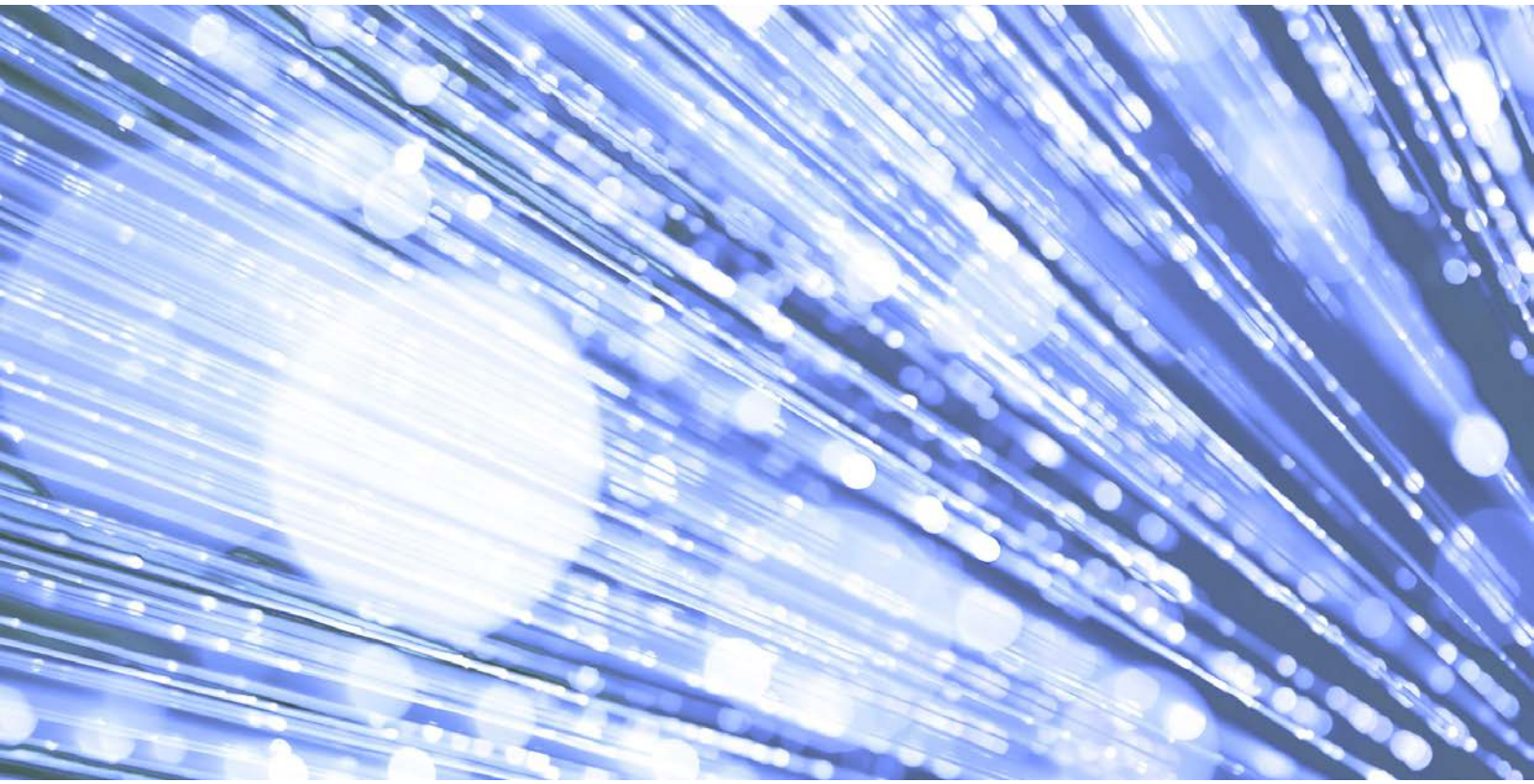
Protective Monitoring

Good Practice Guide

Author: A Heathcote
Date: 22/05/2017
Version: 1.0



Information and technology
for better health and care

Contents

1 Purpose

The purpose of the Protective Monitoring Good Practice Guide (GPG) is to provide guidance on how protective monitoring should be undertaken. This guidance will enable the organisation to have mechanisms and processes to:

- Provide visibility and an understanding of how the IT systems and services are used.
- Provide details of who is accessing data, particularly sensitive data.
- Provide the ability to detect and investigate unlawful activity or security events.
- Assist in making users accountable for their use of the IT systems or services.
- Provide evidence of compliance with policy, standards, legislation and regulations.

