**J M Baxi Group**

Information Security Policy

Standard Operating Policy and Procedures &

Delegation of Authority

Contents

[Information Security Policy 1](#_Toc189074507)

[**1.** **Standard operating policy & procedure (SOPP)** 3](#_Toc189074508)

[**1.1** **Introduction** 3](#_Toc189074509)

[**1.2** **Document Review and approval** 3](#_Toc189074510)

[**2.** **Executive Summary** 4](#_Toc189074511)

[**3.** **Scope** 6](#_Toc189074512)

[**4.** **User Access Management** 6](#_Toc189074513)

[**4.1** **Granting User Access** 6](#_Toc189074514)

[**4.2** **Modifying User Access** 8](#_Toc189074515)

[**4.3** **Removal of User Access** 8](#_Toc189074516)

[**4.4** **Privileged Users** 8](#_Toc189074517)

[**4.5** **User Access Review** 8](#_Toc189074518)

[**4.6** **Password Management** 12](#_Toc189074519)

[**4.7** **Database Access** 12](#_Toc189074520)

[**5.** **Change Management Process** 12](#_Toc189074521)

[**5.1** **Change Process** 12](#_Toc189074522)

[**5.2** **Segregation of Environments** 15](#_Toc189074523)

[**6.** **Data-Backup and Scheduled Job Management** 15](#_Toc189074524)

[**6.1** **Backup procedures** 15](#_Toc189074525)

[**6.2** **Restoration procedures** 16](#_Toc189074526)

[**6.3** **Scheduled Job Monitoring** 16](#_Toc189074527)

[**7.** **Network Management** 16](#_Toc189074528)

[**7.2** **VAPT** 17](#_Toc189074529)

[**8.** **Use of Service organization** 17](#_Toc189074530)

[**9.** **Business Continuity Planning** 18](#_Toc189074531)

[**10.** **Disaster Recovery Programme** 18](#_Toc189074532)

[**11.** **Antivirus** 18](#_Toc189074533)

[**12.** **Mandatory Trainings** 19](#_Toc189074534)

[**13.** **Cybersecurity** 19](#_Toc189074535)

[**14.** **SLA Timelines (AskIT Tool), DOA Matrix and Approval Flow Summary** 20](#_Toc189074536)

# **Standard operating policy & procedure (SOPP)**

## **Introduction**

This Standard Operating Policy & Procedure (SOPP) is a comprehensive document that outlines a series of step-by-step instructions created by J M Baxi Group to guide their employees in executing both complex and routine tasks.

SOPPs are designed to ensure efficiency, maintain high-quality output, and promote consistency in performance. This will help in supporting process excellence by streamlining operations and reducing variability in work practices.

This SOPP aims to achieve the following objectives:

* + 1. Act as a guide and reference document to stakeholders at all levels of the organization
    2. Clearly communicate activities and help to achieve consistency in operational procedures.
    3. Create accountability by assigning responsibilities at each stage of the lifecycle.
    4. Aid governance by documenting auditable processes and detailing control elements at each stage of the lifecycle.

## **Document Review and approval**

This SOPP shall be subjected to an annual review (or more frequently) as determined by author of the document. The assigned reviewer shall ensure the continued accuracy and validity for use of the document.

Revision history

| **Version** | **Created By** | **Document Approved By** | **Date Approved** | **Revision** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

| **SOPP Number** | XX |
| --- | --- |
| **SOP Owner** | CTO – Manish Jaiswal |
| **IT Applications** | SAP HANA  Terminal Operating System (TOS)  DarwinBox (HRMS) |
| **Guidelines / Policy reference** |  |
| **SOPP Cross References** |  |

# **Executive Summary**

This SOP covers activities pertaining to Information Security of J M Baxi including Logical Access Management, Change Management, Network Management, Cyber Security, Managing Service Organization system, Data Backup Operations and Restoration, Business Continuity Plan and Disaster Recovery plan processes at JMBAXI GROUP

1. The purpose of the Logical Access Management procedures is to provide a framework for the management of user access to organization’s business systems, networks and equipment through an IT team approved authentication service. The procedure includes granting, modifying, terminating, and reviewing user access privileges to organization’s systems and applications to protect the privacy, security and confidentiality of information assets and systems.
2. The Change Management procedure ensures that all changes (infrastructure, application, security updates, patches, and configurations) to operational IT systems are recorded, documented, and implemented successfully. It defines standardized processes for managing, controlling, and monitoring changes with minimal disruption, ensuring that approved changes are assessed, authorized, and scheduled efficiently.
3. The purpose of cyber security procedures is to protect systems, networks, and data from cyber-attacks.
4. The purpose of evaluating the SOC (System and Organization Controls) reports is to assess the effectiveness of the control environment at the vendor organization. This evaluation ensures that the respective General Information Technology domains are functioning as intended and operating effectively. The process helps to verify that appropriate procedures are in place to safeguard the integrity, confidentiality, and availability of the services provided to J M Baxi Group.
5. The Data-Backup and Data Restoration Management procedure defines activities for creating or modifying a backup job, monitoring the successful completion of all scheduled jobs and reviewing user access privileges to schedule jobs. The purpose of restoration to ensure that IT systems and data can be restored after a disaster or incident.
6. A business continuity plan (BCP) and disaster recovery plan (DRP) help businesses prepare for and respond to major disruptions and disasters that could impact their IT systems and operations.

The purpose of this process document is to provide an operational process that enables a standard process for backup and recovery process to achieve its stated objectives.

