🏦 Bank IT Production Management Runbook – Infrastructure Support

**1. 📘 Overview**

This runbook provides standardized procedures for monitoring, maintaining, and supporting the bank’s IT infrastructure in production environments. It ensures high availability, performance, and security of systems critical to banking operations.

**2. 🔧 Infrastructure Components Covered**

* Servers: Physical and virtual (Windows/Linux)
* Storage Systems: SAN/NAS
* Network Devices: Routers, switches, firewalls
* Databases: Oracle, SQL Server, PostgreSQL
* Monitoring Tools: Nagios, SolarWinds, Splunk
* Backup Systems: Veeam, Commvault
* Cloud Services: AWS, Azure (if applicable)

**3. 📊 Architecture Diagram**

Below is the updated architecture diagram with dummy IPs labeled for each component.

**4. 🕒 Daily Operations Checklist**

|  |  |  |
| --- | --- | --- |
| **Time** | **Task** | **Owner** |
| 06:00 | Check system health dashboards | Infra Ops |
| 07:00 | Review overnight alerts and logs | Infra Ops |
| 08:00 | Verify backups completed successfully | Backup Admin |
| 09:00 | Confirm network connectivity and latency | Network Admin |
| 10:00 | Patch compliance check (weekly) | Sys Admin |

**5. 🚨 Incident Management**

Severity Levels:

* P1 (Critical): Major outage affecting banking operations
* P2 (High): Partial outage or degraded performance
* P3 (Medium): Non-critical issue with workaround
* P4 (Low): Minor issue or cosmetic bug

**Response Matrix:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **Response Time** | **Resolution Time** | **Escalation** |
| P1 | 15 mins | 2 hours | Infra Head, IT Director |
| P2 | 30 mins | 4 hours | Team Lead |
| P3 | 1 hour | 24 hours | Assigned Engineer |
| P4 | 4 hours | 3 days | Assigned Engineer |

**6. 🛠️ Standard Operating Procedures (SOPs)**

**6.1 Server Reboot Procedure**

1. Notify stakeholders via email.
2. Validate backup status.
3. Reboot during approved window.
4. Post-reboot health check.

**6.2 Disk Space Management**

1. Monitor thresholds via alerts.
2. Clean temp/log files.
3. Extend volume if needed.
4. Document changes in ticketing system.

**6.3 Patch Management**

1. Review patch advisories.
2. Test in staging.
3. Schedule deployment.
4. Validate post-deployment.

**7. 📈 Monitoring & Reporting**

* Daily Health Reports: Sent by 10 AM
* Weekly Infra Summary: Includes uptime, incidents, changes
* Monthly Capacity Planning Report

**8. 📞Escalation Contacts**

|  |  |  |
| --- | --- | --- |
| **Role** | **Name** | **Contact** |
| Infra Head | Ravi Kumar | +91-XXXXXXXXXX |
| Network Lead | Priya Sharma | +91-XXXXXXXXXX |
| DB Admin | Arjun Mehta | +91-XXXXXXXXXX |
| Backup Admin | Sneha Rao | +91-XXXXXXXXXX |

**9. 🧯Disaster Recovery (DR) Details - Applications**

|  |  |  |
| --- | --- | --- |
| **Application** | **Production IP** | **DR IP** |
| Web Server | 192.168.9.10 | 10.10.10.10 |
| App Server | 192.168.9.20 | 10.10.10.20 |
| Payment Gateway | 192.168.9.30 | 10.10.10.30 |
| Core Banking | 192.168.9.40 | 10.10.10.40 |
| CRM | 192.168.9.50 | 10.10.10.50 |
| HRMS | 192.168.9.60 | 10.10.10.60 |
| Email Server | 192.168.9.70 | 10.10.10.70 |
| File Server | 192.168.9.80 | 10.10.10.80 |
| Monitoring System | 192.168.9.90 | 10.10.10.90 |
| Backup System | 192.168.9.100 | 10.10.10.100 |
| Firewall | 192.168.9.110 | 10.10.10.110 |

9.1 Core Banking

Active-Passive setup across DC1 and DC2. DR fallback via DNS switch.

