Strengthening local government

Office of Local Government

GUIDELINE ON THE USE AND MANAGEMENT OF CREDIT CARDS

UNDER SECTION 23A OF THE *LOCAL GOVERNMENT ACT 1993*

September 2021

ADAPTED FROM NSW TREASURY POLICY AND GUIDELINES PAPER TPP-21-02 "USE AND MANAGEMENT OF NSW GOVERNMENT PURCHASING CARDS", FEBRUARY 2021

NSW GOVERNMENT

ACCESS TO SERVICES
The Office of Local Government located at:
Street Address: Levels 1 & 2, 5 O'Keefe Avenue, NOWRA NSW 2541
Postal Address: Locked Bag 3015, Nowra, NSW 2541
Phone: 02 4428 4100
Fax: 02 4428 4199
TTY: 02 4428 4209
Email: olg@olg.nsw.gov.au
Website: www.olg.nsw.gov.au

OFFICE HOURS
Monday to Friday
9.00am to 5.00pm
(Special arrangements may be made
if these hours are unsuitable)
All offices are wheelchair accessible.

ALTERNATIVE MEDIA PUBLICATIONS
Special arrangements can be made for our publications to be provided in large print or an alternative media format. If you need this service, please contact us on 02 4428 4100.

DISCLAIMER
While every effort has been made to ensure the accuracy of the information in this publication, the Office of Local Government expressly disclaims any liability to any person in respect of anything done or not done as a result of the contents of the publication or the data provided.

ISBN 978-1-922001-91-7

Produced by the Office of Local Government

Contents

Introduction

The *Local Government Act 1993* (section 8B) and the *Local Government (General) Regulation 2021* (clause 209) require all councils to establish effective internal control mechanisms for financial management, expenditure and accounting records.

The Guideline on the Use and Management of Credit Cards (the Guidelines), established under section 23A of the *Local Government Act 1993* (LG Act), support these legislative responsibilities and provide specific sector-wide guidance on how to establish effective controls in relation to credit card use and management. They are based on the NSW Treasury guidelines that apply to state agencies.

The Guideline suggests a minimum framework for the use and management of credit cards to ensure that risks associated with their use and management are minimised. The guidance in this document applies equally to the use of Purchase Cards (PCards) and Virtual Cards (VCards) where councils use these facilities.

It provides councils, county councils and joint organisations with the necessary information to put in place internal controls surrounding the establishment, management, review and maintenance of a credit card policy and related procedures. It also seeks to reinforce the responsibilities of council officers when exercising functions in relation to sound financial management.

The Guideline is structured in two parts: core responsibilities and operational guidance. The two core responsibilities and associated actions provide the foundation upon which councils should shape their credit card policy. Operational guidance expands on these actions using a risk-based approach and includes advice on both the management of a credit card program and the responsibilities of individual cardholders.

The use and management of credit cards by councils is an important element of council operations and internal controls that must be included in each council's risk management framework and regularly reviewed as part of the audit, risk and improvement committee's and internal audit function's four-yearly strategic work program[1].

From June 2022, each council (including county councils and joint organisations) in NSW will be required under section 428A of the LG Act to appoint an audit, risk and improvement committee to review the council's financial management, statutory compliance and fraud and corruption controls.

Each council will also be required under the *Local Government (General) Regulation 2021* to establish and operate an effective risk management framework and internal audit function to support the work of these committees.

1 The Guidelines for Risk Management and Internal Audit for Local Councils in NSW will provide more information about councils' statutory requirements in relation to audit, risk and improvement committees, risk management and internal audit. They will be made available at www.olg.nsw.gov.au

Part A
Developing a Credit Card Policy

Core Responsibilities

These core responsibilities are considered fundamental to establishing and maintaining an effective and efficient credit card policy and related procedures that ensures expenditure is always carried out in the public interest. Supporting each of these core responsibilities is a list of suggested actions that, when implemented together, will establish a minimum framework for the use and management of credit cards.

1 Core responsibility 1

The General Manager is ultimately responsible for the proper management and administration of credit cards within the council.

1.1 The General Manager shall ensure that an internal approval process is established for council officers and councillors (the Cardholder) to obtain and use credit cards. This should be consistent with the requirements of the Card Issuer.

1.2 The council's internal approval process should ensure the following before a credit card is provided to a Cardholder:

- the Cardholder has the appropriate financial and operational delegations to incur expenditure on behalf of the council
- the Cardholder has appropriate credit card limits set (monthly spend limit, transaction limit, and (only if deemed necessary for the smooth conduct of council business) ability for cash withdrawal determined and, if so, these limits include a cash withdrawal monthly limit and cash withdrawal transaction limit)
- the council is not exceeding its total borrowing limit or budget limits by issuing the credit card to the Cardholder.

1.3 The General Manager shall establish and implement a Credit Card Policy as well as procedures to support the credit card policy appropriate to the size of the council. As a minimum, the credit card policy and related procedures should address:

- roles and responsibilities relating to credit card use, management and administration. This may include Credit Cards, Purchasing Cards (PCards)[2], Virtual Cards (VCards)[3], Fuel Cards, Store Cards and CabCharge.[4],
- requirements for approval, issuance of credit cards and closure of accounts,
- criteria for eligibility to obtain a credit card,

2 Purchasing card (Pcard) refers to a credit card issued by the Card Issuer (generally a bank, building society or credit union) which is used by Cardholders to engage in transactions relating to the purchase of goods and services on behalf of the organisation. Pcards are also known as corporate cards, government cards and procurement cards.

3 Virtual card (vCard) refers to a credit card that is not issued as a physical card, rather a 16-digit number provided to the supplier for use in card-not-present transactions. The vCard card is not linked to a Cardholder but is established in the council's name (with one or many users). To protect the card security, typically one card is created for use with a single supplier (Merchant).

4 Note that some credit facilities, such as fuel cards, may be covered under different corporate policies, such as a vehicle management policy. If this is the case, noting this in the credit card policy is recommended and the principles outlined in this Guideline should be reflected in these associated policies.

- credit limits, thresholds and restrictions,
- restrictions, including on prohibited items and supplier merchant blocks,
- the types of payments that are to be procured via an alternative method to ensure consistency with other corporate policies (for example, via a purchase order or established council supply contracts),
- Cardholder training requirements,
- requirements for transaction acquittal, including independent reconciliation of the General Manager and Mayor's credit cards as well as the responsible accounting officer / Chief Financial Officer or any other officer that can approve payments for credit card expenditure, and guidance for staff on how to escalate concerns,
- requirements for reconciliation and approval (taking into consideration segregation of duties),
- transaction dispute processes agreed with Card Issuer,
- best practice for Cardholders to ensure the security of credit cards,
- the process for reporting lost or stolen credit cards with Card Issuer,
- infraction, issues management and account cancellation,
- reporting fraud and corruption processes,
- software management (including user access and security),
- Cardholder security digital records management, and
- processes for the review and continuous improvement of the council's credit card policy.

1.4 The council should ensure there is an accessible and up-to-date record of all authorised Cardholders (a Credit Card Register[5]) with approval records from the appropriate line manager as well as the credit card Program Administrator (see section 4.2), authorising the card issuance and credit limit.

1.5 The General Manager should maintain an accessible record of the council's credit card program borrowing limit and aggregate credit limit of individual credit cards currently issued, (as well as PCard, Fuel Card, Store Card, Cabcharge and VCard limits where applicable). This may be combined with the Credit Card Register.

1.6 The General Manager should undertake appropriate actions to not exceed the council's total program borrowing limit and may wish to adjust the credit card program total program borrowing limit to meet the ongoing needs of the council.

1.7 The General Manager should ensure that a direct debit facility is implemented with the Card Issuer for the automatic payment of monthly credit card accounts in full to eliminate any late payment fees and interest charges.

1.8 The General Manager should ensure that the risks associated with the council's credit card program are subject to a risk assessment as part of the council's risk management framework to ensure identified risk treatments remain adequate or are properly remedied in a timely manner. See section 5.3 for further information.

5 A Register may consist of retained credit card applications in a single file; a separate register; and/or a function report provided online by the Card Issuer.

2 Core responsibility 2

Cardholders understand and are accountable for the responsible use of credit cards.

2.1 Cardholders must use credit cards for business purposes only and in a manner compliant with council's credit card policy and related procedures.

2.2 In relation to using their credit cards, Cardholders are responsible for:

- complying with the terms and conditions of the Card Issuer,
- the safety and security of their card, card details and other requirements,
- knowing the administrative conditions of their card and account, including relevant limits, thresholds and restrictions,
- ensuring that the credit limits are not exceeded (purchases must not be split to negate single transaction limits),
- obtaining and retaining all relevant documentation for all transactions. The Australian Tax Office (ATO) stipulates that all transactions above $82.50 must have a tax invoice for GST purposes. It is recommended that all credit card transactions be substantiated, where possible, with an official tax receipt regardless of the amount, and
- the timely acquittal of transactions, ensuring the time given is no greater than the time stipulated by the financial institution to log a dispute over errant transactions.

2.3 Cardholders should notify the Card Issuer directly in the following circumstances to reduce the risk of fraudulent transactions occurring:

- the loss or theft of the credit card, immediately regardless of whether it is a working day or weekend, and/or
- awareness that an unauthorised transaction has occurred, at time of occurrence or at end of month reconciliation (whichever is the earliest).

2.4 Cardholders or their line manager should notify the credit card Program Administrator the next working day or as soon as practicable in the following circumstances:

- cessation of employment with the council,
- a change in the Cardholder's substantive role,
- a change in the nature of the Cardholder's responsibilities that no longer require the Cardholder to use a credit card (whether or not this includes a change in their substantive role),
- a change to the operational or financial delegation limits that are associated with the Cardholder's role,
- a prolonged leave of absence from performing their role (the council's credit card policy should advise what time period is considered a prolonged absence but is usually considered any absence longer than 8 weeks),
- the credit card has been suspended or cancelled,
- the loss or theft of the credit card, or
- on awareness that an unauthorised transaction has occurred, at time of occurrence or at end of month reconciliation (whichever is the earliest).

Part B
Operational Guidance

This Operational Guidance builds on the above core responsibilities by assisting councils to develop and tailor their credit card policy and related procedures to their size, complexity and risk profile, and provides Cardholders with information to help them understand their responsibilities.

3 Risk Management

3.1 A council's credit card policy and related procedures should seek to manage risks specific to the use of credit cards as part of the council's overall risk management framework. There are, however, particular risks associated with the use and administration of credit cards that will need to be identified and managed. Examples include:

- the risk of inappropriate use and waste (defined as any uneconomical, inefficient or ineffective use of resources, authorised or unauthorised, which results in a serious and substantial loss of public funds or resources),
- the potential for transaction and/or accounting errors (e.g. duplication of payments), and
- the application of inappropriate purchase methods (e.g. directly purchasing an item or service on credit card without assessment of any contract terms, rather than seeking to negotiate appropriate contract terms and conditions).

3.2 Risk is defined as the impact of uncertainty on objectives. In the context of credit cards, this risk will largely relate to those aspects of the use and management of credit cards that could affect a council's overall financial position and ongoing financial management. However, risks arising from the use and administration of credit cards can also affect other objectives including those associated with procurement, service delivery and/or reputation.

3.3 One of the most significant risks associated with credit card administration and use that can adversely affect a number of objectives is fraud. The Independent Commission Against Corruption (ICAC) provides some examples of the potential fraud risks associated with credit cards[6] including:

- a Cardholder charging personal expenses to the council credit card,
- a Cardholder and a client colluding to misuse a council credit card,
- a Cardholder using the card's personal identification number to withdraw cash for their own or another's benefit,
- a Cardholder falsifying, destroying or damaging receipts and other records, and
- one or more council officers colluding for improper benefit – for example, the Cardholder colluding with another council officer whose role is to check expenditure.

6 For further information on corruption prevention as it relates to credit cards, see https://www.icac.nsw.gov.au/prevention/corruption-prevention-advice-topics/credit-cards

3.4 While a number of risk types, together with specific examples of risks associated with credit cards have been provided here, it is important that councils engage in a structured risk assessment as part of their overall risk management framework to ensure that they are able to identify and assess the particular risks in relation to the use and administration of credit cards in their organisation. It is important not to rely only on previous experience to identify risks associated with credit card use. This is where it is useful when reviewing risk management strategies to involve key stakeholders including Cardholders, merchants and the Card Issuer.

Councils should also seek to keep up to date with new or emerging risks, especially those associated with the application of new technologies or during times of organisational change. Additionally, councils should endeavour to share their knowledge and experience with other councils, for example through joint organisations, in order to continually improve their management of these risks.

Councils should also refer to various audit reports of the Audit Office of NSW[7] and other jurisdictions[8] that have undertaken audit or assurance work relating to the use of credit cards to familiarise themselves with areas of concern that may be relevant to their organisational context.

4 Preventative Controls

Preventative controls are those designed to prevent errors and irregularities from occurring. Some examples of preventative controls for credit cards include:

4.1 Policies and Procedures

Setting out a council's expectations in a clear and well communicated credit card policy and related procedures is fundamental to the establishment of a strong control environment. Supporting procedures establish and standardise behaviours and help council officers, Cardholders and others to understand and fulfil their obligations.

Councils should consider the appropriate level of guidance required to ensure that their credit card policy expectations are understood and met by all council officers, Cardholders and other stakeholders. This may include, for example, supporting procedures on:

- card issue, transfer, and cancellation. Action to address damaged, lost or stolen cards should also be clearly described,
- routine review of issued cards, specifically to verify that credit cards are issued to staff with an identified business requirement and appropriate financial delegation (to purchase goods or services on behalf of the council) and to ensure that each Cardholder is still the appropriate recipient of a card,
- independent periodic monitoring and review of credit card use, management and overall performance across the council (see section 5.3 for suggested timeframes and further information),

7 For example, the 'Report on Local Government 2019': https://www.audit.nsw.gov.au/our-work/reports/report-on-local-government-2019 and 'Credit card management in Local Government': https://www.audit.nsw.gov.au/our-work/reports/credit-card-management-in-local-government

8 Refer to Australian National Audit Office reports such as https://www.anao.gov.au/work/performance-audit/defences-management-credit-and-other-transaction-cards

- the applicable billing cycle and standardising the approval, acquittal and authorisation of transactions,
- processes for transacting via internet, phone or in person with a credit card, including any mandatory or prohibited methods of transacting,
- the retention of appropriate supporting documentation (including electronic documentation) to be retained in connection with the use of credit cards. This should include information about actions to be taken where the appropriate supporting documentation is unavailable or has been misplaced, or for unusual transactions that might require more than standard supporting documentation,
- allowable uses of the credit card and supporting staff to address unrecognised transactions, discrepancies, errors or inadvertent misuse and procedures for following up issues with merchants and/or the Card Issuer,
- secure storage and security of cards,
- user access to, and security requirements on, administration systems and applications supporting the credit card program, and
- confidentiality and security surrounding the use of credit card and related data, specifically accessing, retaining and sharing of card and cardholder details or other transaction details.

4.2 Nominating a Program Administrator

Councils should nominate the role of Primary Program Administrator (PA) and back-up Program Administrator to act as a central point of contact for Cardholders, Merchants, and the Card Issuer. PA's undertake certain functions within the Card Issuer's Administration System not accessible to other council staff including Cardholders. A nominated PA should be a council officer with relevant skills and experience to undertake the role.

The responsibilities of Program Administrators may include:

- supporting the development, review, implementation and communication of the council's Credit Card Policy and procedures
- receiving completed and approved Cardholder applications and submitting applications to the Card Issuer
- ensuring that Cardholders and approvers have completed reconciliation processes in a timely manner
- liaising with the Card Issuer about the administration of cards, including issuance, changing of limits, thresholds and restrictions, and cancellations
- liaising with the Card Issuer regarding the Card Issuer's Administration System.

4.3 Credit Card Limits and Restrictions

Limits and restrictions should be set for each Cardholder. In setting these the council should consider:

- the responsibilities of the role or position held by the Cardholder,
- the level of current expenditure of the Cardholder (subject to total program borrowing limit of the council),
- the types of expenditures made by the Cardholder, and
- ensuring consistency with other corporate policies.

Spending Limits
Councils can tailor the spending limits for individual Cardholders. Councils should ensure that spending limits align with its procurement policy. For example, the limit might be set to $1,000 consistent with a procurement policy that requires a Purchase Order for any transaction greater than $1,000. Any exceptions should be clearly included in the credit card policy.

It is good practice for councils to set and communicate the following for each Cardholder:

- maximum limits for each monthly billing period
- maximum limits on the amount of any individual transaction.

Cash Withdrawals
It is expected that credit cards will not be used for cash advances or cash withdrawals. For this reason, cards are generally issued with an existing block on cash withdrawals.

Some councils may wish to allow for cash withdrawals in particular circumstances, such as work in rural and remote locations where credit card facilities are not as widely used or when Cardholders are travelling overseas. In those cases, the council will need to manage the cash limits in accordance with internal approval structures. In these instances, it is also good practice for councils to set and communicate the following for each Cardholder:

- maximum transaction limits for cash withdrawals
- maximum monthly limits for cash withdrawal.

Prohibiting 'Purchase Splitting' and certain types of purchases
'Purchase splitting' occurs where Cardholders split one transaction into several purchases in order to avoid exceeding credit limits. This is also known as 'order-splitting' or 'stringing' arrangements. While these types of arrangements will usually be in breach of the terms of use of credit cards, councils should also consider explicitly prohibiting 'purchase splitting' arrangements in its credit card policy and associated procedures. Where a single transaction would exceed a Cardholder's credit limit, alternative payment arrangements (along with appropriate approvals if such a purchase amount is above the person's financial delegation) should be sought. Councils should also look to prohibit the purchase of specific items deemed non-business related or else are covered under alternative purchasing arrangements (refer to risk management at section 3 above).

Merchant Blocks

Banks require suppliers or merchants to have identifying codes based on the type of goods or services they sell. Councils may wish to apply blocks to some merchants based on these identifying codes. This prevents Cardholders from using their credit card to transact with these suppliers or merchants.

4.4 Segregation of Duties

Segregation of duties provides an important mechanism for councils to better prevent and detect errors, fraud and misuse. Credit card expenditure should be subject to independent approval to incur expenditure.

Administration of a credit card program should, where possible, be undertaken by someone who is not a Cardholder. Where a council has limited resources, clearly documented alternative control activities (such as periodic review processes by appropriate council officers) should be implemented instead. In cases where the PA is also a Cardholder, additional controls should be established around the maintenance and reconciliation of the PA's credit card.

4.5 Approvals and Authorisations

As described above, councils should establish an internal approval process for the issuance and use of credit cards. Credit cards should only be issued to individuals who are council employees or on the governing body. Councils are bound by the terms and conditions set by the card issuer and each credit card should be used by the Cardholder only.

While credit cards are assigned to particular individuals, a council's financial and operational delegations will generally refer to roles/positions rather than individuals.

If a Cardholder changes role/position or temporarily acts in a higher position, the continued use of the credit card by that individual, which is likely linked to their previous role/position, should be reviewed, as well as the ongoing appropriateness of any card limits, thresholds or restrictions. Councils should also have processes in place to ensure that credit cards are immediately cancelled upon the cessation of a Cardholder's employment. This should take into account any extended leave a person might take prior to cessation of employment.

4.6 Safety and Security of Credit Cards

Credit cards provide access to council funds. For this reason, the safety and security of the card and its details are paramount to ensuring that a council's resources are not misused or misappropriated. There are various points of interaction between the Cardholder, Council, Merchant and Card Issuer where the credit card and/or card details may be mishandled.

Ongoing Security, Storage and Use of Credit Cards

Councils should make clear to Cardholders their expectations concerning the storage of credit card details. In particular, councils should assess the risks associated with allowing a Cardholder to use their card when travelling overseas.

While credit cards generally have some inbuilt security features, physical security is extremely important and Cardholders should not allow others to undertake transactions on their behalf using their card details.

Furthermore, councils should ensure that Cardholders are aware of card issuer and organisational emergency contact details, including those for the PA, in the event they become aware that the details of the card have been compromised.

Notifying Card Issuer and Council of Loss or Theft

Cardholders should be aware of the process for reporting lost or stolen cards. The Cardholder should immediately notify the Card Issuer (available 24 hours, 7 days per week), as well as their line manager and the Program Administrator. Council should provide all Cardholders with relevant organisational and Card Issuer contact information at the time of issuing the credit card.

'Card-Not-Present' Transactions

There can be additional risks associated with transactions where credit cards are not physically presented, such as in telephone and internet transactions. Councils should consider and address these specific risks in credit card procedures and training.

One of the key risks is the physical separation between the Cardholder and the merchant making it difficult in some circumstances for the Cardholder to verify the identity of the merchant. For all 'card-not-present' transactions, Cardholders should ensure, to the best of their knowledge, that the merchants they are dealing with are known and reputable.

Cardholders using the internet to pay for purchases should ensure that they are familiar with, and adhere to, their organisation's internet use and security policies and procedures. At a minimum, Cardholders should check that the merchant's secure site address starts with https:// and NOT http://. Sites that start with https:// have an added encrypted transaction layer.

Cardholders will need to ensure they obtain proper records of transactions conducted by mail, telephone or internet to support timely acquittal of transactions. Electronic receipts should be properly stored for ease of access at the time of acquittal.

4.7 Security of Systems, Data and Information

Cardholders, PAs and other stakeholders manage and maintain the credit card program through an integrated web of systems and applications. For those councils that operate an electronic system for the management and reconciliation of credit cards, regular consideration should be given to the impact of cyber security risks to their credit card program and risks related to accessing, storing and sharing credit card-related data and information (including Cardholder personal details, credit card numbers, transaction data). This applies to the extent that it impacts on manual, paper-based systems of credit card management.

PAs or other credit card system users with privileged or administration user system access (such as reporting or capability to manipulate or export data relating to card details, Cardholder details, merchant details, account or billing details or other transaction data) should receive an appropriate level of training and only hold a level of access commensurate with the role they are undertaking, with that access removed when they no longer need to have access. Controls should be put in place to ensure that such officers who have a credit card themselves are subject to independent oversight.

Practices for training and continual user awareness surrounding the use of credit card systems may be beneficial to controlling risks associated with systems use. Also, cyclic reviews (such as quarterly or biannually) of user access, automated updates to user access passwords or codes, and/or two-factor authentication are all examples on the types of controls that could be used.

Further, users should be trained on the appropriate classification, labelling and handling of information along with the Information Protection Principles[9] when dealing with council financial data and personal information. Councils should provide details on how users can ensure the proper handling and protection of data and information to ensure the basic obligations to protect information councils collect on their own activities and about individuals.

4.8 Training and Induction

Training Cardholders on their responsibilities is an important control that reduces the risk of credit card misuse. Training should provide Cardholders with the knowledge and skills to effectively deliver on their responsibilities and understand their accountability for credit card use. The training should cover all areas of credit card policies and procedures.

Training on, and council's expectations in relation to, credit card use and management, should be provided to Cardholders at induction or before being issued a credit card. In addition, it is recommended that the Cardholder signs a statement of responsibility to acknowledge their responsibilities with respect to the use and management of their credit card.

Training on the proper use of credit cards should also be provided to councillors, ideally as part of their general induction as new councillors that occurs at the start of each council term.[10] Councillors have a responsibility for the sound financial management and sustainability of the council under the *Local Government Act 1993*.

4.9 Ongoing Communications

An ongoing communications program is good practice as it allows councils to:

- reinforce their policies, processes and procedures, including those related to fraud and misconduct
- remind Cardholders of their responsibilities, including timely reconciliation
- update Cardholders and other council officers on changes to policies, processes, procedures or terms and conditions of use
- ensure awareness of various training and support facilities offered to Cardholders and other council officers.

9 See: https://www.ipc.nsw.gov.au/information-protection-principles-ipps-agencies

10 For further guidance on how to undertake induction and training for new councillors, visit the OLG website: www.olg.nsw.gov.au

5 Detective Controls

Detective controls are designed to identify and rectify errors and irregularities. Some examples of detective controls that councils may employ include:

5.1 Expenditure Acquittals and Reviews

Acquittal and review of credit card transactions are important detective controls for councils. In the first instance, acquittals will be undertaken by a Cardholder to compare expenditure from advice provided by the Card Issuer to their supporting documentation to ensure that transactions are accurate. This process should be completed as soon as possible and, if possible, within 30 days of advice from the Card Issuer to allow any disputed transactions to be reported to the Card Issuer in a timely manner.

A review of the Cardholder's transactions should also be undertaken by the Cardholder's direct manager. The Cardholder's direct manager (or in the case of the General Manager, the Mayor) is usually the most appropriate person to conduct the review as they will be familiar with relevant credit card policies and guidelines for credit card use and have knowledge of the activities of the Cardholder. However, where the council determines that the direct manager is not the appropriate person to exercise the review, they should nominate another reviewer based on the following considerations:

- seniority of the reviewer relative to the Cardholder
- independence of the reviewer
- knowledge of the Cardholder's activities
- knowledge of the council's credit card policy.

The reviewer will be responsible for forming a view on whether the expenditure incurred was for business purposes and was consistent with the Cardholder's responsibilities and activities. The reviewer should assess whether:

- the expenditure incurred was appropriate for the purpose and reasonable
- the expenditure categorisations align with those allowed by the council
- the appropriate supporting documentation has been attached
- financial systems ledger costings information is correct.

In addition to these processes, council should ensure that there are processes for regular independent reviews of a sample of Cardholder transactions.

There should be an audit trail to record the date of all reconciliations and reviews as well as to verify the identity of the Cardholder and reviewer.

Procedures and controls should also be established over the maintenance and storage of records of credit card reconciliations and other supporting documentation as relevant, and in accordance with council's record keeping obligations.

5.2 Detecting Fraud

Fraud by its nature is more difficult to prevent and detect than unintentional errors and irregularities. As fraud is an intentional act, perpetrators will often take actions to avoid detection. This includes circumventing existing controls. While any system of control cannot entirely eliminate the risk of fraud, it is necessary to identify and assess fraud risks and design controls specifically to mitigate the risk of fraud.

Protecting a council's resources from fraud and monitoring for suspicious activity of staff and/or third parties is not a simple task. While it may be appropriate for councils with large amounts of assets and/or expenditure to engage sophisticated and integrated fraud prevention and detection systems, all councils will benefit from targeted monitoring for fraud risk. This may include monitoring for:

- unusual or unexpected levels of expenditure
- transactions with unusual types of Merchants
- the use of 'suspicious' words, as identified by the council, to identify exceptions
- transactions for non-business items and services
- multiple transactions for the same or similar items or for the same amount
- inconsistency between expense description and merchant code
- consistent late submission of supporting documentation or outstanding reconciliations
- transactions that have occurred on weekends, public holidays or while the Cardholder is on a leave of absence.

However, it should not be assumed that fraud has occurred if an instance listed above is identified. There may be legitimate reasons for any of these occurrences. Rather, the indicators should prompt further inquiry to ensure that they reflect appropriate use of the credit card.[11]

5.3 Monitoring and Review of Credit Card Controls

Councils should design and implement a credit card monitoring and review schedule as part of its overall risk management framework. This schedule should provide a systematic and continuing assessment of internal controls of the credit card program to ensure that identified and implemented controls remain effective and fit for purpose. This should include testing whether existing controls are operating effectively using techniques such as re-performance, observation or inspection of documentation. Audit logs of the activities of PAs or other credit card system users with privileged or administration user system access should also be kept and reviewed as part of this schedule.

Regular reviews are also necessary to ensure the system of controls continues to effectively and efficiently mitigate credit card risks, because risks will not be static. Reviews with individual self-assessments or like reports being provided to line or senior management for review may include:

- user reviewed or guided self-assessment (based on a checklist or other tool that identifies key controls to be verified)
- line management or PA reviews (based on a defined set of controls to be verified. This may include data mining and analytics or guided assessment)
- independent or third-party reviews, e.g. internal or external audit.

Councils will need to assess the value of employing different monitoring and review methods. A range of frequent, lower cost, risk-based reviews in addition to less frequent major reviews may provide an appropriate level of assurance.

11 For further information about managing fraud generally, see https://www.audit.nsw.gov.au/our-work/reports/fraud-control-improvement-kit-meeting-your-fraud-control-obligations. Further information and guidance to prevent fraud and corruption is also available from ICAC: https://www.icac.nsw.gov.au/prevention

An adapted version of an example periodic monitoring and review frequency table (Table 1, below) designed by the Australian National Audit Office[12], provides some guidance on the different types of review and monitoring that councils should engage in, and the relevant timeframes.

Table 1: Suggested periodic monitoring and review timetable

Indicative Frequency	Nature of monitoring and review
Ongoing	• Recording of unusual events (e.g. record instances of reported personal use of credit cards so any recurrence is noted; record Merchants involved in disputed transactions). • Assess and act on overdue reconciliations by Cardholders.
6 – 12 months	• Review credit card use against credit limits for possible adjustments. • Review credit cards not used for a significant period to establish if they are still required. • Sample testing of transactions with higher risk of misuse (e.g. check whether transactions properly established value-for-money and compliance with guidelines; check whether transactions with duplicated details are Merchant error). • Statistical analysis of utilisation patterns (e.g. identify opportunities for centralised procurement of some types of goods). • Reconcile Individual Credit Card Application / Statement of Responsibility / Card Statements Issued with the Card Issuer's Card Management Reports.
1 – 4years	• Internal audit review covering credit cards as appropriate (e.g. processes for issue and return; whether reconciliation and review procedures are being followed). • Review expenditure in areas where judgement plays an important role (e.g. travel and meals) in order to assess whether the expenditure is remaining within public expectations.

12 Australian National Audit Office 2013, Controls over Credit Card Use: Report No. 35 2012-13, Australian National Audit Office, Canberra, viewed 3 June 2021.

5.4 Internal Reporting

Councils should utilise the Card Issuers Administration System to ensure that they are aware of each card issued to Cardholders within the council, including the relevant administrative conditions attached to each card. Managers should receive regular reports on credit card usage within their areas, including inactive accounts (where relevant), to allow for review and any updates to be made to the Credit Card Register.

5.5 Internal Audit

A council's Audit, Risk and Improvement Committee and internal audit function have a key role to play in ensuring the integrity of the systems, policies, processes and procedures in place, and should include a review of credit card controls as part of its four-yearly strategic work program[13] (See Table 1 above).

6 Other Controls

6.1 Automated Controls

Automated systems can greatly assist councils to ensure timeliness and support a consistent format for processes associated with credit card expenditure, for example, automated statements can be sent to Cardholders or an Expense Management System (EMS) can be utilised for transaction management and acquittal processes.

Councils should remain vigilant, however, to ensure that processes are being properly utilised and that they have clear control objectives and provide an audit trail that can be readily monitored and reviewed.

13 Refer to the Guidelines for Risk Management and Internal Audit for Local Councils in NSW issued by the Office of Local Government (www.olg.nsw.gov.au) for more information about audit, risk and improvement committee and internal audit work programs.


NSW
GOVERNMENT