Throughout this SOPP, any reference to 'organization,' 'entity,' or 'company' shall be read as J M Baxi Group.

# **Scope**

This policy applies to all users of the organization’s information systems, as well as personnel responsible for managing user accounts or controlling access to information assets and systems, including Business Owners and administrators for both centrally and decentralized managed systems.

It specifically applies to the following applications, along with their operating servers, databases, and servers:

* SAP S/4 HANA
* Terminal Operating Systems (TOS)
* Darwinbox (HRMS)

Note: As Darwin is the HRMS application managed by the vendor, controls beyond user access management are the responsibility of the vendor. To ensure general information technology procedures are operating effectively, the Application Head obtain and evaluate SOC (System and Organization Controls) report from the vendor for these areas.

# **User Access Management**

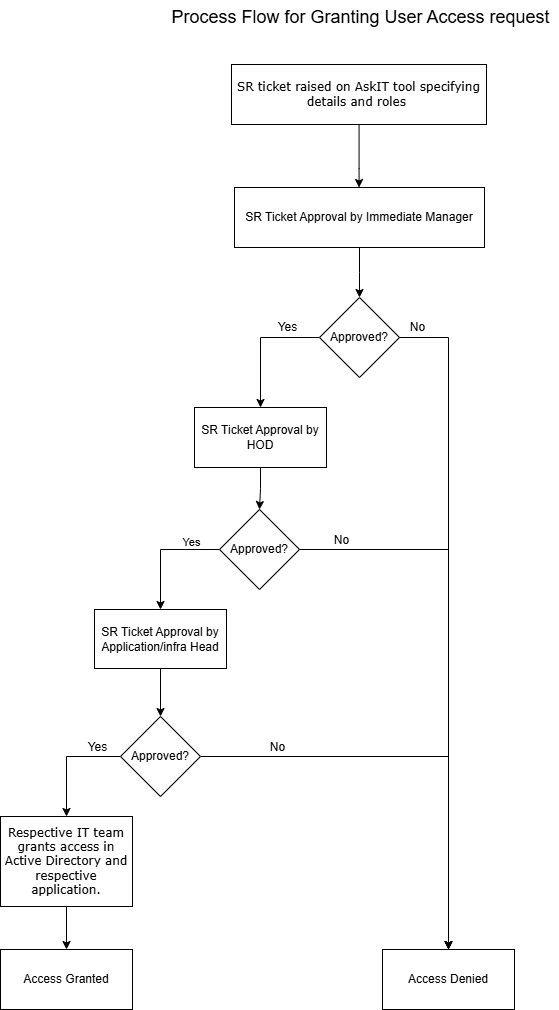
## **Granting User Access**

Access to the organization’s network and applications is granted on a need-to-know basis, determined by the roles, responsibilities, and business activities assigned to the user.

User or respective user’s manager raises an access request for the employee on the relevant applications through a Service Request (SR) ticket on AskIT tool. The roles to be assigned are mentioned in the SR ticket and selected based on predefined roles in the applications, aligned with each user’s roles and responsibilities.

Once the ticket is raised, it goes through defined approval workflow: the Immediate manager, HOD, and the Application/Infrastructure Head. In case of request raised by the respective manager, the first level approval is provided by their immediate reporting manager in the workflow.

After approval, the respective IT team members will create the necessary access in the relevant information system. The same process is followed for generic user, standard user, privilege user, in case of remote access is assigned in the system.



## **Modifying User Access**

In the case of transfers or changes in roles and responsibilities within the organization, reporting manager ensures that the access rights of respective users are modified to align with their new responsibilities. Access rights that are no longer required are removed, while new roles are added.

The process for modifying user roles and accesses follows the same procedure as for granting access. Requests for changes to a user's access rights are raised via a SR ticket on AskIT tool and follows the same procedures as for granting user access.

## **Removal of User Access**

Employees who leave the organization voluntarily or are dismissed/terminated have their access rights revoked within one business day of their last working day from the information system. User accounts will be deactivated across all systems to ensure that there is no unauthorized access to systems after their termination.

On the employee's last working day, the reporting manager will send an email confirming that there are no objections to the employee’s release. Following this, the HR team will raise an incident ticket in the AskIT tool to revoke access. Once the ticket is raised, it is routed to the respective application IT Teams, who will deactivate the user’s access within 1 working day.

## **Privileged Users**

IT Team provides access privileges to organization’s technology (including networks, systems, applications, computers, and other devices) based on the following principles:

