EPC153-10
Version 1.0 approved
2 June 2010

THE USE OF AUDIT TRAILS IN SECURITY SYSTEMS: GUIDELINES FOR EUROPEAN BANKS

Document History

This document was first produced by ECBS as TR409. EPC has revised the document in view of the new developments on this topic during the past years. This new version is now published with an EPC cover page and new number.

This new version is an update of TR409 version 1, dated November 2001; the introduced changes aim to improve clarity and extend the scope of the guidelines.

The scope of the new version includes payments related data. This extension is done because the secure capture and storage of the audit trails of payment records, along with the related security and computer audit events, may be important evidence in any dispute resolution processes. The focus of these guidelines will not be on IT Security and audit trails for security related purposes, but will include the audit trails of business processes of banks: processing of payments.

The changes also include updates of the bibliography and an extensive review of the principles (or recommendations as they were called in previous version); these make the guidelines up to date and improve their clarity.

Contents

1 Introduction 4
2 Background 6
2.1 Bibliography 6
2.2 Glossary of terms 6
2.3 Scope and objective 7
3 Audit system design 9
3.1 Events to be recorded 10
3.2 Audit tools 12
3.3 Fields to be recorded 13
3.4 Event integrity 14
3.5 Confidentiality 14
3.6 Record format 15
3.7 Compression 15
4 Management of audit logs 16
4.1 Ownership & classification of audit data 16
4.2 Generation of audit trails 16
4.3 Naming conventions 17
4.4 Place of storage / archiving 17
4.5 Controls on access 17
4.6 Review period 18
4.7 Records held by third parties 18
4.8 Long term storage of audit logs 18
4.9 Back-up 18
4.10 Disposal of audit trail information 19
5 Retention period 20
6 Application and use of audit logs 21
6.1 Systems management and monitoring 21
6.2 Internal investigations 21
6.3 Presentation in court 22
7 Summary of Principles 23
8 Appendix A: European-wide legal & regulatory requirements 26
8.1 EU Data Protection Directive 26
9 Appendix B: Response to events 28
10 Appendix C: Life-cycle of incidents and investigations 31
11 Appendix D: Treatment of data during investigations 33
11.1 Evidence preservation following an incident 33
11.2 Digital evidence 33
11.3 Computer based electronic evidence 34

1 INTRODUCTION

Audit trails can be used for a number of purposes in banking business processes and security controls, both supported by IT systems. Good audit trails provide and/or support:

- Accounting and other business-related record-keeping, including the need to reconstruct a complete data processing sequence in chronological order;
- Fault detection and resolution;
- Performance monitoring;
- Demonstration of adherence to security policy, contract, regulatory requirements or the law;
- Detection and investigation of breaches of security policy, contract, regulatory requirements or the law;
- Preservation and presentation of evidence relating to any of the above.

This report seeks to provide guidance on the creation and use of audit trails for business {payments) process and security-related purposes, including:

- the logging of actions relevant to business & payment processes and security systems;
- the security of audit records in general.

Importantly the Payment Services Directive sets out requirements on financial institutions that can only be met through establishing sound and effective audit and accounting of IT systems used in processing payments as well as the payment records themselves. The specific article is:

> Article 59
>
> Evidence on authentication and execution of payment transactions
>
> 1. Member States shall require that, where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for his payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency.
>
> 2. Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of his obligations under Article 56.

An audit trail is a series of records of computer events about an operating system, an application, or user activities. Computer systems may have several audit trails each devoted to a particular type of activity. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems and application issues.

Organisations should develop, disseminates, and review/update on a regular basis the following:

- A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Existing organisational policies and procedures may make the need for additional specific policies and procedures unnecessary. The audit and accountability policy can be included as part of the general information security policy for the organisation.

Additionally Financial organisations might consider developing a data protection audit. This audit evaluates how well the organisation is achieving data protection and considers ways by which IT can address data protection problems.

2 BACKGROUND

2.1 BIBLIOGRAPHY

The documents below have been used to create these guidelines. As the documents are reviewed regularly, this list will be assessed on currency and applicability on a regular basis.

- ISO/IEC 27002 - Information technology -- Security techniques -- Code of practice for information security management, section 10.10, 2005 (www.iso.org)
- ISO 15489 - Information and documentation -- Records management -- Part 1: General, 2001 (www.iso.org)
- ISO/TR13569: Information Security Guidelines for Banking, 2005 (www.iso.org)
- BSI PD008: Legal Admissibility and Evidential Weight of Information Stored Electronically, British Standards Institution, 1999
- COBIT (Control Objectives for Information and related Technology) from Information Systems Audit and Control Association (http://www.isaca.org/cobit.htm)
- Payment Card Industry Data Security Standard (PCI DSS) Requirement 10 (https://www.pcisecuritystandards.org/)
- HMG Good Practice Guide for Protective Monitoring for ICT systems, March 2009
- EU Data Protection Directive 1995/46/EC
  (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:EN:PDF)
- Payments Services Directive 2007/64/EC
  (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:EN:PDF)
- CPNI - NISSC Technical Note 01/2005 An Introduction to Forensic Readiness Planning. (http://www.cpni.gov.uk/)
- EU Convention on Cybercrime - http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
- ECB's oversight framework for SCT (http://www.ecb.int/pub/pdf/other/oversightframeworkcredittransferschemesen.pdf)
- ECB's oversight framework for SDD (http://www.ecb.int/pub/pdf/other/oversightframeworkdirectdebitschemesen.pdf)
- ECB's oversight framework for cards (http://www.ecb.int/pub/pdf/other/oversightfwcardpaymentsss200801en.pdf)

These have been used as a check on these guidelines and for some small amount of source material; significant extracts are acknowledged in the text.