2 Scope

The Protective Monitoring GPG relates to all IT systems storing, processing and transmitting NHS and other UK Government information.

3 Applicability

The Protective Monitoring GPG is applicable to and designed for use by any NHS, health and social care or associated organisations that use or have access to NHS systems and/or information at any level.

4 Guidance

The Protective Monitoring GPG supplements the Excample Policy on producing a Protective Monitoring Policy and provides greater detail on how the policy requirements can be achieved. It is not prescriptive and it is realised that different organisations will require different levels of management. This GPG provides the minimum that should be considered. The guidance provided should be scaled according to the size of the organisation. For larger organisations the full process may be followed. For smaller organisations the GPG may be used to drive contractual requirements or to work with any third party provider to enable the appropriate level of protective monitoring to be implemented by that provider. For smaller organisations it may be prudent to use an independent specialist provider to assess the requirements of the organisation before discussing with any third party IT provider.

4.1 General Approach

- In order to implement and manage an effective protective monitoring regime appropriate for the organisation’s information processing and its size, the below will need to be achieved:
  - A risk assessment of the risks, threats and vulnerabilities to the information processed on the IT systems and to the IT systems generally.
  - An assessment of the degree (level or depth) of protective monitoring required to address the threats, vulnerabilities and risks identified from the risk assessment completed for the organisation.

- A review of whether and how those protective monitoring requirements can be implemented and, where it is not possible, a risk based decision made on the acceptance of the residual risk.
- A management process for 'running' the protective monitoring processes and, as importantly, reviewing and addressing its findings, warnings and alerts. A response capability to alerts form protective monitoring is required.

- This GPG provides guidance and, where applicable, examples on assessing and implementing a protective monitoring regime. However, the use of the referenced supporting documents will be required to fully implement and scope the required capability.

4.2 Protective Monitoring Controls

- There a number of ways/methods in which protective monitoring controls (PMCs) can be defined or scoped. For the purposes of this GPG the NCSC/CESG issued Good Practice Guide on Protective Monitoring (GPG 13) has been used as this is the best practice for HMG and the public sector. However, the organisation can use other protective monitoring guidelines, such as those listed within the ISO 27001/27002 control set. Although the NCSC/CESG GPG 13 is currently reflected as archived by NCSC as it is imported CESG material (https://www.ncsc.gov.uk/guidance/protective-monitoring-hmg-ict-systems-gpg-13 refers) it has not been formally replaced and remains a valid and applicable guide as well as best practice. A high-level summary of the PMCs is shown in the below table.

PMC No.	PMC Control	PMC Objective
PMC1	Accurate time in logs.	Accurate time in logs enables synchronisation between systems and system components and facilitates the collation of events.
PMC2	Recording relating to business traffic crossing a boundary.	To provide an accountable record of the import / export of data across a boundary. This can ensure that the data exchanges are authorised, conform to security policy, do not contain malicious content and can prevent or detect external attack.
PMC3	Recording relating to suspicious activity at a boundary.	To detect suspicious activity crossing a network boundary. Network devices can provide traffic trend information that can detect suspicious activity crossing a network boundary identifying common attacks such as port scanning, malformed packets and illicit protocol 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

PMC No.	PMC Control	PMC Objective
		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 known 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.

- Protective Monitoring Controls PMC1 through to PMC9 provide treatment of IT and information compromise methods, whilst PMCs 10, 11 and 12 are specific to the functional requirements of the protective monitoring system itself and their applicability will depend on the complexity of the solution implemented (Note: PMC 12 as a legal requirement should always be applicable).

4.3 Risk Assessment to Determine Protective Monitoring Controls

- There are several mechanisms that can be used for assessing the risks to the organisation’s information and IT assets. This includes formal HMG approved

processes such as Information Assurance Standards Numbers 1&2 V4 (IAS 1&2 V4), ISO/IEC 27005:2011 ('Information technology - Security techniques - Information security risk management') and the Information Security Forum's (ISF) own Information Risk Analysis Methodology (IRAM) through to in-house risk assessment processes. The essential criteria are that it is repeatable and produces risks in a priority/category order as this will be needed to inform the protective monitoring assessment.

