

# Statement on internal control

## 1 Scope of responsibility

As Accounting Officer, I have responsibility for maintaining a sound system of internal control that supports the achievement of NS&I policies, aims and objectives, while safeguarding the public funds and departmental assets for which I am personally responsible, in accordance with the responsibilities assigned to me in HM Treasury's *Managing Public Money* document.

As Accounting Officer I retain sole responsibility for the system of internal control within NS&I. I am assisted in discharging this responsibility by the board, which, in addition to me and the other NS&I Executive Directors, comprises four independent Non-executive Directors and two representatives of HM Treasury, who provide the key assurance link back to the Treasury Ministers.

The Treasury Minister, while maintaining accountability, has delegated day-to-day dealings with NS&I to HM Treasury's Debt and Reserves Management (DRM) team. The NS&I board has assumed overall responsibility for monitoring the effectiveness of the Agency's risk management processes. My senior staff and I also hold regular briefing meetings with other relevant HM Treasury teams, and a monthly performance report is sent to DRM as part of our overall governance arrangements with HM Treasury.

## 2 The purpose of the system of internal control

The system of internal control is designed to manage risk to a reasonable level rather than to eliminate all risk of failure to achieve policies, aims and objectives. It can, therefore, only provide reasonable and not absolute assurance of effectiveness. The system of internal control is based on an ongoing process designed to identify and prioritise the risks to the achievement of departmental policies, aims and objectives, to evaluate the likelihood of those risks being realised and the impact should they be realised, and to manage them efficiently, effectively and economically. The system of internal control has been in place in NS&I throughout the year ended 31 March 2010 and up to the date of approval of the accounts, and accords with HM Treasury guidance.

## 3 Capacity to handle risk

The board, Audit Committee and Executive Management Team (EMT) have primary responsibility for identifying and monitoring the key risks which NS&I faces. The board delegates the responsibility for overseeing the risk management process to the Audit Committee, with the Audit Committee reporting back to the board after each meeting. The Audit Committee, chaired by an independent Director, is responsible for providing assurance, in conjunction with internal and external auditors, to the board and myself as Accounting Officer on the existence and effectiveness of the overall processes for managing risk within NS&I and within those parts of Siemens concerned with NS&I business.

NS&I has a risk management strategy, a risk management framework and agreed risk management reporting protocols, based on government and financial services industry practice. The framework, along with NS&I's risk appetite, is reviewed and approved annually by the Audit Committee.

Every month the EMT considers whether there are any new risks to the business to be registered and discusses the key risks as part of its monthly risk review. The Audit Committee formally reviews the key risks at each meeting and the board bi-annually, to ensure that they remain valid and complete in the light of changing circumstances in the year and business plans for the coming year.

NS&I's business model means that we are critically reliant on our business partner, Siemens, for the delivery of our strategic objectives. Consequently, we have established joint processes with Siemens to manage the partnership as one business. These include Siemens' representation at relevant committees; joint working between project offices; joint project teams; and close co-operation between Siemens' Audit and Risk Management Team and our own internal auditors. Across the whole business, Executive Directors and operational managers are responsible for embedding risk identification and management within the design, documentation and operation of business processes, in line with agreed risk tolerances.

NS&I's committee structure is reviewed every year to enhance governance, empower staff and include Siemens personnel in all appropriate areas. Compliance, Risk, Fraud and Security functions have all been strengthened. Key risks are shared with HM Treasury through the Audit Committee.

The risk management process is led by the EMT, which comprises the Executive Directors and the Siemens Account Director responsible for the NS&I account, and is responsible for:

- implementation of the risk management strategy
- developing and overseeing the risk management framework
- identifying and evaluating strategic risks
- designing, operating and monitoring a suitable system of internal control.

#### 4 The risk and control framework

The management of risks is a key responsibility of the EMT, senior managers and risk policy owners. They are responsible for ensuring the proper management of risks and the implementation of the risk management strategy and framework within their respective directorates and teams.

