A COALFIRE PERSPECTIVE

NERC CIP Version 5 – A Practical Plan for Implementation and Compliance

By **Tim Weil**, Senior Consultant and

Bao Le, VP Corporate Development, Coalfire

June 2013

Introduction

IT Governance and information security

NERC CIP(v5) is an international standard related to information security that has become one of the cornerstones of an effective IT governance framework. Organizations use ISO/IEC 27001 when they need to provide outside parties with evidence of their security level of effort or when they have a corporate culture based on total quality and are seeking the information security equivalent. The NERC CIP(v5) standard provides the fundamental aspects of IT governance for the protection of the information – and the ***availability, confidentiality and integrity*** – on which everything else depends.

The NERC CIP Version 5 information security standards

NERC CIP(v5) was preceded by BS7799, which was created in 1995, by the British Standards Institution (BSI). It was a standard to guide the development and implementation of an **Information Security Management System**, commonly known as an ***ISM***. Since the BS 7799 standard was first published in 1995, the set of ISMS standards has evolved significantly, based in part on existing standards, covering areas like terminology, guidelines, metrics, certification and audits

NERC CIP Standard (version 5)	Requirements
CIP-002 – BES Cyber System Categorization	Requires the identification and categorization of BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.
CIP-003 – Security Management Controls	Requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.
CIP-004 – Personnel and Training	Requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.
CIP-005 – Electronic Security Perimeter(s)	Requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.
CIP-006 – Physical Security of BES Cyber Systems	Intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

CIP-007 – Systems Security Management	Requires responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s).
CIP-008 – Incident Reporting and Response Planning	Ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.
CIP-009 – Reovery Plans for BES Cyber Systems	Ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices
CIP-010 – Configuration Change Management & Vulnerability Assessment	Ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices
CIP-011 – Information Protection	Ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices

NERC CIP(v5) Overview

The NERC CIP(v5) Certification is the only globally recognized standard for certification of a broad-based Information Security Management System (ISMS). NERC CIP(v5) is a risk-based approach for documenting an ISMS that balances a framework of defined controls within the context of a business's unique environment. ISO 27002 is leveraged for more detailed information on implementation of those controls. ISO offers great flexibility in that it can be focused on the whole organization, or a narrowly defined scope, such as an application or service. The approach presented in NERC CIP(v5) encourages its users to emphasize the importance of:

- Understanding an organization's information security requirements and the need to establish policy and objectives for information security;
- Implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks;
- Monitoring and reviewing the performance and effectiveness of the ISMS; and
- Continual improvement based on objective measurement.

The Benefits of NERC CIP(v5) Implementation

The ISACA Journal article *'Planning for and Implementing NERC CIP(V5) (ISACA Journal Vol. 4, 2011)"* has the following to say about the NERC CIP(V5) advantages –

What GRC Industry Says About NERC CIP(v5) Compliance

In the information Security industry there is no single standard security architecture model or framework, but two of the best are: ISO/IEC 27001 & 27002 (incorporated in ITIL and COBIT) and NIST Special Publications 800-37/53. These models intersect at both the Information System tier (IT Risk),and the strategic management layer where NERC CIP(V5) is linked to the Tier 1 Risk Management hierarchy described in the publication – *Managing Information Security Risk (SP 800-39)*.

Managing Information Security Risk (NIST SP800-39)
Organization, Mission, and Information System View

In 2011, the Gartner Group report "How to Make the Most of ISO/IEC 27001" also stated these key findings –

- ISO/IEC 27001 is part of a series of international information security standards that's gaining in importance. ***For global organizations, there's no certification alternative to ISO/IEC 27001***.
- According to a Gartner survey, ***29% of respondents said they would support or consider ISO/ IEC 27001/27002 in the IT compliance projects they undertake***.
- Organizations use ISO/IEC 27001 when they need to provide outside parties with evidence of their security level of effort or when they have a corporate culture ***based on total quality,*** and are seeking the information security equivalent. If they merely want to establish an information security management system (ISMS) informally, they usually apply ISO/ IEC 27002.