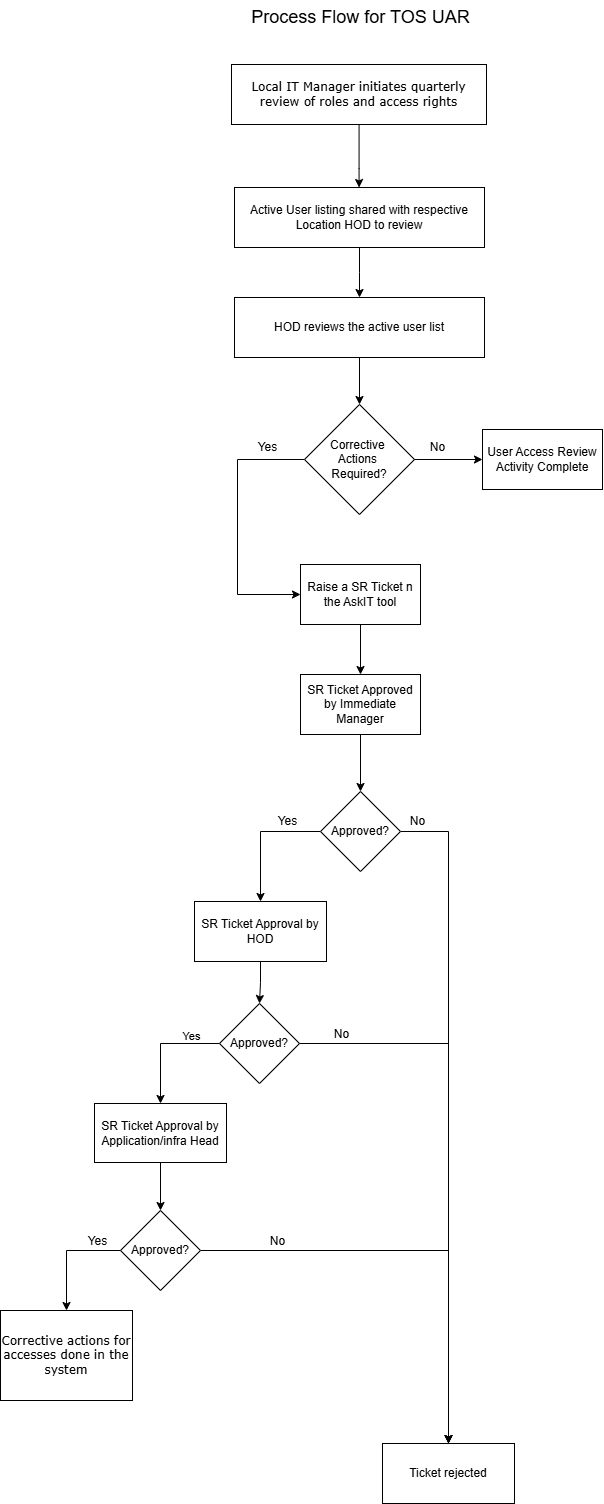
* Need to know – Users or resources will be granted access to systems that are necessary to fulfil their roles and responsibilities.
* Least privilege – users or resources will be provided with the minimum privileges necessary to fulfil their roles and responsibilities.

Requests for access to an administrator or privileged user roles are raised through an SR ticket in the AskIT tool. Such requests will follow the same approval workflow as granting access to new users.

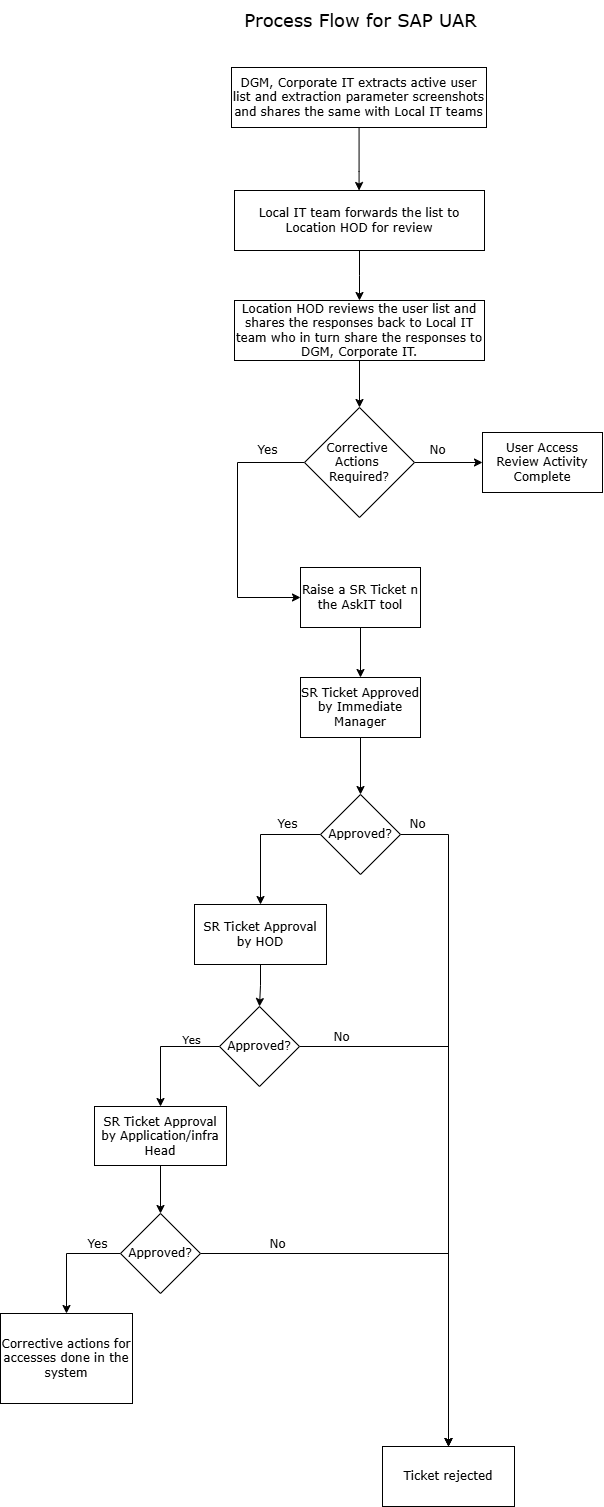
## **User Access Review**

User access review is conducted on a quarterly basis (for SAP and TOS) and monthly (for DarwinBox) to ensure that the user exist in the organization and current access rights assigned are relevant and appropriate for each user. The results and approvals are maintained on email and retained for auditing purposes. It should include a complete list of active users on the respective system. Active user list from the application is compared with the HR listing before initiation.