2.2 GLOSSARY OF TERMS

Accountability:	The property that ensures that the actions of an person, device, entity etc. can be traced uniquely to the person, device, entity etc.
Audit:	A function which seeks to validate that controls are in place, adequate for their purposes, and which reports inadequacies to appropriate levels of management

Audit log:	An audit log is a chronological sequence of audit records, each of which contains evidence directly as a result of the execution of a business process or system function
Audit record:	A single entry in an audit log that describes the occurrence of one single auditable event.
Audit service:	A security service that records information needed to establish accountability for system events and for the actions of system entities that cause them.
Audit trail:	A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.
Auditable event:	An auditable event is generated by any activity in a system that is capable of being audited. An auditable event could lead to the compromise of the integrity and/or security of an information system and therefore indirectly compromise a business process
Digital evidence:	Information stored or transmitted in binary form that may be relied upon in court.
Encryption**:**	Any procedure used in cryptography to convert plain text into cipher text in order to prevent anyone but the intended recipient from reading that data.
Hashing:	The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.
Security audit:	An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.
Security event	See Auditable event.

2.3 SCOPE AND OBJECTIVE

The purpose of these guidelines is to provide advice and principles regarding the use of audit logs, the content of audit logs and the actions that are required as a result of a specific auditable event action occurring.

The guidelines **will**:
• provide practical, easy-to-use guidance that can be used to create the building blocks for implementing a secure audit trail strategy
• underpin the development of organisational policies, topic-specific standards and detailed procedures
• contribute to meeting the objectives of information security-related standards, such as the ISF Standard of Good Practice, ISO / ISO 27002, COBIT v4.1 and PCI / DSS
• are easily measured, for example by using any of the ISF's benchmarking tools (including the FIRM Scorecard, Security Health check and Benchmarking Tool) or by third party tools.

The guidelines **will not**:
• provide a specific secure audit trail strategy
• indentify and list all candidate auditable events that must be captured by a particular institution or organisation.

The guidelines are applicable to any part of an organisation, such as a business unit, corporate headquarters, manufacturing environment or a data centre. They can be used as a basis for protecting:

• critical and sensitive business information in all formats, such as databases, e-mails and paper documents
• critical business applications under development and in live production environments
• all types of computing devices, ranging from mainframes and server farms, through desktop and laptop computers to hand-held devices such as Personal Digital Assistants(PDA's)
• corporate networks, including wireless, Voice over IP (VoIP) and Internet connectivity.

Audit Logs can benefit an organisation in many ways. They help to ensure that computer security records are stored in sufficient detail for an appropriate period of time. Routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such problems. Audit logs can also be useful for performing forensic analysis, supporting the organisation's internal investigations, establishing baselines, and identifying operational trends and long-term problems.

Audit trails can be used in conjunction with access controls to identify and provide information about users suspected of unauthorised modification of data.

Besides the inherent benefits of audit log management, a number of laws and regulations further compel organisations to store and review certain logs. See Appendix A for information regarding European legal and regulatory requirements. The following is a listing of key regulations, standards, and guidelines that help define organisations' needs for log management:

Gramm-Leach-Bliley Act (GLBA): GLBA requires financial institutions to protect their customers' information against security threats. Log management can be helpful in identifying possible security violations and resolving them effectively.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): HIPAA includes security standards for certain health information. NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, lists HIPAA-related log management needs For example, Section 4.1 of NIST SP 800-66 describes the need to perform regular reviews of audit logs and access reports. Also, Section 4.22 specifies that documentation of actions and activities need to be retained for at least six years.

Sarbanes-Oxley Act (SOX) of 2002: Although SOX applies primarily to financial and accounting practices, it also encompasses the information technology (IT) functions that support these practices. SOX can be supported by reviewing logs regularly to look for signs of security violations, including exploitation, as well as retaining logs and records of log reviews for future review by auditors.

Payment Card Industry Data Security Standard (PCI DSS): PCI DSS applies to organisations that "store, process or transmit cardholder data" for credit cards. One of the requirements of PCI DSS is to "track…all access to network resources and cardholder data"

3 AUDIT SYSTEM DESIGN

As part of the audit log management process, an organisation should define the roles and responsibilities of the users who are involved in the management and use of audit logs. Users involved in the management of audit records include:

- Business users
- Help desk / customer support
- Systems management users
- Contract management
- Internal & external auditors
- Security administrators
- Internal investigation teams
- Computer Security incident response team
- Law enforcement agencies

The needs of **all** potential users must be considered when designing audit facilities. Different users will have very different needs; for example, business users will have completely different needs than security administrators or investigation teams.

EPC Principle 1: *Audit facilities should be designed with their specific use(s) in mind, not simply adapted from existing system logs.*

Organisations should:

- create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and
- Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Organisations should develop audit log policies that clearly define mandatory requirements and principles for audit log management. The policies should address who within an organisation can establish and manage audit log infrastructures. Organisations should also ensure that policies, guidelines and procedures that have any relationship to audit logging should incorporate and support the appropriate audit log management requirements and principles.

EPC Principle 2: *Organisations should create and maintain an audit log management structure, including policy, procedures, rules and tools.*

EPC Principle 3: *Where a single business or system transaction will result in the creation of audit data on multiple systems, design consideration should be given to how the complete audit information about that transaction will be collated and made available to a "user of the audit logs".*

EPC Principle 4: *Organisations should provide appropriate support, e.g. training, provision of appropriate tools, for all staff that will be making use of the audit logs.*

Audit Logs held on any storage medium will record large volumes of data on a regular basis. This will impact the resources required to store the data for the appropriate length of time. Many logs have a maximum size and when this is reached the log might overwrite old data resulting in a loss of integrity and availability. It might be appropriate in some cases to record less information and maintain the log's integrity than record everything but be unable to guarantee integrity.

