Software Acquisition *Go Bag*

Decoding SWP Metrics

The *Pack Light, Measure Right* Tactical Guide provided you with principles that enable you to "measure right" and develop metrics as part of your acquisition strategy. This Supplement shows you the hidden value in the metrics that you're already collecting if you are on the Software Acquisition Pathway.

In the tables provided, we list each SWP-required metric with a unique ID number (ID#). (We'll refer to these ID#s in future Supplements.) We also map some (not all) of the key PMO questions to the metrics and recommend combinations of those metrics. We developed this table using a simplified version of the Goal Question Indicator Metric (GQIM) process, which the SEI uses to help programs develop goal-driven measurement programs.[1] We also provide some data sources where you can pull data.

> You can view what the SWP requires by referring to SWP in Sections 1.2.1 and 2.7.d of the Policy. Each SWP metric in the table is listed with the definition provided by the SWP.[2]

Additional Details to Help You Decode SWP Metrics

For the purposes of managing and executing your program, you will need to measure beyond SWP metrics. Future Supplements will provide scenarios that (while not all inclusive) will look at metrics for your program that go beyond what is required by the SWP.

The tables we've provided in this Supplement map key PMO questions to SWP metrics (and recommended combinations of those metrics). Combining metrics creates an indicator that PMO staff can interpret to answer those key PMO questions. In this Supplement, we do not explain how to create an indicator. Keep your eye out for future Supplements on this topic or reach out with questions.

> As a reminder from the Tactical Guide, programs shouldn't rely on a single metric. *A single metric never tells the whole story*. A variety of carefully chosen measures and metrics paint a complete picture. While you should use the same data to derive insight at all levels, you should not use the same metrics and/or the same analyses for all purposes.

Acronyms

ATO	Authority to Operate
CI/CD	Continuous Integration and Continuous Delivery
CMMS	Computerized Maintenance Management Systems
CVE	Common Vulnerabilities and Exposures
DA	Decision Authority
DoW	Department of War
eMASS	Enterprise Mission Assurance Support Service
FRACAS	Failure Reporting, Analysis, and Corrective Action System
GQIM	Goal Question Indicator Metric
ICF	Incident Collection Format
MTBF	Mean Time Between Failures
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
QA	Quality Assurance
SIEM	Security Information and Event Management
SWE	Software Engineering
SWP	Software Acquisition Pathway
WAU	Warfighting Acquisition University

ATO READINESS

Key PMO Questions	SWP Metric	Why Is This Needed?	Potential Data Source(s)
• Are we ready for oversight reviews and accreditation without surprises? • How much does lead time to ATO delay operational deployment? • What is the lead time to obtain an ATO? • How long does it take to get an ATO once a system is ready?	**Average Lead Time for ATO (Days)** [SWP1] *"Average number of days to obtain authority to operate (ATO) by release. If authority is designated something other than an ATO, please provide the data for that ATO-equivalent process"*	• **DA/Leadership** benchmarks security process agility. The average could indicate risk from non-timely deployments. • **The PMO** tracks ATO lead times to identify delays. The average is a strong indicator of expected delays. • **The Product Team/Pipeline** identifies delays with documentation and compliance. • **Policy** determines whether policy reforms are enabling faster, but secure releases.	• ATO tracking in eMASS or equivalent • PMO tracking • Security package submission (timestamped)
	Continuous ATO in-Place (Yes/No) [SWP2] *"Indicator of program's ability to achieve a continuous ATO or similarly expedited approval authority process"*	• **DA/Leadership** benchmarks DevSecOps adoption across the programs. • **The PMO** automates the management of release readiness and understands the timelines for getting ATO. • **The Product Team/Pipeline** contributes to evaluating pipeline health to ensure it continuously meets the continuous ATO requirements.	

CYBERSECURITY POSTURE

Key PMO Questions	SWP Metric	Why Is This Needed?	Potential Data Source(s)
• Is the system secure and are vulnerabilities being fixed fast enough to reduce risk? • How quickly does the program recover from a cyber incident or vulnerability?	**Mean Time to Resolve Experienced Cyber Incident or CVE** [SWP3] *"The mean response time (in hours) a program was able to resolve a Cyber Incident or Common Vulnerability or Exposure (CVE) from the time of identification through resolution. This metric is intended to identify the most meaningful and recurring source of cyber activity for the program"*	• **DA/Leadership** benchmarks across programs to prioritize modernization and training. • **The PMO** assesses mission resilience to improve coordination and reduce downtime. • **The Product Team** monitors real-time vulnerability response and identifies weaknesses or process gaps to optimize workflows or processes. • **Policy** evaluates enterprise performance to assess the effectiveness of policy.	• Security incident ticket timestamps (opened to closed) • Patch or mitigation deployment logs • Risk Management Framework POA&M updates • Cybersecurity dashboard/monitoring system reports • Static application security testing tool CVE reports
How quickly can the program identify that a cyber incident has occurred?	**Mean Time to Detect Cyber Incident** [SWP4] *"The mean time from Cyber Incident start to time of identification (in hours). A Cyber Incident is any action taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein"*	• **DA/Leadership** benchmarks detection maturity across programs to allocate resources. • **The PMO** manages cyber awareness to improve detection processes. • **The Product Team/Pipeline** evaluates the monitoring process and alerting speed to improve incident detection. • **Policy** assesses enterprise detection resilience to improve policy.	• Security monitoring and alerting systems SIEM logs • Incident detection timestamps • Threat intelligence alerts

PERFORMANCE & RELIABILITY METRICS

Key PMO Questions	SWP Metric	Why Is This Needed?	Potential Data Source(s)
• Are we delivering usable capability to the warfighter on a predictable, frequent schedule? • How often and predictably are we delivering and fielding a usable capability? • What is our progress towards meeting mission and operational goals? • Is my program meeting its planned objectives?	**Average Deployment Frequency** [SWP5] *"Execution phase: The average frequency of releases into an operational environment (days)"*	• **DA/Leadership** benchmarks delivery frequency across the programs to identify best practices and confirms that the program is delivering incrementally and reducing integration risks. • **The PMO** manages capability delivery rates to improve planning and integration and monitors steady progress toward operational capability. • **The Product Team/Pipeline** monitors delivery effectiveness to plan capacity and reduce bottlenecks while consistently evaluating workflow efficiency. • **Policy** aggregates across the Department to evaluate pathway effectiveness and to inform policy and the Department's investment strategy.	• CI/CD pipeline release dates and deployment logs • Post developmental test, operational test, and certification • Release notes, version history, and sprint or increment demo records/notes
	Capabilities Delivered This Reporting Cycle [SWP6] *"Execution phase: Summarize your capabilities delivered this reporting period"*	• **DA/Leadership** evaluates whether programs are delivering mission capability in a timely manner. • **The PMO** manages the program to ensure capability is delivered as planned. • **The Product Team/Pipeline** monitors the ability to plan capability delivery and reduce bottlenecks. • **Policy** collects insights across services and programs that inform how policy is supporting the delivery of mission capability.	• Roadmap, sprint/release completion reports • Demo or User acceptance records • Work planning/tracking tool showing completed capabilities
• How reliable are teams at delivering software? • Is the team making progress against prioritized User needs? • How long does it take on average to complete a development cycle for a unit of work?	**Average Cycle Time (Days)** [SWP7] *"Execution phase: The average duration time (in days) to deliver a capability or feature into operation, measured from the time the need is identified for a specific build (moved from the backlog to a planned release) to the time the code is committed (development activity finished)"*	• **DA/Leadership** benchmarks development speed across programs to identify best practices and sources of variation and identifies bottlenecks that affect mission delivery. • **The Program** benchmarks program development times to improve the process, improve coordination between teams, and allocate resources. • **The Product Team/Pipelin**e baselines and monitors the development speed for planning and process improvement. • **Policy** evaluates the effectiveness of the SWP for improving development speed.	• Backlog start and completion timestamps • Sprint/increment histories and planning reports from the tasking tool • Work planning/tracking tool status
How long does it take from when code is first committed to it being available to release to production?	**Average Lead Time for Change (Days)** [SWP8] *"The average duration (in days) to deliver a capability or feature into operation, measured from the time the code is committed (development activity finished) to the time it is available for release to operations (production)"*	• **DA/Leadership** benchmarks post-development delivery performance. • **The PMO** benchmarks the duration of post-development activities to identify bottlenecks and for process improvement. • **The Product Team/Pipeline** monitors post-development activities to improve CI/CD and pre-release practices. • **Policy** evaluates the SWP's effect on post-development deployment speed.	• Backlog approval through deployed capability • Ticket/change request timestamps from code committed to be available for release to production, including testing completion dates • Certification completion dates

PERFORMANCE & RELIABILITY METRICS

Key PMO Questions	SWP Metric	Why Is This Needed?	Potential Data Source(s)
• How efficiently is software moving from development to production? • Are there bottlenecks in the development process? • Do the developers have the tools and automation they need to operate efficiently? • What is the fastest/ slowest we have delivered a change? • Is the software development process so slow that it results in high overhead?	**Minimum Lead Time for Change (Days)** [SWP9] *"The minimum duration (in days) to deliver a capability or feature into operation, measured from the time the code is committed (development activity finished) to the time it is available for release to operations (production)"*	• **DA/Leadership** compares peak to average post-delivery speeds across identified best practices. • **The PMO** compares peak to average post-delivery speeds to manage coordination and standardize practices across program pipelines. • **The Product Team/Pipeline** focuses on the toolchain and process limits to reduce variance and bottlenecks. • **Policy** evaluates the effectiveness of the pathway on reducing best-case deployment times and informs policy revisions.	• Approval and deployment timestamps • Change IDs • Testing completion dates • Certification completion dates
	Maximum Lead Time for Change (Days) [SWP10] *"The maximum duration (in days) to deliver a capability or feature into operation, measured from the time the code is committed (development activity finished) to the time it is available for release to operations (production)"*	• **DA/Leadership** benchmarks delay costs to target modernization efforts. • **The PMO** evaluates delivery risk to manage and mitigate inter-team risk. • **Policy** evaluates the effectiveness of the pathway on reducing worst-case deployment times and inform policy revisions.	
• Is the program ready and able to meet its mission needs? • What is the likelihood that the program will suffer an interruption during a mission? • How often does the system fail in its operational environment?	**Mean Time Between Failures (MTBF) (Days)** [SWP11] *"MTBF is a statistical measure that estimates the average time between two consecutive failures of a software system or component. For complex, repairable systems, failures are considered to be those out of design conditions which place the system out of service and into a state for repair. Failures which occur that can be left or maintained in an unrepaired condition, and do not place the system out of service, are not considered failures under this definition. Units that are taken down for routine scheduled maintenance or inventory control are not considered within the definition of failure. It quantifies the reliability of a system by providing an estimate of how long it can operate continuously without experiencing a failure event. Measures the reliability of the software in production. The average is calculated by dividing 180 days (within reporting cycles-APR & OCT) by the number of qualified failures over the 6 months period. A higher MTBF indicates greater reliability"*	• **DA/Leadership** benchmarks reliability across programs to assess portfolio risk and target modernization investments for reliability. • **The PMO** manages mission readiness, allocates test resources, and manages release schedules. • **The Product Team/Pipeline** monitors operational reliability to quantify the cost of poor quality and evaluate the benefits of quality improvement. • **Policy** evaluates the effectiveness of the pathway in sustaining or improving reliability to inform policy and guidance that balances speed and reliability.	• Incident/outage logs • Operations monitoring dashboards • System error and failure reports from the field • Bug/issue trackers (timestamped)

PERFORMANCE & RELIABILITY METRICS

Key PMO Questions	SWP Metric	Why Is This Needed?	Potential Data Source(s)
• How often does our program suffer problems that require intervention and remediation? • How often do releases or changes cause failures or issues?	**Change Fail Rate** [SWP12] *"The percentage of releases to the production/ operational environment that requires subsequent remediation"*	• **DA/Leadership** benchmarks release quality across programs to identify effective practices. • **The PMO** assesses the effect of release quality on mission risk to establish quality thresholds, improve testing, and manage release speed versus quality tradeoffs. • **The Product Team/Pipeline** detects and remediates deployment failures, improves regression testing, and monitors deployment quality. • **Policy** evaluates the effectiveness of the SWP on deployment reliability and informs policy revisions.	Production failures that are recorded in the following • The FRACAS • Deficiency Reports • Incident logs associated with new changes • QA/Test reports • CI/CD pipeline failure reports Releases that are recorded in the following • Release notes • Repositories • CI/CD toolchains
• In the event of a service outage that affects missions, how quickly can we restore service? • How quickly can the program recover from failures?	**Mean Time to Restore** [SWP13] *"The mean time (in days) to restore the system in response to a downtime event or a defect that requires subsequent remediation"*	• **DA/Leadership** benchmarks operational resilience across programs to identify effective practices and allocate improvement efforts. • **The PMO** measures the effectiveness of incident response and contingency planning as well as manages operational resilience and improves readiness. • **The Product Team/Pipeline** identifies process gaps and recovery improvements as well as monitors recovery speed to improve rollback automation and reduce downtime. • **Policy** evaluates the resilience of SWP programs to evaluate SWP effectiveness, monitor progress, and inform policy and guidance revisions.	• Incident open and closed timestamps • Operations monitoring dashboards • Change management logs • After-action and post-incident reports • Logged in Computerized Maintenance Management Systems (CMMS) • DevSecOps or cloud observability logs • Records from DoW ICF reports

USER ENGAGEMENT

Key PMO Questions	SWP Metric	Why Is This Needed?	Potential Data Source(s)
• Are Users actively involved and is their feedback actively shaping development? • Are we delivering User-requested capabilities at a reasonable cost? • Is delivered software producing measurable mission value?	**Value Assessment Rating** [SWP14] *"The program office's perceived rating based on the last formal Value Assessment received from the operational sponsor"*	• **DA/Leadership** benchmarks the satisfaction of mission needs across programs to align the portfolio with mission needs and prioritize spending. • **The PMO** assesses how delivered products affect mission satisfaction to prioritize new capabilities and features. • **The Product Team/Pipeline** assesses feature relevance to improve backlog management and acceptance criteria. • **Policy** evaluates pathway success by aligning capability development with mission needs to inform policy and guidance revisions.	• User-submitted value assessments • Mission performance indicators tied to software use • Feature adoption usage analytics (if applicable) • After-action reports • Surveys • Focus groups with Users
	Executive Summary from Last Value Assessment [SWP15] *"Summary describing the last formal Value Assessment from the operational user community"*	• **DA/Leadership** understands how the PMO is supporting and impacting the User and the mission. • **The PMO** understands if the agreed-to capabilities are being delivered to the User to support the mission. • **The Product Team/Pipeline** understands how capability development is impacting Users to improve development and backlog planning. • **Policy** evaluates the SWP's impact on the User and mission effectiveness.	

Endnotes

1 Software Engineering Institute (SEI). Goal-Driven Measurement (IGDM) SEMA Course. *SEI Website*. 2016. https://www.sei.cmu.edu/library/goal-driven-measurement-igdm-sema-course/

2 Department of War (DoW). *Operation of the Software Acquisition Pathway*. DoDI 5000.87. DoW. October 2, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF?ver=virAfQj4v_LgN1JxpB_dpA%3D%3D

Software Acquisition *Go Bag*

About the SEI

The Software Engineering Institute (SEI) advances software as a strategic advantage for national security through research, development, and deployment of tools, technologies, and practices in software engineering, artificial intelligence (AI), cyber, and acquisition transformation. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of War (DoW).

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu

This material is based upon work supported by the Department of War under Air Force Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM26-0409

©2026 Carnegie Mellon University | 6554 | C 04.17.2026 | S 04.29.2026