11-2. Three-Pronged Oversight Review Process

a. Surveillance and oversight of the GPC program are a shared responsibility. All stakeholders in the program, including requiring offices, RMs, logistics, contracting, and local audit and oversight organizations, are responsible for ensuring that the GPC is used in the proper manner and only authorized and necessary official purchases are made. Organizations should develop and follow a monitoring and oversight plan that establishes frequencies, methods, participation, etc.

b. Oversight is conducted to:

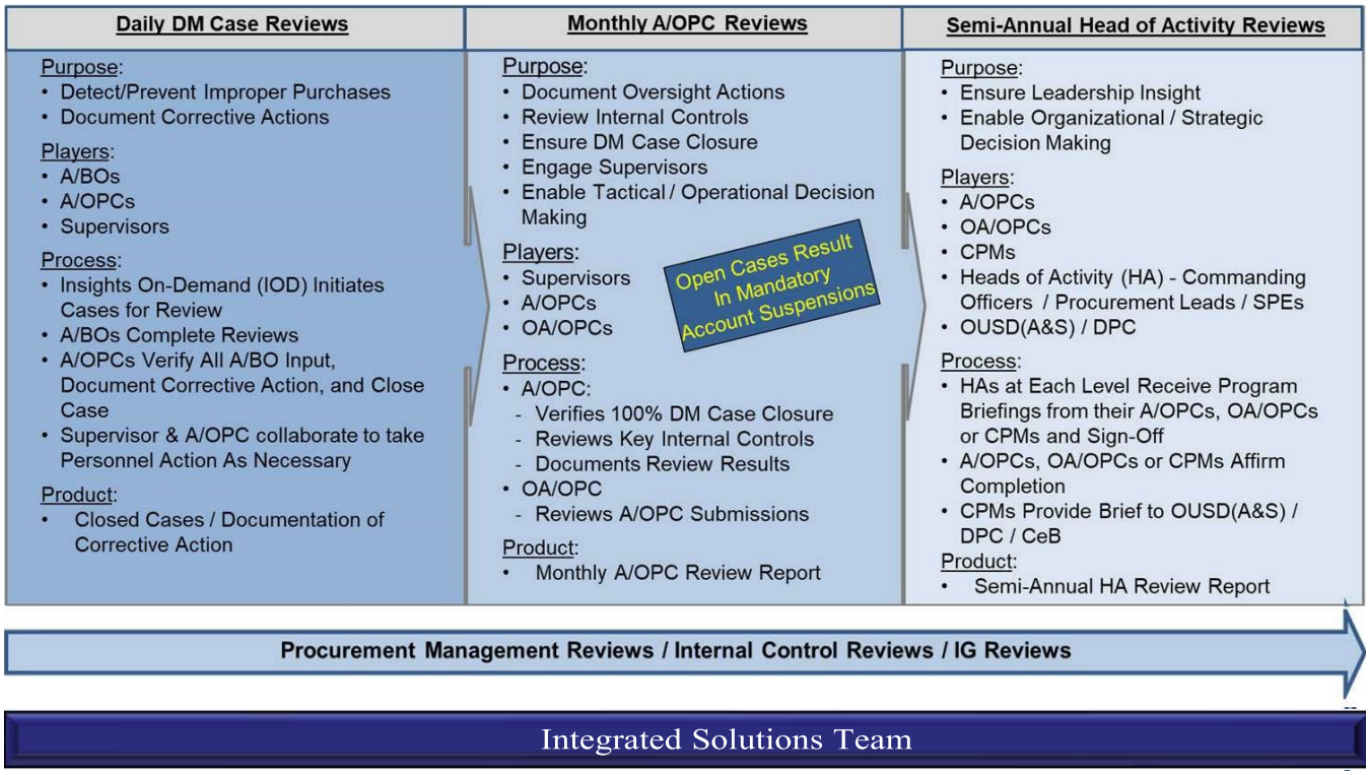
1) Validate and promote compliance with existing internal controls;

2) Identify, report, and resolve systemic material program weaknesses; and

3) Measure the effectiveness of internal controls.

c. To improve auditability of GPC program oversight and realize the cost and other benefits of using the commercially available SP3 technology, DoD uses the integrated three-pronged, system-enabled review cycle depicted in Figure 11-1.

Figure 11-1: Three-Pronged Oversight Review Cycle



d. The three-pronged review cycle supplements existing GPC operational transaction management and account reconciliation and review processes, including:

1) Cardholder-obtained purchasing approvals (e.g., BO pre-purchase approval, special item approval, availability of appropriate and sufficient funds);

2) Cardholder matching and approval of orders to transactions and monthly statement approval;

3) Billing official monthly certification of the managing account billing statement;

4) Resource manager funds certification;

5) A/OPC ongoing oversight and policy compliance efforts; and

6) Disbursing office funds validation and disbursement processing.

The cycle also supplements and informs both the periodic reviews of Army contracting offices (e.g., Army PMRs or DCMA-led PMRs) conducted to assess the effectiveness of the contracting function, and the GPC governance processes conducted to evaluate and improve the effectiveness of GPC internal controls.

e. **Data analytics.** Data analytics is the application of electronic tools (software and/or systems) for automated data sorting, filtering and mining techniques using self-learning algorithms to search GPC transaction data in order to identify patterns, trends, risks, opportunities and other information. A/OPCs should use data analytics tools to assist them in the management and oversight of their GPC program.

f. The Army uses preventive, detective, and directive controls to monitor the GPC program.

1) Preventive controls are designed to discourage errors or irregularities from occurring (e.g., processing a transaction only after it has been properly approved by the appropriate personnel).

2) Detective controls are designed to find errors or irregularities after they have occurred (e.g., IOD data mining, approving statements, and reconciling monthly invoices).

3) Directive controls are designed to encourage a desirable event (e.g., written policies and procedures to assist in compliance and the accomplishment of the goals and objectives of the GPC program).

g. The HCA/SCO and A/OPCs are responsible for adhering to the requirements specified in OMB Circular A-123, Management's Responsibility for Internal Control. The HCA/SCO and A/OPCs are also responsible for adhering to the requirements specified in 10 USC 4754 (as modified by Public Law 112–194, Government Charge Card Abuse Prevention Act of 2012). These statutory requirements mandate the following actions (list not comprehensive):

1) Using effective systems, techniques, and technologies to prevent or identify improper purchases.

2) Invalidating GPCs from each employee who ceases to be employed by the Government or separates from Military Service.

3) Taking steps to recover the cost of any illegal, improper, or erroneous purchases made with a purchase card or convenience check made by an employee or member of the armed forces, including, as necessary, through salary offsets.

4) Taking appropriate adverse personnel actions or imposing other punishments when employees of the Army violate regulations governing the use and control of purchase cards and convenience checks or who are negligent or engage in misuse, abuse, or fraud with respect to a purchase card, including removal in appropriate cases. Violations of such regulations by a person subject to 10 USC Chapter 47, the Uniform Code of Military Justice (UCMJ), is punishable as a violation of section 892

of article 92 of the UCMJ.

5) Requiring the Army Audit Agency to conduct periodic audits or reviews of GPC programs to identify and analyze risks of illegal, improper, or erroneous purchases and payments and report the result to the Director of the OMB and Congress.

6) A/OPCs must provide monitoring, oversight, training, and administration of all BOs and CHs. Supervisors and BOs are responsible for the monitoring and oversight of BOs and CHs under their purview.

h. To minimize losses to the Army, the program must have an expectation of high integrity and ethical behavior from all participants, and sufficient staff to perform the following functions:

1) Conduct periodic risk assessments to identify fraud, waste, and abuse and establish specific controls to reasonably ensure that losses from these risks are minimized, to include data mining.

2) Conduct proper training and complete reporting and data analysis to ensure personnel have the skills and information needed to be effective in their positions.

3) Conduct detailed, effective management and oversight.

4) Implement corrective actions when cardholder management is non-compliant with Army policies and procedures.

i. DPCAP will rely on the signed Semi-Annual HA data provided by CPMs to accomplish DoD GPC reporting required by OMB. DPCAP updates visual trending of statistical and violation information to identify trends in GPC use and variances and shares this information with the Army during the GPC CPM Monthly Calls.

j. The GPC Integrated Solutions Team (IST) is DoD’s GPC governance body. IST membership consists of a GPC Governance Board composed of representatives from DPCAP, Army, Navy, Air Force, other Defense agencies, and supported by the bank team. The bank team consists of U.S. Bank (card-issuing bank), MasterCard (card association), and Oversight Systems (data mining vendor). The IST typically meets semi-annually to achieve the following:

1) Review trends and changes in the GPC industry and the DoD GPC Program.

2) Identify and approve any necessary adjustments to the bank team's electronic capabilities, DoD’s GPC enterprise tools, and/or DoD GPC policies.

3) Identify and approve changes to the DM rules and system parameter settings.

4) Bring efficiencies to the Program by adjusting the business rules/parameters based on transaction risk.

5) Review trends and changes in the GPC industry and the DoD GPC Program.

6) Identify any necessary adjustments to the bank team's electronic capabilities, DoD’s GPC enterprise tools, and/or DoD GPC policies.

7) Identify and approving changes to the Data Mining rules.

8) Review relevant data mining case information and recommendations provided by the bank team (e.g., percentage of data mining cases created for review; frequency with which each rule is

triggered and associated DM case disposition, and information about the findings, determinations, and corrective actions identified) and results of the Semi-Annual HA process to inform its decision making.

Parent topic: CHAPTER 11 - MANAGEMENT CONTROLS AND PROGRAM OVERSIGHT