TRIANZ℠

Information Security Logging and Monitoring Procedure

TRIANZ INTERNAL

trianz.com

Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

Information Classification

☐	Public
☒	Internal
☐	Confidential
☐	Restricted

Table of Contents

1. Objectives

To monitor the logging of events, association of each logged event with a particular user, provision or a mechanism to retrieve and report information on logged events and reporting on the effectiveness and compliance with standards including but not limited to ISO 27001: 2022 & ISO 27701: 2019

2. Scope

This procedure applies to all Trianz users and operating units including the third parties, Cloud Providers, Cloud Customers and all Trianz Information System Resources including corporate data, as well as the application and systems software

3. Procedure

3.1 Purpose of Monitoring

- To safeguard information and computing resources from various business and environmental threats, the activities related to the use of Trianz Information System Resources will be monitored.
- Ensure that the information on these systems is not disclosed to unauthorized individuals and that the integrity of the data is maintained.
- Monitoring is also done to ensure conformity to Logical Access Security Policy and related procedures, Back-up Methods etc.

3.2 Audit Trail Rules

- Auditing must be enabled on all the Servers and Network Devices for recording exceptions and other security-related events.
- If possible, all audit records should be sent to central server for monitoring and correlation.
- All physical and logical access logs, audit trails etc. shall be retained for a minimum of five years.
- A record of successful system access, in addition to rejected attempts, should be created. At a minimum, audit trails must include the following: -

  - ➢ User ID's
  - ➢ Date/time of the most recent attempt
  - ➢ Dates and times for logon and logoff
  - ➢ Terminal identity or location identifier
  - ➢ IP address and source
  - ➢ Computer name and source

3.3 Monitoring of System Use

- The systems use must be monitored to ensure that users are performing processes that have been explicitly authorized.
- The level of monitoring required for individual systems should be determined by a separate risk assessment. Areas that must be monitored are:
- Access failures
- Allocation and use of accounts with a privileged access capability
- Tracking of selected transactions
- The use of sensitive resources
- IDS/IPS activity
- Firewall activity.
- O/S and application access attempts
- Cloud account access details
- Malware and ransomware detection alerts from AV

- Real-time alerts for publicly accessible systems (e.g. external web sites) for any suspicious user activity.
- Browser Weakness and Updates

3.4 Logging: Control

Logs that record activities, exceptions, faults, and other relevant events should be produced, stored, protected, and analyzed.

3.5 Purpose

To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations. Guidance The organization should determine the purpose for which logs are created, what data is collected and .logged, and any log-specific requirements for protecting and handling the log data. This should be documented in a topic-specific policy on logging. Event logs should include for each event, as applicable:

- ➢ user IDs.
- ➢ system activities.
- ➢ dates, times and details of relevant events (e.g. log-on and log-off);
- ➢ device identity, system identifier and location.
- ➢ network addresses and protocols.

The following events should be considered for logging:

a) successful and rejected system access attempts.
b) successful and rejected data and other resource access attempts.
c) changes to system configuration.
d) use of privileges.
e) use of utility programs and applications.
f) iles accessed and the type of access, including deletion of important data files.
g) alarms raised by the access control system.
h) activation and de-activation of security systems, such as anti-virus systems and intrusion detection systems.
i) creation, modification, or deletion of identities;

j) transaction executed by users in applications. In some cases, the applications are a service or product provided or run by a third party.

It is important for all systems to have synchronized time sources (see 8.11) as this allows for correlation of logs between systems for analysis, alerting and investigation of an incident.

3.6 Protection of logs

Users, including those with privileged access rights, should not have permission to delete or deactivate logs of their own activities. They can potentially manipulate the logs on information processing facilities under their direct control. Therefore, it is necessary to protect and review the logs to maintain accountability for the privileged users.

Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility including:

a) alterations to the message types that are recorded.

IS/ISO/IEC

b) log files being edited or deleted.

c) failure to record events or over-writing of past recorded events if the storage media holding a log file is exceeded.

