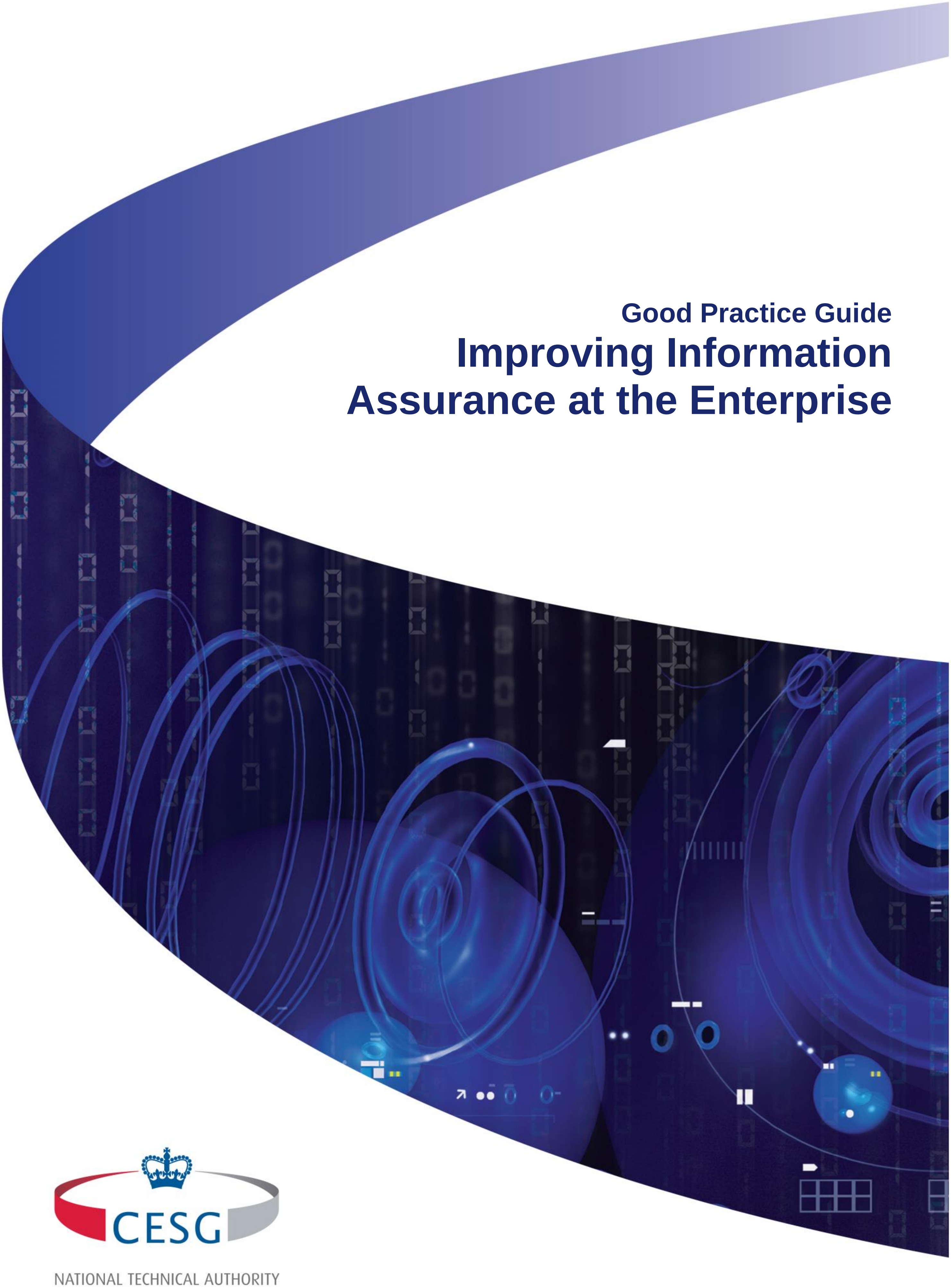
October 2015
Issue No: 1.3



Good Practice Guide

Improving Information Assurance at the Enterprise

CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

Good Practice Guide No. 28

Improving Information Assurance at the Enterprise Level

Issue No: 1.3
October 2015

Document History

Version	Date	Comment
1.0	July 2010	First issue
1.1	September 2010	Second issue
1.2	February 2013	Third issue
1.3	October	First public release

Intended Readership

This Good Practice Guide is intended for senior managers and Information Assurance (IA) professionals tasked with improving the level of IA across an entire government department, agency or other public body (i.e. at the enterprise level). It should be of particular interest to Senior Information Risk Owners (SIROs), IA programme and project managers, Information Asset Owners, Departmental Security Officers, IT Security Officers, Accreditors and CLAS (CESG Listed Adviser Scheme) consultants.

Executive Summary

Driving improvement in Information Assurance across an entire organisation is deceptively complex and challenging. Sustained, cost effective improvement is unlikely without:

- a pro-active board level champion
- a supportive culture of Information Management
- an IA vision that clearly delivers business benefits sought by Directors
- an agreed set of enterprise IA controls
- a well structured delivery programme including the business change activities
- an effective IA audit regime

Aims and Purpose

The aim of this Good Practice Guide is to share lessons learnt across the public sector in driving improvement in Information Assurance at the enterprise level[1]. It complements the HMG/CESG IA Maturity Model (CIAMM®) (reference [a]) and its associated Assessment Framework. In particular, it provides advice to SIROs to meet a fundamental requirement at Level 2 of the CIAMM®; "to have personally made and gained approval for a business case to the Main Board for a targeted programme of work to improve the understanding and control of information risk."

The guide is not intended to be prescriptive as there is no single correct way to improve IA. The guide introduces a range of concepts with the expectation that the reader will consider which are applicable in their circumstances. Application of the concepts is elaborated in the context of a business change framework.

This version was mostly a refresh of references, and to align with GPG40 version 2.

[1] By 'enterprise level' we mean at the organisation level (e.g. Government department, agency or other non-departmental public body) including parts of other organisations embedded within it such as managed service providers.

Contents:

Chapter 1 - Core Concepts for Improving IA to Deliver Strategic Business Benefits

Key Principles

- Improving IA at the enterprise level can enable strategic business benefits[2], but doing so requires concepts in addition to those required to improve IA at the system level

Introduction

1. Improving Information Assurance (IA) is a goal of most boards of Directors in the public sector and of many beyond. Much guidance has already been produced on improving IA of individual Information Systems (IS) but some organisations have hundreds or thousands of IS. Attempting to improve IA across organisations on this scale by repeatedly applying techniques to secure individual systems is inefficient and unlikely to succeed for the following reasons:

    a. IS typically have complex interconnections. Securing one often requires changes in connected systems.

    b. There are large economies of scale when IA controls are designed, deployed and operated across the whole organisation instead of system by system.

    c. Investment in one system may be nugatory if its security is undermined elsewhere. Identifying the best places to invest requires an organisation wide view.

    d. An organisation's overall level of IA is constrained by factors such as its style of information governance, cultural attitudes, Human Resource (HR) policies and compliance monitoring. These factors need to be addressed across the organisation rather than at the system level.

2. This Good Practice Guide (GPG) is about improving IA across an entire government department, agency or other public body to deliver strategic business benefits. We refer to this as improving IA at the enterprise level. For some organisations, this may also entail IA improvement among embedded partners, such as managed service providers. This GPG aims to share the lessons learnt across the public sector as large organisations strive to protect the data, with which they are entrusted, to the standards expected by the public.

3. Some concepts in improving IA become more relevant as the focus of attention moves from the system level to the enterprise level. These core concepts are presented in the rough order in which Senior Information Risk Owners (SIROs) and Information Asset Owners (IAOs) need to be aware of them, if IA is to be improved across their organisation. The list is not intended to be exhaustive; concepts are included according to the tendency for their significance to be

[2] By strategic business benefits we mean benefits of long term value to the organisation and of sufficient concern to Directors that they will be proactive in ensuring their delivery.

under-appreciated. Each concept is elaborated later in the GPG and set in the context of a Business Change Framework (BCF) to improve IA across an organisation.

Improving IA at the Enterprise Level is Deceptively Difficult

4. Improving IA at the enterprise level invariably requires enterprise level change in culture, processes and technology. It is very easy to under-estimate how much time, resource and senior level attention this requires. The concepts introduced in this GPG aim to help senior managers gauge the scale of the challenge for their organisation. The challenges are elaborated in Chapter 3.

Measure the Level of IA

5. The old adage that 'what gets measured, gets managed' applies to IA. The HMG/CESG IA Maturity Model (CIAMM®) (reference [a]) provides a framework for measuring the enterprise level of IA. Whilst this is not sufficient to drive benefit realisation, use of the framework can give Directors confidence that benefits are likely to be realised. A description of the CIAMM® is given at Chapter 4.

Use a Business Change Framework

6. The framework used for driving enterprise level improvement in IA needs to include all the factors required to drive major business change across an organisation. This GPG applies a BCF to the challenge of improving IA. The BCF itself is described in Chapter 5. Chapters 6 to 9 describe the business change activities required to improve IA across an organisation.

Identify the Strategic Business Benefits that Improved IA can Enable

7. Improved IA is not an end in itself. As well as reducing information risks, it can help reduce overall costs and enable valuable business activities that would otherwise be too risky. Identification of the benefits to be delivered, in terms that have resonance across the organisation, is crucial to a successful IA improvement programme. Some guidance to achieve this is given in Chapter 6.

Gain Board Level Commitment

8. Improving IA at the enterprise level requires active support from the board of Directors. Complex change is required across the organisation and managers below board level do not have the breadth of influence or level of resources to achieve this. Guidance on helping the SIRO to produce a compelling case for investment to the board of Directors is given in Chapter 6.

Establish the IA Programme Sponsoring Group

9. A formal change programme is essential to improving IA at the enterprise level. The level of change that the programme can deliver will be constrained by the seniority of the programme sponsoring group. If strategic business benefits are to be realised, typically the sponsoring group will require senior representation from the organisation's major business units. Establishing the IA programme is explained in more detail at Chapter 7.

Good IA requires good Knowledge and Information Management

10. IA is dependent upon Knowledge and Information Management (KIM). Unless the organisation understands what information it has and what the business impacts of compromise would be, it cannot implement effective IA. Examples of the relevance of KIM are included, where appropriate, in Chapters 6 to 9.

Specify the IA Control Set

11. Specifying the set of corporate IA controls is a key device in managing and improving IA. This forces debate on what controls can be resourced, which ones are best value for money and what changes should be made to the set. If the set of controls is not well defined, it is unclear which controls are actually being implemented and therefore to which risks the organisation is exposed. Guidance for specifying the set of IA controls is provided in Chapter 7.

Build IA into the Enterprise Architecture

12. Particularly for larger organisations, Enterprise Architecture (EA) is an important enabler for IA. It provides an organisational framework into which security can be designed in a holistic manner. Without an EA, controls cannot be implemented consistently across the organisation, making some controls unaffordable and increasing the risk that existing controls are undermined in some way. The merits of this approach and sources of further information are presented in Chapter 7.

Develop an IA Audit Regime

13. An effective audit regime is crucial to ensuring that improvements in IA are sustained. As non-compliance with IA policies is more likely to be deterred or detected, it also enables more liberal IA policies supporting more flexible working practices. Guidance for developing a cost effective audit regime is given in Chapter 8.

Include IA as a Component of Corporate Governance

14. IA should be an integral part of the corporate governance regime. This helps ensure that it is resourced appropriately and that information risks are addressed at the appropriate level. The business change activities described in Chapters 6 to 9 help ensure that this takes place.

Influencing People is Key to Progress to Every Stage

15. Influencing people is a major activity in every stage of the business change process. Even in an IA improvement programme delivering controls enabled by technology, the people issues still tend to dominate the challenges faced by the programme manager. People related business change activities feature in Chapters 6 to 9.

Chapter 2 - The Importance of Improving IA Across the Public Sector

Key Principle

- Major government objectives and strategies require improved IA across the public sector if public and political confidence in our ability to protect sensitive data is to be retained

16. Before we describe how to improve IA at the enterprise level, we first ought to briefly explain why it is so important.

17. Citizens increasingly ‘live on the net’. Whether it is through social media, e-commerce or remote working, many of Government’s customers transact online daily and have built up an understanding of what ‘good looks like’ in this environment. Key strategies (e.g. HMG Security Policy Framework (SPF) (reference [b]), The UK Cyber Security Strategy (reference [c]), UK Government ICT Strategy (reference [d])), when considered with cross-cutting concerns (national security, operational efficiencies, public sector head-count reductions and environmental impact), imply a core set of Information Risk Management (IRM) requirements that need to be satisfied if these strategies are to deliver their intended outcomes, and in a way which citizens can accept and from which they can fully benefit.

18. At the same time, government IS and the information they carry face ever increasing threats – from careless operation, casual hackers, through serious crime to action by nation states – at a time when global economic shocks and a world downturn have placed extraordinary demands upon national and local government. Technology paradigms, such as cloud computing and advanced virtualisation, are being used by government and industry to increase efficiency and productivity. Their use fundamentally alters long-established security principles.

