Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

Beyond Compliance: Cultural Change
Enabling Transformation to a IT Security-Focused Culture through Communications

Ellen C. Roth, SPHR, GISO

Abstract—*Within the last two decades, Federal agencies have been directed to engage in large-scale change efforts to develop and implement IT security programs that protect organizational assets. These efforts have been guided by regulations such the Federal Information Security Management Act (FISMA) and Office of Management and Budget Circular A-130, Appendix III, each of which specify that programs must be designed and executed immediately. All too often, program development efforts focus on compliance with these regulations and do not take action that supports changing cultural values.*

This paper advocates Federal agencies taking an approach to program development that reaches beyond compliance and enables cultural change. In doing so, this paper discusses how individual behavior change and organization-wide cultural change occur. Finally, the paper provides a step-by-step process for establishing a communications element within the IT security program to enable lasting change.

Index terms – Information Assurance, Infrastructure Assurance

I. Introduction

Over the last several decades, information technology (IT) security regulations have radically transformed government operations. Starting in 1987 with the Computer Security Act (40 U.S. Code 759 and Public Law 100-235, Jan 8 1988), agencies have confronted pressure to ensure the confidentiality, integrity, and availability of assets managed by the government. This regulation established the National Institute of Standards and Technology (NIST) to develop and promulgate standards and guidelines for protection of federal computer systems and mandated:

- establishment of "security plans" for federal systems that contain "sensitive information"; and
- mandatory periodic training for all persons involved in management, use, or operation of Federal systems that contain sensitive information [1].

In 1996, Office of Management and Budget (OMB) Circular A-130 Appendix III was revised to subsume the Computer Security Act and require agencies to:

- establish a minimum set of controls to be included in Federal automated information security programs; and
- [assign] responsibilities for the security of automated information [2].

Legislation and guidance has shown that IT security is a clear priority. In 2000, the Government Information Security Reform Act (GISRA) was issued to codify OMB A-130 Appendix III and ensure agencies were accountable through annual program reviews. As a final action, Federal Information Security Management Act (FISMA), part of the E-Government Act of 2002 (H.R. 2458/S. 803) ensured the permanency of GISRA's requirements, established Federal Computer Incident Response Center (FedCIRC), and strengthened NIST's role as the government's IT security standards issuer.

Agencies have indeed become accountable for increased security. Now, after three years of GISRA and FISMA program reviews, agencies have made progress in establishing the technological and organizational structures required of such large-scale change. However, many organizations have focused entirely on compliance, stopping short of seeing the larger vision of Federal IT security regulations. Though the vision may be implied rather than expressed outright, organizations must reach beyond compliance and achieve cultural change to build security-focused organizations.

II. A Look at Business Process Reengineering

A starting point for understanding the intricacies of large-scale process changes is business process reengineering. Michael Hammer and James Champy, originators of the concept, define reengineering as "the fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance [3]." Although reengineering is generally associated with private sector reorganization and downsizing, specific concepts translate to government's IT security program development initiatives. The reengineering framework can be a useful lens through which to study the organizational transformation associated with creating IT security programs.

A. Risk: The Federal Government's "Burning Bridge"

One of the most important reengineering concepts is the "burning bridge." Reengineering requires a significant

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

amount of effort, and places stress on the organization that is being changed. Consequently, organizations do not haphazardly reengineer without a serious reason. This reason is the "burning bridge"—a serious fact or happening that has either occurred or is soon to occur, to which an organization must react resiliently and intelligently if it is to survive.

For corporations, the burning bridge is almost always the rise of aggressive marketplace competition and/or a significant loss of revenue. The livelihood of most corporations relies on the ability to meet customer demands. The Federal government's burning bridge is based on threats. The government faces the need to protect the assets that support operations: specifically the networks and systems that process and protect data and enable critical functions. Trend data from many sources including FedCIRC show that both threats and incidents in agencies have risen dramatically and show no signs of decline. In addition, IT security regulations and periodic audits have established urgency and accountability for action within individual agencies.

B. Manganelli and Klein's Reengineering Methodology

Reengineering has proven effective in resolving "burning bridge" issues. During the reengineering process, organizations thoroughly examine existing business processes and new requirements. Then, they build new structures and processes that require organizational transformation to implement. Manganelli and Klein, two industry scholars and management science practitioners, suggest the following five-stage reengineering model to guide this enormous task [4]:

1) Stage 1: Preparation

In Stage 1, the organization generates momentum and impetus for change by examining the criticality of the burning bridge and building the reengineering team. With a through understanding of the challenges ahead, the reengineering team's senior management sponsors build organizational energy to support the changes to come.

