations**

Before designing and planning any kind of security architecture and solution, The *Business Assets* that need to be protected must be understood. The existence of *Business Assets* provides the fundamental reason for information security. A comprehensive list of assets is therefore required. Without the appropriate knowledge and a list of the *business Assets*, there is the risk of implementing expensive solutions that may seem important, but actually achieve few benefits for the cost.

### Example Assets

- **Information assets** - databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, security codes and passwords, audit records, proposals, salary information, public/private keys, and so on.
- **Paper documents** - contracts, guidelines, documentation, documents containing important business results.
- **Software assets** - application software, system software, development tools and utilities.
- **Physical assets** - computer and communications equipment, magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture and accommodations.
- **People** - employees, customers, subscribers.
- **Intangible**. Image, reputation and legal liabilities.
- **Services** - computing and communications services, other technical services (heating, lighting, power, air-conditioning).

## 2.3 Risk Management



*Risk Management*

### Component Description

**Risk Management** is the component that assesses the overall risks associated with SFA. A risk assessment is performed as part of the **Risk Management** function. It involves evaluating threats to *Business Assets*, identifying security vulnerabilities or weaknesses that can take advantage of those threats, and prioritizing business risk. This risk assessment provides information on the status of the enterprise security. Specifically, it provides information on the existence and application of the current security processes and policies. It is a cornerstone activity that must be repeated as often as necessary to maintain an accurate global assessment of the enterprise's security status. *Security Compliance* feeds information into the risk assessment based on potential new vulnerabilities and weaknesses uncovered during *Security Compliance* audits. Other inputs are technology trends and new business opportunities.

The risk assessment consists of the following steps:

- Identify critical *Business Assets*
- Identify threats to assets and likelihood of occurrence
- Identify vulnerabilities and weaknesses
- Determine business impact
- Prioritize business risk
- Recommend mitigating actions

Below is a description of each step in the risk assessment:

- **Identify critical *Business Assets***

**Q:** What are the assets, and what is their value?

**A:** The first step in risk assessment is to identify the critical *Business Assets* and the value placed on them. To effectively implement information security solutions SFA needs to know what requires protection.

- **Identify threats to assets and likelihood of occurrence**

**Q:** What are the threats to the asset, and what are the chances a user may be motivated to carry out the threats?

**A:** It is important to know *who* and *what* is most likely to compromise *Business Assets*. This will help determine the approach to protecting the assets.

- **Identify vulnerabilities and weaknesses**

**Q:** What current vulnerabilities exist that could potentially be exploited, causing certain threats to be realized? What weaknesses could allow an unwanted operation to be mistakenly performed?

**A:** A vulnerability is a weakness in security procedures, design, implementation, or controls that could be taken advantage of to harm the asset. For example, a vulnerability that could be taken advantage of is the threat of a natural disaster for a data center that resides in a flood plain or a tornado alley. Vulnerabilities can include human, organizational, or system-related weaknesses. Poor security controls and tools may also result in assets being vulnerable due to mistakes performed by the operators, for example, an accidental deletion of a customer database.

- **Determine business impact**

**Q:** If this asset is harmed, what effect will that have on the business?

**A:** This analysis requires the business owners to think in terms of consequences to the business if the assets are compromised. Examples of business impacts are: financial and profit loss, exposure of confidential customer data, loss of reputation, etc..

- **Prioritize business risks**

**Q:** What are the most serious business risks?

**A:** Security risk is the potential for damage or loss of an asset. It combines the **value** the owner places on the asset in potential danger, the **impact** the loss of the asset would have, and the **likelihood** that the weakness will be taken advantage of to damage the asset.

- **Recommend mitigating actions**

**Q:** What mitigating actions could be taken?

**A:** The mitigating actions will minimize or eliminate any identified risks in the “*Risk Assessment Matrix*” document. The actions will also provide input to the *Security Strategy*. An example of a mitigating action may be the installation of intrusion detection tools.

### **Implementation Considerations**

A risk assessment may take several weeks to complete. From the risk assessment, an action plan can be developed that addresses risks to *Business Assets*. It is important that all steps in it are completed and documented and that the proper SFA executives support the actions and plans to either mitigate the risks or accept them.

#### **Example:**

*(See Following Page)*

## Sample Risk Assessment Matrix

Classification			Threat/Vulnerability Analysis		Impact Analysis	Risk Calculation			Recommended Action	Recommendations Evaluated						Recommendation Priority		
Area Assessed	Component	Requirement	Vulnerability/Weakness	Threat Description	Business Impact on Assets	Potential for Damage (H,M,L)	Likelihood of Threat (H,M,L)	Risk Factor (H,M,L)	Security Recommendation	Cost to Fix (H,M,L)	Ease of Implementation (H,M,L)	Ease of Administration (H,M,L)	Effectiveness of Solution (H,M,L)	End User Usability (H,M,L)	Fit with Business Priorities (H,M,L)	Priority Calculation	Priority of Recommendation (H,M,L)	What is being done
Human Performance	Security Roles		Individuals (e.g. system and network administrators) are not given an appropriate amount of time to fulfill their security responsibilities	Security processes and controls may not be implemented or may be inadequately implemented.	The assets managed by these individuals may be and subject to disclosure, modification and destruction due to inadequate security controls.	H	H	H	Dedicate personnel to the security function	M	M	H	H	H	H	94.44	<b>H</b>	User ID's and passwords are being used to authenticate customers.
Technology Infrastructure	Web application	Identification	Access to back end systems (database, mainframe) from web application is granted with a shared ID/password, rather than uniquely identifying each user	This shared ID/password could be stolen or misused	Misuse could cause downtime of application, Confidential customer information could be compromised with no accountability	H	H	H	Require individual user authentication of web server users by database and mainframe	M	M	M	H	M	M	80.56	<b>M</b>	Only SSLv3 traffic will be allowed

## 2.4 Security Strategy



*Security Strategy*

### Component description

*Security Strategy* sets the future directions for information security and affects all areas of security within SFA. The primary goal is to give an overview of the future business directions and the security controls which should be in place to support these business functions. The *Security Strategy* determines the overall plan for the security based on new threats, user requirements, development requirements or vendor strategies.

The *Security Strategy* must be aligned with other business strategies to ensure that security is considered when new business capabilities are planned and when new alliances are made. All strategies must work together.

For example, if the business strategy says that students should be able to sign and submit their Promissory Note over the Internet, the *Security Strategy* must reflect and enable this. Alternatively, a conscious decision could be made, due to security concerns and risks, that it is not possible to implement this function. The other strategies must then be updated.

A *Security Strategy* is sometimes divided into a short term strategy with initiatives that can be implemented over the next couple of years and a longer term strategy with initiatives that can be implemented over the next five years. It is important that this distinction be made and that priorities be set for each security initiative. It is also important to demonstrate how security initiatives and recommendations fit within the overall *Security Strategy*. Failure to make these distinctions, and set priorities can lead to an unmanageable list of tasks that may not all get accomplished.

The *Security Strategy* is normally developed after the risk assessment and after a *Security Strategy* session has been held. The *Security Strategy* integrates the results of the *Security Strategy* session and the “*Security Risk Assessment Matrix*” document. The *Security Strategy* inputs are in general:

- Security risk assessment matrix
- *Security Strategy* session
- Advice from security group
- Business strategy direction

The *Security Strategy* is closely linked to the risk assessment and the *Business Assets*. If there are any changes in risks or in the value of *Business Assets* it may be necessary to update the *Security Strategy* to keep it current.

The *Security Strategy* should be high level, focusing on the desired end state of the enterprise security rather than specific security components and the implementation of solutions. The *Security Strategy* defines high-level requirements such as identification, authentication, confidentiality and access control. The *Security Strategy* feeds into *Security Policy and Standards* which provides additional details and metrics. The security requirements will be input to the *Security Development* function which plans, develops and implements new *Security Services* and *Security Infrastructure* components.

The *Security Strategy* is the responsibility of high-level SFA executives such as the CFO, CIO, and Channel General Managers, and must be validated and supported by them. The security organization of SFA provides input, information and guidance to the high-level executives who approve and validate the *Security Strategy*. It is extremely important that the high level executives place a high value on the *Security Strategy*. The *Security Strategy* should be communicated back to the security organization and throughout the executive management structure, including the highest-level executives in SFA.

The *Security Strategy* should be treated as an important asset. Its confidentiality should be protected in a way similar to that of other important strategies.

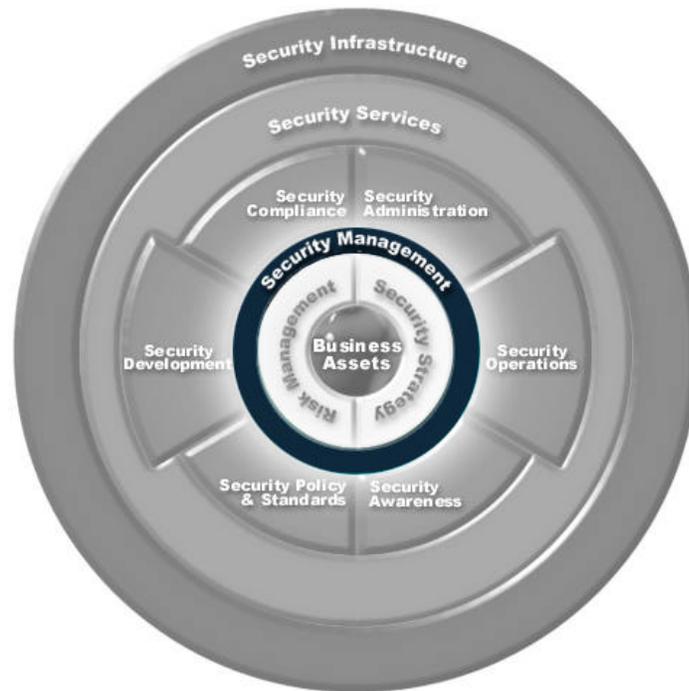
Periodic updates of the strategy should take place, and it should be updated when necessary to meet variances in business and/or operational requirements, perhaps as a result of a *Security Compliance* audit.

