Continuous Improvement - CI Foundations

By Sam Ciccone, Principal Reliability Consultant

The Journey to Security, Resiliency and Reliability

"Security is always excessive, until it's not enough." – Robbie Sinclair

Lew's Lighthouse article in this newsletter discusses CIP-012-1, which requires entities to "mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time monitoring data while being transmitted between Control Centers." This article identifies some Continuous Improvement (CI) and Assessment practices that could improve your information and data security relevant to CIP-012-1.

Continuous Improvement for Data Security

The CI article from the May-June Newsletter presented various CI methods, one of which included Plan-Do-Check-Act (PDCA).

To begin, step back and ask yourself "How does CIP-012-1 fit into the bigger picture?" This is a crucial part of the "P" in PDCA. The PDCA method is discussed in the ISO Standard titled "Information Security, Security Techniques and Information Security Management Systems" (ISO/IEC 27001:2005)[1] that forms the basis of requirements for the ISO/IEC 27000 series of information security standards. ISO/IEC 27001:2005 not only presents information security best practices, but also CI guidance, and defines Information Security Management System (ISMS) as "that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security."[2] Figure 1 of the standard illustrates the PDCA cycle in ISMS processes.

CIP-012-1 requirements correlate to "Plan" and "Do" in the cycle, but the cycle doesn't stop there. Figure 1 includes the "C" and "A" to complete the CI process. Not only must you develop and implement a plan (as per CIP-012-1), but you also should "Check" (i.e., monitor and review the process) and "Act" (maintain and improve it). Per ISO/IEC 27001:2005, "Check" is defined as "assess and measure process performance against ISMS policy, objectives and practical experience and report the results to management for review."[4] Here, you can use, assess and measure process performance by RF's maturity model assessment to benchmark your data security system. The "Act" portion is defined as "maintaining and improving the ISMS, and then taking corrective and preventive actions to achieve continual improvement of the ISMS."[5] After your data security system assessment, you can "Act" through incremental improvements that make the most sense from a security and resource availability standpoint.

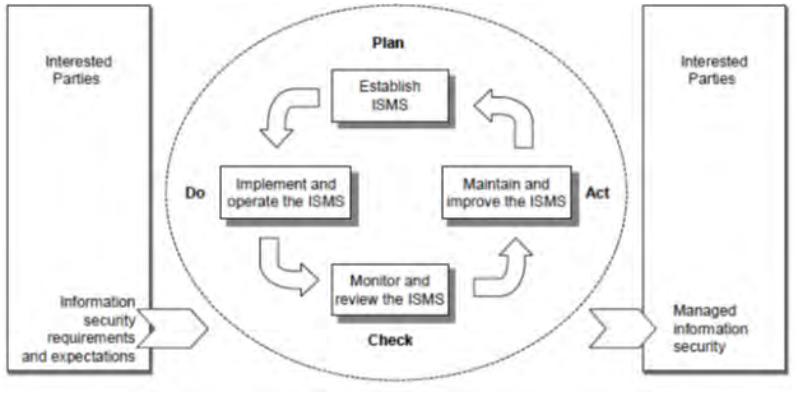

Figure 1 - PDCA model applied to ISMS processes[3]

Assess and Improve with Specific Maturity Domains

What can we do to begin maturing our data security posture?

You can use RF's Information Management maturity domain activities to assess your data security posture. Take the first activity, identification and assessment of information item risk. This includes a risk assessment to determine the relevance and impact of loss, or degradation, of each information item to continued operations. Other important activities involve controlling access to and modification of information.

