

WHITE PAPER



PRESENTED BY:



## **BUSINESS PROCESS ENGINEERING:**

### **HOW THE KNOWLEDGE OF BUSINESS PROCESS ENGINEERING IS APPLIED TO INFOSEC AND WHAT IT ADDS IN VALUE TO AN INFOSEC EFFORT**

James D. Heimberg, ABC, Ph.D., ISSO, CA, ORA

March 22, 2006

Federal Network Services, Inc., Information Security (INFOSEC) Services practice is pleased to present this white paper that describes how business process engineering, as applied to INFOSEC issues, is a required component and adds immense value to the INFOSEC process.

At the heart of business is the basic mechanism that allows organizations to function outside of chaos. The method to overcome chaos is to decide how the organization's business will be conducted. How that business is conducted determines success or failure in the short term and in the long term, the flexibility in how business is conducted and the way changes are implemented are critical to continued success or re-adjusting from a no-longer-tenable methodology. Success comes from efficient, repeatable processes that focus on getting the core business of the enterprise accomplished. Generally, being less than successful is a direct indication of not being able to work efficiently or not being able to perform similarly in a repeated fashion and not being able to adjust to a repeatable process.

The jewel in the crown of management communications is the ability of management to oversee and direct business workflow. The phrase 'business workflow' is used to define the day-to-day business operations of the enterprise (i.e., the work the organization does to meet its goals and objectives). This is true whether the key organizational goal is defined as a product, service, or other accomplishment.

From the INFOSEC perspective, business processes are the critical intellectual property in the form of intangible assets that mark the value of the organization beyond physical assets. There is a strong propensity across business to rely on the IT arena of the organization, the office of the CIO, to assume some responsibility for business processes in a move to take advantage of the efficiencies of automating practices and cost reduction.

At the same time, there are two very different perspectives from which the approach must be taken. The first is from the aspect of shared processes, those processes that are shared not only within the organization, but also in other organizations whether they are in the same business arena as the enterprise or not. For example, most businesses find that their human resource management systems operate on very similar basis and that there is no perceived value in further automating beyond what the competition and teaming partners do, that there is not much room for improvement, as this is not considered to be part of the intellectual property of the enterprise. This argument could also be applied to those processes that are governed by laws and regulations, which further force the system to be the same across the board within different organizations (e.g., certification and accreditation or accounting). The second perspective is that those areas in which the organization excels that are not the ones that are shared across normal business efforts. The areas in which the enterprise must excel are those that create the opportunity for excellence, but that the information that drives the processes must then be maintained securely in order to maintain a competitive edge. For example, Boeing is a critical provider of wing assemblies for aircraft and the processes that are used to engineer and build wings is a critical business process that they would not like shared with competitors.

# Business Process Engineering Methodology

## Overview

In his book Communicating for Productivity, Roger D'Aprix, ABC, created a six-segment pie chart with focuses that are designated the Manager's Communication Responsibility. These responsibilities, which are listed below, describe the information about workflow processes that must be captured in order to ensure an understanding sufficient to allow for business process analysis, business process re-engineering, and/or business process management. This information must be documented in order to identify the methods to add value through INFOSEC efforts.

- Work Unit Mission; Progress
  - Work Unit's Mission
  - Work Unit's Objectives, Targets
  - Accomplishments of the Work Unit
  - Subordinates' Questions and Suggestions on Mission/Progress
- Individual Job Responsibility Standards
  - Subordinate's Job Responsibility, Standards
  - Subordinate's Job Suggestions
  - Questions about the Job
  - Policies and Procedure Affecting Job
- Individual Performance Feedback
  - Performance Appraisal Fully and On time
  - Personal Appreciation for Effective Performance
  - Areas for Performance Improvement, as needed
  - With Subordinate about Actions to Improve Performance, as needed
  - Individual's Value to Work Unit
- Individual's Needs and Concerns
  - Willingness to Listen to Personal Concerns
  - Timely Feedback by Manager to all Job-Related Concerns, Suggestions, Questions
  - Willingness to Listen to Employee Relations Problems
  - Opportunities for Career Advancement
  - Your need for Feedback Regarding your Performance as a Manager
  - Willingness to Assist Subordinates in Resolving their Conflicts
- Upward Communication
  - Successes and Failures of the Workgroup in Meeting Objectives
  - Problems in, or Obstacles to, Meeting Objectives
  - Suggestions for Senior Management Actions, Policy Changes
  - Proposals to Address Opportunities, Efficiencies
- Work Unit's Place in Company
  - How the Major Unit's Mission Affects the Whole
  - Major Business Issues Affecting the Work Unit
  - Basic Business Strategy of the Work Unit
  - Role of Other Work Units, as needed
  - All Business Actions (e.g., reorganizations, RIF, etc.) Affecting Work Unit