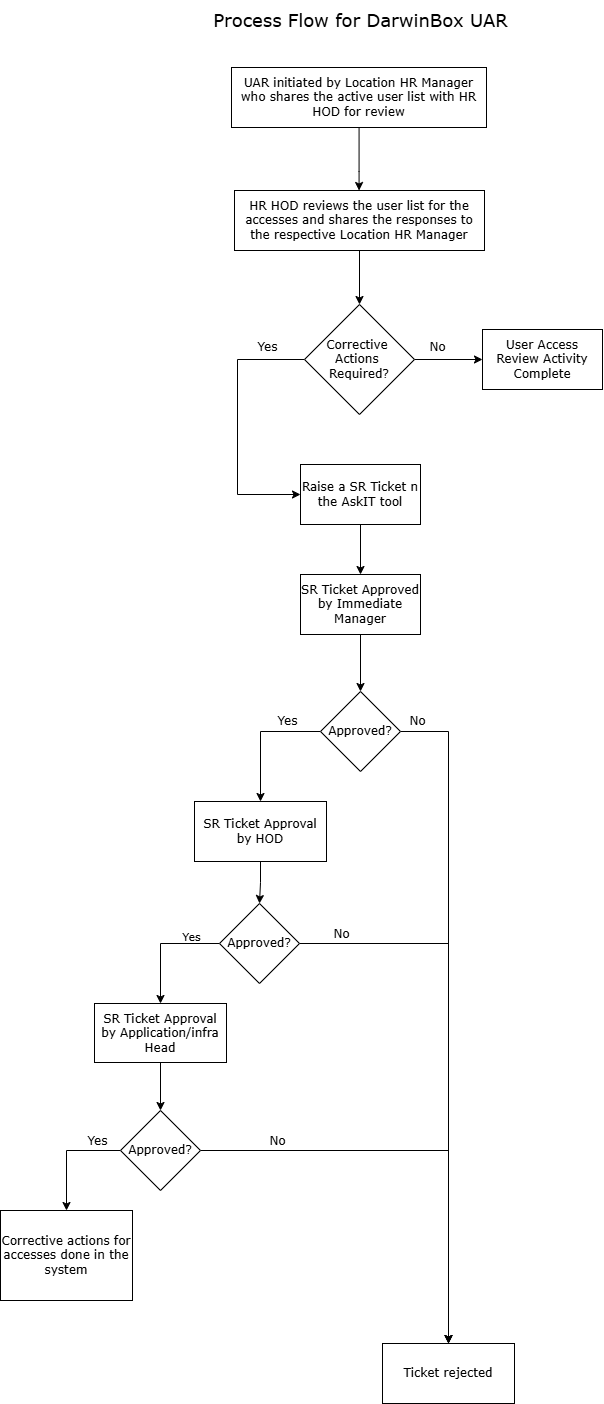
**For Terminal Operating Systems (TOS)**, the Local IT Manager is responsible for initiating the quarterly review of roles and access rights granted to users. Local IT Manager extracts the location-wise active user list from application, along with screenshots of the extraction parameters to validate completeness and accuracy. The review is done by the respective Location HOD. Once reviewed, any required changes to access privileges of users then such changes are requested and processed by raising a SR ticket in the AskIT tool. The SR ticket will follow approval workflow: the Immediate manager, HOD, and the Application/Infrastructure Head.



**For SAP**, the DGM Corporate IT extracts the location-wise active user list from application, along with screenshots of the extraction parameters to validate completeness and accuracy. The list is shared with the respective local IT Managers at each location, who then forward it to the location HOD for review. The central DGM Corporate IT receives the validated responses within two weeks of initiation. Following this, initiator raises a SR ticket in the AskIT tool for corrective actions based on the review, which will follow same approval workflow.



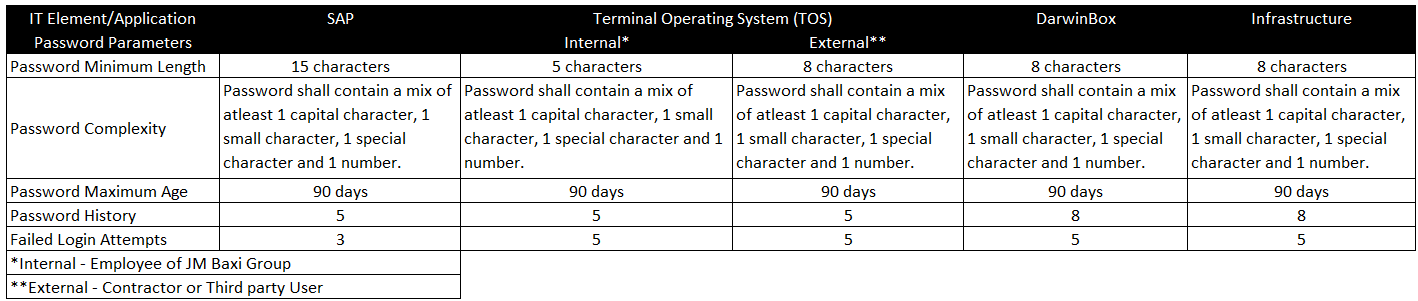
**For DarwinBox**, user access review is performed monthly for each entity. Location HR Manager extracts the location-wise active user list from application, along with screenshots of the extraction parameters to validate completeness and accuracy. The activity is initiated by the location HR manager and reviewed by the HR HOD. Once reviewed, any required changes to user access privileges are requested and processed by raising a service ticket in the AskIT tool.



