October 2012
Issue No: 1.7

Good Practice Guide

Protective Monitoring for HMG ICT Systems

CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

Good Practice Guide No. 13

Protective Monitoring for HMG ICT Systems

Issue No: 1.7
October 2012

Document History

Version	Date	Comment
1.0	March 2009	First issue
1.1	October 2009	Improvement of table references
1.2		Never published
1.3 – 1.5	October 2009; April 2010; August 2010	Minor typographical corrections and formatting updates
1.6	September 2012	Updated to reflect changes in MR numbering, and to reflect the new IS1&2 documentation
1.7	October 2012	Inclusion of document history table and details of changes made

Protective Monitoring for ICT Systems

Intended Readership

Her Majesty's Government (HMG) Information Assurance (IA) practitioners can use this Good Practice Guide (GPG) directly in conjunction with the risk management methodology defined in HMG IA Standard No. 1 & 2 (Information Risk Management" and IS1 & 2 supplement (Technical Risk Assessment and Risk Treatment) (references [a] and [b]). It will help determine the appropriate levels of Protective Monitoring that should be applied to HMG Information and Communications Technology (ICT) Systems.

It is assumed that readers of this Guide have a full understanding of the concepts and methods provided in IS1 & 2 and the associated supplement Application of the guidance provided is closely linked to those methods.

Executive Summary

Protective Monitoring is a set of business processes, with essential support technology, that need to be put into place in order to oversee how ICT systems are used (or abused) and to assure user accountability for their use of ICT facilities.

Protective Monitoring provides a means of treating risks to HMG ICT systems. Even the simplest ICT systems often come with intrinsic facilities for recording logs and raising alerts.

However, if these are never referred to, they provide no value, and more importantly they will enable those who wish to misuse the ICT resources and valuable information assets they contain to continue to do so without fear of getting caught or being held to account. The confidentiality, integrity and availability of those systems can consequently be expected to suffer.

Equally, there is a tendency to believe that advanced technologies such as Intrusion Detection Systems (IDS) can be fitted and forgotten, and that these will provide an automated panacea with "zero administrative" overhead and flawless protection.

This Guide demonstrates how the provision of an effective framework of Protective Monitoring of HMG ICT systems is an essential contribution to the treatment of information security risks.

With it arises inevitable investment that needs to be made in respect of the supporting infrastructure and technology, but most importantly the correct resourcing of the deployed solutions in terms of manpower, expertise, information assurance and defined levels of service such that there can be confidence in an return on investment and the effectiveness of the solution.

Aims and Purpose

The aim of this Guide is to provide advice on good practice that can help to meet the Protective Monitoring obligations, which are already laid down in national IA policy (e.g. such as are defined in the Security Policy Framework (SPF) (reference [c]) and HMG IA Standard No. 1 & 2 supplement (reference [b]).

Another aim of this Guide is to provide assistance in identifying the information that needs to be recorded, events reported and alerts generated in response to anticipated modes of attack of HMG ICT systems. For this aim the focus is on the Compromise Methods defined in the supplement to IS1 & 2. These are listed in Table 1 of the IS1 & 2 supplement..

The purpose of this Guide includes the following objectives:

a. Definition of Protective Monitoring, related concepts and the context in which it is applied;

b. Understanding of the business need for Protective Monitoring within HMG ICT Systems;

c. Defining a set of Protective Monitoring Controls as an aid to the treatment of risks (i.e. providing explicit cross-reference to the concepts and outcomes of the IS1 & 2 supplement risk treatment method);

d. Giving recommendations for application of the guidance to both new and legacy systems, including provision of migration paths from those systems designed to comply with the CESG Infosec Memorandum No. 22, Protective Monitoring (reference [d]), that this GPG supersedes;

e. Detailing the recommended business processes and resources that are required to support Protective Monitoring and integrate it within an SPF (reference [c]) compliant regime;

f. Providing an overview of the types of services, tools and technologies that can be incorporated within Protective Monitoring solutions.

This Guide does not endorse the adoption of any particular proprietary products or services, with the possible exception of those already forming part of the CESG IACS portfolio.

Organisations are reminded that it is important that any particular Protective Monitoring product or service should be the subject of some form of independent assurance plus extensive acceptance testing by the business and not rely upon vendor IA claims alone.

Protective Monitoring services implement important IA functions and the level of assurance for these should be at least as stringent as for the system the services are protecting.

Changes from the Previous Issue

Updates the MR numbering to keep it in line with the new issue of SPF from Cabinet office and updates policy reference (primarily to IS1 & IS2) to reflect recent reorganisation of IA policy documentation. Includes document history table.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Contents:

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 1 - Introduction

Key Principles

- Protective Monitoring provides essential oversight of ICT systems
- A realistic approach should be adopted with a full understanding of the business case for the implementation of Protective Monitoring
- Organisations should adopt a common set of principles in the adoption of Protective Monitoring
- This Guide should be used to support IA Standard No. 1 & 2 risk management by the application of Protective Monitoring to ICT systems

Overview

1. Protective Monitoring is a set of business processes, with essential support technology, that need to be put into place in order to oversee how ICT systems are used (or abused) and to assure user accountability for their use of ICT facilities. Within the scope of this Guide Protective Monitoring activities are limited to those associated with information provided by information security controls of ICT systems (e.g. inspecting firewall logs, investigating operating system security alerts and monitoring an IDS). Protective Monitoring includes putting into place mechanisms for collecting ICT log information and configuring ICT logs in order to provide an audit trail of security relevant events of interest.

Principles

2. Organisations should have a common set of principles in their approach to Protective Monitoring of ICT:

   a. **Strategy** : Adopt an organisation-wide strategic approach;

   b. **Policy** : Identify the specifics of how requirements will be delivered to each project;

   c. **Value** : Recognise and promote the value and benefits brought to the business;

   d. **Provide** : Furnish the infrastructure needed to support requirements;

   e. **Resource** : Ensure skilled and trained resources are in a position to operate the infrastructure;

   f. **Document** : Provide adequate documentation of the associated business processes;

   g. **Review** : Ensure that the processes are performing to requirements.

Benefits

3. There are good business reasons for adopting a thorough approach to Protective Monitoring of ICT:

   a. **Compliance** : Ensuring ICT systems are operated within the requirements of applicable policies, legislation and regulations, and to deter and detect any unlawful activity;

   b. **Risk Management** : Providing an essential contribution to the mitigation of risks to the confidentiality, integrity and availability of information assets processed by ICT systems. They also help to ensure other controls are operating effectively;

   c. **Reporting and Continuous Improvement** : Contributing to the mandatory reporting elements of the Security Policy Framework (SPF: reference [c]) and providing a rich source of information to feed into IA reviews of ICT systems as part of the "Plan ⇒ Do ⇒ Check ⇒ Act" (P-D-C-A) cycle of continuous improvement, as mandated by HMG IA Standard No. 1 & 2 supplement (IS1 & 2 supplement: reference [b]);

   d. **Situational Awareness** : Ensuring that system owners are provided with a real-time feed of information regarding the status of ICT systems and providing awareness of activities of the threat sources and enabling security incidents to be detected, investigated and effectively remediated;

   e. **Enabling Accountability** : Ensuring that ICT is used within the parameters that the business defines and is not used for wasteful or unlawful purposes, or in a manner that diverts users from their true job function;

   f. **Network Defence** : Working with other security controls to provide a complete "defence in depth" approach and facilitate automated responses to threats to ICT.

Costs

4. Delivery of Protective Monitoring does represent a substantial investment by the business. There are a number of factors that contribute to related costs:

   a. **Technology** : Direct costs of hardware, software and related support services needed to deliver Protective Monitoring solutions;

   b. **Storage** : Provision of substantial online storage and archive capacity to handle the data accumulated by Protective Monitoring;

   c. **Oversight** : Staffing of functions that oversee audit activities that are independent of ICT management;

d. **Audits** : The costs and any consequent diversion of effort required to undertake the audit activities;

e. **Monitoring** : Staffing of monitoring positions to the correct level of service (for some projects this may need to be on a 24x7 basis);

f. **Incidents** : Provision of staff and other resources to undertake security incident investigations and other follow-up exercises;

g. **Review** : Provision of a management function to regularly review the performance of Protective Monitoring and incident management functions.

5. However, by balancing these against the benefits, it can be seen that there will be a positive business case for implementation.

Method

6. The approach adopted by this Guide is directly related to the HMG risk management standard: IA Standard No. 1 & 2 (IS1 & 2: references [a] and [b]).

Aim

7. This Good Practice Guide (GPG) provides recommended practice for the use of Protective Monitoring methods as means to contribute to risk treatment on Information and Communications Technology (ICT) Systems by organisations subject to HM Government Security Policy as laid down in the Security Policy Framework (SPF) (reference [c]).

Relationship to Policy

8. This Guide supports national IA policy. It provides advice on good practice that can help to meet the Protective Monitoring obligations, which are already laid down in national IA policy (e.g. such as are defined in the SPF).

9. Use of the **MUST** imperative within this Guide will always be accompanied by a reference to the IA policy direction to which such a clause relates. In general, advice and guidelines are introduced by the **should** imperative, which means that it is recommended that they are implemented, but that each organisation may select alternative approaches, according to their exact needs.

10. In using this Guide organisations should document their reasons for choosing alternatives, in order to provide evidence that can be later provided as justification for such decisions. This Guide is consistent with the relevant requirements and controls set out in ISO/IEC 27001 (reference [e]) and ISO/IEC 27002 (reference [f]) standards relating to Information Security Management requirements.

Recommendations

11. It is recommended that all IA practitioners use this Guide in order to include Protective Monitoring processes as part of a suite of information protection measures for HMG ICT systems, as an extension of the HMG IA Standard No. 1 & 2 supplement (IS1 & 2 supplement reference [b]) risk treatment method. There will be a level of detail required in organisational practices that inevitably cannot be accommodated in this generic guidance. Thus this Guide should be used to inform the development of specific organisational policies and practices.

Supersession

12. This Guide supersedes previous policy and guidance published in CESG IA Memorandum No. 22, Protective Monitoring (IM22) (reference [d]) and CESG Infosec Memorandum No. 37, Intrusion Detection of Managed IT Systems (IM37) (reference [g]). IM22 and IM37 should now be regarded as withdrawn and should no longer be used. Alternative and updated advice to that provided by both IM22 and IM37 are incorporated within this Guide.

Adoption

13. Systems should now be being migrating to compliance with the SPF and, specifically, Issue 4 of HMG IA Standard No. 1 & 2 and the associated supplement (IS1 & 2) (references [a] and [b]). As IS1 & 2 is adopted during this process of migration, the recommendations in this Guide should be considered for the purpose of defining Protective Monitoring requirements. Following this guidance can assist in attaining compliance relating to the implementation of some parts of IS1 & 2:

    a. Controls contained within Baseline Control Set, especially those that are related to collection of system audit logs and system monitoring;

    b. The Audit and Monitoring high level principle of the Segmentation Model.

Structure

14. The remainder of this Guide is provided as a series of structured Chapters and Appendices:

    a. **Chapter 2 - Business Drivers**. Covers the related business drivers and reasons for implementation of Protective Monitoring. As well as providing the background to Protective Monitoring requirements it is also provides the starting points from which a business case for Protective Monitoring can be defined;

b. **Chapter 3 - Key Concepts**. Which is in addition to the Glossary at the end of the Guide, but provides early introduction to the key concepts that relate to Protective Monitoring;

c. **Chapter 4 - Method**. Defines the Protective Monitoring levels and provides recommendations on to how these can be applied during the technical risk treatment phase, by direct reference to concepts introduced in IS1 & 2 supplement (reference [b]). It also includes other recommendations on important Protective Monitoring parameters including responsiveness and retention;

d. **Chapter 5 - People and Processes**. Includes the necessary resources and business processes that need to be put in to place. It also considers issues regarding insourcing or outsourcing aspects of Protective Monitoring;

e. **Appendix A - Protective Monitoring Controls and Baseline Requirements**. Demonstrates the risk management approach adopted by this Guide, introduces the recommended Protective Monitoring Controls and presents tables of baseline Protective Monitoring control specifications;

f. **Appendix B - Detailed Definition of Protective Monitoring Controls**. This includes detailed specification of each Protective Monitoring Control. For each Protective Monitoring Control it includes narrative description, Segmentation Model recommendations, Recordable Events recommendations plus any other additional factors and notes relevant to the treatment implementation;

g. **Appendix C - Accounting Items**. Provides a catalogue of Accounting Items that are included in the output definitions in Appendix B (in **bold**). This also includes possible infrastructure or solution sources for those items that come together to form the Accounting data recorded for a system;

h. **Appendix D - Technology and Assurance Overview**. Provides a primer in regard of the currently available technology based solutions that can support or form part of an Protective Monitoring solution. It also covers integration of these tools into an overall security architecture and related approaches to solution assurance.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 2 - Business Drivers

Key Principles

- Business drivers for Protective Monitoring include all of the following
  - Facilitating compliance with legislation, regulations, policy and standards;
  - Providing an essential component in the risk management approach and allowing increased Protective Monitoring levels to make up for lack of controls elsewhere;
  - Providing information to contribute to mandated SPF (reference [c]) reports and also providing information on the performance of security controls to support continuous improvement;
  - Enhancing situational awareness and increasing understanding of threats and risks;
  - Ensuring accountability of the use of ICT and its use is consistent with business needs;
  - Incorporating network defence capability into ICT.
- These drivers can be referred to during development of business cases for new ICT systems that need to take account of Protective Monitoring requirements

Introduction

15. This section provides details on the business drivers for Protective Monitoring and attempts to answer the questions: "Why do it?" and "What benefits does the business get by doing it?"

Benefits of Protective Monitoring

Compliance with Policy, Standards, Legislation and Regulations

16. It should be noted that the guidance provided in this section provides information to support the production of business cases. CESG recommends that organisations should seek legal advice in regard of compliance with legislation and regulations as part of development of IA Protective Monitoring policy both for the organisation as a whole and for any specific enterprise undertaken by the organisation. All HMG organisations face a combination of policy, standard, legislative and regulatory requirements which they must satisfy. Implementation of appropriate Protective Monitoring Controls with its intrinsic levels of recordkeeping and reporting can help in delivering these requirements by providing evidence of compliance. Protective Monitoring controls can assist in compliance in the following specific areas:

a. Compliance with mandated HMG ICT standards, including:

- HMG Security Policy Framework (SPF) (reference [c]) - Audit is an important part of the mandatory requirements of the SPF, included in Mandatory Requirement 2 (MR2) to contribute to mandatory reporting requirements, MR5 in order to facilitate oversight and compliance requirements, MR8 to support mandated compliance checking and forensic readiness, and MR10 to allow auditing of user accounts. Protective Monitoring is also an essential complimentary requirement to police the effectiveness of technical controls required by MR9 and support incident reporting in MR12 (citations of SPF MRs are provided below);

> MANDATORY REQUIREMENT 2
> Departments and Agencies must:
> * Adopt a holistic risk management approach covering all areas of protective security across their organisation.
> * Develop their own security policies, tailoring the standards and guidelines set out in this framework to the particular business needs, threat profile and risk appetite of their organisation and its delivery partners.

> MANDATORY REQUIREMENT 5
> Departments and Agencies must have an effective system of assurance in place to satisfy their Accounting Officer / Head of Department and Management Board that the organisation"s security arrangements are fit for purpose, that information risks are appropriately managed, and that any significant control weaknesses are explicitly acknowledged and regularly reviewed.

> MANDATORY REQUIREMENT 8 (MR8)
> Departments and Agencies **MUST** comply with oversight arrangements including external audit / compliance arrangements as set out by Cabinet Office.

> MANDATORY REQUIREMENT 9
> Departments and Agencies must put in place an appropriate range of technical controls for all ICT systems, proportionate to the value, importance and sensitivity of the information held and the requirements of any interconnected systems.

> MANDATORY REQUIREMENT 10
> Departments and Agencies must implement appropriate procedural controls for all ICT (or paper-based) systems or services to prevent unauthorised access and modification, or misuse by authorised users.

> MANDATORY REQUIREMENT 12
> Departments and Agencies must have clear policies and processes for reporting, managing and resolving Information Security Breaches and ICT security incidents.

- HMG Information Security Standard No. 6 - Protecting Personal Data and Managing Information Risk (reference [h]) - these requirements, published as a result of the 2008 Data Handling Review, are quite explicit on the need for monitoring of access to protected personal information within HMG Departments (citation following);

All Departments **MUST**:

a). Put in place arrangements to log activity of data users in respect of electronically-held protected personal information, and for managers to check it is being properly conducted, with a particular focus on those working remotely and those with higher levels of functionality. Summary records of manager's activity **MUST** be shared with the relevant IAO and be available for inspection by the Information Commissioner's Office on request;

b). Have a forensic readiness policy to maximise their ability to preserve, analyse and use evidence from an ICT system, should it be required.

- ISO27001 Compliance (reference [e]) - if the organisation is intending, formally or informally, to comply with ISO27001 then the controls in this Guide directly satisfy the group of all 6 controls under A.10.10 (Monitoring) and A.15.3 (Information systems audit considerations).

b. Compliance with legislation and regulations - all organisations must be able to operate within the law, including all of the following:

- Official Secrets Act 1911 to 1989 (OSA);
- Human Rights Act 1998 (HRA);
- Freedom of Information Act 2000 (FoIA);
- Data Protection Act 1998 (DPA);
- Computer Misuse Act 1990 (CMA);
- Regulation of Investigatory Powers Act 2000 (RIPA);
- Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000 (LBPR).

The correct implementation of Protective Monitoring controls help to ensure organisations can comply with these laws.

c. Protective Monitoring is associated with the collection of evidence requirement which has to be to a high standard and may benefit from adherence with specific legislation and guidelines such as:

- Civil Evidence Act 1995 (CEA);
- Police and Criminal Evidence Act 1994 (PACE) and Serious Organised Crime and Police Act 2004 (SOCA);
- CPNI Technical Note 01/2005 - Introduction to Forensic Readiness Planning (reference [i]);
- BS 10008:2008 Evidential weight and legal admissibility - Specification (reference [j]);
- ACPO Good Practice Guide for Computer based Electronic Evidence (reference [k]).

Risk Management

17. The Protective Monitoring processes are integrated with the IA risk management processes. This means including Protective Monitoring within the IS1 & 2 lifecycle (reference [a]) and IS1 & 2 supplement (reference [b]). Doing so ensures that Protective Monitoring controls are optimised for the project under consideration: neither too much nor too little. By application of the Segmentation Model the focus of Protective Monitoring activities will be the areas of highest risk. A risk management approach also allows increased levels of Protective Monitoring to be applied in cases where there is lack of available controls in other areas (e.g. access control).

Reporting and Continuous Improvement

18. SPF MR6 (cited after paragraph 16.) requires that Departments provide annual reports on all aspects of compliance with policy. The information provided by Protective Monitoring processes will provide vital evidence that can contribute to these reports.

19. The information gained from Protective Monitoring activities can also support the "Plan ⇒ Do ⇒ Check ⇒ Act" (P-D-C-A) cycle of continuous improvement mandated by HMG IA Standard No. 1 & 2 supplement (reference [b]). This includes:

    a. Providing information on information security incidents related caused by lack of controls which, can be remedied during reviews;

    b. Monitoring the improvements made by the introduction of additional controls, which should demonstrate effective detection and prevention of incidents;

    c. Providing evidence of improvement in compliance with information security policy and increasing IA maturity in regard of both system operation and user behaviour.

Situational Awareness

20. Protective Monitoring can provide a rich source of business intelligence. Threat trend and pattern analysis can be linked to reports from other quarters (e.g. CPNI) to allow predictions that inform risk management, allowing resources to be focussed where the risks are most likely to be realised. Situational awareness is of strategic importance to organisations that need to manage and accept risk. Organisations can be made aware of:

    a. Awareness of any attacks in as near to real-time as possible and sufficient information on those attacks to allow them to be pinpointed and responded to;

b. Who the real threats are to the specific organisation;

c. What vulnerabilities they are exploiting, now and in the past;

d. Where they are likely to arise in future;

e. How they can be defeated, not just on a case-by-case basis, but systematically.

Enabling Accountability

21. Protective Monitoring facilities assist in making users accountable for their use of ICT systems. This can help not just to enforce information security policy but also to ensure that organisations ICT facilities are used for appropriate business purposes. This can provide direct cost savings by ensuring that the users of ICT are engaged in using those facilities for permitted purposes and are not using them wastefully or in a manner that diverts users away from their true business role.

Network Defence

22. Business cases should make it clear that no one element of a network defence control will be a "magic bullet" that can automatically defeat all attacks. Protective Monitoring can support network defences and measure the effectiveness of network defence controls. All network defences need an Protective Monitoring element:

    a. Each defence should report attacks, which implies some form of logging and auditing;

    b. Defences may raise real-time alerts, these need to be integrated with the monitoring infrastructure;

    c. Defences may have other associated issues (e.g. compliance with regulations and retention periods), these need to be considered and solutions developed that are consistent with IA Protective Monitoring policy;

    d. Defences may support both automated and manual responses. Even with automation oversight is required and manual responses need to be incorporated within Protective Monitoring processes;

    e. With any automated response there is a need for a contingency mode in which those responses are suspended or withdrawn should these automatic responses prove inappropriate.

23. The business cases for network defence and Protective Monitoring become linked. Protective Monitoring supports network defences and network defences can provide metrics that support Protective Monitoring activities.

Costs of Protective Monitoring

24. Having a realistic knowledge of the total costs of implementation of Protective Monitoring is another important input into the business case. Whereas there is some scope for error in predicting benefits, the implications of a flawed cost model are either that it is over-funded, or worse, under-funded. The following is a list of cost factors that need to be considered in implementing Protective Monitoring for ICT systems:

    a. It is essential to support Protective Monitoring with technology that can automate some of the stages of the associated business processes (e.g. Event Log Analysers, Security Information and Event Management (SIEM) suites, Network Behaviour Analysis (NBA), Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS), etc.[1]). Effective technology solutions will have direct costs relating to both procurement and maintenance;

    b. Audit logs provide a significant amount of data to be recorded by the system. That data may be required to be accumulated and retained for long periods. This can have direct bearing on system costs in terms of both on-line and off-line storage requirements;

    c. To be effective, implementation of an ICT audit function needs to reflect the same independence as would be present in a financial audit. This can increase the manpower resources needed to support audit functions by the need of introduction of role separation and segregation of duties;

    d. Audits need to be conducted regularly (with the period and intensity of audits dictated by risk management). These have a direct cost not just in terms of the resources required for the audit itself, but also in terms of diversion of effort and potential increase in system load during audits. Management also need to invest time in considering reports;

    e. Monitoring requirements imply a need for continuous resourcing. This has a direct cost and needs to be adequately resourced by skilled personnel who are able to make judgements regarding "false positives" and "false negatives". Whether insourced or outsourced formal SLAs will need to be defined;

    f. Adverse audit findings and alerts need to be an input into the information security incident management process. The responses to incidents may necessitate further diversion of business resources and have implications on the continued use of the system within which the incidents are detected.

[1] All of these Protective Monitoring related technologies are discussed further in Appendix D.

25. Spreading the cost across the business to serve several ICT projects can also strengthen the business case for Protective Monitoring. Implementation of centralised approaches can be more efficient that project based point solutions. Naturally such approaches introduce further technical challenges resulting from aggregation of information and the maintenance of assured separation of the feeding systems.

Conclusion

26. Although Protective Monitoring of ICT systems comes at a significant price there are many factors that can contribute to a positive argument for its inclusion in the overall business case for projects. These can be combined into an overall argument including other factors to provide a complete business case:

    a. A summary of the value proposition offered by the balance of the costs and benefits;

    b. Demonstration of alignment with overall business strategic aims and objectives;

    c. Specific business opportunities introduced by the adoption of an Protective Monitoring solution;

    d. Functional, non-functional and resource requirements related to Protective Monitoring;

    e. Whole-life "total cost of ownership" and funding profile;

    f. Detailed project plan for implementation.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 3 - Key Concepts

Key Principles

- Protective Monitoring should:
  - Be conducted within an organisation-wide framework of seven general principles;
  - Include development of related policy for each ICT system;
  - Be implemented as a series of fully supported business processes for accounting, audit and monitoring.

Scope

27. Within the scope of this Guide Protective Monitoring, which comprises accounting, audit and monitoring elements, covers those activities associated with information provided by information security controls of ICT systems (e.g. inspecting firewall logs, investigating operating system security alerts and monitoring an IDS).