- Whichever methodology is used in the risk assessment a prioritised risk list with meaningful descriptions of the risks should be the result as this will determine the level/degree of PMC implementation and/or whether that control will mitigate the identified risks. It is recommended that the risk assessment is first utilised to define an agreed baseline level of PMCs (it may still be the case that a PMC is not required) but this approach will enable a basic level of monitoring to be in force. The higher identified risks can then be used to determine if any of the PMCs require greater or more in depth implementation to mitigate the risk further.
- This GPG does not cover the risk assessment process as it is for each organisation to decide on which methodology will be used. However, a common output from any process will be a list of prioritised risks with risk levels. These should have a priority order, a short description of the risk and then the risk level (for example, High, Medium-High, medium, low and very low). This risk output will be sued to drive the protective monitoring solution.

4.4 Protective Monitoring Assessment using Risk Assessment Output

- In assessing the level of protective monitoring required in addition to using the drivers from the risk assessment it will also be necessary to include the below factors in the process:
  - That the information gathered for protective monitoring 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
  - The business and operational requirements; it may be that these impact upon a PMC and due to business or operational drivers the PMC cannot be fully or even partially implemented at all. Where this is the case it should be recorded and the Senior Information Risk Owner (SIRO) accept the residual risk. (This is termed a risk balance case where the operational/business drivers and risk management drivers are assessed and the decision making process recorded.)
  - The costs of implementing the PMCs. If funding is limited then a priority will need to be attached to the PMCs or, if the cost of implementing is greater than a rebuild of the IT system or recovery of the data then that may influence the decision for the level of protective monitoring.
- For whichever risk assessment process has been used, the following methodology is recommended as this will enable the protective monitoring assessment to be completed. The process can be as detailed or as simple as required for the size and complexity of the organisation (or for the discussions with the IT provider if outsourced).

- The proposed methodology for assessing the degree/level of implementation of the PMCs can be summarised as:
  - Baseline protective monitoring assessment to mitigate the majority of the risks.
  - Protective monitoring assessment to mitigate those risks not covered by the baseline assessment – additional PMC implementation.
- This 2-stage process is recommended to be undertaken by the relevant information asset owners (IAOs or equivalent), the Chief Information Security Officer (CISO or equivalent – potentially the information governance lead for smaller organisations) and IT service staff. This process will result in the initial protective monitoring solution (i.e. the degree of each PMC) that will be implemented to manage the risks identified. Once this has been completed the other factors highlighted earlier (business drivers, costs, etc.) then also need to be considered. For this additional stage business and operational staff (potentially IAOs again but also the CISO, IT services, senior management and/or specialist staff such as medical or HR or Finance depending upon which business function the IT system being assessed relates to) should be involved. The process should be recorded and the final decisions recorded and endorsed by the SIRO as the agreed or final protective monitoring posture.

4.4.1 Baseline PMC Implementation

- A baseline level of implementation of the PMCs (1-9 and 12 as a minimum) that will mitigate the majority of the risks should be established. It is recommended that the NSCS/CESG GPG 13 is used as the guide for the PMCs, or if a different set of protective monitoring controls have been used (such as controls listed in ISO 27002 control set for auditing and logging) then the associated guidance should be used to support the process.
- A recommended approach would be to assess the PMCs for mitigating all risks up to and including an agreed minimum level (e.g. Medium or if required Medium-High) and defining what is required for each PMC at the baseline level. This approach enables the majority of the risks to the IT systems to be reviewed and controls put in place, thereby giving a good level of risk managed assurance.
- The essential element of this part of the protective monitoring assessment is the derivation of how each PMC will be implemented. The level of implementation should be risk driven but the other criteria of cost, business and operational impact must also be considered; however, this should be post the risk assessment drivers.
- The result of this process should be a set of ‘rules’ or ‘definitions’ for each PMC on how it is to be implemented and what level of risk is mitigated or managed. This could look like:

PMC No	Control Implementation	Risk Level Treated
7	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. The following logged and reportable on servers:	Medium

PMC No	Control Implementation	Risk Level Treated
	• 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. • Alert all multiple log-on failures resulting in account lock-out. • Logging and capture of all accountable transaction summaries.	

- If there are any obvious functional impacts to the business/operational requirements being performed by the system through the implementation of the determined PMCs these should be identified and recorded. This will be required once the baseline and additional requirements have been completed and business/operational/cost considerations are reviewed.

