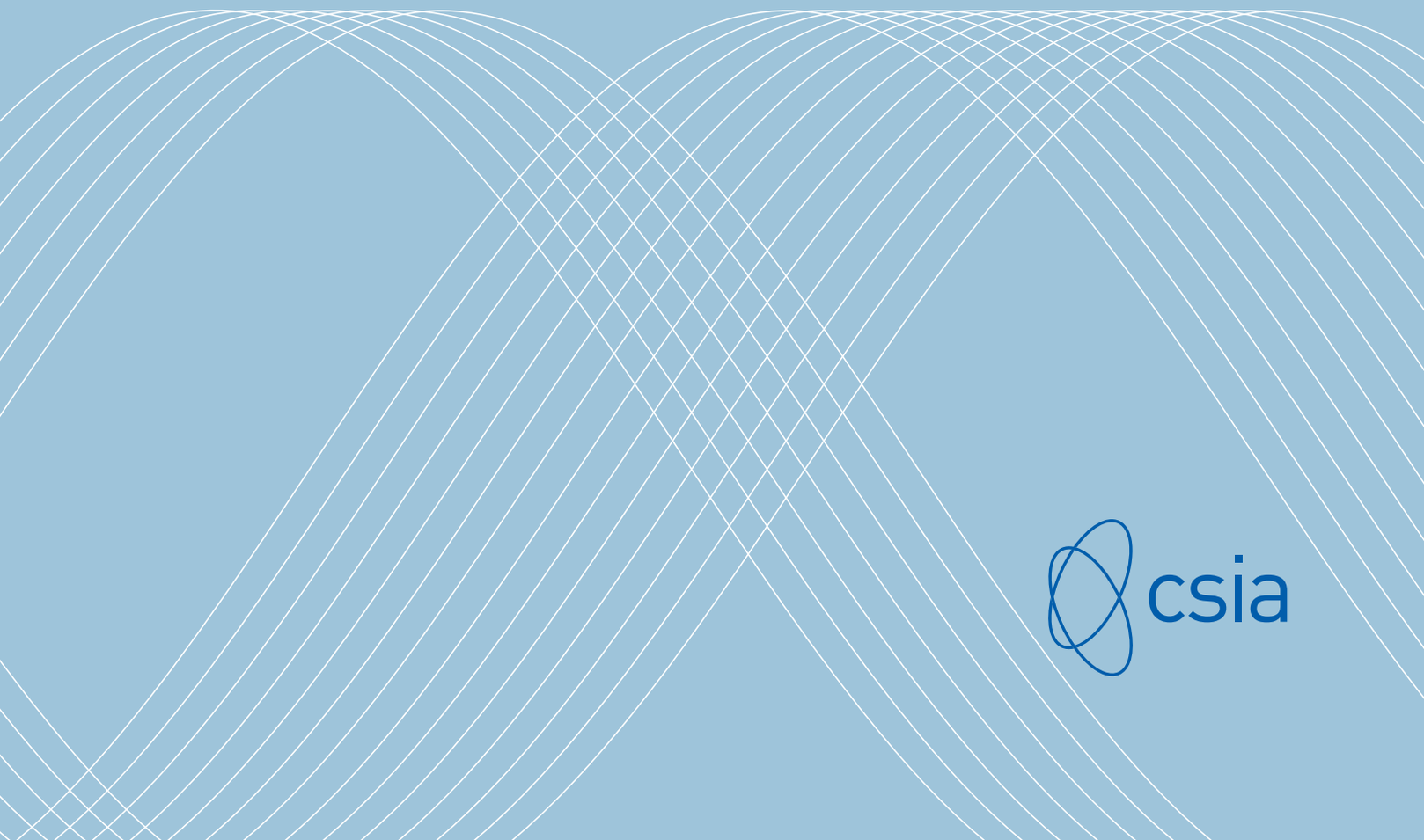
CabinetOffice

Central Sponsor for Information Assurance

# A National Information Assurance Strategy

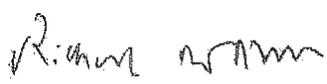


# Foreword

Information and communications technology is changing the way that the public, the private sector and the third sector deliver services, allowing Government, organisations and individuals to connect in more varied ways than ever before. The Transformational Government agenda is designed to take full advantage of this.