### Implementation Considerations

It is important that an up-to-date *Security Strategy* is in place and driving the security initiatives. The lack of a current *Security Strategy* is in itself a risk.

If a *Security Strategy* is not firmly established at the executive level, there is a substantial risk that information security will not be given proper importance in *SFA*. As a result, information security may not be funded sufficiently and *Business Assets* will remain at risk.

## 2.5 Security Management



*Security Management*

### Component description

*Security Management* has overall responsibility for the management of the secure enterprise. Within this section, roles and responsibilities begin being identified. *Security Management* co-ordinates with other security areas including:

- Security Policy and Standards
- Security Awareness
- Security Compliance
- Security Administration
- Security Development
- Security Operations

*Security Management* will initiate and manage enterprise-wide security programs to support SFA's business goals. *Security Management* will develop, build and maintain the security organization and shape its structure. For example, decisions to decentralize security functions and to define the reporting structure belong to *Security Management*.

In any organization, one person should be assigned overall responsibility to establish, implement and maintain the information security program. This role should be created if it does not exist. Ideally, this role should be filled by a full-time security officer who is ultimately responsible for information security and all areas relating to the protection of *Business Assets*. The security officer should be a high level position.

*Security Management* is responsible for coordination with other business areas and departments such as Human Resource, Help Desk, etc. The information security officer should report to a level high enough to enact change in the organization. It is critical that *Security Management* obtain sufficient funding and buy-in from executive management for security initiatives and activities.

The key *Security Management* functions are:

- Identify key security functions
- Determine current security staffing
- Define security officer position
- Define security organization and functions
- Define security organization roles and responsibilities
- Define placement of security within the organization
- Define Security policies, procedures and guidelines
- Develop security organization
- Manage and oversee day-to-day operations
- 
- Coordinate with other Business Areas
- Report to top executives and management

### **Implementation Considerations**

A very strong and highly qualified individual is necessary to serve as the information security officer. The information security officer must have the ability and power to implement the security organization and staff the SFA with qualified people. The information security officer must be able to influence the business units to enact the changes in SFA that will achieve the appropriate level of security.

## 2.6 Security Policy and Standards



*Security Policy and Standards*

### Component description

The *Security Policy and Standards* forms the foundation for all security-related activities. Its aim is to aid in achieving a secure environment by establishing consistency in architecture and to reducing the risk, effect and cost of security incidents. The *Security Policy and Standards* must follow the general security directions in the *Security Strategy*. Support and buy-in from top executives and users is critical for the successful implementation and enforcement of *Security Policy and Standards*. Once developed, the security policy will be used to drive all other infrastructure decisions in the security framework.

All security policies and standards should be documented using the same template. The template should include some or all of the following sections:

- **Purpose** – the overall objective and guiding principles for the security policy or security standard.
- **Scope and audience** – the users, systems, and situations for which the security policy or security standard applies.
- **Overview** – a short description of the security policy or security standards content.

- **Roles and responsibilities** – specifies roles regarding user standards, management, security administration, or other organizations; describes who is responsible for drafting, publishing, and reviewing the security policy or security standard.
- **Policies/standards** – details contained in the security policy or security standard.
- **Reporting** – how violations or deviations from the security policy or security standards should be reported.
- **Related documents** – other documents, standards, policies, or guidelines that help explain the security policy or security standard or its implementation.

### 2.6.1 Security Policies

Security policies are generally high-level, technology-neutral and risk-focused. Security policies set directions and procedures and define penalties and countermeasures if the policy is violated. A policy might read "all user identities accessing internal information resources from the Internet must be authenticated using a two-factor method". Security policies must not be confused with implementation-specific information, which would be part of the security standards, procedures and guidelines.

Security policies are established by empowered representatives from groups responsible for:

- Human resources
- Information systems
- Director of Communications
- Security
- Lines of business

Security policies must be balanced and provide tradeoffs between:

- Degree of security
- User convenience
- Cost

Without an equitable balance among these elements, it is unrealistic to expect that the security policies will be followed. Some policies may need to be modified.

Some of the most important security policies:

- User identification and password policy
- Remote access policy
- Extranet policy

- Internet security policy
- Access to data policy
- Administration policy
- Incident response policy
- Awareness procedure policy
- User behavior policy
- Security monitoring and audit policy
- Privacy Policy
- Auditing
- Records management/disposal

### 2.6.2 Security Standards

A security standard defines a specific mandatory requirement to address the security policy as applied to business asset or security function. Standards may or may not be platform independent. A standard may apply to management, administrators, end users, or a specific group within SFA.

There will be many Security Standards across many areas. Some of these standards are interrelated, and their dependencies should be considered. The following list gives some of the most important standards that should be considered and documented as part of any security architecture:

- Operating system security standard
- Server security standard
- Desktop security standard
- Laptop security standard
- LAN security standard
- WAN security standard
- Router security standard
- Development security standard
- Firewall security standard

### 2.6.3 Security Guideline

A security guideline is a specific recommendation to address an element of the security policy. A security guideline is not a mandatory action, but should be implemented whenever possible. A guideline typically uses words like "should" or "may" in the definition. Guidelines are usually written for a particular environment and are used to help guide behavior. For example, "all successful logins should be logged and monitored." A guideline may apply to management, administrators, end users, or a specific group within SFA.

#### 2.6.4 Security Procedure

A security procedure provides security staff or administrators (system, network, or application) the specific actions required to implement the security policies, standards, and guidelines. Some procedures are unique to a specific information asset (e.g., an application or a platform). Others are general and may be applied to multiple or all information assets. For example, there may be both a UNIX and an NT procedure that specifies the method used to set a minimum password length, and the actions to take when a new user account is requested.

#### **Implementation Considerations**

*Security Policy and Standards* represents an important definition of all work related to security. The most important aspect of *Security Policy and Standards* is to ensure that they are supported by top management executives and adopted throughout SFA. The risk is that security policies and standards are created without being deeply rooted in the organization. Each individual must be aware of the responsibilities and know how the *Security Policy and Standards* can affect their day-to-day work. The security policies must continually be reevaluated and reassessed for change.

It is important to remember that security policies must be balanced between level of security provided, user convenience and cost.

## 2.7 Security Awareness



*Security Awareness*

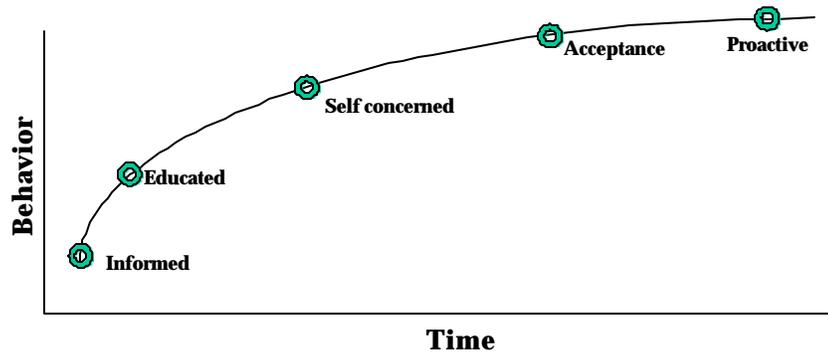
### Component description

*Security Awareness* is a very important part of any effective security organization because people often constitute the weakest link in the chain of securing information. A *Security Awareness* plan must be created, executed and communicated to all employees, business partners and customers. The *Security Awareness* plan will set SFA's expectations regarding information security, and communicate each individual's responsibility for protecting the confidentiality, integrity and availability of *Business Assets*.

A *Security Awareness* plan should include multiple methods to distribute information, such as screen savers, newsletter columns, monthly meetings, e-mails, training seminars, videos, computer security days, and posters. The chosen distribution methods should be appropriate for the target audience. The aim of the *Security Awareness* plan is to reach the audience and take them through the following steps which describe the change in behavior of the audience over time:

- Informed
- Educated
- Self concerned
- Accepting

- Proactive



Regular communication of the *Security Awareness* plan is necessary to reinforce:

- The importance of security.
- The rights and obligations of individuals with respect to the security policy.
- The protective actions individuals are expected to take.

An effective *Security Awareness* plan will increase the visibility and importance of information security and ensure that individuals are always aware that information security is an important component of the organizational culture.

The *Security Awareness* plan should be updated regularly to include new business capabilities.

### Implementation Considerations

Every security organization needs to have a *Security Awareness* function. This is the only way of making security an integral part of the company's culture. People often pose the highest risks in a company due to their ability to cause extensive harm from either malicious intent or ignorance.

## 2.8 Security Compliance



*Security Compliance*

### Component description

*Security Compliance* is one of the core capabilities considered essential to providing complete information security. *Security Compliance* includes all the functions that people perform to ensure that the *Security Policy and Standards* are created, followed, measured, enforced and updated as required. *Security Compliance* for the environment is a necessity: *Security Policy and Standards* have limited value unless they are being followed and enforced. *Security Compliance* is often referred to as security audit. *Security Compliance*, however, is a broader term which includes the audit as well as other tasks and any follow-up actions resulting from the audit.

*Security Compliance* comprises the following tasks:

- Audit current level of security
- Validate new solutions and capabilities
- Validate changes to the environment
- Perform penetration tests
- Correct variance

Below is a description of each task:

- **Audit current level of security.** By using automated tools (policy monitoring tools and log scanners) and manual checks, the security group can audit and check components for *Security Compliance* the *Security Policy and Standards* and external regulations. Reviews of procedures and work processes can also reveal operations that do not comply with policies and standards.
- **Validate new solutions and capabilities.** Before a new solution or business capability goes live, security architects must validate, or certify, that the solution is secure and meets the *Security Policy and Standards*. This usually means checking all solution components (operating system, network, application, configuration, and so forth) against a set of checklists. Not until the required checks have been performed and the solution has passed inspection, should the new capability be deployed.