The communications vehicles that are used to accomplish these goals are:

- Business plans
- Strategic plans
- Project plans
- Contingency plans
- Continuity of operations plans
- Risk assessments & impact analyses
- Contract progress reports
- Proposals
- White papers
- Style guides
- Policies & procedures

Once the processes and their place within the organization can be identified, then tasking will lead the effort, whether determining what business processes exist and contributing to the success of the organization (business process analysis), determining how to change business processes to create greater efficiency (less cost or greater productivity) or improving overall product output and management style (business process re-engineering), or overseeing and managing process execution and improvement (business process management).

### **Approach**

INFOSEC personnel must have some background in process improvement and engineering with a focus on the critical factors regarding process analysis as follows:

- Intent of the process
- Policies controlling the process
- Interfaces with organizations beyond those performing the core process
- Level at which processes and associated policies are documented
  - Top Level – Overall organizational management and administration
  - Mid Level – Focused on the interfaces between equal organizational entities
  - Low Level – Desktop procedures for individual workers or workgroups
- Flow across organizational boundaries, sometimes referred to as entry and exit criteria
- Flowcharting and decision making in processes
- World-class formats for documenting procedures

Although work products will often be designed within the concept of the customer's management, all business process products and deliverables should be reviewed for their relationship with the criteria above and for their applicability to INFOSEC in terms of best-practice capabilities. The intent is to enable INFOSEC personnel to be fully function in the development of:

- Flowcharts of processes
- Policy and procedure manuals
- Standard operating procedures
- Instructional processes
- Project plans
- White papers on organizational structure and their impact on workflow

## **Process Components**

### **General**

Whether performing functions related to business process analysis, business process engineering, or business process management (and re-engineering), INFOSEC practitioners must keep focus on the intent of the core process, which are the intangible assets of the enterprise that allow the enterprise to operate within its core competencies, and the intent of the INFOSEC practice at protecting data, processes, and authority. The tools used to perform in those regards are keys to creating a beneficial INFOSEC program within the enterprise.

## Flowcharting

To understand a process or the policies that must be developed around a process (Tier 2 policies and procedures), the INFOSEC practitioner must be able to develop a view of the steps and decisions made throughout the process. The easiest way to validate the effort is by building a flowchart of the process. The flowchart does not have to contain every minute item to be performed, but should be a chronological step-through of the process with each decision point that could divert the process from the intended goal depicted.

There are many ways of flowcharting processes with the most common forms being the basic flowchart, audit diagrams, Cause-and-Effect (aka Fishbone) diagrams, Cross-Functional (aka Swimlane) diagrams, and Total Quality Management diagrams. Each has its own unique function with regard to presentation, but the basic flowchart remains the clearest working tool of all with regard to gaining an understanding of the process. Only five basic symbols need to be used. They are:

- Start and end points, which are depicted using an oval or rectangle with rounded ends that contain a very brief title of what the start or stop includes. Each start and end point should be included, so that entry and exit criteria are clear.
- Process boxes, which are rectangles containing text describing the step in the process.
- Decision diamonds, which are boxes rotated 45 degrees containing a simple yes-or-no question. Decisions that have more complex answers than simple yes or no should be shown as an array of yes-or-no decision diamonds. A decision diamond should be created for any step that is relied on for any other process box to continue the overall process.
- Connector symbols, which are circles that contain a letter or number. There will always be two, the launching point from one step in the process to the landing point at another step in the process. Connector symbols can be used when traversing a page break (on processes that flow from page to page, as returns when lines would be too complex of a way of moving from one step in a process to another that preceded it in order to ensure that an effort is completed or that repeated processes are done exactly the same way, and to relate steps in a process that are followed based on the outcome of decisions that must be made throughout the process.
- Connecting lines and arrows, which are used between segments showing the chronological nature of following the steps that are charted. Arrowheads should be used to show direction of process flow (generally only in a single direction) and should be placed at the following step even when multiple lines are used (i.e., multiple arrowheads should not be needed for clarification and process steps should not be bi-directional).

A flowchart should be developed before attempting to document any process, but this is especially true for INFOSEC practitioners as the flow chart will clearly indicate the need for process inhibitions and allow the business process developer to see the impact of each step on the whole process.