For protection of logs, the use of the following techniques should be considered: cryptographic hashing, recording in an append-only and read-only file, recording in a public transparency file.

Some audit logs can be required to be archived because of requirements on data retention or requirements to collect and retain evidence

Where the organization needs to send system or application logs to a vendor to assist with debugging or troubleshooting errors, logs should be de-identified where possible using data masking techniques (see 8.11) for information such as usernames, internet protocol (IP) addresses, hostnames, or organization name, before sending to the vendor. Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures should be taken

3.7 Log Analysis:

Log analysis should cover the analysis and interpretation of information security events, to help identify unusual activity or anomalous behavior, which can represent indicators of compromise.

Analysis of events should be performed by considering:

a) the necessary skills for the experts performing the analysis.

b) determining the procedure of log analysis.

c) the required attributes of each security-related event.

d) exceptions identified through the use of predetermined rules [e.g. security information and event management (SIEM) or firewall rules, and intrusion detection systems (IDSs) or malware signatures];

e) known behavior patterns and standard network traffic compared to anomalous activity and behavior [user and entity behavior analytics (UEBA)].

f) results of trend or pattern analysis (e.g. because of using data analytics, big data techniques and specialized analysis tools).

g) available threat intelligence.

Log analysis should be supported by specific monitoring activities to help identify and analyze anomalous behavior, which includes:

- ➢ reviewing successful and unsuccessful attempts to access protected resources [e.g. domain name system (DNS) servers. web portals and file shares].
- ➢ checking DNS logs to identify outbound network connections to malicious servers, such as those associated with botnet command and control servers.
  - o examining usage reports from service providers (e.g. invoices or service reports) for unusual activity within systems and networks (e.g. by reviewing patterns of activity).

    - including event logs of physical monitoring such as entrance and exit to ensure more accurate detection and incident analysis.

- correlating logs to enable efficient and highly accurate analysis. Suspected and actual information security incidents should be identified (e.g. malware infection or probing of firewalls) and be subject to further investigation (e.g. as part of an information security incident management process, see 525), Other information. System logs often contain a large volume of information, much of which is extraneous to information security monitoring.

  To help identify significant events for information security monitoring purposes, the use of suitable utility programs or audit tools to perform file interrogation can be considered. Event logging sets the foundation for automated monitoring systems (see 8.16) which can generate consolidated reports and alerts on system security.

  A SIEM tool or equivalent service can be used to store, correlate, normalize and analyze log information, and to generate alerts. SIEMs tend to require careful configuration to optimize their benefits. Configurations to consider include identification and selection of appropriate log sources, tuning and testing of rules and development of use cases.

  Public transparency files for the recording of logs are used, for example, in certificate transparency systems. Such files can provide an additional detection mechanism useful for guarding against log tampering.

  In cloud environments, log management responsibilities can be shared between the cloud service customer and the cloud service provider. Responsibilities vary depending on the type of cloud service being used.

3.8 Monitoring of Firewall Audit Reports

- The designated IS Administrator in IS Department will review the Internet connection audit reports created on the firewall for any unusual/suspicious activities.
- The period between reviews should not exceed a week. Alarms must be configured to alert the IS Administrator about any suspected activities, security

breaches or violations and any other related events generated by the firewall. The events to be monitored include, but not limited to:

- A session being initiated from the external world
- Spoofing activities
- Suspicious activities taking place internally and from external sources
- Well known hacker signatures
- Password guessing attempts
- Attempts to use privileges that have not been authorized
- Modifications to production application software
- Modification to system software
- Beaconing behavior towards suspicious domains

3.9Windows Environment

Logging and reporting Details/Test:

Windows comes with several monitoring and auditing tools, which enable powerful logging and auditing. In the absence of auditing and logging, it may not be possible to:

Track the attacker in the event of a security breach

Detect unauthorized access attempts to resources.

Track the causes for errors or unauthorized changes (if any).

Have control over changes to critical settings, like the Registry.

Thus, detective controls become very weak in the absence of appropriate monitoring *and auditing.*

It is recommended that the auditing and monitoring features of Windows be used effectively.

Some of such events are:

o Audit account logon events = Success, Failure

o Audit account management = Success, Failure o Audit directory service access = Failure

o Audit logon events = Success, Failure

o Audit object access = Failure

o Audit policy change = Success, Failure

o Audit privilege use = Failure

o Audit process tracking = No auditing

o Audit system events = Success, Failure

o UNIX environment

o Logging and reporting

o Details/Test:

o The following system logs should be reviewed and have restricted access: /etc/wtmp - contains a history of system logins. (This file is not plain text and needs to be

interpreted by a UNIX utility such as “who”.

/usr/adm/sulog - Review the contents of this file, it logs the use of the su command. The su (super user) command can compromise security by accessing files belonging to other users without their knowledge.

In order to access such files, the password of the file owner must be known. Use of this command shall evidence the inappropriate use of a password by other users.

/usr/bin/uulog - contains a history of each use of uucp, uuto, and uux.

/etc/security/failedlogin - Review the log to determine list of failed login.

Enable logging for specific commands such as kill, killall, chown, chmod, shutdown and chgrp using TCB (if installed)

In case of FTP services, FTP logs should also be maintained as this service is highly critical and sensitive from security aspects, therefore, it is recommended to monitor the FTP activities regularly.

Note: The most important files to be reviewed are /usr/adm/syslog and /usr/adm/messages (or equivalent). Enabling only selected auditing features may have limited affect on the performance of the Application or Server.

3.10 Oracle Environment

Logging and reporting Details/Test:

- Policies and procedures to review audit trails in a timely manner and developing an audit trail archiving strategy shall be adopted. This strategy shall address the following:
- archive rotation period (the amount of time before an archive can be overwritten);
- security of the audit trails - archive logs (confidentiality and integrity); and redundancy of the audit trails (disaster recovery planning)

- The enabling of auditing feature in a database shall be as per the business and operational requirements.
- The concerned Department shall first identify the relevant critical tables in a database which are
- required to be kept confidential from the organization's perspective and then the auditing features can be enabled for those critical areas.
- Trianz would ensure that if logs of the User transactional level details at Application level are being captured, then the Auditing at Database Level can be restricted to key actions such as account logon, modification to system settings, etc.
- These activities can be identified after evaluating their impact on the business or operations and shall be monitored for a period to analyze the effect on the performance of the system.

The following auditing features would be logged depending upon the requirements:-

- Application Account Activity
- Failed Attempts to Access Objects
- Failed Attempts to Issue Sensitive Commands
- Failed Connections
- Failed Login Attempts

Fire call Accounts: - 'Fire call' accounts have a very high, if not unlimited, level of privilege within a database. These accounts are only used for emergency purposes and should be secured accordingly. Actions performed by these accounts should be audited for identification of irregular and/or unauthorized use or as a reference as to what occurred when a 'Fire call' account was used in an emergency.

If actions performed by 'Fire call' accounts are not audited, use of these accounts in an irregular or unauthorized manner could go unnoticed. Additionally, retracing the events that occurred during an emergency would not be possible.

3.11 Cloud Environment

- Trianz would maintain the logs of Operations and Maintenance for necessary CAPA (Corrective action and Preventive Action)
- Also, would implement additional logging capabilities, if needed
- Ensures the Controlled Access to Log information (used for Monitoring and Operational Diagnostics) as it would contain the PII Information

4. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Technological Control	8.15 Logging Control Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed. 8.16 Monitoring activities Control Networks, systems and applications shall be Monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.	Information Security Logging and Monitoring Procedure
Organizational Controls	5.28 Collection of evidence Control The organization shall establish and implement	Information Security Logging and Monitoring Procedure

	procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	

Document Control

Owner:	CISO	**Release ID:**	ISAM-PROC-0044

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.00	19-Feb-07	Jyotessh G Nair	_	_	Initial draft	
1.00	26-Feb-07	Jyotessh G Nair	_	_	Baseline is approved by Zulfikar Deen.	Approved Baseline.
1.01	14-May-09	Bharateesha B R	_	_	Risk Assessment and Risk Treatment Plan	Consolidated the controls related to audit management
2.00	03-Jun-09	Balu Nair	_	_	Approval for Baseline	Approved
2.01	30-Dec-10	Chakravarthi	_	_	QMG review	• Formatting entire document • Updated properties
3.00	30-Dec-10	Chakravarthi	_	_	Request for baseline	☒ Baselined
3.01	24-May-11	Srilakshmi	_	_	QMG Review	Modified release id in header and cover page to make consistency

4.00	24-May-11	Srilakshmi	_	_	Approval for Baseline	Baselined
4.01	3-Aug-11	Sudharsana	_	_	QMG review	□ Replace Owner with Management Representative in place of CIO In Document Classification Scheme, "Retention period is 3 Years" row is removed

5.00	3-Aug-11	Sudharsana	_	_	Request for baseline	Approved and Baselined
6.00	28-Sep-12	Sudharsana	_	_	QMG review	Formatted as per latest template format
6.01	16-Oct-16	Sriharsha & Shishir	_	_	Addition of Cloud services as scope of Certification.	Modified the procedure to align with cloud service related process steps . Added Vulnerability Assessment and Penetration Testing (VAPT) under section 4.8
7.00	07-Dec-16	Balu Nair	_	_	Approved by CISO	Baselined

8.00	23-Jun-18	Kamadev Pradhan	–	–	Reviewed the documents	No changes done in the Document
8.1	29-Apr-19	Balu Nair	Joshy VM			• Information classification modified • Trianz Logo Modified No Major
9.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
10.0	24-Nov-19	Vijaya Rajeswari Veldurthy	Phani Krishna	Vivek Sambasivam	Aligning to ISO 27017 & 27018 Standards	Roles and Responsibilities are updated to align to ISO 27017 & 27018 Standards
10.1	11-May-20	Karthik N	Balu Nair		Review	Integrated to new format
11.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
11.1	14-Jan-21	Balu Nair	Phani Krishna		Review	Updated the information classification Formatted and corrected few portions
11.2	11-Feb-21	Balu Nair	Rajesh B		Review	Updated audit trail rules and monitoring of system bulletins
12.0	12-Feb-21	Balu Nair	Phani Krishna	Phani Krishna	Approved for Baseline	Approved and Baselined

12.1	07-Oct-21	Karthik N	Karthik N		Review	Format changes
13.0	11-Oct-21	Karthik N	Karthik N	Sivaramakri shnan N	For Approval	Approved and Baselined
14.0	30th Oct 2021	Pranesh Kulkarni	Siva Krishna / Gangadhar Aka	Gangadhar Aka	Updates and Review	Section 3.3 : Added the monitoring of Browser Weakness and Updates
14.0	21-12-2021	Karthik N	Karthik N		Annual Review	No changes
14.1	06-01-2023	Sanjana	ISDP Team		As per client feedback	Modified log retention period
15.0	06-01-2023	Sanjana	ISDP Team	Srikanth Mantena	For approval	Approved and Baselined
15.1	28-Mar-23	Sanjana, Rama Madhavan	ISDP team		For review	Reviewed with no changes New template change
16.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For Approval	Approved and Baselined
16.1	15-Feb-24	Shalini	Vijaya		For Review	Mapped with New ISO control 27k, 2022 8.15 and 8.16
17.0	23-Feb-24	Shalini	Vijaya	Srikanth	For Approval	Approved and Baselined
17.1	2-May-2025	Vijaya	Balu		For review	Migrated to new template
18.0	14-May-2025	Vijaya	Balu	Srikanth	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com