Senior managers are responsible for the implementation of self-assessment processes and ensuring that line management understands and complies with these policies, and provide assurance back to the EMT that risks are being managed within agreed appetite. Assurance includes reviews of relevant management information, including key risk indicators, service issues and incidents, risk registers and progress on addressing internal and external audit issues.

An analysis of key risks and the consequent significant sub-risks has been established through an ongoing programme of individual and collective discussion with the Executive Directors. With very few exceptions where sub-risks have been retained by the Executive Directors, all sub-risks have been allocated to senior managers. An organisation-wide risk register records all significant risks identified, links lower-level risks through to the key risks, and records mitigating controls and named risk managers. The Audit Committee reviews the key risks at each meeting to ensure that

they remain valid and complete and are being effectively managed in the light of business plans for the coming year.

Our organisational risk appetite is approved annually by the Audit Committee and each key risk and sub-risk identified is assessed both before and after controls using NS&I's risk appetite matrix. Reviews of risks and their risk scores are performed regularly by senior managers and the EMT. Where further action is necessary to reduce exposure, the action, and its intended effect on the status of the risk, is logged, responsibility allocated and a completion date agreed. This ensures that there is ongoing tracking of any risk where exposure remains unacceptably high despite the controls that are in place. These risks are flagged as red, reviewed monthly by the EMT and reported to the Audit Committee.

As part of the annual planning cycle, senior managers are required to identify the significant risks that could impact on the achievement of each main element of their proposed business plans for the year. These risks are then compared with the existing risk register, which is amended as necessary.

Contingency plans are in place or are being implemented for all sub-risks where exposure is inherently unacceptable.

A programme management function ensures that all projects are subject to formal project management disciplines, including an assessment of inherent and residual risks, and regular reviews are undertaken of project and programme risks. The results are overseen by the relevant project board, the EMT, the Audit Committee and the NS&I board.

Senior managers provide assurance to the relevant Executive Directors either that they are satisfied that all their sub-risks are adequately controlled, or that plans are in place to provide that control. In addition, Executive Directors provide me with equivalent assurance for the key risks for which they have responsibility. They also provide me with assurance that an adequate system of internal control operates within their directorates, and that, to the best of their knowledge, their staff comply with all relevant legal and regulatory requirements.

The risk management process continues to be enhanced.

The key achievements in 2009–10 include:

- the introduction of new methodologies for tracking risk indicators to build on our existing policies and risk register
- the further embedding of Treating Customers Fairly within our culture
- the continuing investment in our fraud controls, including introduction of a new customer authentication security system for online and phone transactions
- the development of new e-learning modules to provide more effective compliance training for staff
- the continued embedding of compliance more deeply into our delivery partner, Siemens
- the movement of all customer data into our new purpose-built data centres, providing a more secure environment and enhanced business continuity
- the refinement of the effectiveness of our governance committees to ensure that they are working effectively.

The key risks that NS&I faces – and how they are being managed – are noted on pages 34–35.

Plans for 2010–11 include the continued strengthening of our risk management and compliance assurance processes and increased investment in information security and fraud risk management capabilities.

## 5 Statement of information risk

NS&I holds personal information relating to its customers and readily acknowledges its responsibility to ensure that this information is accurate and up to date, and its duty to ensure that the personal information entrusted to it is properly safeguarded from loss and unauthorised access.

In December 2008, following a review of data-handling in government, the Cabinet Office published Her Majesty's Government's (HMG) *Security Policy Framework*, which sets out mandatory requirements for government departments on protective security, covering physical, personnel and information security.

NS&I has followed the Cabinet Office's recommendations on information security, and is complying with the *HMG*

*Security Policy Framework*. NS&I undertook a gap analysis of practice against the Cabinet Office data-handling guidance and the *HMG Security Policy Framework*, and developed an action plan to address any gaps.

NS&I has produced clear guidance for NS&I staff and those of delivery partners for the management of personal data, and has introduced procedures to ensure that any information shared with third parties is properly authorised, protected at all times, and delivered securely.

In 2009–10, all NS&I staff received training in data protection and information security through e-learning packages, supported by face-to-face training in protectively marking information. In 2010–11 this will be expanded to include Siemens staff working for NS&I.

NS&I regularly refreshes the encryption of laptop hard drives in line with Cabinet Office guidance. For data that cannot be transmitted electronically, it has implemented bulk data transfer via disk using approved encryption and defined procedures.

An information charter is available on the NS&I website.

NS&I's risk register includes a number of sub-risks on data-handling and information assurance. NS&I has zero tolerance for information asset losses, and will continue to reinforce this through policies and procedures and staff acceptance of them.

Roles and responsibilities for information assurance within NS&I have been clearly defined.

NS&I has appointed a network of Information Asset Owners whose role is to understand what information is held, what is added and what is removed, how information is moved and who has access, so as to understand and address risks to the information they use. This role will be extended to Siemens during 2010–11. The Information Asset Owners will provide additional overall assurance quarterly on the use and security of the data for which they are responsible.

The enhanced programme of vetting for all NS&I staff will be extended during 2010–11 to include those in Siemens handling NS&I customer information.

In May 2010 NS&I Head Office moved to a new office with higher security specifications and controls. All information and IT was moved securely to the new location or storage without any incident.

NS&I's policies will continue to be reviewed to ensure that they provide a secure environment for information-handling and to ensure that they continue to meet the requirements set out in the *HMG Security Policy Framework*. All staff will be required to provide written confirmation that they are aware of the policies, and the responsibilities that the policies place on them.

## 6 Review of effectiveness

As Accounting Officer, I also have responsibility for reviewing the effectiveness of the system of internal control. My review of the effectiveness of the system of internal control is informed by:

- the work of key governance committees: the board, Audit Committee and EMT
- those Executive Directors and senior managers within the Department and Siemens who have responsibility for the development and maintenance of the internal control framework. They provide me with assurances that they are satisfied either that their key risks are adequately controlled, or that plans are in place to provide that control
- the work of the internal auditors, which is based on management's assessment of risk throughout the business
- comments made by the external auditors in their management letter and other reports, and
- other external verifications, including: our performance in the Financial Ombudsman Service tables – see page 11; our accreditation by the new Customer Service Excellence award – see pages 11–12; Investors in People accreditation – see page 18; and the escalation and appropriate resolution of two isolated customer service issues – see pages 12–13.

I have been advised on the implications of the results of my review of the effectiveness of the system of internal control by the board and the Audit Committee, and a plan to address weaknesses and ensure continuous improvement of the system is in place. The board, via the Audit Committee, satisfies itself as to the adequacy of the risk management process and reviews the key risks of the Department and

the effectiveness of mitigating actions, including the commitment and speed with which corrective actions are implemented. The board, via the Audit Committee, also reviews the internal and external risk profile for the coming year and considers if current internal control arrangements are likely to be effective. The Audit Committee also reviews annually the assurance on the overall system of internal control provided by the Head of Internal Audit, and advises the board of its assessment of the internal control system.

Internal Audit, led by KPMG from 1 July 2009 (Deloitte up to 30 June 2009), provide the Audit Committee with regular reports on internal audit activity throughout the year. They also provide an overall, independent opinion for the year on the adequacy and effectiveness of NS&I's risk management, control and governance processes. For 2009–10 the Head of Internal Audit concluded that, based on the work undertaken in 2009–10, these processes were adequate and effective to manage the achievement of NS&I's objectives and where work identified opportunities for improving controls and procedures, management responded positively.

In my opinion, there has been a continued improvement in the overall control environment during the year and there are no significant control weaknesses.

We will continue our ongoing process for assessing internal controls against best practice across all systems, processes and products. The approach to reviewing effectiveness and plans to ensure continuous improvement will be further refined in 2010–11.

*Jane Platt*

**Jane Platt**  
**Chief Executive**  
**National Savings and Investments**  
 30 June 2010