## **Password Management**

There is a common policy for both standard and privileged users. Appropriate technical specifications for password management are implemented for both network and applications, respectively:

1. Password Length - Minimum length of user level password shall be eight characters (15 characters in case of SAP and 5 characters in case of Internal ID on TOS).
2. Password Maximum Age - Maximum passwords age for regular users and privilege users shall be 90 days.
3. Password Complexity - Password shall contain a mix of atleast 1 capital character, 1 small character, 1 special character and 1 number.
4. Password History - Password history shall be maintained for last five passwords. (8 for Network)
5. Failed Login Attempts – After 3 (5 for Network and TOS) consecutive failed login attempts, a user account MUST be locked out.



## **Database Access**

Access to the SAP and DarwinBox database is managed directly by the vendor. The IT team from respective application raises a request via email to the vendor, post which the relevant actions are carried out.

For TOS, database access is maintained with the entity, access for the same is granted through SR Ticket, which is approved by HOD, Application Head and Infrastructure Head.

To ensure general information technology procedures are operating effectively for the databases of SAP and DarwinBox, the Application Head obtain and evaluate SOC (System and Organization Controls) report from the vendor for these areas.

(Space left blank)

# **Change Management Process**

## **Change Process**

User (Business or IT Team) at the respective location raises a request regarding any system issue, business requirement to modify any configuration at system, improvement in functionality of system to the location IT Manager (SPOC – Single Point of Contact). The IT Manager then analyses the request, evaluates whether it is a system issue or a new improvement, and categorizes it as either an incident ticket or a change request. IT Manager then instructs the requestor to raise the appropriate ticket.

In case a Change Request ticket is raised by IT Manager (SPOC) directly in AskIT tool, the ticket is then approved by the immediate manager, Business HOD, and Application/Infrastructure Head.

After the three-level approval process, the details are shared with the respective vendor, who provides the costs and efforts required to develop the change. Post which it follows the defined procurement process.

Upon completion of development, the requestor performs User Acceptance Testing (UAT). Once UAT is completed the test results are communicated through comments in the respective tickets or email as part of UAT confirmation process.

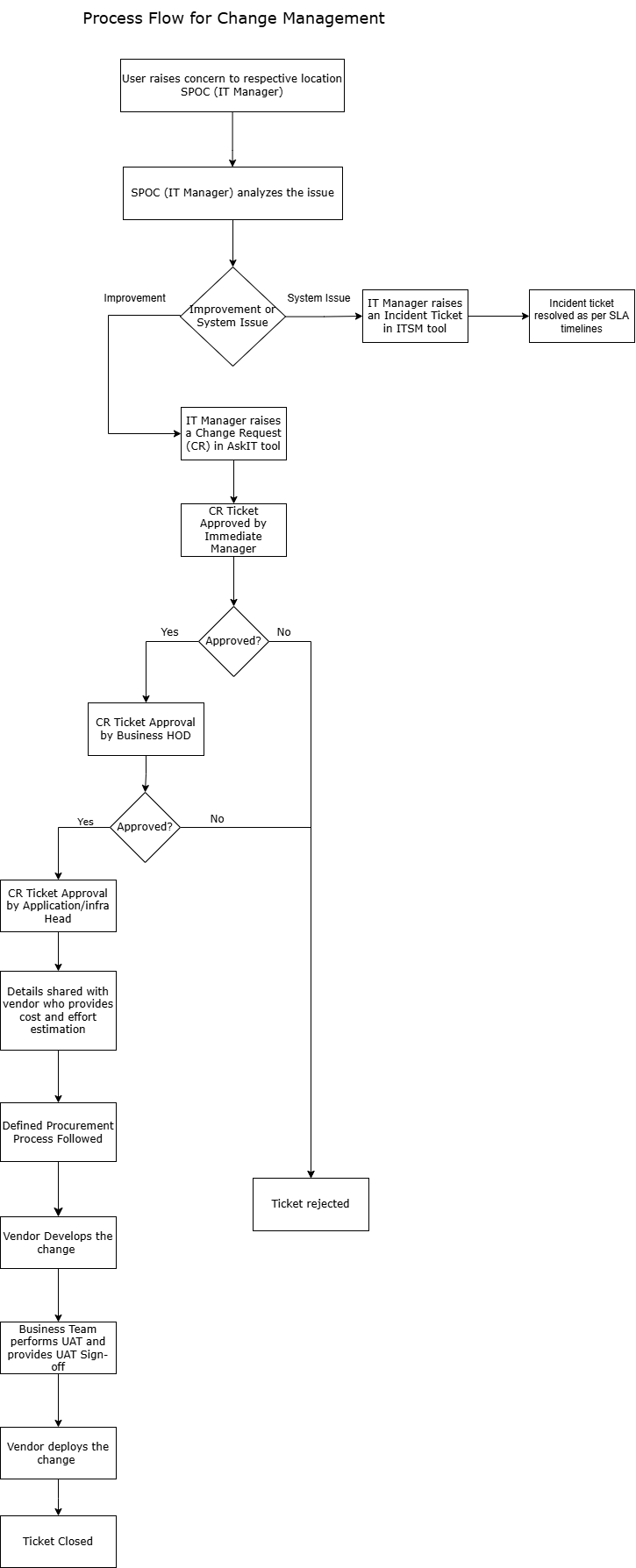
Once UAT sign-off is received, the different team from vendor deploys the change in the production environment with their user id.

