ISSA The Global Voice of Information Security

A Process Mindset: A Foundation for Information Security

By Juhi Vasisht
Juhi@ARKSolutionsInc.com

The Sarbanes-Oxley Act gives increased visibility and importance to processes that financial organizations need to develop, roll out and institutionalize to avoid future economic and corporate fiascoes. However, most people do not understand process. An organization will save time and money by providing their employees a foundation in process thinking or a process mindset before rolling out what is required for Sarbanes-Oxley, Basel II, HIPAA, etc. compliance.

The word process is generic. There are business, security, legal, audit as well as information technology processes. Within this article I use the term process to refer to all types except where I specifically identify.

Pick up any book on Sarbanes-Oxley and the word "process" appears over and over. For example: "The Sarbanes-Oxley Act of 2002 requires public companies to validate the accuracy and integrity of their financial management. The processes and documentation required for compliance are rigorous and require a commitment from all members of the organization."[1]

Just consider:

- Until recently (and even now sporadically) few universities provide courses in process understanding, development and implementation throughout a business organization.
- The plethora of process "help books" (including "fill-in-the-templates") recently available to assist with process identification and documentation for Sarbanes-Oxley compliance.
- Some organizations have implemented frameworks such as ISO 9000, Software Engineering Institute Capability Maturity Model (CMM), but how many continue to comply with process?
- Instant gratification and "get it done now" mentality widespread in business, which is overly dependent on heroics, resulting in poor planning and rushed execution.
- Overwhelming amount of ongoing problems and rework because processes, procedures, guidelines, and steps are not used to reach a repeatable solution.

Inculcating a process mindset throughout the organization will greatly facilitate information security process development, understanding, and subsequently compliance. Having the right processes will create a control environment where people understand their responsibilities as well as limits to what they can and can't do. The control environment clearly identifies the ways things get done. Competent people know that performing within this environment will facilitate efficient and ethical behavior. Before buying or developing processes needed for compliance, an organization would do well to ensure employees are grounded in the fundamentals of process. To put the cart before the horse will result in lots of re-work and re-training.

What is a Process?

Process is a set of ordered repeatable steps that are executed to accomplish specific tasks. It has specific entry and exit criteria. A process addresses problems and solutions in a structured way including interrelationships and dependencies.

Many fast-money gurus have written books about reaping the benefit of chaos. And, while chaos provides a situation to be creative and develop opportunity and thus, money, it also can lead to total disaster and financial ruin.

Process mitigates risk and protects organizations from unbridled recklessness. It creates a means for organizations to have the necessary checks and balances. It offers a safety net and one that is much needed, if you consider Enron, WorldCom, etc.

What is a Process Mindset?

A process mindset is a systemic way of approaching problems and solutions. It produces any associated artifacts (procedures, standards, guidelines) to address requirements for security, business, legal, audit, information technology, etc.

As an example, let's consider the following illustration using a basic information technology database circumstance.

Problem:

Software Developers cannot access production data per Sarbanes-Oxley. This falls under systems security and the separation of duties, preventing unauthorized access to databases from internal threats.

Situation:

Finance needs to obtain data from a database and a query is used to retrieve the information. In the past, Shawn, a software developer, ran the query, but he is no longer allowed to do this.

Non-process approach

The non-process approach would look for a quick solution - find a non-developer, provide a SQL script (query), and have them execute it.

However, this raises many questions. Which non-developer? Are they qualified? Are they getting the result and information needed? Can they taint or modify the data? Are they skilled to understand the result? Will additional queries be needed that are conditioned on the results of the first?

Process approach

A process approach (using a process mindset) would take a much more synergistic approach, for example:

1. State the problem clearly and concisely.
2. Analyze the problem—when and why does production data need to be accessed in the organization?
3. Identify / brainstorm situations and approaches including who, what, when and why.
4. Document draft process(es) following a standard process template that includes:
    a. Boundaries of the process in a scope statement
    b. Entry criteria or inputs.
    c. Specific tasks performed including responsible role(s).
    d. Exit criteria covering the results from the performance of the tasks on the input.
    e. Verification identifies ways to check on process execution 5.

Once the processes are drafted:

a. Obtain management's written approval
b. Train the organization
c. Facilitate / implement improvement suggestions
d. Monitor and report compliance

Benefits of Process

Processes are key to information security. Process benefits apply directly to information security processes and controls.

1. Process provides repeatability. Once a process is documented, approved and institutionalized, it becomes the way things are done. Documented doesn't always mean paper. There are creative ways to execute—i.e. Voice / Data / Video integration. Not everything has to be typed or written, and new technologies can make it a bit easier and perhaps even enjoyable.
2. Process provides continuity. If someone in the organization wins the lottery and leaves within a week, documented processes enable continuity. New people joining are given a quick start with documentation (including processes) that explains what needs to get done and by whom.