General Principles

28. CESG recommends that organisations have a common set of generally agreed principles to the implementation of Protective Monitoring systems. These principles should include:

    a. Adopt an organisation-wide Protective Monitoring strategy that defines a consistent approach and common goals;

    b. Include definition of project or system based Protective Monitoring policies that are tailored to specific requirements;

    c. Recognition of the value and benefits that Protective Monitoring brings to the business;

    d. Provision of adequate infrastructure to support Protective Monitoring requirements within the business;

    e. Adequately resourcing Protective Monitoring roles and ensuring these have adequate training and skills;

    f. Documenting and operating the business processes necessary to undertake Protective Monitoring responsibilities;

    g. Regularly reviewing the performance for Protective Monitoring business processes and embedding these within a culture of continuous improvement.

Protective Monitoring Policy

29. CESG further recommends that a Protective Monitoring Policy should be developed for each ICT system as an integral part of the Risk Management and Accreditation Document Set (RMADS) that needs to be prepared in accordance with HMG IA Standard No. 1 & 2 and associated Supplement (IS1 & 2) (reference [a] and [b]) as part of the accreditation process.

30. It is also important that the information gathered for Protective Monitoring purposes is used for correct and lawful purposes and not abused. Monitoring of user activities is subject to legal requirements that need to be observed and the information generated, especially in raw form, will include personal data that needs to be correctly protected and handled. It is for these reasons that the nature of Protective Monitoring systems to be implemented, their configuration, their correct use and the supporting business processes with associated management roles, responsibilities and procedures are all formalised into a Protective Monitoring Policy. The policy should establish:

    a. What is being audited and monitored, in terms of:

        - Usage scenarios of the project under consideration - what users are allowed to do and which actions need to be accounted for;
        - Exceptions and how they will be detected - what users are not allowed to do or what would constitute suspicious activity;
        - The complexity in terms of the different types of connectivity to support these interactions (e.g. air-gapped systems, electronic exchanges, remote access, wireless, Internet services, etc.).

    b. What information will be collected to support the accounting, audit and monitoring of these activities (this can be determined by application of the method given in Chapter 4);

    c. How the information gathered will be used (including both a list of permitted purposes and a list of prohibited purposes);

    d. Who will access it and their associated responsibilities;

    e. How the information will be protected, stored, retained and disposed of;

    f. How notification of monitoring is achieved and how user consent is obtained, or otherwise.

31. Development of the policy, either at the organisation or project level should be the first step for defining the Protective Monitoring requirements for any enterprise.

Protective Monitoring processes

32. Protective Monitoring comprises three core processes: Accounting, Auditing and Monitoring, each of which is defined separately, combine to provide the whole process of recording information, subsequently analysing it and comparing it to an accepted security policy, and corrective actions that may follow.

33. It also comprises two further subsidiary processes: Management Reporting which provides feedback on the performance of Protective Monitoring status to senior management and supports improvement reviews and Retention and Archive which will maintain the accounting database.

34. This breaks down into the components shown in Figure 1 on page 24. This also corresponds with the "Plan ⇒ Do ⇒ Check ⇒ Act" (P-D-C-A) cycle that is empirical to ISO27001 (reference [e]). For Protective Monitoring this cycle operates at several levels:

    a. Long term reporting cycle over which trends are analysed and overall policy direction reviewed (e.g. the re-accreditation cycle);

    b. Operational audit cycle for which compliance is measured at frequent intervals;

    c. Regular monitoring of accounting output to detect potential security breaches;

    d. Real-time incident response in the event of significant alerts or security breaches.

35. Although this Guide contains information on the technology that may support Protective Monitoring. All of these should be regarded as full business processes. None of these processes can be fully automated.

Accounting

36. Defined as: the process of collecting and recording information about events.

Audit

37. Defined as: the systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.

Monitoring

38. Defined as: the provision of a business process that provides the necessary resources to pro-actively monitor a system for information security incidents.

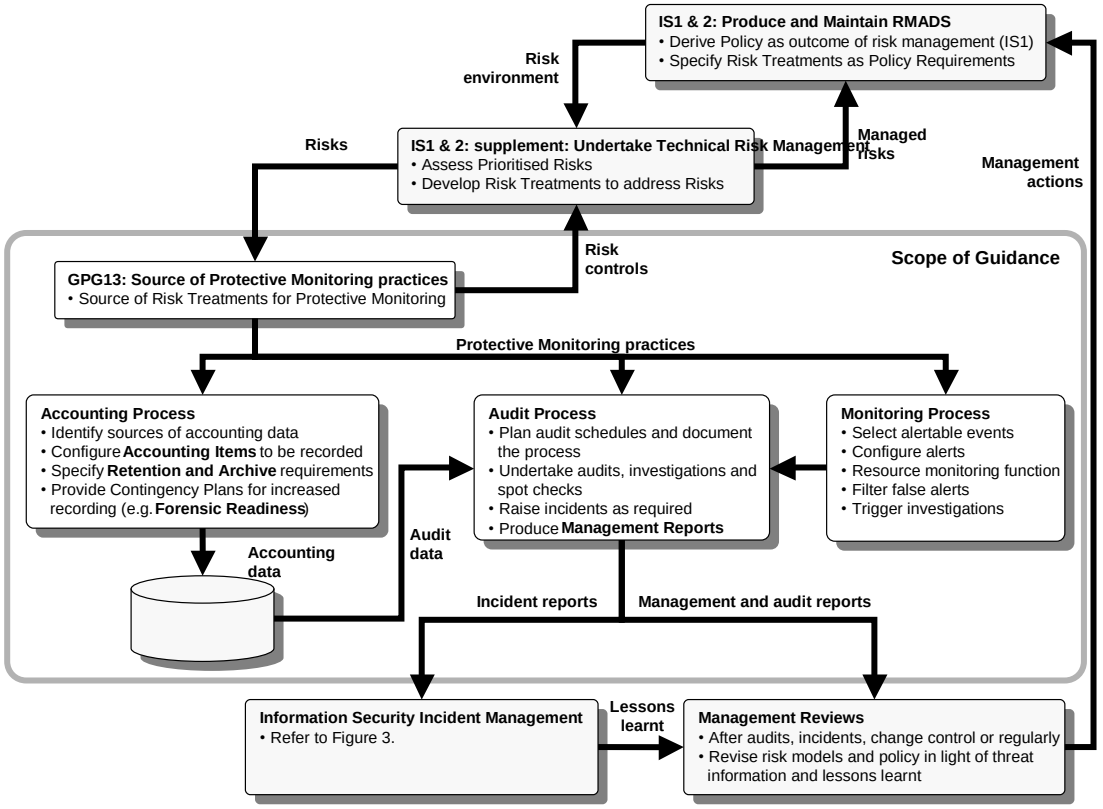

Figure 1 – Protective Monitoring Business Processes

Retention

39. Defined as: ensuring that accounting information is retained only for as long as it is required and that is it disposed of securely after it is no longer required.

Archive

40. Defined as: providing either long-term storage of accounting information or for the protection of the accounting information required for forensic purposes.

Management Reporting

41. Defined as: provision of sanitised and statistical high level reports from the accounting information that are directed at senior management.

Logs

42. Defined as: logs which record user activities, exceptions, and information security events, which are kept for an agreed period to assist in future investigations and access control monitoring.

43. Logs may also be referred to as Audit Logs or Event Logs.

Alerts

44. Defined as: messages raised by a business process that indicates the high probability of an information security incident requiring investigation.

45. There are two significant concepts associated with alerts:

    a. **False Positive** - defined as a situation in which an alert is raised that is then found **not** to indicate an information security incident;

    b. **False Negative** - defined as a situation in which there is an information security incident that fails to raise an expected alert indication.

Protective Monitoring Controls

46. Defined as: Controls that are specific to the implementation of Protective Monitoring on an ICT system.

47. These are associated with application in combination with other ISO27001 controls to the treatment of risks associated with one or more Compromise Methods (as defined by Chapter 3 of IS1 & 2). Further definition of controls is given in Appendix A of the IS1 & 2 supplement.

Accounting Items

48. Defined as: discrete items of information that are recorded as part accounting on ICT systems.

49. Accounting Items recommended to be collected for specific Recordable Events are defined on the back sheets of each Protective Monitoring Control definition provided in Appendix B. Accounting Items are further catalogued and defined in Appendix C.

Recordable Events

50. Defined as: a subset of events that can be recorded as part of a Recording Profile and that implies the need to record a set of Accounting Items as part of the accounting process.

51. Recordable Events are described in terms of the IA relevant event that needs to be recorded and are specified in template against which actual event records can be compared. Recordable Events for each of the Protective Monitoring Controls are defined on the back sheets of each definition provided in Appendix B.

Recording Profiles

52. Defined as: sets of Recordable Events and Accounting Items that contribute to a specific level of protection.

53. Within this Guide these are expressed in the shorthand form as **A**, **B**, **C** or **D** and generally correspond to the levels of protection required for the four different segments of the IS1 & 2 Supplement Segmentation Model. Further information regarding Recording Profiles is provided in Appendix B paragraphs 5 through to 7.

Chapter 4 - Method

Key Principles

- The Protective Monitoring Controls (PMCs) identified in this Guide should be adopted to assist in defining what needs to be recorded as part of the IS1 & 2 risk management process
- Protective Monitoring solutions should be documented in the IS1 & 2 Security Case included within ICT systems RMADS documentation

Protective Monitoring Controls

54. This guide introduces generic Protective Monitoring Controls (PMCs) that are focussed on protection against attacks made via the various Compromise Methods defined in IS1 & 2 (reference [b][b]). This relationship is illustrated in Table A-2 in Appendix A. Practitioners should interpret the precise application of the PMCs within the context of their project. There are twelve PMCs defined which provide complete coverage of all technical compromise methods which any system may be vulnerable to. These are summarised in Table 1 on page 29 and each is fully defined in Appendix B.

Relationship to IA Standard No. 1&2 (IS1&2)

55. Appendix A of this Guide provides advice on application of the PMCs to the Baseline Control Set defined in IS1 & 2 supplement, Appendix A (reference [b]). Appendix B provides further detail on each PMC and how each can be applied for the different levels of the Segmentation Model. Practitioners should refer to these as an aid to selection of appropriate controls for treating risks. Application of this Guide in these cases is precisely in alignment with the STEPs of IS1 & 2 supplement as demonstrated in Figure 2 on page 28. To summarise the method given in the Figure:

    a. When implementing the Baseline Control Set the guidance in Table A-3 of Appendix A of this Guide can be referred to in order to supplement the advice already provided in IS1 & 2 supplement ;

    b. For each Risk that is treated via the Segmentation Model. That is, usually those in the **Detect & Resist** or **Defend** segments, or any other risks to which a fine grained approach is adopted:

    - The relevant Compromise Method for the Risk being analysed can be discovered by referring to the original IS1 & 2 supplement FORM 5 which defines that Risk;

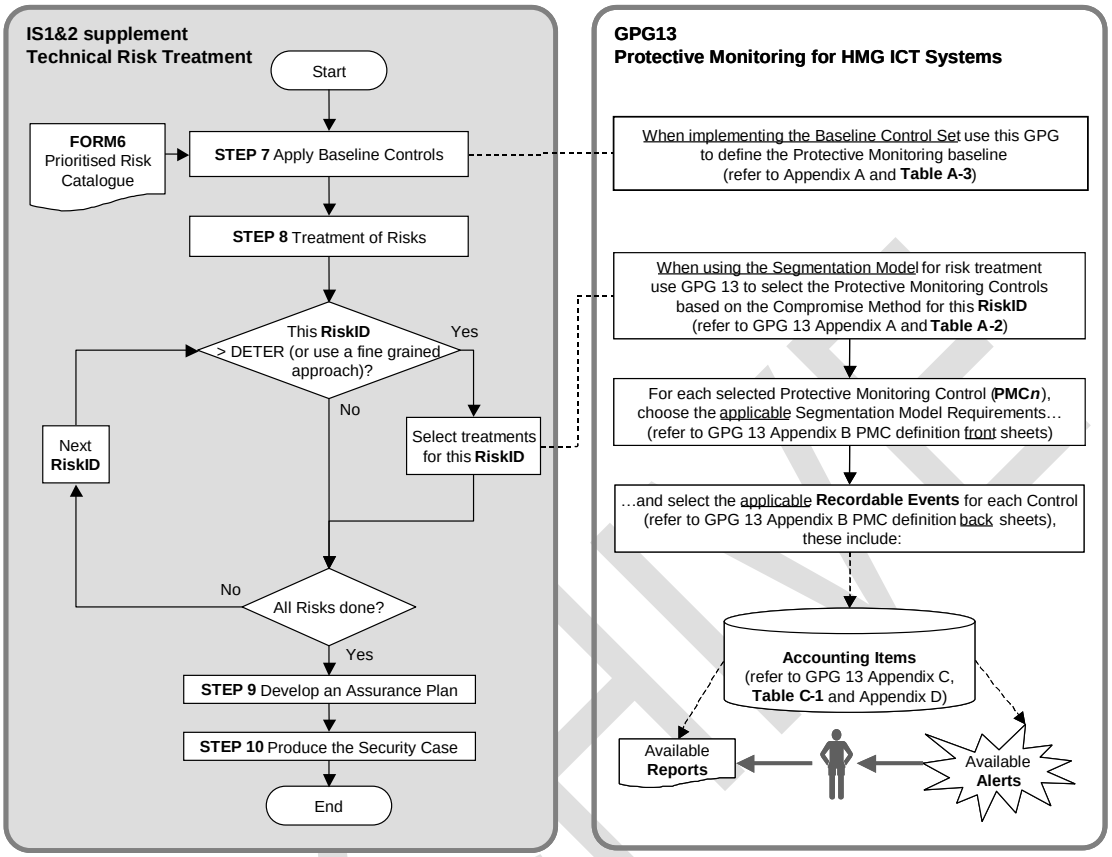

Figure 2 – Relationships Between the Protective Monitoring Method and IS1&2 Part 2

- The matrix Table A-2 in Appendix A of this Guide can be referred to read off the PMCs that are applicable to that Compromise Method;
- Providing it is judged that each PMC is relevant to the system under analysis then for each PMC the corresponding fact sheet in Appendix B can be referred to for further guidance;
- Depending on the Segment of the Segmentation Model for the Risk being considered, recommendations can be read directly from the table on the front of the fact sheet;
- These are supplemental recommendations that should be aggregated with the general Segmentation Model recommendations given in IS1 & 2 supplement (reference [b]);

Protective Monitoring Control		Objective
PMC1	Accurate time in logs.	To provide a means of providing accurate time in logs and synchronisation between system components with a view to facilitating collation of events between those components.
PMC2	Recording relating to business traffic crossing a boundary.	To provide reports, monitoring, recording and analysis of business traffic crossing a boundary with a view to ensuring traffic exchanges are authorised, conform to security policy, transport of malicious content is prevented and alerted, and that other forms of attack by manipulation of business traffic are detected or prevented.
PMC3	Recording relating to suspicious activity at a boundary.	To provide reports, monitoring, recording and analysis of network traffic crossing a boundary with a view to detecting suspect activity that would be indicative of the actions of an attacker attempting to breach an ICT system boundary or other deviation from normal business behaviour.
PMC4	Recording of workstation, server or device status.	To detect changes to device status and configuration. Changes may occur through accidental or deliberate acts by a user or by subversion of a device by malware (e.g. installation of trojan software or so called "rootkits"). It will also record indications that are typical of the behaviour of such events (including unexpected and repeated system restarts or addition of unidentified system processes).
PMC5	Recording relating to suspicious internal network activity.	To monitor critical internal boundaries and resources within internal networks to detect suspicious activity that may indicate attacks either by internal users or by external attackers who have penetrated the internal network.
PMC6	Recording relating to network connections.	To monitor temporary connections to the network either made by remote access, virtual private networking, wireless or any other transient means of network connection.
PMC7	Recording of session activity by user and workstation.	To monitor user activity and access to ensure they can be made accountable for their actions and to detect unauthorised activity and access that is either suspicious or is in violation of security policy requirements.
PMC8	Recording of data backup status.	To provide a means by which previous know working states of information assets can be identified and recovered from in the event that either their integrity or availability is compromised.
PMC9	Alerting critical events.	To allow critical classes of events to be notified in as close to real-time as is achievable.
PMC10	Reporting on the status of the audit system.	To support means by which the integrity status of the collected accounting data can be verified.
PMC11	Production of sanitised and statistical management reports.	To provide management feedback on the performance of the Protective Monitoring system in regard of audit, detection and investigation of information security incidents.
PMC12	Providing a legal framework for Protective Monitoring activities.	To ensure that all monitoring and interception of communications is conducted lawfully and that accounting data collected by the system is treated as a sensitive information asset in its own right.

Table 1 – Protective Monitoring Controls and Objectives

- The recommendations may also refer to a specific profile **Recordable Events** (with Recording Profiles **A**, **B**, **C** or **D**) which can be read from the table on the back of the fact sheet;
- The table on the back of the fact sheet also identifies the applicable **Accounting Items** associated with the Recordable Events (more information regarding each of these is given in an Accounting Item catalogue provided in Appendix C).

c. The accumulation of all PMCs for all the treated risks defines both the nature of the accounting data capture recommendations, the types of report that are recommended to be provided and which events are recommended as needed to be alerted in near-real time. All of these can be documented in the Security Case of a project.

Applying controls based on applicability

56. Note that the PMCs need only be applied where they are applicable in the context of the project under consideration. In particular:

a. These guidelines do not preclude circumstances where no recording or monitoring takes place, but in such cases IS1 & 2 supplement (reference [b]) requires a justifying statement to be made in the Security Case;

b. Neither should Protective Monitoring Controls be applied in a blanket manner across the whole environment to which they are applied; this would lead to inappropriate direction of monitoring resources, which is likely to be both uneconomic and ineffective. Rather, apply the rules provided in the mapping between the IS1 & 2 Compromise Methods applicable at a given point in the solution and the Protective Monitoring Controls to determine which are appropriate (using the matrix given in Table A-2 in Appendix A as a guide to selection).

Selection of Accounting Items and other parameters

57. Once the PMCs have been selected then practitioners should define in detail the infrastructure needed to collect, store, use, retain and maintain the accounting data needed to support them. This Guide provides additional guidance in Appendices B, C and D in these areas. There are certain key parameters that need to be selected in accordance with the IA and business requirements of the project. These are discussed in the following paragraphs.

58. The PMC definitions in Appendix B include **Recordable Events** definitions that highlight **Accounting Items** in **bold** text. These are also further catalogued in Appendix C, which indicates the typical content to be recorded and the potential infrastructure sources. This table can be used to assist in selecting exactly what

is gathered and from where. Appendix C is also supported by Appendix D, which provides an overview of the current techniques and technologies that can be applied to construct technical Protective Monitoring solutions. These are approximate recommendations only. Each solution should be reviewed and common sense judgements applied in the context of the project and systems under consideration.

59. As well as these selections for Protective Monitoring requirements for a system, there are other requirements that need to be defined. These include:

    a. Audit periods;
    b. Retention periods;
    c. Accounting data capacity;
    d. Response times;
    e. Service levels.

Audit periods

60. The audit periods are key parameters that determine the degree of oversight provided by Protective Monitoring processes. Even in systems where there is a high degree of automation (e.g. IDS/IPS) there will be classes of attack that can only be detected by audit functions. These may be directly related to other factors in the risk assessment (e.g. maximum attacker capability level, worst case business impact level or risk level) or they may be driven by unique factors of their own:

    a. Real-time nature of the system being attacked;
    b. Criticality of the system varies over time (e.g. a system holding budget information);
    c. System has a defined pattern of use (e.g. it is only available during business hours);
    d. Degree of vulnerability of the system (e.g. it is connected to the Internet and is the subject of constant surveillance attacks).

    All of these factors should be considered when selecting the audit periods.

61. In complex systems there are also likely to be several layers of audit:

    a. Users can be empowered to audit certain aspects (e.g. report unauthorised log-in attempts or unexpected error messages);
    b. Local system managers may be devolved certain audit rights (e.g. user registration and access rights reviews);

c. Central audit functions will analyse collected logs on a continuous or periodic basis;

d. Systems should be subject of regular compliance reviews.

62. Organisations should develop an IA Protective Monitoring policy that takes into account all of these factors and that implements audit schedules that ensure systems are not left exposed to breaches that could be left undiscovered for undue periods of time.

63. Table 2 on page 33 provides typical parameter ranges that are aligned to the IS1 & 2 Supplement Segmentation Model segment (or Risk Levels) gathered from the outcome of the risk assessment (**Aware**, **Deter**, **Detect & Resist** or **Defend**). These can either be applied on a blanket "worst case" basis or targeted to provide increased protection for the assets most at risk. Each organisation should review their own business requirements when making these selections. Some organisations may have needs that vary greatly from the typical values given.

Retention periods

64. It is impossible to make universal recommendations regarding retention periods. These need to be defined as part of the risk management process for the system. Often retention requirements will be driven by organisation requirements and may be chosen to support business as opposed to information security requirements.

Segment (Risk Level)	Retention Period	Log Checks	Console Manning	Compliance Review Period
Aware (Medium)	Up to 3 months.	Logs reviewed at least once a month.	Console not always manned by alerts raised for critical conditions.	At least annually.
Deter (Medium-High)	Between 3 and 6 months.	Logs reviewed at least once a week.	Console manned during core business hours.	
Detect & Resist (High)	Between 6 and 12 months.	Logs reviewed at least once every working day.	Console always manned.	At least every six months.
Defend (Very High)	More than 12 months.	Logs reviewed at least once an hour.		At least quarterly.

Table 2 – Typical Audit Parameter Selection Criteria

65. The important factors that can yield sensible decisions regarding retention periods include:

    a. Legal advice on any time limits contained in driving legislation or regulations regarding record keeping, these can be primary drivers for specification of retention periods;

    b. Output available from incident and risk management business processes (for the same or similar systems) can be used to determine how long it takes, in the worst cases, to detect and investigate incidents. Retention periods can be set to some margin longer than this;

    c. As dictated by any community based information security policy to which the system under consideration must comply (e.g. the retention period for boundary logging for the GSI Code of Connection is currently 6 months);

    d. At the crudest level, use the ranges in Table 2 as a guide. These provide an increasing scale of retention related to the worst case Segment or Risk Level yielded by risk assessment.

66. It should be noted that the retention requirement does not always need to support all of the recorded data to be maintained in online form, information can be archived to offline storage. However, offline archive should provide the facility to be able to be restored or queried to support retrospective investigations. Depending on how audit management tasks are carried out, the retention requirement is most significant at the original collecting equipment (e.g. workstation or server) and the central management system. The end-to-end requirement shall apply to the latter: however there may be forensic

reasons for providing equivalent retention capacity at the point of origin as this may be required for analysis during computer forensic exercises.

67. As well as the overall retention requirement there may be extended requirements to deal with cases where securing electronic evidence is involved. In these cases the evidence will need to be forensically captured (which may involve taking some original equipment out of service) and this will need to be maintained for a potentially unlimited period while the cases go through the courts (refer also to forensic readiness requirements covered in Chapter 5 paragraphs 106. and 107.).

Accounting data capacity

68. Projects should consult with experts or systems integrators during the design phase regarding the requisite capacities of the actual technology to be deployed to ensure that adequate allowances are made for capacity throughout the project architecture to cater for:

    a. The retention requirements identified and the necessary storage capacity to support these at all points within the solution architecture;

    b. Consideration of the system not just under normal accounting information loads, but under significantly increased loads representing a sustained attack;

    c. Other aspects such as transient connections to the networks and re-synchronisation of log information (e.g. because of transient attachment of mobile devices).

Response times

69. The information security incident management business process will define response criteria for handling various classes of security breaches (with the more critical incidents requiring faster response). Exact requirements need to be defined on a case-by-case basis. Typical first response and investigation initiation times are provided in Table 3, on page 35, based on the Segmentation Model segment (or Risk Level) defined by IS1 & 2 supplement Targets are provided for "critical" incidents, which reflect the upper level of a prioritised schema for classification of incidents (which is part of good practice on information security incident management such as ISO18044 (reference [l])). It is up for individual organisations to make this distinction based upon their unique business environment. Projects should engage with staff, independent experts, service providers and systems integrators during the design phase to ensure that the solution delivered is technically capable of supporting the target response times in terms of end-to-end delivery of alerts. This is especially

important when Protective Monitoring activities are delegated across different organisations and sites, as is common on large distributed systems.

Service levels

70. Regardless if Protective Monitoring processes are insourced or outsourced it is important that formal Service Level Agreements (SLAs) are defined against which the performance of those processes can be measured and assured.

	Critical Incidents	
Segment (Risk Level)	**First Response**	**Investigation Initiated**
Aware (Medium)	Less than 1 day.	No guidance.
Deter (Medium-High)	Less than 4 hours.	Within 2 days.
Detect & Resist (High)	Less than 1 hour.	Within 1 day.
Defend (Very High)	Less than 30 minutes.	Within 4 hours.