## Developing Policies and Procedures

The key of the world-class policy and procedure formats is how information is combined in the form of documentation. For processes, regardless of the level at which they apply, a good general rule of thumb in simple format follows:

- **Summary** – Describes the general topic of and reason for the documented process, including a description of where the procedure fits in the overall business processes of the organization.
- **References** – Contains references to any documents that provide support for technical issues of the process or that are referred to in the procedure document (e.g., perhaps a

higher level procedure, a policy governing the procedure, or a related procedure showing the inter-relatedness of the procedure within the full business process).

- **Supersession** – Names of any documents including earlier versions that are superseded by the version of the procedure contained in the document.
- **Definitions** – Provides definitions for terms that may not be common or that have multiple meanings, only one of which applies.
- **Procedure** – Describes the steps in the procedure in chronological order. Each step should be described sufficiently that someone with the minimum education and experience to be assigned to perform the procedure should be able to follow the steps without further need of references. For instance, if a computer administrator is the focus of a procedure and the company requires certifications, education, and experience at a midlevel, the procedure should not have to be written so simply that it includes instructions to remove a disk from a disk drive before placing a new disk in the drive.
- **Responsibilities** – Describes the process by grouping the steps (restated in general terms) by the organizational entities responsible for performing the steps. This section is critical as it lets every involved organization know the expectations that the procedure has of their performance worded separately in a way that they do not have to read through everyone else's steps.

By developing policies and procedures to this model or any similar model, the repeatability of the process is enhanced, the outcomes are more easily predicted, and the INFOSEC efforts are more easily attained.

### **Developing Standard Operating Procedures**

Standard Operating Procedures (SOPs) are process guides that allow members of a group to gain an understanding of how their group operates or how a system that their group uses operates. SOPs do not take the place of policies and procedures, but should be used when the groups that use a process come from diverse roles and need to ensure that the work being performed is performed the same way or nearly the same way every time. A good example is that the Navy uses SOPs to guide watch standers in performing their assigned duties even though they come from various departments throughout the ship's complement or staff.

SOPs should contain much the same information as a documented procedure from a policy and procedure manual would with a copy of the flowchart outlining the procedure. In addition, an SOP should contain references to guides and manuals with copies of pertinent sections as needed in order to fully describe every part of the procedure.

Depending on usage, an SOP should be published in a form that can be used where the use is expected. For example, an SOP to be used in repairing automotive engines should be printed with plastic-coated pages in a plastic binder in order to withstand the wear and tear that is expected. Another example might be the setting up of border INFOSEC protection where automated rules and policies need to be put in place at the server, equipment rack, or the appliance itself. For this type of use, the SOP might be electronic on a laptop or on a server so that the presentation can be done in a split-screen mode where the SOP is viewed at the time the inputs are being made, even with the potential for cut-and-paste editing. The nature of an SOP is such that it might need to include proprietary information, so the publication format should lend itself to a more privacy-related usage.

### **Developing Instructional Processes (Training)**

Implementation of processes and change of processes requires that personnel who are supposed to be working the issues are properly trained in use of the steps and decision making.

There are many types of instructional tools that can be developed to fulfill this role. Some of the options include:

- Computer-Based Training – Materials can be put together that describe the various functions that need to be performed in a manner that includes screens that must be manipulated to ensure that habitual tendencies in working with computer screens are set properly at the onset.
- Classroom Training – Many of the procedures that are performed repetitively have to do with the many types of hardware and software systems that network administrators and security officers are going to deal with during the course of their activities at work. Some of those are sufficiently complex needing classroom training to teach those who will be tasked with administering the systems with the greatest opportunity to work with the actual system before having full responsibility in the operational environment (e.g., complex cryptographic systems, new server operating systems, a Certification Authority Workstation, etc.).
- On-the-Job Training – Some of the efforts require a brief apprenticeship-like time with an experienced administrator or senior Information System Security Officer (ISSO). In this instance, a specific training regime that includes the various operational facets that will be encountered can be developed that ensures the least amount of training time for the greatest return in the form of a trustworthy, trained administrator.

These types of instructional tools can be prepared using the minimum amount of effort to realize a working model that can be used repeatedly rather than a single use item.

### **Producing Project Plans**

Project plans are detailed descriptions of work to be performed in order to achieve specific outcomes. Project plans can be prepared using semi-automated tools (e.g., Microsoft Project). These types of project planning tools work well in producing PERT, Gant, and other types of charts that can be used to measure progress and to define the critical path and costs of each of the steps that are identified. Additionally a project plan document should be prepared so that the project can be adequately managed from inception through end of lifecycle.

The purpose of project planning is to ensure both the project team and the project sponsor understand and agree to the output of the project: that requirements, deliverables and acceptance criteria are defined and agreed upon; that project tasks and resources are identified and aligned; that the project timeline is defined.