There is no separate process for emergency changes.

In case, an Incident ticket is raised, the ticket is directly shared to the Vendor, and it is resolved as per the SLA timelines defined.

## **Segregation of Environments**

There are three environments: development, testing, and production for SAP and TOS. The entity manages all three environments, although the vendor also has access to all of them. The vendor is responsible for deploying changes to the production environment and obtains internal approval within their respective vendor organization before implementing changes.



# **Data-Backup and Scheduled Job Management**

The backup and restoration activities include maintenance tasks necessary to maintain the backup and restore solution. These tasks include cleaning the media, recycling the media, testing the operation, and performing any input/output maintenance required before or after the backup or restore operation.

## **Backup procedures**

The entity uses the Commvault backup tool to manage its backup processes, with automated triggers in place for failed backups. If a backup fails or encounters an error, the respective Application and Database Head notify the Backup Admin via email, prompting corrective actions to be taken.

Backups are stored on storage which is on premise. The first copy of the backup is written to this on-premises storage, while the second copy is written to a tape, which is then sent offsite to Mumbai (Churchgate location) by the IT team. This offsite backup is essential for disaster recovery. In the event of a disaster at the data centre, data stored solely on-site could be lost, so having a copy offsite ensures that the data can be retrieved and restored from an alternate location.

The Backup Admin has full access to the backup schedulers, enabling them to manage and monitor backup jobs effectively. Any changes to the backup schedule require a Change Request (CR) ticket to be raised in the AskIT tool which follows the same three level approval process defined in AskIT tool to ensure the backup process remains secure and efficient.

For SAP Full Backups are taken every 15 minutes and retained for 30 days. Backup for SAP and Darwinbox are managed by the respective vendors.

Below are the schedules/defined frequencies for Backup on TOS:

1. Daily Backup (Incremental)
2. Weekly Backup (Full Backup)
3. Monthly Backup (Full Backup)
4. Yearly Backup (Full Backup)

Below attachment contains details Backup schedule details for various container and non- container entities:



Tickets for corrective action regarding failed backups are raised on AskIT Tool and follow three level approvals (Immediate Manager, HOD, Application Head). Post the retention period the backups are over written.

## **Restoration procedures**

Backup Admin perform full system restoration on a quarterly basis. Post restoration activity, respective Application Head will log into the application and check if the restored files (transactions) are in line with the expectations or not.

For TOS, accountability lies with Head (Corporate) but responsibility to check for successful restoration lies with respective location Head for verifying usability of restored backup files.

## **Scheduled Job Monitoring**

Access to schedule jobs (Batch Jobs / Interface Jobs / etc.): It provides users with access to create, modify, or delete a scheduled job. Such access shall be given to individuals based on their role.

Scheduled Job Monitoring: Scheduled jobs should be monitored and reviewed on a periodic basis to ensure successful completion and in case of any failure an automated alert / email should be sent to the respective Team Leads / Team members. In case of a job failure, the team should ensure that proper steps are taken to rerun the failed job.

In case a job fails, IT manager will raise a SR ticket on AskIT Tool. Ticket is to be approved by Immediate Manager, HOD, Application Head.

# **Network Management**

* 1. **Firewall, VPN & IDS**

The firewall and VPN services are both provided by Sophos XDR Endpoint Security Solutions. VPN access is role-based and built into the firewall, which has the capability to create multiple VPN connections. VPN management is centralized.

Logs for changes made to the firewall are monitored on a change-by-change basis, with a quarterly review of the changes. Firewall configuration changes are carried out by a designated Security Lead, and a ticket for each change is raised in the AskIT Tool. -Network and Security team lead is responsible for making these changes and has the necessary access to do so.

Logs are maintained directly within the hardware as a built-in feature, and there is no separate log manager. These logs are stored in a readable format and have a retention period of three months. Alerts for intrusion detection are generated through two mechanisms: first, logs configured within the hardware/system itself to trigger alerts, and second, a configuration that sends alerts to an email address. The respective owner of the firewall receives these email alerts for such intrusions. Post which they analyse the root cause of intrusion and business impact due the same.

## **VAPT**

VAPT (Vulnerability Assessment and Penetration Testing) is conducted by a vendor who must be CERT-IN certified. The testing is performed on business-critical applications, such as SAP, TOS, AD firewall, network switches etc. For applications hosted within the entity’s data centre, VAPT is performed twice a year. The vendor is selected based on the best combination of commercial value and mitigation capabilities.

1. **Preparation**: Scope is finalized with the vendor on email before beginning the activity.
2. **Assessment and Reporting:** Based on VAPT scope, generate and review the Vulnerability Scan report. Prepare remediation plan and send to concerned teams along with the report for remediation. The scan report is shared with password protection with the password shared over a different medium.
3. **Remediation:** Follow up with the asset/action owner teams regarding remediation actions to keep track of their implementation status. Raise escalations as per the escalation matrix of the asset/action owner teams whenever Critical and High vulnerabilities are not fixed within stipulated time.
4. **Verification:** Once the remediation is done, asset/action owner teams shall notify VM team. Re-launch scan with the same policies and configuration on the same asset group to check if the vulnerabilities are fixed. If any of the vulnerabilities are not fixed, VM team shall share the report with the concerned asset/action owner team to fix as per the recommendations.

# **Use of Service organization**

Based on the requirements of the entity, activities in IT functions outsourced to suitable vendor / third party service organization. In such circumstance, Head of IT shall ensure that such organization shall have appropriate control and governance framework and shall evaluate their service performance on regular basis by doing a yearly review of the SOC report provided by the vendors/ third party service organization.