    Think about ensuring information security compliance in the midst of personnel turnover. This is very difficult to do without documented processes and associated artifacts—procedures, standards and guidelines.
3. Processes do not require any not heroics or hiring over-paid experts. They simply mean adopting structured actions for what you know—your business.
4. Once institutionalized, processes are significant time-savers. If all tasks are performed according to a process, the results are likely to be correct the first time. There is no need to fix the end-product over and over and over again. Checks and balances (metrics) need to collect the data supporting productivity gains.
5. Process is improved regularly. A key part of process is process improvement. If a process is being used, those using it will find ways to improve it - an unchanged process is an unused process. To ensure control, process must be improved via Process Improvement.

Importance for Information Security

Sarbanes-Oxley and related legislation puts the focus on control processes and provides an urgent incentive for documenting and complying with them.

An organization trained in process thinking will be more effective in producing, improving and following the required security processes. The most important is, of course, the following. Getting people to follow the process is the most challenging. However, if they understand the importance and benefits of process, the following will be a natural result.

Benefits of a process mindset and resulting processes for information security are apparent. They are:

- ▼ Improved Security via a controlled environment
    - ▲ People understand their responsibilities as well as limits to what they can and can't do
    - ▲ Regulatory compliance is an on-going process—improved along the way
- ▼ Reduced Costs and Savings
    - ▲ Doing things right the first time and avoiding rework
- ▼ Improved Productivity
    - ▲ Repeatability and continuity

Adopting a Process Mindset Requires:

1. **Visible Support from Executive Management**

    If an organization uses a process mindset, the work will go along relatively smoothly and those needing to follow the processes will be more apt to do so. For some organizations, a culture shift will be required. For others (those already using process) something less formal will be required. But with all, visible and regular support must start from the executive levels - CEO, CIO, CSO (Chief Security Officer). All executives need to be visible and vocal supporters of process and controls. This will take time and effort for all in the organization.
2. **Communications**

    Communications to ensure a pervasive process mindset throughout the organization include opportunities for dialog as well as information dissemination. These may include:
    - ▼ Town halls (formal)
    - ▼ Roundtables (informal)
    - ▼ Open door (one on one)

    Of course, good communications are frequent, succinct, and accurate and more importantly, provide a forum for feedback, response, and questions.

    The organization must know that information security is serious business and compliance to processes supporting information security is very important. This compliance needs to be a component of performance reviews and bonus determinants. Frequent visible rewards should also be provided for compliance and suggested improvements. The rewards can be simple, but they need to be regular.

    Other important avenues:
    - ▼ Verify compliance with both peer and independent reviews.
    - ▼ Require middle management to periodically report on compliance using basic metrics.
    - ▼ Avoid any regular exceptions to compliance. This is the hardest but the most important step(s) to take every day. Any regular exception to process or controls starts the ball of twine unwinding immediately.
3. **Measurements and reporting results**

    A huge boost to the following of process and process thinking is an indication that things are getting better. This reinforces the belief in the concept. To obtain this indication, basic metrics on process compliance (and improvements) must be collected. Process rollout and measurements of process compliance and improvement must go hand in hand.

Metrics can actually be a wonderful internal competitive enhancer and add a bit of fun along the way. Once defined and collected, the display, posting, reporting by department (or division) can certainly provide an outlet for creativity and hopefully celebration.

4. **Process Improvement**

In order to ensure rapid, broad acceptance by the organization, it's important to include process improvement. It is this concept that captures feedback for needed clarification, efficiencies, and reduction of errors.

As people use a process, ideas for better ways of accomplishing the tasks will begin to percolate. An improvement process provides a documented way of submitting, evaluating, and either accepting or rejecting the suggested improvements. It is key that an organization have an improvement process and provide real incentives for submitting improvements. For example, the "Process Improvement of the Month" obtains theatre tickets and dinner for two.

Summary

The Sarbanes-Oxley Act and other key regulatory influences provide opportunity for organizations to gain substantial cost reductions, improve productivity, and significantly reduce risk.

Quality and effective processes are critical elements needed to meet these important regulations and compliance areas as well as ensure that organizations have accurate and timely data needed for making key business decisions.

Adopting a process mindset and the resulting processes is straightforward. They ensure a proper foundation is set and eliminates the need to fix the same problem(s) and issue(s) over and over again.

People who understand the value and purpose of focused and effective processes (i.e. have a process mindset) will create a well-run business complete with the required checks and balances. Inherent in these organizations will be a foundation and culture that will be poised to exponentially grow with the improved productivity, quality, and reduced chaos. ■

Juhi Vasisht is a lead information security consultant currently with ARK Solutions, Inc.

[1] The Sarbanes-Oxley Guide for Finance and Information Technology Professionals by Sarbanes Oxley Group; p.13, copyright 2004