GUIDANCE FOR CREATING INFORMATION SECURITY CONTINUOUS MONITORING PROGRAMS IN NUCLEAR COMPUTER SECURITY REGIMES

D.N. CHRISTENSEN
Pacific Northwest National Laboratory
Richland, USA
Email: drew.christensen@pnnl.gov

S.D. CRAMER
Pacific Northwest National Laboratory
Richland, USA

Abstract

Historically, compliance-oriented computer security programs were built with a 'set it and forget it' mentality when it came to security control implementation in computing environments. Typically, the security control implementation would be revisited on a set multi-year recurring basis (e.g. every three years) where the security program would re-evaluate the effectiveness of the security controls, make necessary security changes for the current operating environment, and seek reaccreditation from the Authorizing Official. This compliance-based approach to computer security is no longer considered an effective means of managing the security of today's computing environments. Compliance-based programs are not adequate to show current system risks and fail to help provide mitigations to combat modern threats.

Computer security standards bodies have encouraged security programs for years to move to ongoing authorizations that do not have a set date for reaccreditation. The continuous accreditation of the system relies on enhanced, near real-time information about the current security health given the organization's understanding of current threats coupled with current mitigations. Moving to an ongoing authorization strategy is dependent on the establishment of an Information Security Continuous Monitoring (ISCM) program. ISCM programs establish key metrics the organization monitors and provides information which helps govern the overall security health of the computing environment. They create threshold triggers which are set to ensure corrective actions are taken if the metric points move outside the desired threshold bounds. In some instances, the metrics provide information which help lead to quick response when real security incidents occur.

Incorporating an ISCM program helps move organizational computer security programs from sluggish, compliance-based programs to agile, risk-based programs that can quickly adjust to the ever-changing threats of today's computing environments. Nuclear regimes can enhance their ability to identify new threats and maintain current mitigations by adopting an ISCM program. ISCM program effectiveness has been vetted through years of use by various industries and when used appropriately by nuclear regimes, it will increase the efficiency with which nuclear security programs operate and provide better security for the industry. This paper provides guidance specific to nuclear regimes on how to implement an ISCM program including relevant key metrics to monitor nuclear security systems which includes monitoring and assessment frequencies. The paper will also advise how the information from the selected metrics can be used to make rapid risk-based security decisions and how to assess your ISCM program to ensure the organization continues to track the relevant data to properly respond to emerging threats.

1. INTRODUCTION

Since the turn of the 21st century, computer security regulatory requirements, guidance, and best practices have become common place for state- and privately-owned organizations who use computer information technology systems. Computer security teams have been stood up to help combat the current cyber threats of the day. To govern these computer security programs an individual is selected, given authority, and held responsible for the program's success or failure. This person is typically responsible for the certification or authorization of a system to operate in its current state.

At the beginning of the century the practice of gaining security authorization or certification to operate a system relied on an assessment of the systems security controls and based on how well the controls met regulatory compliance

requirements. As the authorizing official granted the system owner the authority to operate the system this would typically be granted to for set period. Typically, authorizations lasted about three years but could be shorter or longer based on the authorizing official's preferences. In many scenarios the security control implementation mind set was "set it and forget it" and no one would analyse the effectiveness of the controls during time the system was authorized to operate. At the end of that period another assessment would be performed, and adjustments made to counter the risks that had developed since the previous authorization.

This set it and forget it mentality has proven to be an ineffective approach to computer security program management. The technology arena moves too quickly for this type of approach to be effective. In the past decade we have seen a large shift in the way people use technology. Mobile devices, cloud computing, and the Internet of Things (IoT) has reshaped the way users store, access, and create data. As new technologies are adopted by organizations, they broaden the threat landscape that computer security programs need to be concerned about. They bring along with them new types of vulnerabilities that have not been know or observed before by computer security experts. Many times, shadow IT operations introduce these new technologies without any security consideration.

One broad set of technologies applicable to nuclear facilities are Industrial Control Systems (ICS). These systems historically had been analogue systems which ran on their own separate network, not accessible from any other system making cyber risks very minimal. These systems are converting to digital systems and integrated into organizational CIT networks to make the management and control of them simpler. While this conversion from analogue to digital systems has made it more convenient for facility operators it has greatly broadened the cyber threat landscape of these systems. Many times, this is done without the coordination of the organization's computer security and CIT groups showing why a 'set it and forget it' mentality to computer security control implementation makes it difficult to keep up with new technologies.