One way to restrict deployment into the live environment is to control and restrict the assigned IP addresses for the new solution. Only when the solution has passed security validation would it be assigned an IP address, making it available to be deployed in the network, extranet or Internet.

- **Validate changes to the environment.** When changing an existing environment it is very important to verify that the security is still intact and is working according to the *Security Policy and Standards*. Any changes must be validated and approved before they can be taken into the live environment. Failure to validate changes in the environment may result in risks to the *Business Assets*.
- **Perform penetration tests.** An important function of *Security Compliance* is to perform penetration tests. They should be both scheduled and unscheduled and can be highly effective in exposing vulnerabilities and holes in security. Security tools and vulnerability scanners can be used as well as manual checks to expose common holes in operating systems, web servers, routers, and so on. The tools will generate reports on all the exposed vulnerabilities.
- **Correct variance.** If a variance is found between the current level of security and the desired one documented in the *Security Policy and Standards*, action must be taken to ensure that this is mitigated and resolved. Before any mitigating actions are implemented a quick risk assessment should be performed in order to determine if the change should be made. Examples of mitigating actions are:
  - Take protective measures such as removing the non-compliant equipment until a fix can be found and deployed.
  - Define and document new *Security Policy and Standards*.
  - Update existing *Security Policy and Standards* to reflect changes in the environment.
  - Design and implement new *Security Services* and *Security Infrastructure* components.

### **Implementation Considerations**

Due to the amount of information required across a large number of components automated tools are necessary to be used for *Security Compliance*. It is important that operators know how they are being assessed and can work to be in adherence to security policies.

## 2.9 Security Administration



*Security Administration*

### Component description

*Security Administration* performs administrative processes, primarily oriented towards managing users throughout their life-cycle within the organization.

*Security Administration* will receive input from *Security Compliance* as it identifies weaknesses in the environment and conditions that do not meet policies and standards. 'Separation of Duties' is an important concept to implement. It is the reason why *Security Administration* is separated from *Security Operations*. No organization or individual should control or perform both administration and operations functions. For example, 'Separation of Duties' helps prevent administrators from performing unauthorized actions and then being able to avoid monitoring and detection by *Security Operations*. The key difference between *Security Administration* and *Security Operations* is that the role of *Security Administration* is to perform user management functions whereas *Security Operations* supervises those and other functions.

Security processes which *Security Administration* perform include:

- Manage approval process and forms for identification, authentication and revocation.
- Manage User Account Control Services: assign roles and manage access rules and authorization levels.

- Update, create and delete user accounts according to *Human Resource and Security Compliance*.
- Resetting passwords.
- Track and manage list of owners and administrators of systems.

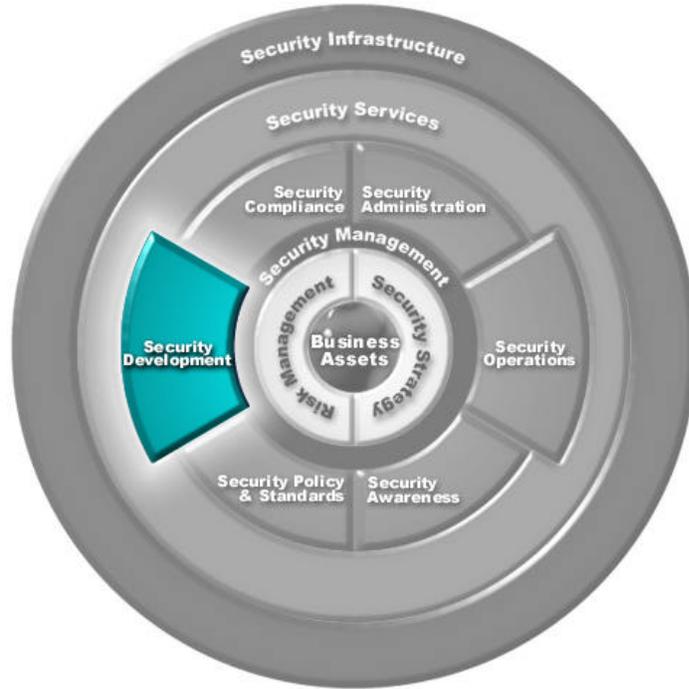
The processes should be documented and distributed to the people performing the function. They should be documented following the same template.

*Security Administration* may also provide help and guidance to security process documentation within SFA. *Security Administration* may also manage and store centrally copies of all documented security processes, *Security Policy and Standards*, security job and role definitions, etc.

### Implementation Considerations

When implementing the *Security Administration* function it is important to understand the organizational aspects of where processes should be performed. User management is a *Security Administration function*, but it is also part of the wider responsibilities of enterprise operations management. In fact, the entire security organization can be thought of as an element of enterprise operations management. The user management function in enterprise operations management is often referred to as the Help Desk.

## 2.10 Security Development



*Security Development*

### Component description

The *Security Development* function reviews and defines detailed technical requirements for security solutions. The *Security Development* function performs technical design and implementation of security solutions. It supports and enables the building of new security technologies, architectures, applications, systems, and business capabilities, as well as new *Security Services* and *Security Infrastructure*. The *Security Development* function must have both wide and deep technical competency in Information Security. *Security Development* will support and assist the re-use of *Security Services* for new business capabilities.

One important aspect of *Security Development* is the secure management of the development environment. The development environment must ensure that software changes and product delivery assures the integrity and reliability of the business capability.

*Security Development* is ideally an integral part of all stages of a traditional technical architecture including the development, execution and operations stage. Security needs to be addressed in all of those stages.

The main tasks of the *Security Development* function are:

- Review and define security requirements
- Design and implement security architectures

- Document security solutions and architectures
- Support application developers

Below is a description of each task:

### 2.10.1 Review and define security requirements

High level security requirements are driven by the *Security Strategy* and *Security Policy and Standards*. *Security Development* reviews, refines and details these according to available technology, budget constraints, etc. The result is a set of detailed security requirements specific for the security architecture being planned. The security architecture may be part of a development, execution or operations architecture.

### 2.10.2 Design and implement security architecture

The security architecture is designed to satisfy the security requirements. The design is then built and implemented as a set of:

- *Security Services*
- *Security Infrastructure* components, and/or
- application or business capability-specific security components

The security architecture may be a specific point solution or may address several security areas as part of a wider security solution. It may be custom built or it may consist of third party products. It may also involve the implementation of a security suite. For more details regarding the technical components of a security architecture, see the sections on *Security Services* and *Security Infrastructure*.

### 2.10.3 Document security solutions and architectures

The *Security Development* function is responsible for documenting and/or making sure that adequate documentation exists for all *Security Services* and *Security Infrastructure* components. The documentation should describe how to implement and use the *Security Services* and *Security Infrastructure*. The audience is application and business capability developers, network engineers, and systems engineers. The document should detail all relevant APIs, protocols, functionality, administration, operations, etc. It is also important to ensure that new security standards, guidelines and procedures are documented for the *Security Services* and *Security Infrastructure*.

### 2.10.4 Support application developers

The *Security Development* area will also support application developers of business capabilities. *Security Development* is responsible for handling implementation-specific questions and issues about *Security Services* and *Security Infrastructure* components that can't be resolved by reference to the documentation.

### Implementation Considerations

When developing security architectures it is important to address all technical architectures:

- Development
- Execution
- Operations

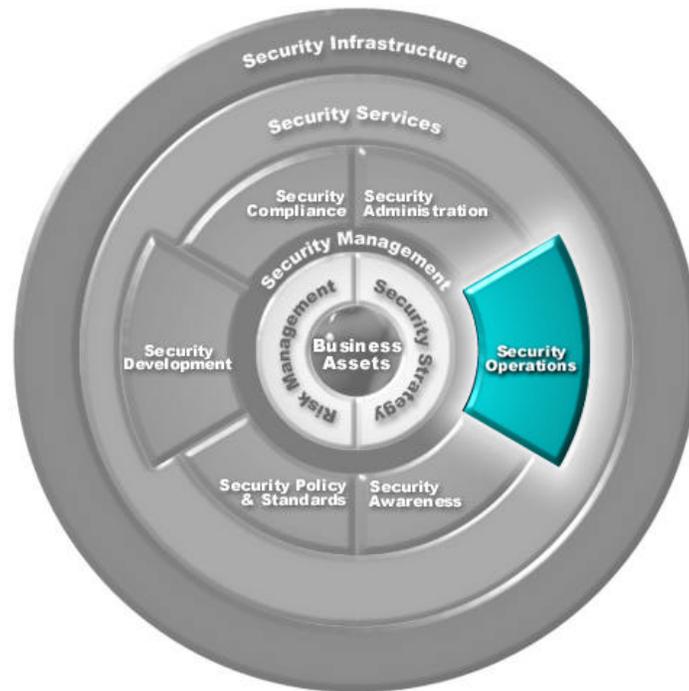
It is important to consider, plan and budget for Security as part of an architecture from the beginning. It is impractical and expensive to retrofit security on top of an existing solution.

It is very important that the *Security Development* process and development environment itself is secure.

### Example

Specific security architectures and components are explained in the *Security Services* and *Security Infrastructure* areas.

## 2.11 Security Operations



*Security Operations*

### Component description

*Security Operations* is the component responsible for the ongoing monitoring of security components and security events. Security monitoring refers to the tracking of relevant events and the subsequent actions to be taken when such events occur.

A *Security Operations* architecture is designed and implemented by the *Security Development* function. Often this is done in co-operation with an Enterprise Operations department who already perform network and systems management, perhaps by utilizing an enterprise management system. When designing the *Security Operations* architecture it is important to decide whether to select tools that are 'best-of-breed' point solutions, or a multi-tool security suite. The selection will depend upon the specific requirements.