19. The public sector IA community needs to respond urgently to these challenges if public and political confidence in our ability to protect sensitive data is not to constrain the services that government could otherwise deliver. Notable improvements have already been made (SPF (reference [b]), HMG IA Standard No 6, Protecting Personal Data and Managing Information Risk (IS6) (reference [e])). However, as public sector IS becomes ever more interconnected, to provide improved public services, the consequences of poor IA, in one part of the public sector, are likely to have wider consequences. For this reason, improving IA across the public sector is a key enabler to improving the public services that we are here to provide.

Chapter 3 - Why is Improving IA at the Enterprise Level so Difficult?

Key Principles

- Improving IA at the enterprise level involves changing culture, process and technology across the organisation
- Benefits are hard to measure and improved IA may not directly benefit those most affected
- People resist changes to their ways of working

20. It is easy to under-estimate the difficulty in improving the level of IA across an organisation. It requires sustained management attention and resourcing. The larger the organisation, the longer it will typically take to make a sustained difference across the organisation. It is tempting for management to believe that simply writing a policy, and also tasking a small team with progressing IA on behalf of the organisation, will be sufficient. However, it is not. The reason for this becomes clear when one considers what is needed to manage information risk effectively.

    a. A governance regime is required to ensure that information risks are systematically analysed across the organisation, escalated to the appropriate level and then treated without imposing undue business constraints.

    b. Technical controls such as access control, malware defences and network boundary management require both implementation and maintenance across the organisation in both new and legacy systems.

    c. Processes such as data labelling, account management, software patching, control of removable media and portable computers have to be embedded into many business units and enacted by staff who are often not particularly motivated to carry it out. This may be because they do not see the work as interesting, or they do not understand the need for it, or they do not believe they will receive much recognition for it.

    d. Cultural attitudes need to support IA. People may be unaware or unconcerned that actions that make their life simpler and easier (such as using simple passwords or untrusted networks) might have very serious consequences; e.g. compromise of data, damage to reputation and loss of operational services due to malware attacks. Developing appropriate awareness of information risks can require major training and awareness programmes tailored to the needs of user groups.

    e. A compliance monitoring regime is established to ensure that the IA policies, appropriate for the organisation, are complied with by staff.

21. Changing the culture, process and technology on an enterprise scale is never easy and none of these can be done independently of the others. However, this is what is required if strategic business benefits are to be realised from improved IA. Visible support from Directors and IAOs through to middle

management and influential users is crucial to success and this takes time and effort to achieve.

22. Other factors which compound the difficulties in improving IA are:

    a. Good IA is intangible and hard to measure.

    b. Project managers often feel that it is delivery to time and schedule that determine whether their project is perceived as a success and that the security requirements are tradable extras.

    c. Whereas many forms of expenditure directly lead to predictable benefits, nobody can know which future security incidents those desired security requirements would have prevented.

    d. Improved IA often requires people to change their working practices, at some immediate cost or inconvenience to themselves, in return for possible future benefits to the organisation, which they do not feel themselves.

23. Overcoming these difficulties requires a coordinated change programme, championed by the SIRO, which identifies realistic objectives and a credible, resourced plan to achieve them. This then has to be implemented in the face of many other business objectives that are competing for management attention and resources.

24. It should also be noted that it is quite possible to improve IA at the expense of the organisation as a whole (e.g. where IA controls unduly prevent useful business activities). Thus, maintaining a good balance between IA and other business objectives requires care and extensive communications across an organisation.

Chapter 4 - Measure the Level of IA

Key Principles

- IA maturity is a measure of an organisation's ability to achieve IA in support of business objectives
- As IA maturity improves, an organisation gets ever closer to the optimum balance between IA and other business objectives to maximise its long term business prospects

Why Measure the Enterprise IA Level?

25. Measuring the level of enterprise IA is a key management device to drive improvement. If there is a framework for measuring IA then it enables management to set objective, measurable targets for improvement. It can also give confidence to those resourcing the investment that demonstrable progress will be made. This Chapter describes the HMG/CESG framework for measuring IA at the enterprise level.

26. For readers not familiar with the concept of IA maturity, a definition of IA, a description of IA maturity and further background on maturity models is provided at Annex A.

What is the HMG Information Assurance Maturity Model

27. To help public sector organisations improve their level of IA maturity, CESG has developed an IA Maturity Model and an associated Assessment Framework (reference [a]). The CIAMM® defines 5 maturity levels:

    a. Level 1 - Initial: Awareness of the criticality of IA to the business and legal requirements.

    b. Level 2 – Established: IA processes are institutionalized.

    c. Level 3 – Business Enabling: IA processes are implemented in critical areas of the business.

    d. Level 4 – Quantitatively Managed: The board has established its broader IA Road Map for all its information, systems and processes.

    e. Level 5 – Optimised: Responsive IA processes are integrated as part of normal business.

28. At each level, the CIAMM® outlines the requirements in 6 capability areas:

    a. Leadership and Governance;

    b. Training, Education & Awareness;

    c. Information Risk Management;

    d. Through-Life Measures;

    e. Assured Information Sharing;

    f. Compliance.

29. Progress through the HMG/CESG IA maturity levels is intended to realise the following IA goals:

    a. IRM culture is embedded in the organisation.

    b. Best practice IA measures are implemented.

    c. Effective compliance is ensured.

30. The CIAMM® is supported by an Assessment Framework, which expands the requirements for each level and category in the style of what was known as an Office of Government Commerce (OGC) Gateway Review assessment, identifying areas to probe and evidence expected to demonstrate compliance with the model. The OGC is now part of the Cabinet Office.

31. The CIAMM® is used, by many departments, as a means to monitor the effectiveness of IRM across government. It is possible that use of the CIAMM®, for reporting purposes, will also spread across government and to major suppliers of IT services to government.

32. Departments can make their own assessments of IA maturity, but CESG provides assessment services. CESG can provide either an independent assessment, or support self assessments, through provision of a trained facilitator.

33. Following the CIAMM® provides one path to the optimum balance between IA and other business objectives, but there will be other viable paths. This GPG aims to help organisations progress along the path that best suits their circumstances and business needs.

Chapter 5 - Use a Business Change Framework

Key Principles

- A Business Change Framework helps organisations identify all the activities required to improve IA at the enterprise level

34. Many organisations have found that delivering a new IT system is not sufficient to realise business benefits. Users have to be trained and persuaded to use the system and the business has to adapt to benefit from its use. A BCF can help change managers understand all the activities required to change a business (or businesses) for the better. The BCF described in this GPG was developed by a government department, in consultation with leading practitioners in the field, and has been successfully used in many projects. Whilst following a BCF does not guarantee success, typical experience is that ignoring the major activities increases the likelihood of failure.

35. This GPG reuses a slightly modified version of the above BCF and applies it in an IA context (reference [f]). The BCF consists of 4 stages:

    a. Make it Essential;

    b. Make it Ready;

    c. Make it Happen;

    d. Make it Stick.

36. The BCF modified for the purposes of this GPG also includes 4 strands that run through each stage.

    a. Stakeholder management;

    b. Planning change;

    c. Improving IA controls;

    d. Learning and Organisational Development.

Chapters 6 - 9 of this GPG are aligned with the 4 stages of the BCF. Each Chapter introduces concepts and activities relevant to a stage of the framework. The core concepts identified in Chapter 1 are elaborated in these Chapters. In each stage, a set of business change activities is presented. These are illustrated in

37. Figure 1.

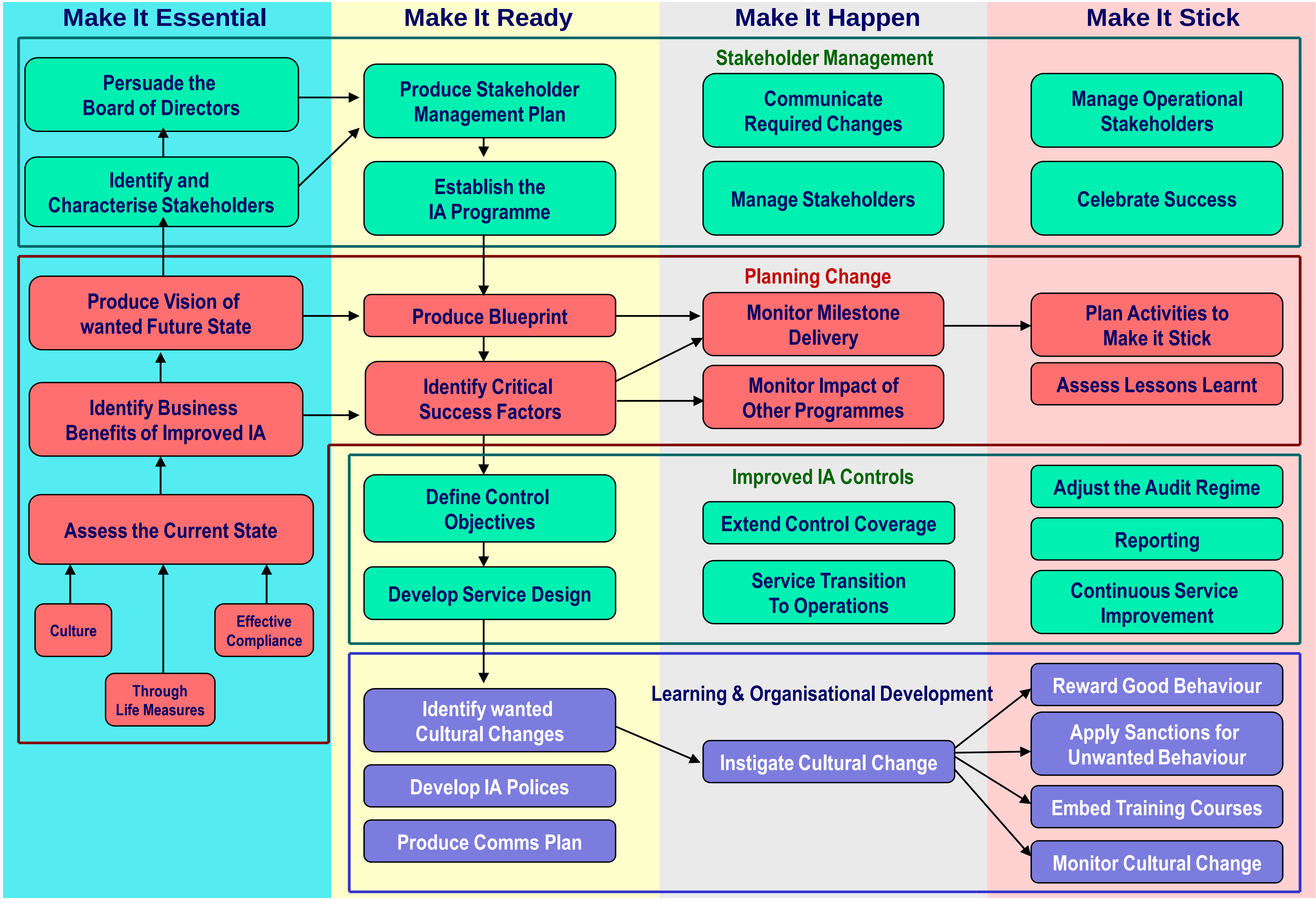
38. It is not suggested that every business change activity is relevant to every organisation. The guidance should be considered as a toolkit from which tools can be drawn if they appear useful.

39. It is not expected that organisations will be able to move more than one IA maturity level in one cycle of the 4 stages of the BCF. It is expected that organisations will cycle through the BCF repeatedly so that IA maturity is continually improving to meet evolving business requirements. For a major government department, one cycle of the BCF could take 2 or 3 years with staged deliveries during this period.

40. The major actors in each stage of the BCF, and sources of key information or guidance, are illustrated in Figure 2.

Relationship Between the BCF and ISO 27001

41. For organisations that use ISO 27001 (reference [g]) and which also need to understand how the BCF relates to their Information Security Management System (ISMS), there is no intended conflict between the two frameworks. An organisation that is compliant with, or certified to, ISO 27001 (reference [g]) is well placed to continue improvements to IA. The management structures established to support the ISMS should form the basis of the governance structures to drive IA improvement.



