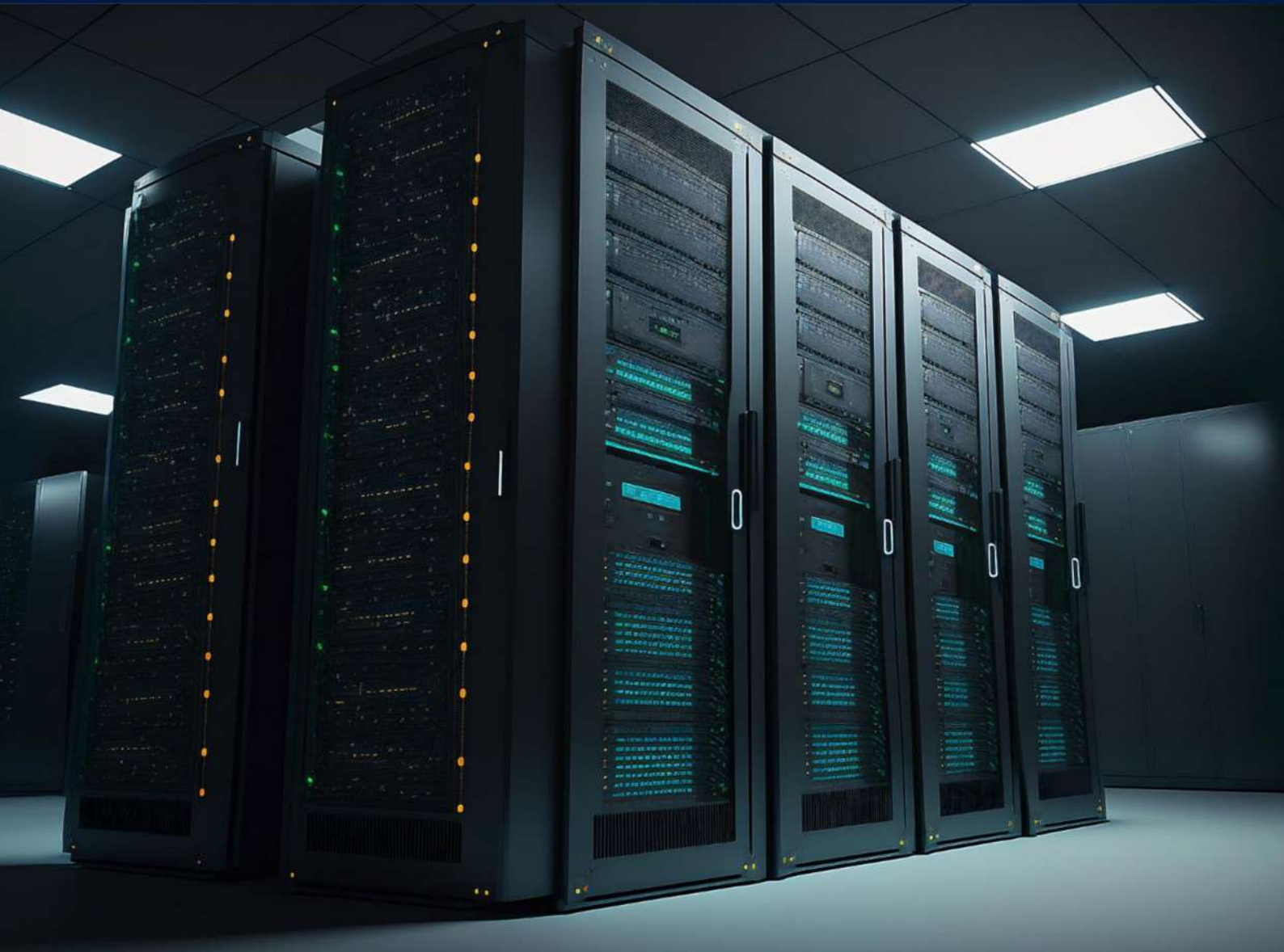




WHITEPAPER

MANAGED SERVICES – IT INFRASTRUCTURE



www.method-hub.com

CONTENTS

1. CORE COMPONENTS OF MANAGED IT INFRASTRUCTURE SERVICES	1
2. BENEFITS	2
3. SCOPE OF WORK (SOW)	2
3.1. OBJECTIVE	2
3.2. SERVICES INCLUDED	2
3.3. DELIVERABLES	3
3.4. SERVICE LEVEL AGREEMENTS (SLAS)	3
3.5. ROLES & RESPONSIBILITIES	3
3.6. EXCLUSIONS	3
3.7. PRICING & BILLING	3
3.8. CONFIDENTIALITY & COMPLIANCE	3
3.9. CHANGE MANAGEMENT	3
3.10. TERMINATION CLAUSE	3
4. MANAGED SERVICES ARCHITECTURE	4
4.1 ARCHITECTURE OVERVIEW	4
4.2 Key Processes & Workflows (Aligned to ITIL)	4
4.3 DASHBOARDS & REPORTING	5
4.4 WORKLOAD CHARACTERISTICS	5
4.5 COMPUTE PARAMETERS	5
4.6 NETWORK REQUIREMENTS	6
4.7 SCALABILITY & AVAILABILITY	6
4.8 DEPLOYMENT MODEL	6
4.9 BUDGET & COMPLIANCE	6
5. REFERENCES	7
6. ABOUT US	8

Managed Services for IT Infrastructure refers to outsourcing the management and support of an organization's IT infrastructure to a third-party service provider, often called a Managed Service Provider (MSP). These services typically include proactive monitoring, maintenance, and support of hardware, software, networks, and related IT systems.

1. CORE COMPONENTS OF MANAGED IT INFRASTRUCTURE SERVICES

1.1 Network Management

- Monitoring and managing LAN, WAN, VPN, firewalls, and routers.
- Ensuring network uptime and performance.

1.2 Server Management

- Maintenance and patching of physical and virtual servers.
- Backup, recovery, and high availability solutions.

1.3 Storage & Backup Services

- Data backup, disaster recovery planning, and cloud storage.
- Storage provisioning and lifecycle management.

1.4 Cloud Services

- Managing public, private, or hybrid cloud environments.
- Cloud migration, cost optimization, and performance tuning.

1.5 Endpoint Management

- Managing desktops, laptops, and mobile devices.
- Applying security updates, antivirus, and configuration management.

1.6 Security Management

- Firewalls, intrusion detection systems, antivirus solutions.
- Security audits, vulnerability assessments, and compliance monitoring.

1.7 Help Desk / IT Support

- 24x7 user support via email, phone, or ticketing systems.
- Tiered support levels (L1, L2, L3) for escalating complex issues.

1.8 IT Asset Management

- Tracking and managing hardware/software lifecycle.
- License compliance and procurement.

