From: https://www.ncsc.gov.uk/guidance/10-steps-monitoring

What is System Monitoring?

System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

What is the risk?

Monitoring provides the means to assess how systems are being used and whether they are being attacked. Without the ability to monitor your systems you may not be able to:

- **Detect attacks:** Either originating from outside the organisation or attacks as a result of deliberate or accidental user activity. Attacks may be directly targeted against technical infrastructure or against the services being run. Attacks can also seek to take advantage of legitimate business services, for example by using stolen credentials to defraud payment services.
- **React to attacks:** An effective response to an attack depends upon first being aware than an attack has happened or is taking place. A swift response is essential to stop the attack, and to respond and minimise the impact or damage caused.
- **Account for activity:** You should have a complete understanding of how systems, services and information are being used by users. Failure to monitor systems and their use could lead to attacks going unnoticed and/or non-compliance with legal or regulatory requirements.

How can the risk be managed?

Establish a monitoring strategy and supporting policies: Develop and implement a monitoring strategy based on business need and an assessment of risk. The strategy should include both technical and transactional monitoring as appropriate. The incident management plan as well as knowledge of previous security incidents should inform the approach.

Monitor all systems: Ensure that all networks, systems and services are included in the monitoring strategy. This may include the use of the use of network, host based and wireless Intrusion Detection Systems (IDS). These solutions should provide both signature-based capabilities to detect known attacks, and heuristic capabilities to detect unusual system behaviour.

Monitor network traffic: Inbound and outbound traffic traversing network boundaries should be monitored to identify unusual activity or trends that could indicate attacks. Unusual network traffic (such as connections from unexpected IP ranges overseas) or large data transfers should automatically generate security alerts with prompt investigation.

Monitor user activity: The monitoring capability should have the ability to identify the unauthorised or accidental misuse of systems or data. Critically, it should be able to tie specific users to suspicious activity. Take care to ensure that all user monitoring complies with all legal or regulatory constraints.

Fine-tune monitoring systems: Ensure that monitoring systems are tuned appropriately to only collect events and generate alerts that are relevant to your needs. Inappropriate collection of monitoring information and generation of alerts can mask the detection of real attacks as well as be costly in terms of data storage and investigatory resources required.

Establish a centralised collection and analysis capability: Develop and deploy a centralised capability that can collect and analyse information and alerts from across the organisation. Much of this should be automated due to the volume of data involved, enabling analysts to concentrate on anomalies or high priority alerts. Ensure that the solution architecture does not itself provide an opportunity for attackers to bypass normal network security and access controls.

Provide resilient and synchronised timing: Ensure that the monitoring and analysis of audit logs is supported by a centralised and synchronised timing source that is used across the entire organisation to support incident response and investigation.

Align the incident management policies: Ensure that policies and processes are in place to appropriately manage and respond to incidents detected by monitoring solutions.

Conduct a 'lessons learned' review: Ensure that processes are in place to test monitoring capabilities, learn from security incidents and improve the efficiency of the monitoring capability.