Table 3 – Typical Guideline Incident Response targets

71. Targets should be established for each element of the performance of Protective Monitoring processes. Examples include:

    a. Time for an event to be processed and centrally recorded;

    b. Time for completion of initial analysis and the raising and communication of alerts;

    c. Schedule of auditing and reporting activities and definitions of report content;

    d. Time for investigation of security incidents and the securing of associated event data as evidence.

72. Wherever possible Protective Monitoring processes and outsourced services should be operating and provided in accordance with good practice on service management such as ISO 20000 (reference [m]) / IT Infrastructure Library (ITIL). Feedback on SLA performance is an essential part of the feedback loop that will enable reviews to determine if the processes are performing in accordance with business requirements and for identifying potential areas for improvement.

Contribution to the Security Case

73. It is important to include in the Security Case produced for a project (as required by IS1 & 2 supplement) all matters relating to the Protective Monitoring solution. The Security Case will be an integral part of the project Risk

Management and Accreditation Document Set (RMADS). The Security Case should include the following:

a. Justification of the selected levels of auditing and monitoring and any claims of applicability (or otherwise) within the Statement of Applicability;

b. Rationale for selection of the minimum level of Protective Monitoring within the context of the Baseline Control Set;

c. Identification of risks within the **Detect & Resist** and **Defend** segments, and any other risks, that are treated by a fine grained approach to Protective Monitoring;

d. How the Protective Monitoring will be established in practice, in terms of technology, resources and business processes;

e. Definition of other Protective Monitoring factors including audit periods, retention, forensic readiness, capacity requirements, response targets and service levels.

Constructing a Solution

74. Once a project has identified its approach to Protective Monitoring this can then be translated into a solution. To aid in the understanding of possible solutions, an overview of current techniques and technologies is given in Appendix D of this Guide. During design of a solution it is important to bear in mind the different aspects of the CESG Assurance Framework. Where Protective Monitoring is aided by technology based solutions, the Protective Monitoring infrastructure itself is an integral part of the project and, in accordance with IS1 & 2 supplement requirements (reference [b]), **MUST** be within the scope of project assurance activities. The assurance requirement for the Protective Monitoring solution will be at least that of the project being assured. In some cases, the impact levels for Confidentiality, Integrity or Availability may be raised for the Protective Monitoring system itself. For instance:

a. Confidentiality impact level may be raised due to concerns over aggregation present within the Protective Monitoring system itself, or

b. Availability and other impact levels may be higher for a Protective Monitoring system where it protects several systems (e.g. where it is located at the hub of a project that implements a “network of networks”, and its failure would have an adverse impact on all attached networks).

75. Therefore, in scenarios such as this and where technology based approaches to Protective Monitoring are adopted, then the IS1 & 2 method should be applied to the Protective Monitoring system itself, in order to ensure that risks to the Protective Monitoring system are identified and appropriately treated (i.e.

the Protective Monitoring system and the information it contains is treated as an information asset in its own right). The CESG Assurance Framework should be applied in order to provide Protective Monitoring as an assured service for the project concerned:

a. **Intrinsic** - delivery of Protective Monitoring services may be able to rely on positive trust properties of those services or the project environment (e.g. Protective Monitoring services are managed from a List-X facility). On the other hand, there may also be constraints reflecting a particular environment in which Protective Monitoring needs to be deployed (e.g. monitoring systems maintained by a third party under a legacy arrangement). In these latter cases then assurance needs to be compensated by other elements of the life-cycle;

b. **Extrinsic** - Protective Monitoring services may also be able to contribute evidence of independent verification of security claims (e.g. relevant ISO27001 certification or CCTM) or Protective Monitoring products may have been independently evaluated (e.g. ITSEC or Common Criteria);

c. **Implementation** - the Protective Monitoring services may be included within the scope of the project implementation assurance activities (e.g. CTAS or IT Health Check). For instance, accounting data produced by Protective Monitoring might be analysed following an IT Health Check to ensure testing produced an expected evidence trail and that alerting facilities were triggered as expected. For automated systems that are based on behaviour analysis or pattern learning, this should also include learning phases that allow the "business as usual" profiles to be acquired;

d. **Operation** - the Protective Monitoring services are appropriately resourced and integrated with business processes, are the subject of a constant cycle of review (“Plan ⇒ Do ⇒ Check ⇒ Act”) and may be updated in line with experience (e.g. improved in response to security incidents). For automated systems based on behaviour analysis or pattern learning, this should also include maintenance and fine-tuning of those patterns in line with business pattern variations, fluctuations and attack discovery. For automated signature based systems this should include signature updates in line with vendor recommendations or project requirements.

76. Appendix D also provides further information regarding the assurance of Protective Monitoring solutions. Chapter 5, following, provides an overview of the requirements for the people and business processes necessary to support a Protective Monitoring system.

Chapter 5 - People and Processes

Key Principles

- Relying solely on a purely automated system of monitoring is often insufficient and can provide a false sense of security
- People form a vital element for the overall solution to ensure that the technology performs correctly and that information security incidents are detected, appropriate remedial actions taken and lessons learnt
- It is essential that Protective Monitoring is conducted within a management framework that actively surveys and acts upon the outputs produced

Introduction

77. In implementing the technical Protective Monitoring Controls given in Chapter 4 and supporting Appendices to protect ICT systems substantial investment will already have been made in terms of hardware, software and storage. In order to use these it is important to put into place the business processes required to make use of the information generated. Even if the Protective Monitoring systems implemented include high degrees of automation, this should not be relied upon alone. All automated monitoring is fallible and will at times generate false output that needs to be ascertained. Indeed, it would be unwise to rely upon automated responses and defences (which are a feature of technology such as Intrusion Prevention Systems (IPS)) until the Protective Monitoring systems have been operated for sometime in manual mode and their behaviour is well understood. Simpler ICT systems may rely on minimal amounts of additional hardware and software dedicated to Protective Monitoring. They may even rely on log analysis of the system components alone.

78. In either case, the largest relative part of the investment in Protective Monitoring will be the people and other resources that are needed to manage it. Some systems may need job functions dedicated to oversight during office hours; others may need the services of a Managed Security Services Provider (MSSP) on a continuous 24x7 basis.

79. Without this investment Audit Logs would accumulate unseen and unmanaged (indeed, systems may even malfunction, as logs overflow the storage provided). Alerts would pass away unnoticed. There would apparently be no security breaches, as there is no one to notify them. But, in practice the confidentiality, integrity and availability of the information will most likely be being repeatedly and seriously compromised.

Governance and Ownership

80. The management framework put in place to implement Protective Monitoring should provide a "top down" approach. It will provide tandem responsibilities, specifically associated with Protective Monitoring, to those proposed by IS1 & 2. For larger systems it would be expected there may be dedicated posts or even a business unit or contracted organisation associated with the major part of Protective Monitoring delivery. It is important that when Protective Monitoring responsibilities bridge organisations then there are formal agreements in place to facilitate collaboration and information sharing. It should also be remembered, in common with other information ownership issues, that ultimate ownership and responsibility should always be retained within the client organisation. Systems that include data of higher protective markings or strong "need to know" requirements may need to implement "segregation of duties" to ensure that roles were potential conflicts of interest arise are separated in order to minimise abuse of related privileges.

Responsibilities

81. In the spirit of risk management and empowerment then every person associated with a system will have some degree of responsibility or interest associated with IA Protective Monitoring policy. It is essential that a culture with the correct degree of security awareness is promulgated throughout the organisation (and beyond) in order to facilitate this. This means that every person is fully briefed in regard to the risk environment and their individual responsibilities. Responsibilities for the various IA roles are summarised in Table 4, on page 42.

Insourcing vs Outsourcing

82. There are relative advantages and disadvantages of insourcing vs. outsourcing the management of all or part of monitoring services (summarised in Table 5 on page 43). Outsourcing is something that would not normally be considered for smaller organisations or projects or systems that are "air gapped" and managed by specially vetted staff. However, it can provide real advantages for medium to large organisations that have large corporate networks and many systems that need to be monitored. It is most likely to be considered when the organisation has already outsourced its IT (to a Managed Service Provider (MSP)). Addition of a MSSP to monitor external, internal and MSP activity can be an effective approach to providing independent monitoring.

83. Regardless of whether the implementation is insourced or outsourced, project management good practice should be adopted to ensure an effective and assured delivery (coupled with the assurance approaches covered in Appendix D of this Guide). It is important that business objectives, requirements and

targets are defined as part of the design phase of any project. For outsourcing, requirements should be formally defined and a risk management exercise undertaken prior to the invitation to tender stage. Contracts should be based on model conditions published by the Office of Government Commerce (OGC). Requirements should be formally specified in a Statement of Requirements. Organisations should also engage their own finance, contracts and legal division early in the project.

84. Appendix B of this Guide has been deliberately designed to provide assistance in identifying the specification of Protective Monitoring requirements for outsourcing. It helps to define required outputs to support the recommended approach of Output Based Specification (OBS) promoted by OGC.

Related Business Processes

85. The following paragraphs cover definition of the business processes that directly support Protective Monitoring. These should fully integrate with other associated business process for:

    a. Information security risk management (refer to Chapter 4);

    b. Information security incident management (refer to paragraphs 103. through to 105.);

    c. Forensic readiness (refer to paragraphs 106. and 107.).

86. Together these processes provide an overall cycle of continuous improvement that mirrors the Plan ⇒ Do ⇒ Check ⇒ Act cycle of ISO27001 (reference [e]). The three core processes that form part of Protective Monitoring are:

    a. Accounting;

    b. Audit;

    c. Monitoring.

87. Protective Monitoring is also supported by the following subsidiary processes:

    a. Management reporting;

    b. Retention and archive.

88. These are defined in the following paragraphs. Figure 1 (on Page 24 within Chapter 3) provides an overview of the Protective Monitoring processes and how they fit with other processes.

IA Role	Responsibilities
Executive and Management Roles	
Senior Information Risk Owner (SIRO)	• Key champion for Protective Monitoring strategy implemented on ICT systems throughout the organisation. • Owns the overall business case for Protective Monitoring within the organisation. • Informed of information security incidents relating to the assets under their ownership.
Information Asset Owners (IAO)	• Owns the risk to the specific information assets that come within the scope of a project. • Own the business case and Protective Monitoring policy for specific assets. • Informed of information security incidents relating to the assets under their ownership.
Security Management Roles	
Accreditor	• Accountable for the management of information security risks. • Source of independent advice on information security risk management. • Signs off the RMADS and Security Case for each project, which includes Protective Monitoring requirements. • Involved in continuous improvement reviews. • Informed of information security incidents.
Departmental Security Officer (DSO)	• Overall responsibility for the day-to-day responsibilities for all aspects of protective security. • Oversight of the operation of the Protective Monitoring business processes. • Delegates responsibilities to more specialist roles within team. • Provides overall management of information security incidents and ensures these are communicated as appropriate.
IT Security Officer (ITSO)	• Oversight of compliance with IT aspects of information security policy. • Undertakes IT compliance reviews, which includes production of audit reports. • Manages IT related security incidents and informs these as appropriate (to other responsibilities as well as GovCERTUK). • Assists in remediation of information security incidents.
Communications Security Officer (ComSO)	• Oversight of compliance electronic communications aspects security policy. • Manages communications, crypto and ACCSEC related security incidents and informs these as appropriate (to other responsibilities as well as CINRAS).

IA Role	Responsibilities
Operational Security Roles	
Security Manager / System Security Officer	• Localised responsibility for oversight of Protective Monitoring systems. • Undertaking of routine analysis and monitoring. • Determination and reporting of information security incidents. • Initial investigation and reporting to ITSO of information security incidents.
Security Operations Centre staff	• Supports monitoring and analysis functions. • First response to information security incidents.
Operational Roles	
System Managers / Administrators	• Reporting of malfunctions and suspected information security incidents related to systems under their control to Security Management. • May have some delegated monitoring and analysis activities.
Network Operations Centre staff	• Reporting of malfunctions and suspected information security incidents related to systems and networks under their control to Security Management.
System Users	• Reporting of errors and suspected information security incidents related their use of IT to Security Management via Line Management or Help Desk.
Supply and Outsourcing	
Service Management Team	• Overseeing performance of outsourced services. • Monitoring service levels in regard of provision of Protective Monitoring related services. • Communications with service providers and propagation of reports. • Establishing lines of communication for information security incidents.
Project Staff	• Delivery of Protective Monitoring technology solutions. • Provision of operational documentation and training to support Protective Monitoring activities.
Vendors	• Provision of supportable Protective Monitoring products including relevant patches and updates for the lifetime of the project.
Systems Integrators	• Provision of Protective Monitoring solutions including products from different vendors.
Managed Service Providers (MSPs)	• May include aspects of monitoring and analysis activities and reporting delegated by contract. • Reporting of malfunctions and suspected information security incidents related to systems and networks under their control via defined channels and procedures.
Managed Security Service Providers (MSSPs)	• Provision of dedicated Protective Monitoring activities. • Provision of tailored reports in accordance with defined service levels. • Reporting of malfunctions and suspected information security incidents related to systems and networks via defined channels and procedures.

Table 4 – Protective Monitoring Responsibilities

Advantages	Disadvantages
Insourcing	
• Staff have excellent knowledge of local business requirements and issues • Control is maintained by the organisation • No information exchange issues	• Diversion of staff and resources to activities away from core business • Visibility of the risk landscape beyond the scope of the organisation is limited • Staff need to be trained for the system to be effective • Skilled staff can have retention issues • Out of hours service limited or not practical
Outsourcing	
• Client organisation can remain focussed on core business • MSSPs offers expert and specialist services, that is their core business • Client organisation can benefit from experience gained across the entire MSSP customer base • Extensive network and real-time SOC can enable attack forecasting • Can provide any degree of service level (including 24x7) • Can operate a level of infrastructure that is beyond the means of most government organisations (redundant SOCs, etc.)	• Longer implementation time • Need of compromise on requirements to match commercial "off-the-shelf" offering (legacy systems may need remain insourced) • Can be difficult to convert business requirements to guaranteed contracted deliverables • Still requires effort to oversee and police contract delivery • Information passes outside of the control of the client organisation (an information exchange agreement is required to enforce data handling requirements) • MSSP needs time to learn the local business essentials

Table 5 – Relative Merits of Insourcing vs Outsourcing

Accounting

89. The accounting process consists of maintenance of the state of the devices within an overall architecture to meet the information security Accounting Items requirements identified as:

    a. As outcome of the risk management exercise (as the normal level of recording);

    b. Temporarily at increased levels for particular circumstances (e.g. to assist in an ongoing investigation or in response to an increased threat environment).

90. The process consists of maintaining the devices and procedures according to pre-defined sets of configurations and contingency plans. It is important that these are pre-planned and that uncontrolled changes on operational systems are avoided, as this could lead to malfunctions or log overflows. The responsibility for selection of the level of accounting should rest with the ITSO (as informed by the method given in Chapter 4 of this Guide). Implementation of configuration changes may be delegated to Security and System Managers, but these should also be recorded as accountable and auditable actions.

91. There should be documented contingency plans for setting accounting levels above the normal level. These should also be subject to occasional exercise and testing. Suggested scenarios to be covered by these plans include varying the level of accounting for (this list is not exhaustive):

    a. Activities of particular users or groups of users;
    b. Activities at particular workstations;
    c. Boundary flows for particular IP services or applications;
    d. Heightened interest in specific threats;
    e. Different threat levels in operation at particular sites;
    f. Accountability requirements that support non-repudiation.

92. For more advanced types of accountability that support non-repudiation then the process can extend and overlap with other processes for managing Public Key Infrastructures (PKI), trust services, transaction tracking and authentication processes (especially for the use of two or three factor authentication and per-transaction authentication present in workflow-like systems). It is especially important that revocation processes can tie up with accounting processes in order that the currency of credentials can either be tested at transaction time or that the use, or attempted use, of any out-of-date or revoked credentials can be linked to accounting records within audit reports. Accounting status of devices should be considered as configured items and only be varied in accordance with change control procedures.

Audit

93. The audit process includes all activities that comprise human intervention in the accounting process and the associated undertaking of analysis and detailed reporting (and correlation, data-mining, etc.).

94. The audit can take place at several levels:

    a. Immediately, in response to monitoring alerts and to support incident investigations;

b. Frequently and methodically, as a matter of surveillance of system usage and operation (measured against information security policy requirements);

c. Randomly, as a series of spot checks implemented as deterrence to policy violation;

d. Less frequently as part of internal or external compliance checking activities.

95. Typically all of these approaches should be applied to each system, with increasing frequency for systems that have higher levels of risk. Systems with less automation and sophistication of analysis tools will need to set aside more time for more intensive manual activities. The ITSO should prepare and maintain a schedule of audit activities and delegate these activities, as appropriate, to Security and System Managers. Audit reports should focus on both identifying cases were information security policy is violated and also establishing patterns and trends of normal behaviour (as comparators for future activities). The primary source of the reports will be the collected, normalised, collated and analysed accounting data. This database will also be the source of information for management reports.

Monitoring

96. This is the process of watching Protective Monitoring outputs for the presence of alerts or other indications of security breaches, either in real-time or as near to real-time as requirements and constraints dictate.

97. It also includes the initial part of the analysis to divide between false and real indications (especially those raised by automated systems including IDS/IPS). This should include monitoring of automated system actions (i.e. IPS) to ensure that:

a. Automated response is correct, and if not, to reverse or remediate it;

b. Provide supplementary or alternative manual responses.

98. Once a security breach has been ascertained this can then trigger either the audit process for further analysis or immediately raise an information security incident notification. The resourcing of this function is key and should be arranged by the ITSO. In real terms these will be activities placed with a roster of Security Managers or a SOC. They may be alerted by a number of means including console messages, email notifications, SMS messages or pager messages. They will then need to gain access to the Protective Monitoring system to analyse further information regarding the notification. The first line responders may also need the assistance of other personnel (e.g. duty System Managers or MSP staff local to the incident) in order to make further decisions or to initiate response to the alerts.

Management Reporting

99. In addition to audit reports it is highly recommended that the Protective Monitoring system is able to produce reports for digest by a wider set of stakeholders. These reports will be published on a regular basis, in accordance with organisation reporting cycle, and will include anonymous statistical information regarding the performance of the system. This is an important part of demonstrating the value of the Protective Monitoring system and its benefits to the organisation. This will encourage continued investment in Protective Monitoring. Suggested items for inclusion in such reports include:

Number of incidents correctly detected by the Protective Monitoring system;

a. Ratios of true/false indications and responses raised by the system;

b. Technical resource utilisation of the system (e.g. accumulation of data online and offline vs. space available);

c. Other statistics from the system (e.g. low level surveillance activity detected by the system);

d. Associated service level performance;

e. Trends of all of the above over time;

f. Summary of status of those incidents within the information security incident management process;

g. Evaluation of the value of business impacts mitigated by the system.

100. It should be noted that although the management reports may only include summary information, they may still warrant a protective marking and should be distributed on a "need to know" basis. The ITSO should have responsibility for production of this report, delegated as appropriate. Some tools and MSSPs may be able to provide continuously available automated reports.

Retention and Archive

101. There also needs to be a process to manage and monitor the technical resources used by the Protective Monitoring system. This includes:

a. Configuration and sizing of related storage and network bandwidth;

b. Monitoring and response to threshold alerts associated with log overflows (from the Protective Monitoring system direct or from other network management systems);

c. Management of the archiving process;

d. Production, on demand, of forensically sound copies of accounting data (from online records, archived records or from seized items of equipment);

e. Restoring data from archive, or search within archive, as necessary, to further support investigations or other operations;

f. Disposal of data and media that is past the retention period.

102. This will typically be delegated by the ITSO to Security or System Managers or other specialist personnel.

Information Security Incident Management

103. Information security incident management process is included in CESG Good Practice Guide 24 GPG 24, Security Incident Management (reference [n]). It is expected that this will form part of the procedures specified in the RMADS for any system. The procedures should cover:

a. Definition of the Incident Management Team;

b. Reporting methods and focal point;

c. Response including intermediate actions and escalation procedures;

d. Documentation and evidential requirements for incident records;

e. Reporting and review outcomes, including changes to prevent re-occurrence;

f. Incident management and reporting procedures;

g. Response and recovery procedures;

h. Implementation of lessons learnt.

104. More detailed guidelines for the implementation of information security incident management are also provided in PD ISO/IEC TR 18044:2004 IT - Security techniques - Information security incident management (reference [l]). This provides a view of the process in a cyclical form, similar to the "Plan ⇒ Do ⇒ Check ⇒ Act" (P-D-C-A) cycle common to ISO27001 (reference [e]) and other ISO standards. This includes a diagrammatic high-level view of the process that is reproduced in Figure 3 on page 49.

105. Policies and procedures should include HMG specific requirements to inform all information security incidents to GovCERTUK and all communications security incidents to CINRAS. Organisations may also wish to adopt the formation of local Warning, Advice and Reporting Point (WARP) resources, as recommended by CPNI.

Forensic Readiness

106. Forensic readiness plans are required as part of SPF MR8 (cited after paragraph 16.) and to support compliance with ISO27001 control A.13.2.3

(Collection of evidence) in cases where electronic evidence might need to be prepared from ICT systems. This is included in IS1 & 2 and needs to be considered for HMG ICT systems. Guidance on the undertaking of forensic readiness planning has been produced by CPNI (Technical Note 01/2005 - Introduction to Forensic Readiness Planning) (reference [i]). The CPNI guidance provides a 10 point plan:

a. "Define the business scenarios that require digital evidence;

b. Identify available sources and different types of potential evidence;

c. Determine the evidence collection requirement;

d. Establish a capability for securely gathering legally admissible evidence to meet the requirement;

e. Establish a policy for secure storage and handling of potential evidence;

f. Ensure monitoring is targeted to detect and deter major incidents;

g. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched;

h. Train staff in incident awareness, so that those involved understand their role in the digital evidence process and the legal sensitivities of evidence;

i. Document an evidence based case describing the incident and its impact, and;

j. Ensure legal review to facilitate action in response to the incident."

107. Items b., e. and f. overlap with Protective Monitoring processes and the information security incident management process. There are other consequent requirements that are presented in Table 6, on page 50.

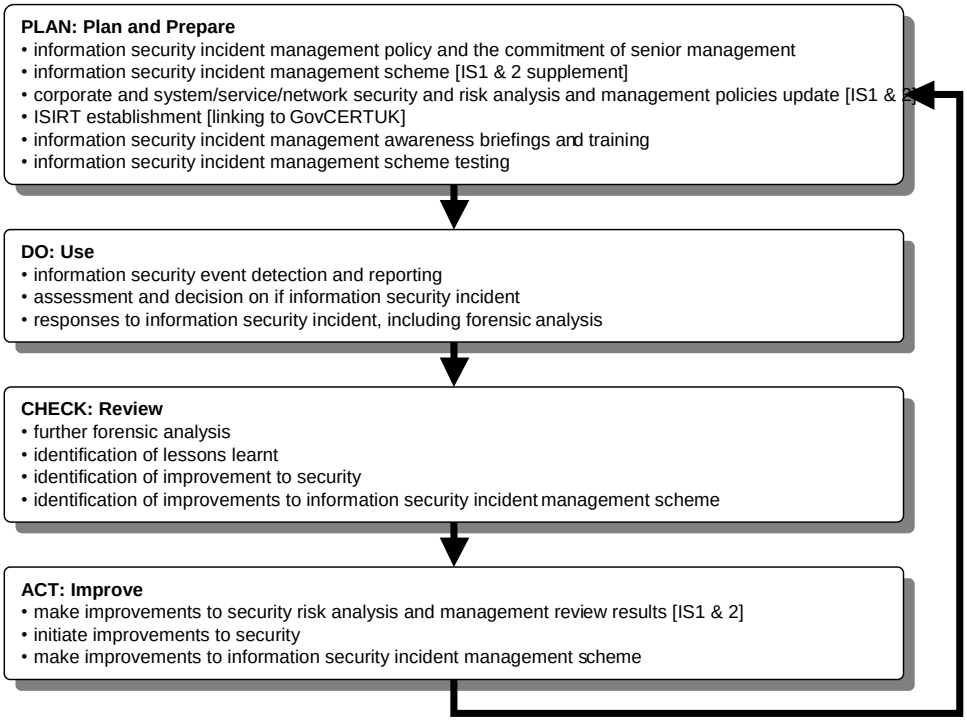

Figure 3 – Information Security Incident Management Process (after Reference [m])

Requirement	Rationale
Protective Monitoring collection process should have minimal effect on logs of the end devices (e.g. workstations and servers). Original operating system functions should manage logs on the end devices (e.g. rotate logs and purge old logs). Agent software should not re-write logs on end devices.	• Storage on end devices might need to be the subject of forensic imaging; • If automated processes interfere with the log records then they may undermine or destroy its forensic value.
Collected logs should be of high integrity and facilitate the taking of forensically sound copies. Copying of log extracts to media that can be secured as read-only and the application of cryptographic checksums should be supported to allow log veracity to be protected and checked.	• Protective Monitoring systems should be able to produce copies of the raw audit data with a high degree of integrity; • It should be possible to provide the raw audit data in a reproducible form to different analysers who arrive at the same result; • It should be possible to work on copies of the raw audit data taken as a snapshot in time, rather than the original Protective Monitoring system.
Clocks should be synchronised to an accurate time source (this is also **PMC1** from Appendix A).	• Data received from devices with inaccurate clocks may make incidents difficult to analyse and undermine the overall evidential value of the incident data.
For applications that need to support non-repudiation requirements may need higher levels of transaction authentication and recording. Protective Monitoring requirements may be linked to systems capable of applying electronic signatures.	• Some high-value transactions require specific audit facilities that meet the requirements for electronic evidence (e.g. BS10008:2008 (reference [j])).