After evaluating the SOC report provided by a service auditor, Application Head assesses the effectiveness of the service provider’s controls, focusing on any identified risks or gaps. They review the **Complementary User Entity Controls (CUEC)** to ensure that the user entity’s own controls align with the provider’s processes and mitigate identified risks. They also examine **Complementary Subservice Organization Controls (CSOC)** to verify that the controls from subservice organizations are effectively integrated into the overall service delivery. They work with the service provider to address any deficiencies, updates internal controls, ensures compliance with regulatory requirements, and reports findings to relevant stakeholders. Ongoing monitoring and follow-up actions are taken to mitigate emerging risks.

1. **Business Continuity Planning**

In the event of Business Continuity Plan (BCP) activation, there is no separate team designated for handling the process. Instead, an incident ticket is raised, a Root Cause Analysis (RCA) is performed, and the RCA is embedded within the ticket. Actions are taken on a case-by-case basis to address the issue.

If an individual is unable to raise a ticket, for example, due to a natural calamity, the issue is escalated to the business head. The business head will take appropriate action and communicate with the IT team regarding the problem.

The BCP primarily focuses on incident management, ensuring that the organization can effectively respond to and manage incidents during disruptions.

1. **Disaster Recovery Programme**

Corporate IT is responsible for deciding the date for the DR drill. Once the date is confirmed, it is communicated to the respective location IT team, who will ensure they are prepared for the drill. After confirmation from the respective location IT team that they are ready, a notification email is sent to the DR vendor to begin the drill. Location IT Team send a confirmation to respective Location / Business Unit for successful completion of the DR Drill, along with additional details.

The approval for conducting the DR drill is granted by the Chief Technology Officer (CTO). The Head of IT) is responsible for seeking approval from the CTO. This approval process involves close coordination with the business unit (BU) to ensure alignment with business needs. The IT Head coordinates with the location’s business head, and after receiving their approval, the IT Head proceeds to obtain the CTO’s approval.

The primary responsibility of the location IT team is to notify employees about the upcoming DR drill, typically through a downtime notification email. If the location IT team encounters any issues during the process, they are responsible for communicating any significant problems back to the corporate IT team for resolution.

The DR drill is executed by the senior database manager at the corporate level. Once the drill is completed, the senior database manager prepares a report, which is sent to the Head of IT. During the monthly meeting, this report is shared with the CTO, who then presents it to the business units and relevant IT teams at the locations.

The DR drill is conducted twice a year to ensure that the systems and teams are prepared for potential disruptions.

1. **Antivirus**

The antivirus solution, provided by the same vendor as the firewall (Sophos XDR Endpoint Security Solutions), performs real-time scanning to ensure endpoint security. Configuration changes are restricted as access is role-based. Every fortnight, the security team extracts a report from the console and shares it with each location SPOC (IT Manager) who will monitor if any further activity is required. If any discrepancies are found, such as a system being out of date, the issue is highlighted via email to the relevant location SPOC (IT Manager) for resolution.

1. **Mandatory Trainings**

During the induction process, all employees receive training, which covers essential topics, such as how to raise an incident and other relevant procedure. In addition, monthly or quarterly security awareness training sessions are held, depending on the entity’s schedule. These sessions educate employees on topics such as performing local backups, understanding backup protocols, and raising incidents using AskIT tool. Training is provided through both prerecorded content and in-person sessions.

