Center for Government Innovation

Office of the Washington State Auditor
Pat McCarthy

Best practices for credit card programs

Government credit card programs vary greatly in size and purpose, as they allow employees to pay for travel, fuel or small purchases. They reduce your procurement and payment costs, allowing you to avoid processing purchase orders, individual invoices and checks – especially for small transactions. Some programs also offer rebates.

While credit cards can provide many benefits, they also carry a high risk of fraud, waste and abuse. When you provide credit cards to employees, it gives them a lot of control over a single transaction and puts considerable pressure on your review and monitoring processes.

April 2024

All too often, these monitoring processes fail to function as planned, and trouble ensues. Performance audits from around the country frequently identify questionable purchases such as personal expenses, gifts, food and refreshments — even when a local government's internal audit department performs audits annually.

You should prepare to address these risks by creating a strong system of internal controls. Consider these best practices when evaluating a credit card program and the related internal control system.

Setting up your program

- **Gain an understanding of requirements.** Local governments should review applicable state laws (RCW 43.09.2855 and 42.24.115), as well as the purchase card section of the Office of the Washington State Auditor's GAAP and Cash-Basis *Budgeting, Accounting and Reporting System* (BARS Manual).

- **Establish or update your policy.** You should clearly communicate with employees about what expenditures are allowed and prohibited, as well as the consequences of policy violations. You might require preapproval for certain types of purchases or those that exceed transaction limits. Also consider requiring employees to enter card information for each purchase, as opposed to saving credit card information in websites or internet browsers. Refer to the Municipal Research and Services Center's credit card policy guidance for additional policy considerations. You should reevaluate your policy annually and update it at least every three years.

- **Provide mandatory training on your policies, program controls, security and card use.** Provide training to cardholders and their approving supervisors before card issuance, and at least every three years thereafter. You may want to include training on related policies that affect card use (such as information technology, meals and refreshments, employee recognition and travel).

- **Consider implementing a digital workflow.** Consider using SharePoint or another available technology to track processes such as for employee acknowledgement of policies, completed training, card issuance or deactivation and card receipt.

Note: If you plan to use credit cards for micro-purchases related to a federal program, then you must clearly indicate the card may be used for these purchases, as well as document and approve the procedures to do so (Uniform Guidance 2 CFR §200.320(a)(1)(ii)).

- **Establish a process for employment change notification.** Implement a process so that human resources will notify the credit card program administrator about internal transfers or expected separations. From there, the administrator can deactivate cards and obtain support for any remaining charges.

Working with your credit card issuer

- **Use a competitive process to select your credit card issuer.** In selecting a provider, consider security controls, access to data and online monitoring, software integration, rebate programs, ability to restrict certain transactions, and training/customer support. You may want to include the services as part of your overall banking services contract.

  Additional service offerings might include automated systems, allowing cardholders to review, approve, and sign off on transactions. If you rely on the controls of third parties to process your transactions, consider obtaining a System and Organization Controls 2 report for confirmation the provider has the proper controls.

- **Design your card to look unique.** When personal charges appear on a government's card, employees often say it is because their government card and personal card look alike. Design a recognizable card or credit card sleeve to reduce confusion (if you use a sleeve, require employees to keep their card in it).

- **Safeguard any RFID credit cards.** You might also hear these cards called "contactless" or "tap-to-pay" cards. If your credit card provider issues RFID cards, take extra steps to protect the cards' information. For example, you might obtain a protective sleeve that will block electronic signals, as well as train employees how to safeguard it.

- **Define merchant restrictions and spending limits.** Work with your provider to block certain types of merchants or expenditure types like travel or cash advances. In addition, impose transaction limits and daily and monthly limits. You might set a transaction limit to prevent cardholders from buying a capital asset or exceeding the threshold for a procurement action (for example, a bid limit). If you approve any exceptions, be sure to document them.

- **Use a credit card provider that has excellent reporting capabilities.** Your provider should allow you to generate exception reports, create ad-hoc reports, access data in real-time (including level 3 data/line-item purchase detail, if available), and download digital transaction data for additional analysis.

- **Develop a working relationship with your credit card issuer/bank and its fraud unit.** You want a proactive fraud department at your bank that has an open line of communication with your credit card program administrator. That way, you can quickly learn about questionable activity.

- **Keep current in new and innovative solutions to detect and identify potential fraud, misuse, and delinquency in your credit card program.** Attend trainings and periodically inquire with your credit card issuer to learn about new options.

Before issuing credit cards

- **Ensure cardholders have a business need.** You should only issue cards to employees that need to use them regularly. You should not automatically issue cards to high-ranking employees. If an employee expects to only need it periodically, perhaps another cardholder can process the transaction instead.

- **Establish appropriate credit limits.** Align credit card limits with the cardholder's expected spending needs. If high-ranking employees need a credit card for government business, you should not automatically assign them high credit limits. It unnecessarily exposes you to fraudulent transactions. You can temporarily increase a limit, if needed. You should use a standardized form to document both the business need and the credit limit approval.

- **Require a detailed cardholder agreement.** Your agreement should outline cardholder responsibilities, approver/reconciler responsibilities, limitations on use, and security protocols. It serves as documented evidence that the employee reviewed the policy and understood and agreed to your terms.

- **Maintain the right number of cards.** Balance the number of cards with your ability to effectively monitor and administer the program.

- **Segregate duties for card issuance.** If one person orders cards, then someone else should receive them. These duties should be segregated so employees cannot order a card that they intend to use for fraudulent purposes without someone else seeing it.

Processing spending activity

- **Require the cardholder to reconcile their own spending activity as promptly as possible.** Cardholders should review their own transactions; they are in the best position to identify inappropriate charges. They should not delegate this responsibility to any other person. Your credit card issuer may offer an application allowing cardholders to review transactions as they occur, rather than wait until month-end. An automated process can help you reduce redundant steps, ensure timely detection of incorrect charges, and facilitate timely approvals. A smaller government might provide weekly reports to each cardholder, so that they may reconcile activity promptly.

- **Retain robust documentation to support charges.** Cardholders should include itemized receipts and descriptive annotations to describe the business purpose of charges, if unclear. They should also support any online purchases. Require a completed form for any lost receipts.

- **Require a supervisory review.** The employees' direct supervisor or manager should review the cardholder's activity. Managers know their employees and their activities, so they are in the best position to identify questionable transactions on employees' cards. However, avoid assigning too many cardholders to any one approver (for instance, no more than 10). Approvers who have too many cardholders to review might not have the capacity to thoroughly review each cardholder's activity.

Note: It is not efficient for your staff to continuously follow up on noncompliance with the same cardholders; take disciplinary action if this occurs.

Some high-ranking cardholders do not have a direct supervisor, per se. Your policy should describe the review and approval process for this official. Some options include the chair of the governing body, the audit committee, or the finance director (so long as you formalize the process they should follow if concerns arise).

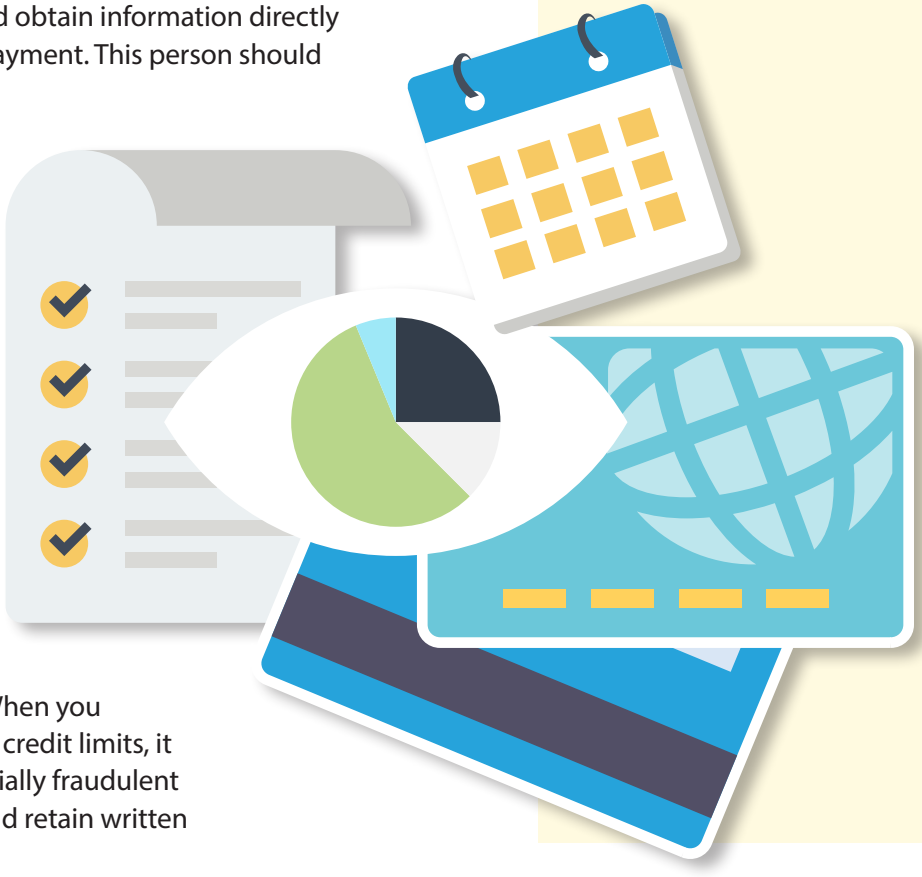
- **Review for policy compliance.** You might also use a second transaction reviewer: a separate person who is well-versed in policy requirements.

- **Consider using a review checklist.** You could use a review checklist, to ensure your reviewer(s) perform the required review procedures.

- **Impose strict deadlines for reconciliation and approval.** Cardholders, and their approving managers, should complete their procedures within an established deadline. Otherwise, you should consider this noncompliance and follow up accordingly.

- **Obtain original credit card statements to pay your bill.** If cardholders access the credit card statements prior to payment, they may alter them to conceal fraudulent charges. To ensure the underlying information meets expectations, someone should obtain information directly from the credit card issuer prior to payment. This person should not have a credit card (segregation of duties principles).

Monitoring your program



- **Review active card holders, at least twice per year.** Obtain a card listing of active cardholders from your credit card provider and compare it to your records of active employees.

- **Review infrequently used cards, at least once per year.** Cardholders with little to no spending may not need their card. When you have active, unused cards with open credit limits, it unnecessarily exposes you to potentially fraudulent activity. Close accounts if possible and retain written justification for any left open.

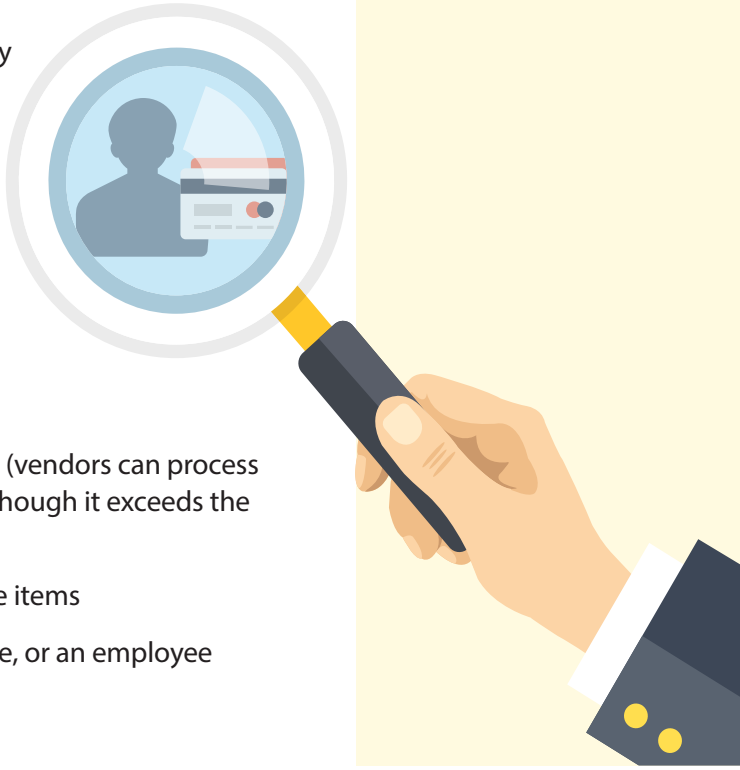
- **Review credit limits, at least once per year.** Evaluate credit limits, given monthly spending trends, to determine if you should lower some of them. Your overall credit card exposure should not exceed your business needs.

- **Physically verify credit cards, at least once per year.** Using a listing of active cardholders obtained directly from your credit card provider, have each cardholder show you the physical card. This is a good time to inspect for damaged protective sleeves too.

- **Perform systematic, timely monitoring of card activity.** You should assign someone to centrally review and monitor transactions, as frequently as daily. Many credit card providers offer online access, downloadable data, and exception reports to allow you to monitor card activity. Only employees without credit cards should access credit card data for monitoring purposes. Under segregation of duties principles, cardholders should not monitor themselves because they could conceal their fraudulent charges.

  When you frequently monitor, you can detect issues quickly. It also helps you deter issues from ever occurring —cardholders will know you monitor their spending. You should perform a risk-based transaction review (not random). Commonly, reviewers look for:

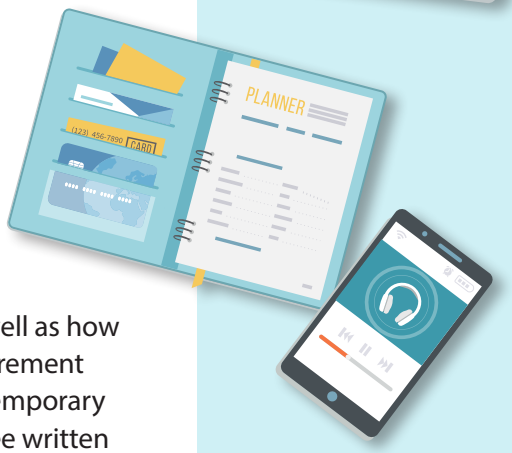
  - Declined and disputed transactions (to identify areas of concern and other red flags)
  - Non-standard, high-dollar transactions
  - Splitting of transactions to avoid a single purchase limit. Cardholders may use their own card to split a transaction, or that of another employee, and it may or may not occur on the same day.
  - Purchases on weekends and holidays
  - Purchases exceeding the single purchase limit (vendors can process these manually, and force a transaction even though it exceeds the single purchase limit)
  - Purchases of restricted and other questionable items
  - Transactions initiated by a separated employee, or an employee on leave
  - Transfer of a card to an unauthorized person
  - Personal purchases (for the employee's personal benefit)
  - Duplicate transactions



- **Perform an annual internal audit or review, if possible.** Ideally, an internal audit department should periodically review and test controls to ensure management has properly designed them and they function as intended. The internal audit department should also test credit card activity and follow up on cardholder infractions, to ensure management followed through with disciplinary actions. If you lack an internal audit department, consider contracting out or assign someone qualified internally to perform the review.

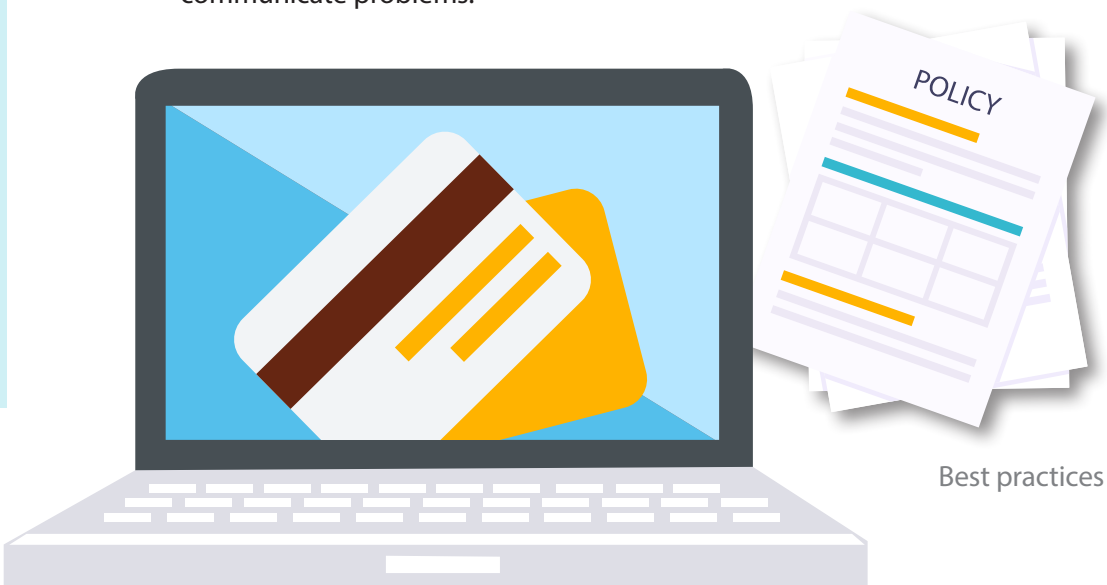
- **React to repeated issues.** As you identify issues when monitoring card activity, look for themes. Reemphasize your expectations to cardholders when needed. Consider whether your policy guidance or cardholder usage agreement needs updating, or if you need to improve your refresher training.

- **Monitor card rebates.** Review the rebate amount to ensure the credit card issuer accurately calculated it. Also, consider how you might maximize rebates, if advantageous and makes sense. You will need additional monitoring controls to successfully manage a credit card program; the rebate revenue can help you pay for it.



- **Actively enforce the policy.** Your policy should describe the consequences for cardholders who violate policy provisions, as well as how they will escalate. Your disciplinary actions might include: a requirement to complete additional training, formal written warning letters, temporary or permanent suspension of card privileges, inclusion in employee written performance evaluations, or disciplinary personnel action.

It is not enough to develop policy, you must also follow through and enforce it. Use a cardholder violation form to document and communicate problems.



Related resources

Municipal Research and Services Center: Credit card use policies

Washington State Auditor's Office: Best practices for travel expenditures

Government Finance Officers Association: Best practices: Using Purchasing Cards to Streamline the Purchasing Process

Washington State Auditor's Office: Budgeting, Accounting and Reporting System (BARS Manual) GAAP and Cash-Basis Purchase cards

Applicable Washington state laws for local government: RCW 43.09.2855, RCW 42.24.115

For assistance

This resource was developed by the Center for Government Innovation at the Office of the Washington State Auditor. Please send questions, comments, or suggestions to Center@sao.wa.gov.

Disclaimer

This resource is provided for informational purposes only. It does not represent prescriptive guidance, legal advice, an audit recommendation, or audit assurance. It does not relieve governments of their responsibilities to assess risks, design appropriate controls, and make management decisions.