Report to:	Strategic Policy & Resources Committee
Subject:	To seek approval to go to tender for the supply of I.T. Security Measures required for Regulatory Compliance
Date:	23 January 2009
Reporting Officer:	Trevor Salmon, Director of Corporate Services
Contact Officer:	Rose Crozier, Head of Information Services Belfast

Relevant Background Information

1 Several high profile cases have been detailed in the media in recent months regarding sensitive data going missing on lost or stolen laptops, or on CD's or other removable media or portable devices.

In April 2008 Audit, Governance and Risk Services produced the **"Final Audit Report - Computer Use & Legislative Compliance"** which identified several areas where the Council could be exposed to major risk of legal/financial/reputational damage.

They detailed several recommendations including:-

"consideration be given to the benefits of encrypting data held on BCC's IT Systems, particularly data of a confidential nature. Consideration should also be given to encrypting any portable IT devices belonging to the Council e.g. laptop hard drives, USB devices etc." and

"that consideration be given to implementing a solution to allow BCC to better manage the use of removable media devices e.g. CDs, USBs etc. Any potential solution should allow the Council more control over what can and cannot be copied to and from USB and similar devices as well as providing traceability of what data is being copied to these devices."

2. As the Council now allows various on-line payments on their Web-Sites and in so doing processes credit card details, we are bound to comply with the payment card industry (PCI/DSS) regulations. Among other things, these regulations require us to analyse our security logs for possible security breaches. These logs are continually produced by all our servers, network and security devices. Each of these logs may have many thousands of entries each day and as such this task cannot be done manually. ISB are therefore seeking to purchase a Security Log Analyser tool.

3. The Local Government Auditor has advocated the use of complex passwords to gain access to our Corporate information systems. Many users need access to several systems. There is a risk that users would be unable to remember several complex passwords and would resort to noting these passwords down. This would increase the risk of their discovery and use by unauthorised persons to access corporate data. A Single Sign on Solution would only require users to remember one complex password to gain access to all their systems.

Key Issues

There are many solutions commercially available to address each of these issues. A lot of work has already been done in researching which of these solutions best fit the Council's requirements, both in terms of existing systems/infrastructure, and financial and human resources required to employ these solutions.

The introduction of encryption/device control solutions (sometimes referred to as Data Leakage Prevention solutions) and a Single Sign On solution will impact on working practices within the Council requiring an awareness campaign and some basic user training. More complex training of ISB personnel will also be required to administer these solutions and the Security Log Analyser.

The awareness campaign will help to smooth the implementation of the solutions, and also educate staff on adherence to our Policy on Using Computers.

Resource Implications

Financial

The estimated costs of the solutions are :

1.	DLP - Encryption/ Device Control	- £65k
2.	Security Log Analyser	- £30k
3.	Single Sign On	- £70k

Provision for this expenditure has been made in the Council's Capital Program.

Human Resources

Training will be required for a number of ISB staff to enable them to administer the solutions.
Basic training will be required for all staff using the Council's ICT facilities.
Working practices throughout the Council will change somewhat in that staff will not be permitted to use removable media unless there is a business case. Individual departments will be required to state these business cases and detail which laptops and mobile devices need to be encrypted.

Asset and Other Implications

Encryption of mobile devices such as Laptops, Smartphones and PDA's will reduce the Council's exposure to risk should they be lost or stolen.

Encryption of data which is to be transferred on removable media such as USB memory keys or CD/DVD's will reduce the Council's exposure to risk should they be lost or stolen.

Recommendations

It is recommended that the Council invites tenders for the provision of the following:

- a combined Data Encryption/Device Control Solution
- a Security Log Analyser tool
- a Single Sign On solution.

Key to Abbreviations

PCI/DSS Payment Card Industry Data Security Standard
PDA's – Personal Digital Assistants e.g. Blackberry
DLP Data Leakage Prevention