Data Perceptions®

Enterprise Identity Maturity Checklist

Enterprise identity is now the first and most important control surface for protecting collaboration in the age of AI impersonation. This checklist helps organizations quickly assess the strength of their identity posture across five maturity levels, from basic hygiene to advanced AI-resilient and agent-aware security. Each level reflects the evolving requirements for verifying users, devices, applications, and now AI agents across meetings, messaging, and contact center interactions. Use this guide to determine where your organization stands today and to identify the most impactful next steps to reduce impersonation risk, strengthen organizational trust, and prepare for the AI-driven threats emerging across digital collaboration workflows.

Level 1 – Legacy Identity Hygiene

- ☐ MFA enabled for all users
- ☐ Strong passwords, no shared accounts
- ☐ Remove dormant accounts
- ☐ Waiting rooms & restricted sharing in meetings

Level 2 – Secure Application & Cross-Tenant Identity

- ☐ SSO across apps; federation + SCIM provisioning
- ☐ Inter-Application secure authentication method (SAML, OIDC)
- ☐ Inter-Application user and group provisioning (SCIM)

Level 3 – Passkeys & Zero Trust

- ☐ Passwordless enabled for everyone
- ☐ Passwordless with secure keys for high-risk personnel and administrators
- ☐ Conditional Access using device posture, location, and risk

Level 4 – AI-Resilient Identity Security

- ☐ Behavioral & continuous authentication
- ☐ PAM with separate accounts and secure keys
- ☐ AI-driven anomaly detection for collaboration
- ☐ XDR/EDR & SIEM/SOAR integration

Level 5 – AI Agent Governance (2026+)

- ☐ Secure identities for all AI agents (nonhuman identities)
- ☐ Inline agent protections (prompt-injection & data-leak controls)
- ☐ Cryptographic meeting-join verification for sensitive calls
- ☐ Integrated deepfake detection in collaboration

Top 5 Priorities

- ☐ **Deploy phishing-resistant passkeys enterprise-wide**
- ☐ **Enable continuous, risk-based authentication**
- ☐ **Implement privilege access (PAM) for admins**
- ☐ **Govern AI agent identities & access**
- ☐ **Integrate real-time deepfake detection into workflows**

Preventing AI Impersonation across Meetings, Messaging, and Contact Center

People, Devices & Avatars

Employees & Execs
- Passkeys / FIDO2
- Phishing-resistant MFA
- Risk-based Conditional Access

Partners / Contractors
- Federated B2B
- Cross-tenant trust
- Verified ID prereg

Devices
- Managed & BYOD
- Device posture checks
- Compliance attestation

AI Avatars / Bots
- Meeting avatars
- Real-time voice/face impersonation
- Disclosure & policy controls

Collaboration & Communications (Meetings / Messaging / CCaaS)

Meetings
- Teams, Zoom, Meet, Webex
- Lobby / waiting room controls
- Cryptographic join for high-risk calls

Messaging & Channels
- Teams/Slack governance
- External guest policies
- Content controls & retention

Contact Center
- Agent identity verification
- Customer identity proofing
- Call deepfake detection

Access Control & Identity Fabric

IAM / SSO
- Microsoft Entra ID
- Okta / Google Identity
- SAML / OIDC / SCIM

Passwordless
- Passkeys (device-bound)
- Windows Hello
- FIDO2 hardware keys

Conditional Access
- Risk-based policies
- Device posture checks
- Step-up authentication

PAM & Secrets
- Segregated accounts
- Session recording
- Vaults (Key Vault, HashiCorp)

AI & Agent Security Controls

Agent Identity Governance
- Microsoft Entra Agent ID
- SailPoint Agent Identity Security
- Ownership & lifecycle governance

Runtime AI Protection
- Google Model Armor
- Prompt-injection defense
- Sensitive data leakage control

Deepfake Detection
- Voice & video verification
- Meeting bot integration
- Liveness challenges

Policy & Provenance
- Disclosure banners
- Content Credentials (C2PA)
- Recording watermarks

Security Operations, Data & Compliance

SIEM / SOAR
- Microsoft Defender / Sentinel
- Google SecOps / Mandiant
- Impersonation playbooks

Data Security & DLP
- Microsoft Purview
- Sensitive data labeling
- Data policies & rules

Audit & Compliance
- Access & meeting logs
- eDiscovery / Legal Hold
- Compliance reporting

Telemetry & Analytics
- Behavior baselines
- Anomaly detection
- Risk dashboards

AI-driven impersonation has transformed collaboration platforms into identity-critical systems, making traditional security controls insufficient. The Identity-First Collaboration Security Architecture provides a modern, layered model for securing meetings, messaging, and contact center interactions by unifying identity, access, AI-agent governance, and real-time threat detection. This architecture illustrates how people, devices, applications, AI agents, and content must be continuously verified to maintain trust in digital communication. It serves as a blueprint for organizations adopting passkeys, Conditional Access, PAM, deepfake detection, and emerging protections like Microsoft Entra Agent ID and Google Model Armor. Use this framework to align teams, reduce impersonation risks, and implement a security posture designed specifically for AI-era collaboration.

Identity-First Collaboration Architecture

Data Perceptions®

Secure Collaboration in the Age of AI Impersonation

Learn more at DataPerceptions.com