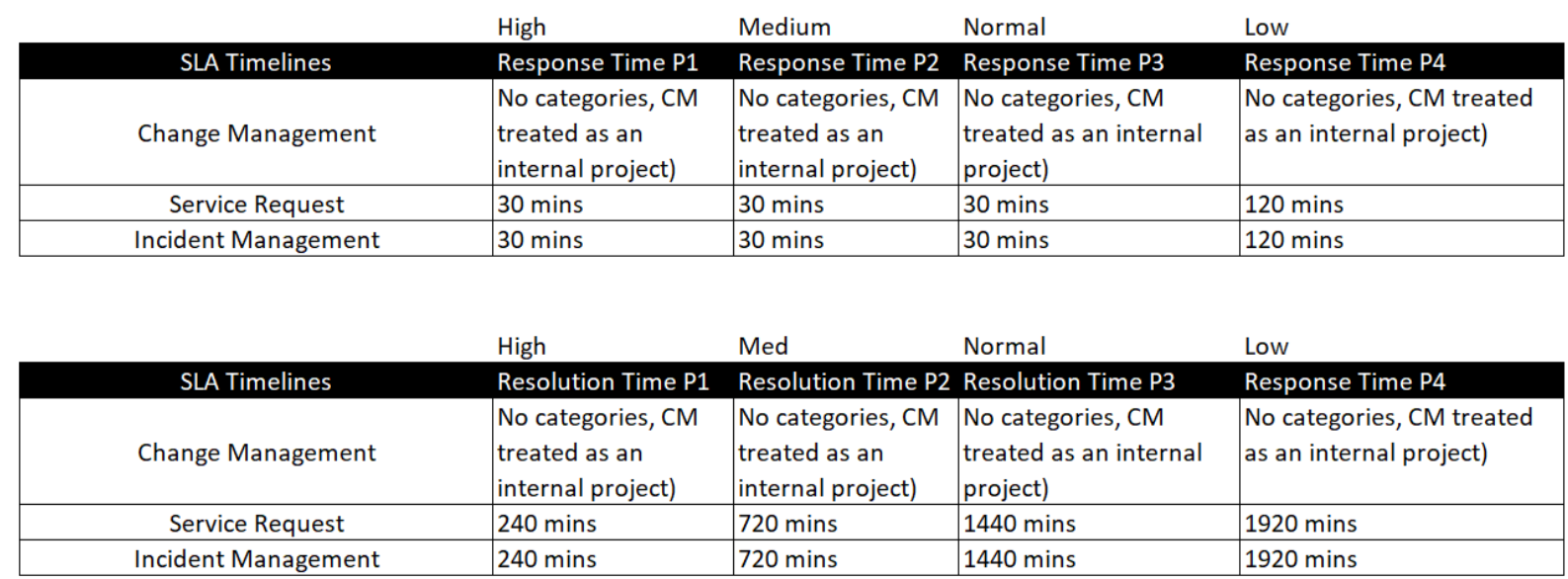
# **Cybersecurity**

Below are some of the initiatives taken by the management to be cyber resilient.

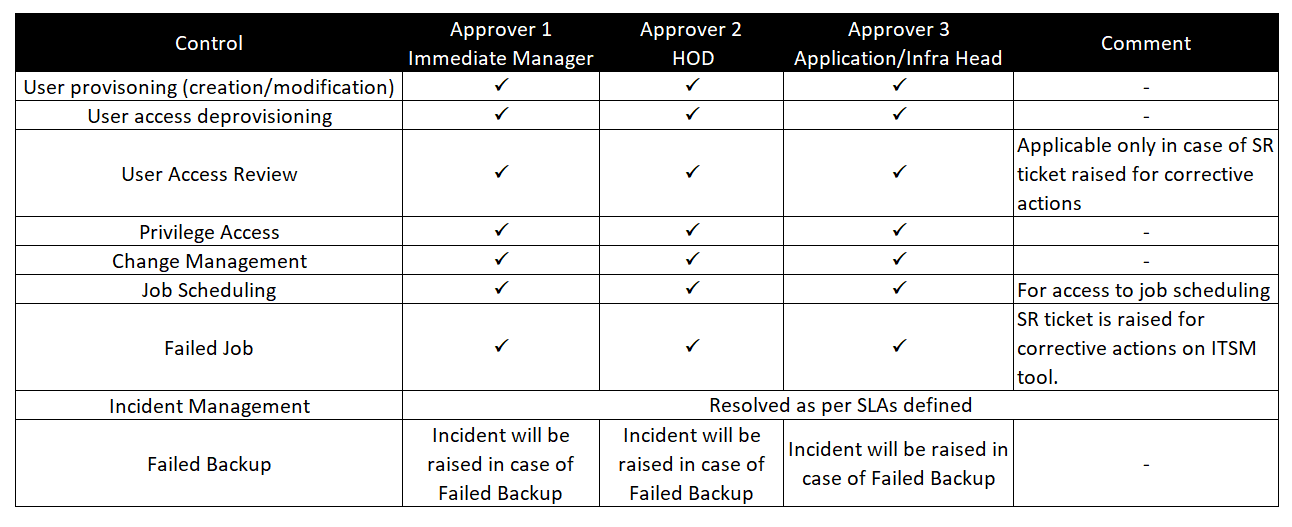
1. **Patch Management**: Monthly reviews are conducted, showing the status of patches enabling proper monitoring of patch installation.
2. **Active Directory (AD) Management**: Previously, manual intervention was required to check logs through remote access to track actions such as who created a user ID. Now, through AD management, logs can be displayed, making this process more efficient. For example, email notifications that were not previously received are now sent.
3. **Domain Scorecard (UpGuard - OEM)**: A Gartner-rated tool that evaluates the reputation of web-facing applications or domains. This project started in September 2024 and is currently being applied to all the organization's domains.
4. **AskIT (IT Service Management)**: A ticketing tool used to raise Change Requests (CR), Service Request (SR), and Incident Management (IM) tickets.
5. **ITAM (Asset Management)**: Inventory is captured and managed through the Asset Management Tool.
6. **Secure Wi-Fi**: Implemented using Cisco solutions (Cisco ISE). The Wi-Fi is integrated with Active Directory (AD) so that passwords are regularly updated. Guest Wi-Fi access is granted through QR codes, which are updated monthly. This was implemented in the current financial year. Mobile Wi-Fi access is managed via MAC address binding.
7. **Cisco Thousand Eyes**: This is an agent-based product used to monitor application bandwidth and throughput. It identifies areas of interruption and helps detect vulnerabilities.
8. **Cloudflare**: A solution for Web Application Firewall (WAF) and DNS management. It provides a centralized dashboard to monitor incoming traffic, assess potential vulnerabilities, and determine the legitimacy of the traffic based on its source country. The tool works at the application level, sitting on top of the firewall, and offers protection against DDOS attacks and cache management.
9. **Data Loss Prevention (DLP)**: Currently implemented for only one entity, this tool prevents data leakage from laptops. It monitors all data movement on laptops, and the tool sends notifications regarding any suspicious activity.

# **SLA Timelines (AskIT Tool), DOA Matrix and Approval Flow Summary**

Below is SLA Resolution and Response timelines for tickets raised on AskIT tool:



**Delegation of Authority (DOA) Matrix**



Appendix A: List of JM Baxi Group entities:



\*Terminal Operating System (TOS) refers to applications which are utilized to manage operations at the respective location.

Appendix B: Process workflow summary:

