DATASHEET

Imprivata Digital Identity Maturity Model

A programmatic guide for achieving a unified and comprehensive digital identity strategy, with actionable steps to maturity based on current-state processes and solutions

Healthcare delivery organizations (HDOs) are under constant pressure.

The IT landscape has become increasingly complicated, with more users and roles requiring immediate access to clinical applications, from countless locations across diverse devices. Care providers need technology that enhances the care delivery process while security teams need to reduce risk and improve operations – particularly with diminishing resources and accelerating cyberattacks.

These challenges can only be solved with a comprehensive strategy to enable, control, and monitor all digital identities across the organization.

Digital Identity Maturity Model

Imprivata developed the Digital Identity Maturity Model to help HDOs prioritize investments to address gaps and optimize their identity and access management strategy.

Based on Gartner's IAM Program Maturity Model and tied closely to the Imprivata Digital Identity Framework, the maturity model introduces five phases of identity maturity with increasing levels of security, compliance, and end-user access:

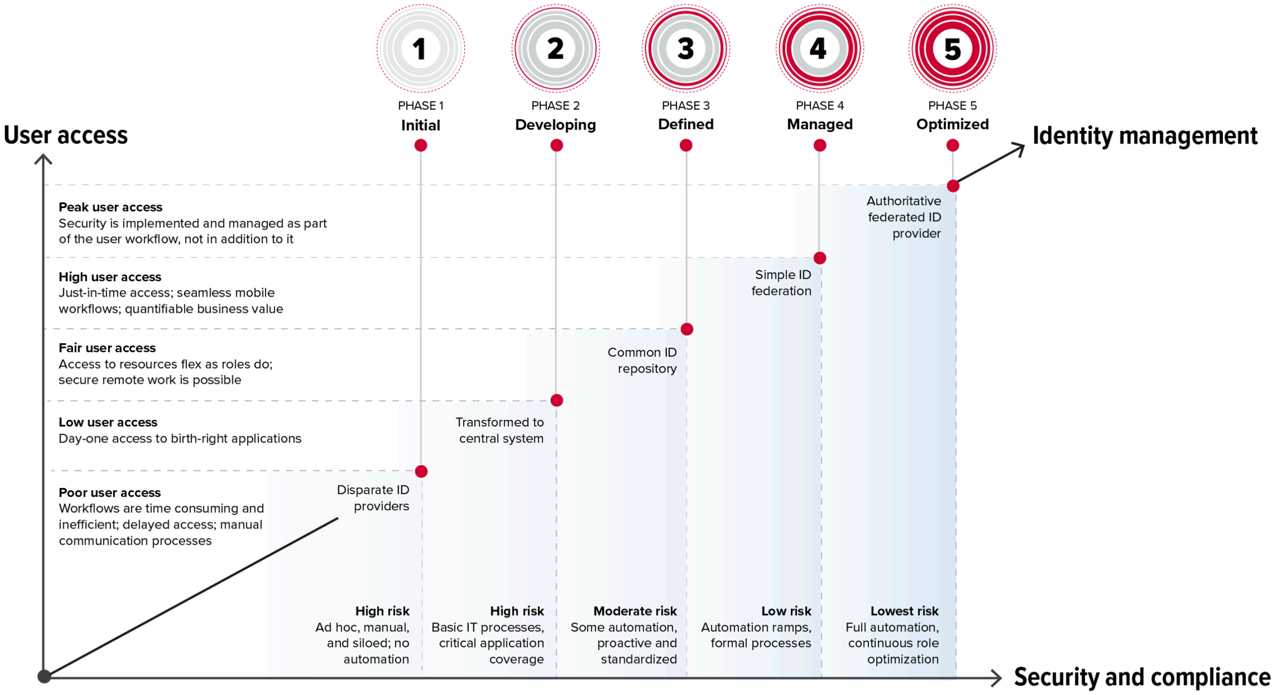
Phase 1: Initial – characterized by high risk and generally poor user access, this phase precedes the implementation of a formal digital identity strategy. Manual workflows and siloed user and account management result in costly mistakes and high security risks.

Phase 2: Developing – organizations in this phase are at high risk and offer poor user access, with the basics of an IAM program in place (i.e., basic tools are used to strengthen the security posture, manageable IT processes are in place, and critical applications are adequately managed).

Phase 3: Defined – associated with moderate risk and fair user access, this phase includes improved quality and reduced security risks as processes become more proactive and standardized across business units and target systems.

Phase 4: Managed – in this stage, risk is lower, and users have faster, more seamless access, with automation in place to create significant IT cost and end-user time-savings.

Phase 5: Optimized – here, organizations are at the lowest risk and deliver optimal user access, where security is implemented and managed as part of the user workflow (not in addition to it).


1
PHASE 1
Initial
2
PHASE 2
Developing
3
PHASE 3
Defined
4
PHASE 4
Managed
5
PHASE 5
Optimized
User access
Identity management
Peak user access
Security is implemented and managed as part of the user workflow, not in addition to it
High user access
Just-in-time access; seamless mobile workflows; quantifiable business value
Fair user access
Access to resources flex as roles do; secure remote work is possible
Low user access
Day-one access to birth-right applications
Poor user access
Workflows are time consuming and inefficient; delayed access; manual communication processes
Disparate ID providers
Transformed to central system
Common ID repository
Simple ID federation
Authoritative federated ID provider
High risk
Ad hoc, manual, and siloed; no automation
High risk
Basic IT processes, critical application coverage
Moderate risk
Some automation, proactive and standardized
Low risk
Automation ramps, formal processes
Lowest risk
Full automation, continuous role optimization
Security and compliance

Assessing your digital identity maturity

Digital identity is the control plane that must be managed and secured. Assess the effectiveness of your current strategy across the four pillars of identity and access management, and find out which phase your organization aligns to on the Digital Identity Maturity Model.

Designed to collect feedback on your current-state processes and tools, the Imprivata Digital Identity Maturity Assessment is a robust, interactive tool that will help you evaluate your organization's maturity level. When finished, you'll receive a custom report with insights to achieve a comprehensive strategy that optimizes user access, security, and compliance.

To get started, contact Imprivata or take the Digital Identity Maturity Assessment at https://www.imprivata.com/assess

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com