ECBS Principle 5: *Audit log files should be periodically saved and moved to another storage space. The periodicity may be influenced by the classification of the data, but should be defined either according to a fixed size (e.g. every time the log reaches 1Mb) and / or according to a fixed period of time (e.g. per day, per week).*

3.1 EVENTS TO BE RECORDED

All business processes comprise of a number activities supported by information technology (IT). To protect and secure correct processing technical and security controls are in place and each of these controls can be linked to creating an entry in audit logs.

To avoid the creation of "oversized" audit logs it is necessary to tailor audit log files to the needs of the organisation. This can be achieved by selecting the auditable events in the business processes of an organisation. An auditable event in this specific instance is defined as a single event (within a business process) that could lead to the compromise of the integrity and/or security of an information system and therefore directly or indirectly compromise a business process. The consequences of such a breach could lead to data loss (theft), misuse of systems & privileges, or fraud. Defining what events should be audited and captured within an IT system, and the processes used to capture such events, is analogous in the real world to placing surveillance cameras on important physical sites to detect activity and to record it for future action.

The number, volume and variety of auditable events has increased greatly, which has created the requirement for security event management – the process for generating, transmitting storing, analysing and disposing of security log data. Security event management helps to ensure that security records are stored in sufficient detail for an appropriate period of time.

EPC Principle 6: *Attacks on systems should be prevented by the use of technical preventive controls. These controls should be preferred above procedural preventive controls if possible. Both measures should be used in conjunction with examination of the audit data.*

EPC Principle 7: *Organisations should consider the use of a Security Event management system due to the large volume of security events.*

In the Response to Events matrix, see Appendix B, the events to be recorded and the urgency of response are expressed as follows:

- **Mandatory (Legal, regulatory or scheme requirement for specific records)**
- **Recommended (Derived requirement from other legal, regulatory or scheme requirement)**
- **Good Practice (As expressed in information security standards and guidelines)**

In addition, the timeliness of the response required as a consequence of the action recorded is shown:

- **Immediate (a system alarm or alert should be raised);**
- **Routine (can be dealt with when the audit log is next scanned);**
- **Historic (need only be referred to in case of a specific investigation).**

The urgency of response is indicated by * in the appropriate column.

It should be noted that the response to any of these events occurring is also dependant on the importance of the system. For high impact systems the response to any of these events occurring should be immediate. For medium or low impact systems the matrix in Appendix B may be useful in considering the response required.

How often the results of the monitoring activities are reviewed should depend on the criticality of the system or application to the organisation's business. Factors that should be considered include:

- The criticality of the application process,
- The value, sensitivity and criticality of the information involved,
- Past experience of system misuse and the frequency of vulnerabilities being exploited,
- Logging facilities being de-activated.

A pro-active view of auditable events should be taken wherever possible. Fraudulent activity has become very sophisticated and reliance on an unauthorised event or an event contravening policy is not always going to prevent a major security breach. Organisations should liaise with appropriate police and other fraud prevention bodies to ensure that the most up to date events, breaches are being monitored and that policies are continually revised as necessary.

EPC Principle 8: *Organisations should not solely rely on unauthorised events or breaches of policy, but should additionally consider proactive monitoring.*

3.2 AUDIT TOOLS

This guidance document does not recommend a specific tool or product to help automate the Audit Log management process. However many types of tools have been developed over the past few years to enable organisations to automate the collection and reporting of the large number of audit events that may occur. It is very possible that millions of audit records could be generated every day as a result of payments across a host of devices, e.g. network devices, security devices, mobile devices, and physical access, servers, desktops, databases. In order to be able to manage the security and risk the development of a central point of collection and analysis is essential. The use of automated tools to help this process is essential.

An example of this type of tool is Security information and event management (SIEM) technology. SIEM provides real-time monitoring and historical reporting of security events from networks, systems and applications. SIEM deployments are helpful in addressing regulatory compliance reporting requirements. SIEM could also be used to improve security operations, threat management and incident response capabilities.

The requirements for compliance reporting, log management, user and resource access monitoring, external threat monitoring, and security incident response should be defined. This may require the inclusion of other groups in the requirements definition effort, including audit/compliance, IT operations, application owners and line-of-business managers.

SIEM technology provides:

- the collection, reporting and analysis of log data (primarily from host systems and applications, and secondarily from network and security devices) — to support regulatory compliance reporting, internal threat management and resource access monitoring. It supports the privileged user and resource access monitoring activities of the IT security organisation, and the reporting needs of the internal audit and compliance organisations.
- the processing of log and event data from security devices, network devices, systems and applications in real time to provide security monitoring, event correlation and incident response. It supports the external and internal threat monitoring activities of the IT security organisation.

> ***EPC Principle 9:*** *Organisations should consider the use of Security information and event management (SIEM) technology to help the automation and collection of auditable events.*

In addition to syslog and SIEM software, there are several other types of software that may be helpful for audit log management. Host-based intrusion detection systems (IDS) monitor the characteristics of a host and the events occurring within it, which might include OS, security software, and application logs. Host-based IDS products are often part of a log management infrastructure, but they cannot take the place of syslog and SIEM software. Other utilities that are helpful for audit log management include visualisation tools, log rotation utilities, and log conversion utilities.

3.3 FIELDS TO BE RECORDED

The information systems should produce audit records that contain sufficient information to establish, at a minimum,

- what type of event occurred, e.g. the server, system process, ip address, mac address etc.,
- when (date and time) the event occurred, e.g. time stamps where the event occurred,
- where from the origination of the event occurred, e.g. source and destination addresses, user/process identifiers,
- where to the event occurred, e.g. the identity or name of the affected data, system or component,
- the outcome (success or failure) of the event, e.g. event descriptions, event integrity, success/fail indications and
- who the identity of any user/subject associated with the event was, e.g. a signature verification process, an IDS, an AV system, a firewall, a payment transaction record etc.

