Checklist

Essential Steps for Successful IAM Implementation

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

An Identity and Access Management (IAM) solution is critical for offering secure access in a world where data is constantly under threat. However, without proper planning, it can lead to bad user experiences and security gaps that decrease customer satisfaction and increase the risk of breaches.

A holistic approach to identity security is crucial, covering all user constituencies—workforce, customers, and partners/third parties. By taking an identity-centric approach to your security strategy, you can proactively safeguard sensitive information across all channels, anticipate potential threats, and adapt to evolving regulatory requirements, all while streamlining user access and enhancing productivity. This comprehensive perspective not only addresses current issues but also prepares organizations for future challenges, ensuring their strategies remain resilient against emerging risks.

After you've completed an RFP, you will gain insights into the solutions available and how they align with your organization's specific needs. This checklist serves as a resource to guide you through each step of implementation, ensuring ongoing security, scalability, and compliance.

Phase 1: Pre-Implementation

Assessment and Planning

- ☐ Clear objectives and business requirements: Identify what business goal you want to achieve (strengthen security, reduce management overhead, etc.) and the organization's IAM objectives.
- ☐ Risk assessment: Perform a thorough risk assessment to understand the potential risks, gaps and vulnerabilities within your organization.
- ☐ Mitigation Strategies and contingency planning: Develop strategies to mitigate identified risks and create a contingency plan to minimize disruption if risks arise.
- ☐ Timeline: Set a realistic timeline with key milestones, and allow adequate time for planning, implementation, testing and training.

Stakeholder engagement

- ☐ Collaboration with key contributors: Engage representatives from various departments including IT, security, compliance and business units for their input and support.

- ☐ Mobilize internal teams: Assemble a skilled internal task force (SIs and GIs) or choose a trusted partner that is empowered to drive the IAM implementation. Ensure team members possess the necessary expertise and training to navigate the complexities of the solution.
- ☐ Secure Executive Sponsorship: Rally support from senior management. Their buy-in is crucial for ensuring that IAM initiatives are prioritized and adequately funded.

Implementation Prerequisites

- ☐ Technical preconditions: Verify that all impacted applications, services and systems are compatible with the IAM solution, including protocol support, integration and infrastructure readiness.
- ☐ Business preconditions: Ensure alignment with company policies, legal frameworks, and strategic goals, especially regarding the use and protection of user data.
- ☐ User lifecycle management: Define how user roles, provisioning, deactivation, and access will be managed throughout the lifecycle to ensure seamless and secure user experiences.
- ☐ Requirements: Clearly define the requirements based on business needs, security policies and compliance regulations.
- ☐ Baseline metrics and KPIs: Establish baseline metrics and KPIs to measure the success of the IAM implementation and ensure continuous improvement post-deployment.

Deployment Efficiency

- ☐ Minimum requirements: Clearly define the essential requirements needed to deploy the solution.
- ☐ Design for performance and resilience: Consider incorporating stress testing, load balancing, failover mechanisms and scalability efforts to ensure the solution can withstand future developments.
- ☐ Time to market: Determine the average duration of product deployment.
- ☐ Evidence of efficiency: Request evidence showcasing how the solution effectively reduces time to market.

Implementation Team Setup:

- ☐ Onboarding procedure: Equip the implementation team with a comprehensive understanding of the customer onboarding process to align it with organizational standards and user needs.
- ☐ Onboarding team composition: Assess the roles and responsibilities of the team members involved in the onboarding process.
- ☐ Automated offboarding capabilities: Determine if the team needs to automated processes for deactivating and deleting inactive or idle accounts.
- ☐ Onboarding process alignment: Ensure the implementation team understands the customer onboarding process and aligns it with organizational standards.
- ☐ Team roles and responsibilities: Define clear roles, skills and responsibilities for team members involved in the onboarding process.
- ☐ Cross-team collaboration: Confirm that senior leadership has allocated the necessary bandwidth for cross-team collaboration.