In 2011, the United States National Institute of Standards and Technology (NIST) introduced a new approach to managing and authorizing information systems. The approach is called Information Security Continuous Monitoring (ISCM) [1] and it is used in support of an ongoing authorization that does not have a set expiration date, unlike the old accreditation cycle. This new approach allows computer security programs to be more agile and by identifying new threats to the organization quicker and responding faster to fill newly exposed gaps. While it is still used to maintain compliance to the regulatory standards it allows the organization to take a more risk-based approach to the implementation of their security controls rather than a compliance based-approach.

The paper is intended to introduce the concept of ISCM to the broader nuclear industry, provide guidance by giving examples of how to implement an ISCM program, and discuss how it can benefit the industry.

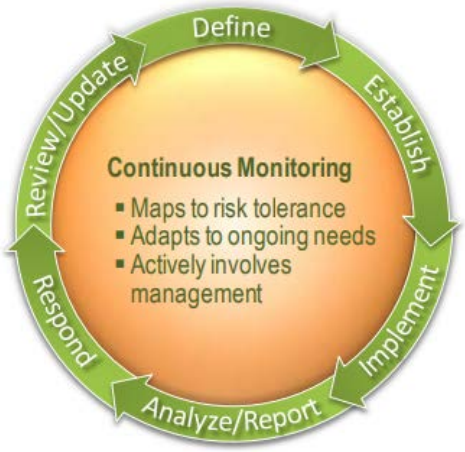

Figure 1. NIST ISCM Process

2. CONTINUOUS MONITORING AS PART OF A RISK MANAGEMENT FRAMEWORK

Information systems are not created as an end in themselves, but to support or enable mission or business functions. The purpose of risk management is to ensure that a computer system is efficiently protected against probable threats, while not being overprotected, thereby degrading the very mission/business functions which the security controls are supposed to support. For security controls to be effective, a computer security risk management program should not only be involved in design of a computer system but should be invoked throughout the lifetime of a system to ensure that it is being properly protected with constant changes to the computer system, mission functions, and threat capabilities.

The following sections provide an overview of basic risk management steps. Although the steps discussed are based heavily on the NIST Risk Management Framework [2][3], an effective continuous monitoring program will add value to any systems development lifecycle or risk management framework.

2.1. Risk Management Steps

2.1.1. *Characterize the System*

Computer system architecture and mission/business functions must be analysed to estimate the probable likelihood and impact resulting from a loss of confidentiality, integrity, or availability of data on the system. This information is then used to develop a security baseline commensurate with the estimated risk.

2.1.2. *Security Control Selection*

Security controls are selected based on requirements to protect information based on mission and system risk, applicable laws, regulations, and internal policies. There are many frameworks and best practices available for security control baseline development [4][5][6].

2.1.3. *Build System and Implement Controls*

The information system is instantiated. Security controls are implemented and documented.

2.1.4. *Continuous Monitoring*

In a static environment with unchanging technologies and threats, deploying the information system and implementing security controls might be the last step. But systems are updated, controls may not have been implemented as planned, pass assumptions may have been incorrect, threats evolve, and missions change. If security controls are not updated as the environment changes, they will not provide adequate protection.

3. INFOMRATION SECURITY CONTINUOUS MONITORING

ISCM means so much more than always having anti-virus software running or having a 24/7 Cyber Security Operations Centre, it means monitoring and tracking all changes in the network, organization, or even adversaries that impact the risk posture of an organization. An ISCM Program should be based on the risk tolerance of the organization, be flexible to organizational needs, and provide actionable information to decision makers.

3.1. Attributes of Successful Continuous Monitoring Program

3.1.1. *Defined Risk Tolerance*

A successful ISCM Program is built upon a clear understanding of organizational risk tolerance. Risk tolerance may be defined per system using a high, medium, low methodology similar to that outlined by NIST [7]. Many control frameworks provide a prioritization or criticality rating for specific security controls that provide insight into risk tolerances per control. Mature IT change management processes rate changes based on their potential impacts to the organization [8]. Organizations often have clear definitions of roles and responsibilities along with what decisions can be made at specific levels. This can form the basis for understanding an organizational risk tolerance. New efforts are being made in quantifying risk tolerance to ensure that organizations are measuring risk consistently and making computer security risks comparable with other organizational risks [9][10]. Understanding the boundaries of risk tolerance guide the development of metrics and delineate thresholds to measure applicable risk factors and act when measured outcomes are outside of desired threshold bounds.