Additional data may be recorded for some events, for example, the identity of the target user where systems management access is being made to their account; a transaction reference number where a single transaction is being tracked across multiple systems.

Accurate timing is crucial to the usability of audit logs, particularly where logs are maintained across multiple distributed platforms.

Audit logs may contain intrusive and confidential personnel information. Appropriate privacy measures should be taken.

EPC Principle 10: *All audit records should contain a time stamp. Ensure that each system's clock is synched to a common time source so that its timestamp will match those generated by other systems.*

Data Protection principles require that the privacy of audit fields, if containing personal data, should be protected.

EPC Principle 11: *The privacy of personal data should be protected.*

Where possible system administrators should not have permission to erase and or de-activate logs of their own activities.

EPC Principle 12: *Measures should be implemented in order that deleting or modifying logs of own activities should be detected and alerted immediately.*

EPC Principle 13: *Administrators should not be able to erase or deactivate logs of activities.*

3.4 EVENT INTEGRITY

The integrity of audit logs must be protected from modification. This may be achieved by signing the logs with digital signatures. This can be achieved either by signing individual records or by signing files of audit logs. To ensure audit data is captured and stored for future use, it is recommended that the current audit log is archived to write-once media (e.g. WORM). The appropriate signature verification software must be available and properly maintained for the whole of the life time of the signed data."

EPC Principle 14: *Audit events should be protected from modification by using digital signatures to sign audit records.*

Audit events may be required to be retained for a considerable time in order to meet regulatory and organisational information retention requirements. The integrity of the information should be preserved throughout this period.

EPC Principle 15: *Audit events should be archived to 'write-once 'media or immediately stored off system to protect the archive from modification or deletion.*

Integrity controls such as MACs or digital signatures may be appended to audit logs as a whole or to individual records of critical events (e.g. PIN verification, digital signature creation) if required, but these should not be viewed as a replacement for adequate access controls.

EPC Principle 16: *Where audit records are subject to cryptographic authentication the input data to the authentication computation should include an accurate timestamp.*

EPC Principle 17: *Archived audit log files should be protected by appropriate logical and physical security mechanisms.*

3.5 CONFIDENTIALITY

As audit logs contain records of system and network security, they need to be protected from breaches of their confidentiality. Audit logs may intentionally or inadvertently capture sensitive information such as users' passwords and the content of e-mails. Unneeded sensitive data, such as passwords, do not need to be logged and should not be recorded. Where possible, logging should be configured to not record events that are not required and may present a significant risk if accessed by unauthorised parties.

This may raise security and privacy concerns involving both the individuals that review the logs and others that might be able to access the logs through authorized or unauthorized means Strong access controls and encryption can be effective in assuring the confidentiality of data in storage and in transit.

EPC Principle 18: *The capture of customer sensitive data in audit logs should be avoided. If necessary sensitive data should be masked, tokenised or encrypted to avoid data breaches.*

The logging of confidential information may be required in some circumstances. If this is the case, the confidentiality of the information should be protected.

EPC Principle 19: *Where audit data are encrypted, the appropriate decryption software and keys must be available and properly maintained, under appropriate access control, for the whole of the lifetime of the encrypted data. Proper maintenance should include periodic testing and adequate back-up to cater for loss of stored encryption keys.*

3.6 RECORD FORMAT

The greatest need to interrogate audit records will often be associated with emergency situations. In addition, audit data should be able to be demonstrated quickly and easily to a non-IT-expert, such as management, personnel functions, law enforcement agencies or courts. Records may need to be accessed a considerable period of time after their creation, using tools for which they were not designed.

A high level of normalisation needs to be established in order to be able to correlate information/audit trails from several different audit log sources. The higher the normalisation - the higher level of correlation advantages and thus easier to trace a transaction from initiation through execution to termination

EPC Principle 20: *Audit records should be created in a simple standard format.*

3.7 COMPRESSION

Compression can be used to reduce the storage overhead for audit data,

EPC Principle 21: *Where audit data are compressed, the appropriate decompression software must be available and properly maintained for the whole of the lifetime of the compressed data. Proper maintenance should include periodic testing.*

4 MANAGEMENT OF AUDIT LOGS

4.1 OWNERSHIP & CLASSIFICATION OF AUDIT DATA

Ownership and classification of audit data should be clearly established in line with organisational policy.

EPC Principle 22: *The ownership of audit data should be clearly defined.*

EPC Principle 23: *Audit records should be classified at a level commensurate with the classification of the systems and data they are intended to protect.*

4.2 GENERATION OF AUDIT TRAILS

In order to assure that audit logs are complete and consistent, security controls should be in place regarding the programs or processes that generate the logs. This includes the supporting configuration files which may be used, for example, to set the level of the logging functionality to conservative initially. A single setting could cause an enormous number of records to be generated. Excessive logging could cause loss of log data as well as operational problems such as denial of service or system slow down. Conservative settings should only be used for the initial period of logging and not be used for extended periods.

EPC Principle 24: *Changes to programs or the configuration of programs (e.g. Job Control Language) that generate audit logs should themselves be logged in an independent change log.*

EPC Principle 25: *Periodic independent tests should be made to assure that all events that are expected to be logged are actually included in the logs.*

EPC Principle 26: *Access to the source code and configuration files of logging programmes should be protected from access by the originator of the events being recorded.*

EPC Principle 27: *The set-up of log programs and procedures should be documented and properly approved and tested.*

EPC Principle 28: *Audit logs should include the registration of any period of time during which logging has been disabled.*

4.3 NAMING CONVENTIONS

EPC Principle 29: *Audit logs should be named using a clear, explicit and efficient naming convention.*

Consideration should be given to using the filename to refer to the system, the recorded period, and the type of recorded event (if different logs are generated for specific events, e.g. system-technical events, application events, user events).

