Assessing Information Security Continuous Monitoring in the Federal Government

Tina AlSadhan and Joon Park
Syracuse University, Information School (iSchool), USA
talsadha@syr.edu
jspark@syr.edu

Abstract: To confront the relentless and increasingly sophisticated cyber assaults from cybercriminals, nation-state actors, and other adversaries, the U.S. Federal Government must have mechanisms to reduce or eliminate compromise and debilitating consequences. Information Security Continuous Monitoring (ISCM) leverages technology to rapidly detect, analyze, and prioritize vulnerabilities and threats and deliver a data-driven, risk-based approach to cybersecurity. Although monitoring information system security became a requirement for government agencies over 20 years ago and billions of dollars are being spent annually for cybersecurity, ISCM remains at a low maturity level across the Federal Government. This research framework presented is part of ongoing doctoral research. The research seeks to identify the challenges achieving an effective ISCM program and inform measures needed to optimize ISCM. The research involves conducting an ISCM Program Assessment in a Department of Defense (DoD) organization using the recently published National Institute of Standards and Technology (NIST) ISCM Assessment (ISCMA) methodology and the companion assessment tool ISCMAx. An ISCM doctrine placement is presented, derived from the NIST ISCM assessment elements, to more clearly articulate and visualize the doctrine of a well-designed and well-implemented ISCM program. This research will also contribute to the knowledge base for assessing ISCM in the Federal government and the functionality of the ISCMAx tool.

Keywords: cybersecurity, continuous monitoring, security assessment

1. Introduction

In an age of frequent and persistent attacks riddled with determined adversaries, cyber defenses must be agile and responsive to explosive rates of new vulnerabilities, persistent threats, determined enemies, as well as the dynamic state of technologies and mission/business functions (Joint Task Force Transformation Initiative, 2011). Defenders must have timely information available to address the cyber situation before attackers do. An incomplete, inaccurate, or delayed representation of the current security state may contribute to a compromise, increased debilitating effects, and delayed responses (Center for Internet Security (CIS), 2021). As the government's attack surface continues to profoundly expand, it is becoming even more apparent that timely, relevant, and accurate cybersecurity data is vital to deliver effective and efficient cyber defenses.

The Federal Information Security Act (FISMA) of 2002 required continuous monitoring and assessing security controls at a frequency commensurate with risk to implement leaner, more responsive, and more effective information security practices (FISMA, 2002). Federal agencies are mandated to incorporate automation to enable risk-based decisions, transitioning from compliance-based to real-time situational awareness and response (Dempsey et al, 2011; Office of Management and Budget (OMB), 2011). FISMA of 2014 emphasized continuous monitoring and securing information systems commensurate with risk (FISMA, 2014). As required by the FISMA of 2014, Circular A-130 was updated emphasizing the use of risk-based cost-effective security controls and a shift from compliance-based security to continuous-risk-based programs (OMB, 2016).

Although security controls and their assessment and monitoring can be manual, semi-automated, or automated, ISCM leverages technology for greater efficiencies and enhanced cyber operations. Technology can enable continuous monitoring by collecting, aggregating, correlating, analyzing, and reporting of volumes of disparate security data in ways not manually feasible (Dempsey et al, 2011). Technology can augment security processes conducted by cyber professionals, reduce the efforts on redundant tasks, recognize patterns and relationships that may not be apparent, and free up time to work on efforts requiring the human analyst (Dempsey et al, 2011).

An effective ISCM program maintains a picture of an organization's security posture, presents security-related data, and incorporates results to portray greater situational awareness (Mell et al, 2012; Dempsey et al, 2020). Through constant observation and analysis, ISCM provides visibility into assets, awareness of vulnerabilities and threats, and improves overall cyber situational awareness. These capabilities enable organizations to transition

from compliance-driven security to data-driven risk management, enabling the prioritization of efforts to focus on what can most improve the security posture.

There are notable efforts in the Federal Government to implement ISCM per directives and NIST guidance. Cybersecurity and Infrastructure Security Agency's (CISA's) flagship ISCM program *Continuous Diagnostics and Mitigation* (CDM) is a comprehensive program providing access to a set of cybersecurity continuous monitoring tools, integration services, and dashboards to Federal civilian agencies (the *.gov domain), as well as state, local, and tribal governments. The program, initially launched in 2013, is estimated to be a $10.9 billion program by 2031 (Government Accountability Office (GAO), 2020a; CISA, 2021). CDM is intended to help government agencies reduce security threats, increase cybersecurity posture, improve response capabilities and streamline FISMA reporting requirements (OMB, 2021a).

Although there are new requirements to influence adoption of CDM program (OMB, 2020), it is not essential to participate in CDM to have an ISCM program. The Department of Defense (DoD), for instance, does not participate in the CDM program, however, deploys a multitude of tools and technologies that can be leveraged for ISCM data-driven risk-based decision making. Any organization, whether public or private, can implement ISCM mechanisms per the NIST or other Continuous Monitoring framework.

2. Research problem

Although monitoring information system security became a requirement for government agencies over 20 years ago and billions of dollars are being spent annually for cybersecurity, ISCM remains at a low maturity level across the Federal Government (OMB, 2020). In 2019 and 2020, the average score of 23 of the largest Federal agencies for the "Detect" capability, corresponding to ISCM, was 2.56 and 2.78 out of 5, respectively (OMB, 2020; OMB, 2021b). In Fiscal Year 2020, only 5 of these agencies met or exceeded Level 4: Managed and Measurable, what is considered an effective level of security (CISA, 2020a; OMB, 2021b). Many government agencies still lack the capabilities to effectively collect, aggregate, correlate, and analyze security-related information to enhance real-time threat detection and response and data-driven risk-based decision making (GAO, 2020a; GAO, 2020b). Multiple agencies have not yet implemented the vital practices for cybersecurity risk management, including establishing a cyber risk management strategy and policies for assessing, responding to, and monitoring cyber risks (GAO, 2019).

According to a GAO study, although federal agencies were using the CDM vulnerability scanning tools to identify vulnerabilities, there was insufficient visibility of the remediation of identified vulnerabilities (GAO, 2020a). The agency dashboards were not utilized as intended to provide agency level awareness of hardware and software configurations and vulnerabilities for security-related decisions. The hardware inventory capability, an essential component, was not fully implemented. The feature to compare configuration settings against both an agency-approved baseline and the federal baseline was not functional. Due to the shortfalls in achieving fully operational CDM capabilities, the CDM agency dashboard data was inaccurate leading to an inaccurate federal dashboard. The study concluded that the billion-dollar CDM program would likely not fully achieve expected benefits without CISA further assisting agencies with implementation (GAO, 2020a).

There is concern that the government cybersecurity capabilities are insufficient to respond to the increasingly sophisticated and egregious attacks. Russian nation-state hackers compromised the supply chain of a widely used network traffic monitoring and management platform *SolarWinds* to exploit networks in at least nine government agencies (CISA, 2020b; The White House, 2021; GAO, 2021). Despite the extensive cyber measures available to these agencies, to include participation in CISA's CDM program, neither the vulnerability nor the anomalous activity was detected by the government. "…the fact remains that despite significant investments in cyber defenses, the federal government did not initially detect this cyberattack," (U.S. Senate Committee on Homeland Security & Governmental Affairs, 2021). More robust ISCM capabilities are needed to understand what the security posture is, reduce the attack surface, and get in front of the threat and adversary.

3. Research design

This research is designed to identify the ISCM elements that need to be improved and recommendations to optimize ISCM. Utilizing the recently published NIST ISCM Assessment (ISCMA) methodology and the accompanying ISCMAx tool, the researcher will conduct an ISCM program assessment within a DoD organization,

hereafter referred to as ORG. The research will also provide insight into using the NIST ISCMA methodology, the assessment elements, and the ISCMAx tool.

3.1 ISCM program assessment instrument

The NIST ISCMA methodology provides an operational approach to assess "ISCM strategies, policies, procedures, implementations, operational procedures, analytical processes, specific reporting, presentation results, risk assessment and risk scoring, risk response, and the program improvement process" (Dempsey et al, 2020, p. iv). NIST has identified 128 ISCM program assessment elements which are foundational statements reflective of a well-designed and well-implemented ISCM program. The NIST assessment elements are drawn from authoritative documents such as FISMA, those from OMB and NIST, and also incorporate the knowledge of ISCM experts. Each assessment element includes the evaluation criteria supporting the determination statement, i.e., "Determine if…" or "There is…", which is an ISCM principle or element that an ISCM program should meet. The element's assessment procedure includes a stated objective, potential assessment methods, and objects (evidence) to facilitate the judgment of the element. The assessment elements will be judged as either *Satisfied* or *Other Than Satisfied*. Each element references its authoritative source(s). An assessment element example is shown in Figure 1.

ID	Assessment Element Text	Level	Source	Assessment Procedure	Discussion	Rationale for Level	Parent	Critical Element in NISTIR 8212 / ISCMAx Tool	Chain Label	Chain Sort
1-002	There is an ISCM program derived from the organization-wide ISCM strategy.	Level 1	NIST SP 800-137	**ASSESSMENT OBJECTIVE** Determine if there is an ISCM program derived from the organization-wide ISCM strategy. **POTENTIAL ASSESSMENT METHODS AND OBJECTS** **Examine:** Organization-wide ISCM strategy, ISCM policy and procedure documentation, ISCM design documents, ISCM concept of operations (CONOPS) **Interview:** Level 1: SAISO, ISCM point of contact (POC)	The ISCM program is comprised of the ISCM policies and procedures derived from the organization-wide ISCM strategy and includes the ISCM documents that guide ISCM implementation (e.g., ISCM technical architecture and ISCM CONOPS).	Level 1 is responsible for defining the ISCM program.	*The Define Step has no parent element*	N	ISCM Program Management	03.01-002

Figure 1: Assessment element example (Dempsey et al, 2020)

NIST links together related assessment elements into traceability chains to depict the parent/child relationship between elements. Figure 2 is the traceability chain related to Control Assessment Rigor, with the parent element being 1-003 and 3 different chains, the first linking elements 2-003 and 3-002, the second linking element 2-003a, and the third linking 2-004, 2-004a, and 3-035.

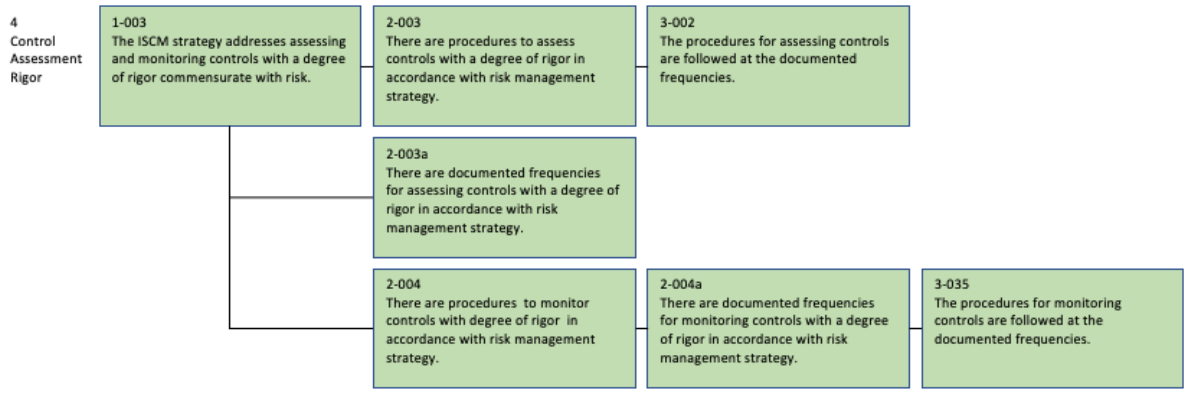

Figure 2: Control Assessment Rigor traceability chain (Dempsey et al, 2020)

The ISCMAx tool will be leveraged to record element judgments, capture annotations, aggregate results from assessment participants, and facilitate data analysis using its scorecard and graphical output (Dempsey et al, 2021). The ISCMAx tool is a ready-to-use Microsoft Excel application containing the 128 ISCMA program assessment elements. It is a companion tool to NISTIR 8212 *ISCMA: An Information Security Continuous Monitoring Program Assessment*. Within the tool, the user can view the element and the guidance, record

judgments, and enter notes and recommendations (Dempsey et al, 2021). In addition, the ISCMAx tool combines judgments, calculates scores, and generates a workbook with the complete assessment results (Dempsey et al, 2021).

3.2 Action research

The ISCM program assessment will be conducted as an action research project, a collaboration between the researcher and ORG. The purest form of action research is one that "participants of a social system are involved in a data collection process about themselves and utilize the data that they have generated to review the facts about themselves in order to take some form of remediation or developmental action" (Lippet, 1979, as cited in Coghlan and Brannick, 2014, p. 47). The organization members have the knowledge of the problems and will live with changes made; therefore, it is important that they be part of the effort (Shani and Pasmore, 1985).

Coghlan and Brannick's (2014) action research cycle: Initial pre-steps and the steps of a) *constructing*, b) *planning action*, c) *taking action*, and d) *evaluating action*, and the corresponding ISCM program assessment actions that will be conducted as part of this research are identified in Table 1.

Table 1: ISCM assessment action research cycle

Cycle	**Steps**		
Pre-Step Constructing	ISCM assessment schedule, identify SMEs to participate, concurrence to conduct ISCM assessment in ORG in conjunction with academic research		
Cycle	*Planning Action*	*Taking Action*	*Evaluating Action*
ISCM Assessment	Design research and ISCM program assessment plan, information/kick off meetings with SMEs and leadership	Artifact review (strategy, policies, processes, plans, reports, former assessment results, etc.), discussions with SMEs, analyze information, element judgement, clarifying notes	Report the findings and recommendations, identify ISCM elements needing improvement and what is needed to optimize ISCM

3.3 Subject organization and participants

ORG is one of several Federal Government organizations facing challenges to achieve the objectives of ISCM and transition to ongoing/continuous assessment and authorization of its information systems. ORG serves as a Cyber Security Services Provider and is responsible for executing the full range of cybersecurity services for its Enterprise information systems. ORG leverages multiple technology solutions to deliver cybersecurity services. ORG has made significant efforts to ensure ORG's information systems are always prepared to pass cybersecurity inspections by increasing compliance audits followed by the remediation of deficiencies. Although extensive resources dedicated to cyber defenses and robust enterprise security automation tools are deployed in the environment, ORG is reliant on labor-intensive processes to gain visibility of the security posture and lacks near real-time situational awareness to inform the most appropriate cyber defenses needed to protect the assets at any given point of time.

ORG's government civilian cybersecurity and IT professionals, hereafter referred to as Subject Matter Experts (SMEs), from focal areas such as Cybersecurity Governance, Assessment and Authorization, Cyber Audit, Change Management, Defensive Cyber Operations, Cyber Compliance, and Cyber Threat Intelligence, will participate in this research.

3.4 Data collection

Data collection activities are performed in the *Taking Action* research step, see Table 1. ORG's artifacts relevant to ISCM program assessment elements will be reviewed, to include cybersecurity policies, procedures, and inspection findings. Artifacts which NIST identifies element "potential assessment objects", such as the ISCM strategy, ISCM policy, system security plans, security-related data from monitoring systems, reports, and briefings will support element judgments (Dempsey et al, 2020, p. 37-38). Based on the review of supporting artifacts, or absence thereof, initial judgments, recommendations, and notes will be recorded by the researcher in the ISCMAx tool.

The ISCM program assessment elements, inclusive of the preliminary judgments, recommendations, and notes compiled from the artifact review will be provided to the SMEs by focal areas via email. The SMEs will be requested to review the data in advance of an online meeting. Updates and/or corrections can be submitted to the researcher via email. The researcher will facilitate discussions with the SME(s) to reach a consensus as to whether the element is *Satisfied* or *Other Than Satisfied*. The discussions will provide knowledge into the lived experiences and perspectives in actual practice that may not be apparent through a review of artifacts alone. If the assessment element includes discussion points, they may be used to clarify the wording or the intent of the assessment element. The discussions will be grouped into element reviews by traceability chains or sections to facilitate the flow of the assessment, the focus of the SMEs, and the linkage between the elements when discussing and preparing evidence. The judgment and relevant insight from discussions with SMEs will be captured as annotations or recommendations in the ISCMAx tool. These notes may identify shortfalls, indicate what further actions would satisfy the determination statement, and contain other information that may be helpful to the development of ISCM program recommendations.

3.5 Data analysis

The ISCMAx tool facilitates data analysis through a detailed scorecard and other visualizations to summarize the assessment (Dempsey et al, 2020, p. 28). The ISCMAx tool scores the elements and aggregates scores for all assessed risk levels and elements. The ISCMAx tool can display the *Other Than Satisfied* judgments in a single worksheet, identifying the weakest areas of the program. The annotations and recommendations captured during the data collection will be particularly helpful to provide additional clarification of what the challenges are faced in regards to the element and/or what is necessary to satisfy the element and to improve ISCM in ORG.

The ISCM Process Steps Scores for ORG are depicted in Figure 3. ORG's scores for the Define, Establish, and Implement steps are all below 15%. These three process steps comprise 77% of the assessment elements. These scores reflect ORG's current state of being in the initial stages of its program. ORG does not yet have a Risk Management strategy or an ISCM strategy. Key foundational governance for security controls, security monitoring tools, security status-monitoring, ISCM data, ISCM technical architecture, and others have yet to be established. ORG scored 37.5% and 45.5%, respectively in the *Analyze/Report* and *Respond* ISCM process steps. These scores reflect ORG's robust security investment and acquisitions processes and cyber threat program. The scores reflect shortfalls in analyzing effectiveness risk responses and security controls, reviewing ISCM metrics and findings, and having ISCM training and resource plans that align to ISCM objectives.

	Define	Establish	Implement	Analyze / Report	Respond	Review / Update	Totals
Elements	24	43	32	10	9	10	128
Raw Score	4.0	9.0	5.0	6.0	5.0	0.0	29.0
Max Score	42.0	65.0	48.0	16.0	11.0	14.0	196.0
Percentage Score	9.5%	13.8%	10.4%	37.5%	45.5%	0.0%	14.8%

Figure 3: ISCM process step scores

The scored Traceability Chains will provide a graphical representation of the related elements, such as Security Status Monitoring, Security Monitoring Tools, ISCM metrics, etc., further identifying the challenge areas, see Figure 4. The Scored Traceability Chain provides the score for each Level assessed in the square; Level 1 – the Organization, Level 2 – the Mission/Business and Level 3 – the System, and then an overall score for the Element. If an assessment element is not applicable to a level, it will be appear as ⦸. *Satisfied* elements will appear as a "1" and *Other than Satisfied* elements will appear as "2" for each level. If the aggregate score for an element is *Satisfied*, it will appear in Green and if *Other Than Satisfied*, it will appear in Red.

Figure 4: Scored traceability chain example

For the Security-Focused Configuration Management chain, ORG lacks a Configuration Management policy. ORG does, however, have documented procedures to establish organizational security-configuration baselines, identify the risk of the deviations from the DoD baseline, and an organizational process to accept the risk of deviations. ORG's Cyber Readiness initiative includes auditing Technology implementations against the DoD security-configuration baselines prescribed in the Defense Information Systems Agency (DISA) Standard Technical Implementation Guides (STIGs) and the approved organizational baselines. ORG is in the process of defining and documenting the frequency to conduct security configuration audits and defining the sample size for each review. Although Security Content Automation Protocol (SCAP) enabled tools do facilitate automated checks of some security configurations, several technologies require manual checks that are time consuming to conduct. ORG utilizes findings from security-configuration baseline checks as input to project its score based on the Command Cyber Readiness Inspection (CCRI) criteria, which is an indicator of its security posture.

3.6 Scope and limitations

The research focus is on ISCM concepts, governance, structure, and requirements levied by FISMA and OMB rather than the evaluation of ISCM technologies or security controls. The research does not delve into specific vendor technologies or solution sets, assessing security data, assessing actual security controls, or examining control assessments. The research is not an audit of compliance with policy or information security controls, or a risk assessment.

The ISCM program assessment will be conducted in a single DoD organization as a self-assessment facilitated by the researcher. Assessment results are dependent on element scoring of the organization, its mission/business, and systems and are unique to the organization. The ISCM program assessment process, rather that the scoring of the subject organization, will most contribute to the community.

4. Expected outcomes

It is expected that ORG's ISCM program assessment score will be low. Although ORG is performing the full spectrum of cybersecurity services, it is only in the initial stages of implementing as ISCM program. Furthermore, nearly 20% of the ISCM assessment elements are dependent on an organization-wide ISCM strategy and Risk Management strategy. Organizations assessed under the ISCM assessment elements will not satisfy 20% of the ISCM elements without these foundational ISCM governance documents in place. Even if the organization has developed other areas of their ISCM program, scoring will be impacted without this governance.

It is expected that SME's participating in the research will have gained knowledge of ISCM upon completion of review of the assessment elements. With this new knowledge, it is anticipated that they may address the governance requirements in subsequent updates of their policies, procedures, and other documentation.

5. Contributions

An ISCM program assessment conducted in a federal organization will contribute to understanding the elements that need to be improved and how to optimize ISCM. It is anticipated that these findings will not only be helpful to government agencies but will also apply to other public and private organizations to improve their cybersecurity operations. This research may be utilized to assist agencies in the performance of their assessments and ultimately mature programs to meet federal compliance requirements for ISCM implementation and deliver cybersecurity in a more responsively and effectively.

The research is expected to provide a deeper understanding of the useability and limitations of the ISCM Program Assessment methodology and the ISCMAx tool. The ISCMAx tool was released by NIST in 2021. There are no other assessments conducted within the DoD known to the research using this tool. As a result of this research, an ISCM Doctrine Placemat, described in 5.1 will facilitate a better understanding of the scope of doctrine involved in a well-developed ISCM program.

5.1 ISCM doctrine placemat

Several of the NIST ISCM assessment elements involve strategies, policies, procedures, and other documentation. An ISCM Doctrine Placemat based on key doctrine identified within the NIST ISCM assessment elements has been developed as part of this research, see Figure 5. The ISCM Doctrine Placement facilitates a single-page visual representation of the key foundational ISCM program doctrine and components without having to delve into the individual assessment elements. The placemat could visually represent the state of an organization's ISCM doctrine by color coding the doctrine that satisfies the requirements in Green and the items that are deficient in Red. The ISCM doctrine is grouped into categories: *Organizational Strategy, Operationalize, Resource, Report, Respond*, and *Related Functions*. *Organizational Strategy* contains the Risk Management Strategy and the ISCM Strategy, the most foundational doctrine of an ISCM program. *Operationalize* doctrine contains the documents which provide structure to the ISCM mechanisms. *Resource* includes funding and budgeting the ISCM program as well as resourcing it with human capital. *Report* covers ISCM reporting mechanisms and *Response* addresses the doctrine for risk-based response activities.

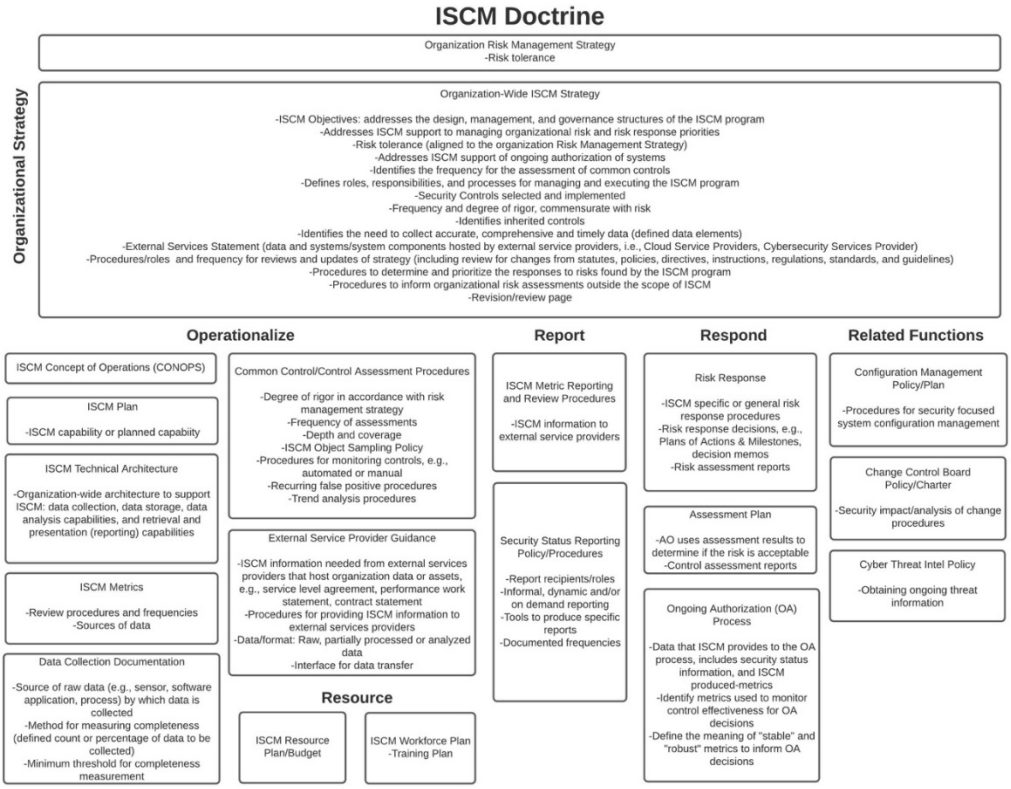

Figure 5: ISCM doctrine placemat

6. Stage of the research

The research design is presented as part of the research conducted for a doctoral thesis. The research proposal has been approved by a doctoral committee. The data collection for all 128 of the ISCM assessment elements has been completed and data analysis is ongoing. Preliminary research findings have been presented at the IEEE 2021 International Conference on Computational Science and Computational Intelligence, Symposium on Cyber Warfare, Cyber Defense & Cybersecurity (AlSadhan and Park, 2021). The final thesis is expected to be defended in 2022. By participation in the research Consortium, the researcher is looking to gain insight for narrative analysis and formulating the research findings so that they are insightful and connect back to the research objectives.

References

AlSadhan, T. and Park, J.S. (2021, December) "Leveraging Information Security Continuous Monitoring to Enhance Cybersecurity", In Proceedings of the 8th Annual Conference on Computational Science and Computational Intelligence (CSCI) Symposium on Cyber Warfare, Cyber Defense & Cyber Security (CSCI-ISCW).

AlSadhan, T. and Park, J.S. (2015, March) "Leveraging Information Security Continuous Monitoring for Cyber Defense", In Proceedings of the 10th International Conference on Cyber Warfare and Security, p 401.

Center for Internet Security (CIS) (2021, May) "CIS Controls Version 8.0", [online], http://www.cisecurity.org/controls/

Coghlan, D. (2001) "Insider Action Research Projects: Implications for Practicing Managers", *Management Learning, 32*(1), pp 49-60.

Cybersecurity and Infrastructure Security Agency (CISA) (2020a, April 17) "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0", [online], https://www.cisa.gov/sites/default/files/publications/FY_2020_IG_FISMA_Metrics.pdf

Cybersecurity and Infrastructure Security Agency (CISA) (2020b, December 13) "Mitigate SolarWinds Orion code compromise (Emergency directive 21-01)", [online], https://cyber.dhs.gov/ed/21-01/

Cybersecurity and Infrastructure Security Agency (CISA) (2021a) "CDM Program Overview", [online], https://www.cisa.gov/sites/default/files/publications/2020%2009%2003_CDM%20Program%20Overview_Fact%20Sheet_1.pdf

Dempsey, K., Chawla, N., Johnson, A., et al (2011) "Special Publication 800-137 ISCM for Federal Information Systems and Organizations", National Institutes of Standards and Technology.

Dempsey, K., Pillitteri, V. Y., Baer, C., et al (2020) "Special Publication 800-137A Assessing Information Security Continuous Monitoring (ISCM) Programs", National Institutes of Standards and Technology.

Dempsey, K., Pillitteri, V., Baer, C., et al (2021) "NIST Internal or Interagency Report (NISTIR) 8212 ISCMA: An Information Security Continuous Monitoring Program Assessment", National Institutes of Standards and Technology.

Department of Defense (2018) "Cyber strategy summary", [online], https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Federal Information Security Management Act (FISMA) Title III of the e-Government Act of 2002., Public Law 107-347 (2002)

Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283 (2014)

Government Accountability Office (GAO) (2019) "GAO-19-384 Agencies Need to Fully Establish Risk Management Programs and Address Challenges"

Government Accountability Office (GAO) (2020a, August) "GAO-20-598 Cybersecurity DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program", [online], https://www.gao.gov/assets/710/708885.pdf

Government Accountability Office (GAO) (2020b) "GAO-20-691T Information Technology Federal Agencies and OMB Need to Continue to Improve Management and Cybersecurity"

Government Accountability Office (GAO) (2021, April 22) "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response", [online], https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

Joint Task Force Transformation Initiative (2011) "Special Publication 800-39 Managing Information Security Risk", National Institute of Standards and Technology.

Mell, P., Waltermire, D., Feldman, et al (2012) "CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture" (No. NIST Internal or Interagency Report (NISTIR) 7756 (Draft)), National Institute of Standards and Technology.

Office of Management and Budget (OMB) (2011) "GAO M-11-33 FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management".

Office of Management and Budget (OMB) (2016) "Circular No. A-130 Managing Information as a Strategic Resource", [online], https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

Office of Management and Budget (OMB) (2020) "Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements", [online], https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-02.pdf

Office of Management and Budget (OMB) (2021a) "Annual Report to Congress: Federal Information Security Act of 2014 Fiscal Year 2020", [online], https://www.whitehouse.gov/wp-content/uploads/2021/05/FY-2020-FISMA-Report-to-Congress.pdf

Office of Management and Budget (OMB) (2021b) "FY 2020 Annual Cybersecurity Performance Summary", [online], https://www.whitehouse.gov/wp-content/uploads/2021/05/FY2020FISMAAnnualCybersecurtiyPerformanceSummaries.pdf

Shani, A. B. and Pasmore, W. A. (1985) *Organization inquiry: Towards a New Model of the Action Research Process. Contemporary Organization development: Current Thinking and Applications, Scott, Foresman, Glenview, IL*, pp 438-448.

United States Senate Committee on Homeland Security & Governmental Affairs (2021, April 6) "Portman, Peters Request Information on Federal Government's Response to SolarWinds Orion and Microsoft Exchange Cyberattacks," [online], https://www.hsgac.senate.gov/media/minority-media/portman-peters-request-information-on-federal-governments-response-to-solarwinds-orion-and-microsoft-exchange-cyberattacks

The White House (2021, May 12) "Executive Order on Improving the Nation's Cybersecurity", [online], https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/