Table 6 – Protective Monitoring Requirements to Support Forensic Readiness

THIS PAGE IS INTENTIONALLY LEFT BLANK

Appendix A – Protective Monitoring Controls and Baseline Requirements

Key Principles

- It is important that a risk management approach is adopted to apply Protective Monitoring Controls in order to provide a justifiable level of recording of data (that is covered by legislation including the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000)
- This Appendix provides information on how the Protective Monitoring Controls can be selected in accordance with a risk management approach and directly relates this enumeration to the HMG information risk management standard: IS1 & 2 and associated supplement (references [a] and [b])

Introduction

1. The Protective Monitoring Controls (PMCs) have been selected to contribute to the protection of all compromise methods included in IS1 & 2 supplement (reference [a]). It should be noted that further controls will be required to provide complete protection. Also, Protective Monitoring Controls will only be effective if integrated with wider business processes (refer to Chapter 5: including information security incident management and forensic readiness). This Appendix includes summary definition of each Protective Monitoring Control, in Table A-1, followed by a matrix given in Table A-2 which demonstrates the coverage of the compromise methods against each treatment. The exact requirements for each Protective Monitoring Control are then presented in Appendix B of this Guide. It also includes a consolidated list of baseline requirements for Protective Monitoring in Table A-3.

Protective Monitoring Controls

2. Table A-1 on page 54 is a catalogue of Protective Monitoring Controls that can be applied to treat any given project risk. Each of these is further defined in Appendix B. It should be noted that not all collection and analysis requirements given are required in all circumstances. Depending on the Segmentation Model levels chosen, the recommended set of requirements vary (refer to Appendix B).

3. Protective Monitoring Controls **PMC1** through to **PMC9** have been chosen to provide treatment of specific IS1 compromise methods. Treatments **PMC10**, **PMC11** and **PMC12** are specific to the functional requirements of the Protective Monitoring system itself and will be applicable depending on the complexity of Protective Monitoring solution implemented (**PMC12** is always applicable).

Compromise Method Coverage

4. Table A-2 on page 55 provides an applicability matrix for each Protective Monitoring Control to the IS1 & 2 supplement Compromise Methods. The columns under Property in the Table indicate if the compromises relate to breaches of C[onfidentiality], I[ntegrity] or A[vailability]. A Y[es] at the row/column indicates applicability. Each of Protective Monitoring Controls (**PMC1** through to **PMC12**) is provided with a separate column in the Table. An X at the row/column intersection between the Compromise Method and a PMC indicates that the control contributes to protection against that a compromise method of that type.

Baseline Requirements

5. Table A-3 on page 56 provides a consolidated list of requirements needed to address the baseline requirements for Protective Monitoring of HMG ICT Systems. These provide recommended treatment profiles for the Baseline Control Set. It should be noted that this is mainly a re-statement of requirements from IS1 & 2 Supplement (although some additional guidance is appended to the last row of the Table).

6. Citing adoption of the GPG 13 approach and Protective Monitoring Control within Statements of Applicability of the RMADS for a system can be expected to provide full justification for addressing the compliance aspects of the relevant controls (subject to assured implementation and operation of those treatments in accordance with the CESG Assurance Framework).

Control ID	Title (refer to Appendix B for full details)
PMC1	Accurate time in logs.
PMC2	Recording of business traffic crossing a boundary.
PMC3	Recording relating to suspicious activity at the boundary.
PMC4	Recording on internal workstation, server or device status.
PMC5	Recording relating to suspicious internal network activity.
PMC6	Recording relating to network connections.
PMC7	Recording on session activity by user and workstation.
PMC8	Recording on data backup status.
PMC9	Alerting critical events.
PMC10	Reporting on the status of the audit system.
PMC11	Production of sanitised and statistical management reports.
PMC12	Providing a legal framework for Protective Monitoring activities.

Table A-1 - Protective Monitoring Controls

Threat Actors / Compromise Methods	Property			Protective Monitoring Control (PMC*n*)												
	C	I	A	1	2	3	4	5	6	7	8	9	10	11	12	#
Normal User																
Accidentally Releases	Y			X	X					X		X	X	X	X	7
Accidentally Corrupts		Y		X						X	X	X	X	X	X	7
Accidentally Disrupts			Y	X				X		X	X	X	X	X	X	8
Deliberately Releases	Y			X	X					X		X	X	X	X	7
Deliberately Corrupts		Y		X						X	X	X	X	X	X	7
Deliberately Disrupts			Y	X				X		X	X	X	X	X	X	8
Changes Configuration	Y	Y	Y	X			X	X			X	X	X	X	X	8
Privileged User																
Accidentally Releases	Y			X	X					X		X	X	X	X	7
Accidentally Corrupts		Y		X						X	X	X	X	X	X	7
Accidentally Disrupts			Y	X				X		X	X	X	X	X	X	8
Deliberately Releases	Y			X	X					X		X	X	X	X	7
Deliberately Corrupts		Y		X						X	X	X	X	X	X	7
Deliberately Disrupts			Y	X				X		X	X	X	X	X	X	8
Information Exchange Partner																
Unexpectedly Receives	Y			X	X							X	X	X	X	6
Provides Misleading Information		Y		X	X						X	X	X	X	X	7
Withholds Information			Y	X	X							X	X	X	X	6
Performs a Business Traffic Attack	Y	Y	Y	X	X	X						X	X	X	X	7
Performs a Network Attack	Y	Y	Y	X		X	X	X	X			X	X	X	X	9
Service Provider																
Passively Intercepts	Y			X			X		X			X	X	X	X	7
Actively Corrupts		Y		X			X			X	X	X	X	X	X	8
Actively Disrupts			Y	X			X		X		X	X	X	X	X	8
Performs a Network Attack	Y	Y	Y	X		X	X	X	X			X	X	X	X	9
Service Consumer																
Performs a Network Attack	Y	Y	Y	X		X	X	X	X			X	X	X	X	9
Bystander																
Observes	Y			X						X		X	X	X	X	6
Substitutes Data		Y		X			X				X	X	X	X	X	7
Steals or Damages Equipment			Y	X			X		X		X	X	X	X	X	8
Impersonates	Y	Y	Y	X						X		X	X	X	X	6
Tampers	Y	Y	Y	X			X		X		X	X	X	X	X	8
Indirectly Connected																
Performs any Hybrid Attack	Y	Y	Y	X	X	X	X	X	X	X	X	X	X	X	X	12
		Count		29	9	5	11	9	7	14	16	29	29	29	29	

Table A-2 - Compromise Methods covered by Protective Monitoring Controls

Control	Baseline Control Set
10.10.1 Audit logging	In accordance with SPF Departments **must** ensure that ICT systems are capable of producing records of user activity to support monitoring, incident response and investigations. For further information Departments should consult the SPF and GPG 13.
10.10.2 Monitoring system use	Departments **must** develop and implement procedures to monitor use of systems and services by users to support incident response and investigation activities. For further information Departments should consult the SPF, ISO 27002, GPG 13 and GPG 18, *Forensic Readiness,* (reference [i]).
10.10.3 Protection of log information	Audit logs **must** be protected in accordance with their sensitivity or protective marking. See 10.7.4 for further information on protecting system information.
10.10.4 Administrator and operator logs	ICT systems **must** be capable of generating audit logs for all system users including system administrators. Departments should consult the SPF, ISO 27002 and GPG 13.
10.10.5 Fault logging	Departments **must** log and review system faults at regular intervals. For further information refer to ISO 27002, ISO 20000, and the OGC IT Infrastructure Library (ITIL).
10.10.6 Clock synchronisation	Departments **must** implement a reliable means to keep all server and device clocks of the ICT System in synchronisation. For further information Departments should consult the SPF, ISO 27002 and GPG 13.
13.2.3 Collection of evidence	In accordance with SPF MR 37 Departments **must** have 'a forensic readiness policy that will maximise the ability to preserve and analyse data generated by an ICT system, that may be required for legal and management purposes'. For further information Departments should consult GPG 18, *Forensic Readiness* (reference [i]).
15.3.1 Information system audit controls	Departments **must** implement plans and controls to ensure that audit and compliance checks do not adversely affect the business operation of an ICT system. For further information Departments should refer to ISO 27002.
15.3.2 Protection of information system audit tools	System audit tools **must** be protected to prevent their use for unauthorised purposes. For further information Departments should refer to ISO 27002.
Additional advice (specific to this Guide)	Most systems requiring protection at the baseline level can be satisfied by implementation of the following recommended minimum set of PMCs at the **Deter** segment which are defined in Appendix B, to the degree appropriate for project: **PMC1**, **PMC4**, **PMC7**, **PMC9**, **PMC10** and **PMC11**. The following controls should also be conditionally applied along with the baseline, as applicable to the project under consideration: • **PMC2** (with electronic information exchanges or import/export); • **PMC3** (with network boundary); • **PMC6** (with remote access or wireless technology) and/or • **PMC8** (with significant backup/restore infrastructure). It is also possible to provide a more fine grained approach to risk management by selective application of the **Aware** or **Deter** profiles given in Table B-1 in Appendix B and the individual Segmentation Model Recommendations for each of the twelve Appendix B PMC sheets.

Table A-3 - Protective Monitoring Baseline Control Set

THIS PAGE IS INTENTIONALLY LEFT BLANK

Appendix B – Detailed Definition of Protective Monitoring Controls

Key Principles

- Once Protective Monitoring Controls have been selected, it is important to have sufficient information as to how these can be applied in practice
- This is true, no matter how a system is implemented, this can include:
    - Developing and operating an in-house solution;
    - Including Protective Monitoring requirements in outsourced solutions;
    - Putting into place Protective Monitoring regimes to oversee either partially or wholly outsourced ICT service provision.
- This Appendix provides detail on each of the Protective Monitoring Controls. It is intended to provide enough detail for related project requirements to be specified to a reasonable degree of detail. It is based on the principle of Output Based Specification (OBS) to be in accordance with current OGC recommendations for ICT requirements specification (reference [o])

Introduction

1. This Appendix provides further detailed information on the recommendations for implementation of each of the Protective Monitoring Controls presented in Appendix A. Each is defined in respect of:

    a. Control description (front sheet);

    b. Segmentation Model requirements (front sheet);

    c. Recording and accounting recommendations (back sheet).

Control Description

2. This provides a high level description of the control as to what the control attempts to achieve.

Segmentation Model Requirements

3. This provides a table of control recommendations in order to align with the Audit and Accounting principle of the IS1 & 2 Supplement Segmentation Model. This includes different sets of recommendations for:

    a. Aware;

    b. Deter;

c. Detect and resist;

d. Defend.

4. These can be applied in cases where the Segmentation Model is used to address risks in the Detect & Resist and Defend segments, or other cases selected by professional judgement. The last row of Table A-3 in Appendix A also identifies a subset of the control recommendations that can be applied to satisfy Baseline Control Set requirements.

Recording and Accounting Recommendations

5. For each control there are four different Recording Profile sets **A**, **B**, **C** or **D** and these generally correspond to the levels of protection required for the difference segments of the IS1 & 2 Supplement Segmentation Model. The main characteristics of these profiles are given in Table B-1.

Recording Profile	Aligns to Segment (Risk Level)	Accumulative Requirement	Margin for Discretion (plus/minus one level)
A	**Aware** (Medium)	Alone.	upper **B**
B	**Deter** (Medium-High)	*plus* **A** records.	lower **A**, upper **C**
C	**Detect & Resist** (High)	*plus* **A** and **B** records.	lower **B**, upper **D**
D	**Defend** (Very High)	*plus* **A**, **B** and **C** records.	lower **C**

Table B-1 - Recording Profile characteristics

6. Note that profile recommendations are accumulative (as illustrated in Table B-1).

7. It can be appropriate to increase the level of Protective Monitoring requirements presented within this Guide for a project, or specific part of a project, to make up for a shortfall of protection in other controls or in-lieu of lack of compliance with Baseline Control Set requirements. For instance, an Accreditor may accept an increased profile of Recordable Events of internal network monitoring due to the lack of available access control technology (e.g. **PMC5** protective monitoring with a Recording Profile of **B**, where only a profile of **A** is identified as recommended by the corresponding **Segmentation Model Recommendations**). In other cases the need for recording can be selectively reduced from the norm to reduce recording overheads, provided adequate mitigation is provided by additional compensating controls. The recommended margin for discretion in the selection of the levels of recording is *plus* or *minus* one profile level. Ultimately it is up to the Accreditor, working with the security analyst, to confirm that the Protective Monitoring facilities for any given solution are adequate.

8. The section includes a table of items that defines the recording, reporting and alerting aspects of the treatment. This includes a table of **Recordable Event** definitions (rows) vs. columns that indicate **Report** and **Alert** recommended requirements. Each intersection is marked with one of the recording profile letters (**A** through to **D**) or left blank indicating membership of that Report or Alert requirement within the indicated Recording Profile. Actual reports (typically delivered by COTS offerings) that approximate to the recommended content should be regarded as sufficient without variation. Indeed, it would be expected that actual reports will add value by virtue of proprietary functions (e.g. structured presentation of reports with drill-down capability) and graphical representation. Items given in **bold** text in the report definitions given in the table's **Accounting Items** column indicate that items that can be captured from various log sources and that are catalogued and further defined in Appendix C.

9. Naturally, the Accounting Items from particular sources are only applicable if they are incorporated within a particular project solution. Elsewhere Recording Profiles are referred to in recommendations by statements such as "Typical Recording Profile is **A**, **B**, **C** or **D**".

Common Factors

10. The following factors are common to all of the Protective Monitoring Controls:

    a. **Business Criticality** - The recording level on each device should be established according to its capabilities and its level of business criticality. Clearly, requirements for servers will usually be in excess of the requirements for workstations. Exact requirements need to be defined for each device as part of detailed system design;

    b. **COTS Functionality** - There will are basic logging and alerting facilities in all commonly available COTS operating systems in use by HMG ICT systems. Lower segments can implement superior facilities if these are available either as part of an enterprise solution or as off-the-shelf provision from an ICT MSP;

    c. **Event Criticality** - Some devices assign different senses of criticality to each event logged ("critical", "error", "warning", etc.). The true sense of event criticality should also be reviewed on a case-by-case basis, in order to determine each event's implications regarding security, as this may differ from the default vendor setting;

    d. **Event Recording Duplication** - There may be degrees of duplication in monitoring at upper profiles of monitoring (e.g. local firewall logs and IDS systems may both log the same event). There may be benefits in providing some degree of such redundancy in order to implement a "defence in depth" approach (typically within the **Defend** segment of the Segmentation

Model). However, in the case of lesser requirements the implementation can be tuned to eliminate duplication and provide recording of the most significant source. Also, one event may produce reports in several places in the network and, without correct understanding, this could lead to mistaken impression there are multiple events;

e. **Log Normalisation** - There will be different proprietary logging capabilities for all devices used to track network attacks. Merging of logs from these devices may require an normalisation process to bring them to a common format that can be audited in a consistent manner;

f. **Logs on Detached Devices** - Workstations and other devices (e.g. PEDs) may operate detached from the network and may accumulate log entries while they are detached. There should be a health check whenever they attach (e.g. verification of the currency of the anti-malware signature base), capture of the log messages while detached and raising of alert conditions. Consideration should be given to completing these checks prior to allowing these devices being allowed full network access;

g. **Log Correlation** - Specific challenges can arise during the correlation of events relating to transactions in complex systems. This especially applies to "N-tier" architectures (e.g. where a transaction passes through separate web, application and database servers). The issue concerns cases where there is a lack of any common transaction identifier maintained consistently along the path. In these cases correlation can be limited to assembling the separately generated logs on a timeline, which can be unsatisfactory. This especially arises where a web service recognises a user by a unique identifier but the corresponding database service uses a "generic" system account and its logs cannot be directly traced to a specific user. The Protective Monitoring solutions should seek to design out such issues and ensure end-to-end correlation and traceability of transactions.

PMC1 - Accurate time in logs

Control Description
Provide a means of providing accurate time in logs and synchronisation between system components with a view to facilitating collation of events between those components. This can be achieved by any or all of the following means: • Providing a master clock system component which is synchronised to an atomic clock; • Updating device clocks from the master clock using the Network Time Protocol (NTP); • Record time in logs in a consistent format (Universal Co-ordinated Time (UTC) is recommended); • As a fallback, checking and updating device clocks on a regular basis (e.g. weekly). Projects should define the error margin for time accuracy according to business requirements. The following issues also need to be considered: • Some devices may not support clock synchronisation and need to be manually maintained; • Although recording time in UTC, the human interface should also support local time; • Clocks drift on mobile devices (e.g. Portable Electronic Devices (PEDs)) may require correction upon attachment.

Segmentation Model Recommendations	
Aware	Simple but accurate time-stamps only. Typical Recording Profile is **A**.
Deter	As **Aware**, plus: All log file collections should include a cryptographic checksum (e.g. Hash Message Authentication Code (HMAC)) that incorporates an accurate cryptographic time-stamp. Typical Recording Profile is **B**.
Detect & Resist	As **Deter**, plus: Typical Recording Profile is **B**, unless: Where there is a significant transaction integrity requirement (IL4) then the use of Public Key Infrastructure (PKI) digital time-stamping of transaction records can be considered. Typical Recording Profile is **C**.
Defend	As **Detect and Resist**, plus: There should be redundant time sources (or time source reception devices) and a means to detect and alert conflicts between those time sources. Typical Recording Profile is **B**, unless: Where there is a significant transaction integrity requirement (IL5+). In this case the typical Recording Profile is **C**.

PMC1 - Accurate time in logs (continued)

Index	Recordable Events	Typical Accounting Items	Report	Alert
	Accounting Recommendations (items in **Bold** text are defined in Appendix C)			
1.	Each and every event record should include a simple time-stamp.	**Date** and **Time**	**A**	
2.	Alert messages may reference related events and should also be time-stamped.	**Date** and **Time** and **Log** record reference		**A**
3.	Log file extracts should include an accurate time-stamp that is digitally signed.	**Date**, **Time**, Log file **Hash** and **Signature**	**B**	
4.	Transactions with a high integrity requirement should have a hash of the transaction time-stamped, digitally signed and a copy of the transaction record retained.	**Date**, **Time**, Transaction **Hash**, **Signature** and **Content(2)**	**C**	

PMC2 - Recording relating to business traffic crossing a boundary

Control Description	
The objective of this control is to provide reports, monitoring, recording and analysis of business traffic crossing a boundary with a view to ensuring traffic exchanges are authorised, conform to security policy, transport of malicious content is prevented and alerted, and that other forms of attack by manipulation of business traffic are detected or prevented. The main requirement is to provide an accountable record of imports and exports executed by internal users and to track cross-boundary information exchange operations and the utilisation of any externally visible interfaces. This includes all checking of cross-boundary movement of information, content checking and quarantining services. Application based checks can be applied to business traffic to accept legitimate transactions and reject and alert malformed exchanges.	
Segmentation Model Recommendations	
Aware	Malware detection and status of signature updates should be logged and reportable (at the boundary). Typical Recording Profile is **A**.
Deter	As **Aware**, plus: Internal user details should be disguised in external interactions. However, logs should record the original user initiating those interactions. User web browsing activity should be checked against an Acceptable Use Policy at the boundary and logged. All imported content should be subject to content checking. On detection of malware or dangerous imports they should be quarantined and alerted to the System Manager. If there are not means to check encrypted content at the boundary (e.g. decrypt-scan, decrypt-scan-encrypt of SSL traffic) then this should either be discarded or quarantined, and the event logged, reportable and audited. Typical Recording Profile is **B**.
Detect & Resist	As **Deter**, plus: All exports should be logged and checked against security policy (e.g. scanning contents for key words) prior to release. All imported web content should be logged. Security policy violations should be alerted to the Security Manager. Typical Recording Profile is **C**.
Defend	As **Detect and Resist**, plus: All exports should be logged and checked for formal release authorisation and compliance with security policy (e.g. security label is a permitted value for export). Security policy violations should be alerted to the Security Manager. Typical Recording Profile is **D**.

PMC2 - Recording relating to business traffic crossing a boundary (continued)

Accounting Recommendations (items in **Bold** text are defined in Appendix C)				
Index	**Recordable Events**	**Typical Accounting Items (plus PMC1 time-stamp)**	**Report**	**Alert**
1.	Malware detection at the boundary.	**Malware** name, **Application(1)** stream detected in, **Direction** and **Console**	**A**	**A**
2.	Every change in status of the boundary anti-malware signatures.	Signature-base **Version(1)** and **Console**	**A**	
3.	Blocked web browsing activities.	**User**, **Workstation**, **URL** and **Reason**	**B**	**B**
4.	Blocked file import attempts across the boundary.	**User, Workstation** or **Process, URL** of file and **Reason**	**B**	**B**
5.	Blocked file export attempts across the boundary.	**User, Workstation** or **Process, URL** and **Reason**	**B**	**B**
6.	Enhancement to Events 4. and 5. records to include file content.	Enhanced to include **Content(1)** of file.	**C**	
7.	Enhancement to Events 4. and 5. records, where processed by a guard processor.	Enhanced to include **Content(1)** plus **Security Label** and **Signature** of file.	**C**	
8.	Allowed web browsing activities across the boundary.	**User**, **Workstation** and **URL**	**C**	
9.	File import across the boundary that are allowed.	**User, Workstation** or **Process** and **URL**	**C**	
10.	Allowed file export across the boundary.	**User, Workstation** or **Process** and **URL**	**C**	
11.	Enhancement to Events 9. and 10. records to include file content.	Same as Event 6.	**D**	
12.	Enhancement to Events 9. and 10. records, where processed by a guard processor.	Same as Event 7.	**D**	
13.	Files entered into a transfer cache.	**URL**, **Content(1)**, **Security Label**, **Signature** and **Time to Live** (all as available)	**D**	
14.	Access of files entered into a transfer cache.	**User**, **Workstation** and **URL**	**D**	

PMC3 - Recording relating to suspicious behaviour at a boundary

Control Description
The objective of this control is to provide reports, monitoring, recording and analysis of network activity at the boundary with a view to detecting suspect activity that would be indicative of the actions of an attacker attempting to breach the system boundary or other deviation from normal business behaviour. The main requirement is to receive information from firewalls and other network devices for traffic and traffic trend analysis. This will enable detection of common attacks such as port scanning, malformed packets and illicit protocol behaviours. An intrusion detection service is a recommended defence at the boundary with any untrusted network (e.g. the Internet). It may also be a mandated requirement in codes of connection for membership of community of interest networks (such as GSI). Whenever it is implemented then it is recommended it includes a Recordable Report profile of at least **B**.

Segmentation Model Recommendations	
Aware	It should be possible to interrogate and review firewall logs to determine current boundary conditions. Typical Recording Profile is **A**.
Deter	As **Aware** plus: There should be an integrated firewall reporting solution that permits attack trend analysis to be conducted at all boundary points. There should be intrusion detection services that cover all boundary servers, firewalls and routers. Typical Recording Profile is **B**.
Detect & Resist	As **Deter** plus: It should be possible to select limited full packet recording and analysis at key boundary points. Typical Recording Profile is **C**.
Defend	As **Detect & Resist** plus: For larger enterprises there should be an integrated Security Information and Event Management (SIEM) solution that supports analysis of attack across the organisation and near real-time alerting. There should be extensive full packet recording of network traffic at the boundary. Typical Recording Profile is **D**.