2) Stage 2: Identification

In Stage Two, the future organization is conceptualized. In a traditional reengineering exercise there is complete freedom to explore the possibilities of what the future organization and process design could look like. Within the government's IT security initiatives most of the design work has been completed. *Office of Management and Budget Circular A-130 Appendix III* articulates requirements to implement current regulations.

3) Stage 3: Vision

Stage Three entails designing the processes that will lead to "breakthrough performance." In the government's case, the breakthrough desired is a change in the security of assets and the establishment of a strong IT security posture. Organizations consider the quantitative level of performance required for new processes to be considered successful, such as the staff necessary to support rollout. The team models the ideal organizational state.

4) Stage 4A: Technical Design

This stage examines how individual processes are interrelated and identifies technology required to make the new operating environment viable. In the security context, the technical design includes designing the network architectures that will support secure operations. In program development, this may also include technical processes and guidance.

5) Stage 4B: Social Design

The social design stage is critical to ensuring the technical design works and cultural change occurs to support reengineering. As described by Manganelli and Klein, "the purpose of this stage is to specify the social dimensions of the new process. This stage produces descriptions of organization, staffing, jobs, career paths, and incentives employed; designs for the interaction of technical and social elements; and preliminary plans for recruitment, education, training, reorganization, and redeployment" [4]. This stage is concerned with how to motivate and persuade the work force to adopt the new processes that have been specified.

6) Stage 5: Transformation

The final stage of reengineering is the most difficult and most important. In this stage, old processes are discarded, and the new process or processes are instituted. As a result of the swiftness with which change is implemented, the work force's reaction and information needs must be carefully monitored. Change management is critical to the success of transformation.

C. Reengineering within the Federal Government

Several stages that Manganelli and Klein outline have been guided by the highest levels of government in writing the visionary policy for IT security program development. The vision has then been delegated to individual Departments for action. Agencies are empowered create their own technology and social designs and change strategy as long as they are compliant with government-wide policy and achieve reasonable results. A one-size-fits-all technology design or a standard approach to people issues would not be practical since each agency has its own culture and processes to manage.

For a reengineering effort to succeed, the change management strategy within the social design must create employee buy-in. In addition, there must be a well-designed organizational transition plan that is supported by

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

senior management and executed through ongoing communications. As Manganelli and Klein explain "One way in which the organization detracts from an individual's performance is by failing to clearly communicate what it wants the employee to do [4]."

III. Fostering Behavior Change

Organizations face an enormous challenge in transforming culture in response to IT security regulations. Even before on-the-ground efforts to change employee behavior begin, many other large efforts must have completed. Specifically, organizations must create or modify its IT governance structure, policies, procedures, and define the roles and responsibilities of all that who are affected. These actions have consumed the energy of Federal agency IT security personnel for the last three years. Some organizations have proactively examined the impact of changes to policy and individual roles. The majority, however, have left thinking about change to the later stages of development. As an added challenge, annual program reviews ask questions about the assessment of risk and certification of systems. This emphasis on action first often forces organizations to move ahead in implementing policies and procedure before they have been crystallized and communicated to staff. As a result, individuals with a security role may be confused about expectations and responsibilities. Future change efforts must be even more coordinated to convey that new policy is mandatory and lasting, and that security is a business enabler.

Understanding how behavior change occurs is essential to changing an organization's culture. Although the goal is to change the behavior of an entire organization, change occurs one individual at a time. The principles of operant conditioning and adult learning shed light on how behavior change occurs.

A. Classical Conditioning

Behavior change theory begins with Pavlov's 1927 classical conditioning model [5]. In the familiar "Pavlov's dog" experiment, Pavlov sounded a buzzer at the same time as food was shown to a hungry dog. After this experiment was repeated many times, the dog began to salivate when the buzzer was sounded, and without seeing food [5]. The important discovery from this experiment is that there are two types of responses given a stimulus: an involuntary response (dog salivating, which is natural) and voluntary response (dog responding to buzzer, which is not natural). Voluntary responses can be shaped or *conditioned* through repeated events. Since the buzzer always sounded at the same time the food was presented, the dog learned to associate the buzzer with food.