Information is a valuable asset that must be safeguarded. In the case of information held by public authorities and businesses, especially personal information, people want to be certain that it is held securely, maintained accurately, available when necessary and used appropriately. Information assurance (IA) is the term given to the management of risk to information. Effective IA ensures that the opportunities provided by new technology can be exploited to maximum benefit.

This National Information Assurance Strategy sets out a coherent approach to managing information risk by making it an integral and effective part of normal business process. Partnership between Government and industry is and will continue to be vital in delivering the clear and agreed standards and products and services that are necessary to effective IA. A Delivery Approach underpinning this Strategy will set out how the Government intends to develop this relationship further, build on existing good practice and drive the wider engagement to ensure that all organisations and individuals across the UK are able to make full use of the opportunities that technology offers us.



**SIR RICHARD MOTTRAM**
Permanent Secretary, Intelligence, Security and Resilience

# Contents

# Executive Summary

## Background

**1.** Information and communications technology (ICT) is a critical asset for any organisation; its exploitation is fundamental to the achievement of business objectives. However, major changes in the way that ICT is used have called for a revision of the previous Information Assurance (IA) Strategy, published in 2003. Government Departments have committed to revolutionise the provision of public services through ICT (the Transformational Government agenda). Embedding IA within the ICT that delivers these public services is a vital part of enabling this agenda. A revised National Information Assurance Strategy (NIAS) is required.

## New Vision

**2.** This revised National IA Strategy meets these challenges by developing the 2003 approach to cover the whole of the UK using a broader approach to IA. It has the following vision for 2011:

*A UK environment where citizens, businesses and government use and enjoy the full benefits of information systems with confidence.*

## Strategic Outcomes

**3.** The vision has three strategic outcomes:

- Government is better able to deliver public services through the appropriate use of ICT;
- The UK's national security is strengthened by protecting information and information systems at risk of compromise;
- The UK's economic and social well-being is enhanced as government, businesses and citizens realise the full benefits of ICT.

## Threat & Vulnerability

**4.** To determine the approach of this Strategy, the threats to the UK's ICT must be understood. These encompass not only attack risks such as e-crime, ID fraud and theft, but also the greater vulnerabilities associated with the ever increasing pace of ICT development and the risks of operating in a global marketplace.

## Benefits

**5.** The benefits to Government and the public sector of embedding IA in its use of ICT are significant:

- Enhanced confidence and trust in the way that information is managed will enable delivery of the Transformational Government agenda;
- Reducing the risk of potential financial, reputational and operational damage to organisations from the growing risk of compromise to ICT;
- Ensures that Departments will get the most appropriate and best value IA products / services.

**6.** The Strategy represents a national approach and implementation within Government is intended to bring wider benefits to industry and the general public:

- ICT and IA industries will benefit from more timely, relevant and valued engagement with government;
- The wider Private Sector and government will benefit from sharing best practice for IA and management of information risks;
- Citizens will benefit from safer access to e-enabled public services and an improved awareness of how to protect their own electronic devices.

## Approach

**7.** The strategic outcomes will be achieved by focusing on three objectives. These will have important implications for the way that organisations, particularly within government, do business.

**Objective 1:** *Clear and effective information risk management by organisations.*

- Clear board-level ownership and accountability for information risks will be required;
- Where information is shared, a single point of risk ownership will be identified.

**Objective 2:** *Agreement upon and compliance with approved and appropriate IA standards.*

- Organisations, particularly those within, or linking to government, will operate within a national framework of IA common standards;
- Trust and confidence in the use of information will be maintained through an effective model of compliance with these standards.

**Objective 3:** *The development and availability of appropriate IA Capabilities.*

- Government will work more closely with wider sectors in the development of 'Capabilities' to enable organisations to manage information risks;
- These capabilities include: availability of the right products and services; coordinated and appropriate efforts on innovation and research; improved professionalism, and awareness and outreach.