PMC3 - Recording relating to suspicious behaviour at a boundary (continued)

Index	Recordable Events	Typical Accounting Items (plus PMC1 time-stamp)	Report	Alert
	Accounting Recommendations (items in **Bold** text are defined in Appendix C)			
1.	Packets being dropped by boundary firewalls.	Packet **Header**, **Size(1)**, **Firewall**, arrival **Interface** and **Rule**	**A**	
2.	All boundary monitoring system console messages at **Critical** status and above.	**Criticality**, **Message** contents and output **Console**	**B**	**B**
3.	User authentication failures on boundary devices and systems.	**User**, **Device**, **Console** and **Reason** for failure	**B**	**B**
4.	The detection of all suspected attacks at the boundary.	Detecting **Probe** or **Agent**, **Attack** type, **Source**, **Target** and attack **Detail**	**B**	**B**
5.	All boundary monitoring system console messages at **Error** status.	**Criticality**, **Message** contents and output **Console**	**B**	
6.	User sessions on boundary devices and consoles of boundary management systems.	**User**, **Device**, **Console**, **Session** and **Status(1)** of session	**B**	
7.	All changes to boundary firewall and other relevant device rule-bases.	**User**, **Device**, **Console**, **Rule** changed and **Content** of rule	**B**	
8.	All actions invoked by users in response to an external attack notification.	Same as Event 7, plus **User, Session** and **Action(1)** initiated	**B**	
9.	Every change in status of the external attack recognition software (Security Information and Event Management systems (SIEM), Network Behaviour Analysis (NBA), IDS or IPS) signature base.	Signature-base **Version(1)**, **Probe**(s) or **Agent**(s) and **Console** reporting	**B**	
10.	All boundary monitoring system console messages at **Warning** status and below.	**Criticality**, **Message** contents and output **Console**	**C**	
11.	All commands issued to boundary devices and consoles of boundary monitoring systems.	**User**, **Session**, **Command** and **Response**	**C**	
12.	Packets being passed by boundary firewalls.	Packet **Header**, **Size(1)**, **Firewall**, arrival **Interface**	**C**	
13.	Enhancement to Event 1. records to include full packet capture.	Same as Event 1, plus **Data** in packet	**C**	
14.	All automated responses at the boundary (by an IPS).	Same as Event 7, plus **Action(1)** initiated	**D**	**D**
15.	Enhancement to Event 10. records to include full packet capture.	Same as Event 10, plus **Data** in packet	**D**	

PMC4 - Recording of workstation, server or device status

Control Description	
The objective of this control is to detect changes to device status and configuration. Changes may occur through accidental or deliberate acts by a user or by subversion of a device by malware (e.g. installation of trojan software or so called "rootkits"). It will also record indications that are typical of the behaviour of such events (including unexpected and repeated system restarts or addition of unidentified system processes). It also attempts to detect other unauthorised actions in tightly controlled environments (e.g. attachment of USB storage devices). This includes extension to extensive monitoring of any business critical file areas.	
Segmentation Model Recommendations	
Aware	It should be possible to check the status of anti-malware software updates and receive alerts of malware detection. File, I/O and other system errors should be logged and reportable. They should be alerted to a network management system, where applicable. Typical Recording Profile is **A**.
Deter	As **Aware**, plus: System start-up and shutdown events should be logged and reportable for all devices. All file system access violation messages should be logged, reportable and alerted. File system monitoring should be active at the storage device or partition (referred to as "volume") level and the attachment of I/O devices (e.g. USB devices) and volume activity logged on business critical devices. Typical Recording Profile is **B**.
Detect & Resist	As **Deter**, plus: Consider extending the **Deter** level of critical logging and alerting to all devices. It should be possible to increase the level of logging for particular file systems and file system areas, to allow all file operations to be logged. For business critical devices: • active tracking of changes to system files or configuration (e.g. registry) settings; • start-up and shutdown of all service processes should be logged and reportable. Typical Recording Profile is **C**.
Defend	As **Detect and Resist**, plus: Consideration should be given to extend the **Detect and Resist** level of logging and alerting for business critical devices to all devices. All critical file system and file system areas should be permanently subject of extensive logging of operations. Typical Recording Profile is **D**.

PMC4 - Recording of workstation, server or device status (continued)

Index	Recordable Events	Typical Accounting Items (plus PMC1 time-stamp)	Report	Alert
	Accounting Recommendations (items in **Bold** text are defined in Appendix C)			
1.	All critical host messages at **Critical** status and above (servers and selected workstations).	**Criticality**, **Message** contents and source **Host**	**A**	**A**
2.	Malware detection incident on any host (workstation or server).	**Malware** name and **Host** on which it is detected	**A**	**A**
3.	All critical host messages at **Error** status and above (servers and selected workstations).	**Criticality**, **Message** contents and source **Host**	**A**	
4.	Every change in status of any hosts anti-malware software signature base.	Signature-base **Version(1)** and **Host** on which it is updated	**A**	
5.	Every failing file system access attempt should be logged and reportable.	**File** or **Path** of attempt, **Host**, **User** or **Process**, **Access** attempt and **Reason** failed	**B**	
6.	Changes to file or path access rights within system folders.	**User** or **Process** initiating, **Host**, **File** or **Path** and **Rights** or **ACLs**	**B**	
7.	Change in status of all networked hosts.	**Host** and **Status(2)** change	**B**	
8.	Change in status of attachment of devices attached to controlled hosts.	**User** or **Process**, **Device**, **Interface**, **Host** and **Status(3)** change	**B**	
9.	Change in status of storage volumes of monitored hosts.	**User** or **Process**, **Host, Volume**, **Detail** and **Status(4)** change	**B**	
10.	Change in software configuration status.	**User** or **Process**, **Host**, **Package** or **Patch** details, **Version(2)** and change **Status(5)**	**B**	
11.	Changes detected to files within system folders.	**File** or **Path**, **User** or **Process**, **Host**, **Detail** of the change	**C**	**C**
12.	All critical host messages at **Warning** status or below (servers and selected workstations).	**Criticality**, **Message** contents and source **Host**	**C**	
13.	Any changes to system configuration (or registry) settings any host.	**File** or **Path**, **Host**, **User** or **Process**, **Setting** and **Detail**.	**C**	
14.	Change in status of system processes on monitored hosts.	**Host**, **User**, **Process**, **Status(6)** and **Detail**	**C**	
16.	Enhancement to Event 10. records to include package software inventory.	As Event 10, plus **Inventory** and per item **Information**	**D**	
17.	Enhancement to Event 11. records to include the contents of changes to files.	As Event 11, plus **Before** and **After** file content	**D**	
18.	Enhancement to Event 13. records to include the content of changes to configuration settings.	As Event 13, plus **Before** and **After** state of setting	**D**	

PMC5 - Recording relating to suspicious internal network activity

Control Description
The objective of this control is to monitor critical internal boundaries and resources within internal networks to detect suspicious activity that may indicate attacks either by internal users or by external attackers who have penetrated to the internal network. Likely targets for heightened internal monitoring include: • core electronic messaging infrastructure (e.g. email servers and directory servers); • sensitive databases (e.g. HR databases, finance, procurement/contracts, etc.); • information exchanges with third parties; • project servers and file stores with strict "need to know" requirements.

Segmentation Model Recommendations	
Aware	Consider implementation of firewalls in front of business critical servers or internal network zones. It should be possible to interrogate and review these firewall logs to determine current internal conditions. Typical Recording Profile is **A**.
Deter	As **Aware**, plus: There should be an integrated firewall reporting solution that permits attack trend analysis to be conducted at internal boundaries (this may be in common with **PMC3**). Typical Recording Profile is **B**.
Detect & Resist	As **Deter**, plus: Consider internal intrusion detection of business critical servers or internal network zones. Apply HIDS agents to business critical servers. Apply NIDS to internal business critical network zones. Typical Recording Profile is **C**.
Defend	As **Detect and Resist**, plus: Conduct internal network behaviour analysis. Consider IPS for internal business critical subnets (consult with CESG for configuration and operation advice). Typical Recording Profile is **D**.

PMC5 - Recording relating to suspicious internal network activity (continued)

Accounting Recommendations (items in **Bold** text are defined in Appendix C)				
Index	**Recordable Events**	**Typical Accounting Items (plus PMC1 time-stamp)**	**Report**	**Alert**
1.	Packets being dropped by internal firewalls.	Packet **Header**, **Size(1)**, **Firewall**, arrival **Interface** and **Rule**	**A**	
2.	All internal monitoring system console messages at **Critical** status and above.	**Criticality**, **Message** contents and output **Console**	**B**	**B**
3.	User authentication failures on internal network devices and monitoring consoles.	**User**, **Device**, **Console** and **Reason** for failure	**B**	**B**
4.	All internal monitoring system console messages at **Error** status.	**Criticality**, **Message** contents and output **Console**	**B**	
5.	User sessions on internal network devices and monitoring consoles.	**User**, **Device**, **Console**, **Session** and **Status(1)** of session	**B**	
6.	All changes to internal firewall and other relevant device rule-bases.	**User**, **Device**, **Console**, **Rule** changed and **Content** of rule	**B**	
7.	The detection of all suspected internal attacks.	**Probe** or **Agent**, **Attack** type, **Source**, **Target** and attack **Detail**	**C**	**C**
8.	All internal monitoring system console messages at **Warning** status or below.	**Criticality**, **Message** contents and output **Console**	**C**	
9.	All commands issued to internal network devices and central consoles of internal monitoring systems should be logged and reportable.	**User**, **Session**, **Command** and **Response**	**C**	
10.	Packets being passed by internal firewalls should be logged and reportable.	Packet **Header**, **Size(1)**, **Firewall** and arrival **Interface**	**C**	
11.	Enhancement to Events 1. records to include full packet capture.	Same as Event 1, plus **Data** in packet	**C**	
12.	All actions invoked by users in response to an internal attack notification.	Same as Event 7, plus **User, Session** and **Action(1)** initiated	**C**	
13.	Every change in status of the internal attack recognition software (SIEM, NBA, IDS or IPS) signature base.	Signature-base **Version(1), Probe**(s) or **Agent**(s) and **Console** reporting	**C**	
14.	All automated responses at internal network control points (by an IPS).	Same as Event 7, plus **Action(1)** initiated	**D**	**D**
15.	Enhancement to Events 10. records to include full packet capture.	Same as Events 10, plus **Data** in packet	**D**	

PMC6 - Recording relating to network connections

Control Description	
The objective of this control is to monitor temporary connections to the network either made by remote access, virtual private networking, wireless or any other transient means of network connection. This includes: • Environments which are permissive and that support Wireless LANs (WLANs), mobile users and remote working and it includes • More restrictive environments in which the attachment of modems and wireless access points are prohibited.	
Segmentation Model Recommendations	
Aware	Provide scope for resolving workstation addresses from dynamic IP to physical address (e.g. resolving to Media Access Control (MAC) address by consultation of Dynamic Host Configuration Protocol (DHCP) or Address Resolution Protocol (ARP) logs). Also provide scope for resolving remotely attached workstations and workstations attached via wireless connections (e.g. by inspection of Remote Dial In User Service (RADIUS), wireless access point or remote access server logs). Typical Recording Profile is **A**.
Deter	As **Aware**, plus: Log and alert unauthorised connections (including non-standard workstations and wireless access points). Capture all remote access authentication exchanges. Apply IDS to remote access and virtual private networking DMZs. Typical Recording Profile is **B**.
Detect & Resist	As **Deter**, plus: Consider limiting attached MAC addresses and using statically assigned IP addresses. Lock-down network ports. Log and alert unauthorised MAC attachments. Typical Recording Profile is **C**.
Defend	As **Detect and Resist** plus: Consider policing for the presence of illegal wireless access point attachments or devices using an all-channel Wireless IDS (WIDS). Typical Recording Profile is **D**.

PMC6 - Recording relating to network connections (continued)

Index	Recordable Events	Accounting Recommendations (items in **Bold** text are defined in Appendix C) Typical Accounting Items (plus PMC1 time-stamp)	Report	Alert
1.	User authentication failures for remote access.	**User**, **Credential**, **Host** and **Reason** for failure	**A**	**A**
2.	All unsuccessful Virtual Private Network (VPN) node registrations.	**Node**, **VPN and Reason** for failure	**A**	**A**
3.	Changes of status of dynamic IP address assignments.	**MAC**, **IP Address** and **Detail** of assignment	**A**	
4.	User sessions via remote access.	**User**, **Credential**, **Host**, **Session** and **Status(1)** of session	**A**	
5.	Changes in status of VPN node registration.	**Node**, **VPN** and connection **Status(7)**	**A**	
6.	All rejected attempts to connect equipment to protected network attachment points.	Network socket **Point**, **MAC** and **Reason** for failure	**B**	**B**
7.	All network connection console messages at **Critical** status and above.	**Criticality**, **Message** contents and output **Console**	**B**	**B**
8.	User authentication failures on network connection consoles.	**User**, **Device**, **Console** and **Reason** for failure	**B**	**B**
9.	All network connection console messages at **Error** status.	**Criticality**, **Message** contents and output **Console**	**B**	
10.	All cases of attachment attempts of wireless devices to legitimate wireless access points.	**WLAN** details, **MAC** and **Status(8)** of wireless attachment	**B**	
11.	User sessions on network connection consoles.	Same as Event 8, plus **Session** and **Status(1)** of session	**B**	
12.	The detection of all suspected wireless attacks.	**Probe** or **Agent**, **Attack** type, **Source**, **Target** and attack **Detail**	**C**	**C**
13.	All network connection console messages at **Warning** status or below.	**Criticality**, **Message** contents and output **Console**	**C**	
14.	All commands issued to network connection consoles	**User**, **Session**, **Command** and **Response**	**C**	
15.	All actions invoked by users in response to an internal attack notification.	Same as Event 12, plus, plus **User, Session** and **Action(1)** initiated	**C**	
16.	Every change in status of the internal attack recognition software (WIDS) signature base.	Signature-base **Version(1), Probe**(s) or **Agent**(s) and **Console** reporting	**C**	
17.	Detection of all rogue wireless interfaces and wireless access points should be logged, reportable and alerted.	**WLAN** details, **Channel(1)**, **MAC** and **Location** information	**D**	**D**

PMC7 - Recording of session activity by user and workstation

Control Description	
To monitor user activity and access to ensure they can be made accountable for their actions and to detect unauthorised activity and access that is either suspicious or is in violation of security policy requirements. This is intended to support accountability requirements such that users can be held to account for actions they perform on ICT systems.	
Segmentation Model Recommendations	
Aware	The following should be logged and reportable on servers: • all network log-on attempts whether successful or not; • log-offs; • creation, deletion or alteration of network privileges; • creation, deletion or alteration of network passwords. Use of application and database server administrative facilities. Typical Recording Profile is **A**.
Deter	As **Aware**, plus: Alert all multiple log-on failures resulting in account lock-out. Logging and capture of all accountable transaction summaries. Typical Recording Profile is **B**.
Detect & Resist	As **Deter**, plus: Logging of all network commands. The following captured from workstation logs: • all local log-on attempts whether successful or not; • log-offs; • creation, deletion or alteration of workstation privileges; • creation, deletion or alteration of workstation passwords. Typical Recording Profile is **C**.
Defend	As **Detect & Resist**, plus: Logging and capture of all accountable transaction request and response contents. Logging and capture of all workstation commands. Typical Recording Profile is **D**.

PMC7 - Recording of session activity by user and workstation (continued)

Accounting Recommendations (items in **Bold** text are defined in Appendix C)				
Index	**Recordable Events**	**Typical Accounting Items (plus PMC1 time-stamp)**	**Report**	**Alert**
1.	User network sessions.	**User**, **Host**, **Domain**, **Session** and **Status(1)** of session attempt	**A**	
2.	User network account status change.	**User**, **Domain** and account **Status(9)** (no password details)	**A**	
3.	Changes to network user privileges and user group status and membership.	**User**, **Host**, **Domain**, **Administrator** or **Process, Session**, **Domain**, **User(s) or Group**, **Privilege details and** change **Action(2)**	**A**	
4.	Use of any application or database administrative facility.	**Host**, **Domain**, **Administrator** or **Process, Session**, **Application(2)**, **Action(3)** and **Result(1)** details.	**A**	
5.	User network account status changes to locked-out state should be alerted.	Includes **Log** reference to corresponding Event 3. report.		**B**
6.	Change in privilege level status of a user on a server or critical workstation.	**User**, **Host**, **Domain**, **Session** and privilege level **Status(10)**	**B**	
7.	Invocation of any accountable user transaction (including interactions with applications and database servers).	**User**, **Host**, **Domain**, **Session**, **Application(2)** and transaction **Action(3)** and **Result(1)** details	**B**	
8.	Local user sessions on critical workstations.	**User**, **Host**, **Session** and **Status(1)** of session attempt	**C**	
9.	Local user account status change on critical workstations should be logged and reportable.	**User**, **Host** and account **Status(9)** (no password details)	**C**	
10.	Changes to critical workstation user accounts and group membership or status.	**Administrator** or **Process, Session, Host, User(s) or Group, Privilege** details and change **Action(2)**	**C**	
11.	Running of all network commands and executables.	**User**, **Host**, **Domain**, **Session**, **Command** and **Result(1)** details	**C**	
12.	Enhancement to Event 7. records to include transaction contents.	Same as Event 7, plus **Content(2)** of transaction.	**D**	
13.	Running of all critical workstation commands and executables.	**User**, **Host**, **Session**, **Command** and **Result(1)** details	**D**	

PMC8 - Recording of data backup status

Control Description	
To provide a means by which previous know working states of information assets can be identified and recovered from in the event that either their integrity or availability is compromised. Providing and audit trail of backup and recovery operations is essential part of the backup process and will enable identification of the most reliable source of the prior know good states of the information assets to be recovered in the event of data corruption, deletion or loss. The need for more sophisticated backup and recovery facilities are generally driven by higher levels of risk to **Integrity** and **Availability** properties. There is a complimentary requirement for online storage failure events to be alerted, this is met by **PMC4** Recordable Event 1 (the detection of any server storage failure should be classed as an alertable **Critical** event).	
Segmentation Model Recommendations	
Aware	All backup, test (verify) and recovery operations should be logged and reportable including completion status. Failure of operation completion should be an alertable event. Typical Recording Profile is **A**.
Deter	As **Aware,** plus: Typical Recording Profile is **A**.
Detect & Resist	As **Deter**, plus: A comprehensive online catalogue of the composition of all backup, test and recovery operations should be maintained including automated cross-reference to media library or storage allocation. Typical Recording Profile is **C**.
Defend	As **Detect & Resist**, plus: The media library or physical storage allocation can be expected to span multiple sites and recovery should be resolvable to any of those sites. File version control should be supported, allowing rollback to previous versions. Typical Recording Profile is **D**.

PMC8 - Recording of data backup status (continued)

Index	Recordable Events	Accounting Recommendations (items in **Bold** text are defined in Appendix C) Typical Accounting Items (plus PMC1 time-stamp)	Report	Alert
1.	Backup, test and recovery operations.	**Operation** parameter, **Media** reference and **Results** status	**A**	
2.	Backup, test and recovery operation failures should be alerted.	Includes **Log** reference to corresponding Event 1. report.		**A**
3.	Enhancement of Event 1. records to include operation file catalogue details.	Same as Event 1, plus **Catalogue** and per file: **File**, **Path**, **Host**, **Attributes** or **ACL**(s) and **Volume** reference	**C**	
4.	Enhancement of Event 3. records to include site reference and version information.	Same as Event 3, plus **Site(1)** reference of media store and **Catalogue** entries include file **Version(3)** information	**D**	

PMC9 - Alerting critical events

Control Description
To allow critical classes of events to be notified in as close to real-time as is achievable. The aware level requirement is for console based alerts that can be watched for by duty Security Managers. It would be expected that extensive projects (with continuous monitoring requirement) would require a Security Operations Centre with summary wall displays (with the most complex scenario implementing redundant monitoring centres). It should be noted that alerts themselves are recordable events. Smaller projects can have a solution to fit their size and would typically only require a profile **A** solution with simple monitoring facilities (a Security Manager workstation). Smaller projects may also consider combination of functions (e.g. security and network management) provided this does not conflict with segregation requirements. Secondary alerting channels may also be supported for projects that cannot provide continuous console manning (e.g. SNMP, email, SMS, etc.) via either in hours or out of hours services.

Segmentation Model Recommendations	
Aware	A summary alert message can be displayed on dedicated Security Manager console(s) that reflects all or part of the associated log message(s). Display of alerts of the same type occurring closely in time and consecutively should be throttled and aggregated into grouped alerts. Typical Recording Profile is **A**.
Deter	As **Aware**, plus: Any secondary alert channel should not contain information useful to an attacker and should provide a reference to corresponding log entries. All alerts should be configurable and tuneable items. Typical Recording Profile is **B**.
Detect & Resist	As **Deter**, plus: Aggregation of alerts from multiple streams can rendered as a graphical representation on Security Operations Centre wall displays. Such alerts must not reveal sensitive information and should be typically limited to "traffic light" status information. Typical Recording Profile is **C**.
Defend	As **Detect and Resist,** plus: It would be expected that there are multiple monitoring points at two different sites or more (although standby facilities may be "lights out"). Typical Recording Profile is **D**.

PMC9 - Alerting critical events (continued)

Index	Recordable Events	Accounting Recommendations (items in **Bold** text are defined in Appendix C) Typical Accounting Items (plus PMC1 time-stamp)	Report	Alert
1.	Alert messages routed to Security Manager console(s).	Alert **Message** content, **Log** reference, **Criticality, Count** of aggregated alerts and **Console** to which sent	**A**	**A**
2.	Simple alert notifications sent via secondary channels (email, SMS, pager, etc.).	**Log** reference, **Criticality** and **Channel(2)** to which sent	**B**	**B**
3.	Configuration changes of alerts and secondary alerts.	**Administrator** or **Process, Session, Domain, Message** class, **Alert** options and **Status(11)**	**B**	
4.	Graphical display of alert streams on consoles or wall displays.	Examples include (any or all of): • Device alert **Criticality** status overlaid in appropriate **Position**s over a network schematic or geographic map • **Statistic**s presented in graph form • **Dashboard** to provide a helpdesk-like display.		**C**
5.	Enhancement of Event 1. reports to include multi-casting of alerts to several sites.	Same as Event 1, plus **Site(2)** list to which alerts are copied	**D**	

PMC10 - Reporting on the status of the audit system

Control Description	
To support means by which the integrity status of the collected accounting data can be verified. The Aware segment requirements comprise the need to inspect log status on end devices and alerting of log error or other security relevant conditions. Upper segment requirements expand to include the requirement for log collection and query systems (ultimately served as a resilient solution). Smaller (especially single location) projects can have a solution to fit their size and would typically only require a profile level **A** solution without log collection facilities (perhaps assisted by COTS log analysis tools).	
Segmentation Model Recommendations	
Aware	Provide information on device log status. Alert log resets, error conditions, failures and threshold exceptions. Typical Recording Profile is **A**.
Deter	As **Aware**, plus: Provide a log collection facility with filtering capability. Record automated log file rotation and collection actions. Provide statistics on each log file collection within the accounting database. Typical Recording Profile is **B**.
Detect & Resist	As **Deter**, plus: Provide log collection integrity checks. To be able to produce a log file extract with integrity check. Provide an accounting data archiving facility. Allow report query across online and (selectively retrieved) offline accounting data. Typical Recording Profile is **C**.
Defend	As **Detect & Resist**, plus: Where Availability requirement is in excess of IL5: support redundant collection paths and a resilient accounting data repository. Typical Recording Profile is **C**.

PMC10 - Reporting on the status of the audit system (continued)

Accounting Recommendations (items in **Bold** text are defined in Appendix C)				
Index	**Recordable Events**	**Typical Accounting Items (plus PMC1 time-stamp)**	**Report**	**Alert**
1.	Log resets, error conditions, failures and threshold exceptions.	**Device** on which log operation, **File** identifier of active log file and log **Status**	**A**	**A**
2.	Query of status of active log storage on all devices on which logs are kept either locally or centrally.	**Device** that is queried, space **Allocated**, **Used**, **Free** and active **Records** count	**A**	
3.	Optionally provide a time record of Event 2. information, displaying trends.	Event 2 information presented in graphical form over time	**B**	
4.	Enhancement to Event 2. records to include log rotation information.	Same as Event 2, plus **Segment** details of new file[1] and **Size(2)** of segment file	**B**	
5.	Movement of segments and messages along the log collection chain. Message time-stamps should not be superseded.	Each part of the chain adds: **Source** of the original, **Handler** identifier of this part of the chain, **Segment** or **Message** files propagated and **Count** plus **Hash** of propagated files	**B**	
6.	Query at central collector(s) to provide a report of log sources.	Query over a time window of: **Source** list of log sources, transmission **Chain**, message **Count** and **Size(2)** of transmission details	**B**	
7.	Optionally provide a time record of Event 5. in graphical form, displaying trends over time.	Event 5 information presented in graphical form over time	**B**	
8.	Integrity checks failures at any point in the log handing chain.	**Segment** or **Message** involved in propagation attempt, **Source** identifier of origin, **Handler** identifier that reports failure, **Hash** (if applicable) and **Reason** for failure	**C**	**C**
9.	Log access query requests including requests for production of log extracts.	**User, Device, Command** used to issue request (as applicable: **File** to which extract made, **Signature** applied to file and **Result(1)**)	**C**	
10.	The central collector(s) should be able to query the online and selectively retrieved archive accounting data[2]	An ad-hoc query facility should be provided to allow the format of report and query parameters to be flexibly defined across the entire accounting data model.	**C**	

[1] Log segment files should be made read-only to all users.