4.4 PLACE OF STORAGE / ARCHIVING

The place of storage of logs (within the company, the region, the country etc.) should be chosen such that audit logs that are stored off line are available in a timely fashion when needed.

EPC Principle 30: *The storage location of audit logs should be chosen such that access to the logs can be made within a clearly defined response time.*

4.5 CONTROLS ON ACCESS

Access control rules and rights should be clearly stated in an access control policy. Access controls are both physical and logical and should be considered together. Audit trails should be reviewed on a regular basis by a party other than the originator of the event.

EPC Principle 31: *Security-related audit records should be protected from modification or deletion by the originator of the event. Changes of security related audit records should be traced by recording the originator of the changed event.*

EPC Principle 32: *System administrator and auditor privileges should not rest with the same individual.*

EPC Principle 33: *Those responsible for reviewing audit records should not have sufficient privilege to be able to originate the events that are recorded.*

EPC Principle 34: *Auditors and anyone authorised to access audit logs should only be granted read-only access; only specific applications & systems which require it should have write access to audit logs.*

EPC Principle 35: *Unauthorised parties should not be able to manipulate processes, files, or other components that could impact audit logging.*

4.6 REVIEW PERIOD

The timing of audit log review depends upon the nature of the event being audited. The table in section Appendix B provides guidance on those events which require immediate attention. It may be appropriate to take automatic action on the detection of an audited event (though note Principle 3); in any event human operators are preferred.

EPC Principle 36: *Routine review of audit logs by human operators should be established in a manner which is commensurate with the risks to the system being protected.*

4.7 RECORDS HELD BY THIRD PARTIES

Audit data may be retained by third parties operating facilities management or outsourced systems. The role of each service provider should be documented. The third party is responsible for validating their compliance to the specified service requirement

EPC Principle 37: *Where systems producing audit data are outsourced, the contracting party should define an appropriate access policy for the third party.*

4.8 LONG TERM STORAGE OF AUDIT LOGS

Organisations have requirements and guidelines for the storage of data, so that audit logs are kept for the required period of time. If the retention period for storage of the audit logs is relatively short, it may be adequate to keep the logs online and capture them in the regular system backups. If the retention period is relatively long (e.g. years) then the logs should be archived.

EPC Principle 38: *Audit log files should be periodically saved and moved to another storage space. The periodicity may be influenced by the classification of the data, but should be defined by the retention period.*

EPC Principle 39: *The integrity of transferred Audit logs should be verified. This could be done by message digests for each audit log file.*

Archived Audit Logs may be required to be preserved for a considerable time. Cryptographic information required for signing and decrypting, , in particular, should be preserved The information should be stored according to the Organisation's policy for long term retention of information.

EPC Principle 40: *The archived Audit logs should be appropriately protected. Unauthorised physical access should be prevented. Appropriate environmental controls should be applied to prevent damage to the media.*

4.9 BACK-UP

As with all data, routine back-up of audit data is essential. Periodic testing of recovery from backups should be carried out in accordance the organisation's normal business continuity policy.

EPC Principle 41: *Audit data which are backed-up should be subject to the same level of access control and the same level of security measures as the original data.*

EPC Principle 42: *Ensure that the backup of the audit data is tested on a regular basis to ensure that it is still readable.*

4.10 DISPOSAL OF AUDIT TRAIL INFORMATION

Once the required retention period has ended it is necessary to dispose of audit logs. This would include audit logs stored on systems, regular backups and archival media. A variety of methods for the secure disposal of media exist and a method appropriate to the sensitivity of the logs (established under Principle 23) should be chosen.

In order to decide on the most appropriate way of disposal of the audit trail information the information should be categorised, the nature of the medium on which it is recorded should be assessed, the risk to confidentiality should be assessed, and the future plans for the media should be determined. The selected type of disposal should be assessed as to cost, environmental impact, etc., and a decision made that best mitigates the risk to confidentiality and best satisfies other constraints imposed on the process.

See NIST Special Publication 800-88 Guidelines for Media Sanitisation for further information

EPC Principle 43: *Audit logs should be disposed of in a fashion commensurate with their security classification.*

5 RETENTION PERIOD

With the recent increase in e-discovery concerns, retention policies have become an essential proactive step in any organisation's information security preparedness. There are many laws, regulations and contracts that may include obligations to maintain information for a given period, and each have their own time periods and criteria. Examples include:

- The Basel II Accord - Affects international banks. Activity logs should be retained 3-7 years
- The Sarbanes-Oxley Act (SOX) - Affects US Corporations. Specifies retaining audit logs for up to seven years.
- VISA Cardholder Information Security Program (CISP) - Specifies retaining audit logs for at least six months.[1]

In most cases, the type of business will define the external requirements for information retention, and these periods range greatly. Legal counsel and audit staff should always be included in the development process for any data retention policies to ensure the business is complying with all contracts, local laws, industry regulations, and national or international laws. Audit logs relating to specific transactions should be kept for at least as long as the transaction data.

Any data retention provisions cannot be successful without first having a clear information classification standard and performing discovery efforts to determine what is stored in the environment and where.

In all cases, the confidentiality, integrity, availability, and accountability of the evidence should be preserved in a documented and defendable manner. Any sensitive data needs to be protected at every stage of its lifecycle in the organisation including handling, storage, and archival. Data retention policies need to address these issues as well as acceptable tools for use in the destruction of data.

The organisation's retention policy should include the retention requirements for audit events. This policy should take into account local national policy and regulatory requirements for retention. For example the Payments Service Directive states that 'An authorised payment institution must maintain relevant records and keep them for at least five years from the date on which the record was created.'

EPC Principle 44: *Organisations should ensure that audit retention is part of the organisation's overall retention policy.*

6 APPLICATION AND USE OF AUDIT LOGS

6.1 SYSTEMS MANAGEMENT AND MONITORING

Section 3 recommends that generation of alarms and alerts from audit data should be considered where timely response is required in reacting to certain critical events. However audit trails should not be regarded as the primary preventative measure.