B. Operant Conditioning

Broadening Pavlov's theory, scientist B. F Skinner developed the principles of operant conditioning in the 1950s. In this type of conditioning "the learner emits voluntary, or active, responses that operate on the environment. If these responses are reinforced, they will become more likely in the future [5]." In operant conditioning, there are four possible outcomes given a voluntary behavior:

- something good can be **given** as a response to the behavior **as a reward**
- something bad can be **removed** as a response to the behavior **as a reward**
- something bad can be **given** as a response to the behavior **as a punishment**
- something good can be **removed** as a response to the behavior **as a punishment**

To understand how the delivery of these outcomes affects behavior, consider how an individual is conditioned not to touch a hot stove. An unaware individual may touch a hot stove, not knowing that the consequence of touching the stove is severe pain. Once the individual has experienced this consequence however, he or she is unlikely to repeat the action a second time—at least not in the near future. The individual therefore has been conditioned not to touch the stove due to the punishment that ensued. Also consider a positive example. An individual who typically completes work at the last minute unexpectedly finishes work two days in advance. As a result, his employer rewards him with verbal praise--a reward. If the praise is delivered regularly, the employee's behavior is likely to change. In summary, an individual will change behavior in response to either a reward *or* a punishment. Positive reinforcement as been proven most effective.

C. Principles of Adult Learning

While Pavlov and Skinner approaches behavior change as the result of conditioning, adult learning theorist Malcolm S. Knowles view behavior change as the result of learning. Adults have specific characteristics and preferences as learners. The following two adult learning principles should guide how change should be introduced to set the stage for learning and behavior change:

- **Adults expect to learn information that is relevant and immediately applies to their lives**: Adults learn better and incorporate new information into behavior when they can see the information's relevancy. Therefore, change communications should be clear and should include no more or less information than required

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

to make a point.

- **Adults want practical answers to their problems and questions**: Adults will have questions when confronted with something new. Providing resources for help or references for further guidance empowers adult learners to make changes.

IV. Compliance and Cultural Change

On the subject of behavior change, Federal agencies face an interesting dilemma. On one hand, the Federal government has mandated that the agency's IT security program be installed and implemented. Consequently, change is mandatory and individuals must fall in line. On the other hand, for change to last, individuals must buy-in to the value of security and feel that the behavior change required to support the program is worth the effort. Alternatively, organizations can view change as a process grounded in behavioral conditioning, which starts with compliance and ends with cultural change.

A. Compliance

In terms of operant conditioning, a compliance approach to change uses punishments to eliminate non policy-compliant behavior. Proceeding in this way may sound like a good way to change behavior in IT security, but implementation presents significant challenges. First, it is very difficult to establish user accountability. Although there are some tools that can track user behavior, it is difficult and costly overall. For example, audit trails can be used to reconstruct the path and actions of the user, but scrupulous monitoring of records requires dedicated resources, which are often in scarce supply for this purpose. Second, many policy statements specify actions that only need to occur periodically. For example, OMB A-130 Appendix III specifies that risk to individual systems must be assessed at least once every three years or upon significant change to a system. Although an agency could apply a penalty upon discovering non-compliance with this particular policy statement, the punishment itself would not occur often enough to make a serious impression on the delinquent system owner. Consequently, it might be possible to tolerate the punishment associated with such a policy since the punishment would happen very infrequently.

Ultimately, "punishment will simply help you stop or suppress an undesirable behavior [6]." For an IT security program to be successful, non-compliant behavior of users and those with a more substantial security role must be eliminated rather than simply suppressed due to a negative consequence. For change to be successful long-term, managers and other stakeholders must feel that the change will improve existing conditions or make the organization stronger. In addition, individuals must feel that their behavior is a positive contribution to success. Otherwise, individuals do not become committed to the new program and may work against its objectives. For each of these reasons, organizations must take a comprehensive, more positive approach to change to ensure enduring results.

B. CHANGING ORGANIZATIONAL CULTURE

An alternative way to change behavior is to change an organization's culture. This systemic approach digs deep into the fabric of the organization and works to change what individuals and the entire work force value. More robust than using a compliance strategy, cultural change is complicated but beneficial.

As described by Cummings and Worley, "Corporate culture is the pattern of basic assumptions, values, norms, and artifacts shared by organization members. These shared meanings help members to make sense out of the organization. The meanings signal how work is to be done and evaluated…. Corporate culture includes four major elements existing at different levels of awareness [6]":

- **Basic Assumptions** consists of unconscious assumptions that dictate how members "perceive, think, and feel about things. They represent non-confrontable and non-debatable assumptions about relating to the environment, as well as about the nature of human nature" (527).