[2] It is assumed archive data will be managed via a backup and restore facility (refer to **PMC8** for recommended requirements).

PMC11 - Production of sanitised and statistical management reports

Control Description	
To provide management feedback on the performance of the protective monitoring system in regard of audit, detection and investigation of information security incidents.	
Segmentation Model Recommendations	
Aware	Management reports will typically be prepared outside of framework using office automation tools and rely on manually updated statistics. Reports which include log extracts (etc.) must be sanitised and have identifying and sensitive information removed (including, but not limited to, User identifiers, workstation identifiers and IP addresses). Some devices may be capable of producing web reports. These will also need to be sanitised if used for management reporting purposes.
Deter	As **Aware**, plus: If external MSSP services are used they may include customer tailored reports, which can be directly used for management purposes. Assuming the content of these can be negotiated or configured, they may be used directly. One benefit of MSSP reports is that it may be possible to compare experiences against their pan-customer profile of security events (etc.) to provide a broader perspective of events and trends.
Detect & Resist	As **Deter**, plus: At this segment, for medium to large projects, it would be expected that an enterprise solution would be deployed (e.g. Security Information and Event Management system (SIEM) or IDS/IPS). These systems typically include reporting facilities. They may also include an audit / compliance check / investigation scheduling facility and support tools. Output of these reports needs to be sanitised as per **Aware**.
Defend	As **Detect & Resist**, plus: This segment may well deploy "defence in depth" with different defence tools from different vendors. Management output may be drawn from all available sources, but there will be the need for a certain degree of manual correlation between reports. It is unlikely there will be any high degree of correspondence or interoperability between the reporting facilities provided by different vendors as there are no international standards at this level. Output of these reports needs to be sanitised as per **Aware**.

PMC11 - Production of sanitised and statistical management reports (continued)

Accounting Recommendations
Exact report content requirements needs to be agreed with management and it needs to be ensured that the contents are readily digestible by the target community. The objectives of such reporting are to: • Promulgate awareness of the current information security situation to management and staff; • Demonstrate the ongoing contribution and return on investment of Protective Monitoring services deployed on a project; • Support business cases for improvement; • Provide evidence for IA capability maturity assessment. All reports need to be designed with this in mind. Examples of appropriate content for management reports includes: • Trends of attacks over current period plus history; • Performance of detection and defence mechanisms (including percentage ratio of: real alerts / (real + false alerts)); • Rolling "top 10" attacks experienced; • Geographic representation of where the attacks are coming from; • Statistics on internal violations; • Sanitised summaries of significant ongoing events or investigations; • Summary of current audit and compliance check results. These will be combined with information from other sources (e.g. SIEM system) to provide a complete information security status report. Due to the broad range of outputs possible no Accounting Recommendations table is provided for this risk treatment. Requirements for management reports will largely dictated by the technology adopted for any given project. The more advanced log management and SIEMs can be expected to provide report tem-plating as well as a series of proforma reports. It is possible that some tools will support multiple purposes and can provide support for: • information security incident management; • computer forensic investigations; In these cases they should be able to provide complete information security status reports.

PMC12 - Providing a legal framework for Protective Monitoring activities

Control Description	
To ensure that all monitoring and interception of communications is conducted lawfully and that accounting data collected by the system is treated as a sensitive information asset in its own right. The most significant aspect of ensuring Protective Monitoring is lawful is ensuring that it is justified. A major part of the evidence for that justification is that the risk management process ensures there is neither too much nor too little. There are certain aspects of user consent that need to be recorded as part of the system implementation. As for the other treatments the degree of rigour and trust in these increased along the scale of increasing segment. It is important to seek legal advice on compliance with the law and wording of all related screen messages and documents. Online electronic sign up may also be supplemented, or alternatively replaced, by manual records of user agreements and monitoring policies.	
Segmentation Model Recommendations	
Aware	At this level the recording of user logon captured by risk treatment **PMC7** Recordable Event 1. satisfies the requirement. This predicates that the system includes a logon warning screen that requires acknowledgement and/or consent of monitoring. There is no additional Recording Profile.
Deter	As **Aware**, plus: Can be augmented by a specific electronic "sign up" to a terms and conditions document presented before or after first user logon (and repeated following every update to the terms and conditions). This can provide a more detailed approach and include more specific information regarding monitoring activities. For this segment the user would be expected to "click" on buttons marked **[I Accept]** or **[I Decline]**, or similar. A positive action is required to record consent. Typical Recording Profile is **B**.
Detect & Resist	As **Deter**, plus: For systems with a raised degree of trust (**Integrity** impact is IL4) user consent can be recorded by a digital signature (at this segment, software generated and protected by a passphrase). Consideration should also be given for the issuing of frequent reminders or requiring regular re-affirmation. Monitoring conditions should be included in the relevant Certificate Policy. Typical Recording Profile is **C**.
Defend	As **Detect & Resist**, plus: For systems with the ultimate degree of trust (**Integrity** impact is IL5+) user consent can be recorded by a digital signature (at this segment, hardware generated, i.e. protected by a smartcard or token). Re-affirmation should be implied by all authorisation transactions and use of the credentials by the user. Typical Recording Profile is **D**.

PMC12 - Providing a legal framework for Protective Monitoring activities (continued)

Index	Recordable Events	Accounting Recommendations (items in **Bold** text are defined in Appendix C) Typical Accounting Items (plus PMC1 time-stamp)	Report	Alert
1.	User sign up operations.	**User** identifier involved, **Workstation** on which sign-up occurred, **Version(4)** of displayed terms and conditions and **Reply** of user: accept, decline, etc.	**B**	
2.	It should be possible to configure alerts for user sign up refusals[3].	Includes **Log** reference to corresponding Event 1. report.		**B**
3.	Enhancement to Event 1. reports to include a user digital signature[4]. Log records should also be recorded for each re-affirmation.	Same as Event 1, plus **Signature** associated with used sign-up response	**C**	
4.	Enhancement to Event 3. reports to include a hardware token or smartcard reference. Log records should also be recorded for authorisation transaction involving that user.	Same as Event 3, plus **Identity** of token or smartcard credential associated with sign-up response	**D**	

[3] Refusal may also prevent the user completing logon or suspend their account (such functionality is not within the scope of this Guide).

[4] There are other processes involved in supporting the issue and maintenance of digital credentials that are beyond the scope of the Guide.

Appendix C - Accounting Items

Key Principles

- Protective Monitoring needs to be supported by accounting data that provides adequate level of recording of information to support the reports and alerts associated with recordable events to be produced and the investigation of potential information security incidents
- The Appendix acts as a full catalogue of the types of accounting data that can be collected to support the Protective Monitoring Controls (PMCs) and the potential sources from which it can be gathered

Introduction

The Accounting Items are highlighted in **Bold** within the Recordable Events tables for each PMC defined in detail in Appendix B. This Appendix provides a table below to catalogue those items and suggest possible content and sources for those items. The list of **Possible Sources** listed in this appendix are also supported by Appendix D, which lists the technologies and techniques that are in common use at the time of the preparation of this Guide.

Definitions Table

Item	Definition	Possible Sources
Access	Type of access attempted to a file (typically: open, create, read, write, rename or delete).	Operating system
ACL	File or path Access Control List.	Operating system
Action(1)	Description of manual or automatic action taken in response to an attack.	Security Information and Event Management systems (SIEM), Network Behaviour Analysis (NBA) or Intrusion Detection System (IDS: manual), Intrusion Prevention System (IPS: automatic or manual)
Action(2)	Description of action in respect of privilege management: create, change, grant or revoke.	Operating system, Domain controller, Directory server or Management console systems

Item	Definition	Possible Sources
Action(3)	Description of action in respect of accountable transactions at the application layer (this can be an application raw command or request/response summary without full content).	Application servers, Database servers, Email servers, etc.
Administrator	User identifier of a privileged System Manager.	Local operating system, Domain controllers, Directory servers, Network equipment or Management console systems
After	Status of a file or configuration item after change.	Operating system
Agent	Host identifier on which an SIEM, NBA, IDS or IPS agent is installed.	Name service, Dynamic Host Configuration Protocol (DHCP) server
Alert	Configuration options for a specific alert.	SIEM, NBA, IDS or IPS, Network management system or Other management console systems
Allocated	Space allocated for logging on a device.	Operating system, Network management system or Other management console systems
Application(1)	Name of application stream malware detected in (File Transfer Protocol (FTP), Simple Mail Transport Protocol (SMTP), HyperText Transport Protocol (HTTP), etc.)	Anti-malware boundary check
Application(2)	Name of the transaction based application, application server or database server.	Application servers, Database servers, Email servers, etc.
Attack	Description of an attack type (readable).	SIEM, NBA, IPS or IDS
Attributes	Attributes, metadata or significant properties associated within a file in a file system (e.g. read-only, hidden, system file, author, etc.)	Operating system, Backup management system, Media library system or Version control system
Before	Status of a file or configuration item before change.	Operating system journaling or Shadow copies

Item	Definition	Possible Sources
Catalogue	Catalogue of a backup operation (including an inventory of files backed up and individual file backup omissions or failures). Each record will include complete file details. This information may be retained online, even if the associated files have been archived.	Operating system, Backup management system or Media library system
Chain	Transmission chain of a log file to the ultimate collectors.	Log relay or collector
Channel(1)	IEEE 802 protocol and channel that a wireless device is detected on.	Wireless IDS (WIDS), Wireless LAN (WLAN) probe, Operating system or Network management system
Channel(2)	Channel identifier on which secondary alerts are delivered (SMS, email, pager, etc.).	Network management system, SIEM, NBA, IDS, IPS or other management console systems
Command	Command issued to a device (including options).	Operating system
Console	Identifier of a console terminal.	Name service, Domain controllers or Directory servers
Content(1)	Complete file contents.	Proxy server, De-Militarised Zone (DMZ) server or Operating system
Content(2)	Complete transaction contents (request and response).	Application servers, Database servers, Email servers, etc.
Count	Count of records within individual log segments and aggregated logs passing along a log handling chain.	Log relay or collector
Credential	User remote access credential identifier.	Remote Authentication Dial In User Service (RADIUS) or other remote access server
Critical	Class of log message implying critical condition.	Operating system

Item	Definition	Possible Sources
Criticality	Criticality of a log message or alert (**Critical**, **Error**, **Warning**, etc.).	Operating system, Anti-malware boundary check, Anti-malware software, Device logs, Simple Network Management Protocol (SNMP) traps, Firewalls, SIEM, NBA, IDS, IPS, Network management system or Other management console systems
Dashboard	Graphical presentation of the top level key system status and performance level indicators. These will typically support "drill down" to allow inspection of underlying data and related events.	SIEM, NBA, IDS, IPS, Network management system, Other management console systems, Reporting tools or Office automation software
Data	Data payload within a packet.	Firewall, Host network interface or Packet sniffer
Date	Date (preferably stored referenced to UTC).	Operating system, Network Time Protocol (NTP) server or UK atomic clock
Detail	Any other information associated with an attack.	SIEM, NBA, IPS or IDS
Device	Identifier of a network device (router or switch).	Name service or DHCP server
Direction	Direction which malware detected (inbound or outbound)	Anti-malware boundary check
Domain	User logon domain identifier.	Operating system, Domain controller or Directory servers
Error	Class of log message implying non-critical error condition.	Operating system
File	File identifier within a file system (filename only).	Operating system
Firewall	Unique firewall identifier (name or IP).	Firewall or Firewall console
Free	Space remaining within the allocated log space.	Operating system, Network management system or Other management console systems

Item	Definition	Possible Sources
Graphic	Accounting information presented in graphical form (including graphs, histograms, pie-charts, topological or geographic overlays, etc.)	SIEM, NBA, IDS, IPS, Network management system, Other management console systems, Reporting tools or Office automation software
Group	User group identifier.	Operating system, Domain controller or Directory servers
Handler	Device identifier of a log handler within a log collection system (may be either a relay or collector).	Log collector or relay
Hash	Cryptographic hash or message authentication check for a transmitted file or other binary object (SHA-256 recommended).	Operating system, Log collector agent, Log relay or Log collector
Header	IP packet header (including all significant fields: Protocol, IP source, IP destination, source port, destination port).	Firewall, Router/Switch, Host network interface or Packet sniffer
Host	Identifier of a network host (typically workstation or server).	Local operating system, Name service, Domain controllers, Directory servers or DHCP server
Identity	Identifier of token used to support identity, authentication and authorisation (e.g. token serial number, smartcard identifier, etc.)	Remote access server, Smartcard drivers or Operating system
Information	Information relating to the version of new and original software components.	Operating system install manager
Interface	Identifier of network interface on a firewall.	Firewall or Firewall console
Inventory	Inventory of software components (files) within a package.	Operating system install manager
Location	Triangulated location of a detected active wireless device.	WIDS

Item	Definition	Possible Sources
Log	Reference to a log entry by an alert.	Operating system, Network management system, Anti-malware boundary check, Anti-malware software, SIEM, NBA, IDS, IPS, Firewalls or Other management console systems
MAC	Device IEEE 802 Media Access Control (MAC) address of its communicating network interface (some devices may be dual- or multi- homed and have multiple addresses).	DHCP server, Address Resolution Protocol (ARP), Operating system, Network equipment or Network management system
Malware	Identifying name of malware infection (proprietary or open).	Anti-malware boundary check or Anti-malware software
Media	Identification of media or storage used for a backup or electronic archive operation.	Operating system, Backup management system or Media library system
Message	Message content included in log messages (etc.). May also be parsed to extract further Accounting Items. Usually these are unstructured and in text form. However, for SNMP based messages they will be structured and conform to a defined Management Information Base (MIB) format specific to the device or agent producing them. Some messages may also be in HTML format, be structured XML data or flat lists of "comma separated variables".	Operating system, Device logs, SNMP traps, Firewalls, SIEM, NBA, IDS, IPS, Network management system or Other management console systems
Node	Identifier of a remote attached VPN subnet	Virtual Private Network (VPN) router, Name service or DHCP server
Operation	Operation and complete parameters used for backup, test (verify) or recovery.	Operating system, Backup management system or Media library system
Package	Software package identifier.	Operating system

Item	Definition	Possible Sources
Patch	Software patch package identifier.	Operating system
Path	Path to where a file is stored.	Operating system
Point	Physical network access point identifier.	Network equipment or Network management system
Position	Position of a device within a topological or geographic graphical presentation.	SIEM, NBA, IDS, IPS, Network management system, Other management console systems, Reporting tools or Office automation software
Privilege	Operating system privilege identifier.	Operating system, Directory servers or Management console systems
Probe	Identifier of an IDS or IPS probe.	SIEM, NBA, IPS or IDS
Process	Software process identifier.	Operating system
Reason	Reason that an access attempt fails.	Web proxy, Web content scanner or Operating system
Reply	Recorded user reply to agreement of terms and conditions of access to ICT: accept, reject, etc.	Operating system, Logon scripting or Specialist "e-signing" applications
Response	Response returned from a device (including code and readable).	Operating system
Result(1)	Outcome of a transaction or command request (success or failure, with any extended result code, including human readable form).	Operating system, Application servers, Database servers, Email servers, etc.
Result(2)	Outcome of a log extract exercise (including reference to parameters used for the extract and the status).	Operating system, SIEM, Log collector, Backup management system or Media library system
Rights	File or path access rights.	Operating system
Rule	Rule included within firewall rule-base (readable).	Firewall or Firewall console
Security Label	Security label attached to a file (e.g. protective marking)	Trusted operating system, trusted email extension

Item	Definition	Possible Sources
Segment	Log segment file produced by a log rotation system (provides files of manageable size and also facilitates protection and collection). Each file holds a collection of log messages.	Operating system
Session	Session identifier associated with a user or process.	Operating system
Signature	Digital signature (applied as record of a user authorisation to support various trusted activities: implies requirement for PKI support)	Trusted email extension or client, Trusted web application, Operating system, Computer forensic tools, Log collectors, Media library system, Specialist "e-signing" applications
Site(1)	Site reference to where a backup archive is stored (or system identifier of the archive system).	Backup management system, Media library system or Version control system
Site(2)	Site reference within lists for multi-casting of alerts.	SIEM, NBA, IPS, IDS, Network management system or Other management console systems
Size(1)	IP packet size.	Firewall, Router/Switch, Host network interface or Packet sniffer
Size(2)	Log segment file size.	Operating system, Log relay or Log collector
Source	Source of a suspected attack (including subnets).	SIEM, NBA, IPS or IDS
Statistics	Output of either automatic or manual numerical analysis. Typically presented as a table of key performance indicators. May also be accompanied by colour coding or other graphic (e.g. "traffic lights", "thermometers", etc.).	SIEM, NBA, IPS, IDS, Network management system, Other management console systems, Reporting tools or Office automation software
Status(1)	Session status (logged in, logged out, disconnected, timed out etc.).	Operating system, Remote access server, Domain controller or Directory service

Item	Definition	Possible Sources
Status(2)	Host status (started, shutdown, etc.).	Operating system or Network management system
Status(3)	Attached device status (attached, detached, disabled, etc.).	Operating system
Status(4)	Volume status (mount, dismount, etc.).	Operating system, Domain controller or Directory servers
Status(5)	Software package or patch configuration status (installed, removed, etc.).	Operating system or Version control system
Status(6)	Process status (started, stopped, suspended, resumed, etc.).	Operating system
Status(7)	VPN node status (attached, detached, timed out etc.).	VPN router, VPN controller, Operating system or Network management system
Status(8)	Wireless node status (attached, detached, timed out etc.).	Wireless access point, Operating system or Network management system
Status(9)	User account status (logon, logoff, timeout, enabled, disabled, etc.).	Operating system, Domain controller or Directory servers
Status(10)	Privilege level status (normal, superuser, etc.).	Operating system, Domain controller or Directory servers
Status(11)	Status of logging functions.	Operating system, Log relay or Log collector
Target	Target of a suspected attack (including subnets).	SIEM, NBA, IPS or IDS
Time	Time (preferably stored in UTC).	Operating system, NTP server or UK atomic clock
Time to Live	Elapsed time before cache item expiry.	Web cache
URL	Universal resource locator - web page address.	Web servers, Domain name service or Internet
Used	Space occupied by active logs and other retained segments within the allocated space.	Operating system, Network management system or Other management console systems

Item	Definition	Possible Sources
User	Unique user identity.	Local operating system, Domain controllers, Directory servers or Remote access servers
Version(1)	Version identifier of malware or attack recognition signature base.	Anti-malware boundary check, Anti-malware software or SIEM, NBA, IDS or IPS
Version(2)	Version identifier of software.	System file lock-down or Version control system
Version(3)	Version identifier of file.	Journaling operating system, Version control system or Backup management system
Version(4)	Version of user sign-up terms and conditions (e.g. Acceptable Use Policy, SyOPs, etc.).	Online documentation
Volume	Mountable storage volume identifier.	Operating system
VPN	Identifier and characteristics of a VPN net.	VPN router or controller
Warning	Class of log message implying (non-error) warning condition.	Operating system
WLAN	The identity of a Wireless LAN, typically parameters such as the Service Set Identifier (SSID) or MAC of the associated Wireless Access Point.	Wireless access point, Operating system or Network management system
Workstation	Logical workstation identifier.	Local operating system, Name service, Domain controllers, Directory servers or DHCP server

Table C-1 - Accounting Items Definitions

Appendix D – Technology and Assurance Overview

Key Principles

- There are many proprietary products that can assist in automation of elements of Protective Monitoring and that can facilitate identification of security policy violations in near real-time. There are usually log recording facilities in even the most basic ICT systems. It is important that these technologies, and their limitations, are correctly understood and utilised in order to provide an effective Protective Monitoring framework
- In systems requiring high degrees of trust it is also important to have confidence in the effectiveness of the technical Protective Monitoring mechanisms. This means application of the CESG Assurance Matrix and Framework to those mechanisms in order that they will be effectively assured as part of the whole-life accreditation process

Introduction

1. This Appendix provides an overview of the state of the art regarding the techniques and technology that can be applied to meet the Protective Monitoring requirements and then demonstrates how those can be assured within an overall solution architecture. This Appendix is provided as current at the time of preparation of this Guide. This information also supplements the definitions of Accounting Items given in Appendix C to provide further information on the Possible Sources of accounting data. It is intended to neither mandate nor prescribe particular technologies to be used on any project. Rather it is intended to provide guidance on the technologies and techniques that can be usefully deployed. These can be implemented with differing balances of automation and manual effort to allow the full spectrum of scenarios, from simple single system projects through to cross-enterprise strategic initiatives.

Techniques and Technology

2. Technology trends are in a constant state of development and progress, and it is expected that the information provided here will gradually become out of date. Projects should appraise themselves of the latest technologies and techniques in use during their development to ensure that the latest good practices can be adopted. The following paragraphs provide description of the main categories of technology and techniques that can form part of an Protective Monitoring solution. This Appendix goes on to present the main types of techniques and technology that can be deployed within those scenarios to deliver Protective Monitoring requirements. It covers:

    a. Intrinsic sources of log data within the components of typical architectures;

b. Techniques for monitoring those logs;

c. Tools to assist with log audit activities;

d. Integrated Security Information and Event Management (SIEM) systems;

e. Behaviour analysis systems;

f. Intrusion detection and prevention systems (IDS/IPS).

Intrinsic Log Sources

3. Many components of ICT systems including logging in some form or another (summarised in Table D-1 on page 99). Some components may also be able to raise alert messages, either as proprietary alert messages or as SNMP traps sent to a network management system. These may also be of relevance to the Monitoring process, if those alerts:

   a. Can be directly associated with likely security policy violations;

   b. Otherwise indicative of suspicious activity or anomalous behaviour;

   c. Provide information on the health of Protective Monitoring mechanisms (e.g. storage alerts);

   d. Contribute to the picture of normal system behaviour.

4. The use of system components for logs and alerts raises some challenges and has some limitations:

   a. They are usually only in a proprietary format and may contain information that is difficult to extract for Protective Monitoring purposes;

   b. They are not specifically designed for Protective Monitoring purposes and contain much "noise" that populates log files and needs to be filtered out by the collection process;

   c. The information they provide may fall well short of what is required for Protective Monitoring purposes;

   d. The degree to which they can be controlled, tuned and configured may be limited;

   e. Correlation of logs from different sources can be a time consuming and difficult activity.

5. It is for these reasons that relying on intrinsic logs alone is only practical for the simpler scenarios and even those can be greatly supported by the use of specific tools. The following paragraphs provide a summary of the typical availability of logs on particular component types.

Log Monitoring techniques

6. Figure D-1 on page 100 shows the activities involved in log monitoring activities. This diagram covers a scenario with a moderate degree of complexity where there are many log sources to be watched, perhaps extending over several sites, in which accounting information will be collected and relayed from original sources and held in a central repository.

7. The diagram highlights a number of techniques and activities that are either applied automatically or need to be considered in manual operational procedures. These include:

   a. Event generation;
   b. Alert generation;
   c. Event filtering;
   d. Event normalisation;
   e. Event parsing;
   f. Event relay and collection;
   g. Event correlation;
   h. Event analysis.

Event Generation

8. Devices that are capable of automatically recording security relevant events need to be configured to support, as closely as possible, the Accounting Requirements recommended in Appendix B. This will be in accordance with the selected Protective Monitoring Controls are their respective Recording Profile level (**A**, **B**, **C** or **D**), which are identified as part of the risk treatment activity.

9. It can be the case that the equipment alone does not gather sufficient information and, if the shortfall is significant, this may need to be augmented by manually kept records, e.g. operator logs. Operational procedures should be prepared that cover any requirements for manual recording and the means by which it can be incorporated within the overall Protective Monitoring processes. Devices that are capable of raising alerts may be able to contribute to real-time or near real-time monitoring.

Class	Types	Logging Capabilities
Servers	• Network Servers • Database Servers • Application Servers	• Provide a source of information regarding access to network resources hosted by server. • May conform to Controlled Access Protection Profile (CAPP) or better, if evaluated to EAL3 or above. • Are essential for tracking privileges and monitoring file system based access control. • May be supplemented by application level logging. • Log collection and analysis tools tend to be primitive. • Database and application servers may either use intrinsic server facilities or their own separate reporting mechanisms.
Clients	• Workstations • Laptops • Thin-clients • Portable Electronic Devices (PEDs)	• Often have similar capabilities to servers. • Are more likely to be subject of manipulation by an attacker. • Can generate logs while offline (especially for access to local resources). • May be of value for forensic analysis or local audit (requirement for collection of local logs would be atypical). • May provide logs and alerts relating to I/O attachments while connected to the network.
Authentication Services	• Domain Controllers • Directory Servers • Authentication Servers (Kerberos, RADIUS, TACACS, etc.)	• Provide source of records regarding network authentication attempts and failures. • May also provide information regarding sessions, privileged assignments, directory information, remote access and token use.
Network Components	• Routers • Switches • Network Management System (NMS) • DNS • DHCP • Wireless Access Points	• Can track network attachments, IP address mapping, wireless access and network health. • Typically have very low local log retention and often reliant upon proprietary add-on or SNMP based management infrastructure. • NMS output covers many events and requires filtering to select those that are security relevant.
Security Services	• Network Firewalls • Application Firewalls • Proxy Servers • Content Scanners • Anti-Malware • Guard Processors	• There are many proprietary products with vendor specified logging characteristics. • May support SNMP traps or other means of sending alerts. • Are essential for tracking and enumerating information regarding alerts raised within DMZs and for tracking boundary operations. • May support integration with NIDS.
Storage Management	• RAID Controllers • SAN Controllers • Backup Servers • Cache Servers	• Provide disposition of storage health and information protection status. • Can track movement of information between storage compartments and network boundaries. • Are essential to support incident recovery.

Table D-1 - Summary of Features of Intrinsic Log Sources

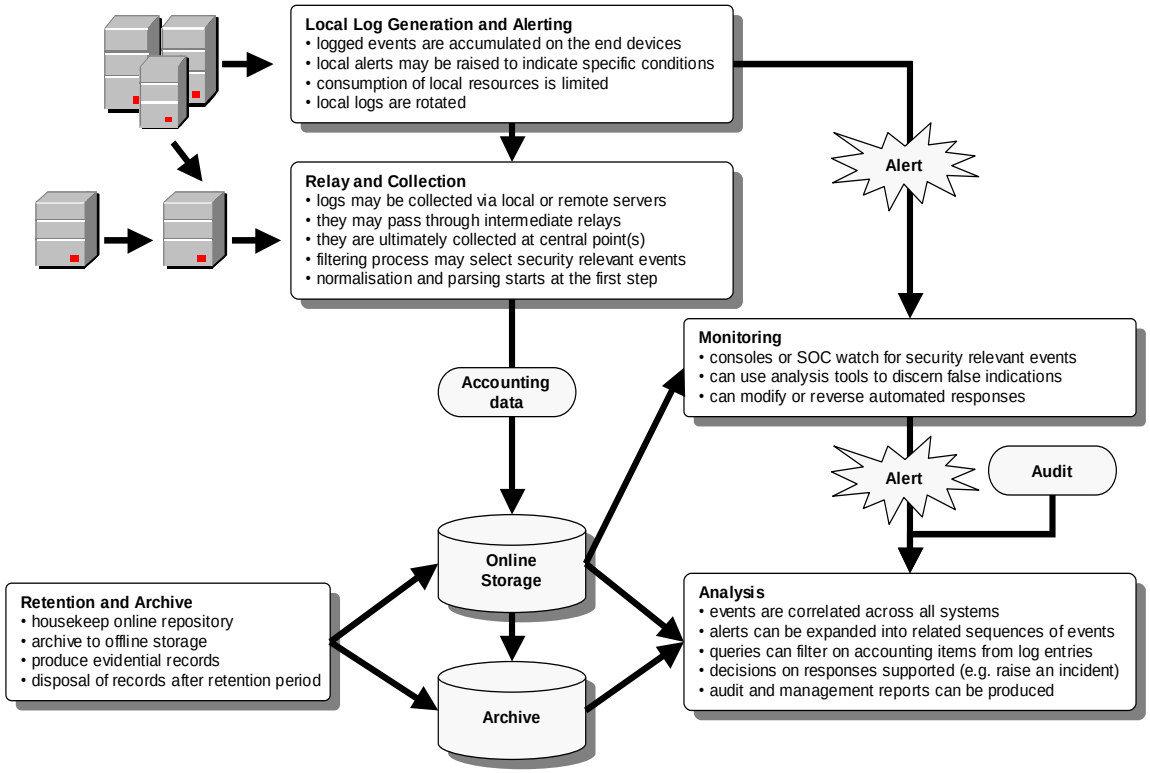

Figure D-1 – Log Monitoring Activities

Alert Generation

10. However:

    a. There are likely to be occasions when automatic alerts provide false positives or false negatives;

    b. The alerts do not by themselves indicate definite occurrence of security events;

    c. There are likely to be several classes of alertable events that cannot be generated automatically due to technology limitations.

11. As automatic alerting cannot be relied upon on its own, it needs to be augmented by all of the following:

    a. Training and awareness of System Users and Managers to be able to recognise and report unusual and suspicious online events;

    b. Consultation with experienced staff who are local to the alert;

c. Building up a historical knowledge database of activities and expected behaviour patterns to inform the current decision making process.

12. Operational procedures should cover alert recognition and confirmation.

Event Filtering

13. Filtering of recordable event records occurs in several ways:

    a. As part of the configuration of log settings on the end devices; these should be tuned to fulfil both system monitoring and security relevant monitoring;

    b. During the collection processes, in which only security relevant log entries are collected (filtering out other system monitoring requirements which may either remain local or are routed instead to a NMS);

    c. During the collation and analysis processes when queries are performed on the Accounting data.

14. In the absence of specialist tools that provide automated filtering or log query facilities, consideration needs to given as to how filtering might be performed manually. In simple cases it may be possible to rely on native ICT tools with limited search and query facilities (e.g. event managers and pattern matching search tools). But even on a system with only a few monitored devices, this is likely to make any audit activity extremely laborious, if not impossible. Regardless of whether filtering is performed automatically or manually, there should be adequate documentation that covers how it will be achieved.

Event Relay and Collection

15. Relay and collection of recordable events refers to the transport of records around a network. This can be considered a hierarchical system of record distribution which comprises:

    a. The source devices from which the records are to be collected;

    b. Relay devices specific to the site that collect records from all devices at that site;

    c. Central collector devices that collect records from all site relays and that store the collected records within an online Accounting database.

16. However, such complexity may not be present on simpler projects.

17. Such a hierarchical system of event record collection is enumerated in the de facto Syslog IP protocol, originally documented in RFC 3164 (The BSD Syslog Protocol, reference [r]) and recently updated in RFC 5424 (The Syslog Protocol,

reference [s]). Note that there are several proprietary conflicts in the various syslog implementations and significant vulnerabilities, these include:

a. Syslog messages (which are dispatched message by message) are transmitted using UDP which provides unreliable delivery;

b. Messages can be corrupted or lost in transit or they may arrive out of sequence;

c. Messages are limited to a maximum size and can be truncated;

d. Messages can easily be tampered with by a "man in the middle" attack to provide substitute or false entries;

e. Messages can be spoofed or malformed to exhaust the storage space of collectors, to hide illegitimate activity or cause a failure of the logging system;

f. Messages are transmitted in cleartext and can therefore be intercepted, and could provide an attacker with a wealth of useful information.

18. There are also Syslog implementations that conform to the newer RFC 3195 (Reliable Delivery for Syslog, reference [t]) that addresses several of these issues. Where projects are implementing Syslog then it is recommended the implementation should comply with both RFC 3164/5424 and 3195 and that the recommendations in paragraphs 19. and 20., following, are also applied. There are also several proprietary solutions for collecting event records and the passing of record messages that are based on alternative approaches to Syslog.

19. Some projects may also implement collection by a manual procedure rather than using automated tools. This may include copying source log files to computer media. Any event record collection system should be secure and be included in the IS1 & 2 and associated supplement (references [a] and [b]) risk management process as a distinct asset in its own right and be subject of appropriate technical risk treatment and other appropriate protective measures. Collected accounting information should be protected to at least the same level as the highest IL or protective marking of the data of the systems it is being collected from. In some cases, for reasons of aggregation, collected Accounting data should be treated as an information asset which has an IL or protective marking that is in excess of the individual systems from which it is being collected.

20. Accounting data in transit over electronic networks should be protected in accordance with its protective marking and related IS4 requirements (reference [p]). Accounting data at rest, or physically in transit, should be protected in accordance with its protective marking and other related SPF requirements

(reference [c]). All procedures relating to event collection should be documented in SyOPs.

Event Normalisation

21. In automated event collection systems normalisation is the process by which event messages and records based of different proprietary forms are converted into a single coherent format. This allows the records within the central Accounting data repository to be captured in a consistent form. Normalisation may happen by virtue of collection agents installed on a source device, or it can be performed on an intermediate (relay) or an ultimate collection device. Standalone tools can provide conversion of Accounting data from one format to another. However, there is no overall standard schema or data model for event records collected from ICT devices.

Event Parsing

22. Even normalised Accounting data yields limited information. The normalised form is typically the "lowest common denominator" amongst possible recording formats. For instance, normalised Syslog format includes the following:

    a. Time-stamp (date and time);

    b. Event code (for syslog this comprises a single number that represents "facility" raising the error and a "severity" indicator);

    c. Source (hostname or IP address raising the message);

    d. Process identifier (process name);

    e. Message text.

23. The message text provides the most informative part of the entry. It will also include any useful message parameters (e.g. the name of a file to which access was refused, the name of the user requesting the access, etc.). Parsing extracts the message parameters in order to help populate additional elements of the Accounting Items. The degree to which parsing can be done manually is limited: some messages are more human readable than others, and some require expert interpretation. There are proprietary tools which can automatically parse raw Accounting data and which have a broad degree of knowledge of the formats of system messages - even extending to messages generated by specific applications. There are software agents that by-pass the parsing issue by providing detailed event information that is prepared in the specific format required. There are also other logging methods in which the end device or intermediate devices provide information in more structured formats (e.g. by the use of SNMPv3 Management Information Blocks or XML format log records).

Event Correlation

24. Correlation is the process of assembling recordable events in sets of related sequences across different devices. Often an initial user action will trigger a whole series of recordable events. For example, a System Manager creating a new user account will create a series of recordable events including the System Manager logging on, requesting an account creation function, from which in turn a number of automatic actions may take place including creating a user authentication record of the domain server, population of a directory record for the user, creation of an associated email account, and so on. Event correlation also relates to the association of events with an alert message. Alert messages on their own can be quite deliberately uninformative and need to be linked to the event records with which they are associated to ascertain their true meaning and implications.

25. The event correlation process can be partially automated, but needs to be backed up by expert interpretation to confirm the event associations. This is the first step to deciding between events that have significant security implications and those that are "false positives". When there are only a few event sources it can still be practical to do event correlation purely manually by extracting events and aligning them on a timescale. Regardless of whether event correlation is manual or automated, the key to the process is the reporting integrity of all the attached devices. Clock synchronisation is a key element as related events should closely correspond in time - at least for short duration transactions. Even with automated collection, issues can arise with cross-device sequences becoming scrambled because of different paths and transmission windows involved in the relay of the logs or log messages to the central repository of Accounting data.

Event Analysis

26. The event analysis process can be triggered in response to an alert or undertaken as part of an audit, spot-check or other routine investigation. Event analysis allows various enquires to be performed upon the Accounting data, which can include any of the following:

    a. Perform further checks to confirm events or alerts are genuinely indicative of security incidents worthy of further investigation and are not false alarms;

    b. Support investigations by data mining and research of (e.g.) the activities at specific end points, the activities of specific users over time, transactions involving specific resources, (etc.);

    c. Provide information for undertaking of compliance checks against specific aspects of online security policy;

d. Provide information for regularly assessing normal online behaviour (against which deviations can be measured);

e. Support application of expert knowledge to detect abnormal or unexpected patterns of behaviour that may indicate security incidents;

f. Provide information for the production of regular statistical results for inclusion in management reports;

g. Provide information for other reports that support housekeeping activities (e.g. producing lists of records that can be archived).

27. Event analysis needs to be focussed on the end products required for each activity (everything prior to event analysis has provided intermediate results that provide no useful function on their own).

Audit tools

28. Table D-2 on page 107 provides an overview of the classes of tools which are available to assist in audits, compliance reviews and incident investigations.

Security Information and Event Management (SIEM) systems

29. SIEM systems, which may also go under the title of Security Event Management (SEM) and Security Information Management (SIM) systems, can be provided by either single vendor or multiple vendors. SIEMs can also represent an aspiration: to have all significant information security delivered to selected Security Manager consoles. Consequently as well as being implemented as a truly integrated software suite it can also be implemented as a collection of separate tools working together and using a common display. SIEMs can be supported by proprietary agents that provide direct reporting from monitored systems and devices to central consoles, or they can be agent-less (having zero impact on the monitored systems and devices) and rely upon pre-existing open reporting mechanisms such as syslog or SNMP.

30. SIEMs typically include integrated log management; collection, analysis and reporting functions to provide a comprehensive log monitoring solution. All SIEMs provide a predefined list of supported hardware, software, open standards and protocols. Some SIEMs come with additional tools and modules to provide an integrated approach to information security management, typically including incident management, investigation support and computer forensic capabilities. There are no open standards with regard to what constitutes SIEM functionality or related Common Criteria Protection Profiles against which SIEMs can be assured. SIEMs can also include other modules with NBA/IDS/IPS capability or provide integration with third party products such as firewalls and network management systems.

Behaviour Analysis Systems

31. Behavioural analysis can be viewed as a discipline as opposed to a single automated system but there are many proprietary products that can provide a large degree of automation. Behavioural analysis systems use a combination of algorithmic, heuristic, "pattern matching" or "artificial intelligence" approaches to determine or "learn" normal behaviours and to then alert significant departures from those behaviours. These alerts can provide clues to potential system misuse or attacks. This contrasts with knowledge based intrusion detection products that use attack signature bases to more directly detect suspicious activity. However, some products are hybrids and include multiple forms of analysis. The advantage of behaviour analysis systems is that they can potentially detect previously unknown attacks that have not been included in the latest signature bases. Behavioural analysis systems are especially useful for identifying "malformed" or blatantly suspicious activity.

32. There is a need for human oversight of any such automated processes as they are particularly prone to "false positives" and "false negatives". "False positives" typically occur when there is a significant but legitimate variation from the traffic norm (e.g. a financial system may have a surge of activity for quarter and year end reporting periods). "False negatives" typically occur when an attack takes place that is subtle in nature or is deliberately disguised to coincide with normal use profiles. False negatives also occur due to "misdirection attacks" were the attacker manipulates the system to generate so many false alerts that the real attack goes unnoticed. It requires both local and specialist expertise to be involved in the decision making processes to be able to filter out the false indications and determine true suspicious activity worthy of investigation or action.

Tool Classes	Class Features
Log Collection	• Log collection systems automate the relay and collection of logs and log messages. • There are many implementation based on the syslog standards (RFC 3164/5424 and RFC 3195, references [q] and [r], refer to Appendix D paragraph 17.). • Syslog messages are also supported by many networking devices including routers and switches. • Other systems are based on proprietary log collection agents and others with linkage to network management systems (using SNMP traps).
Log Analysers	• Log analysers can supplement the functionality provided by limited operating system capabilities. • Log analysers will support log formats of various declared types (typically main stream operating systems). • Log analysers perform parsing to extract additional information from log messages and can provide limited degrees of collation of related events. • Log analysers can provide a number of different views of log data, including "drill down" activities related to a specific workstation, user, session, etc. • Log analysers can also perform graphical analysis showing trends over time. • Log analysers sometimes can also perform behaviour analysis to allow highlighting of suspicious activity (refer to Behaviour Analysis Systems sub-section following).
Filtering, Query and Pattern Matching Tools	• Filtering tools can be either general purpose or specific log filters. • Most filtering tools a query language or pattern matching "regular expressions" to allow selection of log records and messages either on the fly or as a log file query. • Filtering tools can be statically configured in the log pipeline to automatically limit records reaching the Accounting data store. • Filtering tools can be used with a user front end to provide a crude query tool to allow interrogation of the Accounting data store. • Filtering tools also provide a SQL or ODBC connectors to allow the Accounting store to be accessed as a database and enable output to be presented in electronic documents and web pages.
Reporting Tools	• Reporting tools provide further analysis and allow detailed graphical reports and front ends to the Accounting data to be built. • Reporting tools may include general purpose statistical and timeline analysis libraries to facilitate trends over time to be easily produced. • Reporting tools may support macro or programming languages to allow the addition of bespoke analysis elements to be added to reports. • Reporting tools can provide either static reports or dynamic "dashboard" displays that support structured and hierarchical linkages to the collated log records that make up the display, allowing "drill-down" to the underlying raw data. • Reporting tools can be useful for the partial or full automation of the production of management reports.
Computer Forensic Tools	• Computer forensic tools are specifically provided to aid capture and investigation of computer based evidence. • Computer forensic tools include a facility for imaging storage volumes and media. These images are check-pointed and can be verified as bona fide copies of the original at any point in the future. • Sophisticated analysis can be conducted on the read-only images in order to search both apparent and hidden data within the storage images. • Computer forensic tools can conduct searches for illicit content, reconstruct lost or damaged files and can often present files in the appropriate document viewers to allow a thorough examination how the storage has been put to use. • Computer forensic tools may be able to specifically detect tampering with log files as they can reconstruct audit trails of files that have been edited or replaced.
Network Management Systems	• Network management systems are typically used for activities beyond Protective Monitoring. • However, network management systems share many common requirements (including the capture of device messages). • Network management systems are also a useful point of reference, during investigations, as a source of network information and extended network logging that can supplement the picture under examination.

Table D-2 - Audit tool classes

33. There are several technologies and tools that fall into the behaviour analysis category. The most generally useful for ICT Auditing and Monitoring are Network Behaviour Analysis (NBA) systems that sample large volumes of network traffic at strategic points. NBA systems can work along side conventional IDS/IPS. There are also systems that are specific to particular applications, such as fraud detection systems, which monitor transaction patterns and provide alerts for any anomalies detected. These are typically supported by host agent software reporting back to a central analysis and management console system. Many Application Firewalls use a simple form of behaviour analysis. They are focussed on validating requests and responses in particular protocols (e.g. SOAP or SQL). They can catalogue and categorise received transactions overtime and then query any new types of transactions that appear, which can then be either blocked or allowed.

34. A shared characteristic of behaviour analysis systems is that they all require a learning period during which normal behaviours are profiled. During this phase the system initially requires intensive oversight, as each captured pattern will be initially alerted. Some may be deployed in a test or pilot phase during which alerts are suppressed to allow this learning to take place. However, this has an issue in that any artificiality of the behaviour profiles during the learning phase will mean that the exercise will not be fully effective, as when the system becomes exposed to true behaviours after the learning phase, these will be alerted. There are also tools that allow post-analysis of event logs or event log archives that can aid incident investigations or compliance review activities.

Intrusion Detection and Prevention Systems (IDS/IPS)

35. Intrusion Detection and Prevention Systems (IDS/IPS) are the most ubiquitous technology for providing automated attack monitoring and defence. Although individual firewalls provide a measure of intrusion detection, they are limited in that they only provide monitoring at a few discrete points and provide no detection of activity behind the firewalls, on the internal network. However, some IDS/IPS use firewalls as a source of attack information and some IPS provide attack response by automatically modifying firewalls rules on the attack path. But IDS/IPS also deploy other kinds or probes, sensors and agents to allow more comprehensive monitoring of the network infrastructure. IDS/IPS is also a group of technologies, including:

    a. Network Intrusion Detection Systems (NIDS);
    b. Host Intrusion Detection Systems (HIDS);
    c. Wireless Intrusion Detection Systems (WIDS);
    d. Intrusion Prevention Systems (IPS).

36. Some product families provide integrated approaches that can include all of these technology groups. Others specialise in particular groups.

Network Intrusion Detection Systems (NIDS)

37. NIDS rely on strategically placed independent network devices or "taps" that monitor network traffic ("taps" are typically placed on the "spanning ports" of enterprise network switches to allow them to view all traffic passing through the switch). Like firewalls NIDS directly analyse IP traffic. NIDS are also "stateful" and can analyse application level interactions (e.g. allowing inspection of web traffic). Primarily NIDS rely on attack signature databases to recognise known attacks, and these need to be frequently updated as new attacks are discovered and added to the database. They may also include NBA functionality to allow learning of normal traffic profiles and the detection of anomalous traffic conditions (refer to Behaviour Analysis Systems).

38. NIDS has the advantage that the "taps" are totally passive and are invisible to an attacker. The attacker may therefore not easily be able to detect that there is an IDS present to attempt to deceive. The "taps" also act as one-way diodes to ensure that the NIDS infrastructure cannot be subverted to become a means of network attack. This means the NIDS collection network is ideally on a dedicated out-of-band network that is not mixed with normal network traffic (this also has security advantages). A NIDS should also have no impact on network performance and can readily be added to legacy networks. However, the disadvantages are that a NIDS is expensive to implement and that there is a limit to attack detection possible at the application level. It also cannot detect compromised host computers unless they exhibit unexpected network behaviour.

Host Intrusion Detection Systems (HIDS)

39. HIDS can be a standalone technology or be integrated with NIDS. HIDS relies on software agents installed on critical servers and workstations. Like NIDS, HIDS tend to be signature based and provide alerts to a central management console system. The agents will also receive signature updates in the opposite direction. These agents can detect:

    a. Local network related attacks;

    b. Attacks directed at the application layer;

    c. Attempted or actual compromise of the underlying operating system;

    d. Gather information from other agents (e.g. anti-malware software) and operating system facilities to provide unified alerting and reporting from that host.

40. Hence HIDS provides the advantage of a focussed and comprehensive view of activity at that host and can provide a broad series of alerts. Combining HIDS and NIDS provided the advantages of both. HIDS has the disadvantages in that it is a direct host overhead, can impact on host and network performance and may not be compatible with legacy systems. If an attacker compromises the HIDS server there is a risk that they can also subvert the IDS system as a whole or use it as a means to attack the network itself (they can certainly discover the IDS type, and also either disable the agent or use it to send false messages). For this reason, where HIDS is implemented it should be behind other network defences to ensure that there are other barriers in the way to prevent or limit host compromise.

Wireless Intrusion Detection Systems (WIDS)

41. WIDS is a group of different technologies dedicated to detecting attacks via Wireless LAN (WLAN) and Bluetooth (and even mobile wireless including GSM and 3D) technologies or unauthorised access to WLAN facilities. WIDS includes:

    a. WIDS functionality of existing Wireless Access Points or WLAN interface software. This provides a part time ability to provide an unsophisticated scanning function to detect or enumerate in range WLAN devices and access points or to alert upon the appearance of new nodes. They may also include access control features that register particular interfaces and deny others (typically based simply on interface MAC addresses, this is not strong technology);

    b. Dedicated WIDS equipment that can scan or listen in to all WLAN and Bluetooth channels near-simultaneously and immediately detect new devices that appear. Some include diverse and distributed antennas that allow mapping and rapid location of each detected devices. This technology can be used standalone to assist in the enforcement of a "no-wireless" policy or it can be used to police a more permissive WLAN environment;

    c. Integrated approaches with hybrid technology that allows all wireless access points and dedicated WIDS to be networked and provide a centralised reporting facility. These may also tie in with NIDS and HIDS to provide overall attack profiling and attack source tracking;

    d. WIPS (refer to IPS following) that can provide reactive measures to prevent rogue interfaces connecting or to jam an attacker's channels. It should be noted that jamming is not legal in the UK: it is a criminal offence under the Wireless Telegraphy Act 2006, this may severely limit the availability of licensed WIPS equipment available in the UK.

42. A significant issue with WIDS is the increasing number of allocated wireless communications bands and protocols that need to be monitored. The cost of the equipment increases with the diversity the receivers and to be effective for their purpose they need to scan all channels. IEEE 802.11 (WLAN) alone has three standard formats with more on the way (to feed demands for ever increasing bandwidth and range):

    a. 802.11a - 5GHz, OFDM multiplexing;

    b. 802.11g - 2.4GHz, DSSS multiplexing;

    c. 802.11h - 2.4GHz, OFDM multiplexing.

43. Each of these bands are split into multiple channels, although only a subset of these are usable due to overlap and clashes of allocation with other wireless technology and are the subject of regional allocation. A WIDS needs to monitor all channels as an attacker may deliberately use uncommon or illicit channels to attempt to pass unnoticed. Additional bands are also used by IEEE 802.16 WiMAX technology, these are typically encountered in public access wireless hotspots and have increased range in comparison with WLAN.

44. For this reason fully dedicated WIDS system is of considerable cost. Organisations may consider its deployment, in addition to other technologies when the vulnerabilities of wireless technology and presence of such equipment are of particular concern. Other organisations may consider leveraging WIDS functionality present in deployed WLAN equipment.