EPC Principle 45: *Where the execution of sensitive security-related actions cannot be made subject to dual control, then that execution should be monitored in a timely fashion.*

As noted in section 3, users of audit logs will usually be interested in unusual events and wish to use exception reporting rather than routine scanning of log data.

6.2 INTERNAL INVESTIGATIONS

When a computer security incident is identified, as defined by the organisation's incident response policies, the organisation's incident response procedures should be followed to ensure that it is addressed appropriately.

When an incident occurs, affected system-level administrators may be asked to review their systems' audit logs for particular signs of malicious activity or to provide copies of their logs to incident handlers for further analysis. The life cycle of incidents is described in Appendix C.

Some examples of key data sources that may be useful when investigating an incident include:

- Firewall logs including denied and permitted traffic ,
- Internet gateway logs including web proxies, web filters, and network devices ,
- Name and address assignment/resolution history (such as dynamic DNS or DHCP records) ,
- Web, application, and file server logs,
- Email and Instant Messenger communications from server and client logs ,
- Authentication and authorization service logs ,
- Workstation audit logs (account activity, system events, etc.),
- Server operating system audit logs (in addition to application software logging) ,
- Intrusion Detection / Prevention System logs ,
- Malware detection and removal logs,
- Network infrastructure or monitoring devices

EPC Principle 46: *An organisation should determine which data is classified as audit data and should protect and preserve this data appropriately.*

EPC Principle 47: *Personal notes should be kept by incident investigators throughout the whole course of an investigation and those notes should themselves be protected and preserved in the same manner as audit data.*

EPC Principle 48: *Audit records used during an investigation must be preserved at least until the end of the investigation and for any subsequent prosecution irrespective of their normal retention period.*

EPC Principle 49: *Follow the organisation's incident response policy to investigate an audit log incident.*

EPC Principle 50: *System configuration information should be modified, if necessary, to prevent an event from overwhelming the system.*

6.3 PRESENTATION IN COURT

Clearly the legal admissibility of audit records is dependent upon the requirements of the national or local jurisdiction. Nevertheless, in general, records presented in court will need to be supported by a stronger chain of evidence than those used in internal investigations. Guidance derived from the UK Metropolitan Police Computer Crime Unit (as quoted in the CSFI report) is reproduced in Appendix D. It may also be useful to refer to the CPNI – NISSC report on An Introduction to Forensic Readiness Planning.

7 SUMMARY OF PRINCIPLES

These guidelines recommend the following principles:

Audit System design

1. Audit facilities should be designed with their specific use(s) in mind, not simply adapted from existing system logs.
2. Organisations should create and maintain an audit log management structure, including policy, procedures, rules and tools.
3. Where a single business or system transaction will result in the creation of audit data on multiple systems, design consideration should be given to how the complete audit information about that transaction will be collated and made available to a ”user of the audit logs”.
4. Organisations should provide appropriate support, e.g. training, provision of appropriate tools, for all staff that will be making use of the audit logs.
5. Audit log files should be periodically saved and moved to another storage space. The periodicity may be influenced by the classification of the data, but should be defined either according to a fixed size (e.g. every time the log reaches 1Mb) and / or according to a fixed period of time (e.g. per day, per week).
6. Attacks on systems should be prevented by the use of technical preventive controls. These controls should be preferred above procedural preventive controls if possible. Both measures should be used in conjunction with examination of the audit data.
7. Organisations should consider the use of a Security Event management system due to the large volume of security events.
8. Organisations should not solely rely on unauthorised events or breaches of policy, but should additionally consider proactive monitoring.
9. Organisations should consider the use of Security information and event management (SIEM) technology to help the automation and collection of auditable events.
10. All audit records should contain a time stamp. Ensure that each system’s clock is synched to a common time source so that its timestamp will match those generated by other systems.
11. The privacy of personal data should be protected.
12. Measures should be implemented in order that deleting or modifying logs of own activities should be detected and alerted immediately.
13. Administrators should not be able to erase or de-activate logs of activities.
14. Audit events should be protected from modification by using digital signatures to sign audit records.
15. Audit events should be archived to ‘write-once ‘media to protect the archive from modification or deletion.
16. Where audit records are subject to cryptographic authentication the input data to the authentication computation should include an accurate timestamp.

17. Archived audit log files should be protected by appropriate logical and physical security mechanisms.

18. The capture of customer sensitive data in audit logs should be avoided. If necessary sensitive data should be masked, tokenised or encrypted to avoid data breaches.

19. Where audit data are encrypted, the appropriate decryption software and keys must be available and properly maintained, under appropriate access control, for the whole of the lifetime of the encrypted data. Proper maintenance should include periodic testing and adequate back-up to cater for loss of stored encryption keys.

20. Audit records should be created in a simple standard format.

21. Where audit data are compressed, the appropriate decompression software must be available and properly maintained for the whole of the lifetime of the compressed data. Proper maintenance should include periodic testing.

Management of audit logs

22. The ownership of audit data should be clearly defined.

23. Audit records should be classified at a level commensurate with the classification of the systems and data they are intended to protect.

24. Changes to programs or the configuration of programs (e.g. Job Control Language) that generate audit logs should themselves be logged in an independent change log.

25. Periodic independent tests should be made to assure that all events that are expected to be logged are actually included in the logs.

26. Access to the source code and configuration files of logging programmes should be protected from access by the originator of the events being recorded.

27. The set-up of log programs and procedures should be documented and properly approved and tested.

28. Audit logs should include the registration of any period of time during which logging has been disabled.

29. Audit logs should be named using a clear, explicit and efficient naming convention.

30. The storage location of audit logs should be chosen such that access to the logs can be made within a clearly defined response time.

