

IAM BUYER'S CHECKLIST FOR IT MANAGERS

This checklist will help you evaluate Identity and Access Management (IAM) solutions to ensure they meet your organization's needs.

I. CORE IAM CAPABILITIES

USER LIFECYCLE MANAGEMENT:

- AUTOMATED PROVISIONING (ONBOARDING)
- AUTOMATED DE-PROVISIONING (OFFBOARDING)
- SELF-SERVICE CAPABILITIES (PASSWORD RESETS, PROFILE UPDATES)
- CENTRALIZED USER DIRECTORY

AUTHENTICATION:

- SINGLE SIGN-ON (SSO)
- MULTI-FACTOR AUTHENTICATION (MFA)
- SUPPORT FOR VARIOUS MFA METHODS (APP, SMS, HARDWARE TOKEN, BIOMETRICS)
- PASSWORDLESS AUTHENTICATION OPTIONS
- ADAPTIVE AUTHENTICATION (RISK-BASED)

AUTHORIZATION:

- ROLE-BASED ACCESS CONTROL (RBAC)
- ATTRIBUTE-BASED ACCESS CONTROL (ABAC)
- POLICY-BASED ACCESS CONTROL
- PRIVILEGED ACCESS MANAGEMENT (PAM) INTEGRATION

ACCESS GOVERNANCE:

- ACCESS CERTIFICATIONS/REVIEWS
- SEGREGATION OF DUTIES (SOD) ENFORCEMENT
- WORKFLOW-DRIVEN ACCESS REQUESTS
- DETAILED AUDIT LOGGING AND REPORTING

II. INTEGRATION AND COMPATIBILITY

DIRECTORY SERVICES:

INTEGRATION WITH EXISTING DIRECTORIES (ACTIVE DIRECTORY, LDAP)

CLOUD DIRECTORY SERVICES

APPLICATIONS:

PRE-BUILT INTEGRATIONS WITH COMMON SAAS APPS

API AVAILABILITY FOR CUSTOM INTEGRATIONS

SUPPORT FOR INDUSTRY STANDARDS (SAML, OAUTH, OPENID CONNECT)

HRIS INTEGRATION:

INTEGRATION WITH HR SYSTEMS (WORKDAY, BAMBOOHR) FOR USER PROVISIONING

ITAM INTEGRATION:

ABILITY TO LINK USER IDENTITIES TO IT ASSETS

AUTOMATED DEVICE ASSIGNMENT/RECLAMATION WORKFLOWS

MDM INTEGRATION:

ABILITY TO INTEGRATE WITH MOBILE DEVICE MANAGEMENT SOLUTIONS

CLOUD AND ON-PREMISES:

SUPPORT FOR HYBRID ENVIRONMENTS

INTEGRATION WITH CLOUD PLATFORMS (AWS, AZURE, GCP)

III. SECURITY AND COMPLIANCE

SECURITY FEATURES:

PROTECTION AGAINST COMMON ATTACKS (PHISHING, ACCOUNT TAKEOVER)

SESSION MANAGEMENT AND CONTROL

THREAT DETECTION AND RESPONSE CAPABILITIES

COMPLIANCE:

SUPPORT FOR RELEVANT REGULATIONS (GDPR, HIPAA, PCI DSS)

AUDIT TRAILS AND REPORTING FOR COMPLIANCE

DATA RESIDENCY AND SOVEREIGNTY OPTIONS

ZERO TRUST SUPPORT:

ABILITY TO SUPPORT ZERO TRUST ARCHITECTURE

IV. DEPLOYMENT AND MANAGEMENT

DEPLOYMENT OPTIONS:

- CLOUD-BASED DEPLOYMENT
- ON-PREMISES DEPLOYMENT
- HYBRID DEPLOYMENT

EASE OF USE:

- INTUITIVE ADMINISTRATIVE INTERFACE
- USER-FRIENDLY SELF-SERVICE PORTAL

SCALABILITY AND PERFORMANCE:

- ABILITY TO HANDLE A GROWING NUMBER OF USERS AND RESOURCES
- HIGH AVAILABILITY AND RELIABILITY

SUPPORT AND TRAINING:

- VENDOR SUPPORT AVAILABILITY AND RESPONSIVENESS
- TRAINING RESOURCES AND DOCUMENTATION

V. COST AND LICENSING

LICENSING MODEL:

- USER-BASED LICENSING
- RESOURCE-BASED LICENSING
- TIERED PRICING

TOTAL COST OF OWNERSHIP (TCO):

- IMPLEMENTATION COSTS
- ONGOING MAINTENANCE COSTS
- SUPPORT COSTS
- HARDWARE/SOFTWARE REQUIREMENTS

VI. VENDOR EVALUATION

VENDOR REPUTATION:

- MARKET PRESENCE AND STABILITY
- CUSTOMER REVIEWS AND TESTIMONIALS
- INDUSTRY RECOGNITION

VENDOR ROADMAP:

- FUTURE PRODUCT DEVELOPMENT PLANS
- COMMITMENT TO INNOVATION

VII. KEY QUESTIONS TO ASK VENDORS

- CAN THE SOLUTION SCALE TO SUPPORT OUR FUTURE GROWTH?
- HOW DOES THE SOLUTION INTEGRATE WITH OUR EXISTING IT INFRASTRUCTURE?
- WHAT SECURITY CERTIFICATIONS DOES THE VENDOR HAVE?
- WHAT LEVEL OF CUSTOMER SUPPORT IS PROVIDED?
- CAN WE SEE A DETAILED PRODUCT DEMO AND TRIAL?
- WHAT IS THE VENDOR'S STRATEGY FOR ADAPTING TO NEW SECURITY THREATS?