- **Values** consist of "values about what ought to be in organizations. Values tell members what is important in the organization and what they need to pay attention to" (527).

- **Norms** guide "how members should behave in particular situations. These represent unwritten rules of behavior" (528).

- **Artifacts** are "visible manifestations" of basic assumptions, values, and norms. One important artifact would be the observable behavior of others in the work environment.

According to Cummings and Worley's model of the levels of consciousness, individuals are impacted in many ways by their corporate culture. Cultural change affects the entire behavioral system within an organization. Initially, individuals receive the message that change is important through corporate communications. Over time, they also begin to see physical manifestations of the change that is occurring, such as trinkets placed in the work environment, or the behavior of their peers, who "fit in" to the organization and are rewarded for their behavior. As the number of artifacts or physical manifestations increases, so does the importance of the value message and the likelihood that others will internalize the change.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

It is natural for individuals to want to assimilate to corporate culture to "fit in" with what is important and what behavior is rewarded. This is precisely why in the long-term, cultural change is sustained. The experience of working toward a common value is rewarding to the individual. Tangible rewards such as awards are effective stimuli to elicit the response of compliant behavior. Over time, the notion that "security is important to this organization and compliance will bring rewards" becomes a guide for organizational norms, and the value itself becomes one of the basic assumptions about how business is conducted. This leads to transparency within business processes, which is the goal of organizational and process maturity models, such as the one described in the National Institute of Standards and Technology (NIST) Special Publication 800-26, *Security Self Assessment Guide for Information Technology System.*

C. Challenges in Changing Culture

Although the change model described by Cummings and Worley appears straightforward, there are some pitfalls that may thwart the change effort. Each of these regard how change is introduced, communicated, and managed by the IT security program office:

- **Lack of management support for the change effort**: The behavior of leadership sets the tone for the behavior of the rest of the organization. Therefore, leaders are essential in creating norms, transforming them into values, and weaving them into the organization's basic assumptions. Clear expressions of support such as event appearances and memoranda greatly assist the change effort.

- **Inconsistent policies**: Policy and procedure must be consistently communicated and implemented, and consequences for non-compliance must be applied evenly. For example, since FISMA requires all employees to attend annual awareness training, the requirement should be enforced for all employees equally. Preferential treatment for senior management in particular sends the message that new program requirements are optional rather than mandatory.

- **Failure to build change urgency within the work force**: Behavior change requires conscious effort. Unless it is clear why change must occur, the work force will naturally resist new policies and procedures as they interrupt the status quo. From the adult learning perspective, adults like to know "why." In terms of IT security the work force should understand that change is essential to the security of government assets and that the secure operation of one agency strengthens the government as a whole.

- **Failure to keep change at the forefront**: People have the tendency to ignore events or messages unless they are communicated repeatedly. During organizational transition, messages regarding changes and new values should be delivered frequently.

V. COMMUNICATIONS: A POWERFUL TOOL FOR PROGRAM EXECUTION

Effective communication has been proven the most important tool in establishing organizational change. In fact, theorists Edward and Mildred Hall state "although culture is many things, it is fundamentally communication—a process for creating, sending, storing, and processing information" [7]. Communications make organizational values clear, and allow individuals to respond with appropriate behavior because they receive the information they need to act effectively in their roles. By including a communications element within its IT security program structure, Federal agencies can ensure that the change to an IT security focused culture occurs and is maintained. Rather than leaving individuals to discover what behaviors are required to support the security program, continuous communications leave little to speculation.

Building an IT security communications program element starts with creating a strategic communications plan. Creating the communications plan involves engaging in a structured exercise to identify key audiences and their informational needs, and selecting communications channels that will best deliver important messages to each audience. The information gathered during the development process has multiple uses. First, it will help the organization assess what informational needs exist for stakeholders. In addition, information gathering will help identify issues that could stand in the way of cultural change. The overriding benefit of the strategy is that it ensures relevant, useful IT security program information is delivered to each audience group, which makes it easier for each group to respond with appropriate behavior.