A Portfolio of Services – Implementing NERC CIP(v5)

In the process of becoming accredited by the ANAB Certification Body (using ISO 17021), the company Coalfire is strictly regulated in the services it can provide (NERC CIP(V5) Certification Audits). The requirements for Impartiality, Confidence and Conflict of Interest prevent COALFIRE from offering additional audit and consultancy services. There is however, an opportunity for independent Coalfire business units to develop audit, assessment and advisory practices. Areas of business opportunity include the following –

NERC CIP(V5) Implementation (and Advisory) – typically this is a 'Big 4' IS practice with long delivery cycles

NERC CIP(v5) Compliance Testing – this practice may involve internal audits of the NERC CIP(V5)/27002 implementation or a readiness' assessment for the certification audit

NERC CIP(v5) Assessment (and Advisory) – Coalfire has been approach on several occasions by clients wanting to establish a 'best practices' information security framework and our CF consultants will provide analysis and recommendations of different GRC frameworks (PCI vs HIPAA vs ISO 27002).

The following section gives a summary description of the COALFIRE NERC CIP(v5) Certification practice (pending ANAB approval).

Implementation Plan

Coalfire . facilitates the ISO certification process from designing the ISMS thru complete certification as an Accredited Registrar. Our services include:

1. ISMS Analysis: Coalfire reviews [CLIENT]'s ISMS through a collaborative Risk Assessment process. This process validates the scope of the ISMS based on company needs and client expectations. The process is comprehensive by ensuring the ISMS includes the appropriate controls.

2. Stage 1 Audit: This audit ensures that your company has selected the proper controls for the scope of the ISMS, and that they are documented sufficiently to achieve the control objectives. A minimum of six months of operating the controls is required prior to the Stage 2 Audit.

3. Stage 2 Audit: This audit validates that the controls are operating effectively, to include monitoring and management oversight. This is a process audit that includes testing, observation, and evidence review at the company locations(s). The decision whether or not to certify a client organization's ISMS taken by the audit team is made on the basis of the information gathered during the certification process and any other relevant information

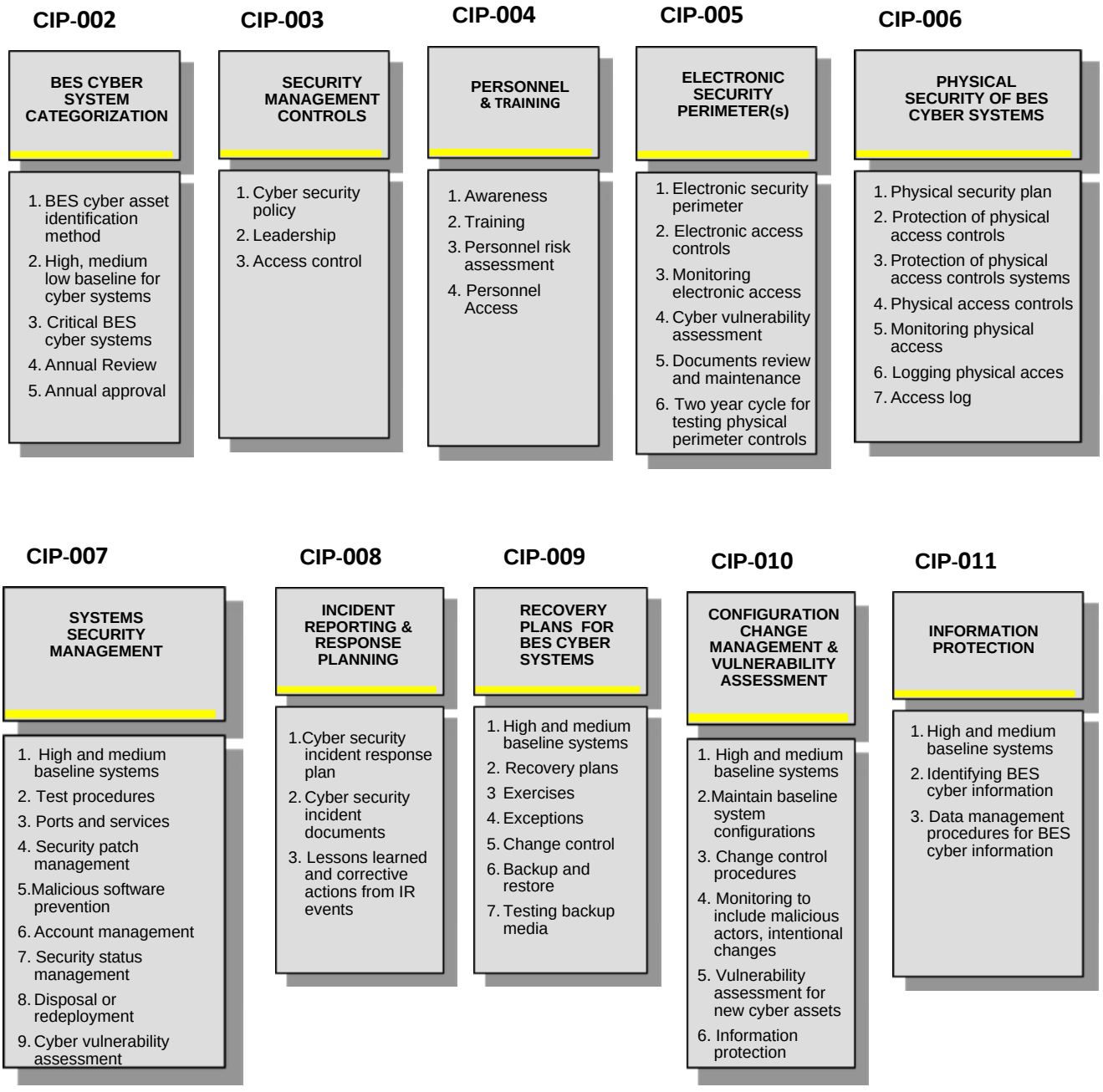
4. Maintenance/Surveillance Audits: Stage 2 audits are required every three years. In off years, Coalfire will conduct annual limited testing and onsite review to ensure controls are being followed according to the ISMS.

This certification audit validates that the ISO controls that are in-scope for the ISMS are operating effectively, to include monitoring and management oversight. This is a process audit that includes testing, observation, and evidence review at the ISMS location.

Through interview, observation and testing, validate that controls are designed and implemented in compliance with the ISMS The NERC CIP(V5) standards includes both ISMS requirements (5 areas) and Security Control objectives and criteria (12 domains).

NERC CIP(v5) Security Control Categories and Requirements

Through interview, observation and testing, validate that controls are designed and implemented in compliance with the ISMS (and the companion ISO 27002 ISMS Code of Practice)



NERC CIP(v5) Advisory Services

Today, Coalfire's solutions are adapted to requirements under emerging data privacy legislation, the PCI DSS, GLBA, FFIEC, HIPAA/HITECH, HITRUST, NERC CIP, Sarbanes-Oxley, FISMA and FedRAMP.

The Coalfire Difference

- Methods
  Coalfire has expertise across all of the major IT security and risk management frameworks and compliance regimes (NERC CIP, NIST, HIPAA, SOX, CoBiT, ISO, FISMA , GLBA, PCI, etc.) and has created our own Common Controls Framework to support efficient cross comparisons. This breadth of experience allows Coalfire to provide an integrated approach. Information and testing that is done to support one set of concerns can also be analyzed and reported for different compliance needs. Controls and recommendations are not viewed in a piecemeal fashion, but integrated to address the broadest concerns. Coalfire examines a security program from policy through procedures, from controls to sustainment; and does so with the understanding that it all has to work seamlessly regardless of the specific regulations by which it may be measured.

- Cost-Effective Services
  Coalfire offers the skills and processes typically provided only by specialized IT security consultants or offered by the large consulting firms, but with the cost sensitivity associated with delivering services to maximize customer value. We understand the constrained environments that many of our clients operate in and we have developed efficient and structured methods supported by technology to produce high-quality results at competitive rates.

Services

- Comprehensive NERC CIP Compliance (versions 3, 4, 5 and beyond)
- Compliance and Security Master Planning
- Compliance and Security Program Development
- Risk Management Assessments and Programs (consistent with DOE guidance)
- Systems Architecture and Design
- Physical Security
- Evidence Management
- Security Training and Awareness
- Compliance Assessments
- Mock Audits
- Vulnerability Assessments
- Incident Response Planning and Support
- Leadership Workshops and Educational Sessions

About the Authors

Tim Weil, Senior Consultant, Coalfire CISSP, CISA, CRISC, PMP, IEEE Senior Member

Bao Le,VP, Business Development, Coalfire , CISM, PE, IEEE Senior Member