

Objective:

Provide a standardized approach to identifying, building, and maintaining automation solutions across business units while ensuring compliance and security.

1. Process Identification:

- Choose processes with high volume, low complexity, and clear rules.
- Prioritize repetitive tasks that consume more than 5 hours weekly.

2. Documentation:

- Record each step of the existing manual process.
- Maintain a process definition document (PDD) for every automation.

3. Development Standards:

- Use version control (Git) for all automation scripts.
- Follow naming conventions and code review checklists.
- Include exception handling and retry mechanisms.

4. Credential Management:

- Store credentials in secure vaults (CyberArk / Azure Key Vault).
- Never embed secrets directly into code or scripts.

5. Testing & Validation:

- Conduct unit testing and user acceptance testing before deployment.
- Keep detailed logs for all automated executions.

6. Monitoring & Reporting:

- Schedule weekly performance checks.
- Report average execution time, success rate, and error trends.

7. Continuous Improvement:

- Review automated processes every 3 months.
- Update scripts based on new business or system changes.

8. Compliance:

- Follow IT security and data privacy policies.
- Ensure automation audit logs are retained for at least 6 months.