3.1.2. *Monitor Internal and External Risk Factors*

Internal monitoring involves tracking factors that the organization directly controls. Monitoring these risk factors enables the organization to catch issues before they lead to large impacts. Common factors that may lead to a change in risk posture are changes to mission or business functions, computer system configuration, system capabilities, staffing, understanding of a security control effectiveness, policy, or vulnerability management.

Monitoring external risk factors includes performing practical risk intelligence with an emphasis less on attribution of attacks and more on understanding common attack techniques, current vulnerabilities, and attack trends against similar organizations. Response to these external factors should change with the attack trends.

3.1.3. *Meaningful Metrics*

Metrics should be meaningful and drive action. A common metric that is not meaningful and would not drive action is measuring the number of phishing messages blocked at the email gateway or the number of reconnaissance port scans blocked by the border firewall. While these may be interesting to those managing the e-mail gateway or firewall, it does not represent a change in risk posture or require any action. A more interesting metric based on these two examples would be an increasing trend of phishing messages being delivered to and clicked on by staff or a reconnaissance scan that made it through the border firewall to the intranet. Both metrics may indicate the failure of security controls that were believed to be functioning properly.

3.1.4. *Automation*

Automating the collection of continuous monitoring metrics increases the consistency of results, decreases the cost of measuring, increases analytic potential, and ensures that metrics will be measured based on data rather than emotion. It is important to note that not all metrics have the ability to be automated, however an organization should use automation whenever possible to monitor its metrics. Automation metrics are performed in real time and lead to timely notification and action.

3.2. Response and Reporting

All metrics should have predefined thresholds that, when exceeded, lead to specified actions. These actions may involve reporting at various levels of management, or they may specify immediate security response actions. The goal of continuous monitoring is to improve decision making at all levels. This can only be done when relevant, actionable data is quickly delivered to individuals who have the power to act upon it. This data can be delivered in many forms from a fully automated dashboard to regularly generated reports. Continuous Monitoring metrics and reports should be regularly evaluated for their value in driving decisions and action.

4. EXAMPLE METRICS

The following table provides example metrics that may be used to monitor the computer security risk posture of an organization. Thresholds have been loosely defined and should be developed with additional clarity according to organization needs before implementation. Actions should also be modified to fit your organization.

TABLE 1. ISCM METRICS

Category	Metric	Threshold	Action
System Authorization Changes	Systems operate in accordance with documented system security plan.	1. New system needs authorization	1. Inform Authorization Official (AO), develop System Security Plan, and obtain authorization to operate.
		2. Security significant changes to the boundary of a current/approved system	2. Inform AO, assess security controls, develop corrective actions, obtain AO approval.
Configuration Changes	Risk of system configuration changes are understood and approved through Change Management Processes.	1. Increasing trend of security significant changes approved by Change Management Board	1. Conduct risk assessment to understand the impact of changes and determine if additional security controls are necessary.
		2. Increasing trend of changes being made without prior approval of Change Management Board	2. Conduct risk assessment to understand impacts and develop corrective actions.
		3. Critical, High, or Moderate vulnerabilities outside of predetermined remediation timeline	3. Inform AO, conduct root cause analysis, and develop corrective actions.