Make It Essential
Make It Ready
Make It Happen
Make It Stick
Stakeholder Management
Persuade the Board of Directors
Identify and Characterise Stakeholders
Produce Stakeholder Management Plan
Establish the IA Programme
Communicate Required Changes
Manage Stakeholders
Manage Operational Stakeholders
Celebrate Success
Planning Change
Produce Vision of wanted Future State
Identify Business Benefits of Improved IA
Assess the Current State
Culture
Effective Compliance
Through Life Measures
Produce Blueprint
Identify Critical Success Factors
Monitor Milestone Delivery
Monitor Impact of Other Programmes
Plan Activities to Make it Stick
Assess Lessons Learnt
Improved IA Controls
Define Control Objectives
Develop Service Design
Extend Control Coverage
Service Transition To Operations
Adjust the Audit Regime
Reporting
Continuous Service Improvement
Learning & Organisational Development
Identify wanted Cultural Changes
Develop IA Polices
Produce Comms Plan
Instigate Cultural Change
Reward Good Behaviour
Apply Sanctions for Unwanted Behaviour
Embed Training Courses
Monitor Cultural Change

Figure 1: Business Change Activity Map

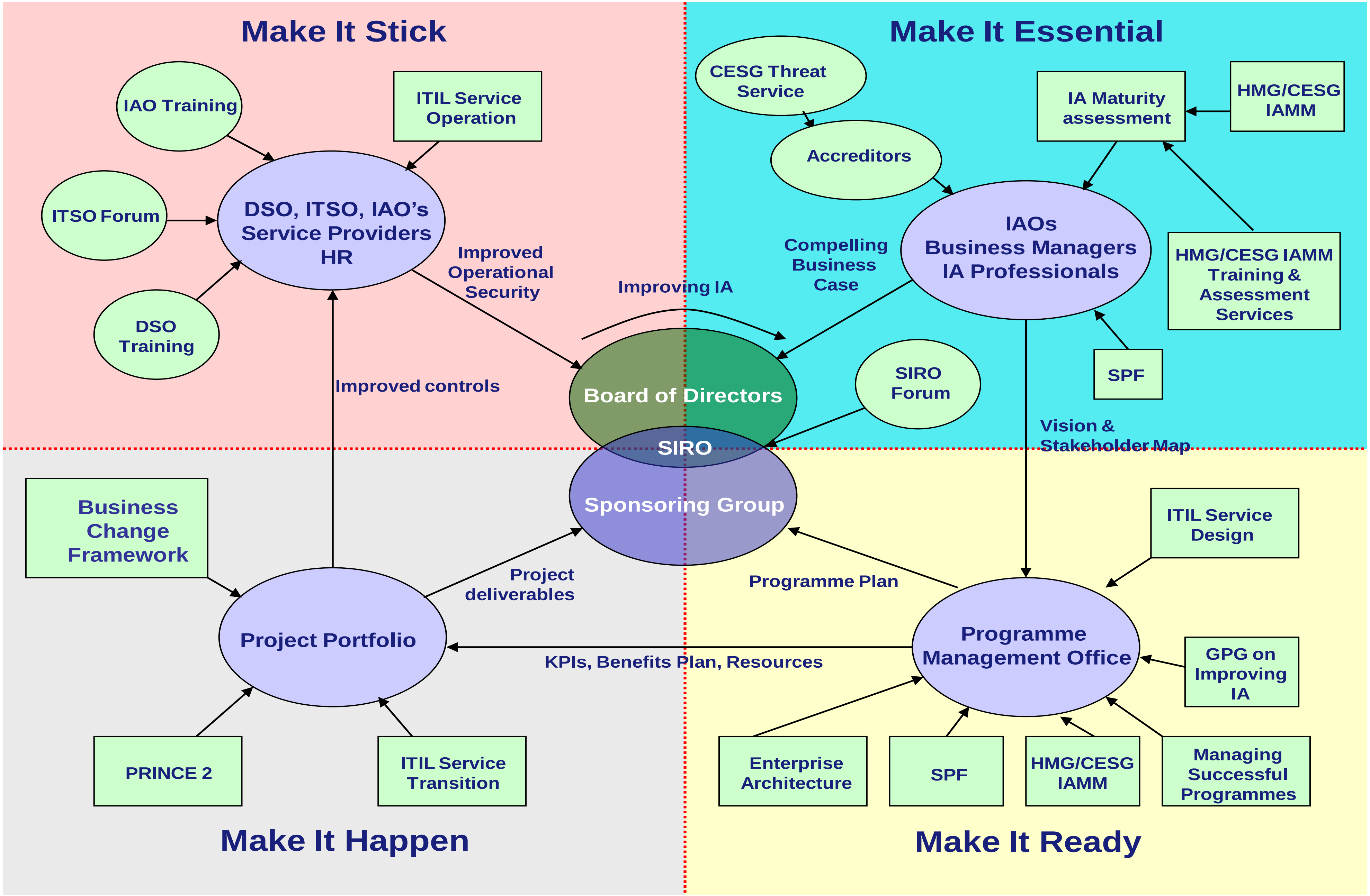


Figure 2: The Business Change Framework applied to IA

Chapter 6 - Making IA Improvement Essential

Key Principles

- Sustained IA improvement requires a compelling case for change supported by the main board of Directors
- Active engagement of the SIRO is crucial to build and maintain support for change

Developing the Compelling Case for Change

42. If an organisation is to make the sustained effort to improve IA, there must be a compelling case to do so that convinces sufficient senior stakeholders, including the board of Directors, to divert resources from other business objectives. The key stakeholder is the SIRO, who has to persuade the board of Directors of the need to invest. For this reason, Level 2 of the CIAMM® states that:

    ‘*a fundamental requirement at this level, is for the SIRO to have personally made and gained approval for a business case to the board of Directors for a targeted programme of work to improve the understanding and control of information of risk.*’

43. If the board does not approve the business case, it is unlikely that any significant, sustained organisational level change will occur, even if there are pockets of IA evangelists driving local improvement.

44. The Cabinet Office requirement for departments to indicate ‘key areas of concern’ and SPF non-compliances in the department’s annual Security Risk Management Overview (SRMO) (reference [h]) should ensure that improving IA reaches the board agenda. If the SIRO is not already aware of their responsibilities for personally making the business case for investment, other security professionals such as the Departmental Security Officer (DSO) or IT Security Officer (ITSO) should alert them to it. The SIRO should then commission the work to develop the business case. The normal time for development and presentation of the business case to the board of Directors will be during the organisation’s annual cycle of investment planning.

45. This Chapter outlines potential content for the business case and how to obtain support from the board of Directors for it. Support for change is likely to be more active and effective if the main board believes improving IA is a genuine enabler to top business objectives, in addition to being a necessary response to a Cabinet Office mandate.

Strategic Business Benefits Enabled by IA

46. Improving IA is not an end in itself but a means to delivering business benefits. A programme to improve IA at the enterprise level will invariably need to deliver strategic business benefits, if it is to justify the resources required to deliver it. Improved IA can enable three categories of strategic business benefits.

Reduced Information Risk

47. Improved IA reduces the risks of security incidents that cause business impacts. The impact of security incidents can be enormous and can potentially cause almost any of the business impacts tabled in Appendix B to HMG Information Assurance Standard No.1&2 Supplement - Technical Risk Assessment and Risk Treatment (IS1&2 Supp, reference [i]). Specific examples of past public sector incidents are given in Managing Information Risk: A Guide for Accounting Officers, Board members and Senior Information Risk Owners (reference [j]), but generic examples are given below.

    a. A rampant software virus that disrupts business services and causes the organisation to isolate, replace or rebuild machines suspected of being infected. A virus can spread very quickly across an organisation causing chaos across geographically separate business units.

    b. Loss of confidentiality through electronic attack, theft or user carelessness can compromise business operations and cause serious reputational damage. For public sector organisations, a loss of public confidence can also result in their decisions and actions being more readily challenged.

    c. Loss of data integrity, or just loss in confidence in data integrity, can destroy or damage the effectiveness of business services.

48. As well as avoiding the direct costs of recovering from incidents, organisations with few incidents enjoy a better reputation and are more trusted by partners. This can help enable benefits in the categories described below.

Reduced Total Cost of Ownership of Information Systems

49. IA costs are typically less than 10% of the Total Cost of Ownership (TCO) for an IS. So improvements in IA that enable reductions in TCO for IS can deliver good value for money even if they represent a substantial increase in IA costs. Examples of how IA can reduce costs are given in Annex B, but a sample is given here:

    a. Secure infrastructure enabling the consolidation of multiple legacy and future applications onto cheaper infrastructure.

    b. Use of less trusted infrastructure: e.g. through encryption at the application layer.

    c. Greater willingness of citizens to access government services via the Internet.

    d. Use of less trusted staff or partners by instigating protective monitoring.

Enhanced Business Capability

50. Improved IA can permit new business practices that were previously outside the organisation's risk appetite. Some examples are given below:

    a. Greater trust from partners or citizens enables access to more useful data.

    b. Secure mobile working or working from home.

c. Wider secure sharing of information across the organisation and with partners enables more collaborative working practices.

d. More rapid deployment of new applications onto trusted infrastructure.

Identifying Strategic Business Benefits that Improved IA can Enable

51. Identifying exactly how IA can **best** enable strategic business benefits, in a particular organisation, may not be straightforward. Often, the people who best understand the weaknesses in an organisation's IA are different from the people who best understand the benefits that removing IA constraints would enable.

52. A simple approach outlined below is to first consult people who have knowledge of the current level of IA and then to consult people who might benefit most from improving it. Some workshops to explore the most promising options might then be useful. The Systems Engineering profession has developed techniques for teasing out the best solutions in complex environments which may be relevant to this problem.

Assess Security Culture

53. Organisational attitudes towards security are a crucial constraint on the level of IA maturity that can be achieved. If most staff are unaware of the need for security, or it is common practice to flout security policies and procedures, investment in technical controls is unlikely to be sufficient to improve IA. Invariably there will be ways to bypass controls if it is acceptable within the corporate culture to do so.

54. Changing the corporate culture, so that it is not acceptable to bypass controls, is an important aspect of improving IA – in some cases it may be **the** most important aspect. However assessing culture and devising the actions to change it is not easy. The Centre for the Protection of National Infrastructure's (CPNI) Security Culture Review and Evaluation tool (SeCURE 2) is recommended for assessing the current culture, identifying the wanted changes and measuring whether they have been achieved. The tool facilitates surveys and provides reports to communicate the findings. For more information on SeCURE 2 contact enquiries@cpni.gsi.gov.uk.

55. Weaknesses in security culture can also be revealed by experiments to see the effectiveness of personnel security controls. Can suitably briefed new recruits, who are unrecognised by most staff, obtain unauthorised access to secure zones? How long can people without a required security pass walk around without being challenged?

56. People to consult on security culture include:

a. IAOs – what are their attitudes to security and how do they perceive the attitudes of those that have access to their information?

b. HR – what do they know about the rate of disaffected staff, unauthorised activity and staff attitudes to security?

c. Vetting officers – what trends do they see in attitudes to security? How confident are they in the effectiveness of the vetting process?

d. Security incident managers – what can they say about the volume, variety and severity of security incidents? What are the underlying causes of incidents?

e. KIM teams – do the practices to share information, that they promote, conflict with IA goals?

f. Users – what policies, or controls, do they find most inconvenient, or are most likely to be ignored?

Assess Effectiveness of Through Life Measures

57. Through Life Measures are the personnel, physical and technical security controls that operate throughout the life of an IS. A well researched case for change will be based on the answers to the questions below.

a. What are the business impacts (see Appendix B to IS1&2 Supp (reference [i])) if information assets are compromised through loss of confidentiality, integrity or availability?

b. What are the threats and vulnerabilities that could cause business impacts and how likely are they; i.e. the information risks?

c. What are the limitations of the controls to mitigate the risks in terms of:

i. The extent of coverage across the organisation?

ii. The level of resourcing?

iii. The strength of the control (sufficient to deter, detect & resist, or defend (see IS1&2 Supp (reference [i]) for definitions of these terms))?

iv. The skills and training of personnel operating the control?

58. People to consult on the effectiveness of Through Life Measures include:

a. The ITSO and system managers – what weaknesses are they aware of in the controls?

b. The DSO – what concerns them most? What changes would they like to see?

c. IT Service Managers – what could most disrupt the services they manage, how many people have some form of privileged access to IT systems, how many transfers of data are there a day on removable media to and from corporate IS?

d. Network management – how much control does management have over new connections to the network, and how many external connections are there to the organisational network?

e. IAOs – are they content with the controls currently in place?

f. Users – what ideas do they have for improvement?

Assess Effectiveness of the Compliance Regime

59. An effective compliance regime will detect whether people comply with IA policy, reward or punish good and bad behaviour, and provide management with visibility of the extent of compliance. The true value of an effective compliance regime is that it enables more liberal IA policies permitting more flexible working practices. For example, if mobile working using personal data is useful to an organisation, a good audit regime might ensure that all laptops were appropriately encrypted, therefore giving the organisation the confidence to permit the use of personal data on laptops.

60. If the compliance regime is ineffective, it should be assumed that non-compliance is common. People frequently assume that if an organisation cannot bother to monitor compliance, that it does not care whether people comply or not. Even reasonably conscientious people will then tend to do whatever is most convenient for them.

61. People to consult on the effectiveness of the compliance regime include:

a. Accreditors - what risks and vulnerabilities are they most concerned about? How effective do they believe is the accreditation process?

b. Internal Audit Units (IAU) – what concerns do they have about IRM?

c. Users of protective monitoring systems – how effective are protective monitoring systems at detecting misuse of IS?

d. KIM teams – how compliant are personnel with records requirements and with recommended KIM good practices including appropriate retention and disposal schedules? Is there an effective digital continuity strategy?