1.9 Monitoring & Reporting

- Real-time dashboards, performance metrics, alerts.
- Regular reporting on system health and service-level metrics.

2. BENEFITS

- Reduced IT operational costs
- 24x7 or 8x5 or 8x6 or customized services monitoring and faster issue resolution
- Enhanced security and compliance
- Scalability and flexibility
- Access to expert-level knowledge and tools

3. SCOPE OF WORK (SOW)

3.1. Objective

To ensure secure, reliable, and efficient operation of the IT infrastructure by Managed Services Provider (MSP) for comprehensive support, monitoring, and management of network, servers, end-points, cloud, and IT security infrastructure.

3.2. Services Included

3.2.1 Network Management

- Configuration, monitoring, and troubleshooting of LAN, WAN, VPN, firewalls, switches, and routers.
- Proactive performance optimization.
- Network availability monitoring (24x7).

3.2.2 Server Management

- Installation, configuration, and patching of physical & virtual servers (Windows/Linux).
- Performance monitoring and capacity planning.
- Regular security updates and firmware upgrades.

3.2.3 Storage & Backup Management

- Data backup scheduling, monitoring, and restoration.
- Storage provisioning and tiered storage management.
- Disaster recovery planning and testing.

3.2.4 Cloud Infrastructure Support

- Management of cloud resources (AWS, Azure, GCP, or private cloud).
- Optimization of cloud workloads and cost.
- Backup and failover configuration in cloud.

3.2.5 Endpoint Management

- Management of desktops, laptops, & mobile devices.
- Antivirus deployment & patch management.
- Device onboarding/offboarding.

3.2.6 IT Security Management

- Firewall and endpoint security configuration.
- Threat monitoring and incident response.
- Periodic vulnerability assessment & security audits.

3.2.7 Help Desk Services

- 24x7 help desk for user support (L1, L2, L3 tiers).
- Ticketing system setup and management.
- SLA-based issue resolution and reporting.

3.2.8 Monitoring & Reporting

- Real-time infrastructure monitoring.
- Monthly performance reports (uptime, incidents, patch status, etc.).
- Quarterly review meetings with stakeholders.

3.3. DELIVERABLES

- Infrastructure Audit Report (initial).
- Monthly SLA Compliance Report.
- Asset Inventory Database.
- Security Incident & Vulnerability Reports.
- Backup and DR Test Reports (semi-annually).

3.5. ROLES & RESPONSIBILITIES

Client

- Infrastructure Audit Report (initial).
- Monthly SLA Compliance Report.
- Asset Inventory Database.
- Security Incident & Vulnerability Reports.
- Backup and DR Test Reports (semi-annually).

3.6. EXCLUSIONS

- Development of new applications or services.
- Hardware procurement (unless explicitly agreed).
- Services outside standard business applications unless covered in a change request.

3.8. CONFIDENTIALITY & COMPLIANCE

- NDA to be signed.
- Compliance with IT security policies and applicable regulatory guidelines.
- Data confidentiality and breach notification clauses.

3.10. TERMINATION CLAUSE

- Termination notice period: [e.g., 30/60/90 days].
- Exit process and knowledge transfer to internal/external team.
- Final deliverables and documentation handover.

3.4. SERVICE LEVEL AGREEMENTS (SLAS)

- Network Uptime: $\geq 99.5\%$
- Server Availability: $\geq 99.9\%$
- Response Time: < 30 minutes for critical issues
- Resolution Time: As per defined priority matrix
- Backup Success Rate: $\geq 98\%$

Service Provider

- Provide services as per agreed scope and SLA.
- Maintain documentation and audit trails.
- Ensure compliance with applicable laws & standards (e.g., ISO 27001, SEBI/RBI, etc.).

3.7. PRICING & BILLING

- Fixed monthly/quarterly/yearly fee.
- Additional services billed as per rate card or change order.
- All applicable taxes extra.

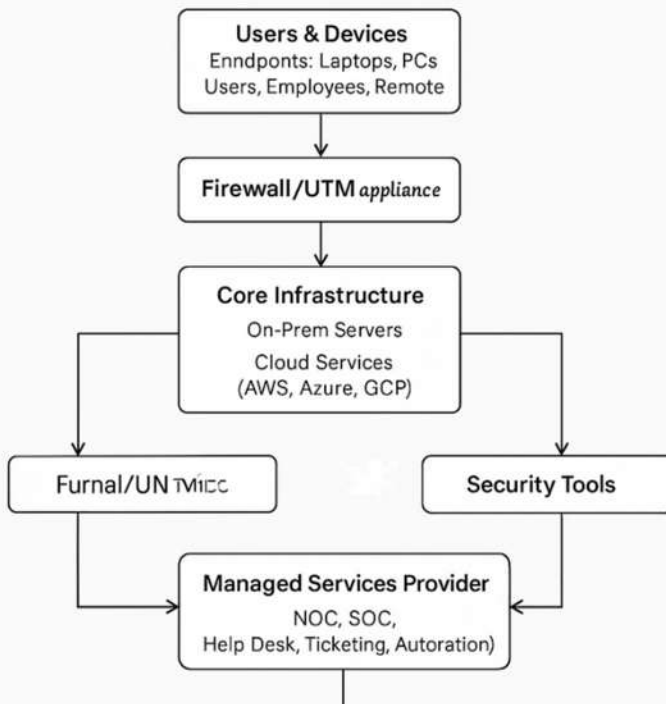
3.9. CHANGE MANAGEMENT

Changes to scope, deliverables, or time lines must be documented via a Change Request (CR) and approved by both parties.

4. MANAGED SERVICES ARCHITECTURE

4.1 Architecture Overview

Managed Services Architecture for SMB



Recommended Tools Stack

- **Monitoring & Management:** Microsoft Intune, NinjoOne, PRTG, Zabbix, UptimeRobot
- **Security:** CrowdStrike Faicon, SentinelOne, Fortinet, Sophos XG, Sonic-Wall, Mimecast, Microsoft Defender
- Qualys, Tenable Nessus, Splunk
- **Backup & DR:** Acronis, Veeam Agent, Druva, MSP360, Backblaze
- Veeam, Zerto

Key Processes & Workflows (Aligned to ITIL)

- Incident Management
- Problem Management
- Change Management
- Asset & Configuration Management
- Backup & Disaster Recovery
- Security & Compliance Management
- User Access Management

1

4.2 Key Processes & Workflows (Aligned to ITIL)

1. Incident Management

- Users report issues via ticket/email/phone
- Tickets triaged (L1, L2, L3)
- Resolved as per SLA & root cause logged

3. Change Management

- Changes to infra (patches, upgrades, config changes) documented
- CAB (Change Advisory Board) approval for critical changes
- Backout plans created for high-risk changes

5. Backup & Disaster Recovery

- Backup policies defined
- Regular DR drills (semi-annual or quarterly)
- RPO/RTO goals documented & tested

2. Problem Management

- Recurring issues analyzed for underlying causes
- Permanent fixes implemented
- Known Error Database maintained

4. Asset & Configuration Management

- Maintain CMDB (Configuration Management Database)
- Track software licenses, hardware assets, warranties

6. Security & Compliance Management

- Regular vulnerability scans
- Patch cycles managed monthly/quarterly
- SOC services for log correlation, incident detection

7. User Access Management

- Identity lifecycle managed (Joiner-Mover-Leaver)
- MFA enabled across all critical services
- RBAC (Role-Based Access Control) enforced

4.3 Dashboards & Reporting

- Real-time dashboards (uptime, incidents, asset status)
- Monthly performance and SLA reports
- Quarterly service review and strategy sessions

4.4 Workload Characteristics

These determine how much CPU, RAM, and storage the workloads need.

Parameter	Description
Type of Workload	Web server, database, file server, virtualization, analytics, etc.
Number of Users	Concurrent users and growth estimate.
Transactions per Second (TPS)	Especially important for databases and applications.
Peak vs. Average Load	For handling usage spikes vs. regular activity.
Data Size	Total dataset and daily growth (important for memory + storage planning).
Latency Sensitivity	For real-time apps, choose higher clock speeds or lower contention.

4.5 Compute Parameters

These are the direct resource requirements you'll plan for.

Parameter	Notes
vCPU / CPU Cores	Based on thread count, concurrency, hypervisor overhead.
Clock Speed (GHz)	For performance-critical applications.
RAM (Memory)	Size based on in-memory processing, caching, DB buffers, etc.
Storage IOPS	For disk-intensive apps, define minimum read/write throughput.
GPU (if needed)	For AI/ML, rendering, VDI, etc.

4.6 Network Requirements

Parameter	Notes
Bandwidth	Uplink and internal throughput needs.
Latency	Inter-zone/region latency for cloud deployments.
Firewall Rules & Segmentation	May impact design (e.g., additional vNICs or appliances).

4.7 Scalability & Availability

Parameter	Notes
Expected Growth Rate	Annual growth in users/data/load.
HA Requirements	Active-passive, clustering, failover configurations.
Load Balancing	Horizontal scaling requirements.
Redundancy Level	N+1, N+2 or failover zones/regions.

4.8 Deployment Model

Parameter	Notes
On-Prem vs Cloud	Impacts design, licensing, scalability.
Virtualization / Containerization	VMware, Hyper-V, Docker, K8s.
OS & Licensing	Windows/Linux, CALs, core licenses.

4.9 Budget & Compliance

Parameter	Notes
Budget Constraints	CapEx vs OpEx.
Compliance Needs	E.g., PCI-DSS, HIPAA, SEBI, GDPR - may dictate redundancy or isolation.
Energy & Rack Space (On-Prem)	If physical infrastructure involved.

5. REFERENCES

1. IT Infrastructure Architecture: Infrastructure Building Blocks and Concepts by Sjaak Laan
2. IT Infrastructure & Management by Narendra Kumar and Surendra Keshari:
3. IT Infrastructure and its management – Phalguni Gupta, Surya Prakash, Umarani Jayaraman
4. Materials from Kepner Tregoe on ITIL processes for managed services

About Us

MethodHub is a global Information Technology services provider offering next-gen business solutions to enhance the digital transformation journey of its clients across the globe. With 30+ customers and over 500 employees globally who bring domain expertise and experience in advanced technologies, MethodHub is in the USA, India, Canada, and Thailand. With capabilities in Cloud Engineering, Data Services, Cyber Security, and ERP/CRM integration, MethodHub aspires to service large enterprises across the globe through a combination of consulting, delivery, fulfillment, support services, and execution capabilities.

MethodHub serves verticals such as BFSI, Health care and life sciences, Oil & Gas/Energy, Telecom/Tech Infra, Automotive & Transport, and Platform Engineering. We offer a unique blend of expertise and innovation that helps companies revolutionize technology, reimagine processes, and transform experiences to stay ahead in this fast-changing world.

With a widespread network and a team of seasoned professionals, we deliver results on a large scale. Our solution experts understand the nuances of local presence and tailor our offerings according to the client's specific needs. Look no further than MethodHub for your digital transformational needs.

Infrastructure Service Team

Jawahar Srinivasan

Global Head- IT Infrastructure Services

Email: datappractice@method-hub.com

Thank you