\*\*Upstream Dependencies:\*\* Database, Firewall, DNS, Load Balancer

\*\*Downstream Dependencies:\*\* Mobile Banking, Loan Origination

9.2 Internet Banking

Cloud-based DR with auto-scaling. Manual failover via load balancer.

\*\*Upstream Dependencies:\*\* Load Balancer, Firewall, DNS

\*\*Downstream Dependencies:\*\* Mobile Banking

9.3 Mobile Banking

Hybrid DR with container replication. Fallback via Kubernetes redeploy.

\*\*Upstream Dependencies:\*\* Internet Banking, Core Banking, Kubernetes Cluster

\*\*Downstream Dependencies:\*\* None

9.4 Payment Gateway

Real-time replication to DR site. Failover via routing switch.

\*\*Upstream Dependencies:\*\* Network Switch, Load Balancer, Firewall

\*\*Downstream Dependencies:\*\* Core Banking, ATM Switch

9.5 Loan Origination

Scheduled sync to DR. Manual activation via DR script.

\*\*Upstream Dependencies:\*\* Core Banking, Database

\*\*Downstream Dependencies:\*\* None

9.6 CRM System

Cloud DR with snapshot restore. Fallback via cloud console.

\*\*Upstream Dependencies:\*\* Database, Storage System

\*\*Downstream Dependencies:\*\* None

9.7 Email System

DR via secondary MX records. Failover automatic.

\*\*Upstream Dependencies:\*\* DNS

\*\*Downstream Dependencies:\*\* Internal Communication Systems

9.8 Document Management

DR via replicated storage. Manual mount and service restart.

\*\*Upstream Dependencies:\*\* Storage System

\*\*Downstream Dependencies:\*\* CRM System

9.9 ATM Switch

DR via redundant hardware. Failover via hardware switch.

\*\*Upstream Dependencies:\*\* Core Banking, Payment Gateway

\*\*Downstream Dependencies:\*\* None

9.10 Reporting System

DR via nightly ETL to DR DB. Manual report engine activation.

\*\*Upstream Dependencies:\*\* Database

\*\*Downstream Dependencies:\*\* Business Intelligence Tools

10.🧯Disaster Recovery (DR) Details - Infrastructure

10.1 Web Server Recovery

Production IP: 192.168.1.1

DR IP: 10.10.10.1

Recovery Steps (UNIX):

1. Identify the impacted server using monitoring tools.

2. SSH into the server using credentials: ssh admin@192.168.1.1

3. Check system logs: tail -n 100 /var/log/syslog

4. Restart affected services: sudo systemctl restart <service>

5. Validate service status: sudo systemctl status <service>

6. Notify stakeholders and update incident ticket.

\*\*Upstream Dependencies:\*\* Monitoring System, DNS

\*\*Downstream Dependencies:\*\* App Server, Internet Banking

10.3 App Server Recovery

Production IP: 192.168.1.2

DR IP: 10.10.10.2

\*\*Upstream Dependencies:\*\* Web Server, Load Balancer

\*\*Downstream Dependencies:\*\* Mobile Banking, CRM System

10.4 Recovery Steps (UNIX):

1. Identify the impacted server using monitoring tools.

2. SSH into the server using credentials: ssh admin@192.168.1.2

3. Check system logs: tail -n 100 /var/log/syslog

4. Restart affected services: sudo systemctl restart <service>

5. Validate service status: sudo systemctl status <service>

6. Notify stakeholders and update incident ticket.

10.6 Database Recovery

Production IP: 192.168.1.3

DR IP: 10.10.10.3

Recovery Steps (UNIX):

1. Identify the impacted server using monitoring tools.

2. SSH into the server using credentials: ssh admin@192.168.1.3

3. Check system logs: tail -n 100 /var/log/syslog

4. Restart affected services: sudo systemctl restart <service>

5. Validate service status: sudo systemctl status <service>

6. Notify stakeholders and update incident ticket.

Oracle DB Recovery Steps:

1. Connect to Oracle DB server: ssh oracle@192.168.1.103

2. Check DB status: sqlplus / as sysdba -> SELECT status FROM v$instance;

3. Restart DB if needed: shutdown immediate; startup;

4. Validate application connectivity.

5. Notify DB admin and update ticket.

\*\*Upstream Dependencies:\*\* Storage System

\*\*Downstream Dependencies:\*\* Core Banking, Loan Origination, CRM System, Reporting System

10.7 Firewall Recovery

Production IP: 192.168.1.4

DR IP: 10.10.10.4

Recovery Steps (UNIX):

1. Identify the impacted server using monitoring tools.

2. SSH into the server using credentials: ssh admin@192.168.1.4

3. Check system logs: tail -n 100 /var/log/syslog

4. Restart affected services: sudo systemctl restart <service>

5. Validate service status: sudo systemctl status <service>

6. Notify stakeholders and update incident ticket.

\*\*Upstream Dependencies:\*\* None

\*\*Downstream Dependencies:\*\* Internet Banking, Core Banking, Load Balancer

10.8 Load Balancer Recovery

Production IP: 192.168.1.5

DR IP: 10.10.10.5

Recovery Steps (UNIX):

1. Identify the impacted server using monitoring tools.

2. SSH into the server using credentials: ssh admin@192.168.1.5

3. Check system logs: tail -n 100 /var/log/syslog

4. Restart affected services: sudo systemctl restart <service>

5. Validate service status: sudo systemctl status <service>

6. Notify stakeholders and update incident ticket.

\*\*Upstream Dependencies:\*\* Firewall

\*\*Downstream Dependencies:\*\* Internet Banking, App Server, Payment Gateway

10.9 Monitoring System Recovery

Production IP: 192.168.1.6

DR IP: 10.10.10.6

Recovery Steps (UNIX):

1. Identify the impacted server using monitoring tools.

2. SSH into the server using credentials: ssh admin@192.168.1.6

3. Check system logs: tail -n 100 /var/log/syslog

4. Restart affected services: sudo systemctl restart <service>

5. Validate service status: sudo systemctl status <service>

6. Notify stakeholders and update incident ticket.

\*\*Upstream Dependencies:\*\* None

\*\*Downstream Dependencies:\*\* All Systems (for alerting and observability)

10.10 Storage System Recovery

Production IP: 192.168.1.7

DR IP: 10.10.10.7

Recovery Steps (UNIX):

1. Identify the impacted server using monitoring tools.

2. SSH into the server using credentials: ssh admin@192.168.1.7

3. Check system logs: tail -n 100 /var/log/syslog

4. Restart affected services: sudo systemctl restart <service>

5. Validate service status: sudo systemctl status <service>

6. Notify stakeholders and update incident ticket.

\*\*Upstream Dependencies:\*\* None

\*\*Downstream Dependencies:\*\* Database, Document Management, CRM System

10.11 Network Switch Recovery

Production IP: 192.168.1.8

DR IP: 10.10.10.8

Recovery Steps (UNIX):

1. Identify the impacted server using monitoring tools.

2. SSH into the server using credentials: ssh admin@192.168.1.8

3. Check system logs: tail -n 100 /var/log/syslog

4. Restart affected services: sudo systemctl restart <service>

5. Validate service status: sudo systemctl status <service>

6. Notify stakeholders and update incident ticket.

\*\*Upstream Dependencies:\*\* None

\*\*Downstream Dependencies:\*\* Payment Gateway, VPN Gateway

10.12 VPN Gateway Recovery

Production IP: 192.168.1.9

DR IP: 10.10.10.9

Recovery Steps (UNIX):

1. Identify the impacted server using monitoring tools.

2. SSH into the server using credentials: ssh admin@192.168.1.9

3. Check system logs: tail -n 100 /var/log/syslog

4. Restart affected services: sudo systemctl restart <service>

5. Validate service status: sudo systemctl status <service>

6. Notify stakeholders and update incident ticket.

\*\*Upstream Dependencies:\*\* Network Switch

\*\*Downstream Dependencies:\*\* Secure Remote Access

10.13 Cloud Service Recovery

Production IP: 192.168.1.10

DR IP: 10.10.10.10

Recovery Steps (UNIX):