Identify Benefits from Removing IA constraints on the Business

62. People to consult to identify the business benefits of improved IA include:

a. The SIRO – what risks are they most concerned about?

b. The Chief Information Officer (CIO) – what improvements do they wish to make in the use of information?

c. The Chief Technology Officer (CTO) – what changes to the organisation do they wish to enable?

d. The Operations Manager – what changes do they seek and how does security most constrain operations?

e. Business Managers – what constraints does security impose upon their business?

f. IAOs – what do they most worry about?

g. KIM team – how does IA support the realisation of the benefits of secure information sharing and re-use?

Case Study

One government department, routinely processing very sensitive data, required much greater use of industry to develop new applications at the rate demanded by the business environment. Rapid application development entailed giving suppliers unprecedented access, from their own premises, to operational IT infrastructure to develop and test new applications. To mitigate the added risks, from misuse of the privileged access granted, IA controls to defend the department's IT infrastructure, from Electronic Attack mounted at the supplier premises, were strengthened. This enabled a vital improvement to core business agility.

Produce a Vision of the Wanted Future State

63. Once the wanted business benefits have been identified, a Vision Statement can be a powerful tool to make the case for change compelling. The Vision Statement should briefly explain the new organisational capabilities and what difference that makes to high level stakeholders. If there is a Public Service Agreement or similar top level statement of organisational purpose, what impact will the changes proposed have on the organisation's ability to meet its objectives? Typically, a good Vision Statement will link to existing corporate strategies and objectives.

64. Good Vision Statements, although short, often take a long time to write, with multiple drafts being circulated to stakeholders to establish what captures their interest. Once the Vision Statement has been developed, it needs to be visibly owned and communicated. Seniors also have to be seen to be adhering to the spirit of it. If senior staff are known to flaunt its values, achieving cultural change becomes even harder. Selling the IA vision is easier if it is referenced in a higher level corporate strategy or vision.

Identify and Characterise Stakeholders

65. If the Main Board of Directors is to be persuaded by the SIRO of the case for change, it is helpful if most Directors have been alerted to the need for change by their own senior managers. Identifying key stakeholders who can play this role is important. Informal networking with IAOs and other senior business managers by those developing the case for change also provides invaluable information on what Directors are likely to find compelling.

66. Figure 3 illustrates how stakeholders can be categorised according to their importance and commitment to the programme. The objective is to obtain sufficient support that stakeholders, whose active participation is required, will provide it, and that those stakeholders who can oppose, or obstruct, change will not do so.

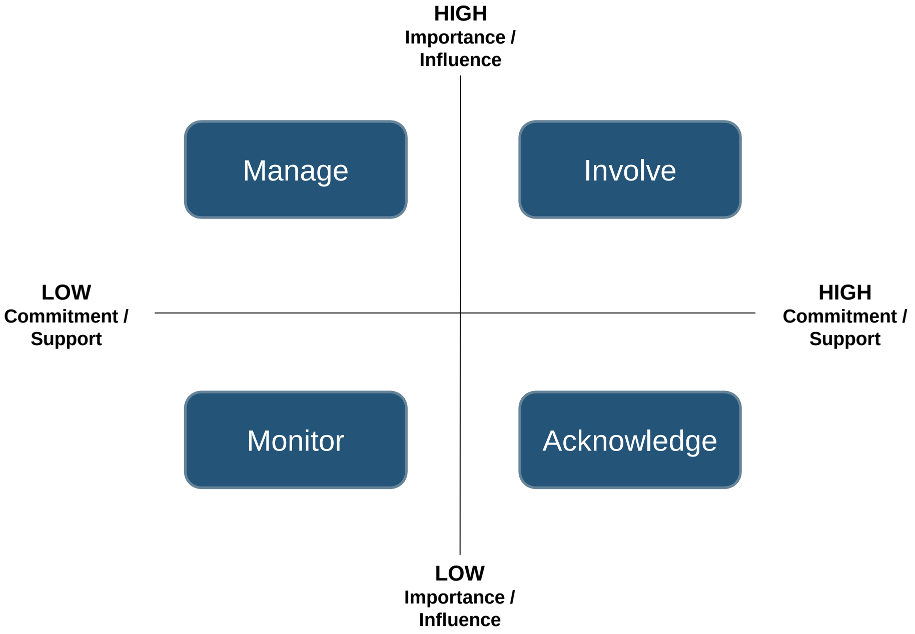


Figure 3: Stakeholder Mapping: Analysing Importance & Influence

67. For most individuals, a compelling case for change will require more than a few simple facts (the exceptions being those organisations that have just suffered a major security incident), but an aggregation of facts that combine to make the need for change compelling. Many business managers, who already feel under-resourced, will be reluctant to vote for diverting more resources to IA activities following a single meeting or presentation. However, they might be persuaded of the case for change by a longer exposure to IA issues. For example, a sequence of articles, bulletins or newsletters announcing the importance of IA, the need for corporate investment and the potential benefits of doing so, followed by a meeting to discuss what that might mean for their business unit, could gain their support.

68. An effective way of persuading people that security needs improving is to demonstrate its vulnerabilities. IT vulnerabilities can be demonstrated using the myriad of tools available on the Internet to identify and exploit vulnerabilities. Live hacking demonstrations (e.g. IT Health Check Penetration Test) can be risky as they may advertise your weaknesses and introduce dangerous tools on to your network, but sometimes they quickly change the opinions of business managers and data owners.

Chapter 7 - Making the Organisation Ready for IA Improvement

Key Principles

- Identify stakeholders and manage their concerns
- Clarify the business benefits to be realised
- Establish a Sponsoring Group to resource the change programme
- Use a structured project or programme management methodology
- Define the project portfolio that enables the wanted business benefits

Objective

69. The objective of this stage is to develop a credible, resourced plan to deliver the programme objectives agreed with the board of Directors and which will gain the support it requires from stakeholders to achieve the expected business benefits.

Produce Stakeholder Management Plan

70. Once the board of Directors has endorsed the SIRO's business case for a programme of work to improve IA, a Critical Success Factor (CSF) is stakeholder management. If realistic plans are to be developed, stakeholders need to be identified and categorised according to their level of influence and commitment to improving IA. Most IA improvement programmes will include a range of diverse tasks to deliver the cultural, process and technological changes needed and consequently will have a diverse range of stakeholders. Figure 4 provides an illustrative stakeholder map which aims to help the IA improvement programme identify who needs to be involved in the programme and in what capacity. Some stakeholders will have more than one relationship with the programme; e.g. they may provide direction and guidance at the start of the programme but have a customer, supplier or partner relationship later on.

71. Improving IA may entail changing business practices to something less popular and convenient. The people who most need to change (users) are seldom the primary beneficiaries of the changes (data owners and business managers) and will have other competing objectives. If they are to change, both they and their management need to be consulted, so that they feel that they have been consulted and also to have their needs and opinions factored into the change programme. If not, their long term commitment to improved IA will not be gained, without which sustained improvement is unlikely.

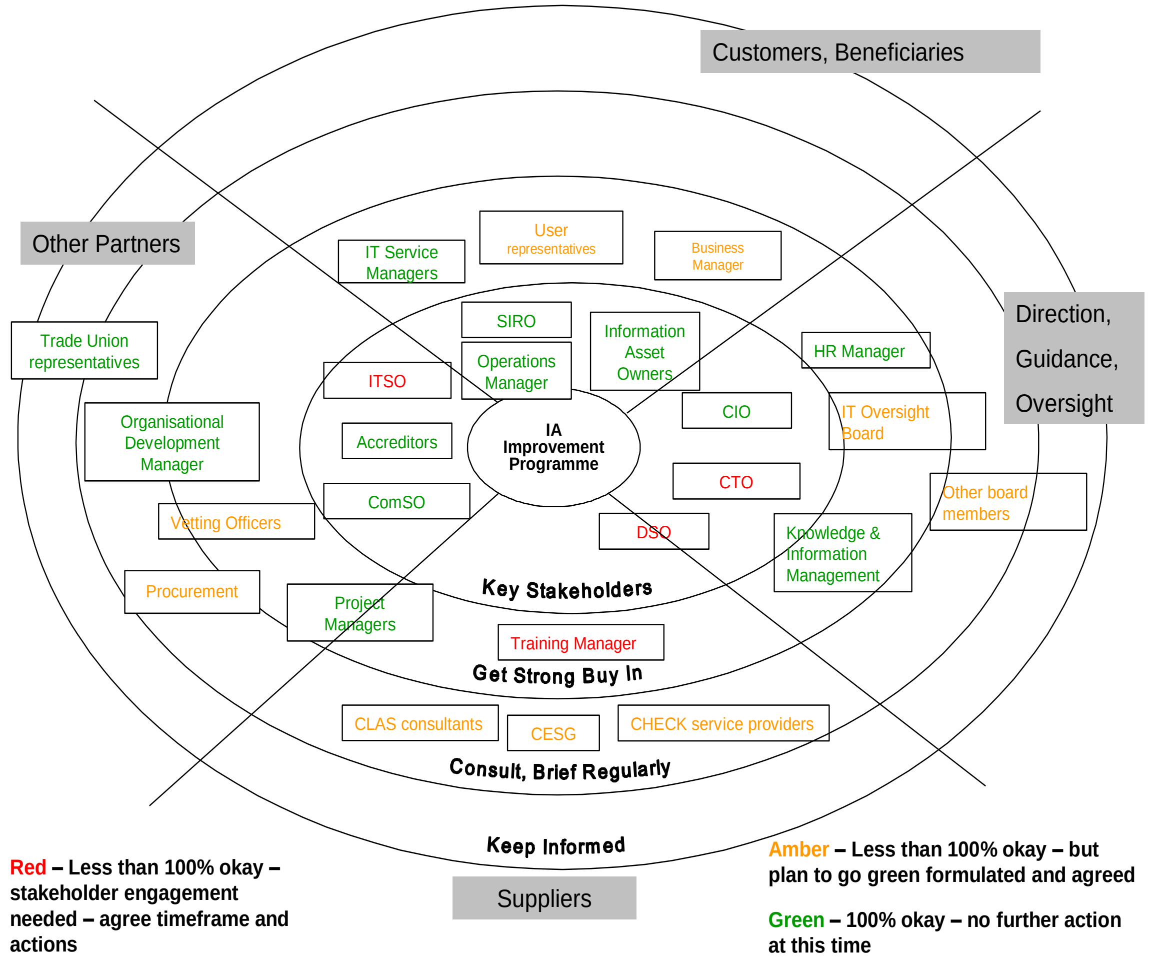


Figure 4: Illustrative Stakeholder Map

Establishing the IA Programme

72. The OGC (now part of the Cabinet Office) had developed much guidance on Managing Successful Programmes (MSP) (reference [k]). MSP describes a programme as:

> *"a temporary flexible organisation structure created to coordinate, direct and oversee the implementation of a set of related projects and activities in order to deliver outcomes and benefits related to the organisation's strategic objectives. A programme is likely to have a life that spans several years."*

73. Improving IA invariably requires the implementation of a diverse set of related projects and activities. Without the structure of a formal programme, success is unlikely. Key concepts in MSP, which are particularly relevant to improving IA maturity, are described below.

Creation of the Sponsoring Group

74. MSP describes the Sponsoring Group as representing 'those senior managers who are responsible for:

- The investment decision

- Defining the direction of the business
- Ensuring the ongoing overall alignment of the programme to the strategic direction of the organisation

75. MSP recommends that the Sponsoring Group's responsibilities include:

- Establishing the organisational context for the programme
- Authorising the Programme Mandate
- Approving funding for the programme
- Leading by example the values implied by the transformational change
- Providing continued commitment and endorsement in support of the programme objectives at executive and communications events
- Championing the programme

76. An active Sponsoring Group clearly greatly increases the prospects of making sustainable improvements to IA maturity. The chair of the Sponsoring Group would normally be the SIRO. Other members could be the CIO, CTO, DSO, Head of HR and managers of business units most affected by the change. If members choose to delegate their membership of the Sponsoring Group, they still need to ensure that the programme will have sufficient influence across the organisation to realise the vision.

Identifying and Defining the Programme

77. MSP provides guidance on identifying and defining the programme such that the programme deliverables combine to deliver the wanted benefits in a managed way. This is particularly relevant to improving IA maturity due to the breadth of the problem space.

78. The CIAMM® assesses maturity in 6 areas: Leadership & Governance; Training, Education & Awareness; Information Risk Management; Through-Life IA Measures; Assured Information Sharing and Compliance. An IA maturity assessment will identify the organisations limitations in each of these areas and suggest ideas for improvement. Consequently, a programme to improve IA maturity is likely to include a mix of projects and activities covering the spectrum of culture, process and technology change. Some objectives may be achieved by making changes to existing projects or initiatives; e.g. adding security requirements to IT infrastructure projects.

79. A key MSP technique is the use of programme executives who are members of the programme management team, reporting to the programme manager, who act as project executives on PRINCE2 project boards. Programme executives can bring co-ordination across a range of projects that combine to deliver business benefits.