## Delivery

**8.** Recognition of the importance of an effective governance structure to provide leadership on IA and appropriate mechanisms for the delivery of these objectives is at the heart of this Strategy. Within organisations too, a commitment at the top to provide clear leadership on this issue will be vital to effecting the cultural change required.

**9.** The NIAS is owned by the Official Committee on Security (SO). To ensure that a business approach to IA is taken across central government, this community will look to the Information Assurance Policy and Programme Board (IAPPB) and the Chief Information Officer (CIO) Council working closely together to enable implementation of this Strategy, alongside delivery of the Transformational Government agenda.

**10.** Work to deliver the NIAS on behalf of these communities will be driven by a 'Wider IA Centre' (WIAC) comprising the Central Sponsor for Information Assurance in the Cabinet Office (CSIA), CESG and the Centre for the Protection of National Infrastructure (CPNI). Where existing effort on IA is ongoing this will be aligned with new work under the direction of the IAPPB.

**11.** Where the approach to IA set by the IAPPB has a direct bearing on closely related agendas, for example around protective security or counter-terrorism, the WIAC will ensure that the appropriate bodies are aware of and brought into the decision-making process, as required.

**12.** The scope of the NIAS means it will be necessary to implement in stages. Therefore, an effective leadership and governance model will initially be a priority to enable implementation across government. The first version of the supporting Delivery Approach sets out how such a model is to be put into place to deliver actions and activities across government.

**13.** However, the governance structure will also need to bring in wider organisations to implement the Strategy nationally. To this end, more detail on how other sectors can best be engaged through the governance framework will be provided in subsequent iterations of the Delivery Approach after further consultation.

# Introduction

**14.** Information is a critical asset for any organisation. Its exploitation is fundamental to the achievement of business objectives. The Government sets out here a National Strategy for Information Assurance (NIAS) to enable organisations and individuals in the UK to fully exploit the benefits of information and information and communications technology (ICT), while at the same time ensuring that enduring strategic, national priorities are maintained.

**15.** The term 'information assurance' (IA) is used to describe confidence in the processes of information risk management. Effective IA should ensure appropriate levels of availability, integrity, confidentiality, non-repudiation and authentication of information and information systems. This confidence is particularly important in the present environment, which is subject to unprecedented levels of malicious activity with intent to compromise UK information and information systems.

**16.** This document is to be supported by a more detailed IA Strategy Delivery Approach, which will set out further detail on implementation. Together, both documents will provide organisations with an approach to managing their information risks within a national framework. Organisations may also find it useful in developing related elements of organisational business continuity, disaster recovery and wider resilience planning.

## Vision

**17.** The vision for this Strategy is a UK environment where citizens, businesses and government use and enjoy the full benefits of information systems with confidence.

## Strategic Outcomes

**18.** Three strategic outcomes will be achieved by embedding IA in the way that ICT is used across the UK:

- *Government is better able to deliver public services through the appropriate use of ICT;*
- *The UK's national security is strengthened by protecting information and information systems at risk of compromise;*
- *The economic and social well-being of the UK is enhanced as government, businesses and citizens realise the full benefits of ICT.*

**19.** The achievement of the Transformational Government agenda is a key driver for this Strategy (see text box on page 5). Fundamental to the better delivery of public services through ICT is enabling effective communications and sharing of information between departments, as under the Shared Services Agenda, while at the same time ensuring the two latter strategic outcomes are met. The Delivery Approach will set out how all three of these outcomes are to be achieved by 2011, in line with the realisation of the Transformational Government agenda.

**Transformational Government**

Three 'transformations' are required to better deliver public services through ICT:

- Services must be *designed around the citizen or business*. For these benefits to be fully realised, individuals and organisations must have confidence in government's ability to manage their personal information securely;
- Government must *move to a Shared Services culture*. To achieve this, information must be increasingly shared between organisations and by information systems that are increasingly inter-connected;
- There must be a *broadening and deepening of government's professionalism* in terms of the planning, delivery, management, skills and governance of ICT-enabled change.

