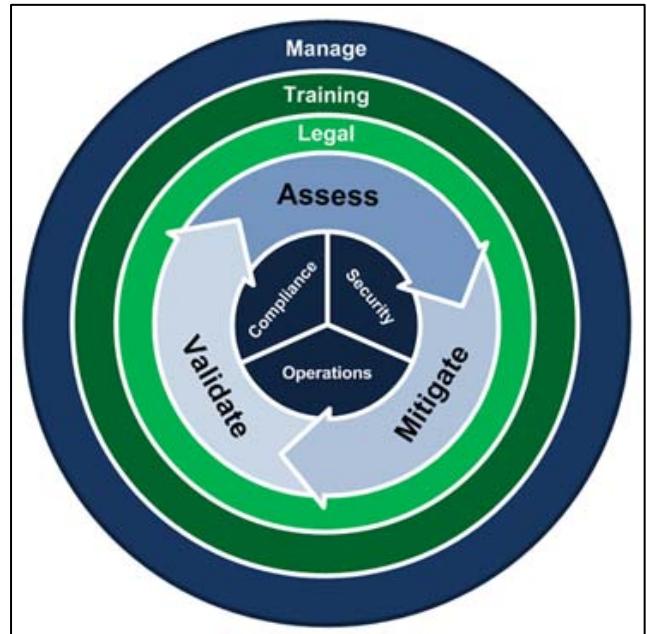




The Holistic Lifecycle Model for Security and Compliance™

The Holistic Lifecycle Model for Security and Compliance™ consists of proven methodologies aimed specifically at Critical Infrastructure and Industrial environments. It is designed to assist operators with maximizing security and achieving regulatory compliance, while minimizing liability from legal action and broad auditor interpretation. The model is a complete and thorough set of processes that go far beyond just the typical SVA (Security Vulnerability Assessment), gap analysis, or self assessment (which are all actually smaller pieces of an entire compliance process). Each phase of the model builds on the other as an integral part of a complete lifecycle, creating a seamless set of security methods and solutions supported by solid due diligence for compliance. The model spans across all aspects of compliance, security and operations by including methods for proper standards/guidelines/best practices selection, security assessments (physical, facility, cyber, and operational), gap analyses, risk analyses, organizational threat modeling, mitigation/remediation strategies and integration, legal support, and management/maintenance programs.



How it works

The following section will address the basic flow for each phase of the model. Much of the technical detail for this section goes beyond the scope of this article and is highly dependent on direct interaction with each individual operator's environment.

Phase 1 - Assessment

Whether you are using a self assessment tool such as CS2SAT, or a 3rd party consultant to perform an SVA or Gap analysis, the goal of an assessment is to identify vulnerabilities and/or gaps in your current environment. An SVA or gap analysis alone, however, will not ensure that your organization is secure or compliant. In fact, if done improperly, they can actually create liability for your organization. Many organizations are not aware that there are many necessary steps to a proper assessment, which are all part of a larger lifecycle that help build solid due diligence. A complete assessment phase consists of the following steps:

1. Standards Identification and Selection – The first step in achieving security and compliance is to initiate an exhaustive search of all the regulatory requirements, industry standards, guidelines, and best practices that may fall within your industry vertical. Even if some of the standards, guidelines and best practices were originally intended for another industry vertical, it is recommended that you review and/or include them in the list of potential requirements to achieve compliance. For example, a petroleum company may fall under CFATS if they transport certain chemicals. This list can then be narrowed down to the hand full of documents that you believe

provides the best set of requirements matching your organizations infrastructure. The idea is that you can show you have performed due diligence in your research and exclusions to achieve compliance, in the event an auditor or attorney doesn't see a specific document referenced. All of these documents must now be put into a matrix, identifying a comprehensive list of categories, cross referenced to the relevant sections in each document.

CATEGORY	DHS BASELINE	PRIORITIZED LIST OF BASELINE STANDARDS, GUIDELINES, AND BEST PRACTICES							CORPORATE INTERNAL	
		1	2	3	4	5	6	7	116	117
		API 1164	CFATS	ISA SP99	NIST 800-82	ISO/IEC 27002	NIST 800-53	DHS CSPL		
SECURITY POLICY	2.1	1.1, 7.1			2	5	2, AT		2	
Information security policy	2.1.1					5.1	AT-1		2.1	
Information security policy document		2.3, 2.6, 7.2				5.1.1				
Review and evaluation of information security policy		B.4.2, B.5.1.5				5.1.2				
VULNERABILITY ASSESSMENT / RISK ANALYSIS	2.16, 2.18		240, 215		4.2.6, 6.1.1		CA, RA			
Asset Identification	2.16.1									
Conducting a risk assessment	2.16.2, 2.18.4	2.1, 5.1.1-2, B.2	250				CA-2, RA-3			8.4
Three layer analysis (holistic)										
Security architecture analysis	2.18.3						RA-2			
Successive compromise analysis										
Quantitative risk analysis										
Qualitative risk analysis										
Risk management process	2.18.6	B.2					3.1			
Mitigation program		5.1.2, B.2.3			4.2.7					
Equipment backup		5.1.2, B.2.3.5, B.3.5.1								3.3
General considerations for conducting a risk and vulnerability assessment	2.18.11	5.1.2, B.2								
ORGANIZATIONAL / OPERATIONAL SECURITY	2.2	B.5			3.3.1, 6.2	6	2.1			
Information security infrastructure		B.5, B.5.1			2.2	6.1	2.2, 2.3			
Management information security forum	2.2.1	B.5.1.5				6.1.1				
Information security coordination (within the organization)	2.9	B.5.1.5				6.1.2				
Allocation of information security responsibilities (for assets and processes including leadership and management.)	2.2.2	B.5.1.5				6.1.3				
Authorization process for new information processing facilities						6.1.4				

2. Policies and Procedures Analysis – Once you have created the regulatory requirements, industry standards and best practices matrix, your organizations internal policies and procedures must be added to ensure compliance with Corporate mandates. A policies and procedures analysis should be performed. Personnel interviews should be added as well for improved accuracy. This will give you a clear picture of how well your current written policies and procedures cover the regulatory requirements, industry standards and best practices contained in the matrix.
3. Critical Asset Identification and Classification – Certain industry verticals such as Electric Utility and Chemical, for example, require identification of critical assets by quantifying certain attributes. This should be done according to the standards for that particular industry vertical, with the understanding that this process may be governed by specific regulations regarding confidentiality and management of information.
4. Security Vulnerability Assessment (Cyber, Physical, and Operational) – The majority of standards, from all industry verticals, prescribe at least some version of a vulnerability assessment (SVA - Security Vulnerability Assessment). These assessments typically focus on cyber elements, leaving gaps in compliance and security. Even if, in your current role, you are only concerned with the cyber aspects of compliance and security, you are still leaving vulnerabilities in your cyber security, as the physical, operational, and human elements can provide an attack vector to your cyber systems. As a result, it is highly recommended that, in addition to your SVA, you also perform additional tests to include a physical SVA and/or a “Red Team” test. These tests will help evaluate all aspects of your cyber, physical, operational, and “human factor” security.

(TECHNICAL NOTE: Only proper, SCADA or process control system (PCS) approved assessment methods should be used to assess these environments. Such methods should only be performed by individuals with extensive experience in assessing and testing SCADA and PCS environments. For example, all tests should be run on a backup system, in a test lab or another form of non-production environment of like systems and configurations. Only very specific *true passive tests* that have been proven safe on non-production systems should be performed on production environments).

(LEGAL NOTE: It is critical how an operator documents and communicates the results of any security vulnerability assessment. Failure to manage the documentation may result in the assessment simply serving as a road map for attorneys or agencies to attack security programs. Such misuse can happen even if such attacks take the necessary self-critical analysis involved out of context and fail to consider that the company based security decisions on a risk matrix that carefully considered probability and consequences to address the most viable and serious threats).

5. Assessment Validation – All analysis and SVA results must be validated. This can be accomplished by a combination of results analysis, penetration testing and interviews. For Cyber assessments, simply running vulnerability assessment tools such as Nessus and reconnaissance tools such as NMap will not achieve a complete and proper vulnerability assessment. In addition to leaving gaps in security, these tools can produce false positives as well as false negatives.

(TECHNICAL NOTE: It is critical that proper SCADA or process control system approved testing methods should be used to test these environments.)

6. Risk Analysis – All of the data that has been gathered thus far in this phase must be analyzed to provide a clear picture of the current levels of security, compliance and risk. Any risk formulas and threat models used, should be specific to your industry and customized for your organization. This can be a complex step, requiring an experienced professional versed in risk analysis formulas and threat modeling.

Phase 2 - Mitigation/Remediation

In this phase, policies and procedures will be revised and enhanced to reflect the current environment. A mitigation strategy will be built, based on the data from the Assessment Phase, with mitigation/remediation solutions identified and put in place. We are often asked, “How do you know that your interpretation of the standards is correct when developing policies and procedures and mitigation/remediation solutions?” What is important to remember here is that the standards, guidelines and best practices are not being interpreted. They are being referenced by specific sections in the matrix. If you can show that you have performed exhaustive due diligence, in an effort to clarify and satisfy any vague requirements of a particular standard, you should have a solid defense in the event of an audit or possible litigation.

Phase 3 - Validation

Validation verifies that implemented remediation and mitigation have been deployed and are being effective at improving security and achieving compliance. This is accomplished by revisiting certain aspects of the Assessment Phase. A complete vulnerability assessment should be re-run, along with any other step from the Assessment Phase, in order to address any key areas of concern. Use this phase to fine tune strategies and solutions as needed. The Validation Phase should also be revisited at least once a year or as prescribed by changes in regulatory, industry and corporate requirements in the particular industry vertical.

Phase 4 - Legal

Many organizations are not aware that simply performing an SVA or other self-critical analysis can actually create liability if the data is not properly handled. It is also very important to remember that improper standards and best practices selection can create liability as well. The following questions must be asked - Has the organization performed the necessary due diligence and covered all angles necessary to prevail should someone take legal action against you as a result of an incident? Is the organization prepared for auditor interpretation that could lead to regulatory fines? The Legal Phase is active throughout the entire Holistic model lifecycle, ensuring no other processes undertaken in good faith to reduce risk have the unintended result of creating liability, both short and long term, for the organization, and that regulatory changes are worked into the model.

Phase 5 - Management

Once remediation and mitigation have been deployed and validated, a long-term program must be put in place to ensure that all processes, procedures, and technical safeguards are monitored, maintained and kept current with emerging threats and changing industry requirements.

Phase 6 - Training

Training is a critical part, if not the most critical part of the Holistic Lifecycle model to achieve security and compliance. All stakeholders must be trained in understanding the strategic approach and tactical implementation of the model or the organization will not achieve the desired outcome. Training is reference in many of the regulatory requirements and industry standards as a critical component of security and compliance. A training program should be developed and implemented, with a strong communication component, to ensure success. All stakeholders should have a clear understanding of roles and responsibilities, communication security and protocol, and document security and transmission protocol.

Contact Information

Jeff Whitney

Berkana Resources Corporation

1616 17th St. Suite 362

Denver, CO 80202

Phone: (303) 293-2193

Fax: (303) 293-3764

Email: jwhitney@berkanaresources.com

Web: www.berkanaresources.com



Berkana Resources Corporation