Identify Critical Success Factors

80. Once the programme has been defined, good programme management will identify the CSFs. These are things that must be achieved, or pitfalls that must

be avoided, if the programme is to succeed. Monitoring progress against CSFs is particularly important in large, complex programmes. Examples are:

a. Maintaining the confidence of critical stakeholders such as the CIO, CTO, IT Service Providers and senior business managers. This could simply be by meeting early milestones.

b. Delivering recognisable benefits early in the programme such as some improvement to IA controls, or a better understanding of information risks.

c. Making the necessary cultural change such as through a communications campaign on IA awareness, or an IA training programme.

Specify the IA Control Set

81. The use of controls is an important concept in IA. IA controls are the defences that most directly prevent threat actors from causing business impacts. Examples are the anti-virus system that defeats malware, the authentication system that blocks unauthorised users and the well-configured firewall that blocks electronic attacks. These are distinct from activities such as appointing staff to mandatory roles (SIRO, DSO, ITSO, IAOs) or writing policies. Although these might be essential to developing effective controls, threat actors are not aware of these. The use of controls is central to ISO 27001 – Information Security Management System - Requirements (reference [g]).

82. Specifying the set of corporate IA controls is a key device for reconciling the desire to minimise information risk with the resources affordable to implement and operate IA controls. It is tempting for organisations to fudge this issue, through issuing policies prohibiting particular activities or behaviours, but not undertaking the other steps necessary to deter, detect & resist, or defend against the unwanted activities (see IS1&2 Supp, reference [i]) for definitions of these terms). Merely issuing a policy, or assigning a role, is not sufficient to produce a control, although they may be necessary first steps.

83. Making a management commitment to specify the set of corporate controls forces debate on what controls can be resourced, which ones are best value for money and what changes should be made to the set. If the set of controls is not well defined, it is unclear which controls are actually being implemented and therefore the risks to which the organisation is exposed.

Define Control Objectives

84. Delivering the business benefits wanted by the SIRO and Sponsoring Group will, in addition to specifying a set of largely existing controls, invariably require improvement in some controls. Figure 5 illustrates how the IA control set bridges the gap between the IA maturity goals, identified in the CIAMM®, and enabling business benefits. If the IA maturity goals have not been achieved, the effectiveness of IA controls is likely to be undermined, either because they are not supported by the IRM culture, or they are not underpinned by IA capabilities, or the compliance regime is ineffective.

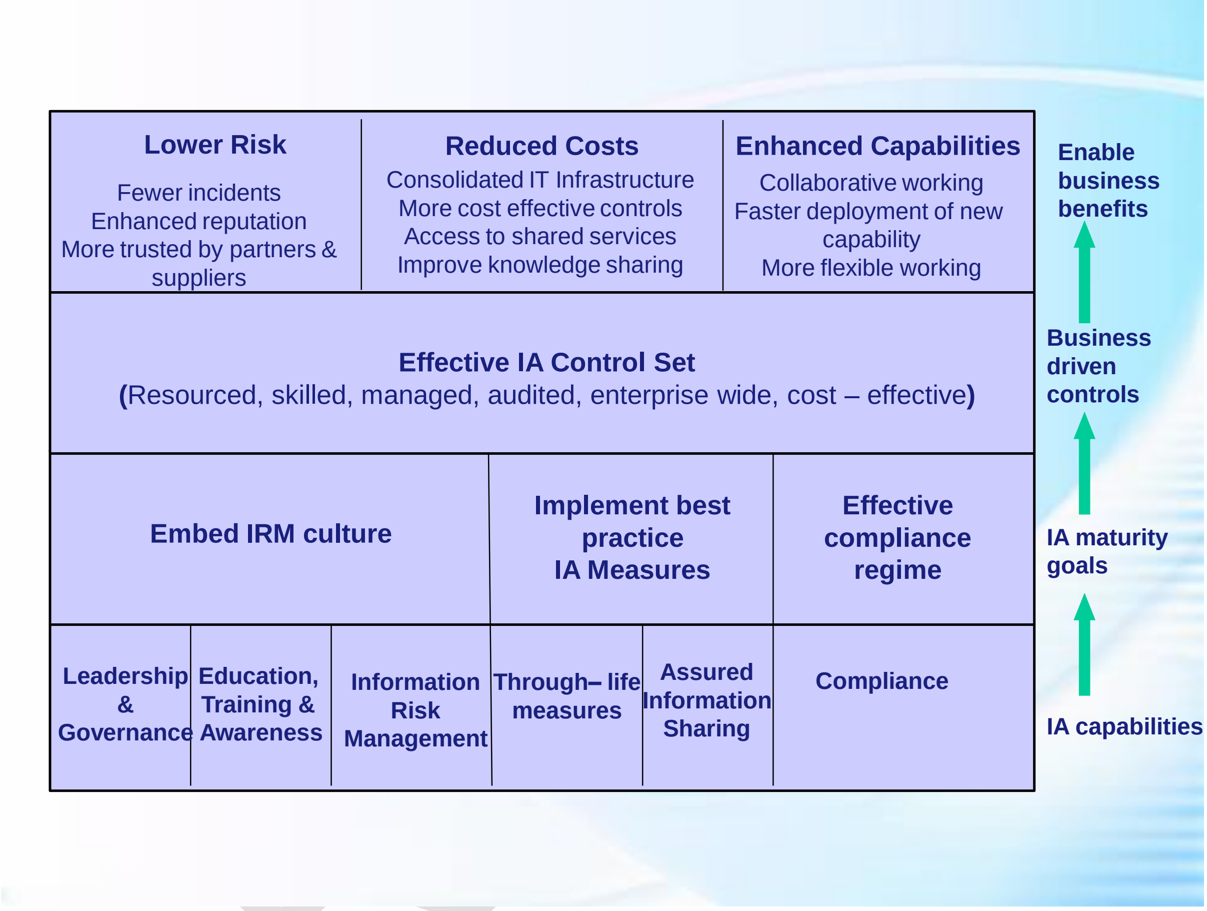
85. Effective controls have the following features:

a. Defined objectives, inputs and outputs.

b. Their effectiveness is measured and monitored.

c. The staff who operate them have appropriate skills, knowledge, tools and training.

d. Ownership is assigned to an individual who is responsible for its effective operation.



Lower Risk
Fewer incidents
Enhanced reputation
More trusted by partners & suppliers

Reduced Costs
Consolidated IT Infrastructure
More cost effective controls
Access to shared services
Improve knowledge sharing

Enhanced Capabilities
Collaborative working
Faster deployment of new capability
More flexible working

Effective IA Control Set
(Resourced, skilled, managed, audited, enterprise wide, cost – effective)

Embed IRM culture

Implement best practice IA Measures

Effective compliance regime

Leadership & Governance

Education, Training & Awareness

Information Risk Management

Through– life measures

Assured Information Sharing

Compliance

Enable business benefits

Business driven controls

IA maturity goals

IA capabilities

Figure 5: Building Blocks for IA Enabled Business Benefits

86. Controls are relatively easy things to manage. Unlike cultural attitudes and customers' perceptions, controls are largely within management's gift to define, operate and monitor for effectiveness. In a programme to improve IA, the identification of IA controls and control objectives is therefore a key step towards successful programme delivery.

87. It is highly desirable to introduce controls that make the user's life easier. If a control is being introduced across the whole organisation, the economies of scale may make it economic to introduce something more sophisticated and easier to use than the current version.

88. Well designed controls can balance IA objectives with other business objectives. For example, controlling the import of potentially malicious software can be achieved by letting users decide what they import, educating them on the risks and providing virus scanning tools. This maintains business flexibility, but places much trust upon users behaving responsibly. An alternative approach is to deny user access to removable media ports on their computers and force them to import all software through centralized points which scan for malware (Ideally, this centralised point would be physically separate from the main network to reduce the risk of malware propagating). The latter approach provides more assurance, but at the cost of business flexibility. A compromise approach is to permit the use of removable media ports subject to a suitable business case, which retains business flexibility, where the benefits justify the risks.

89. The symbiotic relationship between KIM and IA should be noted at this point. Although the roots of KIM and IA lie in separate professional disciplines, the controls developed under KIM to label and structure data can be extremely useful to IA. For example, an effective Electronic Data Records Management (EDRM) system supports secure information sharing and re-use, including an audit trail and access controls.

90. ISO 27002 (reference [l]) defines a useful set of security control objectives. A well used set of IT control objectives is defined at reference [m].

91. Control objectives can be defined in terms of:

   a. **Purpose** - What is the threat, vulnerability and potential business impact that the control is intended to mitigate?

   b. **Assurance level** - How strong should the control be? Is it intended to deter, detect and resist, or defend.

   c. **Process maturity** - How reliable must the operation of the control be? The Capability Maturity Model Integration (CMMI) (reference [n]) provides definitions of generic process maturity.

   d. **Coverage** - Is the control to be applicable across the entire enterprise or to parts of it? The wider the coverage, the greater the economies of scale, but also the greater overall cost. Staged increases in coverage may be appropriate, through first addressing highest priority areas.

Build IA into the Enterprise Architecture

92. An Enterprise Security Architecture (ESA) is a key enabler for developing effective controls. The larger and more complex an organisation becomes the less assurance can be achieved without an ESA. If there is no ESA, control objectives have to be implemented in different ways in different parts of the organisation, which prevents the economies of scale that are so often necessary to make good controls affordable. Additionally, if compliance with an ESA is not enforced, little assurance can be given that controls cannot be bypassed. For example, if there is no network security architecture, what assurance can be given that there are no unauthorised connections to the Internet that bypass network boundary controls?

93. An ESA should not be developed in isolation from an overall EA but should be a subset of it. It is important that IA is factored into the design of the EA. Many common IA controls are most cost effectively implemented when designed into the EA. Examples include:

    a. Physical access controls;

    b. User identification and authentication;

    c. Selection of secure protocols for communicating between IS;

    d. Provision of software patches;

    e. Anti-virus systems;

    f. Network boundary controls;

    g. Intrusion detection;

    h. Auditing misuse of legitimate access to information.

94. Relevant CESG GPGs to this topic are:

    a. GPG No 8 – Protecting External Connections to the Internet (reference [o]).

    b. GPG No 13 – Protective Monitoring for HMG ICT systems (reference [p]).

95. If there is no official EA or no recognised ESA components within it, the programme may need to initiate development of the ESA[1]. However, care needs to be taken that this does not delay delivery of the programme. The focus should be on establishing just those aspects of an EA that are needed to achieve the programme objectives.

Service Design

96. Once the programme has selected control objectives and identified a means of implementing them, it is important to ensure that they are implemented in a corporate manner, such that they continue to operate after the programme closes. For organisations that follow HMG's IT Infrastructure Library (ITIL) (reference [q]), IA controls look much like ITIL services. Controls have properties similar to the service attributes of inputs and outputs, owners and

[1] Using, for example, the Sherwood Applied Business Security Architecture (SABSA).

service levels. The ITIL service properties of utility and warranty are analogous to control objectives and maturity. For ITIL compliant organisations, it is therefore logical to develop IT based IA controls through the ITIL Service Design process, so that they become part of the corporate set of IT services.

Identify Wanted Cultural Changes

97. Driving cultural change will frequently require large scale training and awareness. The Cabinet Office had developed a free E-Learning package to improve the awareness of information security issues, although the Protecting Information Levels 1-3 E-Learning packages are now accessible via Civil Service Learning (reference [r]). Also, a downloadable set of packages was available from the Office of Cyber Security and Information Assurance (reference [r]), although the delivery of public sector IA training is now the responsibility of the National Archives (reference [r]).

98. The extent to which cultural change is required will also depend upon the effectiveness of controls. If user access to information and IT system privileges is tightly controlled, reliance on the user behaving correctly is reduced.

Policy Development

99. In most organisations, major changes will not occur without some form of official new policy or information bulletin. Creation of the change programme may be in response to a high level policy but many of the changes to be achieved by the programme will require policy development and communications in their own right. For example, if an organisation wishes to adopt a more rigorous policy on the use of passwords and to hold people to account if the policy is repeatedly ignored, the changed policy has to be formally promulgated. If the sanctions for non-compliance include dismissal or loss of security clearance, it may be necessary to consult trade unions and gain their agreement to the change.

100. Creation of good policies that are meaningful across a large organisation, and readily accepted by the workforce, are not easy to develop. Widespread consultation and many iterations of the text are normal. Time and resources need to be factored into the programme of work for policy development.

Case Study

One Government Department needed to urgently change cultural attitudes to security following a security incident in 2007. Steps the Department took included:

- Developing its Golden Rules of Data Security
- Issuing a Data Security Rulebook to every member of staff
- Half day training for every member of staff from Chairman to front line
- Establishing a security ‘brand’, including cartoon characters, through coasters, posters, roadshows and other documents.
- Data security roadshows at major sites with senior manager floorwalkers
- Developing and issuing a Managers’ Support Pack
- A Security Zone on the Department’s intranet giving access to more information

Communications Plan

101. As with any change programme, good communications is critical to success. If the organisation is to realise sustained business benefits from improved IA maturity, the workforce must be persuaded to change their working practices, if it is required to improve security. That means that the vision and business case, that persuaded the main board, needs to be communicated in terms that motivates the workforce. In practice, that means repeated communications, through a variety of media and mechanisms, explaining why organisational changes are needed and what the implications are for individuals.

102. The communications plan should cover the Making It Ready, Making It Happen and Making It Stick stages of the BCF and take into account the varying messages that need to be communicated to different groups of stakeholders. Further guidance on communications, for business change, is provided on the CESG website (reference [f]).

Chapter 8 - Making IA Improvement Happen

Key Principles

- Use a structured project management methodology
- Establish milestones and monitor delivery
- Monitor the impact of other programmes on IA
- Drive the cultural change

Objective

103. Once the programme to improve IA maturity is properly established, the next objective is to deliver the programme as planned and realise the intended benefits. The usual guidance to project and programme management is applicable, but the following points may be helpful in an IA maturity context.

Communicate Required Changes

104. In line with the communications plan, the existence of the IA programme should be widely communicated, as it is likely to affect many users. The initial communications may not explain exactly how it will affect each user, but if the reasons behind the programme are explained, and endorsed, at a senior level, users are more likely to be co-operative when asked to modify their working practices.

105. A frequent comment, from those implementing IA improvement programmes, is that people affected often do not understand why the organisation needs them to change their working practices. Often, the changes requested of individuals have to be set in a national, or organisation level, context and incident scenarios explained in such a way as to indicate that their actions make a large difference, before individuals are motivated to change their working practices.

Manage Delivery Stakeholders including Suppliers

106. As the organisation starts to feel the impact of the business changes, there will inevitably be some opposition to the changes. The Programme Management Office (PMO) must be receptive to the reactions, responding to concerns, perhaps by modifying plans or by further explanation of the reasons for change.

107. A common problem among organisations is improving the IA performance of their delivery partners such as Managed Service Providers. Where a contract already exists, the first option should be to amend the terms detailing the IA controls that the service provider is to provide e.g. see CESG GPG No. 6 Outsourcing & Offshoring: Managing the Security Risks (reference [s]), Mandatory Requirement 11 of SPF (reference [b]), and the Government ICT Offshoring Guidance (reference [t]). When payment for the improved IA functions is an issue, suppliers can be referred to the CIAMM® and its Assessment Framework as illustration of the increased public sector focus upon IA. A version of the model for assessing major suppliers of IT services to the public sector was also created with the industrial body Intellect (i.e. a leading

trade association which serves to represent its members in the UK technology industry with HMG). Suppliers who have a track record of delivering IT services at a high level of IA maturity are likely to have a competitive advantage, over those without, in future procurements.

108. In cases when a new contract is to be let for an IS or an IT service, there is an opportunity to build IA controls into the contract from the outset. A simple approach is to state mandatory and desirable security requirements in the Invitation to Tender (ITT), but too many mandatory controls constrain supplier design options and too few provide little guidance.

109. A better approach is to negotiate over the set of IA controls that the supplier will deliver, in the context of the environment into which the system, or service, is to be deployed. In this approach, the customer provides background information on the IA controls within the hosting environment and the potential business impact of security incidents. These context setting documents should give the potential supplier an understanding of what additional controls will be valued by the customer.

110. The key security question in the ITT then becomes, 'given the environment into which this system is to be deployed, what additional IA controls do you propose?' In the case of an IS, these might be in the form of security functions that the system will provide. In the case of an IT Service, the supplier might be expected to operate the controls as well, e.g. maintain an anti-virus capability with regularly updated virus signatures. For some controls, there might be a division of responsibility, e.g. for access control the supplier will operate an authentication service, but the customer will maintain the list of authorised users.

111. A good framework for eliciting from potential suppliers details of the controls they propose is ISO 27001 (reference [g]). The standard identifies over 130 potential controls, which can be selected and tailored to local needs.

112. Once a tender containing a set of controls has been received, IA specialists can assess whether they are adequate to mitigate the perceived information risks. The procurement schedule needs to allow time for the controls to be analysed, their meaning clarified, their effectiveness challenged and refinements made. As negotiations become more detailed, control objectives, and the means of measuring compliance, become more relevant. These issues are examined in ISO 27002 (reference [l]) and ISO 27004 (reference [u]) respectively.

113. For contracts delivering an Information Service that is to be operated by the supplier, requesting certification to ISO 27001 is a powerful tool, provided the contract entitles the customer visibility of the management review and audit process. An ISO 27001 certificate, on its own, does not guarantee any particular level of security, but it does give management, and therefore potentially customers, reasonable visibility of the effectiveness of the IA controls being implemented by the supplier. Similarly, contract conditions that reserve the right to audit against the CIAMM®, or subsequent versions, give the customer visibility of the supplier's approach to IA.

Case Study
For one Government Department, their programme to improve IA maturity required considerable stakeholder management by the Security Business Unit and key IAOs to initiate the programme. Defining the programme content involved more stakeholder management over a 6 month period, as the scale of wanted change became apparent. Delivering the programme required another round of stakeholder management, mainly with system managers, who were most impacted. Embedding the change required yet more stakeholder management to resource the changes wanted to the audit regime. A key lesson from the programme was the ongoing need for stakeholder management with an evolving set of stakeholders.

Monitor Benefit Enabling Milestones

114. Measuring progress is important in managing delivery. Deliverables can be identified at each of the 3 layers (see Figure 5, page 26) that enable benefit realisation: process, process goals and controls. The IA Maturity Assessment Framework refers to many products or documents, the production of which can constitute project deliverables. The planned implementation of controls provides good opportunities for identifying benefit enabling milestones. Suitable milestones could include the following:

a. Roll out of a control to a specified level of coverage in terms of the number of systems, interfaces, computers or people.

b. Initiation of a control to a given specification.

c. Improved process maturity of a control.

d. Improved strength of a control.

e. Reduced cost of a control.

115. How frequently progress should be reported should also be considered. Typically, project managers will report to the programme manager who will report to the Sponsoring Group who will report to the board of Directors. Reporting will normally be more frequent from the project manager than it will be from the Sponsoring Group. The less frequently reports are raised, the longer it will take to resolve problems, potentially leading to delays in realising the wanted benefits.

Monitor Impact of Other Programmes on Information Assurance

116. Other programmes and initiatives are likely to have an impact upon IA, both positive and negative. The IA Programme needs to maintain a watch across the organisation for changes that help, or hinder, it achieve its intended business benefits. IT infrastructure programmes provide opportunities to build additional controls, or strengthen/extend the coverage of existing controls. Building refurbishment provides opportunities to strengthen physical controls.

117. New IS often increase the level of residual Information Risk, even when carefully designed and accredited, because they usually extend access to information. If accreditation is well established across the organisation, accreditors can provide a network of IA agents to report relevant changes back to the PMO.

Identify and Deliver Quick Wins

118. It is important for the IA Programme to establish its credibility by quickly delivering something of value. As well as the value obtained for stakeholders, invariably programmes learn from initial deliveries and this assists future deliveries. Quick wins might consist of:

   a. A survey, or IT Health Check, that establishes the extent of some type of vulnerability across the enterprise. This can be used to prioritise deliveries.

   b. Pilot use of a new control.

   c. Trial of a new tool.

   d. Production of a new policy.

Extending the Coverage of a Control

119. IA programmes that aim to extend the coverage of a control, across the organisation, will often find that coverage is best extended in stages. The first stage can be chosen to form a pilot. The pilot stage will preferably have supportive stakeholders and the territory should be familiar to the project team, so the chances of success are high. Experience gained on the first stage can be used to develop a repeatable process which is then deployed and refined on subsequent stages. This enables more realistic plans to be developed for extending control coverage across the entire organisation.

120. Frequently, each stage will require renewed effort to influence local stakeholders. Identification of supportive and influential local stakeholders can be crucial in persuading all staff affected to support the change.

Case Study
A Government Department wished to improve software patching levels to make its IT infrastructure more resilient to malware. It was difficult to persuade operational users of the need to resource this and to accommodate the consequent system down time.

One day there was a very important and urgent operational requirement to import a large volume of data from an untrusted source onto the prime operational system. Operations did not want to wait for the data to be virus swept before using it and its transfer without virus sweeping was authorised at a senior level. The data did contain some malware but the consequences were minor. However the incident was sufficient to persuade senior operations staff that they did not want to have to take that risk again and they were subsequently supportive of the case for patching, authorising greater down time to accommodate it.

Service Transition to Operation

121. For organisations following ITIL practices, during this stage of the BCF, new or extended IA controls should Transition to Operation, so they formally become part of business as normal.

Instigate Cultural Change

122. If the CPNI SeCURE 2 tool has been used, it will suggest areas for cultural change. Cultural change activities are likely to include some form of user training and awareness, so that all staff understand their responsibilities and the reasons for them.

123. There may also be a need for training specific to the new controls that are being implemented. Staff who implement or operate the control (e.g. Intrusion Detection) may require substantial training to be fully effective.

Chapter 9 - Embedding the Change

Key Principles

- An effective IA audit regime enables more liberal IA policies which permits more flexible business practices
- Audit compliance with new policies
- Monitor corporate culture
- Establish sanctions for non-compliance
- Devise metrics to monitor
- Develop a reporting framework

Objective

124. Once improved IA controls have been established, it is important to ensure that the change is embedded in the organisation and that working practices do not slowly revert back to the previous state. Old habits die hard. This Chapter outlines techniques for embedding the change.

125. In addition to embedding changes by monitoring compliance with policies, IA audit regimes have two other benefits:

a. Enabling the adoption of more liberal IA policies as the organisation has greater confidence that abuse of the policy will be detected. This can enable more flexible working practices, which helps justify the cost of auditing.

b. Providing evidence of the limitations of existing controls to justify further investment in improvement.

The HMG Audit Regime

Auditing or compliance monitoring comes in many forms, but typically involves an independent, objective assessment of whether a particular practice is being followed. HM Treasury uses an audit model comprising 3 layers of defence (see reference [v]). The 3 layers are described below and illustrated in an IA context in

126. Figure 6 (page 39). The layered approach helps make the audit regime more efficient, as the top 2 layers monitor the effectiveness of the layer below. Without a layered, structured approach, the costs of auditing can quickly become uneconomic, with the costs better spent on improving already known weaknesses.

Risk Control

127. The Risk Control layer includes the day-to-day controls such as Access Control, Anti-Virus scanning, Intrusion Prevention System and Configuration Control. It is at this layer that routine security is provided. Outputs from this layer include alerts, incident reports and reports confirming that the control is operating. Management responsible for the control undertakes some form of audit to confirm that the control is operating effectively.

128. Recommendations and ideas for controls or control objectives can be found in ISO 27002 (reference [l]), Control Objectives for IT (reference [m]), HMG's IT Infrastructure Library (reference [q]), the SPF (reference [b]) and the CESG IA Policy Portfolio (reference [w]).

129. Key actors in risk control will be IT service providers, security staff and system managers.

Risk Management

130. The Risk Management layer checks that the corporate set of IA controls is operating appropriately. The SIRO is responsible for this layer and it includes accreditation and IA maturity assessments. Typically the accreditation process will check that controls are being applied to IS both during accreditation and re-accreditation. The annual IA maturity assessment considers how well information risk (IR) is being managed across the organisation.

131. If the risk management layer is to be effective, risk managers need clear points of contact, within the risk control layer, to consult on points of concern. These contacts may fill roles such as Information System Security Officer, Information System Security Manager, System Manager, Service Manager or System Administrator. Whatever the role is, their duties to risk managers should be made clear in their terms of reference, otherwise questions from risk managers tend to be passed from person to person without effective resolution.

132. CESG provides a range of schemes to support risk managers. For example Commercial Product Assurance (CPA), IT Health Check Service (CHECK) and the Assisted Products Service (CAPS). These are detailed at www.cesg.gov.uk.

Risk Assurance

133. Within most government departments, the Risk Assurance layer is the province of the IAU. The IAU follows audit standards and guidance from HM Treasury. It is tasked by the Accounting Officer and reports its findings to the Audit Committee which is chaired by a Non Executive Director. The IAU is therefore outside the control of management and is able to provide an independent view of the effectiveness of management controls. IAUs are concerned with all forms of risk and not just with IR. For other parts of the public sector, the Risk Assurance function is undertaken by other audit bodies, such as the Audit Commission.

Adjusting the Audit Regime

134. When new controls are brought into use or improved in some way, the audit regime should be adjusted to monitor compliance. The IA Programme should consider how day-to-day effectiveness of the control will be monitored in the Risk Control layer. Points to consider are:

a. Who is the control owner?

b. Who will operate the control?

c. How will they provide assurance that the control is operating correctly?

d. Who should receive reports on control effectiveness?

e. Who should be informed when the control detects some form of unwanted behaviour?

135. Minor changes to controls may not require any additional audit resourcing, but frequently the introduction of a new control, or the major expansion of an existing control, will require some increase in audit resource, if control effectiveness is to be sustained.

At the Risk Management layer, the accreditation function should reflect the introduction of a new control by updating the set of corporate controls which are considered for applicability in each accreditation decision. Also, they should update the guidance given to accreditors. Typically, implementation of a new control will require consideration in each of the business change activities described below.

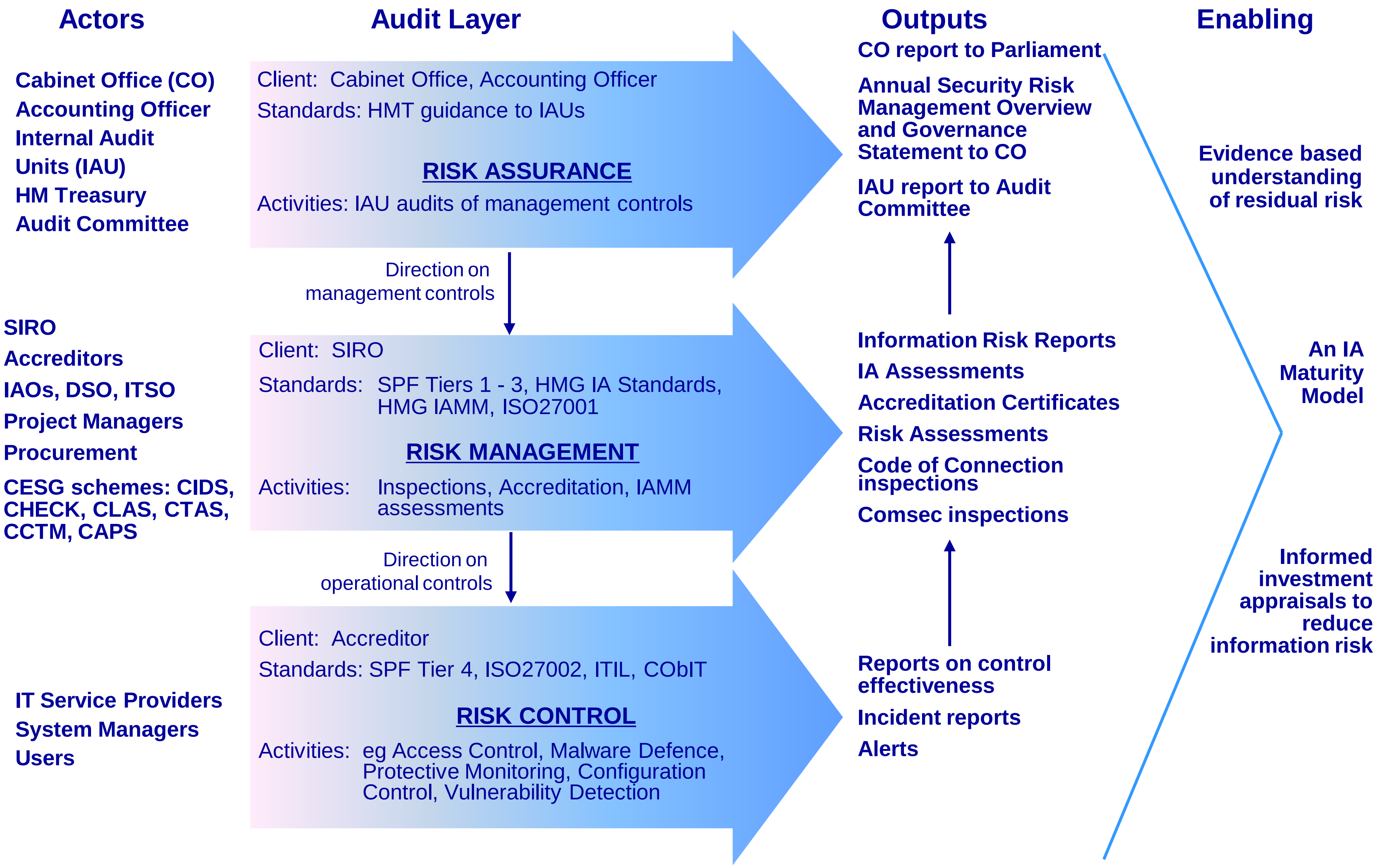

Actors
Audit Layer
Outputs
Enabling
Cabinet Office (CO)
Accounting Officer
Internal Audit
Units (IAU)
HM Treasury
Audit Committee
Client: Cabinet Office, Accounting Officer
Standards: HMT guidance to IAUs
RISK ASSURANCE
Activities: IAU audits of management controls
CO report to Parliament
Annual Security Risk Management Overview and Governance Statement to CO
IAU report to Audit Committee
Evidence based understanding of residual risk
Direction on management controls
SIRO
Accreditors
IAOs, DSO, ITSO
Project Managers
Procurement
CESG schemes: CIDS, CHECK, CLAS, CTAS, CCTM, CAPS
Client: SIRO
Standards: SPF Tiers 1 - 3, HMG IA Standards, HMG IAMM, ISO27001
RISK MANAGEMENT
Activities: Inspections, Accreditation, IAMM assessments
Information Risk Reports
IA Assessments
Accreditation Certificates
Risk Assessments
Code of Connection inspections
Comsec inspections
An IA Maturity Model
Direction on operational controls
IT Service Providers
System Managers
Users
Client: Accreditor
Standards: SPF Tier 4, ISO27002, ITIL, CObIT
RISK CONTROL
Activities: eg Access Control, Malware Defence, Protective Monitoring, Configuration Control, Vulnerability Detection
Reports on control effectiveness
Incident reports
Alerts
Informed investment appraisals to reduce information risk

Figure 6: The HMG Information Assurance Audit Regime

Establish a Reporting Chain

136. It is important that findings from the Risk Control layer are reported to the Risk Management layer in a systematic manner, so that management understands how effectively the Risk Controls are operating. It may be helpful to convene a regular meeting at which reports from the Risk Control layer are presented to a panel of stakeholders. The panel can decide how to respond to specific findings, but the panel also drives improvement in the Risk Control layer. Ultimately, the SIRO is responsible for establishing the reporting chain, but will generally delegate responsibility for organising the reporting to the DSO.

Continuous Service Improvement

137. If the organisation follows ITIL practices, the principles of Continuous Service Improvement should be applied to the IA controls in this stage of the BCF. The audit regime should be designed and used to assist this, providing the metrics upon which service performance can be measured.

Reward Good Behaviour

138. If there is no organisational process for rewarding people who contribute to good IA, it should be no surprise if IA maturity fails to improve. Many people have some active involvement in maintaining IA and this should be recognised in their performance objectives and annual performance reviews. For some people, their work will be driven by IA requirements and they should feel that this provides them with reasonable opportunities for demonstrating good performance and career progression. If they do not, it will be difficult for the organisation to attract capable people into IA roles.

139. People are also influenced by how they believe other people are behaving. People who are rewarded for good behaviour tend to tell others about it, even if the reward is fairly minor, thus encouraging others to behave similarly. Rewards may simply consist of appearing on a list of commendations in a staff newsletter or a complimentary e-mail to the individual and their line manager. They do not need to include a financial element.

Apply Sanctions for Unwanted Behaviour

140. If unwanted behaviour (i.e. failure to comply with security policies and procedures) is to be deterred, it is important that the organisation has a range of sanctions to apply. Many people occasionally make minor security mistakes, the very large majority of which have no direct security consequences. Such minor incidents need not be punished, but ideally individuals should be alerted to their mistake. If they continue to breach policies, there should be a set of escalating sanctions that the organisation can apply, such as informal and formal warnings, loss of security clearance and ultimately dismissal or prosecution. Without an appropriate range of sanctions, some forms of unwanted behaviour will have no appropriate level of sanction, which implies some individuals might be treated either unduly leniently or unduly harshly.

141. It can be worth publicising the use of sanctions by stating the number of staff who have been reprimanded or disciplined in some form for failing to comply with IA policy. If such occurrences are never publicised, staff tend to assume that the policies are not policed.

Embed Training Courses

142. Cultural change will normally entail some form of training and awareness courses. Such courses need to be embedded into routine training programmes such that all staff receive at least some form of annual training.

Monitor Cultural Change

143. Monitoring cultural change is a key indicator of whether the IA programme has been successful. The CPNI SeCURE 2 tool enables cultural change to be monitored and in particular to monitor the wanted changes that were identified in the Make It Ready stage. If the organisation operates an annual staff survey, it may be used to monitor whether the cultural changes have been sustained. Mechanisms for building IA into day-to-day business include:

a. Frequent communications from seniors on IA issues.

b. Include IA in induction and refresher training courses.

c. Include IA in staff surveys.

Case Study

One Government Department had for many years operated a policy of storing logs of staff use of computers but rarely used them to detect misuse. Through an IA programme, it bought and developed tools to analyse the logs and allocated a couple of members of staff to look for evidence of misuse. Evidence was soon found and it demonstrated the value of centralised auditing. Based on this, a business case was approved for a team of 12 auditing a wider range of controls. Findings that the audit team could not resolve were input to the corporate Security Incident Management system. A set of sanctions was developed with HR to give staff informal warnings of minor infringements and initiate formal disciplinary procedures for repeated or major infringements. The system gave management a better understanding and control of misuse of computer systems and more options for extending access to the IT systems, whilst monitoring how it is used.

Annex A - An Overview of Maturity Models in the Context of IA

What is Information Assurance?

1. Information Assurance (IA) can be described as the steps taken to gain 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 (SPF (reference [b])).[1] Confidence is typically derived from a variety of factors, including objective examination of compliance with recognised standards, by competent people. For a public sector organisation in the Information Age, achieving a high level of IA is important, but it has to be balanced with other business objectives that compete for resources and management attention.

What is IA Maturity

2. IA maturity is a measure of an organisation's ability to achieve IA in support of business objectives. As IA maturity improves, an organisation gets ever closer to the optimum balance between IA and other business objectives, to maximise its long term business prospects. The optimum balance takes into account not just the level of security in an organisation, but also how well it is managed to provide assurance that security processes operate as expected and in line with business objectives.

What is a Maturity Model?

3. In order to measure IA maturity, we need some form of benchmarks to compare with an organisation's actual IA maturity state. A set of benchmarks defined for the purpose of assessing maturity is commonly referred to as a 'Maturity Model'. Maturity models can be described as a reference model of mature practices in a specific discipline, used to assess a group's capability to practice that discipline. They have existed for many years and cover many disciplines including software development, system development, acquisition and HR management. Most models have 5 levels of increasing maturity, illustrated in the diagram below.

4. The use of 5 levels enables organisations to assess their level of maturity and set objectives for improvement in high level terms, that are readily appreciated by Directors, but also contain the detail to be useful to practitioners.

[1] Note: In this context the term 'Information System' refers not just to computer based information systems, but also to systems based on paper or other media.

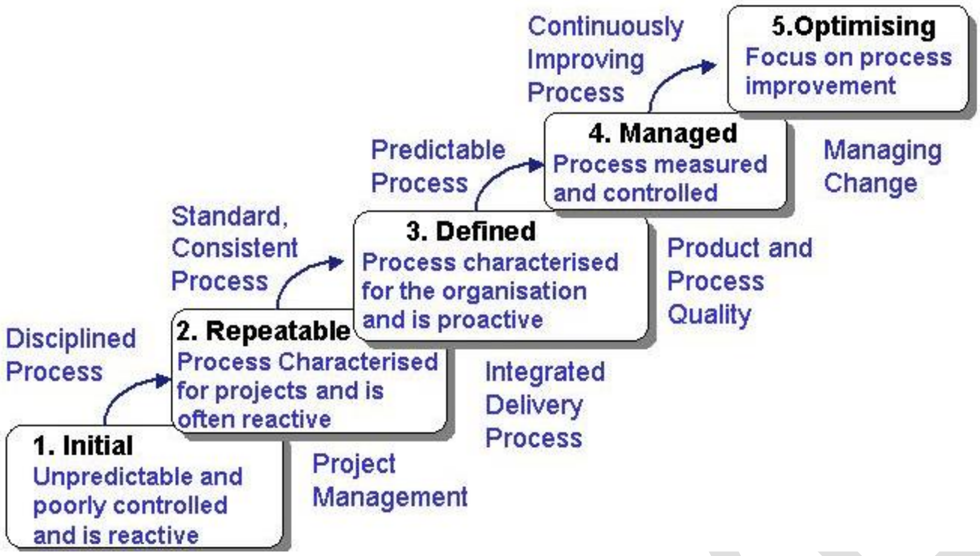


Figure A1: Illustration of the maturity model for systems development, CMMI

5. The sophistication of maturity models varies enormously. Probably the best known maturity model is the one developed by the Software Engineering Institute at Carnegie-Mellon University, USA. Now titled CMMI (Capability Maturity Model Integration) (reference [n]), it applies to system development and is a derivation of its earlier software development maturity model known as CMM (Capability Maturity Model). CMM was developed in the 1980s in response to concerns, in the US Department of Defence, at frequent cost and schedule overruns in software development projects. It provided a framework by which potential suppliers could be assessed on how likely they were to deliver in line with what they had predicted. CMMI is freely available and covers over 600 pages. It has had enormous influence across industry with hundreds of organisations gaining certification to Level 3 or above. Most maturity models have been influenced by CMM and CMMI.

6. Key features of CMM and many other maturity models are:

   a. The application of process management and quality improvement concepts to improve predictability of delivery.

   b. A focus on the outcomes sought in the discipline, rather than how they should be achieved.

   c. Guidance on developing a culture of excellence.

   d. The organisational structure for assessing capability and processes.

7. As organisations progress up a maturity model, management should obtain greater visibility of the activities that constitute their discipline and consequently have greater control over the outputs. In a typical maturity model:

- At Level 1, there is little structure in the way that work is done. The cost, quality and timeliness of delivery of products, or services, is unpredictable

- At Level 2, some structure appears, but it is managed locally, so performance may vary widely between units performing similar activities
- At Level 3, policies and processes are defined across the organisation and are tailored to local needs, as required
- At Level 4, process and capability performance is measurable
- At Level 5, the performance is improving measurably

8. Other relevant maturity models are contained within:

    a. Control Objectives for IT, which was produced by the IT Governance Institute (reference [m]).

    b. IT Infrastructure Library, which was developed by the HMG Office of Government Commerce (OGC), which is now part of the Cabinet Office (reference [q]).

Annex B - Reducing the Total Cost of Ownership of IS through Investment in IA

1. For most Information Systems (IS), IA costs are only a small part of the Total Cost of Ownership (TCO). If IA costs are less than 10% of the TCO, a 5% increase in IA costs, to achieve a 1% reduction in TCO, still delivers a healthy return on investment. Even higher returns may be achieved, if improved IA enables new ways of doing business that were previously too risky to be accepted.

2. Below are 10 ways in which good IA can help organisations cut costs. References are provided for further information.

3. Remember that it is invariably cheaper to build security into IS at the start of the system lifecycle than to attempt to bolt it on at the end. Good security might be implemented very cheaply when designed in at the start. If it is not considered at all during the design stage, the security of the system may be fundamentally compromised with no practical way of securing it.

Home or Mobile Working

4. More people working away from the office reduces the need for expensive office accommodation and it can increase business agility and flexibility. But home, or mobile working, bypasses the office safeguards. CESG Good Practice Guide No. 10 (GPG 10) on Remote Working (reference [x]) provides advice on managing the risks of doing so.

Improved IT Capacity Management

5. Many IT departments wish to reduce costs by consolidating their applications onto a smaller number of servers. Virtualisation is a common technology for achieving this, but it comes with risks. CESG Good Practice Guide No. 12 (GPG 12) on the Use of Virtualisation Products for Data Separation: Managing the Security Risks, (reference [y]) helps organisations judge how far they can trust virtualisation products to separate data of differing sensitivities.

Outsourcing IT Services

6. Specialist commercial IT service providers can often deliver services more cheaply than government. However, if the supplier fails to protect your data, you still remain accountable for the consequences. ISO 27001 (reference [g]) details the requirements for an Information Security Management System and it is widely used in industry. However, simply demanding that your supplier be certified as compliant with the standard is not sufficient to ensure that your data is protected appropriately. The standard does not mandate any particular level of security, but it does mandate how it will be managed and that is sufficient for the client IA professional to monitor information security and drive changes, where required. Ask for sight of the ‘Statement of Applicability’, which details which of the controls will be applied. Also, ask for the option to participate in

the management review process. An Internet based search on 'ISO 27001' provides a mass of information on certifiers and training.

Offshoring

7. Offshoring is the delivery of services from outside the European Economic Area (EEA), which often realises savings related to low labour costs. Under EU law, countries inside the EEA are obliged to implement a law equivalent to the UK Data Protection Act. Countries outside the EEA may not provide this legislation. CESG GPG No. 6 Outsourcing & Offshoring: Managing the risks (reference [s]) and the CIO Council Government ICT Offshoring (International Sourcing) Guidance (reference [t]) provides guidance.

Shared Services

8. Rather than develop your own application, or IT infrastructure, it may be cheaper to share use of a service developed for other parts of government. Cabinet Office is driving the use of shared services, particularly in the areas of networking, data storage and desktop services. How can you trust the security of services that you don't own or control? The Pan Government Accreditation service, now provided by CESG, aims to meet this need, making judgements on behalf of, and in consultation with, data owners on whether the residual risks of an IS are acceptable. Enquiries on this service may be made through enquiries@cesg.gsi.gov.uk.

Use of Untrusted Networks

9. Organisations increasingly need to make connections to the Internet to share information with the public and business partners. The Internet can also provide a cheap network for supporting home or mobile working and enabling team working across disparate geographic areas. GPG 8, Protecting External Connections to the Internet, (reference [o]) describes how to manage related risks.

Application Hosting

10. Application Hosting (AH) is a term for an IT infrastructure that is designed to host multiple applications. AH can substantially reduce the TCO per application and the time taken to deploy a new application. However it is akin to putting a lot of eggs in one basket. Vulnerabilities in the AH infrastructure, and even vulnerabilities in a single application, can compromise all data hosted. Advice on developing AH systems can be obtained through CESG consultancy services or through some CESG Listed Adviser Scheme (CLAS) consultants. CESG Good Practice Guide No. 9 (GPG 9) Taking Account of the Aggregation of Information (reference [z]) provides advice on the potential effect of aggregation on impact levels. Penetration testing of an AH system can be obtained through the CHECK scheme (e.g. this is detailed at www.cesg.gov.uk/servicecatalogue/CHECK/ Pages/index.aspx).

Improved Risk Analysis & Treatment

11. Many organisations accept security constraints that have evolved over time in relation to the way that they do business. In some cases, scrutiny will reveal that whilst the constraint removes multiple risks, some can be cost effectively mitigated by other means and the rest are worth accepting, thereby enabling removal of the constraint. IS1 & 2 Supplement (reference [i]) provides a methodology for risk assessment and treatment.

Centralised Controls

12. A common practice in IA is to mandate policies, or practices, that need to be implemented by many users, project managers, or system managers. The total implementation costs may be large, but mainly hidden from management. Access management, anti-virus defences, network management, and patching can come into this category. In such cases, it is often cheaper to implement controls centrally and a higher level of assurance can be obtained at the same time.

Use of KVM Switches

13. Some users need access to multiple IT systems that cannot be logically connected due to different sensitivities. CESG IA Top Tips 2013/01, Managing the Risks from Desktop KVM Switches (reference [aa]) provides advice on the use of keyboard, video and mouse (KVM) switches that enable one user terminal to access multiple IS environments of different sensitivities or protective markings.

References

[a] CESG Good Practice Guide No. 40, the Information Assurance Maturity Model and Assessment Framework, (UNCLASSIFIED) – latest issue available from the CESG website.

[b] HMG Security Policy Framework (SPF), Cabinet Office, available from www.cabinetoffice.gov.uk/resource-library/security-policy-framework .

[c] The UK Cyber Security Strategy – protecting and promoting the UK in a digital world, November 2011, available from www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy

[d] UK Government ICT Strategy, available from www.cabinetoffice.gov.uk/content/government-ict-strategy

[e] HMG Information Assurance Standard No 6, Protecting Personal Data and Managing Information Risk, Issue 2.0 October 2011 (UNCLASSIFIED). Available from the CESG website.

[f] CESG's Business Change Framework, available from www.cesg.gov.uk/publications and search on "business change".

[g] ISO/IEC 27001:2005, Information Security Management Systems – Requirements.

[h] Security Risk Management Overview (SRMO). This should be provided, to appropriate HMG bodies, by the Cabinet Office www.cabinetoffice.gov.uk .

[i] HMG Information Assurance Standard 1&2 – Supplement – Technical Risk Assessment and Risk Treatment, (UNCLASSIFIED) – latest issue available from the CESG website.

[j] Managing Information Risk: a guide for Accounting Officers Board Members and Senior Information Risk Owners (March 2008), prepared by National Archives, available from www.nationalarchives.gov.uk/services/publications/information-risk.pdf

[k] Managing Successful Programmes, developed by the Office of Government Commerce, which was moved into the Cabinet Office, available from www.cabinetoffice.gov.uk/resource-library/best-practice-and-methodology-projects-programmes-and-portfolios , www.msp-officialsite.com , and www.best-management-practice.com/Programme-Management-MSP .

[l] ISO/IEC 27002:2005, Code of Practice for Information Security Management.

[m] CObIT, IT Governance Institute, www.isaca.org .

[n] Capability Maturity Model Integration, www.sei.cmu.edu/cmmi .

[o] CESG Good Practice Guide No. 8, Protecting External Connections to the Internet, (Not Protectively Marked) – latest issue available from the CESG website.

[p] CESG Good Practice Guide No. 13, Protective Monitoring for HMG ICT Systems, (Unclassified) – latest issue available from the CESG website.

[q] IT Infrastructure Library v3, Service Design (Originally developed by the Central Computer and Telecommunications Agency [CCTA], which was later merged with the Office of Government Commerce [OGC], which has now moved to the Cabinet Office), www.itil-officialsite.com .

[r] Office of Cyber Security and Information Assurance, Cabinet Office, available from www.cabinetoffice.gov.uk/content/office-cyber-security-and-information-assurance-ocsia , and downloadable packages from http://www.ocsia-nfa-elearning.org [Username and password required, so it is necessary to contact OCSIA]). National Archives IA training, www.nationalarchives.gov.uk (e.g. senior level training programme available from www.nationalarchives.gov.uk/information-management/training/information-assurance-training.htm). Civil Service Learning, www.civilservicelearning.civilservice.gov.uk (e.g. e-learning for Protecting Information – Levels 1 to 3).

[s] CESG Good Practice Guide No. 6, Outsourcing & Offshoring: Managing the Security Risks, (Not Protectively Marked) – latest issue available from the CESG website.

[t] CIO Council Government ICT Offshoring (International Sourcing) Guidance, v1, July 2011, available from www.cabinetoffice.gov.uk/resource-library/government-ict-offshoring-international-sourcing-guidance .

[u] ISO/IEC 27004:2009, Information technology - Security techniques - Information security management - Measurement.

[v] HM Treasury Good Practice Guide; The Internal Audit Role in Information Assurance, January 2010, available at www.hm-treasury.gov.uk/d/internalaudit_informationassurance180110.pdf .

[w] CESG IA Policy Portfolio (for those with authorised access), http://cesgiap.gsi.gov.uk/ia-policy-portfolio/index.shtml .

[x] CESG Good Practice Guide No. 10, Remote Working, (UK RESTRICTED) – latest issue available from the CESG website.

[y] CESG Good Practice Guide No. 12, Use of Virtualisation Products for Data Separation – Managing the Security Risks (Not Protectively Marked) – latest issue available from the CESG website.

[z] CESG Good Practice Guide No. 9, Taking Account of the Aggregation of Information, (Not Protectively Marked) - latest issue available from the CESG website.

[aa] CESG IA Top Tips 2013/01, Managing the Risks from Desktop KVM Switches, issued 15 January 2013 (Not Protectively Marked). Available from the CESG website.

Glossary

AH	Application Hosting
BCF	Business Change Framework
CAPS	(CESG) Assisted Products Service
CCSMM	CESG Cyber Security Maturity Model (Also known as the CIAMM)
CHECK	(CESG) IT Health Check Service
CIAMM	CESG IA Maturity Model (Also known as the CCSMM)
CIO	Chief Information Officer
CLAS	CESG Listed Advisers Scheme
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
CPA	Commercial Product Assurance
CPNI	Centre for the Protection of National Infrastructure
CSF	Critical Success Factor
CTO	Chief Technology Officer
DSO	Departmental Security Officer
EA	Enterprise Architecture
EDRM	Electronic Digital Records Management
EEA	European Economic Area
ESA	Enterprise Security Architecture
GPG	Good Practice Guide
HMG	Her Majesty's Government
HR	Human Resources
IA	Information Assurance
IAO	Information Asset Owner
IAU	Internal Audit Unit
IR	Information Risk
IS	Information System
ISMS	Information Security Management System
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSO	Information Technology Security Officer
ITT	Invitation to Tender
KIM	Knowledge & Information Management
KVM	Keyboard, Video and Mouse
MSP	Managing Successful Programmes
OGC	Office of Government Commerce (This no longer exists, as it was moved to the Cabinet office)

PMO	Programme Management Office
SeCURE	Security Culture Review and Evaluation tool (produced by CPNI)
SIRO	Senior Information Risk Owner
SRMO	Security Risk Management Overview
TCO	Total Cost of Ownership

CESG provides advice and assistance on information security in support of UK Government. Unless otherwise stated, all material published on this website has been produced by CESG and is considered general guidance only. It is not intended to cover all scenarios or to be tailored to particular organisations or individuals. It is not a substitute for seeking appropriate tailored advice.

CESG Enquiries
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Email: enquiries@cesg.gsi.gov.uk