A. Communications Planning Process

1) Step One: Discovery

The first phase of creating a communications plan is the discovery. This entails identifying how IT security communications currently occur. Organizations may want to skip this step in order to reduce time or expense. Others may feel that this step is unnecessary because it is already clear that communications happen poorly or do not occur at all. However, completing this phase of the planning process will make subsequent steps easier and more precise.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

Security information commonly travels throughout the organization in many ways. Within organizations that have developed a governance structure, there is often a staff of individuals who support the CSO who are responsible for IT security program development. These individuals generally issue data calls, provide informational briefings, send memos, and draft policy or procedures for other parts of the organization. In addition, they engage frequently with groups in casual conversation and possibly during training events. Each of these types of information dissemination is a communication.

The outcome of Phase One is to select a single entity that will coordinate and disseminates all IT security-related communications in the future. This not only ensures that messages are consistent, but also establishes accountability for executing the communications plan once it is implemented. This entity may be an individual within the CSOs office or a group. It may be practical to include this function as part of the standard training and awareness program element since this element also concerns people and behavior change. However, if the communications function is integrated into training and awareness, communications must be a priority and not be left as a secondary task. Another approach would be to have a stand-alone communications program that delivers the messages that the awareness program creates in addition to those of other IT security program elements.

2) Step Two: Identify Target Audiences

Step Two entails looking at agency's population and deciding upon major, discrete groups that have similar IT security program roles and therefore similar informational needs. Most agencies will have an end user group, a management group, and a group of individuals with specialized security responsibilities. These groups are a good starting point, but other groups may exist as well. Audit and compliance audiences such as the Government Accounting Office (GAO), Office of Management and Budget, and the agency Inspector General may comprise their own audience group as these groups receive updates on the progress of IT security program development and implementation After identifying each group, state the characteristics of that group. For example, the end user group can be defined in the following manner: "This group includes every member of the Department's staff. Users in this group receive communications and awareness messages that are appropriate for a general, non-technical audience."

The overall goal of the communications program is ensure that every target audience looks to the CIO's office or whatever entity is responsible for IT security program management for security guidance and information. Since the structure of the security function within most government agencies consists of a small staff of program managers along with a decentralized IT security professional work force, it is difficult to forge this relationship. There is often no automatic accountability relationship between security professionals and the program management office because there is no official reporting/annual review relationship. Informal relationships such as these will be strengthened over time because the program management office or similar entity will be the central source of IT security communications. Therefore, this office will hold informal power that can be used to build more uniform program execution. Overall, as relationships are built over time, security will become less decentralized, more coordinated, and more consistent.

3) Step Three: Setting Goals

The objective of step three is to set communications goals for each target audience identified in Step Two. This provides structure to the communications plan, and clarifies the relationship between the CSOs office and this group. For example, a Department-level communications plan might have the following goal for communicating with Subagency Heads: "Create a partnership between each Subagency Head and the CIO's office to ensure Departmental policies are implemented effectively within respective subagencies." The goals of the plan are critical, because they articulate the cultural change objective for each audience. The above goal is a primary example. This goal demonstrates that the CSO's office will work closely with Subagency Heads in implementing the IT security program. Subagency Heads, then, are change agents.

4) Step Four: Identify Types of Information Needed By Target Audiences

In this step, the types of information that were identified in Step Two within the audience description are broken down more specifically, according to each goal that was identified in Step Three. For example, if the senior management audience requires high-level security, the specific types of high-level security information that need to be disseminated would be listed. Some examples of what would constitute "high-level security information" may be policy summaries, metrics, or security briefings regarding specific security issues. Some groups will require the same information as other groups, but often messages will need to be tailored to meet the needs of each audience. Senior management, for example, may need short informational bullets regarding an organizational standard. In contrast, those who must implement the standard would need to receive more detailed information.

5) Step Five: Identify Communication Channels

The method of delivering the specific messages, or communication channels, must be defined as part of the communications planning process. Some communications channels will already exist within the organization, and others will need to be augmented or created. For example, individuals with specialized IT security responsibilities will need virus updates and patch information on a regular basis.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

One channel that could be used to ensure the audience receives this message is a Web site, likely produced and maintained by the CSO's office or the staff responsible for program development. It is possible that the agency's current Web site will have to be expanded and enhanced to take on this function. In addition, procedures may need to be written to specify how information is to be gathered from industry sources and updated for the Web site.