Data migration

- ☐ Data quality assessment: Before data migration, evaluate the quality of your existing data to identify and address issues such as duplicate or incomplete records.
- ☐ User data handling: Confirm that user credentials and data are safe and encrypted to maintain consistent access and a seamless user experience across platforms.
- ☐ Data preservation: Ensure data is not lost during migration, and user passwords are migrated as-is to avoid requiring password resets post-migration.
- ☐ Compliance alignment: Ensure that the data migration process adheres to regulatory requirements, helping maintain compliance with privacy and data protection standards like GDPR and DORA.
- ☐ Backup and recovery plans: Establish robust backup protocols prior to migration to protect against data loss and determine a clear recovery strategy.

Phase 2: Implementation & Deployment

MVP Launch Strategy

- ☐ MVP purpose: Start with a Minimal Viable Product (MVP) approach to deliver essential capabilities quickly, demonstrating immediate value and allowing for faster feedback and stakeholder buy-in.
- ☐ Scope: Define a specific business line, application or service as the focus of the MVP launch to prioritize essential needs and address high-impact use cases.
- ☐ Timeline: Plan a 3-4 month launch window to get tangible results early in the process.

Go Live Checklist

- ☐ System integration testing: Determine if your tool needs to integrate with existing applications and infrastructure to ensure all components function together seamlessly.
- ☐ User acceptance testing: Engage end users in the testing process to validate that the IAM solution meets their needs and functions as expected in real-world scenarios.
- ☐ Load/stress testing: Simulate high traffic and peak usage scenarios to ensure the IAM solution can perform under pressure and scale effectively.
- ☐ Penetration testing: Conduct ethical and controlled hacking to identify vulnerabilities and ensure the solution is secure from external threats.
- ☐ Security testing: Perform appropriate security assessments to verify that the solution meets industry standards and is resistant to common attacks.
- ☐ Operational readiness: Prepare operational documentation, SOPs, FAQs and other training materials for the support team to ensure smooth operations and efficient troubleshooting post-launch.

Scalability and Future Developments

- ☐ Scalable framework: Define and implement a scalable framework that meets current needs and can adapt with future growth, ensuring seamless performance as business demands increase.
- ☐ Solution enhancement roadmap: Obtain an ongoing roadmap for future developments and updates to the IAM solution.

Phase 3: Operational & Post-Deployment

Ongoing & Global Support

- ☐ Incident response review and updates: Regularly review and update the incident response plan based on actual incidents and emerging threats.
- ☐ Always-on monitoring: Establish ongoing monitoring and maintenance processes to ensure the solution is effective, secure and compliance with evolving business needs.
- ☐ Support organization: Understand how ongoing support will be organized post-implementation
- ☐ User training: Invest in training programs for end-users, administrators, and support staff to familiarize users with the solution.
- ☐ 24/7 Support: Confirm if 24/7 support and services are available for offices around the world to troubleshoot issues, provide technical fixes, and maintain operations without disruption.

Audit and Compliance

- ☐ Compliance: Ensure compliance with internal policies and external regulations like GDPR, FEDRAMP, CCPA and others, while maintaining a detailed audit trail.
- ☐ Periodic audit checks: Perform regular audits to verify ongoing compliance and identify any potential gaps or areas for improvement.
- ☐ Customer support: Provide dedicated support to customers during audit periods to address any questions or issues that may arise.

Ongoing Optimization & Enablement

- ☐ Proactive support: Ensure that the vendor provides ongoing support for refining and optimizing the solution post-deployment, including guidance on integrating new features or addressing changing business needs based on business goals.
- ☐ Internal empowerment: Verify if the vendors have the training sessions and documentation needed to allow you to handle the solution independently and make minor optimizations where appropriate.

By following this checklist, your organization will be well-prepared to implement an IAM solution that meets your specific needs. A thorough, well-planned approach ensures not only a smooth deployment but also continuous security, compliance, and scalability as your business grows.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.