Information Security Framework / Program

Overview

The Information Security Framework / Program is the development of organizations security solutions into an organized service catalog items that can be offered to internal and external parties. It also can help create the specific details for each item within the service catalog. Emagined Security defines these as the following:

- Information Security Framework – A comprehensive list of security processes organized into categories
- Security Processes – Individual process level components of an Information Security Framework
- Implementation Plan – The plan for rolling out a process that includes resource requirements, timelines, and other key details

Benefits

The Information Security Framework / Program can help your company organize services into groups that can be effectively providing services to your internal customers (Business lines, Information Technology, Human Resources, Legal, etc.) and measure the overall effectiveness. By fully defining the framework and the detailed security processes your organization will be able to meet and exceed you internal customers' expectations.

Description of Service

The Information Security Framework / Program is broken down into 2 major sections.

- Information Security Framework / Program Creation
- Security Processes Creation

Information Security Framework / Program Creation

Emagined Security will work with you to create overarching Information Security Framework (Security Objectives). In order to perform the project, Emagined Security will follow a methodology that will proceed through these phases:

Phase	Description
1	Review Existing Security Program
2	Interview Staff Members
3	Develop Information Security Framework

Phase 1 - Review Existing Security Program

Emagined Security will review existing security program, security organization documentation, security architectures, and formal and informal documented or undocumented security policies, procedures, processes, and practices to acquire information to support the development of the Information Security Framework.

Additionally, Emagined Security will identify current security technology and solutions, associated processes, and assigned staff in order to develop a gap analysis with will be used in creating the framework.

Phase 2 - Interview Staff Members

Emagined Security will interview appropriate staff members about the Information Security Framework and Process Assessment Methodology. Emagined Security will interview primarily the following types of personnel as appropriate:

- Security Organization
- Information Technology
- Operations
- Legal
- Etc.

Phase 3 - Develop Information Security Framework (Security Objectives)

Emagined Security will use your company vision and goals to help determine potential risks that should be considered during the development of the Information Security Framework.

Emagined Security will develop a matrix of risks that should be considered during in the Information Security Framework. The following chart is a sample of types of risks that will be considered. The final list of risks will be determined during this project.

	Process Risk	Decision Making Risk	Environmental Risk
Strategic Issues	Empowerment/Leadership Authority/Limits Outsourcing Performance Incentives Change Readiness Communications Integrty/Fraud Unauthorized Use Reputation	Environmental Scan Business Portfolio Valuation Performance Measurement Organization Structure Resource Allocation Planning Life Cycle	Competitor Sensitivyt Soverign/Political Legal Regulatory Industry
Operational Issues	Customer Satisfaction Human Resources Product Development Efficiency Capacity Performance Gap Cycle Time Sourcing Obsolescence/Shrinkage Compliance Business Interruption Products/Service Failure Environmental Health & Saftey Trademark/Brand Name Erosion	Pricing Contract Commitment Performance Measurement Alignment Regulatory Reporting	Catastrophic Loss
Financial Issues	Price Liquidity Credit	Budget Planning Accounting Informatio Financial Reporting Evaluation Taxation Pension Fund Investment Evaluation Regulatory Reporting	Shareholder Relations Capital Availability Financial Markets

Combining your company's vision and goals and the completed risk matrix, Emagined Security will develop the Information Security Framework. A sample Information Security Framework is shown below.

	People	Processes	Controls
Program	Security Strategy Security Organization	Secure Operations Business Continuity	Network & System Security Application Security Data Security
Operations	Security Architecture & Planning Security Governance & Definition of Roles Security Program Metrics & Quality Executive Sponsorship Risk Management Legal Framework Security Awareness Personnel Security	Threat/Vulnerability Awareness & Management Security Policies & Procedures Identity Management Policy & Regulatory Compliance Management Logging, Monitoring, & Reporting Audit Function Secure Development Life Cycle Partner & Third Party Evaluation & Integration Backup Recovery, and & Archiving Change Management Data Management	Malicious Code Protection Perimeter Security Directory Services Authentication & Authorization Product Security Secure Design & Coding Privacy Confidentiality & Segmentation Secure Communications Data Integrity Storage Security Clustering & Data Availability
Monitoring & Reporting	Physical Access Control Data Loss Prevention	Configuration & Patch Management Provisioning & Implementation Information Classification Asset Management Contingency/Disaster Planning Incident Handling & Response Media Control & Handling	Mobility & Wireless Secure Network Design Secure Builds & Host Hardening Remote & Extranet Connections Encryption Intrusion Detection & Prevention

Security Processes Creation

For each Security Service / Process that needs improved, Emagined Security will follow a methodology that will proceed through four phases:

Phase	Description
1	Review Existing Policies, Processes, Practices and Documentation
2	Interview Staff Members
3	Create Security Service Flow
4	Create Documentation on Security Service

Phase 1 - Review Existing Policies, Processes, and Practices and Documentation

Focusing on the updating and documenting the current Security Service, Emagined Security will review existing formal and informal documented or undocumented policies, procedures, processes, and practices to document the current Security Service methodology. Emagined

Security will document the current service and determine from field experts in the current service methodology and determine any unwritten gaps in the current service.

This will take into account the following:

- Risk of not performing the service at all
- Risk of not performing the service well
- Determination if service is part of the core business
- Determination if the service is in good alignment with the overall security program
- Current Documentation (any current documentation on Security Service)

Phase 2 - Interview Staff Members

For each Security Services(s) being updated, Emagined Security will interview appropriate staff members about the Security Service. The purposes of these meetings will be to determine policies, processes, and assess the adoption of information security practices. During these meetings, program data will be gathered and used to document the current state of functions. Emagined Security will interview primarily the following types of personnel as appropriate:

- Management Staff
- Project management
- IT Technical Penetration Testing Staff
- Appropriate Business Units as directed
- Information Security Officer(s) & Staff
- Etc.

Phase 3 – Create Security Service Flow

Based on information obtained in Phases 1 and 2, Emagined Security will document the current and recommended service flows for the Security Service. Emagined Security will identify areas for improvement and determine the desired state (short & long term).

This process will take into account risks from the various areas of the Emagined Security's risk models in determining required security functions:
Developed service flows will also take into account:

- Process Owners
- Key Tasks
- Key Decisions
- Reporting Requirements

Phase 4 – Create Documentation on Security Service

Emagined Security will work with your company to develop Security Service Documentation. Documentation may include as directed:

- Security Service Policy
- Security Service Overview
- Formal Management Procedures
- Duties & Responsibilities
- Service Flows
- Management Documentation
- Service Level Agreements