



Capacity Management Policy



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

<input type="checkbox"/>	Public
<input checked="" type="checkbox"/>	Internal
<input type="checkbox"/>	Confidential
<input type="checkbox"/>	Restricted

Table of Contents

1. PURPOSE	4
2. OBJECTIVE	4
3. SCOPE	4
4. POLICY STATEMENTS	4
1.1 4.1 Thresholds	5
5. ROLES & RESPONSIBILITIES	6
6. APPLICABLE STANDARDS	7
7. REFERENCE POLICIES & PROCEDURES	7
8. EXCEPTIONS(S)	7
9. 12.1 ISO CONTROL MAPPING	7

1. Purpose

The use of resources shall be monitored, tuned and projections made for future capacity requirements to ensure the required system Performance. Capacity demands shall be monitored, and projections of future capacity requirements shall be made to enable adequate processing power and storage is made available.

2. Objective

The objective of Capacity Management is to understand the business requirements, the organization's operations, and the IT infrastructure to ensure that all the current and future capacity and performance aspects of the business requirements are provided cost-effectively.

3. Scope

- This policy applies to all Trianz Associates, Contractors, and Vendors, Clients, Cloud Service Providers, Cloud Service Customers, Products and who are using Trianz IT infrastructure and communication services.
- The requirements of this policy shall be implemented in all the systems under the ownership of Trianz, either on premises or on cloud and for all other Trianz managed systems, wherever applicable.
- It is applicable for all Trianz Products and services.

4. Policy Statements

- Capacity demands shall be monitored, and projections of future capacity requirements shall be made to enable adequate processing power and storage to be made available.
- IS team shall keep a track of information processing needs of various users from time to time. This is done in coordination with the respective operations Manager. As a part of an engagement, project Manager along with IS Team will estimate the critical computer resources required and hardware or software procurement. Indent will be raised to the finance department to acquire the new hardware or software.
- In addition to the above, System-tuning and monitoring shall be applied to ensure and, where necessary, to improve the availability and efficiency of

systems, Detective & preventive controls shall be put in place to indicate problems in due time.

- Sufficient capacity shall be achieved by increasing capacity or by optimizing resource utilization. Examples of managing capacity demand include:
 - a) Deletion of obsolete data (disk space);
 - b) Decommissioning of applications, systems, databases or environments;
 - c) Optimizing batch processes and schedules;
 - d) Optimizing application logic or database queries;
- e) Denying or restricting bandwidth for resource-hungry services if these are not business critical (e.g. video streaming).
- For Cloud Services, computing systems adapt to workload changes by provisioning and de-provisioning resources in an automatic manner (Elastic Scaling), such that at each point in time the available resources match the current demand precisely, it is dynamic adaptation of capacity, by altering the use of computing resources, to meet varying workload. To optimize cost and utilization by using Cloud Reservations and periodical review of the consumption.
- In case of capacity constraints such as the number of Processor core applications, the amount of storage available, the network bandwidth availability – either changing the subscription or changing the cloud service provider shall be considered.

1.1 4.1 Thresholds

#	Threshold Value	Description	Action
1	Threshold Value - 70%	Warning Alert Message will be emailed to IT Admins/Stake holders	Reviewed in SMR and appropriate action will be initiated

2	Threshold Value - 80%	High Alert Message will be emailed to IT Admins	RCA will be performed, and immediate correction will be done; Corrective action will be identified & initiated
3	Threshold Value - 90%	Critical Alert Message will be emailed IT Admins	Capacity will be suitably enhanced

5. Roles & Responsibilities

Sl. No	Item	Roles	Responsibility
1	Capacity Management	Cloud Provider	<p>Monitoring total capacity to prevent any information security incidents caused by resource shortages.</p> <p>Resources will be made available to the Cloud Service Customer shall be under the terms of MSA and a related SLA.</p> <p>These resources include software, processing hardware, Data storage and Network connectivity.</p>

2	Capacity Management	IS Team/ Cloud Service Customer	<p>Shall have the responsibility and authority to cause this policy to be implemented and maintained.</p> <p>Shall monitor the use of Cloud service and forecast the capacity to ensure the performance of Cloud services.</p> <p>Cloud service customer shall have access to relevant statistics on resource usage such as Statistics for particular time period and maximum level of resource usage etc.</p>
---	---------------------	------------------------------------	--

6. Applicable standards

ISO 27001:2013

7. Reference Policies & Procedures

- Asset Management Policy
- Asset Management Procedure
- System and Software Change Management Policy and Procedure

8. Exceptions(s)

None. Exceptions to the Capacity Management policy shall follow the Exception handling policy.

9. 12.1 ISO Control Mapping

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Technological Controls	8.6 Capacity Management	Capacity Management

Commented [VRV(1)]: Add the below section and fill the details

Document Control

Owner:	CISO	Release ID:	CMP-POL-0030
---------------	------	--------------------	--------------

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.01	19-May-15	Sudharsana.cv			Initial Draft	None
1.00	19-May-15	Sudharsana.cv			Reviewed and approved	Baselined
1.01	24-Oct-16	Sriharsha G			Addition of Cloud services in the scope of audit	Added content related to elastic services provided by Cloud Trianz's Logo changed
2.00	07-Dec-16	Balu Nair			Approved By CISO	Baselined
2.01	30-Apr-19	Balu Nair	Josh VM			Information classification modified

3.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
4.0	25-Nov-2019	Vijaya Rajeswari	Phani Krishna	Vivek Sambasivam	Updated to align to ISO 27017 and ISO 27018 Standard	Roles and responsibilities for Cloud Provider and Cloud Customer updated
4.1	11-May-2020	Karthik N	Balu Nair		Review	Formatting changes incorporated
5.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
5.1	28-May-20	Pranesh Kulkarni	Gangadhar Aka		Inputs from External Audit	Thresholds values are updated in the policy.
6.0	03-June-20	Pranesh Kulkarni	Gangadhar Aka	Phani Krishna	For Approval	Approved and Baselined
6.1	14-Jan-21	Balu Nair	Phani Krishna		Review	Updated the information classification
7.0	14-Jan-21	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
7.1	3-Jan-22	Divya G	Karthik		Review	Updates on Cloud consumption. Modified as per the new template

8.0	3-Jan-22	Divya G	Siva N	Siva N	For Approval	Reviewed, Approved and Baselined
8.1	13-Mar-22	Sanjana	Divya G	Siva N	For Review	The scope has been extended to products and services
9.0	18-Mar-22	Sanjana	Divya G	Siva N	For Approval	Approved and Baselined
9.1	11-Apr-2023	Sanjana, Rama Madhavan	Karthik N		For Review	Updated roles & Responsibilities New template updates
10.0	08-May-2023	Sanjana	Karthik N	Srikanth M	For Approval	Approved and Baselined
10.0	23-Feb-24	Shalini	Vijaya		For Review	Reviewed and No changes
10.1	06-May-25	Balu Nair	Vijaya		Yearly Review	Migrated to a new Template
11.0	14-May-25	Balu Nair	Vijaya	Srikanth M	For Approval	Approved and Baselined



Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com



The content in this document is copyrighted; any unauthorized use – in part or full – may violate the copyright, trademark, and other laws. This document may not be modified, reproduced, or publicly displayed, performed, or distributed, or used for any public or commercial purposes. The Trianz name and its products are subject to trademark and copyright protections, regardless of how and where referenced.