31. Security-related audit records should be protected from modification or deletion by recording the originator of the event. Changes of security related audit records should be traced by recording the originator of the changed event.

32. System administrator and auditor privileges should not rest with the same individual.

33. Those responsible for reviewing audit records should not have sufficient privilege to be able to originate the events that are recorded.

34. Auditors and anyone authorised to access audit logs should only be granted read-only access; only specific applications & systems which require it should have write access to audit logs.

35. Unauthorised parties should not be able to manipulate processes, files, or other components that could impact audit logging.

36. Routine review of audit logs by human operators should be established in a manner which is commensurate with the risks to the system being protected.

37. Where systems producing audit data are outsourced, the contracting party should define an appropriate access policy for the third party.

38. Audit log files should be periodically saved and moved to another storage space. The periodicity may be influenced by the classification of the data, but should be defined by the retention period.

39. The integrity of transferred Audit logs should be verified. This could be done by message digests for each audit log file.

40. The archived Audit logs should be appropriately protected. Unauthorised physical access should be prevented. Appropriate environmental controls should be applied to prevent damage to the media.

41. Audit data which are backed-up should be subject to the same level of access control and the same level of security measures as the original data.

42. Ensure that the backup of the audit data is tested on a regular basis to ensure that it is still readable.

43. Audit logs should be disposed of in a fashion commensurate with their security classification.

Retention Period

44. Organisations should ensure that audit retention is part of the organisation's overall retention policy.

Application and use of Audit Logs

45. Where the execution of sensitive security-related actions cannot be made subject to dual control, then that execution should be monitored in a timely fashion.

46. An organisation should determine which data is classified as audit data and should protect and preserve this data appropriately.

47. Personal notes should be kept by incident investigators throughout the whole course of an investigation and those notes should themselves be protected and preserved in the same manner as audit data.

48. Audit records used during an investigation must be preserved at least until the end of the investigation and for any subsequent prosecution irrespective of their normal retention period.

49. Follow the organisation's incident response policy to investigate an audit log incident.

50. System configuration information should be modified, if necessary, to prevent an event from overwhelming the system.

8 APPENDIX A: EUROPEAN-WIDE LEGAL & REGULATORY REQUIREMENTS

The most important EU Directive relating to preservation of audit records is that “on the protection of individuals with regard to the processing of personal data and on the free movement of such data”, 95/46, commonly known as the Data Protection Directive.

8.1 EU DATA PROTECTION DIRECTIVE

This applies to the **processing** of **personal data**, with the terms defines as follows:

- "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
- "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

The basic principles are set out in Article 6:

> 1. Member States shall provide that personal data must be:
>
> (a) processed fairly and lawfully;
>
> (b) **collected for specified, explicit and legitimate purposes** and not further processed in a way incompatible with those purposes. **Further processing of data for historical**, statistical or scientific **purposes shall not be considered as incompatible** provided that Member States provide appropriate safeguards;
>
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or for which they are further processed;
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
>
> (e) **kept in a form which permits identification of data subjects for no longer that is necessary** for the purposes for which the data were collected or for which they are further processed. **Member Sates shall lay down appropriate safeguards for personal data stored for longer periods** for historical, statistical or scientific use.

Those parts which are directly relevant to the storage of audit records are emboldened.

Article 13 sets out exemptions and restrictions:

> 1. **Member States may** adopt legislative measures to **restrict the scope of the obligations and rights provided for in Articles 6(1)**, 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure **to safeguard**:

(a) national security;

(b) defence;

(c) public security;

(d) **the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions**;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) **a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority** in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

Finally, Article 17 addresses the security of processing

1. Member States shall provide that **the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorised modification, disclosure or access,** in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the costs of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Members States' national legislation should support these aims.

9 APPENDIX B: RESPONSE TO EVENTS

	RECORDING			RESPONSE			
Event	Mandatory	Recommended	Good practice	Immediate	Routine	Historic	**Other comments** *Could include specific fields to be recorded (see 4.1)*
Account management							
Account creation	*				*		Immediate response is recommended for the allocation of the highest privilege level.
Re-setting of users' passwords	*				*		
Account deletion	*				*		
Modification of Privileges	*			*			
Cryptographic key management							
Key generation	*			*			
Key backup	*				*		
Key Renewal	*				*		
Certificate creation	*				*		
Certificate revocation	*			*			
Key withdrawal / destruction	*			*			
Token management							
Token issue	*				*		

	RECORDING			RESPONSE			
Event	Mandatory	Recommended	Good practice	Immediate	Routine	Historic	**Other comments** *Could include specific fields to be recorded (see 4.1)*
Change of token access credentials (e.g. PIN)	*				*		
Token failure or withdrawal	*				*		
Other system administration							
Create data backups		*			*		
Restore data from backups	*				*		
Install new software	*				*		
Install new hardware	*				*		
Modification of audit logs	*			*			
Delete audit logs	*			*			
User access							
Single successful log-on	*					*	Passwords themselves must **not** be recorded
Log-on from remote location	*				*		
Concurrent log-on from different locations	*			*			
Single failed log-on	*					*	
Multiple failed log-on	*				*		Say > 5 unsuccessful attempts. Link to lock-out limits if implemented.
User-initiated password change		*				*	

	RECORDING			RESPONSE			
Event	Mandatory	Recommended	Good practice	Immediate	Routine	Historic	**Other comments** *Could include specific fields to be recorded (see 4.1)*
All privileged operations	*				*		Use of privileged accounts
User actions							
Create / delete file		*		*	*	*	Dependent on data classification
Edit / print file			*	*	*	*	Dependent on data classification
Modify file access permissions			*			*	Dependent on data classification
Creation of a value-transfer transaction [1]	*				*		May require consideration of actual value involved
Authorisation / authentication of a value-transfer transaction	*				*		
Unauthorised access attempts	*			*			Includes alerts from intrusion detection systems
System alerts or failures							
Console Alerts or messages		*			*		
System Log exceptions		*			*		
Network Management alarms	*			*			
Access Control System alarms	*			*			

[1] This might include a payment instruction, a contract or a securities transfer such as share dealing.