Data Loss	Data should only be located on approved systems. Data Loss occurs when sensitive information is found on a system not authorized to process it through inadvertent or intentional action.	1. Sensitive data found outside of security boundary	1. Inform AO and data owner, conduct root cause analysis, clean up data, and develop corrective actions.
		2. Significant upward trend in the frequency of information spillage events	2. Conduct root cause analysis, report results to AO, and develop corrective actions.
Risk Tolerance	Cumulative increases to risk are monitored to determine if any additional security action is required.	1. Significant change to mission or business function	1. Conduct risk assessment to understand the impact of changes and inform AO if security significant.
		2. System owner desires to change the security categorization or security baseline	2. Conduct risk assessment, assess security controls, update security plan, & obtain AO approval.
Security Incidents	Monitor the quantity and impact of computer security incidents.	1. Occurrence of significant computer security incident	1. Report per incident response requirements, perform root cause analysis, and develop corrective actions.
		2. Upward trend in minor computer security incidents	2. Perform root cause analysis and develop corrective actions.
Control Efficacy	Controls are assumed to be functioning properly. If they are not, corrective actions are necessary.	1. Significant deficiency in computer security control	1. Conduct root cause analysis, report results to AO, and develop corrective actions.
		2. Upward trend in minor deficiencies in computer security controls	2. Conduct root cause analysis, report results to AO, and develop corrective actions.
Threat Intelligence	Threats are tracked to evaluate current tactics, techniques, and tools being commonly used by threats.	1. Significant change in the intent, capability, or attack methods for threat actors	1. Evaluate environment for exposed weaknesses, determine likelihood of attack, develop corrective actions, report results to AO.

5. APPLICABILITY TO NUCLEAR REGIMES

As we broach the idea of implementing an ISCM in a nuclear regime, let us consider the Graded Approach to Computer Security in section 5.5 of the IAEA Nuclear Security Series No. 17, titled “Computer Security at Nuclear Facilities” [11]. In this section the guide introduces the concept of segmenting nuclear facility computing environments into levels and zones. The example given in that section shows five security levels, Level 1 being the most critical and encompasses the most vital systems to the facility, up to Level 5 being the least critical of systems. A simple example of this architectural stratification is provided by the United States Department of Homeland

Security's Industrial Control System – Computer Emergency Response Team (ICS-CERT) in Fig. 2 below. Zones are further segmentations within each level to group computer systems where they have similar safety or security needs as well as similar administrative and operational needs.

It is imperative that we protect our most vital systems. The best way to accomplish this is not by only putting protections around the security level they reside in. A defence-in-depth approach is the best method to protect our assets. Implementing security at every security level creates barriers between the attacker and the vital components of organizational systems. Each barrier becomes an obstacle an attacker must overcome to get to the most critical assets.

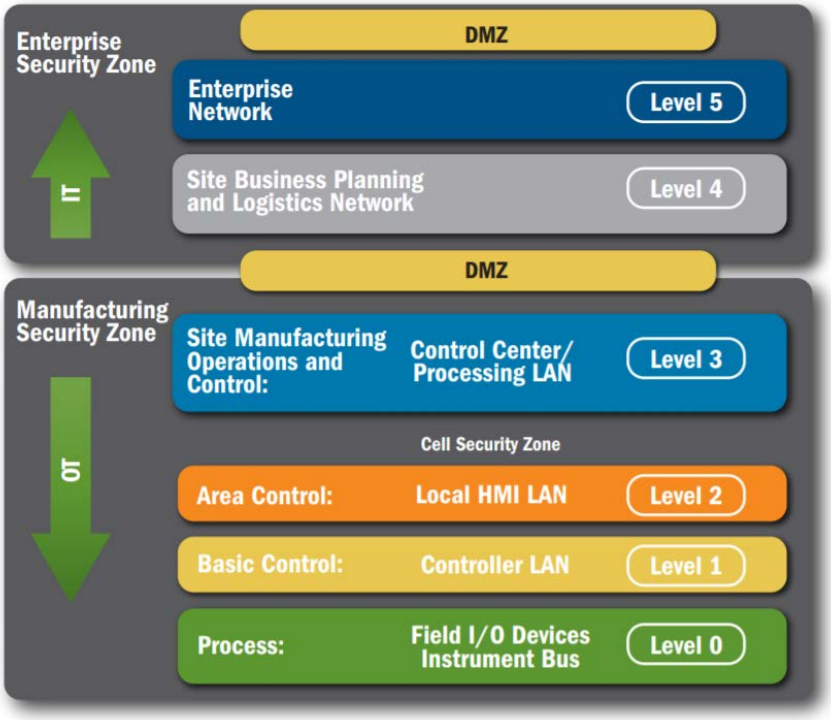

Figure 2. Security Levels and Zones Example [12]

When taking this recommended architectural model into consideration the ISCM approach can be applied by determining what metrics in each level would be important for the organization to track and monitor to determine the cyber health of that level. Metrics may need to be determined for each zone in the architectural breakdown because they may have additional security considerations beyond those of the security level they reside in.