[1] https://www.iso.org/standard/42103.html. This is the 2005 version of the standard; the 2013 (and latest) version does not prescribe or show PDCA as an example. This was due to ISO/IEC adopting PDCA in their high level Annex SL (now just L) Directive, which ensures consistency and compatibility among the other management system standards such as ISO 9001 Quality Management, ISO 14001 for Environmental Management Systems and ISO 50001 Energy Management Systems. This ensures these standards follow the PDCA and 10 clause format.
[2] IOS/IEC 27001:2005Section 3.7
[3] IOS/IEC 27001:2005 Figure 1
[4] IOS/IEC 27001:2005
[5] IOS/IEC 27001:2005

Continued on page 7

Continuous Improvement - CI Foundations

Continued from page 6

Information Management (INFO)	
Activity	**High Level of Maturity**
Identification and Assessment of Information	A risk assessment is performed that includes a focus on the risks to the BES. Also, information items are identified and risks are formally analyzed as to their potential impact to the BES.
Control Access to Information Items	Access control roles, individual access and logs are regularly reviewed. Logical and physical vulnerability tests are performed on a regular basis to assess that access controls are working. Different levels of the system from application, server, database, network devices, SCADA/EMS/PLC devices, physical access controller systems, and third-party hosted systems are considered.
Control Modification of Information	Information items are tracked and communicated, logs are regularly reviewed, and regular reviews are performed to assess information items.

External Interdependencies (EXID)	
Activity	**High Level of Maturity**
Establish Specifications for External Interdependencies	Documented agreements are in place noting key specifications tailored to each external entity, including incentives for reducing risk. A clearly identified internal manager is assigned to the external entity with clear roles and responsibilities.
Monitor	A key internal liaison provides periodic status, and monitoring of performance is in place (e.g., a measurement or analytics department tracking the performance).
Reduce the Risk of Interdependencies through CI Initiatives	A formal agreement is in place requiring continuous improvement in the identification and mitigation of risks at the external entity. It includes incentives when external entities continuously improve, and there is language encouraging continuous improvement at the external entity.

What can we do to mitigate the risks of relying on external partners for data security and integrity?

CIP-012-1 Requirement R3 Part 1.3 requires "identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers, if the Control Centers are owned or operated by different Responsible Entities."

Therefore, some organizations face additional security risks with data transmission due to their reliance on external organizations, vendors and other third parties. One way to assess and mitigate these external risks is to use the RF External Interdependencies (EXID) domain: see the table below for examples of items assessed under this domain.

What can we do to begin maturing our data availability per future changes to CIP-012-1?

The Order[6] approving CIP-012-1 directed NERC to make modifications to "require protections regarding the availability of communication links and data communicated between control centers." This is an established NERC project: Project 2020-04 Modifications to CIP-012.

In preparation for this change, one of the first things you can do is follow the development of this standard on NERC's website. We encourage you to follow standards development to prepare for your compliance obligations. Further, RF's Information Management maturity domain has activities applicable to the CIP-012-1 directive, specifically ensuring availability, confidentiality and integrity of information. This will help ensure that your information items are managed and protected.

[6]FERC Order 866 Docket No. RM18-20-000; Order No. 866

Continued on page 8

Continuous Improvement - CI Foundations

Continued from page 7

Information Management (INFO)	
Activity	**High Level of Maturity**
Ensuring Availability, Confidentiality and Integrity of Information	Formal controls assessments are performed addressing physical, technical and administrative controls, including a gap analysis to determine additional controls needed.

Conclusion

CIP-012-1 fills an important gap in the CIP standards, requiring protection of operational data transmitted between control centers, and it provides additional opportunities to strive for CI while meeting compliance obligations. To recap:

- Branch out from the NERC standards to the ISO standards, specifically the 27000 standards series, which provide tools for data security success. ISO/IEC 27001:2005 recommends improvements to data/information management including Continual Improvement, Corrective Action and Preventative Action.

- Benchmark the state of your data security and determine improvements through RF assessments. Assessments provide a roadmap to incremental improvement (i.e., improvement that fits your organization's strategic objectives at any given time). You can learn more about the maturity model used for Assessments in RF's Knowledge Center.

- Learn and apply Lew's article material and reference documents provided in his Lighthouse article on CIP-012-1. This arms personnel with knowledge of the standard and may drive ideas for improvement in data security.

For more information on how RF can help you improve your CI efforts, please contact Brian Thiry, Manager, Entity Engagement.