10 APPENDIX C: LIFE-CYCLE OF INCIDENTS AND INVESTIGATIONS

No two computer investigations are identical. However, the timeline shown below gives an indication of the number, complexity and duration of typical corporate tasks that may occur, and for which a management framework is essential. The actual details may vary considerably.
The table concentrates on what happens in an "incident". Note that many of the tasks shown here will operate concurrently. This table is adapted from the IAAC report 'Directors and Corporate Advisors Guide to Digital Investigations and Evidence' http://www.iaac.org.uk/Portals/0/DigitalInvestigationsGuide.pdf

Incident Lifecycle

Detection: Detection may be prompted by a dramatic event, such as the arrival of an extortion demand or the failure of major services or by no more than a suspicion triggered by anomalous behaviour.
Reporting: All organisations need a designated point to which reports can be made, whether corporate security, computer security, audit, the company secretary, human resources or a legal adviser. In practice the full extent of an incident may take some time to evolve, so there could be several reports. In addition, some reports will turn out to be false.
Diagnosis – initial: Whoever receives the report should have the skill, experience, resources to make an assessment of what may have happened and to provide initial guidance about how the organisation should tackle the problem
Management actions based on initial diagnosis: At this point, the relevant executives will be informed and staff detailed to carry out specific tasks. This will usually involve setting up a special "taskforce".
Evidence collection:
This is one of the most important early stages. It includes identifying likely sources of evidence, collection under controlled conditions and preservation.
Diagnosis – mature:
Initial diagnoses are likely to be wrong. Evidence collection soon moves into evidence assessment, with a consequential effect on how the problems are perceived. Few crises are so purely computer-based that the only kind of evidence is obtained from computers. The ongoing process of diagnosis will take in evidence from and about individuals and businesses and paper based documents.
Management actions based on mature diagnosis:
As the nature of the problem becomes clearer, the organisation is able to define its objectives with greater clarity and certainty. Once the immediate risks to the integrity of information systems have been resolved, corporate aims will have a more long-term focus.
Business/asset recovery activity:
If computer systems have been compromised, there has been some interruption to business, assets have been lost or some aspect of the crisis has become public, there will need to be a business recovery phase, similar to that after premises have been affected by fire or flood., Experience from the established disaster recovery/business contingency planning industry suggests that full recovery

always takes much longer than expected. Typical tasks include: restarting computer systems; recovering lost assets; and public relations.
Remedial activity:
This includes learning lessons, preventing repetition, introducing new management and audit procedures, and new security engineering facilities. These lessons may extend beyond the immediate events to problems with corporate culture and management structure
Civil legal activity:
This covers, for example, insurance claims, asset recovery, claims for damages, negligence, breach of confidence, etc.
Law enforcement agency activity:
There may be several phases of law enforcement activity: initial enquiries; collection of statements and evidence; return visits for further interviews and search for evidence; preparation for trial; and attention to defence requests for disclosure.
Criminal and regulatory proceedings:
A complex criminal trial may go through several phases, including committal and the substantive trial. Further information may be requested during the trial process.

11 APPENDIX D: TREATMENT OF DATA DURING INVESTIGATIONS

11.1 EVIDENCE PRESERVATION FOLLOWING AN INCIDENT

It is critical that as much evidence (and other information) as possible is gathered at this stage as there may not be an opportunity to gather it at a later time. It should be noted that the quality of the outcome of an investigation will be highly dependent on the quality of the information that is provided as a result of the incident response. Preservation of evidence (for subsequent presentation in court in the event of a prosecution) is a critical factor in any criminal investigation. The appropriate action to take to preserve the evidence will depend on the circumstances but may involve actions ranging from copying unmodified computer logs to CD/DVD through to forensic copying of computer hard drives.

Forensic copying of computer hard drives by appropriately trained personnel is the most effective means of preserving ALL of the evidence; however, it is also the most intensive and time consuming.

Sources of evidence may include any or all of the following:

- Systems that have been compromised;
- Hard drives of systems that have been compromised;
- Web, mail, ftp or any other relevant server logs;
- Proxy logs;
- RADIUS logs;
- Intrusion Detection System (IDS) logs;
- Firewall logs;
- Router logs.

11.2 DIGITAL EVIDENCE

The International Organisation on Computer Evidence (IOCE) has developed a set of principles when establishing procedures for the collection, preservation and use of digital evidence, according to its national law and standards bodies, and to be aware of potential differences when collecting evidence at the request of other States. See http://www.ioce.org/core.php?ID=1 for more information. These principles are:

- When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
- All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.

- An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

11.3 COMPUTER BASED ELECTRONIC EVIDENCE

Shown below are brief recommendations for the collection of computer based electronic evidence, derived from the UK Metropolitan Police Computer Crime Unit.

- Keep a written log of all action taken during the investigation of an incident
- Put a single individual in charge of any investigation
- Preserve system logs by archiving off the target system
- Record any discrepancies in the system clock and do not adjust it during an investigation
- Do not rely on the integrity of the target machine's operating system or other utilities (so examine it from a remote machine if possible)
- Where an attack is still in progress, adopt a clear policy on whether to continue monitoring or to attempt to exclude the intruder – this is wholly up to the organisation being targeted
- Once it has been secured, conduct a thorough investigation of the means used to access the system; do not exclude the possibility of internal collusion
- Pay particular attention to gathering network address information originating from the attacker (IP addresses, CLI data etc.)
- Identify and preserve previous system backups, which can be used to establish modifications to the system made by the intruder
- Notify the police as soon as possible

See the link below for further information.
http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf