WHITE PAPERS

DYONYX

Designing Compliant and Sustainable Security Programs

1 INTRODUCTION

The subject of this White Paper addresses several methods that have been successfully employed by DYONYX to efficiently design, and more importantly can be used to sustain, compliant Security Programs. Security Programs, in the context of this discussion, include the underlying policies, procedures, processes, instructions, controls, metrics, and evidentiary documentation required to comply with the requisite standards and, of course, to secure protected infrastructures and related sensitive information. While cyber security is the predominant focus of most Security Program discussions, physical security is an equally integral component of Security Programs and is applicable to the discussions herein.

DYONYX has a great track record in applying these methods in designing Security Programs to protect critical infrastructures and sensitive documents in nuclear and fossil generation facilities, electric transmission infrastructures, oil storage facilities, public health facilities, federal agencies, and the financial services industry. A number of our comprehensive Security Program designs have received "zero deficiency" audit reports from regulatory agencies.

2 BACKGROUND

Security continues to be an ever increasing critical function in a multitude of industries towards assuring operations are reliable and information is secure. For example, the North American Electric Reliability Corporation (NERC[1]) has been given the authority to develop and enforce mandatory standards (including cyber and physical security) for the reliable operation of the bulk electric systems [2] throughout North America. For nuclear facilities, the Nuclear Regulatory Commission (NRC) will enforce a set of complex new standards[3] to ensure that digital computer and communication systems and networks are adequately protected against cyber-attacks.

In the federal space, the Federal Information Security Management Act (FISMA), through the Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) publications, is triggering the need for comprehensive Security Programs to protect sensitive information and secure information systems. A long list of other

[1] NERC develops and enforces reliability standards; assesses adequacy annually via a 10-year forecast, and summer and winter forecasts; monitors the bulk power system; and educates, trains and certifies industry personnel.
[2] The Bulk Electric System is generally defined as the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, operated at voltages of 100 kV or higher.
[3] In January 2010, the NRC staff issued RG 5.71, "Cyber Security Programs for Nuclear Facilities". This guidance provides an approach that the NRC staff deemed acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber-security attack. Subsequently the Nuclear Energy Institute (NEI) issued a new guideline NEI 08-09 Revision 6 which the NRC has approved for use to comply with the requirements of 10 CFR 73.54."

security standards applicable to health information, financial information, and privacy concerns are also increasingly being applied to every day operations in many organizations. Accordingly, it is more important than ever to design and implement sustainable Security Programs that intrinsically add value and operational resiliency without burdening the impacted organizations.

3 METHODS

The focus of this document is to describe several methods that can be employed to accelerate the design and implementation of a customized and sustainable Security Program. It is important to note that while designing a compliant Security Program is a sizable task, the task of implementing the program can be equally significant, the effort for which is frequently underestimated. In this regard, while some of the methods may appear to be too time consuming, we believe the baseline framework and level of documentation will ultimately prove to be robust, reusable, and essential for implementing and sustaining the Security Program. In addition, the methods described herein can also be employed to evolve and optimize the initial Security Program design in response to implementation issues, changing standards, and configuration modifications of the infrastructures. With this understanding, three specific methods are discussed in the following subsections as follows:

- Application of business process reengineering concepts;
- Utilization of structured logic in constructing self-documenting processes and procedures; and
- Utilization of a functional framework for use in organizing the Security Program architecture.

3.1 BUSINESS PROCESS REENGINEERING

A compliant Security Program contains a number of components as illustrated in Figure 1. Requirements are derived from a variety of security standards as discussed in Section 2.0. Functions provide a framework to organize the Security Program for design, implementation, and sustainment (more about Functions in Section 3.3). Policies define "what / shall" be done in addressing the requirements. Processes, on the other hand, delineate a clear understanding of the "Who, How, When, Where, Why" the work control actions must flow to complete the requirements, ensure the integrity of the Security Program, and document all actions taken. Processes may be supplemented with instructions and detailed procedures. The important evidentiary documentation and metrics are generated from the processes and procedures.

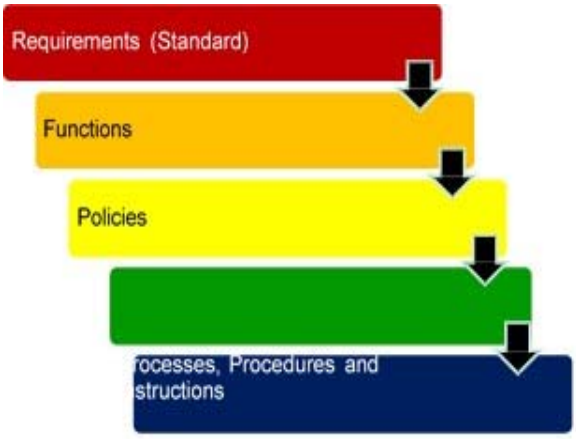

Figure 1 – Security Program Components

In designing a Security Program, the development of the core components, specifically the processes, procedures, and instructions, represents the most time consuming task of the endeavor. Recognizing the complexities of the requirements and the multiple organizations

involved in sustaining a Security Program, we believe industry proven business process re-engineering techniques are especially relevant in designing compliant processes and appropriately incorporating procedures and instructions.

Generically, business process re-engineering techniques were developed years ago by Michael Hammer[4], H. James Harrington[5], and others. Their application is applicable to changing existing processes to incorporate more efficient and effective methods to accomplish the underlying functional objectives. In terms of Security Program upgrades, we believe the same methods can be carried forward to develop processes that are compliant with the new requirements while leveraging existing processes and procedures. In summary, these proven process design oriented techniques are the most effective means for integrating the components of existing Security Programs with the requirements of new standards.

Figure 2 represents a simplified example of a generic business process map associated with a "security incident". The process includes multiple Tasks, Triggers, Decisions, and Results along with the roles and responsibilities[6] for carrying out the processes and making the decisions. The approach is to leverage the use of visual maps in the design of the process. Visual "process maps" can effectively delineate a clear understanding of the "who, where, why, when, and how" the work control actions flow and responsibilities for the same. They also provide a means to:

- Efficiently, through table top discussion sessions, develop customized processes commensurate with the operations and organizational responsibilities of the specific entity;
- Document the specific tasks that need to be completed setting up the requirements for creation of the evidentiary documentation;
- Provide a means to subsequently train users in the processes; and
- Provide a means to effectively document the baseline process for use in evolving or enhancing the process with future operational or requirement changes[7].

In the generation of a process, a representative "trial / strawman" process is first produced for use in discussion sessions with the process owner and relevant subject matter experts, process users, and stakeholders to critique and refine the process. Subsequently, through appropriate table top review sessions, assurance can be provided that the resulting Security Program is compliant and commensurate with current operations.

Utilizing these business process re-engineering techniques, DYONYX has developed a set of generic compliant process templates (including rules and notations), evidentiary documentation, record layouts, and logical process matrices heretofore not available in the

---

[4] Michael Hammer, Reengineering the Corporation, 1993

[5] H. James Harrington, Business Process Improvement, 1991

[6] Roles and responsibilities are visually represented within "Swim Lanes" and may represent a single individual or a group of individuals.

[7] DYONYX maintains process templates and customized processes in a commercially available process mapping tool facilitating the ability to easily modify the process as standards or other requirements change. More than 60 generic functionally organized (See Section 3.3) process maps and 100+ documents have been developed by DYONYX to facilitate the creation of custom Security Programs.

industry. The templates, organized into a functional framework[8], which represent strategic intellectual property for DYONYX, provide our clients with significant advantages in designing, from the ground up, custom Security Programs in an efficient manner.

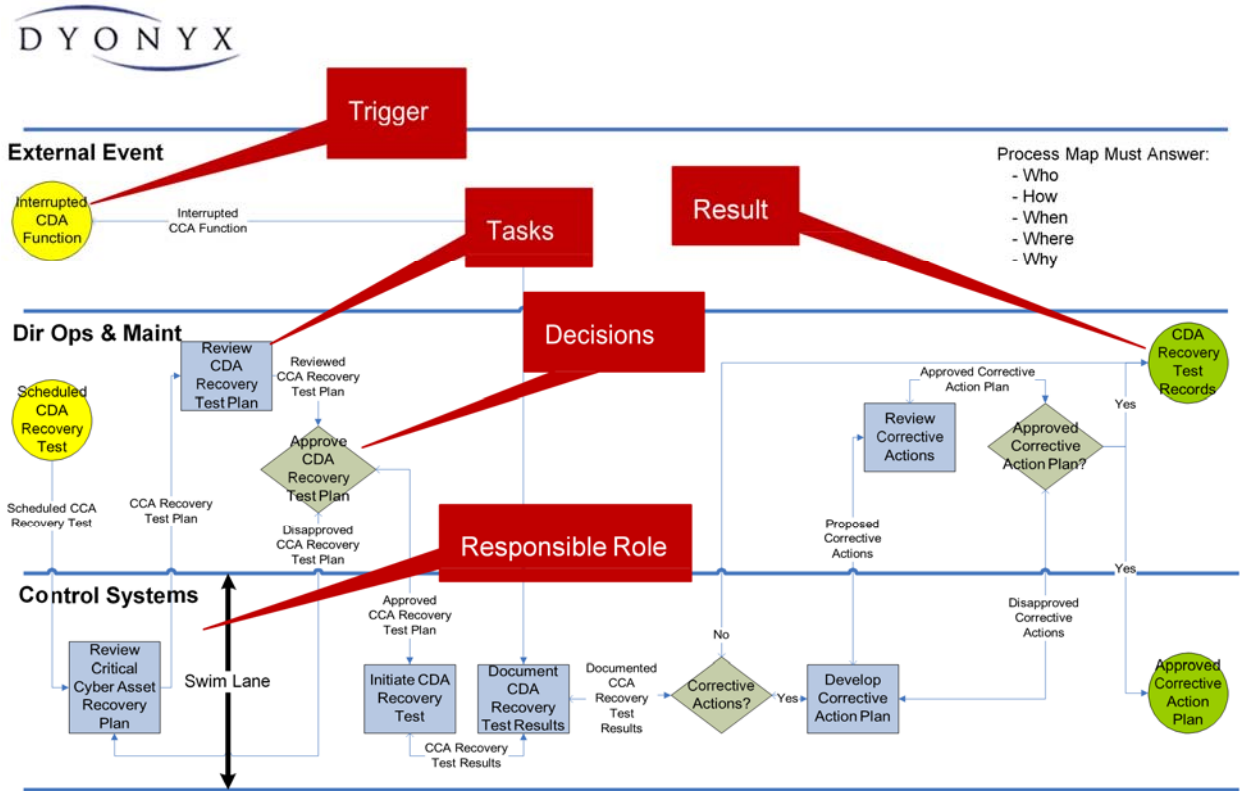

Figure 2 - Customizable Process

3.2 SELF DOCUMENTING PROCESSES

The creation of evidentiary documentation and performance metrics is essential in evaluating the effectiveness of the Security Program, ensuring all relevant processes have indeed been completed, and supporting subsequent audit initiatives. Ideally the evidentiary documentation should be created during, not after, the execution of the processes. DYONYX has created a method whereby each Task within a defined process is documented in a document called the "Traveler". Each time a process similar to the one in Figure 2 is completed, a new "Traveler" document is created. Depending upon the decisions made during the process, different sections of the "Traveler" document will have been completed. Two unique concepts are employed in this methodology:

- Creation of evidentiary documents during the execution of the underlying process ensuring the relevant documents and performance metrics are indeed completed; and
- Where appropriate (especially suitable for complex or critical processes), incorporation of our highly efficient ExPerT[9] methodology to ensure accurate execution and

[8] As discussed in Section 3.3.

[9] "ExPerT" Performance Transfer methodology is a proprietary procedure documentation methodology licensed by DYONYX from CATADR. A detailed White Paper is available that describes this methodology in more detail.

documentation of the process is achieved in an efficient manner.

The "Traveler" document may be a hard copy document or electronic document embedded in an automated work flow implementation of the process depending upon the degree of automation and repeatability nature of the process. In summary, the timely generation and documentation of "Travelers" or other evidentiary documentation is critical to the integrity of the Security Program.

3.3 FUNCTIONAL FRAMEWORK

It is important that a Security Program, including the policies, procedures, instructions, controls, metrics, and evidentiary documentation, be organized in a meaningful and sustainable manner. The organization of requisite standards does not necessarily provide an appropriate structure for the organization of a Security Program. For example, in the design of NERC CIP Reliability Standard (CIP Standard) compliant Security Programs, one might envision that the requirements can be addressed through a straight-forward "standard-by-standard" set of policies, processes, etc. However, a more detailed analysis of the specific requirements of this particular CIP Standard revealed that a complex array of dependencies and interrelationships existed between the forty-three (43) high-level requirements distributed across eight (8) topical areas of the CIP Standard. This irregularity is apparent in many security standards. Organizations and standards have unfortunately been frequently used to frame a Security Program design neither of which offers a stable structure. In the worst case, if the organization changes or the structure of the standard changes (which is forthcoming for the CIP Standard), an inappropriately designed Security Program may require a complete redesign.

In addressing this confusion and mitigating the risks of a redesign effort, DYONYX developed the highly- praised functional framework[10] concept for functionally organizing the Security Program components (policies, processes, plans, programs, procedures, evidentiary records). Functions represent "what" the organization does to accomplish the stated mission, goal and objectives of the underlying entity. As such, unlike organization structures or standards, functions do not frequently change. The functional framework provides the most effective program framework to design, implement, and most importantly sustain the operations of a Security Program. While the initial functional framework (15 functions) was developed for the NERC CIP Reliability Standard compliant Security Programs (see Figure 3), the concepts can be equally applied to other standards, albeit many are more aligned with the functional framework concept. For example, for the more complex nuclear Security Programs, nineteen (19) functions were defined.

[10] Concept was published in Public Utilities Fortnightly, September 2006.

Figure 3 - NERC CIP Reliability Standard Security Program Functional Framework

In summary, we highly recommend that the architecture of a sustainable Security Program needs to be structured around a stable functional framework.

For more information:
DYONYX, LP
solutions@dyonyx.com
1-855-749-6758