# Context

**20.** A number of significant changes in the way that ICT is used have called for a revision of the previous IA Strategy published in 2003. Much work has been taken forward across government to implement the nine critical actions set out in that document and this Strategy builds on that work; developing, rather than replacing, the 2003 approach. However, a revised and re-energised framework is required to meet new challenges. Significantly, in 2005 the Government committed to the Transformational Government agenda[1]. Within the public sector, achieving this agenda, particularly the Shared Services element, will require a more rigorous approach to the way that departments and other organisations use ICT to do business. It will also require new ways of working for those private sector organisations involved in the delivery of public services or ICT products and services.

**21.** At the same time as pursuing this considerable agenda, government must also continue to ensure that enduring strategic priorities are met. The national security and economic and social well-being of the UK remain vital.

# Threat

**22.** There has been a significant increase in the threat to information and information systems, particularly that associated with the rise of the internet and the ability to attack and disrupt at a distance. This has manifested itself in the rise of e-crime, ID fraud and theft and other malicious activity aimed at disrupting information and/or information systems.

**23.** The increasing risk of compromise by organisational 'insiders', either malicious or non-malicious, is also a serious concern. Such acts pose a real threat to business delivery in government and the wider public and private sectors. Compromise can result in the disruption, or even breakdown of services and significant financial and reputational losses. Where the information at risk is particularly sensitive lives may be lost, for example, as a result of the failure of parts of the critical national infrastructure (CNI)[2].

**24.** The scale of these threats is set out in the text box on page 6, which draws on the 2006 DTI Information Security Survey[3]. By helping individual organisations to ensure they have appropriate measures in place to protect themselves against these threats, this Strategy also meets the wider requirement to build a national capability to remain resilient in the face of hostile action.

[1] www.cio.gov.uk/documents/pdf/transgov/transgov-strategy.pdf

[2] A nationally critical function is a function of a set of assets the loss or compromise of which would affect the well-being of the UK, whether through widespread loss of life, significant social disruption, a significant impact on the national economy or through the realisation of a threat to national security.

[3] http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults06.pdf

### The Scale of the Threat

The internet is a common part of business delivery; 97% of businesses make use of it. On average, every UK company suffers several security breaches a day. Over 50% of very large businesses experience hundreds of attempts to break into their networks on a daily basis. New technologies pose a particular threat: Only 1% of UK businesses have a comprehensive approach for identity management; 20% of wireless networks are completely unprotected.

Two thirds of UK businesses would suffer significant business disruption if their critical information were corrupted. Overall, the cost of security breaches to UK plc has increased by roughly 50% since 2004, and is of the order of £10Bn p.a. These threats are expected to increase: 63% of UK businesses expect their number of security incidents to rise in 2007 and a similar percentage (60%) believe it will be harder to detect security breaches in the future.

## Vulnerability

**25.** At the same time as the threat has increased, changes in the ICT environment have brought with them additional risks which have made the mitigation of these threats more difficult. Specifically:

- The **ICT industry is moving at an ever-increasing pace**. The rate of development of new approaches to communication of information, including the increasing use of wireless devices and equipment that combine different types of media, presents particular challenges. Conventional assessment of vulnerability and its mitigation is increasingly ineffective in such a fast moving environment. A new approach to IA is required that will be sufficiently flexible to anticipate changes to the way in which organisations and people use ICT to deliver business benefit. Government must play a key role in influencing the market to ensure the innovation and expertise of industry is fully harnessed in the provision of IA products and services. As part of this, IA must become embedded in a system's life cycle, in the same way that safety features, such as a seatbelt, are now a fundamental part of a car's design.
- The **ICT environment is enabling people to become more joined up and global**. Organisations are increasingly able to share information across organisational and international boundaries. This increases the vulnerability of their information and information systems. Within government, for example, this is a clear challenge for the Shared Services agenda. Organisations, particularly large businesses, are already having to account for the increased risks around outsourcing and procurement associated with operating within a global environment. The DTI Survey reports that four-fifths of such organisations rely on offshoring as a part of their IT operations.