1. Identify the impacted server using monitoring tools.

2. SSH into the server using credentials: ssh admin@192.168.1.10

3. Check system logs: tail -n 100 /var/log/syslog

4. Restart affected services: sudo systemctl restart <service>

5. Validate service status: sudo systemctl status <service>

6. Notify stakeholders and update incident ticket.

\*\*Upstream Dependencies:\*\* Internet

\*\*Downstream Dependencies:\*\* CRM System, Email System, Cloud Applications

**11. Change Management Process**

CAB Workflow: Request → Review → Approval → Implementation → Validation

|  |  |
| --- | --- |
| **Step** | **Description** |
| 1 | Submit change request in ServiceNow |
| 2 | CAB reviews impact and risk |
| 3 | Approval from stakeholders |
| 4 | Implement during change window |
| 5 | Post-change validation and closure |

**12. Capacity Planning Guidelines**

Monthly review of CPU, Memory, Disk usage across servers. Threshold: 80% utilization.

|  |  |  |
| --- | --- | --- |
| **Resource** | **Threshold** | **Action** |
| CPU | 80% | Upgrade or load balance |
| Memory | 75% | Add RAM or optimize apps |
| Disk | 85% | Extend volume or archive data |

**13. Security Monitoring & Compliance Checks**

Tools: Splunk, Qualys, Nessus. Daily scans and monthly compliance reports.

|  |  |  |
| --- | --- | --- |
| **Check** | **Frequency** | **Tool** |
| Vulnerability Scan | Daily | Nessus |
| Log Review | Daily | Splunk |
| Patch Compliance | Weekly | Qualys |

**14. Automation Scripts or Tools Used**

Tools: Ansible, PowerShell, Bash scripts.

|  |  |
| --- | --- |
| **Tool** | **Purpose** |
| Ansible | Server provisioning |
| PowerShell | Windows patching |
| Bash | Unix health checks |

**15. Audit & Compliance Reporting Templates**

Monthly audit reports include access logs, change history, and patch status.

|  |  |  |
| --- | --- | --- |
| **Report** | **Frequency** | **Owner** |
| Access Logs | Monthly | Security Team |
| Change History | Monthly | Infra Ops |
| Patch Status | Monthly | Sys Admin |

**16. Integration with CI/CD Pipelines**

CI/CD tools: Jenkins, GitLab. Infra scripts versioned and deployed via pipelines.

|  |  |
| --- | --- |
| **Tool** | **Function** |
| Jenkins | Automated deployment |
| GitLab | Version control |
| Terraform | Infra provisioning |

**17. Visual Timeline for DR Drills or Maintenance Windows**

DR Drill Timeline:

|  |  |
| --- | --- |
| **Time** | **Activity** |
| 08:00 | Initiate DR drill |
| 08:30 | Failover DB to DR site |
| 09:00 | Validate application connectivity |
| 10:00 | Rollback to primary site |

**18. Change Category Timelines**

|  |  |  |
| --- | --- | --- |
| Change Type | Timeline | Approval Required |
| Emergency | Within 1 hour | Infra Head |
| Standard | 2 business days | CAB |
| Major | 5 business days | CAB + IT Director |

**19. Capacity Planning Breach Steps (UNIX)**

1. Monitor disk usage: df -h
2. Identify large files: du -sh \* | sort -h
3. Clean up temp/log files: sudo rm -rf /var/log/\*.gz
4. Extend volume if needed: lvextend -L +10G /dev/mapper/root
5. Resize filesystem: resize2fs /dev/mapper/root
6. Update capacity planning dashboard and notify stakeholders.

**Appendix:**

**Useful Commands & Troubleshooting Tips**

Common commands:

Unix: df -h, top, ps aux, netstat -tulnp

Windows: ipconfig, tasklist, netstat -an