4.4.2 Additional PMC Implementation

- If the implementation of the baseline control does not mitigate/address all the risks (i.e. those that remain above what the baseline protective monitoring posture would mitigate – for instance Medium-High or High if Medium was taken as the baseline level) then the risks above this level need to be reviewed individually to identify whether a greater degree of implementation of any of the PMCs would provide the necessary mitigation or some more mitigation.
- For each risk above the agreed threshold all the PMCs should be viewed using the guidance from GPG 13 (or whatever protective monitoring guidance has been used) to determine which additional elements form any of them may mitigate the risk further. It is likely that only one or 2 controls with a greater degree of implementation may be required; it is very unlikely that every control would need enhanced implementation to address these higher risks.
- As with the baseline assessment any obvious functional impacts to the business being performed by the system through the implementation of the determined PMCs should be identified and recorded.

4.4.3 Determination of Initial and Final Protective Monitoring Posture

- The results of the baseline and the additional PMC implementation assessment from the derived risks should be combined to make the initial protective monitoring posture. This initial posture should also include any identified potential impacts to business/operation of the system and an estimate of the cost of its implementation.
- Using this information, the IAOs, CISO, IT Service staff and the necessary business/operational/Finance/HR staff should assess the below 2 types of factors to produce a final agreed protective monitoring posture that the SIRO will be required to endorse.

  - Is the necessary funding available and is the funding of the proposed protective monitoring posture appropriate to mitigate the financial, business, reputational risks to the organisation if they are not implemented?
  - Are any of the identified business/operational impacts of implementing any elements of the PMCs unacceptable to the organisation?
- The decisions made during this process should be recorded and the result will be the final protective monitoring posture, which should be endorsed by the SIRO and/or Chief Executive.

4.5 Legal Requirements

- As highlighted within the PMCs, particularly PMC12, the monitoring process must be justified and legal. In addition to the PMC actual requirements the process of assessing the protective monitoring posture must comply with applicable legislation. Below is what is considered to be always applicable. The organisation undertaking this activity may be subject to additional legislation or regulations that impact their information and users; if so these should be incorporated into the process. Below is a list of the legislation that must be considered:
  - Official Secrets Act 1911–1989 – unauthorised disclosure of sensitive government information.
  - Computer Misuse Act 1990 – inappropriate use of computing technology.
  - Data Protection Act 1998 – relating to protection of personal data.
  - Regulation of Investigatory Powers Act 2000 – relating to surveillance and investigation of users on IT systems.
  - Freedom of Information Act 2000 – relating to disclosure of information from ICT systems processing public body data.
  - Caldicott data guardian requirements.

4.6 Administration and Management of the Protective Monitoring Posture

- Once the protective monitoring posture has been agreed and then implemented; either directly by the organisation's own in-house IT services or through an out sourced third party provider it is as important to have the ability for the alerts, events and logs to be regularly reviewed and acted upon.
- For larger organisations using their own IT and IT staff this will require the 'team' to be appropriately resourced in terms of staff numbers, the software required and the training necessary to undertake the role.
- For smaller organisations using outsourced IT providers this will require contractual arrangements to include the ability and requirement for the IT provider to review logs etc. and report to the organisation.

4.7 Information to Users on Monitoring

- To ensure the organisation complies with legal requirements and is open and transparent to all users the below demonstrative actions should be made clear to users; either through written procedures that are signed by users, within the Acceptable Use Policy or as a banner on the IT system for each logon. The core

elements that should be covered are explanations in simple terms in a brief statement of the facts:

- That the use of the system is being monitored and audited.
- That information that will be collected.
- That the information will be protected, stored, retained and disposed of.
- That if the monitoring identifies inappropriate or illegal use of the system the user may be prosecuted.

5 Further Reading and Advice

- In addition to the documents listed under Related References, Links and Documents further details and advice on protective monitoring can be found at https://www.ncsc.gov.uk/. This GPG does not list the particular references as these change on a frequent basis, however, searches under the below headings will help to locate the current applicable HMG policy and standard or an assured provider or mechanism of the technique or technology that may be required:
  - Protective monitoring.
  - Auditing.
  - Risk assessment.
- This GPG is supported by other GPGs, which should be used in tandem. This includes, but is not limited to:
  - Protective Monitoring
  - Information Security Incident
  - Audit Policy
  - Network Security

6 Key Words

Protective Monitoring, Protective Monitoring Controls, PMCs, Risk Assessment