## Benefits

**26.** A number of direct benefits flow from the implementation of this Strategy for Government Departments and the wider Public Sector:

- Enhanced public, commercial and industrial confidence in government's ability to manage and handle information;
- Greater trust and confidence when sharing information across organisations;
- Better protection will reduce the risk of reputational or financial damage or legal liability resulting from compromise of a department's information or information systems;
- Better value for money in their information risk management solutions.

**27.** However, the Strategy represents a *national* approach and implementation within government is intended to bring wider benefits to industry and the general public:

**28.** The ICT/IA Industry will have:

- greater clarity of government's IA requirements through timely and valued engagement between government and industry in the development of IA products and services and;

- Gain from the development of a more resilient UK IA marketplace through greater understanding of the need for IA within organisations.

**29.** CNI and business will have:

- an enhanced provision of information about threats and advice on how to mitigate these and;
- Clearer links for engagement with government and opportunities to develop best practice and share knowledge.

**30.** Citizens will be able to access public and private ICT services safely and with confidence, enjoying the benefits their equipment brings to the full.

## Approach

**31.** The NIAS broadens the scope of the 2003 approach in two important ways.

**32.** Firstly, the Strategy now provides a single framework for IA for the whole of the UK. The framework will enable a consistent and coherent approach across all sectors, whilst also allowing for the flexibility required by organisations with different risk tolerances. This will be essential to the achievement of the Shared Services agenda.

**33.** Secondly, this Strategy takes a holistic approach to IA. The changing nature of the threat confirms the approach of the 2003 Strategy to expand the focus from the traditional 'confidentiality' element of IA to a broader-based requirement that covers the other elements: availability, integrity, non-repudiation and authentication.

**34.** This Strategy also recognises that IA is about more than just technology. To ensure effective information risk management, the thread of IA should run through all elements of business processes. This should also mean that resource expended on each of the elements of IA is consistently and coherently applied.

**35.** A broader approach is vital if the government is to deliver its Transformational Government agenda. However, this will not be at the expense of previous commitments to focus effort and resource at the higher-threat end of the spectrum. Specifically, the initiative commenced under the 2003 Strategy to establish an enduring UK sovereign IA capability continues unabated. This will be an important part of maintaining the UK's national security at the high-threat end, as well as providing a bedrock for broader IA capabilities to be applied more widely.

## Objectives

**36.** Three strategic objectives are intended to be 'enablers' for organisations, helping to deliver business more effectively through the appropriate mitigation of information risks. Government will put in place the appropriate framework to provide organisations with the right 'tools' to ensure these objectives are achieved:

- Clear and effective **information risk management** by organisations;
- Agreement upon and compliance with approved and appropriate **IA standards**;
- The development and availability of appropriate **IA Capabilities**.

**37.** Organisations will have realised the full benefits of ICT when IA is embedded within the culture of organisations and is an invisible, but indivisible, part of the everyday processes driving business delivery.

# Information Risk Management

**38.** Organisations should take clear ownership of and responsibility for the management of risks to their information. This will require that:

- There is clear ownership of and accountability for the information risks within an organisation at board level;
- Within an organisation, information risks should be as visible and as integral a part of the business decision-making process as financial and project-based risks;
- For information systems that span different organisations, or communities of interest, a single point of risk ownership is identified. Government will work with stakeholders as a matter of priority to establish a mechanism which allows the identification of a single point effectively.

**39.** Within government, this means effecting a significant change in the way that some departments own and manage the risks to their information and information systems. Departments will need to take responsibility for determining a level of risk tolerance, or 'appetite', and tailoring the management of their information risks appropriately. As part of this, Departments are responsible for ensuring a coherent approach to information risk management across affiliated agencies and Non-Departmental Public Bodies. They should lead efforts to engage these stakeholders to satisfy themselves that the appropriate levels of information risk management are maintained in these wider organisations.

