TRIANZ℠

Information System Audit
Trial Management 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 ISO 27001:2022 standard.

2. Scope

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

3. Reference(s)

None

4. Procedure

4.1 Purpose of Monitoring

In order to safeguard information and computing resources from various business and environmental threats, the activities related to the use of Trianz Information System Resources monitoring will be done. It will also 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

4.2 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. IT Department to maintain all audit records for at least one month and maximum to a period of one year to assist in future investigations and access control monitoring. 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

- Dates and times for logon and logoff
- Terminal identity or location

4.3 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
- Real-time alerts for publicly accessible systems (e.g. external web sites) for any suspicious user activity.

4.4 Monitoring of Firewall Audit Reports

The designated IT Administrator in IT 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 IT 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

4.5 Windows 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. There are apprehensions that logging and auditing everything will bloat the log and would also result in performance degradation. However, we suggest that by logging and auditing only selected events based on business needs and requirements, there may be limited effect on the performance of the system. Some of such events are:
    - Audit account logon events = Success, Failure
    - Audit account management = Success, Failure
    - Audit directory service access = Failure
    - Audit logon events = Success, Failure
    - Audit object access = Failure
    - Audit policy change = Success, Failure
    - Audit privilege use = Failure
    - Audit process tracking = No auditing
    - Audit system events = Success, Failure

4.6 UNIX Environment

- Logging and reporting
- Details/Test:
- 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 will 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.

4.7 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 should be adopted. This strategy should 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 should be as per the business and operational requirements. The concerned Department should 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.
- We need to 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 should be monitored for a period to analyse the affect on the performance of the system.
- The following auditing features can 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
- Firecall Accounts:- 'Firecall' 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 'Firecall' account was used in an emergency. If actions performed by 'Firecall' 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.
- SYSTEM Account Activity
- Vendor Account Activities

4.7 Vulnerability Assessment and Penetration Testing (VAPT)

Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure.

A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, service and application flaws, improper configurations, or risky end- user behavior.

VAPT provides Trianz with a comprehensive and detailed view of the threats facing its Information assets, enabling it to better protect its systems and data from malicious attacks.

However, because of the nature and the intent of VAPT, such testing in a production environment during normal business hours may impact business operations. To avoid disruptions and to speed up testing, a separate environment that is identical to the production environment may be used for testing instead of the production environment, ensure the same application and network-layer controls as production exist in the testing environment.

Another advantage of performing VAPT in a test environment is that by directly performing attacks against a system being audited, the attack script can push the system into an unknown state or completely disable it making the remote system useless for further testing and virtually eliminating the possibility of attaining detailed vulnerability reports against this device from future tests

All exploitable vulnerabilities identified during the testing must be corrected on production systems and testing repeated to verify that security weaknesses have been addressed.

5. ISO Control Mapping(s)

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Technological Controls	Clause 9.2 Internal audit	Information System Audit Trail Management Procedure

Technological Controls	8.34 Protection of information systems during audit testing	

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 templet format
6.01	16-Oct-16	Sudharsana & Shishir			Addition of Cloud Service 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	17-Dec-16	Balu Nair			Approved by CISO	Baseline
7.01	29-April-19	Balu Nair	Joshy VM			• Information Classification modified • Trianz Logo Modified
8.00	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baseline
8.01	12-May-20	Karthik N	Balu Nair			Integrated with New Template
9.00	14-May-20	Karthik N	Balu Nair	Phani Krishna	For Approval	Approved and Baselined
9.01	30-May-20	Vijaya Rajeswari	Phani Krishna		For Review	Information Classification Update
10.00	30-May-20	Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
10.01	15-Mar-22	Krutideepta	Krutideepta			Scope has been extended to products
10.2	28-Mar-23	Krutideepta, Pravakar Patra from Studio Team	Siva N	Siva N	For Review	Reviewed & no changes Migrated and packaged to new template

11.0	15-May-23	Krutideepta	Karthik N	Srikanth M	For Approval	Approved and Baselined
11.1	15-Feb-24	Shalini	Vijaya	Srikanth	For review	Mapped with new ISO 27001, 2022 Clause 9.2 Internal Audit
12	23-Feb-24	Shalini	Vijaya	Srikanth M	For Approval	Approved and Baselined
12.1	06-May-25	Balu Nair	Vijaya		Yearly Review	Migrated to a new Template
13.0	14-May-25	Balu Nair	Vijaya	Srikanth	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com