The *Security Operations* architecture may be offered as *Security Services* by offering application activity recording services for developers.

A *Security Operations* architecture supports tasks such as:

- Document policy and define security events to monitor
- Define the data to record
- Security Monitoring
- Security Investigation and Incident Response

Below is a description of each task:

#### 2.11.1 Document policy and define security events to monitor

Together with the *Security Development* function, *Security Operations* define which events to monitor and documents this in the Security Monitoring and Audit policy. The policy should describe the responsibilities and processes for performing the detailed functions in *Security Operations*.

The events to be monitored are normally divided into several categories depending upon their criticality. The most critical events are security breaches when they are in progress.

It is very important to find a balance of which events to monitor and which to ignore. Without careful selection of the events to monitor, it is possible for the monitoring system to be overwhelmed by the number of events recorded, leading to performance and network traffic problems.

The list of monitored events needs to be updated regularly to adjust to newly discovered security holes and changes in system activity patterns. It may be sufficient to simply update the Security Monitoring software on a regular basis.

#### 2.11.2 Define the data to record

The data to be recorded and the actions to be taken must be defined for each type of security event that will be monitored. Some events may require additional to capture event-specific information.

#### 2.11.3 Security Monitoring

Security Monitoring is performed through a combination of security tools and manual checks. Common security tools used for monitoring security are:

- Intrusion Detection Tools (IDT)
- Log scanners

These tools will recognize system activity patterns and generate reports or alarms if suspicious activities occur. To alert and notify operators of security events several methods are used, including screen messages, e-mails, sound, lamps and pagers. When a critical security alert is issued, operators may need to activate an incident response team.

#### 2.11.4 Security Investigation and Incidence Response

If there is suspicion or confirmed evidence of a security breach, it is critical that an investigation is performed quickly. An incident response team will assess the immediate risk to the *Business Assets* as a result of the incident, and take appropriate short-term actions.. Examples of these actions may include:

- Terminate the corporate internet connection
- Disconnect the systems under attack
- Track and identify the perpetrator
- Escalate the situation to legal affairs

Subsequent investigation of the incident will determine whether a revised risk assessment is required for the business asset, and whether changes in security controls are indicated.

### **Implementation Considerations**

It is important to understand where in SFA the *Security Operations* fit. If *Security Operations* and enterprise operations management are to be separate organizations, their respective responsibilities should be clearly defined. They must work closely together since systems management and network management, both crucial to the *Security Operations* function, are normally part of enterprise operations management.

## 2.12 Security Services



*Security Services*

### Component description

*Security Services* are re-useable common security architecture components which have been documented and packaged to facilitate easy re-deployment. The objective of the *Security Services* is to achieve consistency and standardization across the enterprise for common security functions such as authentication, encryption, etc. There are many advantages to the implementation of *Security Services*:

- Consistency and standards in architecture.
- Central administration and operations.
- Shared development resources and less 're-invention'.
- Reduced cost.
- Increased speed of deployment and reduced time to market.
- Higher security due to fewer solutions and systems for similar requirements.

*Security Services* are designed, built and implemented by the *Security Development* function as a result of requirements derived from the *Security Strategy* and *Security Policy and Standards* functions. A security architecture for a new business capability may be created by combining several existing *Security Services* and *Security Infrastructure* components.

The *Security Services* comprise two component categories:

- Security Base Services
- Security Management Services

### 2.12.1 Security Base Services

Security Base Services are reusable components available to application developers to incorporate security functions into applications or business capabilities. A Security Base Service is implemented using one or more of the Core Security Components of the *Security Infrastructure*. There may be several implementation options for each Security Base Service. The Security Base Services comprise:

- Registration / Identification services
- Authentication services
- Single Sign-on services
- Access Control services
- Encryption services
- Digital Notarization services
- Content / Virus Inspection
- Logging services
- Non-repudiation services

#### 2.12.1.1 Registration / Identification services

The ability to effectively control access to system resources depends fundamentally on accurate identification of individuals during the registration process. Failure to do so properly may result in users gaining unauthorized access to system resources by impersonating a legitimate user. Ensuring proper identification and registration of users is especially important in a Netcentric environment, where users may register themselves over the Internet.

The following security requirements for registration and identification services need to be considered:

- Simple and user friendly.
- Confidentiality and integrity for the submitted information.
- Assigning roles to the registered user
- Easy to integrate with host/legacy systems and business applications.
- Support many to many relationships – provide means to link new registration information to existing user data, and to map multiple UserIDs to a unique individual.

### Implementation Considerations

It is important to verify the identification data before registration. It is also important to consider factors such as future requirements, integration with host systems, usability, etc., when designing the Registration / Identification service.

 More implementation information is found in the *Security Infrastructure* area, Core Security Components under Registration / Identification.

#### 2.12.1.2 Authentication services

Authentication is the process of ensuring that an entity in a system transaction (including users, servers, and clients) is who he, she, or it claims to be. Authentication services are a means of enabling Access Control.

Authentication is often divided into the following categories:

- Knowledge-based – something you know (such as a password)
- Token-based – something you have (such as a smartcard)
- Attribute-based – something you are (biometric factors such as fingerprints)

Authentication can rely on a single technique (“one-factor” authentication), or on multiple methods used together (“two-factor” or “strong” authentication).

Authentication services are used by applications and business capabilities in conjunction with Access Control services to protect resources. Two common ways to use authentication are:

- People use authentication to gain access to systems and data.
- Servers and systems use authentication to ensure that they communicate with the intended entity.

### Implementation Considerations

There are many different ways to implement authentication services and they provide various levels of authentication. Username/Password based authentication is considered to be basic and widely implemented, but is the weakest method when used alone. If strong authentication is needed then two-factor authentication, for example token based authentication that also requires a password, may be required.

 More implementation information is found in the *Security Infrastructure* area, Core Security Components under Authentication

#### 2.12.1.3 Single Sign-on services

Single Sign-on services provide application developers a reusable and common interface by establishing a single UserID that can be used for access to multiple applications or systems. A single sign-on service in conjunction with an authentication service will eliminate the need for users to authenticate themselves to each application or system.

A good single sign-on and authentication service architecture can pass the UserID to each application or system, which can then provide access to required resources on an individual basis. This is especially important in a Netcentric/Internet architecture.

A single sign-on service has many benefits:

- By taking advantage of a common UserID, the speed of application development is increased and time to market is reduced.
- Centralized control makes user administration easier since there is a single tool to create users, change passwords and delete users.
- Elimination of multiple authentication steps increases usability.

### Implementation Considerations

The security of a single sign-on service must be carefully designed. If properly designed and implemented the security of the system will be higher. On the other hand a poorly designed single sign-on service may add vulnerabilities to the system as a security breach in the system may open up many other systems.

In a diverse organization, such as SFA, the multiplicity of systems and applications poses a significant barrier to enterprise-wide single sign-on. Careful planning is required for each system that is to be included in the single sign-on capability. The use of pilots and incremental implementation of the single sign-on capability may be necessary.



More implementation information is found in the *Security Infrastructure* area, Core Security Components under Single Sign-on.

#### 2.12.1.4 Access Control services

Access Control refers to mechanisms and policies that restrict access to computer resources. Access control services are implemented to protect information *Business Assets*. Access control products often provide authentication and authorization services as well. There are multiple methods and locations to implement access control in a security architecture.

The access control technology to use will depend on the general access control requirements and on the level of granularity that must be achieved. These may range from relatively basic user based access control to complex dynamic role-based access control of individual data units.

A re-useable access control service will allow application developers to define the resources which should be protected and to then rely on the access control service to enforce security based on a set of access rules.

### Implementation Considerations

It is important to determine where the access control should be located and what type of access control is required. Access control may be implemented at the firewall, web server, application server, database, network, etc., or a combination of these.

 More implementation information is found in the *Security Infrastructure* area, Core Security Components under Access Control.

#### 2.12.1.5 Encryption services

Encryption services protect information during transmission or storage with cryptographic techniques. Encryption services protect the privacy of a transaction, assure contents of the transaction cannot be altered without detection, and provide non-repudiation with digital signatures.

Encryption services may be implemented either as hardware or software and in different layers, for example:

- Application layer
- Session layer
- Transport layer
- Transport / Channel layer
- Network layer

Application developers commonly implement encryption services using an encryption toolkit.

### Implementation Considerations

The specific implementation methods used for encryption are critical. Even if the cryptography algorithm employed is strong, a poorly designed implementation may introduce vulnerabilities that make it easy to break. There are several things to consider when implementing encryption, for example:

- Management of encryption keys
- User interface design
- Encryption strength
- Performance implications
- Legal implications



More implementation information is found in the *Security Infrastructure* area, Core Security Components under Encryption

#### 2.12.1.6 Digital Notarization services

Digital Notarization services provide the ability to assign a timestamp and a digital signature to an electronic document: being able to prove that a document had a given content at a precise point in time and has not been altered.

Digital Notarization services are becoming more important as the value of information and electronic transactions in eCommerce grows.

### Implementation Considerations .



More implementation information is found in the *Security Infrastructure* area, Core Security Components under Digital Notarization

#### 2.12.1.7 Non-repudiation services

Non-repudiation services provide tamperproof evidence that a specific action or transaction has occurred. Non-repudiation services should be able to produce legally binding evidence. Non-repudiation services consist of the following services:

- Non-repudiation of origin - protects against a message originator denying that a message was sent
- Non-repudiation of submission - protects against a Message Transfer Agent denying that a message was submitted for delivery
- Non-repudiation of delivery - protects against a message recipient denying that a message was received

Non-repudiation is commonly implemented in financial systems where electronic funds transfers take place.

An application developer utilizes the non-repudiation service through:

- An application developer toolkit

- Third party services

### Implementation Considerations

For non-repudiation services to work, many legal aspects and issues must be resolved; this may be the biggest challenge. It is important to understand how non-repudiation is intended to be used and what the requirements are. The requirements may have to take both local and international laws into consideration, especially in the case of eCommerce transactions which cross international borders.

 More implementation information is found in the *Security Infrastructure* area, Core Security Components under Non-repudiation services.

#### 2.12.1.8 Content / Virus inspection services

Content / Virus inspection services provide the means of inspecting, filtering and deleting harmful content before it causes damage to information systems.

The Netcentric evolution has produced new technologies enabling new business opportunities. But with these new technologies, new threats in the form of viruses, hostile applets and other forms of downloadable executables, and e-mails have increased dramatically.

This has put an even greater emphasis on the importance of proper security to protect against content threats.

Content / Virus inspection services are provided by:

- Firewalls – offer some protection in this area. In general they are not focused on content / virus inspections, but more towards access control, authentication and encryption. Depending on the requirements a firewall may be sufficient.
- Point solutions – these are tools specifically designed for protection against malicious mobile code, e-mail or viruses.

The distinction between solutions for mobile code inspection, e-mail filtering and anti-virus is vague as many products provide some or all of the functionality found in the other categories.

### Implementation Considerations

An important factor to consider when implementing a Content / Virus Inspection service is that it must be updated regularly. Failure to update regularly will result in vulnerabilities to the system from new viruses and damaging forms of mobile code that are designed to circumvent existing security measures. Proper *Security Policy and Standards* for monitoring new content threats and responding to them must be in place and must be enforced.

Content / Virus inspection can be implemented either at the server or client level. Commonly both server and client protection is implemented as they complement each other. For laptop users it is a requirement to have client level protection in addition to what may be implemented at the server level.

 More implementation information is found in the *Security Infrastructure* area, Core Security Components under Content / Virus Inspection.

#### 2.12.1.9 Logging services

Logging services provide a centralized repository for security-related events. A good security architecture uses the logging service to record all security events. This will provide *Security Operations* with the means of detecting security breaches and tracing them if an intruder penetrates the system. The logging service will ensure that the proper system information is recorded in a tamper-proof manner, since the logs may be used as evidence against an intruder.

Application developers may integrate application-specific security events with the logging service to benefit from the security monitoring functions provided by the *Security Operations*. *Security Operations* will need to cooperate with application developers to define which events to log.

#### Implementation Considerations

When designing a logging service, consider the following issues:

- Administration
- Security and integrity of the logs
- The location of the data and files
- Volume of data recorded
- Performance implications
- Log management and archiving
- Who will analyze log information
- How will the logs be analyzed

 More implementation information is found in the *Security Infrastructure* area, Core Security Components under Logging service.

### 2.12.2 Security Management Services

The operational aspects of any security solutions need to be considered alongside the security aspects. Security Management Services are services which intersects with both enterprise operations management and security management.. Security Management Services tries to identify some of the interfaces which needs to be in place. An example is an enterprise directory which may be administered by the Help Desk function, but which the Security Organization must develop and monitor. . The Security Management Services comprise:

- Enterprise User Management
- Policy Management services
- Certificate / Key life-cycle Management services
- Availability and performance services
- Directory Integration Administration services

#### 2.12.2.1 Enterprise User Management

Enterprise user management is commonly a central function provided by the Help Desk. Central user management is an important tool to administer all users across multiple systems and environments. Enterprise user management is a function provided as part of an operations architecture but with close ties to the security organization. The security organization may be a part of enterprise operations or alternatively be a completely separate organization.

##### **Implementation Considerations**

Responsibilities needs to be clear of who performs what functions between enterprise operations and the security organization. A role based access control system should be considered. A role based system with clearly defined responsibilities for each function and role. Once implemented a role based access control system is more flexible as an organization changes

#### 2.12.2.2 Policy Management services

Between the enterprise operations management and the security organization there needs to be clear responsibilities for policies and how they are to be implemented, managed and enforced. A close working relationship is required. Areas that need to be addressed are for example backup/restore, file transfer, disaster recovery, event management, systems and network management. In each one of these areas there are security considerations and the policies should detail how these security considerations are being met.

#### 2.12.2.3 Certificate / Key life-cycle management services

As part of a Public Key Infrastructure the life-cycle of certificates and keys must be managed. The options are to outsource to a third party the management of the PKI or to implement it yourself and to manage it internally. Certificate / Key life-cycle management services include:

- Registration services
- Distribution Services
- Recovery Services
- Storage Services
- Revocation Services

#### **Implementation Considerations**

The management of certificates / keys throughout their life-cycle is a very important part of PKI. There may be legal requirements to follow as well as numerous technical and operational challenges. The management of the PKI is the most important aspect for its success.

#### 2.12.2.4 Availability and performance services

Most *Security Services* and solutions have high availability and high performance requirements. This is due to the fact that the *Security Services* often are mission critical or are used by mission critical systems. The operational aspects of the security solutions need to be considered alongside the security aspects.

#### **Implementation Considerations**

When designing a security architecture which is mission critical, high availability and performance requirements need to be a part of that solution.

#### 2.12.2.5 Directory Integration and administration services

If a directory server is being implemented it will most likely need to interface to other systems. If the directory contains user profiles which need to be managed the directory needs to be interfaced to the enterprise user management system. As the directory may contain sensitive information such as username/password and certificates it must be kept secure.

## 2.13 Security Infrastructure



*Security Infrastructure*

### Component description

The *Security Infrastructure* area consists of the actual security components which provide protection for the *Business Assets*. *Security Services* such as an authentication service or encryption service are implemented using the security components in the *Security Infrastructure*.

The *Security Infrastructure* area comprises two component categories:

- Core Security Components
- Security Tools

### 2.13.1 Core Security Components

The Core Security Components provide the implementation method or technology for the Security Base Services. For example, an authentication service may be implemented using either certificates or tokens.

The Core Security Components are:

- Registration / Identification
- Authentication
- Single sign-on
- Access Control

- Encryption
- Digital Notarization
- Non-repudiation
- Content / Virus Inspection
- Logging
- Firewall
- PKI
- Platform security
- VPN

The following sections describe typical implementation methods for each security component.

#### 2.13.1.1 Registration / Identification

Registration and identification refers to the process of creating new users in a system. Ensuring proper identification and registration of users is necessary to allow effective authentication.

- *On-line registration* – with the evolution of the Netcentric environment, on-line registration has become a popular method for obtaining access to specific resources via the Internet. It allows customers to register and modify information about themselves that is stored by the host site. Consider using SSL for encryption of the data entered during the registration process.
- *Data verification services* – this is the process of verifying data such as address, social security number or other data submitted during registration for the purpose of ensuring the integrity of the data. This can be done through financial institutions or government services. This is critical if a strong authentication service is to be implemented.
- *Registration Authorities (RA)* – used in Public Key Infrastructures. The role of the Registration Authority is to certify that a public key is associated with a known entity (the entity may be an individual or a system). After authenticating the identity of the entity, a certificate is generated and assigned to the entity. The robustness of the identification and authentication step determines the strength of the certificate. The security requirements of the business capability will determine the strength of the certificate needed.

 More information is found in the *Security Infrastructure* area, Core Security Components under PKI and also in the *Security Infrastructure* area, Core Security Components, Authentication under PKI.

- *Directories and meta-directories* – registration information is often stored in an enterprise-wide directory server. Advantages of directories are performance, compared to a traditional database, and their usefulness as a central repository for user profiles (for example, customer information, certificates, etc.). Directory standards include X.500 and LDAP. LDAP directories are typically used for storing and retrieving certificates and certificate revocation lists. A directory may be used as a meta-directory providing mapping between UserIDs in different systems. This is useful when data in older legacy systems can not be changed.

### Implementation Considerations

 More information is found in the *Security Services* area, Security Base Services under Registration / Identification services.

#### 2.13.1.2 Authentication

Authentication is the process of identifying and ensuring that an entity is who it claims to be. For individuals this is usually based on a username and password. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

- *Username/Password* – one-factor authentication in its simplest and most common form. Username/Password authentication can be implemented using many standards and technologies. Advantages are ease of use, low cost and portability. Pure username/password authentication provides only basic authentication. A security architecture with username/password must implement encryption when transferring the username/password. Authentication standards include: RADIUS, TACACS, TACACS+, RACF, NT login and UNIX login. The major weakness of password-based authentication is the ease of breaking it with password-guessing and brute-force techniques. It is important to educate users about strong password policies, and to enforce the policies with password monitoring processes.
- *Token and one time password* – two-factor authentication which uses a hardware device that generate a one time password to authenticate its owner. Also sometimes applied to software programs that generate one-time passwords. This authentication is also known as a challenge response mechanism. SecurID and Enigma Logic are examples of password calculator products.

- *Certificates* – part of PKI. Certificates may be implemented for individual users or for systems such as individual servers. Different classes of certificates can be generated with defined levels of trust. The highest levels of trust are typically used in financial transactions and where confidentiality requirements are high. Different types of certificates are required for specific cryptographic protocols such as SSL, S/MIME or IPSEC. The X.509 standards defines the data in a certificate. Other standards include PKCS, PKCS#6, PKCS#9 and PKCS#10. Certificates are commonly stored in a directory.
- *Time dependent password* - a password that is valid only at a certain time of day or during a specified interval of time. Depending on how the passwords are made available to the users (a printed list of passwords changed daily, a token card, etc.), this authentication approach can be considered as either one-factor or two-factor.
- *Biometrics* - Biometrics is the science and technology of measuring and statistically analyzing biological data. This is sometimes considered a three-factor authentication by adding the concept of “what you are” (i.e. fingerprint) to “what you know” (i.e. password) and “what you have” (i.e. token card). In information technology, biometrics usually refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authenticating an individual user.
- *Smartcard* - credit card-sized devices that can be used to store information. They typically contain an integrated circuit with secure memory and hardware support for security functions. The chip can store data and a variety of application programs that can be updated whenever necessary. A high level of security protects the card issuer as well as the card holder from unauthorized access.

Typical applications are bank cards, travel cards, and campus cards; they can be used for electronic purses, personal identification, building access, and payments. A PIN code is necessary to activate the smartcard. Smartcards are considered two-factor authentication.

- *Authentication server* – a central server which authenticates and authorizes access to requested systems or services. The purpose of an authentication server is to centralize and standardize the interface to and from multiple authentication services. The authentication server will maintain user profiles in a central database that all remote servers can share. It provides better security, allowing SFA to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics. One of the most common ways to implement this is via RADIUS. RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central authentication server to authenticate dial-in users and authorize their access. RADIUS is a *de facto* industry standard. Radius is commonly used with a directory server over LDAP.

- *Directories* – directories support multiple authentication methods, such as Username/Password and digital certificates. Applications query the directory by passing it appropriate security data (for example a Username/Password) and receiving back either a message indicating the success or failure of the request. Advantages of directories are fast performance and their ability to function as a central repository for user profiles (for example customer information, certificates, etc.). Directory standards include X.500 and LDAP. LDAP directories are typically used for storing and retrieving certificates and certificate revocation lists (CRL).
- *PKI - Public Key Infrastructure*. A PKI is a networked system of certificate authorities (CAs), registration authorities (RAs), certificate management systems (CMSs) and X.500 or LDAP directories. It enables two parties unknown to each other to exchange sensitive information over an unsecured network like the Internet. PKI uses public and private keys to authenticate and encrypt information.

 More information is found under Core Security Components, PKI.

### Implementation Considerations

Authentication is an enabler for many other security functions, for example access control, and is often the first security measure an end-user will see. Authentication, when implemented in a complete security architecture, will be fairly transparent to the end-user and yet secure to allow access to a network.

 More information is found in the *Security Services* area, Security Base Services under Authentication services.

#### 2.13.1.3 Single Sign-on

Single sign-on enables a user to sign on using a single UserID and be connected to multiple systems without having to sign on to each one of them. Single sign-on provides two main benefits: a user friendly system and a system that is easy to administer.

- *Cookies / Session Management* – in order to provide single sign-on capabilities, session management functions are needed. Session management is a service which keeps track of each open session between entities, such as between servers and clients. Session management is usually implemented with a token that is passed between the client and server. The token is sometimes called a cookie. The token may also be posted within a URL. The token contains a session ID and other information required to maintain a separate identity for each session. For additional security, the token often contains timestamps and the IP address of the client to prevent spoofing or hijacking a session. Session management techniques are commonly used on the Internet to provide personalization, such as “shopping cart” features on a consumer retail site.

Single sign-on across multiple servers is more complex. It involves transferring the session information among distributed servers. A distributed session management architecture can implement such functions, and commercial products for this purpose are becoming more common.

Session management with cookies and URL-based tokens use the functionality built in to HTML browsers. To prevent eavesdropping or replay attacks the information carried in the token should be encrypted.

- *Access Control product* – provides single sign-on through the use of advanced session management as described in Cookies / Session Management, and additionally provides for authentication, authorization and access control. Advanced access control products can provide single sign-on capabilities across numerous servers.
- *Scripting solutions* – a single sign-on solution which provides strong authentication of the user as part of the initial sign-on. Once this has been accomplished, sign-on to all the other applications and resources take place through their individual sign-on protocols, but they are automated and transparent to the user.

Scripting solutions and products work through a scripting language that is used to develop login scripts for each application or system. The scripts issue the commands and transfer information needed by each application or system for user authentication and access to resources. The login information required for the remote applications and systems must be encrypted and stored securely. Similarly, the transmission of login information to the remote applications and systems must also be secure.

- *Password Synchronization* – password synchronization allows users to authenticate to different services using the same password. Password synchronization may be an element of an "Enterprise User Management" solution.

Password synchronization operates by having participating systems monitor user password changes. When a user changes his/her password, the monitor communicates the new password to other systems. This is known as "propagation" of the password change.

Often, the password synchronization system will enforce password quality requirements (e.g., length, composition, history, etc.). Examples of systems using password synchronization are NIS and NIS+, NDS, and Windows NT domains.

### Implementation Considerations

Single sign-on can provide many benefits and a quick return on investment if implemented well. In a Netcentric environment a single sign-on solution may be a way to gain access to many new and older systems. The security requirements need to be high, as a single point of access into multiple systems in a network is dangerous should it be compromised.

One important aspect is to ensure that the operations environment can provide high availability and good performance. A single sign-on solution may become a single point of failure.

 More information is found in the *Security Services* area, Security Base Services under Single Sign-on services.

#### 2.13.1.4 Access Control

Access control refers to the process of limiting access to the resources of an IT system to only authorized users, programs, processes, systems or other IT products. There are several access control methods and it can be implemented in many places in an IT environment.

- *Firewall* – provides for access control by restricting packet types, protocols, filters, sockets, ports, services and providing network address translation (NAT). Firewalls can also provide authentication, encryption and access control based on users and groups. Firewalls can be implemented as hardware or software. A firewall is an essential part of Netcentric security architectures. Firewalls are commonly implemented for network perimeter security. For access control firewalls are highly effective as they limit unwanted communication to an internal network. Firewalls are usually combined with other access control mechanisms such as access control products, web access control or operating system access control.

 More information is found under Firewall

- *Operating System* – access control is provided by many Operating Systems (OS). OS's such as Unix and Windows NT provide for control by multiple access parameters. Examples include: user, group, time of day, workstation address, files and directories.
- *Network Operating System* – similar to Operating System access control access parameters include: user, group, time of day, workstation address, files and directories.

- *Access Control product* – specific access control products provide advanced access control. In addition to Operating System access control, more control of access to resources can be provided. This is done by using additional conditions which are checked to verify if access should be granted. An example would be to grant access if the user a) belongs to the finance group b) logs in between 7am and 7pm and c) has been employed more than 6 months.

The access control products may be interfaced with databases, by using SQL for example, to enable conditional access control.

- *Web Access Control* – these tools are specifically designed for use in Netcentric environment together with web/application servers. They are able to provide a high granularity of access control. They provide access control and resource protection by installing a plug-in component for the web/application server which intercepts all incoming HTTP requests. By examining the HTTP request, the resource which is being accessed can be determined.

The web access control product can protect all resources which are accessible via a URL from a browser. Examples of these resources are: HTML pages, cgi-scripts, Java applications, business applications, databases, objects on an HTML page, links, etc.

Web access control products also provide authentication, authorization, single sign-on and logging services.

- *Role based* – role based access control is based on assigning access rights for resources to a role, not to an individual. An individual is then assigned a role and inherits the access rights of the role. While holding that role the individual can perform all actions for which the role has authorization. The benefit of role based access control is that it is easier to administer. For example: if an employee quits, his or her roles can be removed and assigned to a replacement. This alleviates the problem of deleting user accounts and creating new ones every time an employee changes jobs. An individual may have several roles. Example roles are: preferred customer, administrator, executive team, finance director, etc.

A complete role based system requires significant work to determine which roles are necessary and which functions they should be authorized to perform. Careful design is therefore required. Usually a matrix of all roles and the functions performed is used during the design process.

### Implementation Considerations

 More information is found in the *Security Services* area, Security Base Services under Access Control services.

Encryption is the process of making information unreadable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on a cryptographic algorithm and at least one key. Even if the algorithm is known, the information can not be decrypted without the key(s). There are several methods to implement encryption.

- *Public Key Cryptography* – a type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature. Because of the relatively large keys and slow speed, its use is generally limited to the encryption of small amounts of data, such as distribution of symmetric keys, authentication, and digital signature creation and verification. Public Key Cryptography relies on a Public Key Infrastructure (PKI). A Public key infrastructure (PKI) is the set of *Security Services* that enable the use of public-key cryptography and certificates in a distributed computing system. Within security domains, PKI enables the use and management of both encryption keys and certificates, providing services such as key management (including key updates, recovery and escrow), certificate management (including generation and revocation), and policy management.
- *Symmetric Key* - a secret key or symmetric key is shared between the two entities in a transaction. Since the success of secret key encryption depends upon the encryption keys being kept secure from all others besides the communicants. For such encryption to be usable and useful, support must be provided for the generation of unique keys, their storage, distribution, retirement, replacement, and secure retrieval. In particular, secure symmetric key management mandates a strong policy of hardware-enforced key separation. This is a high priority requirement for financial institutions doing financial transactions around the world. The most common implementation of a symmetric key is the Digital Encryption Standard (DES).
- *Key-exchange protocols* – a protocol interaction or mechanism for symmetric key encryption to exchange the secret key between two unrelated entities in a transaction.
- *One-time pads* - a one-time pad is a very simple yet completely unbreakable and secure *symmetric* cipher. It relies on a completely random key which must be kept safe. One-time pads are used by intelligence agencies around the world and where the confidentiality requirements are extremely high.
- *Key-stream generation algorithms* – encryption algorithm which changes keys during transmission. Relies on two key stream generators which must remain synchronized for the process to work successfully.

### Implementation Considerations

For increased security and performance a hardware based encryption device may be considered. Hardware encryption provides secure key storage and recovery mechanisms. Hardware encryption offloads the computationally intensive public key operations from the server to a cryptographic hardware module, thus eliminating the bottlenecks associated with software cryptographic functions. Functionality provided by hardware encryption includes: cryptographic co-processor for key generation, certificate generation, certificate and signature verification, signing, and hashing.

 More information is found in the *Security Services* area, Security Base Services under Encryption services.

#### 2.13.1.6 Digital Notarization

Digital Notarization is the process of ensuring that electronic information, such as a document or file, contained specific content at a specific moment in time and can be proven to not have been modified since then.

- *Digital Signature* - a cryptographic method, provided by public key cryptography, used by a message's recipient and any third party to verify the identity of the message's sender. It can also be used to verify the authenticity of the message.

A sender creates a digital signature or a message by transforming the message into a message digest and encrypting it with his or her private key. A recipient, using the sender's public key, verifies the digital signature by applying a corresponding transformation to the message and the signature.

 More information is found in the Security Infrastructure area, Core Security Components under Non-repudiation, Digital Signature.

- *Time stamping* - a method used by corporations and professionals to notarize, time-stamp and validate any type of computer-generated file, including e-commerce transactions, email correspondence, database records, word processing documents, images, and video clips. Companies can use it to detect any type of tampering with electronic data. Time stamping prevents adding, deleting data or backdating transactions. Time stamping provide tamperproof security which is especially critical in industries such as financial services, e-commerce and industries in which intellectual property and regulatory data must be protected.

Time stamping uses a hashing algorithm to create a unique document fingerprint, also known as a message digest. It is effectively impossible to change any of the documents without changing the hash values. When a document's authenticity needs to be verified, the hash value for the document is mathematically calculated from the published root hash. If the calculated hash value matches the document's hash value it can be concluded that the document has not been altered.

- *Hashing* – the algorithm used to create a message digest of a document. Hashing algorithms take a message of any length and, using a one-way function, compute a unique message digest of a constant length. Since a one-way function is used, the message can not be recreated from the result. This process will always yield the same result from identical starting data, but it is extremely unlikely that two different messages could produce the same result. The message digest can then be encrypted using the originator's private key and sent with the message. The recipient can compute the message digest of the received message using the identical hash function, decrypt the message digest sent with the message using the originator's public key, and compare the results. If a single bit of information has been changed during transmission, the two digests will differ, and the recipient will know that the integrity of the message is suspect and should be discarded. Standards include: SHA, MAA, MAC, MD2, MD4 and MD5.
- *PKI* – PKI can create digital signatures that prove that a unique individual has created a document. PKI can be used to provide Digital Notarization.

### Implementation Considerations

 More information is found in the *Security Services* area, Security Base Services under Digital Notarization services.

#### 2.13.1.7 Non-repudiation

Non-repudiation is the method used to prove that certain actions have taken place and can not be denied.

- *Digital Signature* – a reliable cryptographic method of signing electronic documents that provides sender authentication, message integrity and non-repudiation. Digital signatures provide a convenient, time-saving, and secure way of signing electronic documents. Digital signatures provide stronger evidence of the authenticity of information than a hand-written signature, which could easily be forged.

Digital signature is provided by public key cryptography. It can be used by a message's recipient and any third party to verify the identity of the message's sender and non-repudiation of origin.

Digital signatures can also be used to verify the authenticity of the message as a digital notarization service. Standards include: DSA and DSS.

### Implementation Considerations

 More information is found in the *Security Services* area, Security Base Services under Non-repudiation services.

#### 2.13.1.8 Content / Virus Inspection

There is always a chance that content is arriving and contains harmful data or applications. Content / Virus Inspections provide a method to detect and remove any harmful content before it can cause damages.

- *Mobile Code Inspection* – mobile code inspection is a method to protect an internal network from receiving hostile content. Mobile code inspection occurs at the gateway, away from critical resources, and can identify potential hostile attacks before they enter the network.

Mobile code inspection allows control, management and enforcement of organizational security policy for Java, ActiveX, JavaScript, Visual Basic Script, Plug-ins, URLs, Cookies and other content.

Mobile code inspection works with leading firewall products. Mobile code inspection is commonly also implemented at the client as well as server level.

- *E-mail filtering* – similar to mobile code inspection, e-mail filtering takes place at the gateway. It can protect the companies environment from email threats before they reach their network and compromise *Business Assets*. Organizational security policies may be implemented with e-mail filtering technologies to monitor e-mail usage. Some firewalls provide basic e-mail filtering capabilities.
- *Anti-virus* – anti-virus software is a requirement for any network connected to the internet. Anti-virus technologies will scan incoming traffic and e-mails for viruses. Anti-virus technologies can also scan e-mail attachment for hostile applications. Anti-virus software is commonly implemented at the server level and client level. Some firewalls provide anti-virus functionality. A point solution for anti-virus should be taken into consideration because general purpose anti-virus solutions may not provide as strong protection. Any anti-virus solution needs to be updated regularly.

### Implementation Considerations

 More information is found in the *Security Services* area, Security Base Services under Content / Virus Inspection services.

#### 2.13.1.9 Logging

Logs are the primary method to trace problems and security breaches in a network or IT system. By logging events from multiple devices an operator can trace the events leading up to a problem and determine the cause of the problem. Logs can be used for reactive actions as well as preventative actions. There are two methods to implement logging.

- *Centralized Event Logging* – event logging is used to record the occurrence of significant events. An event may be, for example, a user logon, an addition to a file, or a change to a user's privileges.

Centralized event logs provide a centralized collection point for security events, error reports, system alerts, diagnostic messages, and status messages generated by a system. Event logs are especially important for system security to help track and trace the actions of users in a system.

Centralized event logging is commonly implemented by using SNMP event management. SNMP events can be interfaced to an enterprise operations management system to record and log all security events centrally. The benefit of using a centralized system is that all the information can be correlated and analyzed more easily. These security events come from many devices, for example: intrusion detection tools, custom applications, operating systems, network routers, web/application servers, etc.

- *Distributed Event Logging* – in distributed logging each device and application writes to its own log file. The solution is not connected to an enterprise operations management system. A log scanning tool may be used to collect the most important events and create reports. These tools can be configured to run at specific intervals. Security events for all devices should be recorded.

**Implementation Considerations**

When designing the logging architecture it is important to take performance and network traffic into consideration.

 More information is found in the *Security Services* area, Security Base Services under Logging services.

**Example**

Examples of what events and activities to log are found in the table below:

Type of Log	Information Contained in the Log
User activity	<ul style="list-style-type: none"> <li>• login activity</li> <li>• changes in user identity</li> <li>• file accesses by the user</li> <li>• authorization information</li> <li>• authentication information</li> </ul>
Process activity	<ul style="list-style-type: none"> <li>• commands run by users</li> </ul>

	<ul style="list-style-type: none"> <li>• running-process information including program name, user, start and stop times, and execution parameters</li> </ul>
System activity	<ul style="list-style-type: none"> <li>• restarts and shutdowns of the system</li> <li>• administrative logins</li> </ul>
Network connections	<ul style="list-style-type: none"> <li>• details (when, where, what kind) of connections attempted or established with the system</li> <li>• details of connections established from the system</li> </ul>
Network traffic monitoring	<ul style="list-style-type: none"> <li>• records of all network traffic transactions</li> </ul>
Web server activity	<ul style="list-style-type: none"> <li>• remote hostname or IP address</li> <li>• date and time of the request</li> <li>• request</li> <li>• response code indicating whether the request was successful or not</li> <li>• remote login name of the user (if available)</li> <li>• username which the user has authenticated himself under (if available)</li> </ul>

#### 2.13.1.10 Firewall

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

- *Packet Filtering* – packet filter firewalls provide access control at the network layer. It accepts, rejects or drops packets of data based on the source/destination computer network address and the type of application being accessed. For example, FTP and Telnet are commonly restricted. Packet filtering firewalls can also restrict traffic by time of day, day of week, etc. Packet filtering firewalls are highly effective for implementing a SFA’s network security policy. A packet filtering firewall can be implemented using hardware such as a network router. There are also many purpose-built firewalls which perform packet filtering.

Firewalls are also used to set up secure communications via encrypted channels, so called Virtual Private Network (VPN).

 More information is found in the *Security Infrastructure* area, Core Security Components under VPN.

- *Application Proxy* – an application proxy firewall serve as a proxy for the internal server. The proxy establishes a connection to the internal server on behalf of the external user, copies the data received from the server and then retransmits it to the user. This method ensures that an intruder will not use the actual server containing the data and other sensitive information. The application proxy is commonly placed in the demilitarized zone (DMZ). Access to the application proxy is possible only from the IP address of the external packet filtering firewall, on specified protocols/ports, and from the IP address of the internal packet filtering firewall.
- *Stateful Inspection* - Stateful packet inspection uses communication- and application-derived state and context information to regulate packet traffic. The state and context information is stored and updated dynamically. This method can allow, for example, an FTP upload connection, but disallow packets with commands that switch directories during the session. Stateful inspection is a powerful tool which allows high granularity of the access control.

## 2.13.1.11 PKI

PKI consists of several components:

- Certificate Management – certificate repository, certificate revocation and cross-certification.
- Certificate Authority - an entity authorized to issue certificates.
- Key Management - key updates, key backup/recovery, key history, and key encryption algorithm. Keys can be created as private/public key pairs or as a private key only (shared secret)
- Time Stamping – prevents adding, modifying, deleting data or backdating transactions. Time stamping provides tamperproof security.

These components are used to verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and becoming more widespread. The methods to implement PKI are:

- *PKI Toolkit* – these toolkits allow a company to build and integrate a PKI. Administration and management of the PKI is performed internally. This service is intended for organizations that demand the data security and access control enabled by digital certificates and choose to build and operate their own system. There is considerable overhead to maintain a PKI and manage the life-cycle of a digital certificate. One benefit is increased control. A drawback is that rigorous security and facilities, must be implemented to protect the infrastructure. An example of a PKI Toolkit vendor is Entrust.
- *Third party managed* – This service is intended for organizations that demand the data security and access control enabled by digital certificates, but choose not to build and operate their own system. Instead they rely on the infrastructure and management of the PKI by third party companies. The benefit is that the third party vendor will manage the infrastructure and have the secure facilities to do so. The drawback is that you must trust the vendor. You also give up some control. An example of a vendor providing PKI services is Verisign.

## 2.13.1.12 Platform Security

It is important to secure the platform on which sensitive servers and applications run. A failure to secure the platform may result in the platform, server and application being compromised. There are many publicized articles about the vulnerabilities in servers and applications. Many of them are a result of weaknesses in the underlying platform.

- *Hardened Operating System* – a hardened OS, also known as a bastion host, provides for confidential, secure network communications within a defined trusted networking environment. A hardened OS includes specific security enhancements compared to standard OS versions. It can also be used to provide a hardened base for applications needing a higher level of trust, such as a Web server or application server. A hardened OS is essentially a bare-boned operating system, specifically designed for high security environments. Many of the normal OS services, such as FTP and Telnet, have been taken out and only core services required for specific functionality are enabled. A hardened OS is resistant to buffer overflows and other vulnerabilities found in a normal OS. By using protected memory space, a ‘sandbox’ is created for each service or application to limit the harm they can do.
- *Active Security Enforcement* - active security enforcement tools proactively control access to data and applications located on servers throughout an organization.

There are two approaches to active security enforcement:

- *Application Programming Interfaces (API)* – by integrating security application through an API, interoperability between security products is provided. Two major initiatives are under way Adaptive Network Security Alliance (ANSA) and Open Platform for Secure Enterprise Connectivity (OPSEC). API integration will provide powerful integration between security tools. The downside is that they are time consuming to implement and you have to maintain compatibility with all products supplied by different vendors. Two competing standards are emerging, ANSA driven by Internet Security Systems (ISS) and OPSEC driven by Check Point.
- *Event Management* – uses industry standard event management and can be integrated into already existing enterprise operations management systems. The active security enforcement components communicate with each other via SNMP events to a central console which filter, correlate and take action on security events. This form of active security enforcement is essentially an advanced form of event management specifically for security. Upon detection of a hostile security event a policy may be executed which shuts down a compromised server. This solution is driven by Network Associates.

 More information is found in the *Security Operations* area and in the *Security Infrastructure*, Core Security Components under Logging.

- *Policy Enforcement* - these tools perform scheduled and selective probes of your network's operating systems to search for those vulnerabilities most often used by unscrupulous individuals to probe, investigate, and attack networks. These tools can be used to eliminate identified vulnerabilities.

### Implementation Considerations

Platform security is an important measure to secure an environment. A hardened OS is a requirement, for example, in financial transactions. Active security enforcement is an important security management tool which can be integrated with a wider enterprise operations management framework. Policy enforcement should be used on all servers exposed on a network. It will eliminate the most common ways of penetrating a network or server.

#### 2.13.1.13 VPN

A Virtual Private Network (VPN), also known as an encrypted tunnel, is built atop a public network, such as the Internet. Hosts within the VPN use encryption to talk to other hosts. The encryption excludes hosts from outside the VPN even if they are on the public network. For two hosts to communicate with each other a VPN must be established between the two hosts. The two key standards for creating a VPN tunnel are: IP Security (IPSec) and Layer 2 Tunneling Protocol (L2TP). Together L2TP and IPSec provide complementary approaches to solid, secure tunneling.

At the initiation of a VPN, public keys are used to authenticate the users and exchange symmetric keys. The symmetric keys are then used as the session key for encrypting subsequent traffic. Symmetric keys provide faster performance than public/private keys. Depending on the level of trust in a network and security requirements VPN are implemented in two ways:

- *Personal tunnels* –where a network is not trusted a VPN is established end-to-end between the hosts. This means that the connection starts, for example, at a workstation and ends at the server with which it communicates. This provides higher security but also adds to a more complex implementation because each client wishing to establish a VPN needs client software.
- *Group tunnels* – group tunnels are commonly implemented on firewalls. The VPN starts at the firewall and ends at a firewall. This assumes that the network is trusted from the firewall to the desktop, which is not part of the encrypted tunnel. The advantage is that no client software is required; all encryption is performed by the servers or firewalls.

### Implementation Considerations

When implementing a VPN consider the type of applications and network protocols which you need to encrypt and tunnel. This will determine which standard you use for creating and managing the tunnel. L2TP has the advantage of being able to encapsulate and tunnel other networking protocols such as IPX and SNA. IPSec works with the IP protocol. The two tunneling techniques can be used together.

#### 2.13.2 Security Tools

The Security Tools support security management services and the people performing the security functions and processes. The tools help manage and control the security environment.

##### 2.13.2.1 Intrusion Detection

Intrusion Detection tools can detect suspicious activities on a network or on a platform. They work by recognizing common patterns which may indicate an attack. Intrusion detection tools provide a fast and automated mechanism which allows SFA to be more pro-active in identifying and stopping intruders.

- *Network* - these tools act like a network packet capture program, analyzing packets of information as they travel across the network, and interpreting hostile activity on your network by recognizing the network traffic patterns that indicate attacks.
- *Platform* - These tools detect intruders or abuse by analyzing audit data from the operating systems it supports. Using a rules engine, the tool spots obvious violations, such as multiple login failures. It also detects more subtle irregularities in user behavior that can indicate a masquerading user or other potential troublemaker.

### 2.13.2.2 Vulnerability Assessment

Vulnerability assessment tools assist in finding common security holes and help to eliminate them by hardening them. Vulnerability assessments are generally performed on all hosts and servers, critical or non-critical. Often these tools measure against a set of criteria or standards. Vulnerability assessment tools assist in closing the gap between the security policy and actual security by providing information about security vulnerabilities.

- *Network probes* - these tools perform scheduled and selective probes of your network's communication services, operating systems, and routers in search of those vulnerabilities most often used to probe, investigate, and attack your network. Network scans should include probing for auto-answer modems connected to the network.
- *Operating system* - these tools scan the operating system looking for common vulnerabilities. Vulnerabilities may include FTP and Telnet services, default user accounts, old and vulnerable versions of sendmail, patches not applied, xhost + enabled, etc.
- *Policy enforcement* - these tools perform scheduled and selective probes of your network's operating systems to identify any discrepancies to the SFA Security Policy.

#### **Implementation Considerations**

Vulnerability assessment tools are very important to identify vulnerabilities so they can be eliminated. It is important to update vulnerability tools regularly. Plan for the processes that are needed to periodically run assessment tools, analyze the results, and respond to problems that are identified. Vulnerability assessment tools meet the requirements of the *Security Compliance* area.

### 3 Glossary of terms

**Authentication** - a process used to assure the identity of a party on the other end of a transaction.

**Bastion Host** - analyzes traffic to the firewall and either accepts or rejects it based on a predefined set of rules.

**Certificate** - binds a public key and an entity.

**Certificate Authority** - an entity authorized to issue certificates.

**Certificate Directory** - lists all entities with valid certificates.

**Certificate Hierarchy** - a domain of issuing authorities, each categorized with respect to its role in a "tree structure" of subordinate CAs.

**Cryptography** - protects the privacy of a transaction, assures contents of the transaction cannot be altered without detection, and provides non-repudiation with digital signatures .

**eCommerce** - commercial exchanges of value between an enterprise and an external entity, either an upstream supplier, a partner, or a downstream customer over a universal, ubiquitous electronic medium.

**Digital Signature** - an encryption mechanism used to guarantee the authenticity of a message or file. A digital signature is equivalent to a digital fingerprint.

**Encryption** - the process of transforming data into a complex code so that it cannot be recovered without using a decryption process.

**Identifier** - a piece of data used to uniquely identify an entity in a transaction.

**Internet** - a publicly accessible electronic medium typically used for consumer-oriented transactions, though also used for business-to-business transactions.

**Internet Service Provider (ISP)** - entity which provides access from a user or entity to the Internet.

**Password** - confidential authentication information, usually composed of a string of characters used to provide access to a computer resource.

**Private Key** - a mathematical key kept secret by the holder used to create digital signatures and to decrypt messages or files encrypted with the corresponding public key.

**Public Key** - a mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding private key; Public keys are also used to encrypt messages or files which can then be decrypted with the corresponding private key.

**Public Key Cryptography** - a type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.

**Public Key Infrastructure (PKI)** - the architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system; the necessary support systems and processes to assure that all entities are properly bound to their public/private key pairs.

**Registration Authority** - an entity trusted to register other entities and assign them a relative distinguished value such as a distinguished name or, a hash of a certificate; a registration scheme for each registration domain ensures that each registered value is unambiguous within that domain.

**Registration Process** - the act of validating an entity's request to participate in a system, generating a unique identifier, binding that identifier to the requesting entity, and distributing the identifier to the now participant entity.

**Reissue Process** - the process of assigning an operational period of a certificate following the re-registration for a new certificate.

**Revocation Process** - the process of permanently ending the operational period of a certificate from a specified time forward.

**Router** - the primary obstacle between the Internet and another entity, such as the DMZ; filters out unauthorized traffic based on a set of filtering rules built into the firewall.

**Shared Secret** - bound to the identifier and used to verify that the entity presenting the identifier is who they claim to be.

**Security** - comprised of identification, authentication, authorization, confidentiality, integrity, and non-repudiation.

**Security Controls** - A practice, procedure or mechanism that reduces security risks.

**SMTP** - Simple Message Transfer Protocol.

**S/MIME** - a specification for E-mail security exploiting a cryptographic message syntax in an Internet MIME environment.

**Symmetric Key** - a key shared between two entities in a transaction; the most common implementation is the Digital Encryption Standard (DES).

**Token** - a hardware security token containing a user's private key(s), public key certificate, and, optionally, a cache of other certificates, including all certificates in the user's certification chain.

**Transaction** - an electronic transfer of business information which consists of specific processes to facilitate communication over global networks.

**Verify** - in relation to a given digital signature, message, and public key, to determine accurately that the digital signature was created during the operational period of a valid certificate by the private key corresponding to the public key contained in the certificate and the associated message has not been altered since the digital signature was created.

**World Wide Web (WWW)** - A hypertext-based, distributed information system in which users may create, edit, or browse hypertext documents. A graphical document publishing and retrieval medium; a collection of linked documents that reside on the Internet.

**X.509** - the ITU-T (International Telecommunications Union-T) standard for certificates. X.509 v3 refers to certificates containing or capable of containing extensions.