EAST AYRSHIRE COUNCIL

CABINET – 21 MAY APRIL 2008

NEGOTIATED PROCUREMENT OF HOSTED CARD PAYMENT SERVICE

Joint Report by Depute Chief Executive/Executive Director of Corporate Support and Executive Head of Finance & Asset Management

1. PURPOSE OF REPORT

1.1 To seek the approval of Cabinet for the negotiated purchase of a Hosted Card Payment Service contract which will support the Council's move towards full compliance with Payment Card Industry Data Security Standards (PCI DSS).

2. BACKGROUND

2.1 Civica is a well established company involved in the delivery of IT solutions to local government for more than 20 years. Over 80% of all local authorities use one or more of their products. East Ayrshire Council currently uses Civica to provide Housing and Council Tax Benefit Administration, Council Tax and Rates Collection Systems and Cash Receipting/Income Management all of which have assisted in improved service performance.

2.2 The main financial systems of general ledger, creditor payments and sundry debt management are currently being migrated to a Civica based system – Authority Financials.

3. CURRENT POSITION

3.1 The Civica Cash Receipting/Income Management application (ICON) provides functionality to input and process card payment transactions online and directly with the banking systems. Card payments for the Council are processed through one of the Civica ICON user interface products, i.e. Local Office Workstation, Internet and Intranet payments, Automated Telephone Payments. The Palace Theatre processes booking payments through the Ticket.com application. Both ICON and Ticket.com utilise a third party product from CommsXL to process the card transactions to the bank.

3.2 PCI DSS is a compulsory security standard that all merchants (card payment transaction processors) must comply with as defined in the commercial contracts with their acquiring bank. Failure to do so could result in financial penalties from the acquiring bank, reputational damage/loss of customer confidence, and potentially loss of ability to process card payment transactions. The requirements of PCI DSS are extremely detailed, and are subject to change over time, as new risks or risk management methods emerge with new technology. The requirements cover all aspects of card payment transactions from the software applications, telephony and communications networks, data storage and business processes.

3.3 Approximately 45,000 card payment transactions are processed per year through ICON and 5,000 per year through Ticket.com. The Council currently stores at least 6 months worth of detailed card payment transaction data on two secure card servers, one for ICON and one for Ticket.com. Retention of detail is required for refunds and disputed transactions.

3.4 The Council's current position in regard to each of the PCI DSS requirements has been assessed and a risk and management analysis produced. Several requirements have been identified where the risks are high and the measures required for risk management would require significant financial and resource costs. It is unlikely that the Council could make systems fully compliant in the short to medium term although compensating controls to demonstrate that the Council is proactively seeking to comply with these requirements are in place. It is understood that most local authorities are in a similar position. A draft Sensitive Data Policy and Data Security Incident Response plan have been circulated for internal review.

4. PROPOSAL

4.1 It is proposed that the Council outsource the card payment transaction handling to mitigate the most serious financial and reputational risks and risks which would have significant costs to eliminate. This will be done in a staged manner so as to minimise disruption to the Council's business processes.

4.2 The outsourcing option will remove all of the detailed card payment transaction information from Council servers. All internet payments will be directed through an externally hosted website. This is included in the stated costs. Some additional work, and potentially costs, will be required to integrate Ticket.com with the outsourced card payment transaction handling.

4.3 A revised risk assessment will be undertaken after implementation if this proposal is accepted. The potential to manage further risks will be examined and proposed where appropriate. This could potentially include further mitigation by outsourcing of Automated Telephone Payments, replacement of the Local Office Workstation and WebStaff Intranet interfaces with externally hosted interfaces. These options are an integral part of the development and modernisation of the Civica ICON suite of products which are not sufficiently established for consideration at this point in time.

5. EXPECTED BENEFITS & OUTCOMES

5.1 The partnership of Civica and CommsXL can provide an outsourced function that provides a level of data security that could not be replicated in-house. The Council's most serious financial and reputation risk would be the wholesale loss of card payment transaction information. This risk would be mitigated by outsourcing.

5.2 The work undertaken to integrate Ticket.com with the outsourced solution will utilise an application interface, Paylink XML, already purchased by the Council. The work will involve Civica negotiating with Ticket.com to ensure the stability of the product during the change process.

5.3 The outsourcing option, and any potential future extension to outsourcing, will include product upgrades, some of which would have a licence cost implication to host in-house. The Council will benefit from a more rapid transition to upgraded and replacement products than could be achieved in an in-house environment.

5.4 The core functions of Fund Distribution and Bank Reconciliation will remain within the Council Finance service. There will be some business process changes required to reconcile the card payments.

5.5 The outsourced option should provide a mechanism to integrate card payment transactions with other applications. Civica have already demonstrated several examples where this is working at other sites.

6. FINANCIAL IMPLICATIONS

6.1 Civica UK Ltd has indicated that the initial set up of the hosted card authorisation service would be in the region of £7,000. Thereafter annual costs associated with the volume of transactions together with annual licence/subscriptions would be in the region of £17,500 per annum. It is expected that these costs will be incorporated within the overall bank charges budget and recovered through the normal reallocation of these costs across Council services.

7. IMPLEMENTATION

7.1 The project will follow a "PRINCE2" project management methodology and a project board will be established to ensure that all key decisions are taken and implemented in a timely and effective manner, which will require representation from Information Technology, Finance and other key service users as appropriate.

7.2 A Project Director, responsible for the overall coordination of the implementation plan, ensuring that timescales and deadlines are met, and appraising the project board of developments and progress throughout the project. A representative of the Company will be nominated to the project and will be responsible for all input together with attendance at project review meetings and for liaison with the Project Director.

8. LEGAL/POLICY IMPLICATIONS

8.1 The Council's Standing Orders paragraph 9(2) requires formal committee approval where it is proposed to negotiate a contract with one party.

8.2 Failure to comply with the Payment Card Industry Data Security Standards could result in financial penalties being imposed on the Council.

9. RECOMMENDATIONS

9.1 It is recommended that the Cabinet:

i) approves the negotiation of contract terms in respect of the procurement of a hosted card payment service and related services with Civica Financial Systems Ltd in terms of paragraph 9(2) of the Council's Standing Orders relating to contracts; and

ii) otherwise notes the contents of the report.

Elizabeth Morton
Depute Chief Executive/Executive Director of Corporate Support

Alex McPhee
Executive Head of Finance& Asset Management

RB/JB
3 April 2008

LIST OF BACKGROUND PAPERS
Nil

Members wishing further information should contact Robin Baker, Financial Controller, (Tel 01563 576331) or Jacqueline Shearer, IT Account Manager (Tel 01563 576814).