Intrusion Prevention Systems (IPS)

45. IPS implies the ability to automate preventative response to detected intrusions. This can vary from filtering traffic at specific points, altering boundary firewall rules to drop traffic associated with an attack or playing an active part in attack streams and modifying potentially harmful behaviour to become harmless. Increasingly the distinction between IDS and IPS is disappearing. Original vendor IDS products are being supplanted by new versions that have both capabilities. This applies to all classes of products including NIDS, HIDS and WIDS (hence NIPS, HIPS and WIPS). The distinction between IDS and IPS is now more one of configuration. It is a deployment or operational choice to configure the prevention aspects of these devices.

46. There is one significant difference in as far as NIDS/NIPS is concerned: whereas NIDS required only passive network taps, NIPS have additional types of active network connections: these can manipulate network traffic using techniques, such as:

    a. Dropping selected traffic from a flow (much like a firewall);

b. Switching to "open circuit" to form a total disconnect;

c. Providing other responses such as manipulation of specific traffic flows to render an attack harmless (e.g. convert a malformed request into a protocol compliant request);

d. Diverting specific traffic flows. e.g. from the original target to a "honeypot" resource;

e. Throttling of flows that have become overloaded by the introduction of selective transmission delays (and potentially defeating denial of service attacks).

47. Similarly HIPS agents may take local automated responses including reconfiguring the operating system or local software firewall to filter network traffic or terminate attacker activity on the local host. As IPS provides both active devices and agents there are significant concerns introduced: they are now directly implementing a Security Enforcing Function (SEF) and would warrant the same degree of assurance as any other SEF component within the system (few IPS products are formally assured under the Common Criteria scheme and currently none have CCTM certificates). Furthermore, any use of the prevention functionality of IPS faces various issues:

a. Automatic prevention follows automatic detection, any "false positive" detections may trigger inappropriate automated responses. Alerts should be are attached to any automated responses so that they can be reviewed as soon as possible after they are activated, providing the opportunity for Security Managers to review the action and confirm or reverse the response, or provide alternative manual response.

b. Responses need to be proportionate and carefully configured (and this applies if the responses are invoked either automatically or manually). For instance, it may be inappropriate to completely close an entire communication channel because of a single attack detected from a single source: this could be, in effect, a self-imposed denial of service. A more fine grained response would be to only block traffic from the specific source;

c. The "automatic" nature of the responses should not be overly relied upon. This is not only an ineffective strategy; it leads to a false sense of security. Some attacks may go unnoticed ("false negatives") or may be the subject of deliberate diversion by the attacker ("misdirection"). System monitoring is essential to detect the more subtle attacks. There should be a series of pre-planned manual measures put into place that can be invoked in case of such incidents.

d. It can be assumed that a sophisticated attacker will find out the nature of the network defences. Sophisticated attackers can also exploit such technology to effect undesirable responses leading to critical denial of service. They may also seek to raise the number of alerts raised to the system to such a level such that the monitoring team becomes fully occupied. Even some classes of "worm" type malware can hunt for internal defences such as IPS and potentially attempt to exploit their presence. Contingency plans should be put into place should such attacks occur and these plans include consideration as to how they may be defeated;

e. Consideration needs to be given to the learning nature of heuristic, NBA-like, IPS systems. The quality and accuracy of learnt normal profiles are even more critical if the detection of abnormal conditions triggers automated responses. If traffic conditions change for legitimate reasons this could trigger inappropriate responses. The induction process may therefore need to have additional stages added to it: 1) learn normal behaviour patterns, 2) act only in detection mode for a period and provide only manual responses during this period, and then 3) gradually introduce limited automated responses as confidence is gained in the fidelity of the detection capabilities paired to those responses and the effectiveness of those responses.

48. Consequently utilisation of automated prevention facilities warrants comprehensive care in planning, configuration, testing and operation. Projects considering implementation of IPS technology should engage with CESG network defence experts at the earliest possible phase of the project lifecycle.

Conclusion

49. There is a vast and increasing array of technology and techniques that can be deployed for monitoring ICT systems. It should be remembered that no single product or technology, nor a combination of products or technologies, can provide 100% protection. System designers should consider the merits and limitations addressed by each option and consider the whole-life costs of implementing and operating those solutions.

50. Significant projects should consider implementing of all forms of available attack detection and analysis technology (using tools from multiple vendors) in order to provide a "defence in depth" approach. This is especially true for treating risks that are in the **Defend** segment of the Segmentation Model. Smaller projects should consider that the Security Managers and others operating the system are provided with adequate degrees of support in terms of the technology and tools made available to them in order to effectively discharge their Protective Monitoring responsibilities.

Assurance

51. It should be remembered that technology deployed to assist in Protective Monitoring becomes part and parcel of the project. Just as for other security mechanisms, there needs to be a source of confidence in the effectiveness of technology solutions adopted. Information Assurance for Protective Monitoring solutions can come from several sources and this is considered in IS1 & 2 supplement (reference [b]). This sub-section discusses how the aspects of IS1 & 2 supplement can be applied.

Application of the IS1 & 2 Assurance Matrix to Protective Monitoring

52. Appendix D of IS1 & 2 supplement Form 8 can be used to determine the types of independent assurance applicable to Protective Monitoring technologies. The relevance of each different type of assurance is given in Table D-3 on page 115.

Applicability of the Assurance Framework to Protective Monitoring

53. All aspects of the CESG Assurance Framework can be applied to Protective Monitoring controls. The relevance of each aspect of the framework is given in Table D-4 on page 116.

Assurance Source	Relevance and Issues
Product Assurance	• There is fairly good coverage of IDS/IPS products within the Common Criteria catalogue (refer to: http://www.commoncriteriaportal.org/). Most products are certified to the EAL2 level, with some EAL3 and others EAL4. However, none of these have assured via the UK ITSEC scheme. • There are some network integrity products that have current CCTM certificates (http://cctmark.gov.uk/). • Other categories are not represented.
Service Assurance	• There are a few services associated with network de-perimeterisation controls and email anti-malware that have current CCTM certificates (http://cctmark.gov.uk/). These services can provide organisations with incident reports that can contribute to Protective Monitoring activities.
System Assurance	• Project based application of the CESG Tailored Assurance Scheme (CTAS) may be a means of providing assurance of project specific Protective Monitoring mechanisms in the absence of other assurance methods.
System Configuration Test	• CHECK and CREST services can be expected to include Protective Monitoring mechanisms within the scope of their IT Healthcheck activities. • Projects should consider testing monitoring facilities during IT Health Checks, as this is an ideal opportunity to prove their response to abnormal traffic and simulated attack conditions. • It should be noted that IPS prevention capabilities and IDS learning modes should be disabled during IT Health Checks as they may skew the results and provide incorrect traffic patterns which should not be learnt.
Compliance Process	• Protective Monitoring Controls, as per other information security controls, should be documented in the Statement of Applicability and Risk Management and Accreditation Documentation for projects and compliance should be checked as for any other control.
Cryptographic Assurance	• Where Protective Monitoring traffic needs to be protected in transit, either "in band", over untrusted networks or as bulk data transfers then encryption of this traffic should be applied in accordance IS4 requirements (reference [p]) and GPG 3 (reference [q]). • Assurance of the cryptography applied should be in accordance with the Cryptographic Assurance requirements given in the IS1 Assurance Matrix and IS4.

Table D-3 - Relevant Assurance Sources for Protective Monitoring technology

Assurance Elements	Relevance and Issues
Intrinsic Assurance The actions and activities necessary to understand and affect the risks associated with the origin of an ICT component.	• Assurance is based on product and vendor heritage, track record and, to some extent, country of origin.
Extrinsic Assurance The actions and activities that are undertaken independently of the development environment, and that seek to find vulnerabilities through the response of the ICT solution to context-, threat- and risk-informed stimuli.	• Suitable sources of independent assurance for products, such as the UK ITSEC scheme which is based upon Common Criteria, as per Table D-3. • In the absence of already evaluated and certified products then the security enforcing aspects of Audit and Accounting technology adopted should be included within the project security targets that are the subject of CTAS assurance activities.
Implementation Assurance The actions and activities necessary to combine one or more components and so establish and verify the properties of a solution such that they meet the needs of the business at an acceptable level of residual risk.	• Protective Monitoring technologies should be incorporated as part of the overall system integration process and be subject of adequate functional, integration and user based testing. • These technologies should be included within the scope of IT Health Check exercises, as per Table D-3.
Operational Assurance The actions and activities necessary to maintain the risk assessed baseline once the ICT solution has entered use, including provision for activities to monitor changes in vulnerability and/or threat	• Operational support aspects of the solutions chosen need to be understood. • Adequate guarantees are obtained fir availability of support arrangements, maintenance of certified states, availability of patches and any signature updates for the ICT system lifetime. • Operations staff must have their levels of manning, skills and experience maintained and should be trained in the use of the technologies at their disposal.

Table D-4 - Relevance of Assurance Framework elements to Protective Monitoring solutions

References

[a] HMG IA Standard No. 1 & 2, Information Risk Management, , Issue 4.0, April 2012 (UNCLASSIFIED). Available from the CESG IA Policy Portfolio.

[b] HMG IA Standard No. 1 & 2 supplement, Technical Risk Assessment, and Risk Treatment, Issue 1.0, April 2012 (UNCLASSIFIED). Available from the CESG IA Policy Portfolio.

[c] HMG Security Policy Framework, 2012. Tiers 1-3 (Not Protectively Marked). Available at: http://www.cabinetoffice.gov.uk.

[d] CESG Infosec Memorandum No. 22, Protective Monitoring, Issue 1.0, April 2002.

[e] ISO/IEC 27001:2005 Information Security Management Systems - Requirements.

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

[g] CESG Infosec Memorandum No. 37, Intrusion Detection of Managed IT Systems, Issue 1.0, January 2005.

[h] HMG IA Standard No. 6, Protecting Personal Data and Managing Information Risk, Issue 1.2, March 2009 (Not Protectively Marked). Available from the CESG IA Policy Portfolio.

[i] CESG Good Practice Guide No. 18, Forensic Readiness, Issue 1.0, October 2009 (Not Protectively Marked). Available from the CESG IA Policy Portfolio.

[j] BS 10008:2008 Evidential Weight and Legal Admissibility of Electronic Information.

[k] ACPO nhtcu Good Practice Guide for Computer based Electronic Evidence - Version 3.0, September 2003.

[l] PD ISO/IEC TR 18044:2004 Information Technology - Security techniques - Information security incident management.

[m] ISO/IEC 20000:2005 Information Technology - Service Management (Parts 1 and 2).

[n] CESG Good Practice Guide 24, Security Incident Management, Issue 1.0 August 2010, Issue 1.0, August 2010. Available from the CESG IA Policy Portfolio.

[o] OGC - Expected outputs and outcomes (output based specification) - http://www.ogc.gov.uk/outputs_and_outcomes_output_based_specification.asp.

[p] HMG IA Standard No. 4, Management of Cryptographic Systems, Issue 5.1, April 2012 (UNCLASSIFIED. Available from the CESG IA Policy Portfolio.

[q] CESG Good Practice Guide No. 3, Securing Bulk Data Transfers, Issue 2.0, March 2009 (UK RESTRICTED). Available from the CESG IA Policy Portfolio.

[r] RFC 3164 - The BSD Syslog Protocol, August 2001 - http://www.rfc-editor.org/rfc3164.txt (recently obsoleted by RFC 5424, reference [s]).

[s] RFC 5424 - The Syslog Protocol, March 2009 - http://www.rfc-editor.org/rfc5424.txt.

[t] RFC 3195 - Reliable Delivery for Syslog Protocol, November 2001 - http://www.rfc-editor.org/rfc3195.txt.

Glossary

3G - Third Generation mobile telecommunications network allowing a variety of services to be offered to consumers, such as high speed data access and location based services.

ACPO - Association of Chief Police Officers

ARP - Address Resolution Protocol - Ethernet protocol used to translate between MAC and IP addresses.

Accounting - The process of collecting and recording information about events.

Accounting Items - Discrete items of information that are recorded as part of the accounting process.

Agent - Software driver that runs on a host that provides messages and notifications to a central management console system.

Alerts - Messages raised by a business process that indicates the high probability of a information security incident requiring investigation.

Archive - An offline store of accounting data. This requires infrastructure to support retrieval from the archive to allow investigation of past events.

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

Audit - The systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.

Audit Logs - Event Logs - System Logs - Logs which record user activities, exceptions, and information security events, which are kept for an agreed period to assist in future investigations and access control monitoring.

Baseline Control Set - Set of controls defined by IS1 & 2 (reference [a]) to provide a baseline level of protection for ICT systems.

Bluetooth - A short-range wireless protocol typically used to enable wireless connection between mobile handsets, PEDs, laptops and desktop computers.

BSD - Berkeley Software Distribution - Unix operating system derivative developed and distributed by the Computer Systems Research Group of the University of California.

Behaviour Analysis System - Software or hardware system, or even manual processing that analysed the behaviour of systems, users, applications or networks (see NBA) overtime, and that can provide associated reports and alerts.

Black-listing - Barring access to specific content or web-sites on the basis of a "black list" of known rogue sites.

CAPP - Controlled Access Protection Profile - Common Criteria Protection Profile for basic controlled access to file system objects, which implements the principles of discretionary access control.

CCTM - CESG Claims Test Mark - A scheme that provides a government quality mark based on accredited independent testing to prove the validity of security functionality claims made by vendors.

Compromise method - The means available to a Threat Actor to compromise the Confidentiality, Integrity or Availability of an Asset.

CHECK - CESG IT Healthcheck scheme.

CINRAS - Communications Incident Reporting and Alerting Scheme - CESG scheme for managing incidents relating to UK cryptographic items (those designated as ACCSEC and CRYPTO).

CPNI - Centre for the Protection of the National Infrastructure - Agency associated with promotion of good practice in the Critical National Infrastructure community, with the responsibility for ensuring availability of critical services in the event of UK national emergencies and implementation of UK national civil contingency plans.

CREST - Council of Registered Ethical Security Testers - Organisation providing certification of ethical penetration testers.

CTAS - CESG Tailored Assurance Scheme - CESG tailored ICT evaluation scheme and associated supporting services focussing on HMG ICT systems and services requiring IA evidence to support formal accreditation.

DHCP - Dynamic Host Configuration Protocol - Internet service to assign IP addresses to physical devices from a dynamic pool.

DMZ - Demilitarised Zone - Distinct logical and physical network space or "zone" between the exterior boundary and the corporate network. This can offer limited exposure of external services without requiring full remote access into the corporate network.

DNS - Domain Name Service - Internet protocol and supporting services to allow translation of abstract IP addresses into human readable domain names.

DSSS - Direct-Sequence Spread Spectrum - Form of multiplexing used for WLAN protocols.

EAL - Evaluation Assurance Level - Specification of the level of evaluation attained by products evaluated under the Common Criteria and UK ITSEC schemes (ranging from EAL1 through to EAL7).

FTP - File Transfer Protocol - Internet protocol used for transporting files electronically.

False Negative - A situation in which there is an information security incident that fails to raise an expected alert indication.

False Positive - A situation in which an alert is raised that is then found not to indicate an information security incident.

Guard Processor - A processor that is typically located as a network boundary of ICT systems running at different levels of trust. The guard processor will validate business traffic obeys security policy rules usually by checking the security labels of messages sent between those systems.

GSM - Global System for Mobile communications - GSM is a cellular mobile telecommunications standard, in common use across the world.

GovCERTUK - The HMG Computer Emergency Response Team.

HIDS - Host IDS - Category of IDS that is based on agents installed on hosts (servers, workstations, etc.).

HMAC - Hash Message Authentication Code - Message integrity and authenticity check based upon a cryptographic hashing algorithm (e.g. SHA).

HTTP - Hyper-Text Transport Protocol - Internet protocol that facilitates the exchange of web pages and traffic.

Honeypot - Honeynet - ICT resources set aside that contain no information assets of value but that appear as genuine targets to distract an attacker or facilitate analysis of their behaviour.

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

IACS - Information Assurance Consultancy Services - Combined term for reference to CESG consultancy services and associated schemes including CHECK, UK ITSEC, CTAS, etc.

ICT - Information and Communications Technology - Collective term for describing information systems and communications technology.

IDS - Intrusion Detection System (or Service) - Hardware, software or services that monitor systems for attack indicators and report these to central management console systems.

IL - Impact Level - Business impact level as defined in IS1 & 2 (ranging from IL0 through to IL6).

Integrity Check - Describes a process where a log file or event message check-sum (e.g. HMAC) is calculated and verified against the file or message contents. If a mismatch occurs then the integrity check has failed and the log file is considered to have been corrupted or truncated during either transmission or storage.

IP - Internet Protocol.

IPS - Intrusion Prevention System (or Service) - Development of IDS that includes automated responses to defend against the attacks.

ITIL - IT Infrastructure Library - Original form of the de-facto good practice for definition of IT outsourcing framework requirements (now expressed as an international standard in ISO/IEC 20000).

ITSEC - IT Security Evaluation Criteria - UK incarnation of the Common Criteria IT product security evaluation scheme.

Log Collector - Collector - Device that acts as the central collection device in a log acquisition system.

Log Extract - A portion of log file data extracted to support a specific investigation (which may be supported by one or more queries of either online or archived

accounting data). The extract may also be produced in a form compliant with forensic readiness requirements and stored long term for potential use as evidence.

Log File - A system file used to save log event data. This may represent all or part of the Audit Log for that system.

Log Relay - Relay - Device that acts as the intermediate log-relaying device in a log acquisition system.

Log Reset - Operation that resets (purges) all records in a log file or log file collection.

Log Rotation - Used to describe and automatic process on an ICT system in which the current log file segment is saved and a new segment opened.

Log Segment - A log file in a rotation system in which the entire log is stored in a collection of segment files allowing for easier maintenance and capture.

Monitoring - The provision of a business process that provides the necessary resources to pro-actively monitor a system for information security incidents.

Meta-data - Literally "data about data", that is supplemental data stored in electronic files, messages, etc.

MAC - Media Access Control - Ethernet physical device address.

MSP - Managed Services Provider - a commercial organisation to which ICT or other services can be outsourced.

MSSP - Managed Security Services Provider - an MSP that specialises in the delivery of security based services.

NBA - Network Behaviour Analysis - Software or hardware system that learns network behaviour patterns, that can analyse and present trends and alert departures from those trends.

NIDS - Network IDS - Category of IDS that is based on network probes.

NMS - Network Management System.

NOC - Network Operations Centre - Dedicated facility for managing network operations.

OBS - Output Based Specification - Current recommended requirements specification approach from OGC (reference [n]).

ODBC - Open Database Connectivity - Programming interface to facilitate access to underlying databases.

OFDM - Orthogonal Frequency-Division Multiplexing - Form of multiplexing used for WLAN protocols.

P-D-C-A - Plan-Do-Check-Act - Common management review lifecycle present in several ISO standards, including both ISO27001 and ISO20000.

PED - Portable Electronic Device - A generic term for any portable electronic device that has the ability to transmit, record, process or store data.

PKI - Public Key Infrastructure - Technology and services required to support digital certification which can support digital signatures, etc.

PMC - Protective Monitoring Control - Designation used to identify each of the twelve Protective Monitoring controls within this Guide (**PMC1** through to **PMC12**).

Protective Monitoring - The whole process of recording information, subsequently analysing it and comparing it to an accepted security policy, and corrective actions that may follow.

Query - An ad-hoc reporting process that inspects accounting data for a match against pre-defined criteria (e.g. events attributable to a specific user name, events occurring on a specific day, etc.).

RADIUS - Remote Authentication Dial In User Service - Top-level remote access connection service. "Dial in" is an anachronism as this protocol persists for any remote connection based service.

RAID - Redundant Array of Independent Drives - A set of hardware protocols for resilient arrays of storage hard drives.

RMADS - Risk Management and Accreditation Documentation Set - System risk management and accreditation documentation, as defined in IS1 & 2 (reference [a]).

Recordable Event - A subset of events that can be recorded as part of a Recording Profile and that implies the need to record a set of Accounting Items as part of the accounting process.

Recording Profile - Sets of Recordable Events and Accounting Items that contribute to a specific level of protection.

Remote Access - When a user working remotely has a communications link back to their corporate infrastructure to view or process data stored on that network.

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

SAC - Security Assurance Co-ordinator - Specialist position on project or programme boards.

SAN - Storage Area Network - Network based mass storage capability.

Security Label - An item of meta-data attached to an electronic message that indicated the security marking of the message. This may be coupled with an electronic signature indicating the message origin.

SEF - Security Enforcing Function - Security functionality implemented in hardware or software (that needs to be considered as a target of IA activities).

Segmentation Model - Concept introduced in IS1&2 and supplement) as a means for focussing technical treatment of information security risks.

SHA - Secure Hash Algorithm - Set of cryptographic hash functions designed by the US National Security Agency (NSA).

SIEM - Security Information and Event Management - SEM - Security Event Management - SIM - Security Information Management - Category of hardware and software systems that provide high degree of integration of security information and event management functions including alerting, log collection, log analysis, etc. They may also provide a high degree of integration with firewalls, IDS/IPS, etc.

Signature - Electronic Signature - Digital Signature - This is meta-data attached to an electronic message or file that is created by the originator. When coupled with a system of PKI this can provide strong authentication of the originator and message contents.

SMS - Short Message Service - Service provided over digital mobile phone networks (including GSM and 3G) that enables the sending of short text messages.

SMTP - Simple Mail Transport Protocol - Internet protocol allowing the exchange of email messages.

SNMP - Simple Network Management Protocol - Internet protocol that supports network device management and monitoring traffic (for the absence of doubt reference to SNMP always refers to the more secure Version 3 of the protocol).

SOAP - Simple Object Access Protocol - Internet protocol for exchanging XML format messages over ICT networks.

SOC - Security Operations Centre - Dedicated facility for managing security operations.

SQL - Structured Query Language - Open protocol supporting database operations.

SSID - Service Set Identifier - Open protocol service identifier (used by WLAN access points).

Syslog - De-factor internet standard for transmission over a network of device log messages (refer to references [r], and [s]).

TACACS - Terminal Access Controller Access-Control System - Internet protocol for remote access authentication.

TCP - Transmission Control Protocol - Internet protocol for reliable communications sessions.

Threat Actor - A person or group of people who are in a position to attempt to exploit a particular set of Compromise methods.

Threat Agent - A person, or group of people who are in a position to exploit a vulnerability.

Threshold Exception - Describes a condition in which a log file exceeds a pre-defined threshold and may be at risk of exhausting its allocated storage space.

TLS - Transport Layer Security - Internet protocol providing an encrypted transport layer.

USB - Universal Serial Bus - High-speed general purpose peripheral interface common on ICT devices.

UTC - Universal Co-ordinated Time - International adjusted standard time as specified by the International Telecommunication Union. Also referred to as "Zulu" time.

VPN - Virtual Private Network (or Networking) - Use of cryptography to provide a secure overlay on to a wider network in order to support private traffic between VPN nodes.

WARP - Warning, Alerting and Reporting Point - Local organisational information security incident handling resources recommended to HMG and Critical National Infrastructure organisations by CPNI.

WIDS - Wireless IDS - Category of IDS that is based on wireless technology.

Wireless Access Point - A user forms an association with a Wireless Access Point to provide them with access to a wireless network.

WiMAX - A form of WLAN with increased range typically used by public Wireless Access Points.

White-listing - Allowing access to specific content or web-sites on the basis of a "white list" of known sites that are reputable or are consistent with business purposes.

WLAN - Wireless LAN - Wireless networking, defined by standard IEEE 802.11 and 802.16.

XML - Extensible Mark-up Language - Hyper-text extensions to allow the flexible representation of structured data, messages and transactions.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Customer Feedback

CESG Information Assurance Guidance and Standards welcomes feedback and encourage readers to inform CESG of their experiences, good or bad in this document. We would especially like to know about any inconsistencies and ambiguities. Please use this page to send your comments to:

Customer Support
CESG
A2b
Hubble Road
Cheltenham GL51 0EX
(for the attention of IA Policy Development Team)

Fax: (01242) 709193 (for UNCLASSIFIED FAXES ONLY)
Email: enquiries@cesg.gsi.gov.uk

For additional hard copies of this document and general queries please contact CESG enquiries at the address above

PLEASE PRINT

Your Name:

Department/Company Name and Address:

Phone number:
Email address:

Comments:

CESG's Good Practice Guides are issued by the UK's National Technical Authority on Information Assurance with the aim of informing intended recipients of the general security issues they should consider in their approach to information and communications technologies. They are not a replacement for tailored technical or legal advice on specific systems or issues. GCHQ/CESG and its advisers accept no liability whatsoever for any expense, liability, loss, claim or proceedings arising from reliance placed upon this Guidance

IA
CESG
A3e
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Fax: +44 (0)1242 709193
Email: enquiries@cesg.gsi.gov.uk