There are two important considerations in choosing communications vehicles. First, it is most effective to convey each major message to an audience group needs to more than once, using two communications channels. This ensures message saturation, which is key to ensuring individuals absorb the message and act upon it. For example, if end users need to receive general awareness messages, they could receive these through posters, emails, tip sheets, and the organization's Web site, and articles in various existing publications. As pointed out in NIST SP 800-16, "If a stimulus, originally an attention getter, is used repeatedly, the learner will selectively ignore the stimulus" [8]. For this reason, the more ways a message is delivered, the better the chances of success. Second, it is important to balance the number of communication vehicles and the time and effort required to send the message. It would be impractical to focus all available resources on communicating a few messages to a single audience group, while neglecting the others. Similarly, it would be impractical to implement a plan that entailed building fifty new communications channels unless there were significant resources that could be devoted to this effort.

6) Step Six: Create a Communications Matrix for Each Audience

Once all previous steps have been completed, agencies should create a matrix for each audience that lists the:

- Type of information that will be disseminated,
- Communications channel used,
- Frequency of dissemination, and
- Individual or office responsible for dissemination.

This matrix represents the culmination of communications planning efforts. Each matrix is a roadmap for how the communications point of contact will interact with each audience group. The matrices should comprise the majority of the communications plan document.

7) Step Seven: Specify the Evaluation Method

Step Seven involves deciding how the effectiveness of the plan will be judged. It is important to monitor how well the target audiences are receiving the messages that are being sent, to determine if any modifications need to be made to the plan. This can be done by surveying the target audiences individually, or through other indicators such as the number of hits a Web site for individuals with specialized IT security responsibilities receives. Whatever the method, by focusing on evaluation an organization can ensure that the initial step of instituting culture change is progressing effectively via the communications program.

VI. Communications Plan Execution

Given the pitfalls that can be encountered during the change effort, the most effective way to manage transition is by communicating with target audiences throughout the IT security program development and execution process. Creating a communications strategy at the beginning of IT security program and starting a dialogue with the work force prior to program execution will ensure a smooth transition to long-term cultural and behavioral change. Instead of trying to assess needs as they arise, or realizing that communications are necessary after the change process proves difficult, a structured communications process will help alleviate predictable trauma and frustration. However, if an agency is ready to execute its IT security program, or if the organization has already begun implementation, it is still beneficial to develop a communications plan. Frequent, focused communications will help transition individuals to new roles and responsibilities within the IT security program. Regardless of the circumstances upon which the communications strategy is written, once the communications plan has been developed an organization is ready to start managing the program.

Since the communications program is created to introduce and sustaining cultural change, it is important to regularly monitor the effectiveness of communications. This includes making sure that messages are being initiated and disseminated when necessary, and are issued by the planned sender. It also means following up periodically on the status of communications, and taking the time to analyze if the plan itself considers the informational needs of all target audiences. This will provide insight into whether the messages necessary to promote cultural change to a security-minded culture are being sent and received and what can be improved. If significant change is required, the plan should be revisited, starting with Phase One in which organizational dynamics are evaluated and documented.

VII. SUMMARY

For most government agencies, it has been challenging to develop IT security programs that include the elements specified in OMB A-130 Appendix III. Beyond creating policy, procedure and new organizational and technology structures, agencies face the even greater challenge of ensuring that the work force commits to new values. Organizations must ensure that individuals understand changes to familiar processes and know how to perform.

Effective communications are essential to promoting cultural change. Implementing a communications program

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

means developing a communications plan, which removes lack of information as a potential obstacle that could stand in the way of making IT security cultural change. Agencies are successful in moving beyond compliance when they implement strategies to achieve organization-wide cultural change.

VIII. References

[1] http://www.itsc.state.md.us/oldsite/info/InternetSecurity/Regulations/CompSecActSummary.htm

[2] http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

[3] Hammer, M. and Champy, J. Reengineering the Corporation: A Manifesto for Business Revolution. New York: Harper Collins, 1993.

[4] Manganelli, R. and Klein, M. The Reengineering Handbook: A Step-By-Step Guide to Business Transformation. New York: AMACOM, 1996.

[5] Gagne, R. and Medsker, K. The Conditions of Learning: Training Applications. New York: American Society for Training and Development, 1996.

[6] Cummings, Thomas G., and Worley, Christopher G. Organization Development and Change, Fifth Edition. New York: West Publishing Company, 1993.

[7] Rothwell, W., Sullivan, Roland, and McLean, Gary. Practicing Organization Development: A Guide for Consultants. New York: Pfeiffer Wiley, 1993.

[8] Wilson, Mark, Ed. Information Technology Security Training Requirements: A Role- and Performance-Based Model. National Institute of Standards and Technology, 1998.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE