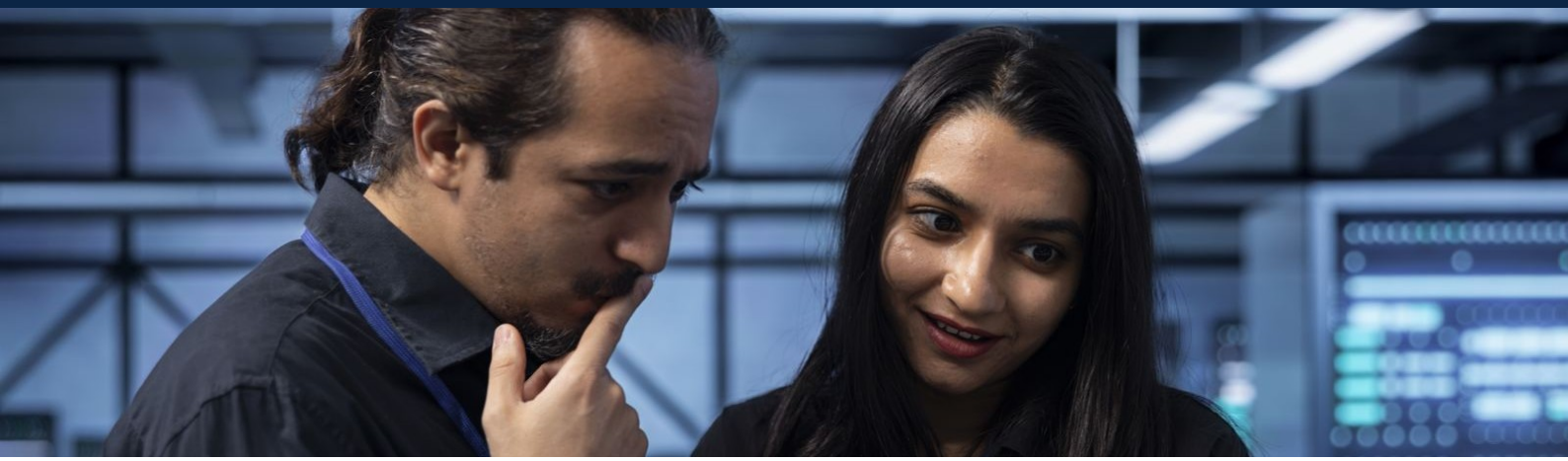
DCM Infotech

CASE STUDY · MISSION-CRITICAL MANAGED IT SERVICES

Managing mission-critical IT infrastructure in an air-gapped defence environment

Delivering >99.99% SLA performance, 24×7 support and operational resilience across approximately 80 locations in India



Company overview

- Sensitive defence establishment operating across approximately 80 Indian locations
- Three principal sites: DC, Near DC and DR
- Original infrastructure implemented by DCM in 2018–19
- Managed services transitioned from IBM back to DCM after approximately two years

Operating environment

- Air-gapped production infrastructure; no conventional external remote access
- SAP on IBM AIX; Windows and Linux clusters; DB2 and SQL Server
- RSA SIEM, EDR, IBM IAM, Netcool, Cognos and Maximo
- IBM Spectrum backup and enterprise storage; distributed end-user support

01 · OVERVIEW

The customer handed full infrastructure and security management back to DCM

A defence establishment with approximately 80 locations across India operates a sensitive, air-gapped IT environment spanning a Data Centre, Near Data Centre and Disaster Recovery site. DCM Infotech implemented the environment in 2018–19. After an initial managed services engagement with IBM, the customer transitioned complete infrastructure and security management back to DCM after approximately two years.

>99.99%
CPU, memory and network SLA parameters

24×7
Help Desk and L2 coverage

~80
Locations with distributed end-user support

0
Complete system-wide outages during DCM's managed services tenure

02 · THE CHALLENGE

Stringent availability, without remote access or internet-based OEM support

The customer needed stringent availability without conventional remote access or internet-based OEM troubleshooting. Its heterogeneous landscape includes SAP on IBM AIX, Windows and Linux clusters, DB2 and SQL Server, security and IAM tools, Netcool, Cognos, Maximo, backup and storage. Ageing technology, restricted offline updates and approximately 80 distributed establishments intensified the challenge.

> **How can a geographically distributed, air-gapped defence environment sustain critical IT services without conventional remote support?**

Four constraints shaped the support model

Air-gapped operations
Remote OEM access, cloud monitoring and direct patch downloads were unavailable or restricted.

Heterogeneous infrastructure
Interdependent applications, databases, operating systems, networks, security and storage.

Ageing technology
Legacy support skills, lifecycle risks and controlled offline updates.

Geographic scale
Consistent support required across approximately 80 establishments.

03 · THE SOLUTION

A three-layer support model, with engineers on site, replaces remote support

Three-layer support model	24×7 Help Desk and Operations Control Centre, dedicated 24×7 L2 specialists and L3 subject-matter experts.
On-site engineering	Personnel at DC, Near DC and DR, plus end-user support across distributed locations.
Integrated operations	Monitoring, incident escalation, preventive maintenance, backup, security and change management.
Institutional knowledge	DCM’s original implementation expertise and IBM technology specialisation.

How the model is delivered

01

24×7 operations control
Incident logging, monitoring, first-level troubleshooting, SLA tracking and coordinated escalation through a Help Desk and Operations Control Centre.

02

Dedicated L2 specialists
Round-the-clock expertise across AIX, Linux, Windows, DB2, SQL Server, networks, security, IAM, backup, storage and monitoring.

03

L3 expert escalation

Senior specialists support complex root-cause analysis, performance, failover, database recovery and security issues, with critical escalation arrangements.

04

On-site & distributed support

Engineers at DC, Near DC and DR, with end-user support across approximately 80 establishments and approved offline change processes.

04 · IMPACT & BUSINESS BENEFITS

SLA parameters held above 99.99%, with no system-wide outage

SLA reliability

CPU, memory and network parameters consistently exceeded 99.99% SLA performance.

Critical incident handling

P1 response <15 minutes, resolution within 2 hours; P2 response within 2 hours, resolution <4 hours; P3 resolution within 8 hours.

Operational continuity

No complete system-wide unavailability during the managed services tenure.

Nationwide coverage

Local end-user support across approximately 80 locations, coordinated with central infrastructure specialists.

Specialist knowledge

DCM's 2018–19 implementation knowledge supports troubleshooting across ageing and interdependent technologies.

Partnership continuity

Multiple renewals reflect the customer's continuing confidence in the managed services model.

05 · STRATEGIC OUTCOME

DCM's three-layer support architecture, on-site engineering presence and specialist knowledge sustain mission-critical infrastructure in a highly restricted, geographically distributed environment. Looking ahead, technology lifecycle assessment, controlled patching, resilience testing and knowledge continuity remain important for modernisation without compromising operations.

www.dcminfotech.com/managed-service.html