It is axiomatic in project management that time spent in project planning is time well spent. Poor planning is the leading cause of project failure.

The project plan should at a minimum include:

- The project or program name and types - Provide the name of the project or program and describe the type of effort with regard to issues such as operational program, operations and maintenance project, development project, special project, etc.
- A description of what is intended to be accomplished by operating the program or project
- A Concept of Operations – This should describe how the program or project will function, its management style (e.g., inhouse, contractor operated, remote operation, etc.); size (in terms of both financial resources applied and/or needed and number of people needed); duration; etc.
- List of Applicable Documents – This should contain a list of documents that:
  - Documents that drive program or project requirements or that are deliverables on the project or program
  - Management oversight requirements (e.g., system architecture or lifecycle development plan, etc.)

- References that are contained in Sections 3 and 4
- System Requirements including:
  - A system definition that describes any system (physical, software, or virtual) that is the intended outcome of the program or project
  - Characteristics, such as:
    - Performance Characteristics - For a product development project or program, describe fully how any developed product that results from the project or program. For an operations and maintenance project or program, describe the minimum project or program performance results (e.g., metrics or successful operations). For a management program, describe the minimum acceptable operational goals for the program. For other unique efforts, describe the minimum successful parameters of the project or program.
    - Interface Characteristics – This should include both internal and external interfaces.
  - Reliability Factors that describe how the system should function with indications of mean time between failure or other indicators that the system is not performing up to the highest performance characteristics.
  - Training Factors that describe any training that will be required for operational success during duration of the program or project and/or that will be needed for successful implementation of the product that results from the program or project.
  - Logistical Factors that describe any logistic requirements associated with the project or program. Such issues include any warehousing, packaging, transportability, distribution, or dissemination issues associated with the product and putting the product into use.
  - Project Plan Factors that describe the workings of the project during the phases before operational inception. Such requirements might include design reviews, prototype requirements, etc.
- Quality Assurance Requirements – For every requirement listed in the System Requirements Section, there must be a quality assurance requirement in Section 4 that provides the tools to measure how effectively minimum requirements are going to be met. The quality assurance requirements will provide for future checking on the success of the program or project management team as well as the success of the effort with regard to what was originally intended.
- Preparation for Delivery Requirements that define the method for documenting and receipting any deliverables for the program, with a specific focus on the documents that were referenced in Section 2.
- Any notes that are required or that provide any other additional information that will assist the reader of the program or project specification in understanding the full scope and/or impact that will result from program or project operations.

In addition, a scope specification should be prepared that defines:

- Project Sponsor
- Date of Issuance
- Expected Outcome
- Alignment with the Organization's Strategic Plan
- Coordination and Acceptance Requirements that identify those responsible for coordinating and approving this specification. The approving authority is usually to project sponsor.
- References
- Scope Requirements
- A List of Assumptions and Constraints
- Acceptance Criteria that define what deliverables will result as products of this project and how each will be tested to ensure that the product of the plan is acceptable. Each deliverable should be tied to one or more requirements. For the acceptability, list a test,

metric, or measurement that will be used to ensure that each of the requirements has been met. If necessary, define the range or level within the measurement that indicates acceptability.

- Formats for Deliverables (Applicable to software and documentation deliverables.)
- Project Completion and Acceptance Criteria that define the minimum acceptable standards for completion of the project. In other words, define the criteria that will be used in order to gain customer acceptance of the outcome of the project and what will signify acceptance. Identify in the customer organization (by name or office symbol) who will do the acceptance for each deliverable.

### **Writing White Papers about Organizational Workflow and Impacts of Change**

White papers are simply descriptions of items, systems or concepts that are to be evolved into final products or systems. White papers are used to share understanding and to develop scope before work is performed or to share understanding of the meaning of projects to be performed.

Like this document, each white paper should include sections on overview, method for completion, individual components of the whole effort, and a summary. If this was based on research that was conducted in a laboratory setting or a documentation search, additional sections on findings and recommendations should be added. Typically, the recommendations should be the initial section after the overview and/or introduction, so that the tone for what follows is properly set. However, there may be instances where the project description is more important to the reader than the recommendations, in which case it should precede the recommendations. There is no standard format for this type of document.

## **Summary**

It is a widely held belief that INFOSEC can only be practiced successfully by those who have a background in business process development and description. For this reason it is a key part of the plan for Federal Network Systems' INFOSEC Services Practice to only field ISSOs and Information System Security Engineers (ISSEs) who have a background in business process engineering.

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

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