In Level 5 you may be more concerned with the number of known vulnerabilities found within this level because this is the level that is most likely to be exploited by attackers because it has direct communication with systems on the internet. The use of network vulnerability scanner data or application security testing data, which shows common weaknesses in web applications, may be important metrics to monitor. The increase of these vulnerabilities or weaknesses could indicate your system patching activities are not keeping up with organizational policies and the organization is becoming more susceptible to an attack. This metric provides timely and actionable results that lead to direct action to close security gaps in a cyber program.

In Level 1 you may be concerned with the integrity of the dataflow on the network. Level 1 systems data patterns tend to be very consistent, unlike traffic patterns in the higher levels. This consistency can make it easier to monitor if something has changed. Monitoring for anomalous traffic could be an indication that traffic patterns have

changed, which could be a malicious act by a nefarious actor. These triggers can lead to quick investigations and stop an attack as it is happening.

An organization may determine some metrics need to be tracked across the whole organization without exception. A metric like performing self-assessment activities may be an example that could be applied across all levels and zones. Self-assessment activities are important to understand how well the organization is implementing required security controls. If the organization fails to perform these self-assessment activities the security control implementation could degrade over time through attrition of staff and lack of visibility. This could lead to the deterioration of the organization's computer security posture and to organizational managements false sense of security.

In most cases the different levels' and zones' security goals and needs will vary. The methods to track and monitor the cyber health of these levels and zones will be different as well. Nuclear organizations should carefully consider each level and zone to determine what metrics it should track and monitor. As security controls are implemented and metrics are monitored it creates the needed defence-in-depth strategy to protect the most vital assets to the organization.

6. CONCLUSION

New technologies will continue to be developed and incorporated into nuclear regime technology stacks. This will undoubtably introduce new threat vectors to our nuclear computing systems. The best way today to keep abreast of the ever-changing environment is to incorporate ISCM into computer security programs. With key metrics to monitor the cyber health of the computing environment as well as the health of the governance of security controls the organization will have more data to show they are meeting their security needs and more confidence their systems are secure.

ISCM programs have been vetted in numerous industries over the past decade and have proven to be effective tools in reducing the risk of the organization. When properly implemented in nuclear facilities the organization will be more aware of shifts in the computer security status; respond quicker to address identified security gaps, preventing the adversaries from exploiting them; better prioritize when to address security concerns; and take a risk-based approach when implementing security controls across the organization. ISCM enables an agile computer security program that is up to date on its current security posture and can show from day to day that it is meeting its compliance requirements. ISCM ends the need for obsolete periodic security compliance reviews, and it leads to the establishment of an ongoing authorization. The authorizing official can be confident that the system is compliant and protect against ever changing computer security threats.

REFERENCES

[1] National Institute of Standards and Technology (NIST) Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal information Systems and Organizations, Gaithersburg, MD (2011).
[2] NIST, Risk Management Framework Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST Special Publication 800-37 Revision 2, NIST, Gaithersburg, MD (2018).
[3] NIST, Managing Information Security Risk: Organization, Mission, and Information System View, NIST Special Publication 800-39, NIST, Gaithersburg, MD (2011).
[4] ISO, Information Technology Security Techniques: Code of Practice for Information Security Controls, ISO/IEC 27002:2013, International Organization for Standardization, Geneva, Switzerland (2013).

[5] NIST, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 4, NIST, Gaithersburg, MD (2013).
[6] CIS, CIS Controls (2019), Center for Internet Security, https:/www.cisecurity.org
[7] NIST, Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publication 199, NIST, Gaithersburg, MD (2004).
[8] NIST, Guide for Security-Focused Configuration Management of Information Systems, NIST Special Publication 800-128, NIST, Gaithersburg, MD (2011).
[9] Freund, J., Jones, J., Measuring and Managing Information Risk: A FAIR Approach, Butterworth-Heinemann, Waltham, MA (2015).
[10] Josey, A., The Open FAIR Body of Knowledge: A Taxonomy and Method for Risk Analysis, The Open Group Security Series, Van Haren, Berkshire, United Kingdom (2014).
[11] IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities, Vienna, Austria, (2011).
[12] Recommended Practice: Improving Industrial Control System Cybersecurity with Defence-in-Depth Strategies, DHS ICS-CERT (2016).