PRIOR, BRIAN CRAIG, M.S. Assessing the Effectiveness of Defensive Cyber Operations. (2017)
Directed by Dr. Hamid Nemati. 101pp.

Enormous amounts of resources are being allocated for defensive cyber programs. The White House's Cyber Security National Action Plan proposes a 35% increase in federal spending on cyber security during Fiscal Year 2017. Without an appropriate understanding of how well the people, processes, defenses, and risk are measured, there will naturally be unproductive tasking, inefficient spending and ineffective reporting. In 2016, the White House established the Commission on enhancing National Cybersecurity to assess the state of our nation's cybersecurity posture. The report recognized both the difficulty and the need to develop meaningful metrics for cybersecurity in order to better secure the cyber landscape as it pertained to the broader digital ecosystem and its connection to our economy, government, and defense. The commission focused on both the private sector as well as the government and suggested the need to perfect policies, practices and technologies. Additionally, the Marine Corps University recently released research topics addressing some of the most important concerns affecting warfighters. One of the concerns was the lack of a methodology for determining the performance of Defensive Cyber Operations (DCO). Specifically addressed was a need to better understand how actions taken by network defenders facilitate network protection. Previous analysis of this topic led to a reactive and un-actionable approach which was tied to negative events such as the quantity and category of incident reports. As there is currently no framework or scorecard built to evaluate DCO as a whole effort, a

methodical approach was taken to scope the problem, compare existing frameworks, develop a framework, and present a scorecard.

The first phase of research required scoping exactly what is involved in DCO at the most basic level and understanding how the DoD evaluates performance. This resulted in an understanding of the actionability of metrics, the levels of warfare, and the counterbalance of cyber asymmetry. Also identified was the military doctrine for assessments, which frames evaluations in terms of Measures of Effectiveness and Measures of Performance and supports continuous assessments that provide actionable information to decision makers. The second phase required a detailed analysis of existing frameworks that measured related functions of cybersecurity. Specifically utilized were industry accepted compliance, incident handling, governance, and risk management frameworks. The outcome identified four functional areas common to most frameworks; people, processes, defenses, and risk. The third phase involved developing a framework that evaluated the four functional areas of DCO identified in the problem-framing phase, utilizing the most appropriate features of the already established frameworks. A key facet of this evaluation was that assessments should be weighed over time to demonstrate progress but also be measured against standards, peers, and the adversary. The final phase identified the continuous reporting criteria and the tangible mechanism for evaluating an organization in terms of a scorecard.

The framework is not a static list of measurements but rather supports tailoring metrics to the organization's specific requirements. The fundamentals of the framework are organized into elements, levels, categories, ends/ways, and measures. These metrics

should be documented utilizing a standardized rubric that assesses the capability and performance of the metrics. The results should be reviewed and analyzed to determine trends, areas for improvement or investment and actionable information to support decision making. Additionally, a modified Delphi analysis with expert consensus validated the major concepts put forward in this paper. Overall, this research provides a comprehensive framework to evaluate the performance of Defensive Cyber Operations in terms of people, processes, defenses, and risk, filling a knowledge gap that is increasingly vital.

ASSESSING THE EFFECTIVENESS OF DEFENSIVE CYBER OPERATIONS

by

Brian Craig Prior

A Thesis Submitted to
the Faculty of The Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Master of Science

Greensboro
2017

Approved by

_____
Committee Chair

APPROVAL PAGE

This thesis written by BRIAN CRAIG PRIOR has been approved by the following committee of the Faculty of The Graduate School at The University of North Carolina at Greensboro.

Committee Chair_____

Committee Members_____

_____

_____
Date of Acceptance by Committee

_____
Date of Final Oral Examination

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

The purpose of this research was to ascertain a comprehensive framework for assessing the effectiveness of Defensive Cyber Operations (DCO). Defensive Cyber Operations is an encompassing military term for cyberspace operations designed to preserve the ability to utilize friendly cyberspace.

Enormous amounts of resources are being allocated for defensive cyber programs. The White House's strategy to create the Cyber Security National Action Plan is a perfect example. The plan proposes a 35% increase in federal spending on cybersecurity during Fiscal Year 2017.[1] Yet, without an appropriate understanding of how well the people, processes, and defenses reduce risk to the network, there will naturally be unproductive tasking, inefficient spending and ineffective reporting. Specifically, this information must be framed in a manner that our commanders can understand and use to take action.

In 2016, the White House established the Commission on enhancing National Cybersecurity to assess the state of our nation's cybersecurity posture. The report recognized both the difficulty and the need to develop meaningful metrics for cybersecurity in order to better secure the cyber landscape as it pertained to the broader digital ecosystem and its connection to our economy, government, and defense. The

[1] Whitehouse.gov

commission focused on both the private sector as well as the government and suggested the need to perfect policies, practices and technologies.[2]

The Marine Corps University recently released research topics addressing some of the most important concerns affecting warfighters. One of the concerns was the lack of a methodology for determining the performance of DCO. Specifically, addressed was a need to better understand how actions taken by network defenders facilitate network protection. Previous analysis of this topic led to a reactive and un-actionable approach which was tied to negative events such as the quantity and category of incident reports.[3] As there is currently no comprehensive framework or scorecard built to evaluate DCO as a whole effort, a methodical approach was taken to scope the problem, compare existing frameworks, develop a framework, and present a scorecard.

The first phase of research required scoping exactly what is involved in DCO at the most basic level and understanding how the DoD evaluates performance. This resulted in an understanding of the actionability of metrics, the levels of warfare, and the counterbalance of cyber asymmetry. Also identified was the military doctrine for assessments which frames evaluations in terms of Measures of Effectiveness and Measures of Performance and supports continuous assessments that provide actionable information to decision makers. The second phase required a detailed analysis of existing frameworks that measured related functions of cybersecurity. Specifically utilized were industry accepted compliance, incident handling, governance, and risk management

[2] Report on Securing and Growing the Digital Economy
[3] "Marine Corps Research Topics AY 2016-2017." Marine Corps University

frameworks. The outcome identified four functional areas common to most frameworks; people, processes, defenses, and risk. The third phase involved developing a framework that evaluated the four functional areas of DCO identified in the problem-framing phase, utilizing the most appropriate features of the already established frameworks. A key facet of this evaluation recognized that assessments should be weighed over time to demonstrate progress but also be measured against standards, peers, and the adversary. The final phase identifies the continuous reporting criteria and the tangible mechanism for evaluating an organization in terms of a scorecard. The framework should not be a static list of measurements but rather support tailoring the metrics to the organization's specific requirements. The final results should be reviewed and analyzed to determine trends, areas for improvement or investment and actionable information to support decision making.

The framework is not a static list of measurements but rather supports tailoring metrics to the organization's specific requirements. The fundamentals of the framework are organized into elements, levels, categories, ends/ways, and measures. These metrics should be documented utilizing a standardized rubric that assesses the capability and performance of the metrics. The results should be reviewed and analyzed to determine trends, areas for improvement or investment and actionable information to support decision making. Additionally, a modified Delphi analysis with expert consensus validated the major concepts put forward in this paper. Overall, this research provides a comprehensive framework to evaluate the performance of Defensive Cyber Operations in

terms of people, processes, defenses, and risk, filling a knowledge gap that is increasingly vital.

Scope

This paper seeks to provide a thorough account of the functional nature of DCO by utilizing unclassified DoD publications, academic research, and industry white papers in order to frame the problem and propose a solution. A single concept for assessing the performance of DCO will empower the community to standardize reporting, increase command and control and improve defenses. The scope of this paper primarily focuses on improving processes within the DoD, however the general concepts put forward should empower other federal agencies with similarly structured cyber defenses. Additionally, the same struggle in measuring cybersecurity has been plaguing commercial enterprises for years. Although the specific metrics put forward may not be as relevant to the private sector, the general concepts may well hold weight, especially within the financial, telecommunications, and energy industries.

Defensive Cyber Operations (DCO)

DCO is an intangible categorization of numerous actions that provide freedom of maneuver in cyberspace. It is much more than the civilian construct of cybersecurity. Yet, at its core, remain the same objectives of confidentiality, integrity, and availability. The DoD has done its best to structure cybersecurity into three encompassing missions: Department of Defense Information Network Operations (DODIN Ops); Defensive

Cyberspace Operations Internal Defensive Measures (DCO-IDM); Defensive Cyberspace Operations Response Actions (DCO-RA). [4]

The first mission is DODIN Ops, which includes the planning, installing, operating, maintaining, and securing of the Department of Defense Information Network (DODIN). It is important to note that DODIN Ops are not considered part of DCO. In many cases, it is a disparate dimension focused primarily on the availability of the network without due emphasis on confidentiality or integrity. Joint Publication 3-12 separates DCO into Internal Defensive Measures and Response Actions. DODIN Ops are normally considered information technology (IT) functions that are carried out by system administrators and network engineers.[5] Many organizations have pigeonholed DODIN Ops into this role, discounting the umbrella notion that DODIN Ops supports DCO. The key concept to understand is that DODIN Ops should create a secure baseline in the layered defense in depth strategy of the DODIN. In this mission, the DoD must be able to assess its ability to execute tasks such as patching vulnerabilities, encrypting data, and training users. While, DODIN Ops is not doctrinally an entity of DCO it needs to be considered a supporting role and thus comprehensively evaluated.

The second mission that provides the freedom of maneuver within cyberspace is DCO-IDM. The baseline security architecture provided by DODIN Ops is not capable of defending against a determined and persistent adversary. Thus, internal defensive measures are mission focused and threat specific actions that complement the limited

[4] JP 3-12 Cyberspace Operations
[5] Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations."

security of DODIN Ops. The objective is to detect and mitigate threats to the operating environment by outmaneuvering the adversary. A key tenant of DCO-IDM is the identification and prioritization of key terrain within cyberspace and a complementary defense dedicated to counter the enemy's capabilities.[6] Specific tasks within DCO-IDM include the identification of threats through hunting and the implementation of custom signatures for active blocking and alerting. Followed actions include incident response, reporting, sharing of intelligence, and the employment of countermeasures. Internal defensive measures respond to malicious activity, threats, and alerts leveraging intelligence while prioritizing cyber key terrain. [7]

While DCO-IDM refers to measures and countermeasures applied within the DODIN, DCO-RA are actions taken outside the DODIN. DCO-RA must be deliberate, authorized and taken only to defeat ongoing or imminent threats in accordance with the standing rules of engagement. Assessing the effectiveness of DCO-RA is not within the scope of this paper.

[6] Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations."
[7] JP 3-12 Cyberspace Operations

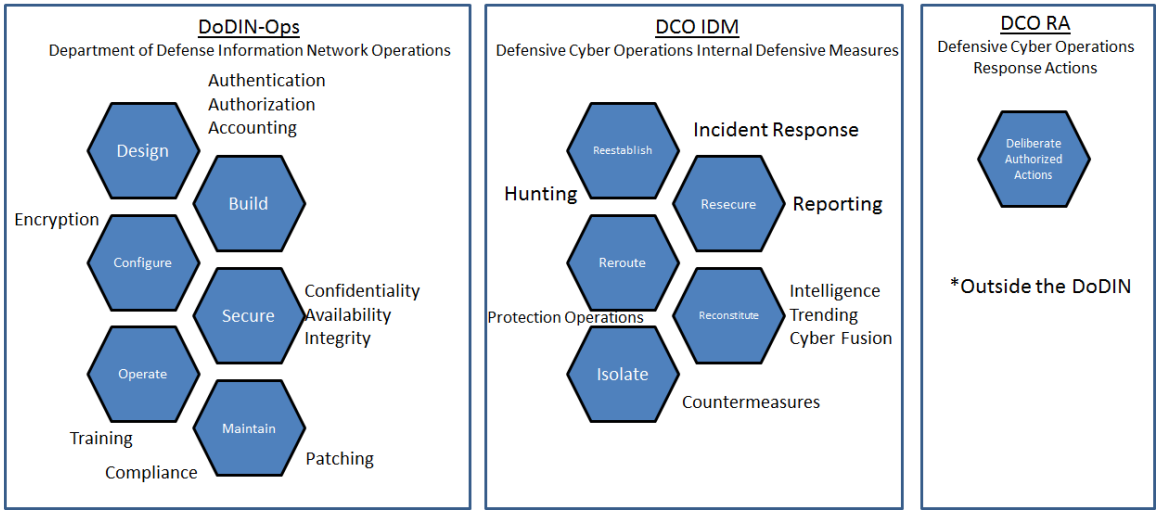


Figure 1. DODIN Ops and DCO Missions

Assessments

To put forward a useful framework for evaluating DCO, we must explore the nature of how the DoD measures success and mission accomplishment. Joint Publication 3-60, *Joint Targeting* describes the purpose of assessments as the measure of progress toward mission accomplishment. This is a continuous process that commanders must gauge to understand progress towards their desired end state.[8] This continuous nature of assessments in cyberspace enables commanders at all levels to make decisions about the deployment of cyber defense forces, tools, and sensors.

The assessment process should begin during planning and be re-evaluated throughout the preparation and execution of a given mission. This process assists the commander's staff in deciding what and how to measure success. Therefore, the DoD would decide how to assess DCO actions prior to the engineering of their networks, the

[8] JP 3-60 Joint Targeting

establishment of sensor grids, and the employment of internal defensive measures. However, a major struggle with evaluating DCO operations is that most networks are already built and sensor grids already established. Thus the measurements that are derived today may be inadequate or require a significant investment of time and money to implement.

Assessments occur at all levels of command. MCDP 1 *Warfighting*, defines three interrelated levels of war which must be used to understand all other concepts. The strategic level consists of establishing goals, assigning forces, and providing assets. The tactical level describes the methods we use to achieve a mission. The operational level of war joins the strategic and tactical levels in that it is the use of tactical effects to attain strategic goals.[9] In terms of DCO, leaders need to ensure our metrics for success and the models we use to report those measurements provide an effective assessment at all three levels of warfare.

Joint doctrine states that at each level of war, operations are evaluated utilizing two different forms of metrics. Measures of Effectiveness (MOE) are used to evaluate changes in system performance, capability, or the operational environment. These measures are designed to express a trend toward or away from a military objective. Measures of Performance (MOP) are intended to assess changes that are tied to an end state. [10]A simpler way of looking at these two ideas is that MOE measure the ends and MOP measure the ways. Looking back at the levels of warfare, MOE and MOP are

[9] MCDP1 Warfighting
[10] JP 3-12 Cyberspace Operations

inherently related, and a MOP at one level may be a MOE at another. The traditional example states that our desired endstate at the operational level is to reduce enemy movement. An MOE would be the amount of enemy movement from current positions. The MOP would be the amount of bridges that were destroyed. At the tactical level the endstate would be the destruction of a particular bridge. The MOE would be the level of bridge destruction and the MOP would be whether that mission was flown on time and the correct ordinance was delivered.

In terms of DCO, we could state that our desired endstate at the operational level is to isolate a rapidly spreading malware infection. An MOE would be the amount of hosts that were compromised by lateral movement. A MOP would be the number of routers that were reconfigured to isolate infected LANs. And then at the tactical level the endstate would be the reconfiguring of a particular core router. The MOE may be the level of isolation and its impact on the tenant of availability and the MOP may be whether certain ports and protocols were still aloud access to other networks.

Assessments are especially effective if they incorporate both quantitative and qualitative analysis. Reliance on either raw data or human opinion easily skews the assessment process, yet when they work in concert a balanced picture of reality is revealed. [11] Additionally, according to NIST Special Publication 800-137, effective metrics yield specific, measurable, actionable, relevant, and timely information. [12]

[11] Commander's Handbook for Assessment Planning and Execution
[12] NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

Metrics vary in scale and purpose from situational awareness to actionable information. While neither should be outright discounted, for the purpose of determining the overall efficacy of an organization, management should strive to provide leadership actionable metrics that can be used for decision-making. For example, a situational awareness metric could be the number of closed incident reports last month. This information by itself may be used to provide situational awareness on incident reporting trends, and may potentially be used to develop future manpower requirements when combined with other metrics. However, a more actionable metric would be the number of reports in which the adversary was able to achieve milestones towards their objective on the DODIN, such as users opening spearphishing links or attachments. Leadership could then choose to conduct organizational level training if the numbers are high.

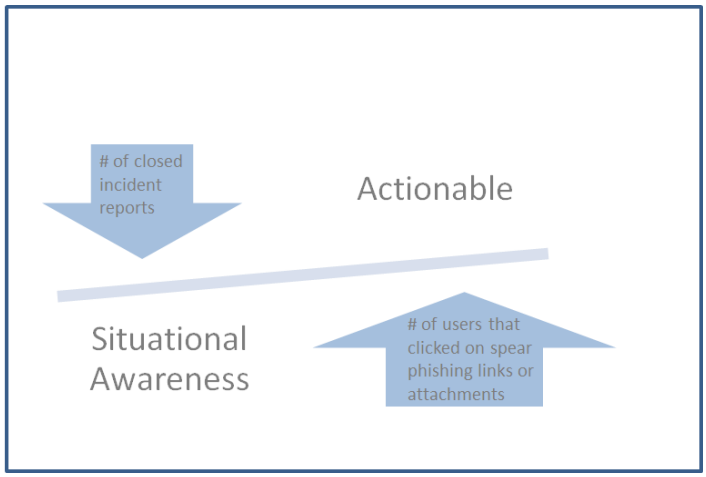


Figure 2. Actionable Metric Scale

MCDP 1-3, defines asymmetry as "a means of gaining the advantage through imbalance, applying strength against an enemy weakness."[13] Asymmetric Warfare means fighting the enemy in terms that are advantageous to us and in ways in which traditional military capabilities such as superior manpower is not necessary. Symmetric Warfare entails the use of similar capabilities, such as utilizing ground forces to fight ground forces. However, asymmetric warfare would capitalize on advantageous capabilities such as airpower to fight ground forces in open terrain. In terms of Cyberspace, Defensive Cyber Operations as well as Offensive Cyber Operations are both symmetric as well as asymmetric.

The symmetric nature of Offensive Cyber Operations is clear. To a certain degree, all actors must operate on a relatively even playing field. Open source penetration tools, access to the internet, and standard protocols such as IPv4 and IPv6 stabilize the environment, reducing the gap between a highly resourced actor and a low resourced actor. Defensive Cyber Operations are also commonly recognized as symmetric in nature. The public disclosure of vulnerabilities and the sharing of indicators of compromise through common reporting sources like Virus Total and others, assists defender's in reacting and preparing for an attack. Additionally, readily available open source defensive tools and public encryption standards provide the means for most defenders to provide confidentiality, integrity, and availability of their organization's data for a relatively low budget.

[13] Marine Corps Doctrinal Publication 1-3 Tactics

Sophisticated actors may capitalize on the asymmetric aspects of both defensive and offensive cyberspace operations. An asymmetric offense may gain advantage over a defender by applying the strength of a large botnet or the scalability of cloud infrastructure to conduct a distributed denial of service attack against a defender's critical vulnerability. An attacker may also develop or purchase zero day exploits to gain an asymmetric advantage over the defender's signature based sensors. Technological research into the domain of quantum computing may eventually grant an asymmetric advantage to the attacker that is able to leverage advanced cryptanalysis and break secret messages in a fraction of the time it takes conventional cryptanalysis systems.

The defense may also take advantage of asymmetric tactics and tools. Non-signature based sensors that utilize heuristics and detect anomalies may counteract zero day attacks. Artificial intelligence based sensors and big data analytics may predict and mitigate future attacks. Cloud based services may be equally useful to the defender, enabling the agile pivot from virtual infrastructure to virtual infrastructure. For each asymmetric attack, it seems there is also an asymmetric defense. One of the main findings the Cyber National Action team presented in their 2016 report to the President was that both offense and defense adopt the same innovations. Specifically addressed were topics such as machine learning, artificial intelligence and advances in encryption technologies which may be used for offense and defense. [14]

[14] Report on Securing and Growing the Digital Economy

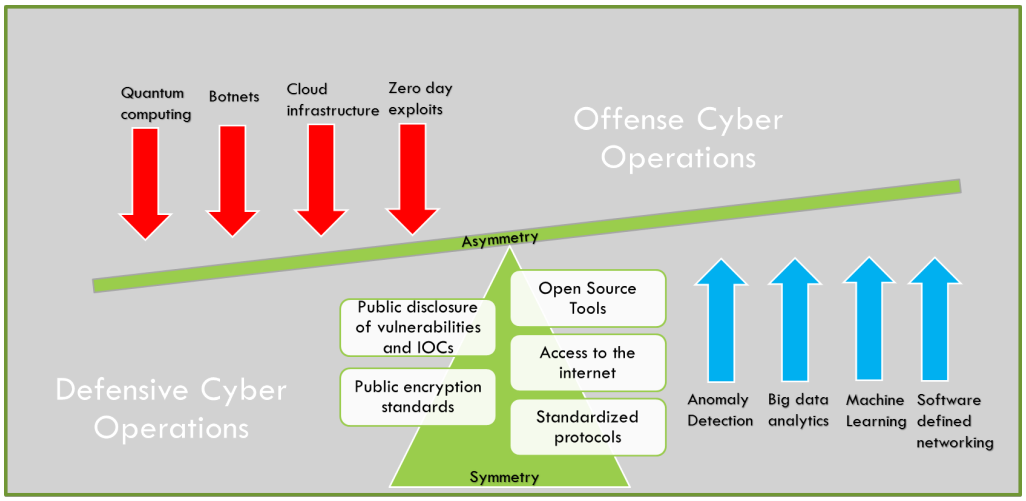


Figure 3. Cyber Asymmetry

In itself these attacks and their countermeasures reveal an overall symmetric environment in which asymmetric strategies and tools can be implemented to gain an advantage. However, in general, asymmetric strategies and tools cost resources. The attacker or defender that can spend more, process more, or mount more man hours than their opponent should be able to gain the advantage. However, according to another finding in the report on Securing and Growing the Digital Economy, the attacker has the default advantage. A less skilled actor can purchase tools, botnets for hire, and even receive technical support to attack a network for a fraction of the cost to defend it. [15]

When possible, we should attempt to utilize the asymmetric capabilities of DCO and assess the effectiveness of these capabilities. As resources, such as financial capital, processing power, and human resources assist an organization in gaining the asymmetric advantage within the cyber domain, economy of force strategies should be applied that

[15] Report on Securing and Growing the Digital Economy

expand the ability of machines to execute the decision process and minimize the need for human interaction. Additionally, careful attention should be paid to the return on investment of tools, to ensure the appropriate use of resources.

A worthwhile framework does not simply dictate a list of metrics that all organizations should measure. This is because metrics are not equally actionable at all levels. A tactical level metric being reported at the enclave may not be useful to the Chief Information Officer (CIO) of the enterprise. Yet this is how reporting is too often conducted. Many of the metrics that are currently utilized fall heavily to the left side of the scale and the same metrics are employed at all levels.

Challenges

There are many issues that have prevented a single concept for evaluating DCO. First, there are numerous dimensions of DCO, from incident handling and response to intelligence and reporting. Many cybersecurity frameworks explore a single dimension of DCO. While these models may provide an increased understanding of specific concepts, they generally do not provide a means to evaluate how successful an organization is at DCO as a whole. Furthermore, DoD doctrine often separates the functional nature of cybersecurity into compliance and network hardening (DODIN Ops) and hunting and response actions (DCO-IDM). This fractional method of evaluating DCO as a partial concept means that we are not providing the commander with an adequate representation of how our conceptual shield is prepared for enemy engagement.

As with any system, planning for how we will evaluate the effectiveness of that system will ideally be completed before the process or procedure will be put into place.

This ensures there are tools engineered into the plan to capture the metrics needed. However, the unique challenge of DCO is that the network is already built, sensor grids already firmly established, and reporting processes already developed. This particular challenge may be overcome with a significant amount of planning, time, and fiscal resources. Yet, another option would be to completely rebuild the network from the ground up. While this paper does not focus on this idea, it does support it. Many organizations are experimenting with virtual networks that can be completely set up and torn down in a matter of minutes. This restructuring of the network would enable management to reestablish tools and processes to provide the most useful metrics possible.

The DODIN is a disparate network of networks, operated by many services and agencies. Each organization defends its network according to policies dictated by its higher-level cyber component. This mesh has created an incongruent reporting structure that is not only difficult to defend, but nearly impossible to assess. The recent creation of Joint Force Headquarters – DODIN has sought to provide cohesion to this mesh. Yet, this transformation is still developing and there is no clear framework or model for how to measure and evaluate the success of DCO throughout the DODIN. However, the DoD has made tremendous progress in improving standardized reporting of compliance through the adoption of the DOD CIO's Cybersecurity Scorecard, which will be covered later.[16]

[16] DoD Cybersecurity Discipline Implementation Plan

Additionally, most frameworks focus specifically on incident handling and do not evaluate success against an adversary or even a peer organization. Others such as Lockheed Martin's Cyber Kill Chain do provide a quality concept for understanding how an organization should analyze and respond to an adversary intrusion. Yet, it does not provide a mechanism for continually evaluating success or failure. Without a framework to continuously evaluate DCO as a whole of effort, commander's resort to infrequent security audits, vulnerability assessments, and penetration test. While certainly useful, these tests only give a commander insight into a snapshot of DCO. It is also a common misconception that organizations are conducting cybersecurity well if they have not been hacked or are not in the news. This fallacy may provide the organization with a false sense of confidence and may result in management not identifying areas for improvement.

CHAPTER II

FRAMEWORKS

The Department of Defense (DoD), defense contractors, and the private sector have developed many different frameworks for understanding information and security. The next phase of research consists of a detailed literature review that examines the most prevalent frameworks, analyzing their strengths and weaknesses for assessing Defensive Cyber Operations (DCO). In order to organize this exposition cogently, the following categories of frameworks were chosen; risk management incident handling, compliance, and governance.

Risk Management Frameworks

Risk management is perhaps the most important indicator of the effectiveness of a cybersecurity program. Defensive Cyberspace Operations Internal Defensive Measures (DCO-IDM) and Department of Defense Information Network Operations (DODIN Ops) should both be assessed by their ability to effectively manage risk.

NIST Risk Management Framework

The Risk Management Framework (RMF) is the approved certification and accreditation process for DoD information systems. The RMF is a six-step process that assigns tasks and responsibilities that must be accomplished prior to a system being put online, during the system's lifecycle, and throughout decommissioning. The Risk

Management Framework promotes the idea of real time risk management through continuous monitoring. The concept of continuous monitoring will be examined under the compliance frameworks but is tied back to the higher level RMF.[17]

The RMF is a checklist of tasks that form the baseline security posture for the DoDIN. The process ensures that both technical and administrative controls are applied to an information system prior to being put on the network. In step 1, the system is categorized, described, and registered. Step 2 calls for the identification and selection of security controls. Most importantly, step 2 requires the development of a continuous monitoring of these security controls and their effectiveness. This is then codified into a security plan, which is approved by the authorizing official. Step 3 involves the implementation and documentation of security controls. Step 4 of the RMF requires a process for developing, reviewing, and approving a plan to assess security controls. These controls are then assessed; a report generated, and initial remedial actions taken. In step 5, the information system is authorized, but only after a Plan of Action and Milestones (POA&M) has been developed for any findings identified in step 4 that could not be quickly remediated. Finally, a risk assessment is conducted based on the security assessment and POA&M. If the risk is acceptable then the authorizing official will accredit the system.[18]

The final step stands alone from the accreditation process. Step 6 involves the continuous monitoring of the information system after it has been connected to the

[17] NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems
[18] NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems

network. Here, changes to the information system and environment are assessed according to the security impact. Technical, management, and operational controls are also continuously monitored and remediated. The security plan is updated and the security status, to include effectiveness, is reported to leadership.

This continuous assessment needs to be tied back to the incident handling process in which each incident is considered a change to the environment and forces step 6 of the RMF to be initiated. Each time an incident occurs, a scored evaluation of the overall risk to the information system is evaluated and processed, which affects the overall evaluation of all other connected information systems. In this way, a commander or authorizing official can understand the total risk to their affected networks.

The problem with the RMF, like the other frameworks discussed in this paper, is that it does not provide a thorough understanding of how to measure security controls. Standing alone, this framework is an excellent guide for accrediting a system but it only assesses the information system defenses and subsequent risk to the system according to the controls developed in the security plan. This oversight does not evaluate the people or the processes, against adversaries, peers, or standards.

Incident Handling Frameworks

Incident Handling is perhaps one of the most important functions of DCO. It covers the largest part of DCO-IDM in that it is these actions that are taken in response to threat activity on the network.

CJCSM 6510.01B Incident Handling

The DoD has already established a Cyber Incident Framework that provides a meaningful understanding of incident handling. However, it is focused on providing situational awareness reporting of attacks and does not address evaluation, although many of the metrics that an organization needs to assess incident handling are required to be reported in this framework. The Computer Network Defense (CND) Framework is a tiered defense in-depth model that is organized into three layers; global, regional, and local. Each of these tiers is responsible for executing three defined CND services. The first is to protect. The second is to monitor, analyze, and detect. The last is to respond. The framework also includes a fourth category for capability sustainment. This represents how an organization maintains its training, policies, procedures, and contracts.[19]

One of the most significant strengths of the CND is its focus on the cyber incident life cycle phases and its relationship to the OODA loop. The OODA loop is a process for analyzing and increasing efficiency of each phase of a decision cycle; observe, orient, decide, and act. The incident handling life cycle chronologically characterizes the appropriate steps that should be taken in response to an incident. These steps include the detection of the event, preliminary analysis and identification, preliminary response actions, incident analysis, response and recovery, and post-incident analysis. This logical process encourages network defenders to evaluate their progress in terms of flash to bang or more commonly known as time intervals. Yet, this framework goes one step farther

[19] CJCSM 6510.01B Cyber Incident Handling Program

and abstractly addresses these intervals in terms of the iterative decision cycle known as the OODA loop, encouraging its adoption without providing clear guidance as to how to employ it.

Perhaps the greatest achievement of CJCSM 6510.01B is its decree for standardized reporting and the mechanism to achieve such reports. The reportable information is designed to be input into the Joint Incident Management System (JIMS) which is the tool the DoD uses to report, track, and search for incident tickets.[20] This is significant because it is one of the main mechanisms the DoD currently uses for analyzing reporting metrics. Aside from basic incident characteristics, this document requires events to be categorized by the significance of the event. It also states that organizations must identify additional characteristics of the incident including the delivery vector, system weaknesses, and root cause. These characteristics are useful for correlation and trending, and can provide insight into how successful or unsuccessful the people, strategies, and technologies are at defending the network. Additional characteristics include the Battle Damage Assessment or the impact assessment, which includes the technical and operational impacts of an incident. This is important because if management can show that throughout the last X number of incidents, the technical and operational impact has been low than despite the overall quantity of DCO events, systems are providing an adequate level of defense. This is especially true if there is no mission impact to task critical assets or those assets which are critical to accomplishing a unit's mission essential function.

20 "Joint Incident Management System." Defense Information Systems Agency

This document provides standardized reporting timelines that organizations should use to measure how well they are performing compared to a set requirement. Specifically, it provides timelines for how long each organization must report to the next tier. However, the genius of this model is that it combines the category of incident with the impact to provide the reportable timeline.

There are a few major drawbacks with assessing DCO by this framework. Most importantly, it only frames DCO in terms of incidents. Additionally, through no fault of the framework, standardized reporting is difficult to fully achieve. Without an effective and homogeneous enforcement of reporting, measuring the success of one's organization can only be measured internally. While internal measures of effectiveness are useful if they can be measured against adversarial action or even show progress over time, they lose some of their value if they cannot be evaluated against a peer organization. This also reduces the ability of higher organizations to set goals for subordinates.

Lockheed Martin Cyber Kill Chain

Another widely accepted framework within the security industry is Lockheed Martin's Cyber Kill Chain (CKC). The CKC is an intelligence based approach to computer network defense. This model focuses on identifying and preventing intrusions at the earliest stage of an attack. This model is unique because it demonstrates how the defender has the advantage. An attacker must successfully accomplish every stage of the

attack in order to achieve success. The defender can break this cycle at any phase, thus inoculating the attack.[21]

In order to develop the CKC, Lockheed Martin analysts reviewed many of the NIST publications. In 2012, NIST published the "Computer Security Incident Handling Guide" SP 800-61 Rev 2. The key take away from this revision was that it incorporated post incident activity into preparation for future incidents. Lockheed Martin based its new model off of this intelligence feedback loop. [22] Utilizing this feedback model, they revolutionized the process from a defender-focused defense to an attacker focused defense.

The seven phases of the CKC include; Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives. [23]

---

[21] Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform. Rep. Lockheed Martin Corporation

[22] Hutchins, Eric M. "Understanding the Cyber Kill Chain."

[23] Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin, Ph.D. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*

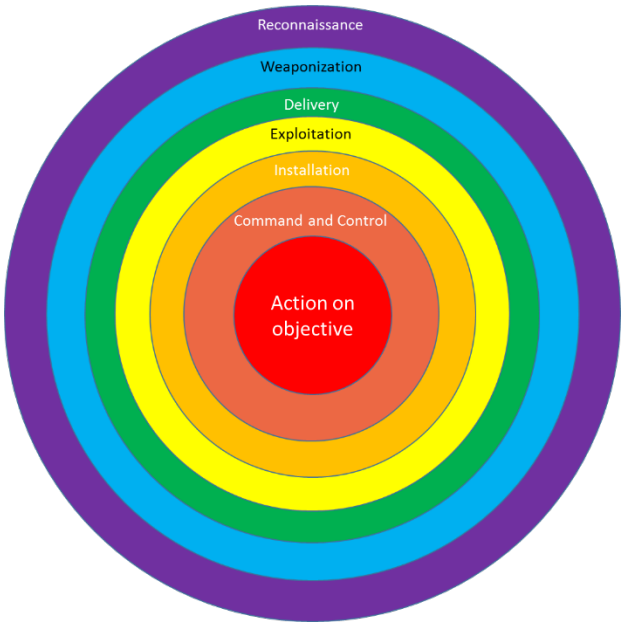


Figure 4. Cyber Kill Chain

Reconnaissance – Target selection, Open Source Intelligence, Scanning

Weaponization – Development of malware, exploit, or payload for the attack

Delivery – Transmission of the weaponized payload, spearphishing email, malicious website, removable media

Exploitation – Execution of malicious code

Installation – Installation of backdoor or persistence on the target

Command and Control (C2) – Establishment of C2 channel that provides the attacker the ability to interact with the target

Actions on objective – Actions that compromise the confidentiality, integrity, or availability of the target.

Lockheed Martin has identified a number of applications to implement the kill chain framework. Understanding these applications supports a greater understanding of how we can measure the effectiveness of our organizations ability to conduct DCO. The first application is to prioritize sensor alerts by the phase of the CKC. Enterprise sensors provide millions and millions of alerts each day. It is not feasible for a human to investigate each alert, thus they must be triaged in a way that ranks alerts. Lockheed Martin suggests associating events to sensors and events to CKC phase. In this way higher priority alerts, those that correspond with phases farther along in the kill chain, are investigated quicker.[24] Management can use this method to determine how well organization are triaging alerts. A similar application is to utilize the CKC phase for escalation and notification to leadership. For example, incidents associated with actions on objective or command and control should receive the attention of leadership. The currently adopted model previously described in CJCSM 6510.01B prioritizes the triaging and notification timelines for incidents by simple category and impact. While this method was revolutionary at one time, its initial assessment of impact is a simple matrix that associates category of event by the network device that is affected. For example, a Category 1 or root level intrusion on a workstation is assessed as low impact where a Category 7 or malware event is assessed as moderate impact. Utilizing the CKC

[24] Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform, Lockheed Martin Corporation

model for triage enables us to better communicate to leadership how far an intrusion has progressed. [25]

Another application for the CKC helps an organization identify gaps in sensor coverage. By comparing the CKC to the cyberspace tasks outlined in JP 3-12, and filling in the table with the sensors and tools that achieve each objective at that phase of the CKC, an organization can identify gaps in sensor coverage and prioritize investment. [26]

	Detect	Deny	Disrupt	Degrade	Deceive
Reconnaissance					
Weaponization					
Delivery					
Exploitation					
Installation					
Command & Control					
Actions on Objective					

Figure 5. Sensor/Tools Gaps

[25] CJCSM 6510.01B Cyber Incident Handling Program
[26] Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform. Rep. Lockheed Martin Corporation

However there is a major problem with this approach. It overemphasizes the fact that an attack need only be stopped at one place in the CKC. Most organizations rely on a Defense in Depth approach to layering their countermeasures. Thus this framework would benefit from adding a third dimension that represents the logical layers of defense. This would demonstrate the gaps in coverage at each layer. Another issue with the CKC is that it is framed around the typical adversary, which is remotely attempting to compromise the network. This specific analysis limits management's ability to use the CKC as an overall DCO framework. Insider threats, both intentional and unintentional, cannot be clearly assessed within the confounds of reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objective. An argument could be made that insider threat and non-compliance activities would automatically be placed within the ring of actions on objective. Yet, according to this scenario, the attacker is able to succeed bypassing the defenses setup to break the kill chain.

The most important parts of the framework for the purposes of this paper are its ability to measure the effectiveness of defenses. A key metric is the phase in which the intrusion was stopped. Ideally, this metric would be utilized over a period of time to demonstrate a trend of stopping an adversary higher and higher in the chain as countermeasures are developed and implemented. Additionally, the CKC can be utilized to measure resilience, in that if an attack is stopped at one phase of the CKC, it would be stopped in a lower phase or multiple phases. Over time, improvement in resilience confirms a robust, layered, and effective defense. Lockheed Martin proposes an

effectiveness scorecard that shows the efficacy and resilience of an organization based on where the intrusion was stopped and where alternative countermeasures are in place for each threat actor campaign. Additionally, this scorecard could be utilized to justify the return on investment for each tool based on how well it blocked or could have blocked an attack. [27]

There are many strengths to consider when reviewing the CKC. Distinctively, utilizing the perspective of an attacker to hone your defenses means an organization is focused on defending against specific threats rather than a defense of everything, which is really a defense of nothing. Additionally, it provides a detailed understanding of the threat actor and how they executed their attack. This intelligence on the capabilities and intent of the actor can be used against them in future attacks.

NIST Cybersecurity Framework

The next framework to explore is the NIST Cybersecurity Framework. NIST presents a risk-based approach to improving the security of critical infrastructure within both the private and public sector. The framework's core elements include functions, categories, subcategories, and informative references of cyber security. These components are assembled into a graphical table that provides an organization with guidance in determining what activities they should be doing to achieve specific cyber security outcomes. While NIST emphasizes the need for each organization to align this

[27] Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform. Rep. Lockheed Martin Corporation

framework to their particular organization needs, they do accentuate five key functions which all organizations must accomplish; identify, protect, detect, respond, and recover.[28]

The end state of completing this table is to develop a profile that determines gaps within the five functions listed above. This profile is then graded on a tiered system that measures how well an organization has implemented the framework and thus reduced risk. The Cybersecurity Framework does not measure the effectiveness of an organization's ability to conduct DCO. Rather, it is a theoretical framework for implementing activities to reduce risk. The strength of the Cybersecurity Framework is the development of the five key functions, the structure of the table, and the ability to apply the framework to almost any organization.

Compliance Frameworks

Compliance is generally considered a DODIN Ops function and does not always receive the attention it deserves from a DCO perspective. However, the DoD is beginning to refocus the need to shore up basic cybersecurity requirements to reduce the attack surface. Per the Secretary of Defense, Ashton Carter, "Cyber defense of DoD systems is [my] highest cyber priority; if DoD systems are not dependable in the face of cyber warfare, all other DoD missions are at risk."[29]

Cybersecurity Scorecard

In October 2015, the Department of Defense Chief Information Officer published the DoD Cybersecurity Discipline Implementation Plan. This document focused on

[28] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity
[29] DoD Cybersecurity Discipline Implementation Plan

aligning DoD cyber security requirements by Lines of Effort. Each line of effort concentrates on a key aspect of cyber security that can be strengthened to better defend against adversaries. This plan utilizes compliance-based metrics to report the cybersecurity posture of tactical units up through strategic level service components and combatant commands through the use of the Defense Readiness Reporting System (DRRS).[30]

DRRS delivers decision makers at every level of military command a quantitative readiness report capturing readiness metrics in near real time. Furthermore, business intelligence tools and readiness dashboards provide detailed analysis into the metrics being reported. Specifically, DRRS utilizes mission-essential tasks (MET) to identify a given unit's responsibilities that are critical to the success of their mission. Metrics then derived from these METs are designed to demonstrate the effectiveness and the preparedness of the unit in question. [31]

The DoD CIO chose four lines of effort to build his DRRS report metrics. These lines of effort are in fact abstract goals and not in themselves measures of performance. The first line of effort is strong authentication. This line of effort ensures commanders posture their cyber defenses to require multi-factor authentication, strong encryption keys, and strict passwords. These requirements prevent unauthorized access of DoD systems and help ensure confidentiality and non-repudiation. The second line of effort is device hardening. Device hardening entails patching, configuration management, and

[30] DoD Cybersecurity Discipline Implementation Plan
[31] Department of Defense Readiness Reporting System (DRRS)

other endpoint security measures. The third effort is to reduce the attack surface, thereby making the DODIN simpler to defend and harder for the opponent to find weakness. The fourth line of effort is to align organizations to a Computer Network Defense Service Provider.

The title "Cybersecurity Scorecard" is rather deceiving. It is not an all-encompassing scorecard; rather it is strictly focused on compliance. It lacks metrics for DCO-IDM. The main strength of this initiative is the mechanism for reporting. The DRRS reporting structure enables cyber reporting at each level of command and agency. These MOPs/MOEs are developed to provide an overall picture of how well the DoD is defending the DODIN. However, there is no room for tailoring specific DCO objectives to an organization. For example, commanders at the operational level cannot require their tactical units to report additional metrics than the metrics set forth at the strategic level. This lack of customization ultimately degrades the usefulness of the Cybersecurity Scorecard. The second weakness of the Cybersecurity Scorecard is the almost binary pass/fail approach to grading an organization. Compliance is a continuous objective that resets each time a change is made to the network or a new vulnerability needs patching. Thus a percentage demonstrating completeness would more accurately depict the defensive posture of an organization.

NIST Continuous Monitoring Program

NIST Special Publication 800-137 provides an essential analysis into the effectiveness of an organization through the perspective of risk tolerance. The strategy incorporates metrics that measure the technology, processes, procedures, operating

environment, and people, marking this framework the most comprehensive analysis of an organization's cybersecurity status. The Information System Continuous Monitoring Program (ISCM) is a reiterative process of identifying problems, assessing those problems, and remediating them. Two measurements can be derived from this process; the speed it takes an organization to execute and the assessed risk along the way. [32]

Another benefit of implementing ISCM is that it provides an encompassing security status that assesses each information system individually and aggregates the information to provide an overall score much the same way that the Cybersecurity Scorecard attempts to do. Though the Cybersecurity Scorecard was built off the ISCM model, it only assesses very specific "problems" or vulnerabilities and does not provide a means to truly evaluate the effectiveness of an organization. Through the ISCM tiered approach, detailed security measurements are assessed and monitored using automated tools. Additionally, these metrics are not designed to remain static and should be constantly reassessed based off their relevance and actionability. [33]

Governance Frameworks

Governance is a key concept involving the management of IT systems. In particular, DCO requires well-defined metrics that assess the performance of management in executing governance. There are many laws and frameworks relating to security governance. Perhaps the most important document outlining management's roles

[32] NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
[33] NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

and responsibilities in an organization is derived from the Clinger – Cohen Act which in part defined the responsibilities of the DOD CIO. For the purposes of DCO, the major functions of the CIO can be consolidated into five responsibilities.[34]

- Acquisition and investment
- IT Architecture
- Policy
- Manpower development and training
- Performance results and technology assessments

However, Craig Simmons proposed a simplified IT governance framework that examined four similar dimensions of IT governance; IT value and alignment, risk management, accountability, and performance measurement. Simmons borrowed heavily from existing works in his assessment of the four dimensions of IT governance, utilizing frameworks such as Control Objectives for Information and related Technologies (COBIT) and the Information Technology Infrastructure Library (ITIL). He argued that utilizing a combination of various governance frameworks provided the best value to an organization. [35]

COBIT

The COBIT framework was designed as an auditing tool for IT organizations but has been expanded to form the baseline framework for the IT security of many organizations. The current version, COBIT 5.0, consists of five major principles that form

[34] Department of Defense Chief Information Officer Desk Reference
[35] Symons, Craig. "IT Governance Framework."

the core of the framework. The first principle involves meeting stakeholder's needs. This process ensures that senior management has buy in for the IT alignment strategy and business needs are being assessed and met. Furthermore, it provides a tiered system that begins with enterprise goals and works its way down to IT related goals, and finally enabler goals.[36] This concept is similar to how Mission Essential Tasks are derived in the military. Utilizing this approach, IT requirements are assessed at each level of an organization from the strategic to the tactical. COBIT takes these requirements farther by assessing their achievement through the use of a balanced scorecard. [37]

Principle two, covering the enterprise end to end, provides a holistic approach for addressing governance and management of the IT organization. It joins governance requirements for the enterprise and those requirements specifically related to IT. Principle three advocates utilizing COBIT as a single and integrated framework because it has already completed integrating other frameworks into its core. Principle four is perhaps the most important aspect of COBIT, as it enables a holistic approach to IT governance. In this inclusive approach, COBIT 5 documents seven enablers that influence the success of an organization.

- Principles, policies, and frameworks
- Processes
- Organizational Structures
- Culture, ethics, and behavior

[36] COBIT 5 A Business Framework for the Governance and Management of Enterprise IT
[37] COBIT 5 A Business Framework for the Governance and Management of Enterprise IT

- Information
- Services, infrastructure, and applications
- People, skills, and competencies

These seven enablers are each associated with metrics that address how stakeholder's needs are addressed, enabler goals achieved, life cycle managed, and whether good practices are applied. [38] However, in terms of applicability to a DCO framework, these seven enablers are so diverse that even these generic metrics need to be focused on the individual enabler itself. The concluding principle involves separating governance from management. Governance involves the determination of objectives as well as the monitoring of performance. Ideally this is separated from the management function that executes those objectives.

The final benefit of the COBIT framework is the utilization of a maturity capability model to assess an organization based on attributes and various levels of achievements. Each level of achievement has a pre-determined description explaining the degree of performance required to receive a particular grade.[39] This is an improvement over the DOD CIO Cybersecurity Scorecard which merely assesses a pass/fail grade for each security metric. Additionally, this ensures a common standard amongst various governance personnel.

[38] COBIT 5 A Business Framework for the Governance and Management of Enterprise IT
[39] COBIT 5 A Business Framework for the Governance and Management of Enterprise IT

CHAPTER III

PROPOSED FRAMEWORK

A complete review of the above frameworks, concepts, and procedures identifies clear gaps in our ability to adequately assess how effective we are at Defensive Cyber Operations (DCO). Each framework stands alone measuring the performance of one aspect of DCO. For example, risk assessments and continuous monitoring programs do not specifically evaluate the performance of our users, neither do they assess our reaction time to managing an incident, nor the effectiveness of our tools.

The NIST SP 800-137 forms the most complete strategy for assessing information security activities. Specifically, it recognizes that an encompassing Information Security Continuous Monitoring Program should begin with technology, processes, procedures, operating environments, and people.[40] Using this assessment as a guide for a more specific and applicable strategy tailored to the Department of Defense (DoD), a comprehensive framework to measure the effectiveness of people, processes, defenses, and risk was developed. This framework adapts and builds on the previously discussed frameworks and strategies to produce a serviceable and practical guide for assessing DCO. The four dimensions; people, processes, defenses, and risk, were chosen as the

[40] NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

overarching concepts to be assessed in this framework because they assimilate the greatest ideas put forward in the previously reviewed chapter.

The assessment of people as a dimension is derived partly from the compliance frameworks, which assess the decision-making skills of management, as well as the incident handling frameworks that identify end users as a strength and a weakness of the DCO posture. The incident handling frameworks also identified system administrators and cyber security analysts as key players within the defense of the network.

Processes and procedures were amongst the most discussed topics within the incident handling and risk management frameworks. Yet, there were very few meaningful strategies for assessing those processes aside from their mere completion.

Defenses, as in tools and their value to an organization's defense in depth strategy, were a major focus of the compliance frameworks. Guidance was provided to implement automated solutions for the collection, aggregation, analysis, and reporting of organization-defined metrics. Additional requirements defined by the NIST cybersecurity framework included tools to support the five key functions of DCO; identify, protect, detect, respond, and recover. The Lockheed Martin Cyber Kill Chain (CKC) advocated for tools that could break the enemies process before the attacker reached actions on objective.

Risk, and an organization's ability to reduce, transfer, or accept is a key concept of the Risk Management Frameworks. An effective and continuous risk assessment is perhaps the best means to aggregate the performance of a security organization.

All four topics were considered enablers of COBIT 5. People, skills, and competencies were associated with making accurate decisions and taking remedial action. Processes were labeled as those activities that produce a set of outputs that support the achievement of IT related goals. Services, infrastructure, and applications were put forward as the tools that enable the processing of IT related goals. Finally, COBIT used information as an enabler of IT driven goals. For the purposes of this paper, the information enabler generally described in COBIT 5 has been specifically associated to risk within this framework. Again, this framework is designed to be both academic and practical in that it provides potential metrics for an organization to utilize.

People

Utilizing a tiered approach based off the previously discussed frameworks, three general categories of people were chosen for evaluation; management, analysts/administrators, and end users. Management consists of those decision makers who develop and decide on courses of action, implement policies and procedures, and purchase tools and equipment. Analysts and administrators are those employees actively defending the network. End users make up the bulk of the people that are evaluated and are perhaps the most crucial as they are the final line of defense but also the largest vulnerability.

Management

Management functions are relatively uniform throughout the strategic, operational, and tactical levels of DCO. However, the specific tasks and metrics for each task may vary. Utilizing the main functions of management identified in the Clinger-

Cohen Act, which are similar in nature to the functions described in COBIT, we can put together a matrix that assesses each function at the strategic, operational, and tactical level.

	Strategic	Operational	Tactical
Acquisition and investment	% of technologies with unfavorable ROI value at the strategic level	% of technologies with unfavorable ROI value at the operational level	% of technologies with unfavorable ROI value at the tactical level
IT Architecture	% of network actively monitored by Cyber Security Service Provider (CSSP)	% of network actively monitored by Cyber Security Service Provider (CSSP)	% of network actively monitored by Cyber Security Service Provider (CSSP).
Policy	% of policies which have not been reviewed or updated in the last two years	% of policies which have not been reviewed or updated in the last two years	% of policies which have not been reviewed or updated in the last two years
Manpower development and training	% of the cyber workforce meeting minimum levels of certification and training	% of the cyber workforce meeting minimum levels of certification and training	% of the cyber workforce meeting minimum levels of certification and training
Performance results and technology assessments	% of technologies being assessed	% of technologies being assessed	% of technologies being assessed

Figure 6. Management Metrics

Analysts/Administrators

The security workforce should be a highly trained populace. This category represents the people whose daily actions protect the network. Measuring the effectiveness of these personnel is difficult to assess. Both qualitative and quantitative measurements are required. For example, the level of training required by the DoD is provided in the Information Assurance Workforce Improvement Program (IA). Specific certifications are required for different tiers of the IA workforce. [41]A quantifiable metric that expresses the percentage of the workforce that is in compliance with this requirement demonstrates an actionable metric for assessing IT personnel. Another metric could assess the average level of training based off of certifications and degrees. While these metrics may be actionable, they do not necessarily demonstrate effectiveness. Effectiveness relates more to how well an analysts or administrator performs his/her job. In many cases analysts are assessed by how many tickets they close or how many alerts they process. This simple metric leads to quantity over quality. However, quality is difficult to quantify, thus a qualitative analysis is required. A standardized qualitative assessment of personnel by a supervisor is required.

End Users

End users are potentially the most important subject to be evaluated. An end user may be the last line of defense if a malicious email makes its way through the boundary, gateway, and enterprise defenses. End users maintain the responsibility to appropriately report these types of incidents. Also, if a spillage occurs, it is normally an end user that

[41] DoD 8570.01-M Information Assurance Workforce Improvement Program

detects the loss of confidentiality. Yet, our users are also the most vulnerable to social engineering, which cannot be adequately mitigated by automated defenses. Untrained or negligent users also create incidents when they do not operate according to regulations and standards. Non-compliance through cross domain incidents, weak passwords, and unauthorized devices compromise the strength of the DODIN. Thus to improve our end user detection capability and reduce the vulnerability associated with social engineering and non-compliance we must train our users to a high standard. Metrics associated with users must be able to identify deviations from baseline trends which may be the result of personnel moves, changes in management, or simply the amount of time since the last mandated training. Decision makers must be able to identify trends in user reported detections, cross domain violations, and social engineering compromises and provide focused, out of cycle training. The characteristics of end users do not change from the tactical to the strategic level; therefore we can develop uniform metrics for determining the effectiveness of our users.

Users as a Layer of Defense

Although users are not normally considered a layer of our defense in depth strategy, it is the user's responsibility to report social engineering attacks. Timely self-reporting by the user may decrease the incident handling life cycle. Analysts must investigate vast quantities of alerts; however, if a user reports a compromise on the system the time to detection is greatly decreased. Metrics that prove the effectiveness of our users might include:

- % of users affected by spear phishing email that reported the incident

- % of users affected by spillage that reported the incident

A more general metric for the percentage of incidents that were self-reported is not valuable because users cannot identify many incidents.

Users Vulnerability to Social Engineering

Social engineers violate inherent human trust. Metrics for determining user's vulnerability to social engineering could include:

- The % of users that clicked on a malicious link or attachment in a spear phishing message
- The % of users that visited or attempted to visit malicious sites

A useful approach to gauge the user's vulnerability to these types of threats is to develop a continuous monitoring program that incorporates the periodic assessment of users. Management can implement fake spear phishing campaigns and incorporate metrics into their overall DCO scorecard.

Users Non-Compliance

Non-compliance activity potentially exposes the DODIN to increased risk as a result of the action or inaction of users. This includes cross-domain violations, installation of unapproved software, connecting USB devices, etc. A simpler approach would be to utilize the total number of non-compliance reports. Metrics for determining the compliance of users may include:

- The number of Cross-Domain Violations
- The number of installations of unapproved software
- The number of unapproved devices connected to the DODIN

Processes

Process is a general term that can be used in many different ways. COBIT describes a process as an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT related goals.[42] Craig Simmons defines processes as making good decisions about IT. [43] Both of these definitions are correct. For the purpose of this paper, we will examine how to assess the effectiveness of an organization's processes in terms of the iterative decision process known as the OODA Loop.

Colonel John Boyd originated the OODA Loop after analyzing the superiority of American fighters in the Korean War. He hypothesized that four unique steps create a loop that characterizes each process: observe, orient decide, and act.[44] The goal of the OODA Loop is to create an environment which facilitates a more rapid execution of the loop then one's enemy or competitor. In terms of cybersecurity, the use of the OODA Loop has already been widely incorporated into theory and publications. The CJCSM 6510.10 Incident Handling Manual includes a detailed section on which incident handling processes are associated with which phases of the OODA Loop. [45]Yet there are no metrics associated with each phase of the OODA Loop to be used as part of an assessment. Furthermore, the OODA Loop's application is far greater than incident handling alone.

---

[42] COBIT 5 A Business Framework for the Governance and Management of Enterprise IT
[43] Symons, Craig. "IT Governance Framework."
[44] Enck, Robert E. "The Ooda Loop."
[45] CJCSM 6510.01B Cyber Incident Handling Program

OODA Loop for Incident Handling

CJCSM 6510.01B synchronizes the incident handling life cycle to the OODA Loop. It describes the observe phase in terms of monitoring and detecting anomalous activity. The orient phase is characterized by collecting and analyzing information about the incident. The decide phase involves course of action development and is followed by the act phase in which the course of action is executed.[46] In order to make these phases measureable, certain metrics had to be generated. Ericka Chickowski suggests two important measurements regarding the time to detection and the time to response.[47] By reducing the average time to detect in the observe phase, more time is provided to the defender in the orient and decide phase of the OODA Loop. The time to respond measures the entire OODA Loop process. Reducing the average time to respond should reduce the overall cost of incidents. These flash to bang analytics measuring the delta between incident and observation or action, provide an effective measurement of an incident response program.

[46] CJCSM 6510.01B Cyber Incident Handling Program
[47] Chickowski, Ericka. "10 Ways To Measure IT Security Program Effectiveness."

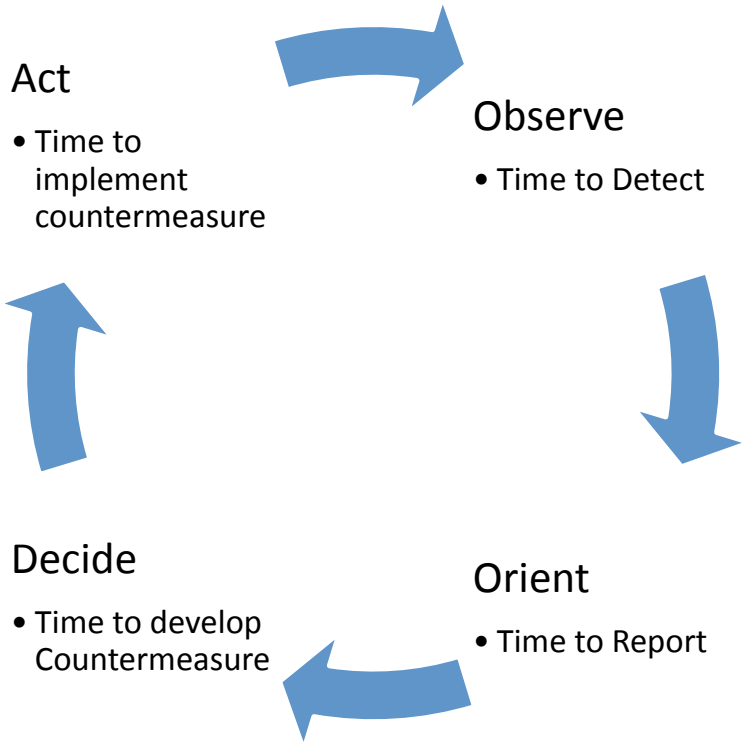


Figure 7. Incident Handling OODA Loop

OODA Loop for Overall DCO Processes

The OODA Loop is an iterative cycle that is designed to understand and improve processes. There are a lot more processes involved in DCO than incident response. The NIST Cybersecurity Framework presents five functions that cover the core cybersecurity activities; identify, protect, detect, respond, and recover. These core functions are then designed to be broken down into categories and subcategories that form the baseline

actions of cyber security.[48] Utilizing the OODA Loop, we can place these functions within the iterative cycle to assess how well we are executing DCO processes.

Figure seven illustrates the OODA Loop assessing the Vulnerability Management process. The NIST SP 800-40 *Guide to Enterprise Patch Management Technologies* defines Patch Management as "the process for identify, acquiring, installing, and verifying patches for products and systems." [49] Placing this process within the OODA Loop, we can derive several measurements to measure our reaction to patch management. This concept of the vulnerability management OODA loop is not revolutionary and has been previously discussed by the Center for Internet Security.[50] The key is to provide meaningful measurements to evaluate DODIN Ops and DCO processes like vulnerability management and incident response within the context of a decision cycle such as the OODA Loop. Within the observe phase, we measure our ability to identify the vulnerability by taking the delta between when the vulnerability was made public through security bulletins or Information Assurance Vulnerability Management (IAVM) messages and when the organization identified the vulnerability. The orient phase is focused on assessing the vulnerability within the operating environment. Here, the patch is acquired and a risk assessment is conducted. The decide phase is characterized by developing a remediation course of action and may be measured by the time to test the patch. The final phase of the patch management OODA Loop examines the patch rollout

[48] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity
[49] NIST Special Publication 800-40 Guide to Enterprise Patch Management Technologies
[50] The Cyber OODA Loop: How Your Attacker Should Help You Design Your Defense

and subsequent monitoring of the operating environment. The obvious measurement for this phase is the time it takes to implement the patch organization wide.

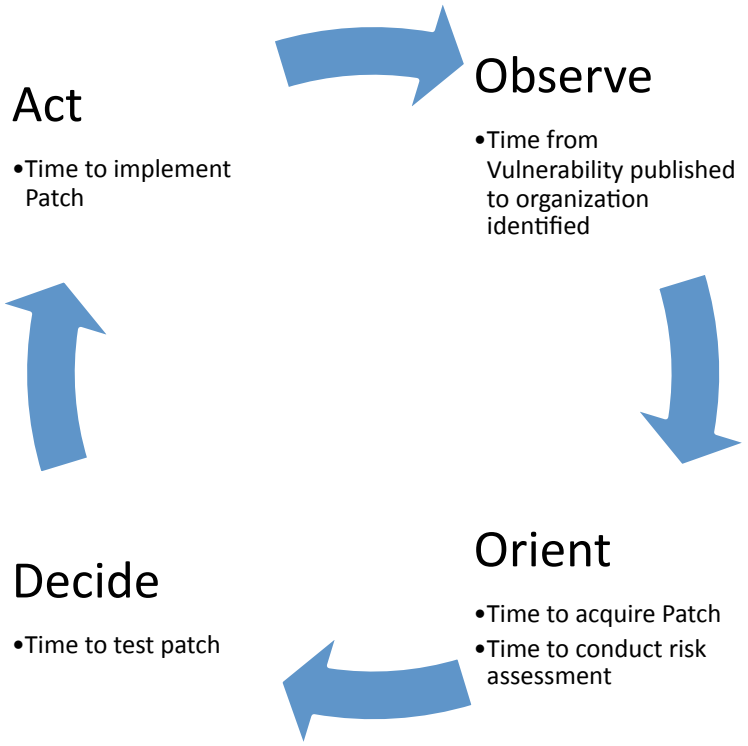


Figure 8. Vulnerability Management OODA Loop

Using the OODA Loop to Assess DCO Against Past Performance, Peers, Standards, and the Enemy

The OODA Loop has been applied to many different areas of study, from business, to medical, to the military, for which it was originally created. The design was intended to increase the speed of the entire decision making process over that of the enemy. While means have been put forward in which to measure one's own OODA Loop, comparing one's own OODA Loop to the enemies is a difficult task in terms of

cyber. This requires the defender to completely understand the actions and intent of the enemy. The Lockheed Martin CKC provides the leading theory for assessing the actions and intent of the adversary in the seven phases required for an attacker to execute actions on objective. Therefore, we can measure our OODA Loop versus the enemy's by placing the OODA Loop process within the CKC. Success equates to any time our OODA Loop executes before the enemy reaches actions on objective. However, we can show improvement in our OODA Loop by executing our defenses higher in the kill chain.

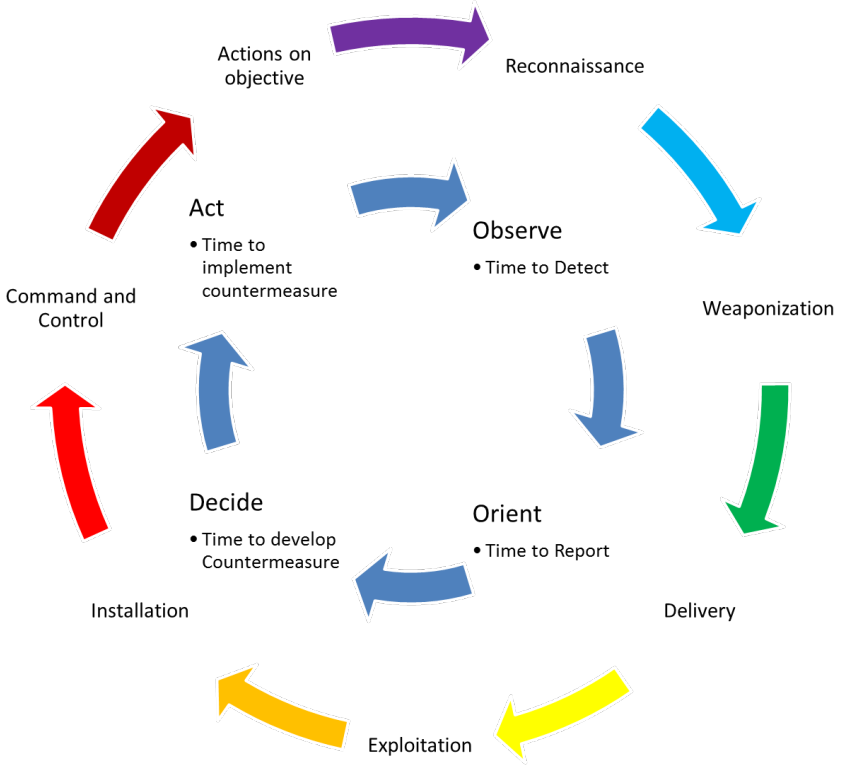


Figure 9. OODA Loop within the Context of CKC

Many of the processes required for DCO cannot be adequately assessed against an enemy. In these cases there are three options for measuring the effectiveness of a given process. The first is past performance or the demonstration of improvement or decline over time. The OODA Loop uses time as a system of measurement. For example, if management can show that they have reduced the average observe phase of a process over the last quarter from one hour to forty minutes, then this is a valid and actionable metric for our commanders. Another option is to take the metrics of the OODA Loop and assess performance against peer organizations. This option is only available if like organizations are utilizing the same measurements. For example, if one organization measures success of the observe phase of incident handling by the amount of time it takes to identify an intrusion and another measures the amount of time it takes to generate a report on an incident then the two cannot be accurately compared. Another option is to assess an organization based off of standardized criteria. Currently CJCSM 6510.01B provides certain standards for incident handling based on the type of incident, initial risk assessment, and the amount of time required to report on these incidents. However, these standardized report timelines do not encompass all aspects of the OODA Loop. Therefore, standardized metrics should be put forward based on the OODA Loop for all functions of DCO.

Defenses

Most organizations create a DCO posture that is built to support a defense in depth strategy. Various tools are used at many different layers to support this strategy.

However, most organizations do not have an effective way to measure the effectiveness of these tools or gauge their return on investment.

Figure 9 provides a crucial answer to measuring a defense in depth strategy. Utilizing the OODA loop discussed previously, tools are placed into the phase in which they execute their mission; observe, orient, decide, and act. Within each phase, tools are further broken down by the defense in depth layer in which they operate. For this purpose, the boundary layer is considered to be the region that touches both the ISP and the organization's internal network. The enterprise layer is the region in which enterprise services must pass. For example, this may be an email gateway. The third section is the regional layer. Many organizations are subdivided by regions and maintain separate security stacks of firewalls, intrusion protection systems, access control lists, etc. The final layer is the endpoint, which is protected by antivirus and host based security systems. This particular defense in depth model is only a general image of what a defense in depth posture may look like. Each organization will be different and will be required to determine which tools and which layers operate at which phase of the OODA Loop. The table below sets up the structure from which to evaluate individual incidents. It builds on the metrics discussed in the incident response processes and overlays individual tools at each layer, providing the commander with an actionable evaluation of the different tools.

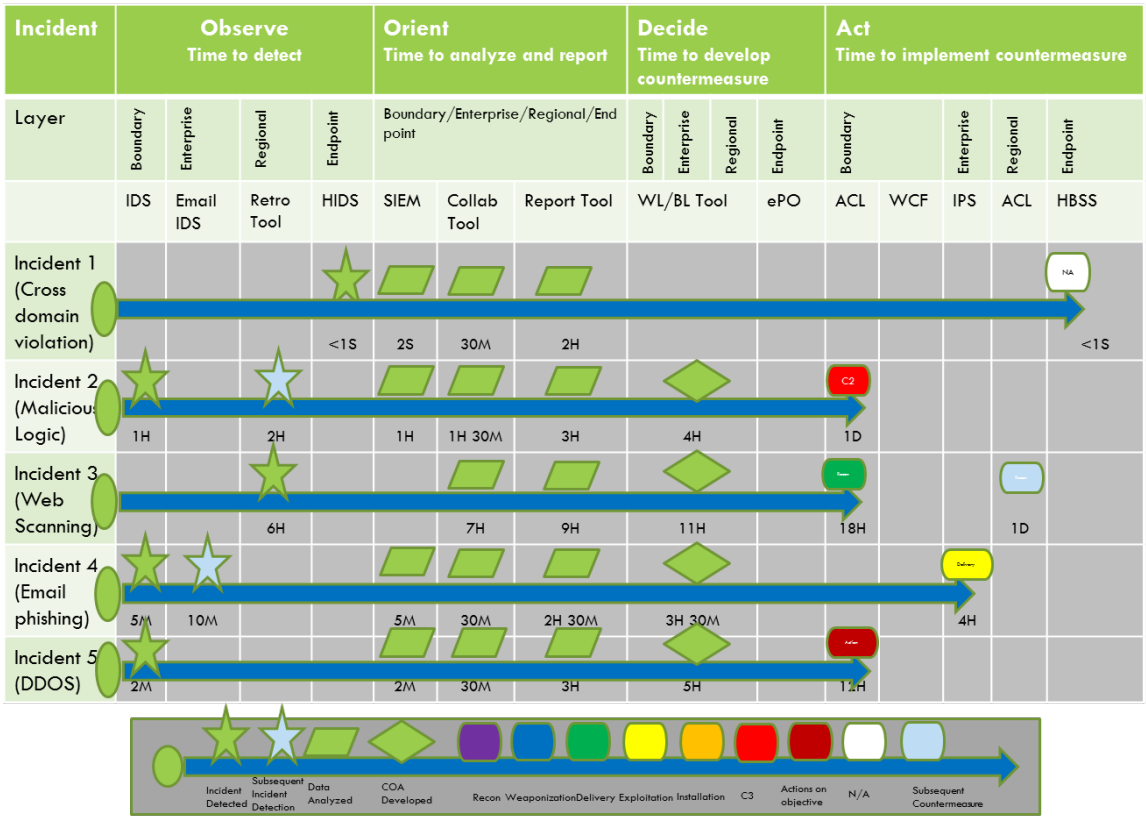


Figure 10. Defenses

There are several applications for this method of evaluation. Utilizing a similar concept proposed in Lockheed Martin's whitepaper on *The Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform*, this table provides a simple return on investment. This information can easily be aggregated for a commander to identify which tools are observing malicious traffic and which tools are not. Gaps in coverage can lead to increased investment expenditure. This concept also illustrates layers of

resiliency, depicting tools with subsequent observations of threat activity as well as tools that introduced countermeasures after the initial countermeasure was implemented. [51]

Improving on the Lockheed Martin concept, the incorporation of the OODA Loop, as well as the layered defense approach, enables leadership to clearly identify delays in the OODA Loop and prioritize investment in technologies that will decrease the time it takes to observe, orient, decide, and act in response to an intrusion. Furthermore, this process accurately pits the defender's OODA Loop against the enemy's by demonstrating at which stage of the CKC the defender was able to mitigate the attempted intrusion. Effectiveness could be measured over time by showing the defender's OODA Loop breaking the CKC in the earlier stages. In order to accurately apply this concept, data points must be automatically captured at each stage of the process to create a chronological record of when each tool was utilized and at what point in time.

Risk

Perhaps the best way to measure the overall effectiveness of an organization is to qualitatively measure the amount of risk to that particular organization. Both the NIST Risk Management Framework and the NIST Continuous Monitoring Program provide general instructions explaining how to conduct this type of assessment. Risk should be scored in a way that aggregates the risk to each system, in order to provide an overall score for an organization's collection of systems.[52] However, neither publication provides

[51] Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform, Lockheed Martin Corporation

[52] NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

a specific strategy for continuously scoring risk. In fact, SP 800-137 even suggests that it is impractical to continuously score risk in near real time, instead relying on periodic assessments. It is this paper's argument that risk must be scored in real time and must take into consideration threats and vulnerabilities as they are identified as well as safeguards that are put into place.

In order to provide realistic measurements for continuously assessing risk for all information systems, we must return to examining the formula for risk and the process involved with assessing risk. The NIST Risk Management Framework defines risk as " a measure of the extent to which an entity is threatened by a potential circumstance or event, and a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."[53] Applying this definition to a concept that enables a continuous risk assessment, we can utilize currently generated reporting with qualitatively assigned values. Figure ten illustrates this concept. Intelligence reports provide information on threats, which can be categorized by severity and tied to the vulnerabilities they exploit. Additional vulnerabilities are identified in Information Assurance Vulnerability Management bulletins and are associated with individual systems or assets. These assets are prioritized as either standard assets or task critical assets that are tied to an organization's mission essential tasks. Finally, incident reports provide the level of exposure of these assets. The product of this formula equals risk, which is then subtracted from the control gap of those countermeasures that reduce the exposure of assets, ultimately resulting in residual risk. This residual risk is then

[53] NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems

utilized as a measure of performance which can be trended over a period of time indicating an increase or decrease in the overall risk of an organization.

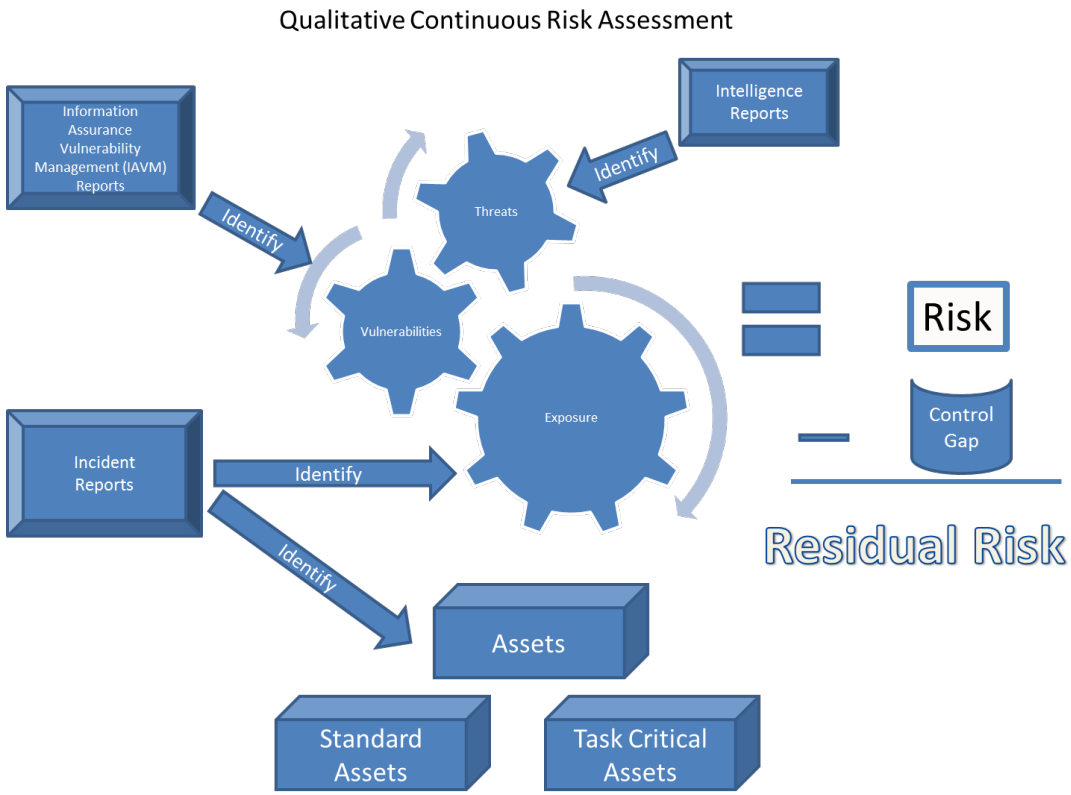


Figure 11. Qualitative Continuous Risk Assessment

CHAPTER IV

APPLYING THE DCO FRAMEWORK

People, processes, defenses, and risk make up the core components of this framework. Up to this point, the paper has provided an analysis of each of these elements as well as numerous concepts to evaluate each one. This chapter provides a specific reference for identifying the current baseline effectiveness of an organization as well as the ability to assess the change in performance over time. Specifically, it enables an organization to measure the attainment of specified goals. This process is similar to the NIST Cybersecurity Framework.

Presented are three methods for transforming the framework from an academic study to a practical implementation of the framework by modifying processes, tools, and reporting structures that are already in place. Additionally, this chapter explores potential Measures of Performance and Measures of Effectiveness tied to assessing task accomplishment and the end state of a mission.

The Framework Fundamentals

- **Elements:** The framework provides a standard of measurement that can be analyzed to determine the overall effectiveness of the core elements of DCO; People, Processes, Defenses, and Risk. These elements form the four basic building blocks that must be assessed within each organization.

- **Levels:** Each element is designed to be evaluated at different levels or tiers based upon the evaluating organizations role. Yet, the common method of evaluation designs itself to roll a single organization into an overall evaluation of all tiers.
- **Category:** Each element is subdivided into categories extending the evaluation to target specific DCO functions.
- **Ends/Ways:** Individual categories have an end state or a targeted objective called ends. Each end requires the accomplishment of certain task to achieve the endstate. These task are called ways.
- **Measure:** End states are assessed according to Measures of Effectiveness (MOEs), "a criterion used to assess changes in the behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect."[54] Ways are assessed according to Measures of Performance (MOP), "a criterion used to assess friendly actions that are tied to measuring task accomplishment."[55]

Tailoring the Framework

The process of implementing the framework requires customization on the part of the organization and supports agile development to the organization's requirements. The elements, levels, categories, ends/ways, and measures are intended to be manipulated and merely provide a baseline for an organization to build from. An organization may be tempted to remove some of the rudiments of the framework if it believes it is already

[54] Joint Operations Annex 3-0 Operations and Planning
[55] Joint Operations Annex 3-0 Operations and Planning

successfully achieving the desired outcome so that reporting structures can focus on improving gaps. However, caution should be granted, as this may leave an organization vulnerable to complacency. As new objectives are improved upon, foundational objectives may slack.

The first step to tailoring the framework entails identifying an organizations basic requirements. When building out processes, this means ensuring that all Mission Essential Tasks and Mission Essential Functions are identified. Each Mission Essential Function and Task should at a minimum be assessed by the time to completion and the level of completion, though the specific means to measure level of task completion must be further developed. The framework only identifies the most basic categories of people within an organization. During this phase of tailoring the framework, additional categories should be identified to best support the organization. This may include subcategorizing users into mission functions such as intelligence analysts, incident responders, Cyber Protection Team members, etc. Additionally, tool requirements should be identified utilizing use cases to defend against known threats.

Once the requirements are identified, an adjustment needs to be made to the scoring rubric to ensure each is accounted for and scored appropriately. This may entail modifying the levels, categories, ends and ways. Specific tool requirements may generate additional end states and objectives.

After an organization has built tailored end states and subsequent tasks to achieve those end states, it must develop MOEs and MOPs. These MOEs and MOPs should deliver a repeatable assessment metric that can be assessed against past performance,

peers, standards, and if possible the enemy. A standard metric rubric should be utilized that documents the metric with a specific identifier and describes the capability of the metric as well as how it should be applied. As discussed in previous chapters, metrics should be above all else actionable and repeatable in addition to providing situational awareness. Furthermore, metrics should be evaluated over time to identify progressing or declining trends. If standards have been developed, then the metric may be evaluated against policy, however, if no standard has been put forth then evaluation should take place against near peer organizations. Finally, in certain cases, the metric may be evaluated against the adversary.

Identifier	Definition	Characteristics			Evaluation				Use	Value
		Actionable	Situational	Repeatable	Time	Standards	Peers	Adversary		
MOE.PR.OB1	Time to detect malicious activity	X	X	X	X		X	X	Lower values are targeted Measurement is taken from the time the adversary begins the activity to the time it takes the defender to recognize it .	Provides insight into the observe phase of the defender's OODA loop and can be assessed against the adversary utilizing the Cyber Kill Chain.
MOP.PR.DT1	Amount of False Positives	X	X	X	X		X		Lower values are targeted. Measurement is the quantity of false positives over a given period of time.	Action may be taken to tune sensors and customize signatures to reduce false positives.

Figure 12. Metric Rubric

NIST SP 800-55 and MITRE's Cyber Resiliency Metrics provide examples of detailed templates for documenting and evaluating individual metrics. The table above demonstrates a basic template for documenting metrics. The MITRE example also includes a measurement scale, collection methods, data storage methods, cost associated

with collection, and supporting strategy.[56] The NIST template includes a few other characteristics such as target or threshold for achieving success and frequency of data collection and analysis.[57] These additional attributes are useful and the individual organization should decide on the level of depth necessary for their metric rubric.

The next phase should include conducting the assessment and scoring of each MOE and MOP. The specific means to measure the metric should be outlined in the metric table designed in the previous phase. The assessment phase is iterative and is designed to be continuously assessed. However, a snapshot must be taken in order provide analysis.

In the final phase of the framework, the results of the assessment are reviewed and analyzed to determine trends, areas for improvement or investment, and actionable information to support decision making. Graphs and scorecards should be utilized to provide an easily understood explanation of progressing or declining trends.

Additional Applications of the Framework

This DCO framework is intended to provide a useful and effective guide for organizations attempting to measure the effectiveness of their cybersecurity programs. Though comprehensive in nature, it is currently not postured to support wide spread adoption without the use of already existing reporting mechanisms. Current reporting mechanisms have been previously described in Chapter 2 as being limited in scope and purpose. These existing reporting mechanisms are not perfect and have been

[56] MITRE. Cyber Resiliency Metrics
[57] National Institute of Standards and Technology. Performance Measurement Guide for Information Security

implemented on top of the existing architecture as opposed to being built into the infrastructure. However, if these existing mechanisms are adapted to assess the people, processes, defenses, and risk to the organization utilizing concepts such as the OODA loop, the Cyber Kill Chain, and defense in depth within the context of Measures of Performance and Measures of Effectiveness, then they will provide an adequate assessment of the effectiveness of that organization. For example, the Continuous Monitoring and Risk Scoring (CMRS) system already provides a basic mechanism for evaluating the risk to an organization in near real time. Additional features could be included to support the assessment of certain processes, the effectiveness of tools, and to a certain extent the evaluation of users or administrators. Understandably, a single tool will likely not be able to aggregate all required evaluations, some of which may be qualitative in nature, yet it could provide a basic standardization for many of the metrics across various organizations. Likely, numerous other tools for evaluating people, processes, defenses, and risk will have to be developed. Monitoring and Reporting tools are only half of the requirement. Policy must also support the adoption of a comprehensive assessment. The DoD Cybersecurity Scorecard would be an excellent instrument for this policy, through the assimilation of additional categories of measurement as well as a more refined scoring mechanism that is not simply a binary pass or fail for each objective.

Evaluation and Justification

Due to the sensitive nature of an assessment of this magnitude on DoD systems, a trial was not feasible for incorporation into this paper. Instead this framework was

initially validated by eight industry professionals with 115 years of combined DCO experience. The evaluation was a modified Delphi type analysis with expert consensus. It was determined that two rounds of questions augmented with supplemental discussion would adequately provide expert consensus on the fitness of this framework. The eight experts that validated this paper during round one were an average age of 38 years old and held bachelors or master's degrees within the computer science or information technology fields. Additionally, they maintained an average of three industry respected information security certifications.

The initial questionnaire was developed based on research and analysis of DCO as well as the main concepts promoted throughout the paper. The questionnaire contained 33 questions distributed across the six major parts of the paper. The industry professionals were asked to evaluate each sub concept on a five-point scale from strongly disagree to strongly agree. The questionnaire was made available through the UNCG affiliated qualtrics platform, enabling respondents to answer questions securely and at their leisure. The detailed results of the evaluation are presented within Appendix B.

The second round of questions focused in on the trends identified during the initial round. For example, questions in which there was widespread agreement or disagreement of more than 75% were withdrawn from the second round, as consensus was considered achieved. Additionally, the results of the first round were made available to all the respondents. The intent was to gain consensus on the validity or invalidity of the debated concepts. This form of modified Delphi analysis has been utilized in medical

studies to identify desirable characteristics of review.[58] In total, there were eight questions in which expert consensus had not been achieved during the first round. Three of these eight questions were re-worded for clarity without losing their meaning. In total, eight respondents chose to participate in the second round, providing expert consensus and feedback aimed at the originally contested notions. However, five of the eight respondents although invited, had not participated in the first round of questions. This was perceived as a benefit as it added fresh perspectives to the consensus garnering processes. The second round of experts averaged 39 years of age, with 124 years of combined experience, and an average of 3 industry respected certifications.

Of note, there was widespread agreement on the scope of the thesis. Most prominently, all the respondents agreed on the need to develop a comprehensive framework for evaluating DCO. In terms of the points made regarding the assessment process, there was a marginal lack of consensus as to whether MOPs and MOEs are effective forms of assessments as well as the asymmetric nature of cyber warfare. Additionally, there was a significant neutral opinion on whether economy of force strategies such as the ability of machines to execute the decision process and minimize the need for human interaction should be applied.

The overwhelming majority of the respondents agreed in the second round, that economy of force strategies that expand the ability of machines to execute the decision process and minimize the need for human interaction should be applied. However, there

[58] Expert consensus on the desirable characteristics of review criteria for improvement of health care quality

was some level of reluctance to apply this logic holistically. For example, some of the experts proposed constraining machine level decision making to the most mundane tasks and broad-based threats while inserting human decision making processes against advanced persistent threats. This debate highlighted the fact that the time it takes to make a decision or complete a process should not be the only measure to evaluate success.

Disagreement also occurred when discussing the challenges associated with evaluating DCO, specifically, how commanders measure success without a framework. 25% of the respondents disagreed with the paper's analysis that assessments currently come in the form of infrequent security audits, vulnerability assessments, and penetration tests. During the second round, this question received widespread agreement and even comments on how some of the individuals had personal experience with this challenge.

Perhaps the most notable contention involved the frameworks discussed in Chapter 2 and their applicability to support a comprehensive DCO assessment. Only 50% agreed with the decision to use incident handling, compliance, governance, and risk management frameworks as a baseline. Unfortunately, during the second round, there were still notable concerns with the types of frameworks referenced to create this approach, with the concept achieving only 57% agreement. Suggestions were made to include business process analysis as well as asset management frameworks. Based on the requirements of the given organization, the framework can be tailored to assess businesses functions and asset management within the element of processes. Many of the recommended MOEs and MOPs are derived from COBIT, the NIST Risk Management Framework and subsequently the NIST Cybersecurity Framework, which takes into

consideration both business processes and asset management. Additionally, the element of People, specifically addresses acquisition and investment as well as IT architecture, key components of asset management.

The questions involving the proposed framework received widespread agreement and all concepts received at least 75% agreement. Of note, there was unanimous agreement that a comprehensive DCO framework should evaluate people, processes, defenses, and risk, the most basic concept of this paper. However, there were four questions in which 25% of the respondents either had a neutral or opposing view of a concept. Risk was perhaps the most deliberated topic of the second round discussion on the proposed framework, with respondents suggesting that the measurement for risk should take into consideration the certainty or uncertainty that an actor has knowledge of the asset. Suggestions were also made to weight each asset in terms of its criticality. This paper embraces the concept of weighting assets and measures assets as either standard or task critical. The user of this framework may wish to explore non-binary options to further weight assets by means of tiers or cost as a form of measure. There was also unanimous agreement on the suitability of utilizing a defense in depth posture that captures data points in terms of the OODA loop and the Cyber Kill Chain.

The concepts associated with applying the framework were widely accepted during Round I. As previously mentioned, this finding is particularly significant as there was unanimous agreement that a comprehensive DCO framework should evaluate people, processes, defenses, and risk, the most basic concept of this paper. This was further validated with unanimous consensus that the framework fundamentals provide a

suitable structure to assess people, processes, defenses, and risk. There was also widespread agreement on the concepts of applying the DCO framework.

Conclusion

In conclusion, there is a clear desire for a comprehensive framework that assesses the efficacy of DCO. Without the adoption of a framework there will naturally be unproductive tasking, inefficient spending and ineffective reporting. A framework should support military doctrine for assessments and frame measurements in terms of MOEs and MOPs. Additionally, it should support continuous assessments that provide actionable information to decision makers. A truly comprehensive framework assesses people, processes, defenses, and risk. Assessments should be gauged over time to demonstrate progress but also be measured against standards, peers, and the adversary. The framework should not be a static list of measurements but rather support tailoring the metrics to the organization's requirements. These metrics should be documented utilizing a standardized rubric that assesses the capability and performance of the metrics. The final results should be reviewed and analyzed to determine trends, areas for improvement or investment and actionable information to support decision making. However, current reporting mechanisms and policy must be adapted in order to capture these metrics suggested by this framework.

BIBLIOGRAPHY

Bodeau,, Deb, Rich Graubart,, Len LaPadula,, Peter Kertzner,, Arnie Rosenthal,, and Jay Brennan. Cyber Resiliency Metrics. Rep. 1st ed. Vol. 1. Bedford: MITRE, 2012. Web.

Caralli, Richard A., James F. Stevens, Lisa R. Young, and William R. Wilson. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Tech. no. CMU/SEI-2007-TR-012. Carnegie Mellon, May 2007. Web.

Chickowski, Ericka. "10 Ways To Measure IT Security Program Effectiveness." Dark Reading. N.p., 16 Mar. 2015. Web. 18 Oct. 2016.

COBIT 4.1. Rep. no. 4.1. The IT Governance Institute, 2007. Web.

COBIT 5 A Business Framework for the Governance and Management of Enterprise IT. Publication. ISACA, 2012. Web.

Dhanarani, Angeline Janet, and Deepen Chakraborty. Get Proactive: Strategies for Hardening Security with Oracle Enterprise Manager. Rep. no. CON6987. Oracle, Sept. 2016. Web.

Enck, Robert E. "The Ooda Loop." Home Health Care Management & Practice. 24.3 (2012). Web.

"FACT SHEET: Cybersecurity National Action Plan." The White House. The White House, 09 Feb. 2016. Web. 02 Sept. 2016.

Hearnshaw, H M, R M. Harker, F M. Cheater, R H. Baker, and G M. Grimshaw. "Expert Consensus on the Desirable Characteristics of Review Criteria for Improvement of Health Care Quality." Quality in Health Care. 10.3 (2001): 173-8. Web.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin, Ph.D. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Rep. N.p.: Lockheed Martin Corporation, n.d. Web.

Hutchins, Eric M. "Understanding the Cyber Kill Chain." Applying Intelligence to Computer Network Defense. Lockheed Martin. Web.

"Joint Incident Management System." Defense Information Systems Agency, n.d. Web. <http://www.disa.mil/cybersecurity/jims>.

"Marine Corps Research Topics AY 2016-2017." Marine Corps University. N.p., n.d. Web.

Sager, Tony. "The Cyber OODA Loop: How Your Attacker Should Help You Design Your Defense." The 2015 Cybersecurity Innovation Forum. NIST Computer Security Resource Center. Web

Schneider, Ralph W. A Model for Measuring Effectiveness in a Security Organization. Thesis. Naval Postgraduate School, 1976. N.p.: n.p., n.d. Defense Technical Information Center. Web.

Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform. Rep. Lockheed Martin Corporation, 2015. Web.

Smart, Steven J., Maj. "Joint Targeting in Cyberspace." Air and Space Power Journal XXV.4 (2011): n. pag. Defense Technical Information Center. Web.

Symons, Craig. "IT Governance Framework." Forrester (2005): n. pag. Mar. 2005. Web.

The White House. Office of the Press Secretary. Presidential Policy Directive -- United States Cyber Incident Coordination. Whitehouse.gov. N.p., 26 July 2016. Web.

United States. Department of Defense. Joint Staff. Joint Targeting. N.p.: n.p., n.d. 3-60. Joint Electronic Library +. Web. 20 Aug. 2016.

United States. Department of Defense. Joint Staff. Joint Operation Planning. Washington, D.C.: n.p., 2011. 5-0. Defense Technical Information Center. Web. 25 Aug. 2016.

United States. Department of Defense. Joint Staff. Cyberspace Operations. Washington, D.C.: n.p., 2013. 3-12. Defense Technical Information Center. Web.

United States. Department of Defense. Joint Warfighting Center. Commander's Handbook for Joint Battle Damage Assessment. Washington, D.C.: n.p., 2004. Defense Technical Information Center. Web.

United States. Department of Defense. CIO. DoD Cybersecurity Discipline Implementation Plan. N.p., Feb. 2016. Web.

United States. Department of Defense. Department of Defense Readiness Reporting System (DRRS). Washington, D.C.: n.p., 2015. Ser. 7730.65. Defense Technical Information Center. Web.

United States. Department of the Army. United States Army War College. Strategic Cyberspace Operations Guide. N.p.: n.p., n.d. Center for Strategic Studies. Web. 1 June 2016.

United States. Department of Defense. Chairman of the Joint Chiefs of Staff. INFORMATION ASSURANCE (IA) AND SUPPORT TO COMPUTER

NETWORK DEFENSE (CND). Washington, D.C.: n.p., 2015. 6510.01F. Defense Technical Information Center. Web.

United States. Department of Defense. Chairman of the Joint Chiefs of Staff. Cyber Incident Handling Program. N.p.: n.p., 2014. CJCSM 6510.01B. Defense Technical Information Center. Web.

United States. Department of Defense. DOD CIO. Cybersecurity. Washington, D.C.: n.p., 2014. Ser. 8500.01. Defense Technical Information Center. Web.

United States. Department of Commerce. National Institute of Standards and Technology. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Gaithersburg: n.p., 2011. 800-137. Web.

United States. Department of Defense. CIO. DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER DESK REFERENCE. N.p., Aug. 2006. Web.

United States. Department of Commerce. National Institute of Standards and Technology. Guide for Applying the Risk Management Framework to Federal Information Systems. Vol. 800-37. Gaithersburg: n.p., 2010. National Institute of Standards and Technology. Web.

United States. Department of Commerce. National Institute of Standards and Technology. Guide to Enterprise Patch Management Technologies. Vol. NIST Special Publication 800-40. Gaithersburg: National Institute of Standards and Technology, 2013. Web.

United States. Department Commerce. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. N.p.: n.p., 2014. Web.

United States. Department of Defense. Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. Information Assurance Workforce Improvement Program. Vol. DoD 8570.01-M. N.p.: n.p., 2015. Defense Technical Information Center. Web.

United States. Department of Defense. Department of the Navy. Marine Corps Doctrinal Publication 1-3 Tactics. Washington, D.C.: United States Marine Corps, 1997. Web.

United States. Department of Defense. Chairman of the Joint Chiefs of Staff. Joint Operations Annex 3-0 Operations and Planning. N.p.: n.p., n.d. Web.

United States. Department of Commerce. National Institute of Standards and Technology. Report on Securing and Growing the Digital Economy. Commission on Enhancing National Cybersecurity, 1 Dec. 2016. Web.

United States. Department of Commerce. National Institute of Standards and Technology. SP 800-55 Performance Measurement Guide for Information Security. N.p., n.d. Web.

United States. Department of Commerce. National Institute Standards and Technology. Security and Privacy Controls for Federal Information Systems and Organizations. 4th ed. Gaithersburg: n.p., 2015. 800-53. Web.

Warfighting. Washington, D.C.: U.S. Marine Corps, 1997. www.marines.mil. Web.

Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations." Joint Forces Quarterly 2nd Quarter 73 (2014): n. pag. National Defense University Press. Web. 29 May 2016. <http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-73/Article/577499/the-joint-force-commanders-guide-to-cyberspace-operations/>.

Wynn, Jackson, Joseph Whitmore, Geoff Upton, Lindsay Spriggs, Dan McKinnon, Richard McInnes, Richard Graubart, and Lauren Clausen. "Threat Assessment and Risk Analysis." (2016): n. pag. MITRE, Oct. 2011. Web.

APPENDIX A

FRAMEWORK SCORING

This appendix provides the central integrity of the framework for evaluating the success of an organization. The below tables provide the elements, levels, categories, ends/ways, and measurements for assessing DCO. It represents a baseline concept for assessments and is designed to be tailored and customized to an individual organization.

Table 1. People Scoring

The element People is scored at the strategic, operational, and tactical levels. However, many of the tasks at one level are similar to the tasks at other levels. The categories for people are broken down into Management, Analyst and Administrators, and Users. Specific end states are assigned to each category. The end states for management involve improvements in acquisition and investment, IT architecture, policy, manpower development and training, and finally assessments. Analysts and administrators are to be assessed on improvement of their skills and certifications as well as their compliance to policies and standards, and their aptitude for detecting and reporting incidents. Finally, users are assessed on their compliance and resistance to social engineering as well as their ability to detect and report incidents. Specific means for accomplishing each end state are provided with a corresponding MOE/MOP.

Table 1. People Scoring

Element: People					
Level	**Measure**	**Category**	**Ends/Ways**	**MOE/MOP #1**	**MOE/MOP #2**
Strategic	MOE	Management	Improve Acquisition and investment	Amount of Return on Investment	Amount of requirements not being met
			Improve IT Architecture	Amount of IT Architecture improvement	Percent increase in network being monitored
			Improve Policy	Amount of Policies that need to be reviewed	Frequency of policy audits
			Improve Manpower Development and Training	Amount of training sessions held per quarter	Amount of training resources available
			Improve Assessments	Percent of assessments that target Task Critical Assets	Percent of assessments that support Mission Essential Functions
		Administrators Analysts	Improve Skills/Certification	Percent of unqualified employees per 8570 requirements	Percentage of privledged workforce that has received specialized training
			Improve Detection/Reporting	Percent of incidents that are identifed through hunting	Number of incident reports that provide actionable indicators
			Improve Compliance	Amount of privledged user non-compliance reports	Amount of Operations Security Violations
		Users	Improve Compliance	Amount of user non-compliance reports	Amount of Operations Security Violations
			Improve Detection/Reporting	Amount of users that report incidents	Percent of users that delete malicious messages or files
	MOP	Management	Improve implementation of Acquisition and Investment	Percent of projects on schedule	Percent of projects on budget
			Improve Security Posture of IT Architecture	Percent of Architecture that is defended by CSSP	Percent of network traffic that is encrypted
			Update Policies	Percent of Policies that are more than 2 years old	Percent of policies that have been reviewed in the last year
			Conduct Training	Percent of workforce that completed annual training	Percent of workforce that received specailized training
			Provide comprehensive assessments	Percent of network that underwent CCRI.	Amount of assessments that measure people, processes, defenses, and risk
		Administrators Analysts	Improve education	Average number of CEUs	Average level of higher education
			Improve reporting process	Average time to release report	Average time to close report
			Improve privledged user behavior	Amount of privledged users that click on phishing emails	Amount of privledged users that attempt to install unapproved software or hardware
		Users	Improve user behavior	Amount of users that click on phishing emails	Amount of users that attempt to install unapproved software or hardware
			Improve user reporting	Amount of incidents that are user reported	Time to report suspicious incident
Operational	MOE	Management	Improve Acquisition and investment	Amount of Return on Investment	Amount of requirements not being met
			Improve IT Architecture	Amount of IT Architecture improvement	Percent increase in network being monitored
			Improve Policy	Amount of Policies that need to be reviewed	Frequency of policy audits
			Improve Manpower Development and Training	Amount of training sessions held per quarter	Amount of training resources available
			Improve Assessments	Percent of assessments that target Task Critical Assets	Percent of assessments that support Mission Essential Functions
		Administrators Analysts	Improve Skills/Certification	Percent of unqualified employees per 8570 requirements	Percentage of privledged workforce that has received specialized training
			Improve Detection/Reporting	Percent of incidents that are identifed through hunting	Number of incident reports that provide actionable indicators
			Improve Compliance	Amount of privledged user non-compliance reports	Amount of Operations Security Violations
		Users	Improve Compliance	Amount of user non-compliance reports	Amount of Operations Security Violations
			Improve Detection/Reporting	Amount of users that report incidents	Percent of users that delete malicious messages or files
	MOP	Management	Improve implementation of Acquisition and Investment	Percent of projects on schedule	Percent of projects on budget
			Improve Security Posture of IT Architecture	Percent of Architecture that is defended by CSSP	Percent of network traffic that is encrypted
			Update Policies	Percent of Policies that are more than 2 years old	Percent of policies that have been reviewed in the last year
			Conduct Training	Percent of workforce that completed annual training	Percent of workforce that received specailized training
			Provide comprehensive assessments	Percent of network that underwent CCRI.	Amount of assessments that measure people, processes, defenses, and risk
		Administrators Analysts	Improve education	Average number of CEUs	Average level of higher education
			Improve reporting process	Average time to release report	Average time to close report
			Improve privledged user behavior	Amount of privledged users that click on phishing emails	Amount of privledged users that attempt to install unapproved software or hardware
		Users	Improve user behavior	Amount of users that click on phishing emails	Amount of users that attempt to install unapproved software or hardware
			Improve user reporting	Amount of incidents that are user reported	Time to report suspicious incident
Tactical	MOE	Management	Improve Acquisition and investment	Amount of Return on Investment	Amount of requirements not being met
			Improve IT Architecture	Amount of IT Architecture improvement	Percent increase in network being monitored
			Improve Policy	Amount of Policies that need to be reviewed	Frequency of policy audits
			Improve Manpower Development and Training	Amount of training sessions held per quarter	Amount of training resources available
			Improve Assessments	Percent of assessments that target Task Critical Assets	Percent of assessments that support Mission Essential Functions
		Administrators Analysts	Improve Skills/Certification	Percent of unqualified employees per 8570 requirements	Percentage of privledged workforce that has received specialized training
			Improve Detection/Reporting	Percent of incidents that are identifed through hunting	Number of incident reports that provide actionable indicators
			Improve Compliance	Amount of privledged user non-compliance reports	Amount of Operations Security Violations
		Users	Improve Compliance	Amount of user non-compliance reports	Amount of Operations Security Violations
			Improve Detection/Reporting	Amount of users that report incidents	Percent of users that delete malicious messages or files
	MOP	Management	Improve implementation of Acquisition and Investment	Percent of projects on schedule	Percent of projects on budget
			Improve Security Posture of IT Architecture	Percent of Architecture that is defended by CSSP	Percent of network traffic that is encrypted
			Update Policies	Percent of Policies that are more than 2 years old	Percent of policies that have been reviewed in the last year
			Conduct Training	Percent of workforce that completed annual training	Percent of workforce that received specailized training
			Provide comprehensive assessments	Percent of network that underwent CCRI.	Amount of assessments that measure people, processes, defenses, and risk
		Administrators Analysts	Improve education	Average number of CEUs	Average level of higher education
			Improve reporting process	Average time to release report	Average time to close report
			Improve privledged user behavior	Amount of privledged users that click on phishing emails	Amount of privledged users that attempt to install unapproved software or hardware
		Users	Improve user behavior	Amount of users that click on phishing emails	Amount of users that attempt to install unapproved software or hardware
			Improve user reporting	Amount of incidents that are user reported	Time to report suspicious incident

Table 2. Process Scoring

The Process Scoring table replaces levels with the OODA loop and incorporates the five categories of the NIST Cybersecurity Framework; Identify, Protect, Detect, Respond, and Recover. In this way, the framework incorporates the functions, categories, and subcategories presented in the NIST Cybersecurity Framework (blue)[59] and expands upon the NIST framework by tailoring specific DCO end states and objectives (red) within the context of the OODA loop. Furthermore, the process scoring table measures each MOE and MOP individually, assessing the time to complete each objective within the framework of the OODA loop and the level of completion. NIST Special Publication 800-55 describes these forms of metrics as measures of effectiveness and efficiency. [60]

[59] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity

[60] National Institute of Standards and Technology. Performance Measurement Guide for Information Security

Table 2. Process Scoring

			Element: Processes		
Level	Measure	Category	Ends/Ways	MOE/MOP #1	MOE/MOP #2
Observe	MOE	Identify	Asset Management (ID.AM)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Business Environment (ID.BE)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Governance (ID.GV)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Risk Assessment (ID.RA)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Management (ID.MA)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Intelligence (ID.IN)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Protect	Access Control (PR.AC)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Awareness and Training (PR.AT)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Information Protection Processes and Procedures (PR.IP)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Detect	Anomalies and Events (DE.AE)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Security Continious Monitoring (DE.CM)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Respond	Analysis (RS.AN)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Improvements (RS.IM)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Recover	Improvements (RC.IM)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
	MOP	Identify	ID.AM-1: Physical devices and systems within the organization are inventoried	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.AM-2: Software platforms and applications within the organization are inventoried	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.BE-1: The organization's role in the supply chain is identified and communicated	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.GV-1: Organizational information security policy is established	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.RA-1: Asset vulnerabilities are identified and documented	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.MA-1: Task Critical Assets are identified (ID.TA)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.MA-2: Mission Essential Tasks are identified (ID.MT)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.MA-3: Commander's Critical Information Requirements are identified (ID.IR)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.IN-1: Monitor cyberspace activity	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Protect	PR.AC-1: Identities and credentials are managed for authorized devices and users	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.AT-1: All users are informed and trained	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Detect	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM-1: The network is monitored to detect potential cybersecurity events	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM-4: Malicious code is detected	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM-5: Unauthorized mobile code is detected	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM-8: Vulnerability scans are performed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM-9: Sensor requirements established	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM-10: Sensor grid configured	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM-11: Sensor data collected	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM-12: Compliance scans are performed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Respond	RS.AN-1: Notifications from detection systems are investigated	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RS.IM-1: Response plans incorporate lessons learned	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Recover	RC.IM-1: Recovery plans incorporate lessons learned	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
Orient	MOE	Identify	Asset Management (ID.AM)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Business Environment (ID.BE)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Governance (ID.GV)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Risk Assessment (ID.RA)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Risk Management Strategy (ID.RM)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Intelligence (ID.IN)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Management (ID.MA)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Protect	Awareness and Training (PR.AT)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Information Protection Processes and Procedures (PR.IP):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Protective Technology (PR.PT):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Prevent (PR.PV)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Detect	Security Continuous Monitoring (DE.CM):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Anomalies and Events (DE.AE):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Detection Processes (DE.DP)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Respond	Response Planning (RS.RP):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Communications (RS.CO):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Analysis (RS.AN):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Improvements (RS.IM):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Recover	Improvements (RC.IM)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Communications (RC.CO):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
	MOP	Identify	ID.AM-3: Organizational communication and data flows are mapped	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.AM-4: External information systems are catalogued	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.RA-4: Potential business impacts and likelihoods are identified	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.IN -2: Conduct threat fusion and correlation	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.IN-3: Cyber trends identified	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.MA-4: Conduct impact assessment	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Protect	PR.AT-2: Privileged users understand roles & responsibilities	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.AT-4: Senior executives understand roles & responsibilities	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.AT-5: Physical and information security personnel understand roles & responsibilities	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.PV-1: Threat signatures developed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Detect	DE.AE-2: Detected events are analyzed to understand attack targets and methods	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.DP-4: Event detection information is communicated to appropriate parties	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM-13Threat signatures developed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Respond	RS.RP-1: Response plan is executed during or after an event	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RS.CO-1: Personnel know their roles and order of operations when a response is needed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RS.CO-2: Events are reported consistent with established criteria	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RS.CO-3: Information is shared consistent with response plans	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RS.CO-4: Coordination with stakeholders occurs consistent with response plans	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RS.AN-2: The impact of the incident is understood	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RS.AN-3: Forensics are performed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RS.IM-2: Response strategies are updated	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Recover	RC.IM-2: Recovery strategies are updated	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion

Decide	MOE	Identify	Business Environment (ID.BE):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Governance (ID.GV):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Risk Assessment (ID.RA)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Risk Management Strategy (ID.RM):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Inteligence (ID.IN)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Management (ID.MA)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Protect	Information Protection Processes and Procedures (PR.IP):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Detect	Anomalies and Events (DE.AE):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Security Continuous Monitoring (DE.CM):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Respond	Analysis (RS.AN):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Mitigation (RS.MI):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Recover	Communications (RC.CO):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
	MOP	Identify	ID.BE-5: Resilience requirements to support delivery of critical services are established	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.RM-2: Organizational risk tolerance is determined and clearly expressed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.IN-4:Threat actor attribution conducted	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.MA-5: Review and recommend course of action	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Protect	PR.IP-2: A System Development Life Cycle to manage systemsis implemented	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.IP-3: Configuration change control processes are in place	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.IP-7: Protection processes are continuously improved	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Detect	DE.AE-4: Impact of events is determined	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.AE-5: Incident alert thresholds are established	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.DP-5: Detection processes are continuously improved	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.AE -6: Conduct hunt mission	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.CM- 14:Threat signatures implemented	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Respond	RS.AN-4: Incidents are categorized consistent with response plans	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RS.MI-1: Incidents are contained	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Recover	RC.CO-1: Public relations are managed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
Act	MOE	Identify	Asset Management (ID.AM):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Governance (ID.GV):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Risk Assessment (ID.RA):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Risk Management Strategy (ID.RM):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Inteligence (ID.IN)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Management (ID.MA)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Protect	Access Control (PR.AC):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Data Security (PR.DS):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Information Protection Processes and Procedures (PR.IP):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Maintenance (PR.MA):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Prevent (PR.PV)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Detect	Protective Technology (PR.PT):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Detection Processes (DE.DP):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Respond	Mitigation (RS.MI):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Recover	Recovery Planning (RC.RP):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Communications (RC.CO):	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			Compliance (RS.CM)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
	MOP	Identify	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.GV-4: Governance and risk management processes address cybersecurity risks	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.RA-6: Risk responses are identified and prioritized	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.IN-5:Battle Damage Assessment executed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.MA-6:Implement Cyber Condition	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.MA-7:Task DCO forces	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			ID.MA-8:Publish Order	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Protect	PR.AC-2: Physical access to assets is managed and protected	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.AC-3: Remote access is managed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.DS-1: Data-at-rest is protected	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.DS-2: Data-in-transit is protected	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.DS-4: Adequate capacity to ensure availability is maintained	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.DS-5: Protections against data leaks are implemented	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.DS-7: The development and testing environment(s) are separate from the production environment	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.IP-6: Data is destroyed according to policy	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.IP-12: A vulnerability management plan is developed and implemented	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.PT-2: Removable media is protected and its use restricted according to policy	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.PT-4: Communications and control networks are protected	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			PR.PV-1: Implement indicators and signatures for blocking (ACL, IPS, HBSS)	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Detect	DE.DP-2: Detection activities comply with all applicable requirements	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			DE.DP-3: Detection processes are tested	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Respond	RS.MI-2: Incidents are mitigated	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
		Recover	RC.RP-1: Recovery plan is executed during or after an event	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RC.CO-2: Reputation after an event is repaired	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion
			RS.CM-1: Software patches are implemented	Time to complete objective (Observe, Orient, Decide, Act)	Level of completion

Table 3. Defense Scoring

Defense scoring utilizes the logical placement of tools according to a defense in depth layers as levels. This approach measures the effectiveness of defenses in categories of Processes, Resilience, Strength, and Return on Investment. The effectiveness of the defense processes returns measurements to the OODA loop, referencing the time it takes for sensors and tools to detect, analyze, develop mitigations, and implement countermeasures. Resilience is assessed in terms of the redundant nature of the defenses and where strength is the overall success the defense in the reduction of incidents. Return on investment observes the capability of tools in comparison to the cost of the tools. This analysis provides a comprehensive assessment of the effectiveness of an organizations Defenses.

Table 3. Defense Scoring

Element: Defenses					
Level	Measure	Category	Ends/Ways	MOE/MOP #1	MOE/MOP #2
Boundary	MOE	Process	Improve Observervation	Time to detect	Amount of attacks detected at boundary
			Improve Orientation	Time to analyze	Time to report
			Improve Decisions	Time to develop countermeasure	Percent of tools that can develop countermeasure without human interaction
			Improve Action	Time to implement Countermeasure	Percent of tools that can implement countermeasure without human interaction
		Resiliance	Improve Resiliance	Number incidents that would have been mitigated with multiple tools	Number of incidents that are detected with multiple tools
		Strength	Improve Strength	Amount of incidents	Amount of events that were mitigated at the boundary
		Return on Investment	Improve Return on Investment	Cost of tools and maintenance	Cost of incidents
	MOP	Process	Improve detection accuracy	Amount of False Positives	Amount of False Negatives
			Improve analyzing	Level of analysis	Amount of actionable indicators identified
			Improve mitigation development	Percent of signatures that are implemented on multiple tools	Percent of signatures that are not tied to a domain or IP.
			Improve mitigation execution	Number of events that are blocked by mitigation control	Percent of mitigation controls that have adverse affect on the network
		Resiliance	Improve Redundancy	Amount of redundant capabilities	Percent of boundary being monitored
		Strength	Improve Success	Amount of incidents that achieved success per CKC	Time between incidents
		Return on Investment	Improve Return on Investment	Percent of tools that fufill multiple usecases	Percent of tools that are opensource
Enterprise	MOE	Process	Improve Observervation	Time to detect	Amount of attacks detected at boundary
			Improve Orientation	Time to analyze	Time to report
			Improve Decisions	Time to develop countermeasure	Percent of tools that can develop countermeasure without human interaction
			Improve Action	Time to implement Countermeasure	Percent of tools that can implement countermeasure without human interaction
		Resiliance	Improve Resiliance	Number incidents that would have been mitigated with multiple tools	Number of incidents that are detected with multiple tools
		Strength	Improve Strength	Amount of incidents	Amount of events that were mitigated at the boundary
		Return on Investment	Improve Return on Investment	Cost of tools and maintenance	Cost of incidents
	MOP	Process	Improve detection accuracy	Amount of False Positives	Amount of False Negatives
			Improve analyzing	Level of analysis	Amount of actionable indicators identified
			Improve mitigation development	Percent of signatures that are implemented on multiple tools	Percent of signatures that are not tied to a domain or IP.
			Improve mitigation execution	Number of events that are blocked by mitigation control	Percent of mitigation controls that have adverse affect on the network
		Resiliance	Improve Redundancy	Amount of redundant capabilities	Percent of boundary being monitored
		Strength	Improve Success	Amount of incidents that achieved success per CKC	Time between incidents
		Return on Investment	Improve Return on Investment	Percent of tools that fufill multiple usecases	Percent of tools that are opensource
Regional	MOE	Process	Improve Observervation	Time to detect	Amount of attacks detected at boundary
			Improve Orientation	Time to analyze	Time to report
			Improve Decisions	Time to develop countermeasure	Percent of tools that can develop countermeasure without human interaction
			Improve Action	Time to implement Countermeasure	Percent of tools that can implement countermeasure without human interaction
		Resiliance	Improve Resiliance	Number incidents that would have been mitigated with multiple tools	Number of incidents that are detected with multiple tools
		Strength	Improve Strength	Amount of incidents	Amount of events that were mitigated at the boundary
		Return on Investment	Improve Return on Investment	Cost of tools and maintenance	Cost of incidents
	MOP	Process	Improve detection accuracy	Amount of False Positives	Amount of False Negatives
			Improve analyzing	Level of analysis	Amount of actionable indicators identified
			Improve mitigation development	Percent of signatures that are implemented on multiple tools	Percent of signatures that are not tied to a domain or IP.
			Improve mitigation execution	Number of events that are blocked by mitigation control	Percent of mitigation controls that have adverse affect on the network
		Resiliance	Improve Redundancy	Amount of redundant capabilities	Percent of boundary being monitored
		Strength	Improve Success	Amount of incidents that achieved success per CKC	Time between incidents
		Return on Investment	Improve Return on Investment	Percent of tools that fufill multiple usecases	Percent of tools that are opensource
Endpoint	MOE	Process	Improve Observervation	Time to detect	Amount of attacks detected at boundary
			Improve Orientation	Time to analyze	Time to report
			Improve Decisions	Time to develop countermeasure	Percent of tools that can develop countermeasure without human interaction
			Improve Action	Time to implement Countermeasure	Percent of tools that can implement countermeasure without human interaction
		Resiliance	Improve Resiliance	Number incidents that would have been mitigated with multiple tools	Number of incidents that are detected with multiple tools
		Strength	Improve Strength	Amount of incidents	Amount of events that were mitigated at the boundary
		Return on Investment	Improve Return on Investment	Cost of tools and maintenance	Cost of incidents
	MOP	Process	Improve detection accuracy	Amount of False Positives	Amount of False Negatives
			Improve analyzing	Level of analysis	Amount of actionable indicators identified
			Improve mitigation development	Percent of signatures that are implemented on multiple tools	Percent of signatures that are not tied to a domain or IP.
			Improve mitigation execution	Number of events that are blocked by mitigation control	Percent of mitigation controls that have adverse affect on the network
		Resiliance	Improve Redundancy	Amount of redundant capabilities	Percent of boundary being monitored
		Strength	Improve Success	Amount of incidents that achieved success per CKC	Time between incidents
		Return on Investment	Improve Return on Investment	Percent of tools that fufill multiple usecases	Percent of tools that are opensource

Table 4. Risk Scoring

The table for risk scoring is rather simple. The levels, categories, ends, means, and MOPs/MOEs are straightforward. At each level the objective is to reduce risk which is accomplished by implementing controls. The measurement is simply the amount of risk before and after controls are put into place. However, determining a value for risk is exceedingly difficult. Each organization must develop a quantitative or qualitative process for achieving this value. In chapter 3, a method was presented to continuously assess risk in near real time by identifying threats, vulnerabilities, and exposure of assets with qualitatively assigned values and subtracting this value from the control gap, providing the residual risk value.

Table 4. Risk Scoring

Element: Risk				
Level	**Measure**	**Category**	**Ends/Ways**	**MOE/MOP #1**
Strategic	MOP	Risk	Reduce Risk	Amount of Risk
	MOE	Risk	Implement Controls	Amount of Residual Risk
Operational	MOP	Risk	Reduce Risk	Amount of Risk
	MOE	Risk	Implement Controls	Amount of Residual Risk
Tactical	MOP	Risk	Reduce Risk	Amount of Risk
	MOE	Risk	Implement Controls	Amount of Residual Risk

APPENDIX B

EVALUATION FORM

As part of my Master's thesis at the University of North Carolina at Greensboro, I am conducting a survey to validate the ideas and concepts put forward in my thesis. Any information obtained in connection with this study will remain confidential and only be associated to an anonymous industry professional.

Professional's Details:

Name: _____ Age: _____ Years of experience within industry: _____

Education: _____ Certifications: _____

Strongly Disagree (**1**)	Disagree (**2**)	Neutral (**3**)	Agree (**4**)	Strongly Agree (**5**)

Questions	(1)	(2)	(3)	(4)	(5)	Comments
Scope						
There is a need to develop a comprehensive framework for evaluating DCO.						
Without a comprehensive framework for evaluating DCO there will be unproductive tasking, inefficient spending and ineffective reporting.						
DODIN Ops and DCO are inherently interconnected and should be evaluated utilizing the same overarching framework.						
Assessments						
The assessment process should be continuous in nature.						
Assessments should be planned prior to the engineering of our networks, the establishment of sensor grids, and the employment of internal defensive measures.						
Metrics should provide an effective assessment at all three levels of warfare.						
MOPs and MOEs are effective forms of assessments.						
Assessments are especially effective if they incorporate both quantitative and qualitative						

analysis.						
Metrics vary in scale and purpose from situational awareness to actionable information.						
Defensive Cyber Operations as well as Offensive Cyber Operations are both symmetric as well as asymmetric.						
When possible, we should attempt to utilize the asymmetric capabilities of DCO and assess the effectiveness of these capabilities.						
Resources such as financial capital, processing power, and human resources assist an organization in gaining the asymmetric advantage within the cyber domain.						
Economy of force strategies should be applied that expand the ability of machines to execute the decision process and minimize the need for human interaction.						
Current Framework Challenges						
DoD doctrine often separates the functional nature of cyber security into compliance and network hardening (DODIN Ops) and hunting and response actions (DCO-IDM). This fractional method of evaluating DCO as a partial concept means that we are not providing the commander with an adequate representation of how our conceptual shield is prepared for enemy engagement.						
The DODIN is a disparate network of networks, operated by many services and agencies. This mesh has created an incongruent reporting structure that is not only difficult to defend, but near impossible to assess.						
Without a framework to continuously evaluate DCO as a whole of effort, commander's resort to infrequent security audits, vulnerability assessments, and penetration test.						
Frameworks						
A literature review of Incident handling, compliance, governance and risk management frameworks provides a satisfactory baseline to support a comprehensive DCO assessment.						
Proposed Framework						
A comprehensive DCO framework should						

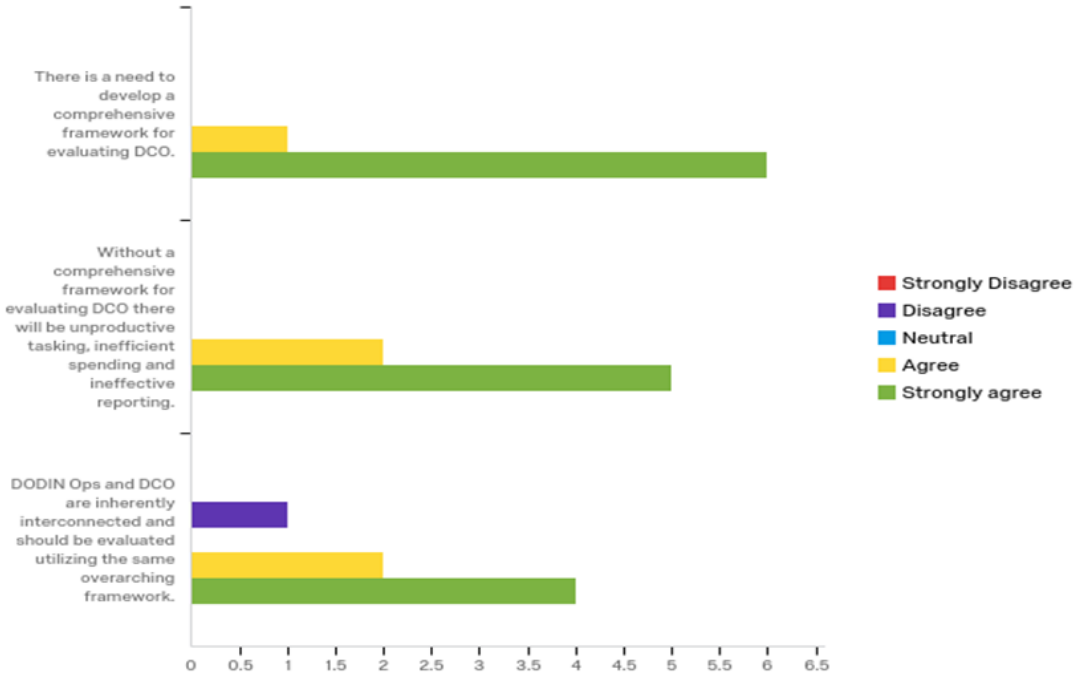
evaluate people, processes, defenses, and risk.						
People should be measured in terms of management, analysts/administrators, and users.						
Management should be evaluated in terms of acquisition and investment, IT architecture, policy, manpower development and training, and performance results and technology assessments.						
Qualitative performance assessments of analysts/administrators can be more effective then quantitative assessments.						
End users should be evaluated as a layer of defense and as a vulnerability.						
The OODA loop is an effective form of assessment for processes.						
The OODA loop within the context of the Cyber Kill Chain provides a means to assess our incident handling processes versus the adversary.						
Utilizing a defense in depth posture that captures data points in terms of the OODA loop and Cyber Kill Chain assesses effectiveness, resilience, and return on investment.						
Risk should be scored in a way that aggregates the risk to each system to provide an overall score for an organization's collection of systems.						
Risk must be scored in real time and must take into consideration threats and vulnerabilities as they are identified as well as safeguards that are put into place.						
Residual risk should be utilized as a measure of performance.						
Applying the DCO Framework						
The framework fundamentals provide a suitable structure to assess people, processes, defenses, and risk.						
The process to tailor the framework to an organizations specific needs supports agility and does not limit an organization to a simple set of metrics.						
A standard metric rubric should be utilized that						

documents the metric with a specific identifier and describes the capability of the metric as well as how it should be applied.						
Metrics should be above all else actionable and repeatable in addition to being situational.						
Metrics should be evaluated over time, and against standards, peers, and when possible the adversary.						
Assessments should be reviewed and analyzed to determine trends, areas for improvement or investment, and actionable information to support decision making.						
Current reporting mechanisms and policy must be adapted in order to capture the metrics suggested by this framework.						

APPENDIX C

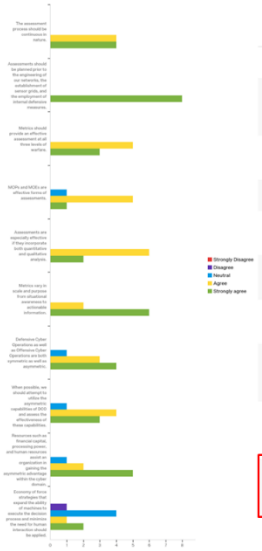
EVALUATION REPORT

Round I Expert Consensus: Scope



#	Field	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree	Total
1	There is a need to develop a comprehensive framework for evaluating DCO.	0.00% 0	0.00% 0	0.00% 0	14.29% 1	85.71% 6	7
2	Without a comprehensive framework for evaluating DCO there will be unproductive tasking, inefficient spending and ineffective reporting.	0.00% 0	0.00% 0	0.00% 0	28.57% 2	71.43% 5	7
3	DODIN Ops and DCO are inherently interconnected and should be evaluated utilizing the same overarching framework.	0.00% 0	14.29% 1	0.00% 0	28.57% 2	57.14% 4	7

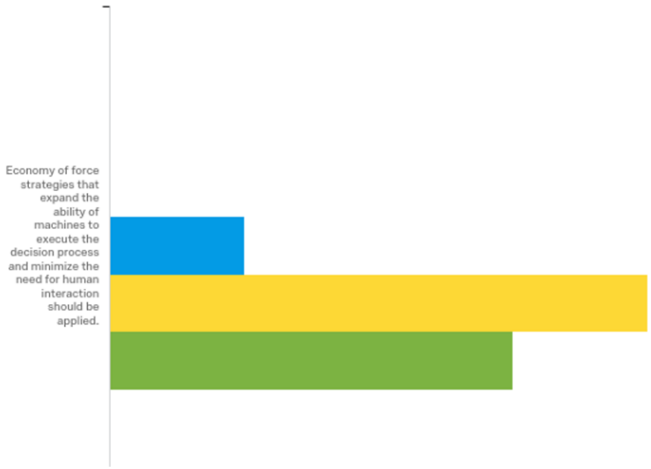
Round I Expert Consensus: Assessments



#	Field	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree	Total
1	The assessment process should be continuous in nature.	0.00% 0	0.00% 0	0.00% 0	50.00% 4	50.00% 4	8
2	Assessments should be planned prior to the engineering of our networks, the establishment of sensor grids, and the employment of internal defensive measures.	0.00% 0	0.00% 0	0.00% 0	0.00% 0	100.00% 8	8
3	Metrics should provide an effective assessment at all three levels of warfare.	0.00% 0	0.00% 0	0.00% 0	62.50% 5	37.50% 3	8
4	MOPs and MOEs are effective forms of assessments.	0.00% 0	0.00% 0	14.29% 1	71.43% 5	14.29% 1	7
5	Assessments are especially effective if they incorporate both quantitative and qualitative analysis.	0.00% 0	0.00% 0	0.00% 0	75.00% 6	25.00% 2	8
6	Metrics vary in scale and purpose from situational awareness to actionable information.	0.00% 0	0.00% 0	0.00% 0	25.00% 2	75.00% 6	8
7	Defensive Cyber Operations as well as Offensive Cyber Operations are both symmetric as well as asymmetric.	0.00% 0	0.00% 0	12.50% 1	37.50% 3	50.00% 4	8
8	When possible, we should attempt to utilize the asymmetric capabilities of DCO and assess the effectiveness of these capabilities.	0.00% 0	0.00% 0	12.50% 1	50.00% 4	37.50% 3	8
9	Resources such as financial capital, processing power, and human resources assist an organization in gaining the asymmetric advantage within the cyber domain.	0.00% 0	0.00% 0	12.50% 1	25.00% 2	62.50% 5	8
10	Economy of force strategies that expand the ability of machines to execute the decision process and minimize the need for human interaction should be applied.	0.00% 0	12.50% 1	50.00% 4	12.50% 1	25.00% 2	8

Showing Rows: 1 - 10 Of 10

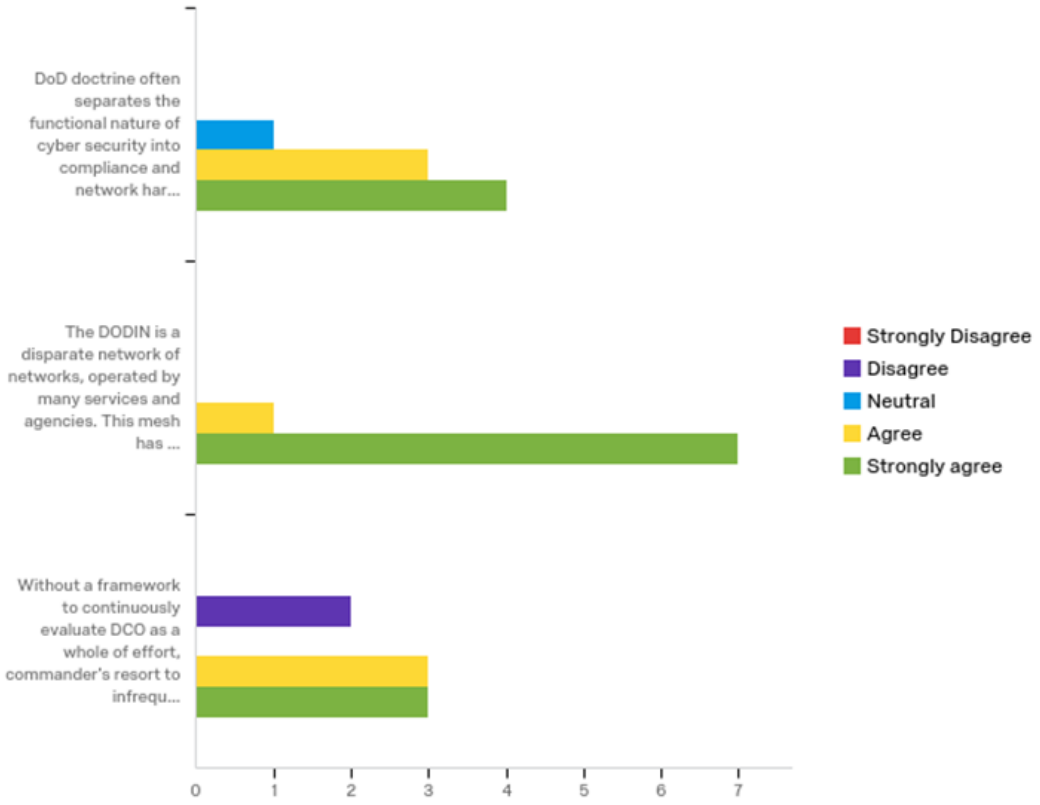
Round II Expert Consensus: Assessments



#	Field	Choice Count
1	Strongly Disagree	0.00% 0
2	Disagree	0.00% 0
3	Neutral	12.50% 1
4	Agree	50.00% 4
5	Strongly agree	37.50% 3
		8

Showing Rows: 1 - 6 Of 6

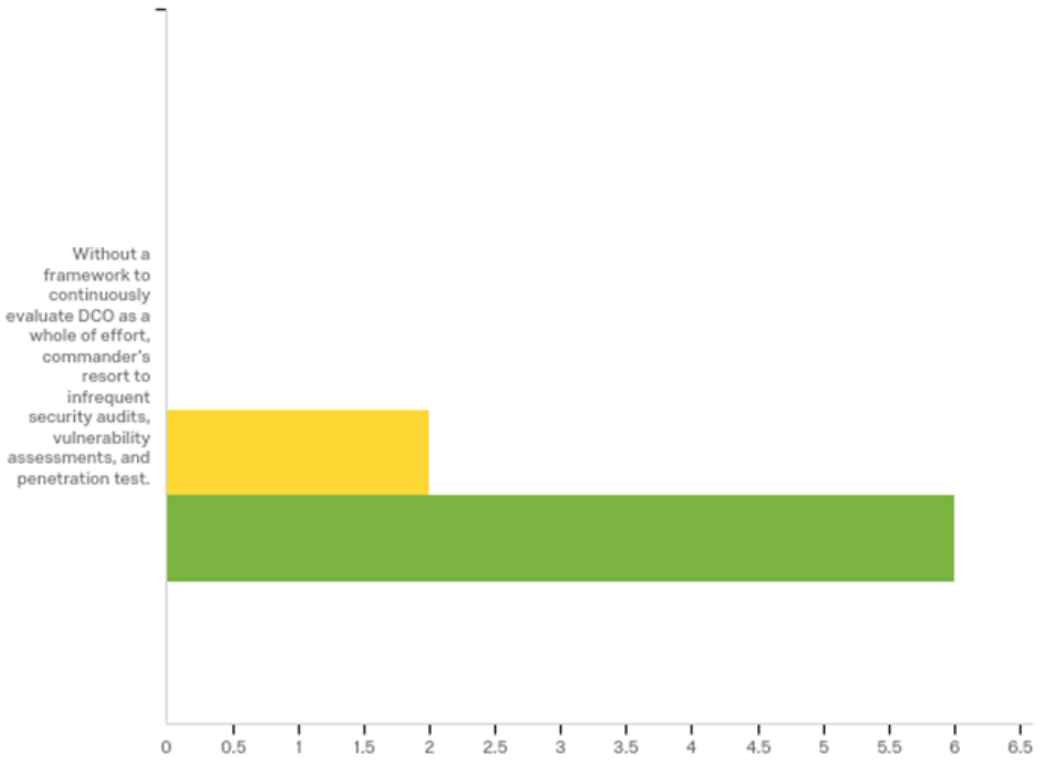
Round I Expert Consensus: Current Framework Challenges



#	Field	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree	Total
1	DoD doctrine often separates the functional nature of cyber security into compliance and network hardening (DODIN Ops) and hunting and response actions (DCO-IDM). This fractional method of evaluating DCO as a partial concept means that we are not providing the commander with an adequate representation of how our conceptual shield is prepared for enemy engagement.	0.00% 0	0.00% 0	12.50% 1	37.50% 3	50.00% 4	8
3	The DODIN is a disparate network of networks, operated by many services and agencies. This mesh has created an in-congruent reporting structure that is not only difficult to defend, but near impossible to assess.	0.00% 0	0.00% 0	0.00% 0	12.50% 1	87.50% 7	8
4	Without a framework to continuously evaluate DCO as a whole of effort, commander's resort to infrequent security audits, vulnerability assessments, and penetration test.	0.00% 0	25.00% 2	0.00% 0	37.50% 3	37.50% 3	8

Showing Rows: 1 - 3 Of 3

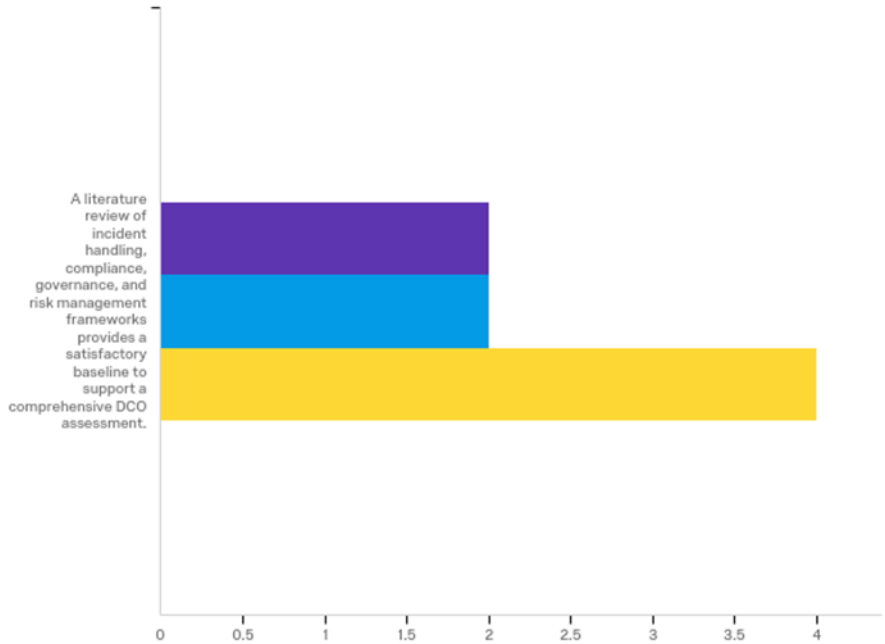
Round II Expert Consensus: Current Framework Challenges



#	Field		Choice Count
1	Strongly Disagree	0.00%	0
2	Disagree	0.00%	0
3	Neutral	0.00%	0
4	Agree	25.00%	2
5	Strongly agree	75.00%	6
			8

Showing Rows: 1 - 6 Of 6

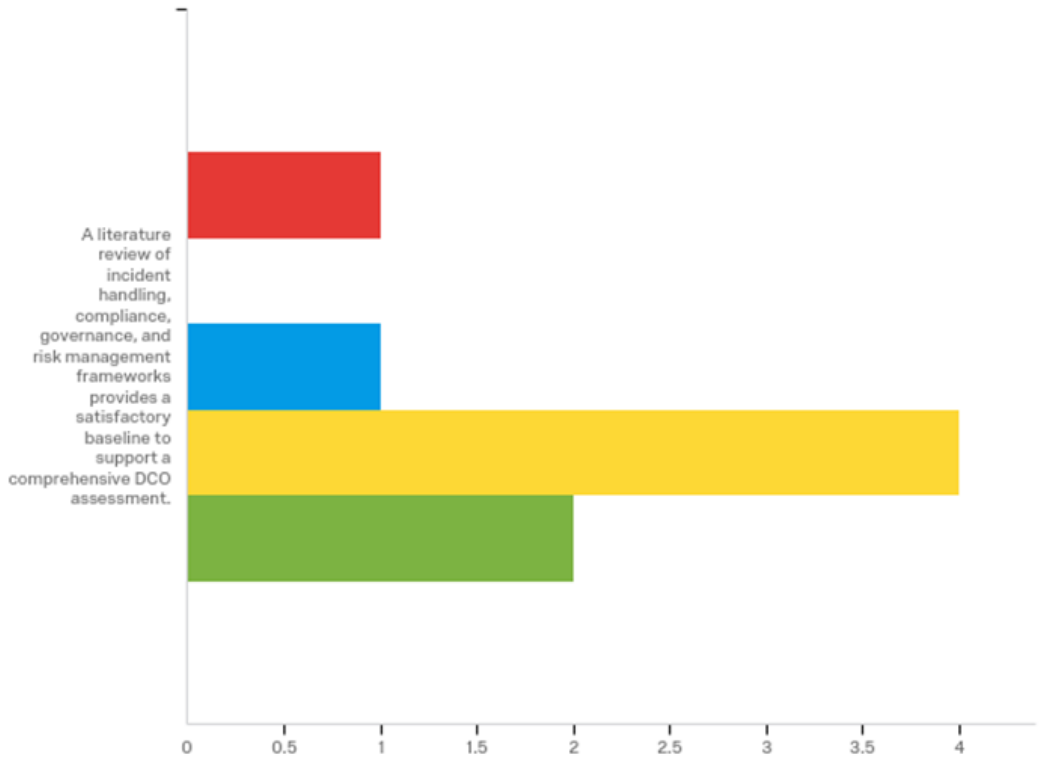
Round I Expert Consensus: Frameworks



#	Field		Choice Count
1	Strongly Disagree	0.00%	0
2	Disagree	25.00%	2
3	Neutral	25.00%	2
4	Agree	50.00%	4
5	Strongly agree	0.00%	0
			8

Showing Rows: 1 - 6 Of 6

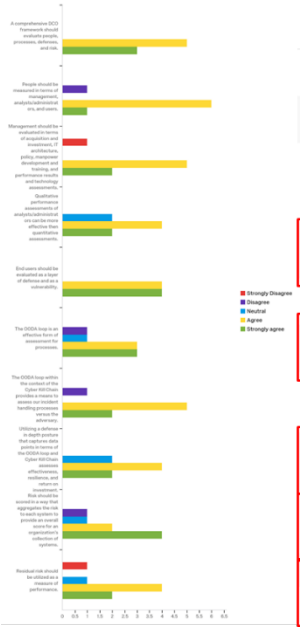
Round II Expert Consensus: Frameworks



#	Field		Choice Count
1	Strongly Disagree	12.50%	1
2	Disagree	0.00%	0
3	Neutral	12.50%	1
4	Agree	50.00%	4
5	Strongly agree	25.00%	2
			8

Showing Rows: 1 - 6 Of 6

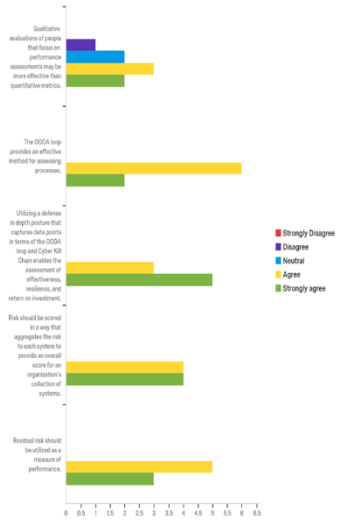
Round I Expert Consensus: Proposed Framework



#	Field	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree	Total
1	A comprehensive DCO framework should evaluate people, processes, defenses, and risk.	0.00% 0	0.00% 0	0.00% 0	62.50% 5	37.50% 3	8
2	People should be measured in terms of management, analysts/administrators, and users.	0.00% 0	12.50% 1	0.00% 0	75.00% 6	12.50% 1	8
3	Management should be evaluated in terms of acquisition and investment, IT architecture, policy, manpower development and training, and performance results and technology assessments.	12.50% 1	0.00% 0	0.00% 0	62.50% 5	25.00% 2	8
4	Qualitative performance assessments of analysts/administrators can be more effective then quantitative assessments.	0.00% 0	0.00% 0	25.00% 2	50.00% 4	25.00% 2	8
5	End users should be evaluated as a layer of defense and as a vulnerability.	0.00% 0	0.00% 0	0.00% 0	50.00% 4	50.00% 4	8
6	The OODA loop is an effective form of assessment for processes.	0.00% 0	12.50% 1	12.50% 1	37.50% 3	37.50% 3	8
7	The OODA loop within the context of the Cyber Kill Chain provides a means to assess our incident handling processes versus the adversary.	0.00% 0	12.50% 1	0.00% 0	62.50% 5	25.00% 2	8
8	Utilizing a defense in depth posture that captures data points in terms of the OODA loop and Cyber Kill Chain assesses effectiveness, resilience, and return on investment.	0.00% 0	0.00% 0	25.00% 2	50.00% 4	25.00% 2	8
9	Risk should be scored in a way that aggregates the risk to each system to provide an overall score for an organization's collection of systems.	0.00% 0	12.50% 1	12.50% 1	25.00% 2	50.00% 4	8
10	Residual risk should be utilized as a measure of performance.	12.50% 1	0.00% 0	12.50% 1	50.00% 4	25.00% 2	8

Showing Rows: 1 - 10 Of 10

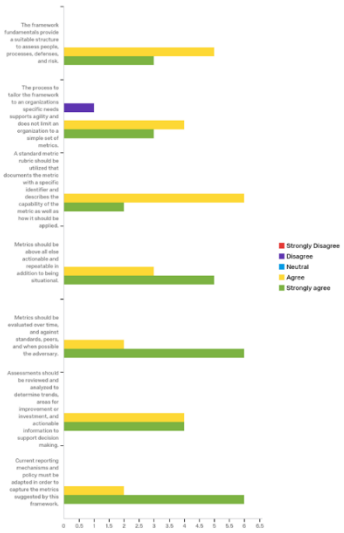
Round II Expert Consensus: Proposed Framework



#	Field	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree	Total
4	Qualitative evaluations of people that focus on performance assessments may be more effective than quantitative metrics.	0.00% 0	12.50% 1	25.00% 2	37.50% 3	25.00% 2	8
6	The OODA loop provides an effective method for assessing processes.	0.00% 0	0.00% 0	0.00% 0	75.00% 6	25.00% 2	8
8	Utilizing a defense in depth posture that captures data points in terms of the OODA loop and Cyber Kill Chain enables the assessment of effectiveness, resilience, and return on investment.	0.00% 0	0.00% 0	0.00% 0	37.50% 3	62.50% 5	8
9	Risk should be scored in a way that aggregates the risk to each system to provide an overall score for an organization's collection of systems.	0.00% 0	0.00% 0	0.00% 0	50.00% 4	50.00% 4	8
10	Residual risk should be utilized as a measure of performance.	0.00% 0	0.00% 0	0.00% 0	62.50% 5	37.50% 3	8

Showing Rows: 1 - 5 Of 5

Round I Expert Consensus: Applying the DCO Framework



#	Field	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree	Total
1	The framework fundamentals provide a suitable structure to assess people, processes, defenses, and risk.	0.00% 0	0.00% 0	0.00% 0	62.50% 5	37.50% 3	8
2	The process to tailor the framework to an organizations specific needs supports agility and does not limit an organization to a simple set of metrics.	0.00% 0	12.50% 1	0.00% 0	50.00% 4	37.50% 3	8
3	A standard metric rubric should be utilized that documents the metric with a specific identifier and describes the capability of the metric as well as how it should be applied.	0.00% 0	0.00% 0	0.00% 0	75.00% 6	25.00% 2	8
4	Metrics should be above all else actionable and repeatable in addition to being situational.	0.00% 0	0.00% 0	0.00% 0	37.50% 3	62.50% 5	8
5	Metrics should be evaluated over time, and against standards, peers, and when possible the adversary.	0.00% 0	0.00% 0	0.00% 0	25.00% 2	75.00% 6	8
6	Assessments should be reviewed and analyzed to determine trends, areas for improvement or investment, and actionable information to support decision making.	0.00% 0	0.00% 0	0.00% 0	50.00% 4	50.00% 4	8
7	Current reporting mechanisms and policy must be adapted in order to capture the metrics suggested by this framework.	0.00% 0	0.00% 0	0.00% 0	25.00% 2	75.00% 6	8

Showing Rows: 1 - 7 Of 7