DIT Identity & Access Management Solutions

Addressing the challenges of rapidly evolving, advanced persistent threats, compliance, legacy complexity and the demands for effective, enterprise IAM business solutions

ABOUT DIT

Distributed Information Technologies, Inc. (DIT) delivers industry-leading advisory, engineering and integration services to effectively configure and support Identity & Access Management (IAM) solutions

DIT is an authorized software solutions partner with: CyberArk, RSA, IBM, Omada, Oracle, Micro Focus NetIQ and ForgeRock.

Strategic Planning
Assessments
Audits & Compliance
Gap Analyses
Roadmap & Investments
Technology Consolidation
Maturity & Priorities
Validation & Certification
Rationale & Justification

Enterprise IAM Business Solutions

Contact Information:

Ray Brisbane
(571) 483-2735
rbrisbane@dtec.com

www.dtec.com

Overview

Identity and Access Management is a discipline aimed at ensuring that all users and devices are properly identified, that their affiliation to an organization is understood and that they have proper access to information assets.
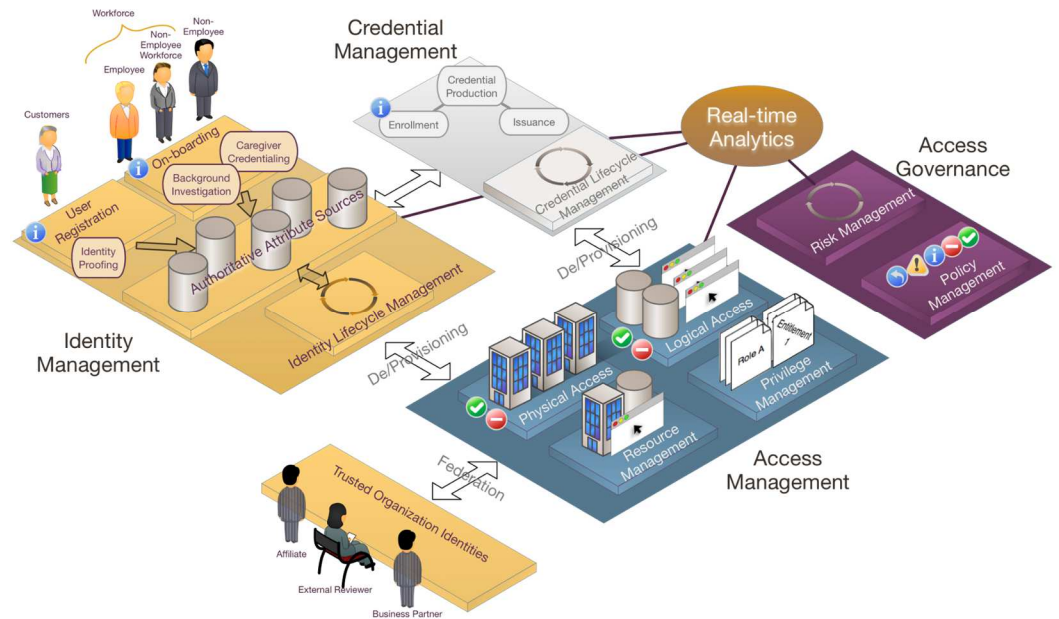
Threats and risks inevitably arise from the failure of an organization to put into place policies, processes and technologies that effectively execute this discipline.

Wherever policy definition and enforcement are not centralized; workflow and notification processes are not unified; or the creation, modification and termination of accounts are manually fulfilled by various teams; the impact is often a significant difficulty in assessing who has access to what across vast ecosystems. Manual, disjointed processes lead to errors, productivity loss and significant confusion surrounding credential lifecycle management.

Compliance requirements, and the associated audit process validations and remedies, compound the detrimental impact. Sarbanes-Oxley (SOX) and Payment Card Industry Data Security Standard (PCI DSS) affect virtually every industry. HIPAA, FISMA, the NIST Security Lifecycle, and the Critical Infrastructure Protection Standards, directly affect healthcare, government and virtually every industrial sector.

Additional complexity caused by legacy technologies, privileged accounts, cloud migration, next generation devices, federated interoperability and operational technologies, further compound the challenges of Identity & Access Management.

Solution

Implementing cohesive, centralized policy interaction, with credentialing integrity and efficiency via automation, is the cornerstone of effective Identity & Access Management. The resulting benefits include: an increased security posture, regulatory compliance, decreased administrative costs, and a competitive advantage through facilitated business.

IAM Capabilities
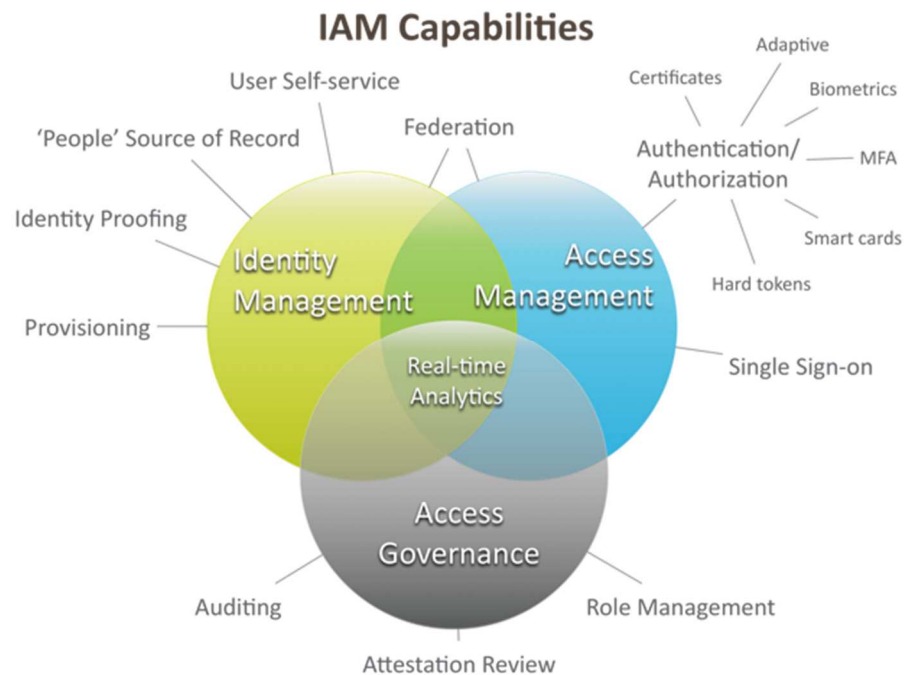
- Provide enterprise-wide visibility into who has access to which information resources, how they got it, who approved it and whether it is appropriate based on their business relationship with the organization

- Automate the monitoring, reporting, certification, exception handling and remediation of user entitlements and roles

- Enable a comprehensive and continuous role lifecycle management approach for governing user access, providing auditable proof of compliance

- Provide an effective, business-relevant process for requesting access and orchestrates the processes associated with access fulfillment (provisioning) and change management

- Help organizations establish efficient business processes around employee lifecycle events (joining the organization, changing roles and leaving the organization), with automated analysis and enforcement of access policies

- Suggest entitlements for new and existing users based on similar users' attributes and job roles

- Hide "off-limits" entitlements for certain sensitive entitlements that users should not be able to request or obtain

- Provide a single, centralized, business-user friendly system by which end users can request access and which enforces policies and approval processes