**40.** These principles are also applicable outside of government. Transformational Government will increasingly allow organisations across different sectors of the UK to join up. This means that, where information is shared, organisations will need to relinquish (or recognise that they have already relinquished) some autonomy in the handling and management of their information.

**41.** There is clear evidence that the efficient and effective conduct of business will only occur if responsibility for managing risk lies in one place. For most pan-government systems and projects the Senior Responsible Owner will be expected to act as, or appoint, a single information risk owner. For those circumstances where this is not the case, for example for some existing systems, a single information risk owner will be appointed through the CIO Council.

# Standards and Compliance

**42.** A national framework of IA Standards will be developed to provide organisations with the confidence that they are managing information risks appropriately. Establishing confidence and trust lies at the heart of enabling effective and responsible information sharing. These standards will define a 'segmented model' for information and information system requirements across the UK. Systems will operate within one of a number of broad 'segments', according to the level of impact that failure of the information carried on those systems would have. Segments will be informed by impact levels based upon the Government's Infosec Standard No1.

**43.** Within each of these segments, the level of IA achieved by adherence to the segment's IA standards will be broadly comparable. However, the balance of adherence to various types of IA standard may differ within the segment depending upon the user's IA specific requirements and risk appetite. For example, an organisation may choose to apply a higher standard than the minimum within the segment, if one element of IA (e.g. confidentiality) is of particular importance to that organisation. Where an organisation has systems that lie within more than one segment, it will need to

determine whether to enable full connectivity between the segments, in the wider context of business planning and delivery considerations.

**44.** These common standards will provide organisations with a level of confidence when connecting their systems or sharing their information with other organisations within the same segment. In the context of Shared Services, for example, this will mean that an organisation will be able to assure itself that shared information will be appropriately managed by other organisations. To ensure that the standards remain relevant, they will need to be responsive to the rapidly evolving business needs of organisations.

**45.** Government's role in enabling the wider application of these standards will be directed towards those areas where it is most needed through a process of risk impact assessment. This Strategy recognises that in most cases government does not have the authority to mandate standards. For businesses, such as those within the CNI, where compromise would have a bearing on national security, government will work with organisations, providing advice and guidance on how an appropriate level of IA may be achieved.

**46.** The Delivery Approach will set out how work to develop an appropriate set of IA standards and a compliance model is to be taken forward.

# IA Capabilities

**47.** In order for organisations to be able to own and to manage their information risks to the appropriate standards, they will require appropriate 'IA Capabilities'. These capabilities describe the IA elements that should be embedded within all parts of an organisation's everyday business processes. Government will engage with all sectors of the UK to ensure that knowledge and best practice is shared wherever possible in the delivery of these capabilities.

### The development and availability of the right products and services

**48.** Government will adopt and encourage others to adopt a model for assuring confidence in the development of products and services. The model will help to ensure that IA is effectively embedded within ICT products as an ongoing through-life activity, beginning at the earliest design stage and continuing throughout the usage stage. As part of this approach government will have an active role to:

- Develop improved operational assurance capability;
- Engage more directly with industry to provide clarity of cross-government requirements and develop appropriate products and services;
- Establish and operate a clear model for the provision of IA advice and services to stakeholders;
- Exploit the investment in the present IA Technical Programme to embrace a wider range of IA products, while retaining primary focus on the needs of high-threat organisations.

### Coordinated and appropriate efforts on innovation and research

**49.** Considerable resources are applied to IA research and innovation efforts across the UK. Government recognises that there is value in coordinating this expertise, as this increases the likelihood that the most appropriate products and services are developed to meet future requirements of UK organisations. To this end, government will lead efforts to build links and where possible to collaborate and share information with other members of the national and international research communities.

**50.** As part of this, government will maintain its position at the forefront of UK technical awareness and knowledge in order that it remains in a position to steer, lead, and participate in the IA technical community. This knowledge will also help to ensure that it is able to clearly understand and articulate its needs to industry and that, where necessary, it has the capability to meet those needs not able to be met by the commercial market place.

### Improved professionalism across all areas of the IA sector

**51.** Greater professionalism across the IA community will be an important part of ensuring that staff within an organisation are able to implement the approach set out in this Strategy. As such, government will continue to pursue the agenda started under the 2003 Strategy with renewed vigour. Efforts to establish an Institute of Information Security Professionals (IISP), InfoSec training and an Accreditors Forum have been a useful start. Further work will be taken forward to ensure that IA professionals are given the same recognition and training opportunities as those within the Government IT Profession.

### Improved awareness and outreach across the UK

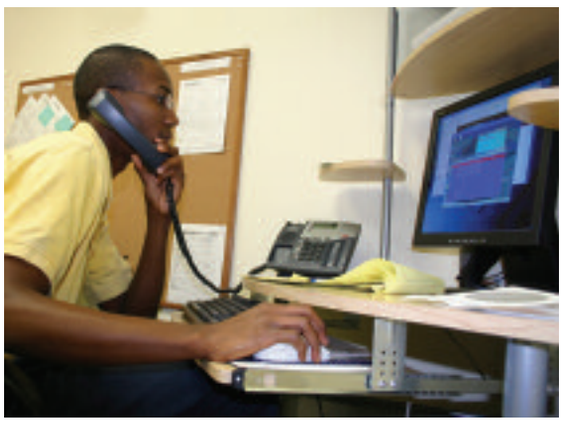
**52.** Achieving wide understanding of the importance of IA to the UK through effective communication is an important part of the implementation of this Strategy. Existing schemes such as "GetSafeOnline" have had some impact in promoting greater awareness and understanding of IA amongst businesses and the general public. There will continue to be a role for such schemes, but government must do more to ensure that these are part of a wider coherent strategic message. A targeted communications strategy to reach key audiences utilising portals such as Direct Gov and Business Links will play an important part in the implementation of the NIAS.


## Leadership & Delivery

**53.** A 'Wider IA Centre' (WIAC) will provide the required leadership and expert knowledge to implement this Strategy. As part of this, it will pull together existing and new IA activity under a single framework and drive this work forward in a coordinated and coherent manner. A key part of this will be to provide IA advice and guidance to a range of organisations to assist their implementation of activities set out in the Delivery Approach. The WIAC comprises the following organisations:

- The Central Sponsor for Information Assurance (CSIA) in the Cabinet Office has overall responsibility for this Strategy and will provide strategic oversight and direction for IA across the UK. It will ensure that strategic and policy developments are coordinated and directed to support the implementation of this Strategy.
- CESG will lead on the provision of technical IA risk management guidance, standards of good practice, advice and assurance services across Government. In line with this, CESG will contribute to a national alerting and response function, focusing on alerts intended for government, and responding primarily to threats to government information systems.
- The Centre for the Protection of National Infrastructure (CPNI) will lead the provision of IA advice and services to the Private Sector CNI, as part of broader protective security advice[4] to the CNI. CPNI will contribute to a

[4] Protective security includes physical, personnel and information security and CPNI advice will be increasingly integrated across these disciplines.



national alerting and response function, focusing on alerts intended for the Private Sector, and responding primarily to threats to information systems belonging to the Private Sector CNI.

**54.** Within government, a key objective for the WIAC will be to draw upon the expertise of the CIO and CTO Councils to enable the delivery of this Strategy.

**55.** A number of departments and organisations outside the WIAC will continue to have a key role to play in leading particular strands of IA activity. The Department for Trade and Industry will remain a valuable link in engaging industry, Europe and the rest of the world on specific elements of IA policy. The Home Office will continue to play a leading role in the development of government's strategy on identity and identity management, through the Identity and Passport Service (IPS). Established outlets for more general information and advice on IA will also continue to play a role for specific sectors. Where these, and wider functions in the Private Sector, currently exist and presently provide a useful channel for the provision of advice, they should clearly continue.

# Implementation

**56.** The Delivery Approach will develop the three strategic objectives of this Strategy into actions and activities to be implemented under the direction of the Information Assurance Policy and Programme Board (IAPPB) by 2011. Wherever possible, these activities will build on or incorporate existing IA work and utilise existing mechanisms or channels for delivery.

**57.** CSIA will lead the coordination of the implementation, supporting the IAPPB and its subcommittees and using that structure to allocate and monitor tasks. Accountability for particular strands of implementation will be determined by the IAPPB or its sub-committees as appropriate. Where existing IA activities are ongoing, and these are adding value, they will continue, and be brought into the wider mechanism for implementation under the IAPPB.

**58.** More generally, the role of IA as an 'enabler' means that it will clearly have an influence on much activity across business delivery by helping organisations use ICT. However, in a number of cases within government, the approach to IA set by the IAPPB may have a direct bearing on closely related agendas, for example around protective security or counter-terrorism. In such cases, the WIAC will ensure that the appropriate bodies are aware of and brought into the decision-making process as required.

**59.** The scope of the Strategy and the scale of delivery required are significant and it will be practical to implement in stages. The first version of the Delivery Approach will focus effort initially, though not exclusively, on implementation within Government. Other sectors will be drawn more fully into subsequent iterations of the Delivery Plan after further consultation.

**60.** It is envisaged that organisations across all sectors will take on key roles and responsibilities as part of each stage of implementation. These are complex and warrant full consideration within the Delivery Approach. It is acknowledged that there will be cost implications as part of the implementation and these are addressed in the Affordability section of the Delivery Approach.

# Glossary

**Accreditor**
qualified professional who examines an organisation's processes to ascertain if particular standards are being met.

**Asset**
Anything that has value to the organisation, its business operations and its continuity.

**Authentication**
Ensuring that the identity of a subject or resource is the one claimed.

**Availability**
The property of being accessible and usable upon demand by an authorised entity.

**Confidentiality**
The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

**CNI – Critical National Infrastructure**
Within the nine national infrastructure sectors there are critical elements (these may be physical or electronic), the loss or compromise of which would have a major detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life. These critical elements of infrastructure comprise the nation's critical national infrastructure.

**Impact**
The result of an information security incident, caused by a threat, which affects assets.

**Information Assurance**
The confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

**IA capabilities**
Elements such as IA professionalism, products and services, and awareness and education that should be embedded within an organisation to achieve the appropriate level of assurance

**IA products**
IT products which provide a recognised level of security efficiency.

**Information Risk Management**
Overall process of analysing, evaluating, assessing and mitigating the impact of risks to an organisation's ICT and the information they handle.

**Integrity**
The property of safeguarding the accuracy and completeness of assets

**Mitigation**
Limitation of the negative consequence of a particular event

**Non-repudiation**
The ability to prove an action or event has taken place, so that this event or action cannot be repudiated later.

**Risk**
The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

**Risk Appetite or tolerance**
Attitude taken by an organisation, which in relation to risk minimises the negative and maximises the positive business consequences and their respective probabilities

**Risk Impact Assessment**
The process of risk analysis and risk evaluation and assessment of impact.

**Senior Responsible Owner**
An appointed senior manager that owns responsibility for a particular area of an organisations business and its risks.

**Shared Services**
The sharing of services and information such as ICT systems and or processes/management, facilities and maintenance contracts across one or more public sector organisations.

**Threat**
A potential cause of an incident that may result in harm to a system or organization.

**Vulnerability**
A weakness of an asset or group of assets that can be exploited by one or more threats.

**WIAC – (Wider IA Centre)**
Comprising of the Central Sponsor for Information Assurance within the Cabinet Office, the CPNI (Centre for Protection of the National Infrastructure) and CESG – the national IA technical authority, an arm of GCHQ.

For more information about the CSIA go to www.cabinetoffice.gov.uk/csia

If you would like to comment on this Strategy, please contact:
CSIA
2nd Floor
26 Whitehall
London SW1A 2WH

Telephone: 020 7276 5026
Or email us at csia@cabinet-office.x.gsi.gov.uk

Your responses will be used to help develop and inform the Strategy which will be kept under review and updated as appropriate.

Printed in June 2007



The material used in this publication is constituted from 75% post-consumer waste and 25% virgin fibre.