



# 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*

## Public Sectors



Today's Public Sector leaders are faced with many complex challenges relating to their information and operational technologies management; the inherent demands for effective cybersecurity; protection of critical infrastructure; the challenges of establishing, and sustaining, interoperability with federated partner organizations; and protecting their operational technologies. These sectors include:

- State/Local Government
  - Public Housing, Infrastructure, Transportation, Utilities, etc.)
  - Criminal Justice (police, courts, etc.)
  - Education
- Higher Education
- Not-for-Profit Healthcare & Healthcare Exchanges
- Associations
- Non-Profit Organizations

Managing the information technology systems required to conduct business; mitigating the constantly evolving cybersecurity risks; adhering to laws and regulations that demand compliance; and responding to audits in the context of this landscape; demands leadership attention and partner support from expert, and experienced, industry best-practice resources.

DIT's Identity and Access Management solutions organization has been supporting enterprise identity and Access management solutions, to help organizations address the risks associated with unauthorized access to enterprise systems and data, for almost two decades. Our IAM Framework provides a proven model for supporting all aspects of analysis, strategy, and roadmap advisory services; in the context of business, risk and compliance drivers; legacy technologies; the industry's leading IAM software platforms; and the engineering know-how to plan, execute, and transform an organization's cybersecurity capabilities and maturity.

Of course, 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. The challenge for everyone is to be able to meet and exceed all cybersecurity-related business objectives, at the lowest possible costs.

DIT understands that effectively deployed IAM solutions deliver:

- Increased Security Posture
- Decreased Administrative Costs
- Regulatory Compliance and Lifecycle Audit Support
- Improved Competitive Advantage via Facilitated Business

### 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, EMC 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:

[info@dtec.com](mailto:info@dtec.com)  
(703) 524-3309

[www.dtec.com](http://www.dtec.com)



# DIT Identity & Access Management Solutions

## *Risks*

Industrial Sector organizations must leverage a Risk Management Framework and perform Risk Assessment on its information and operational technology management; and, cybersecurity policies, practices and technologies. Critical risk areas include:

- Financially Sensitive Applications
- Sensitive Data (proprietary, confidential)
- Sensitive Access (logical assets, physical assets, operational technologies)
- Platform Information Technologies (DoD)
- Records Management (personal, medical, supply chain, asset management)
- Anti-Fraud
- Internal Threats
- External Threats

Clearly, cybersecurity and IAM solutions play an essential role in establishing, executing and enforcing the disciplined policies and work processes required to mitigate risks. But therein lies an additional layer of risk. The needs of the business demand ever more-efficient access to the right information, at the right time, by the right people. How can we ensure that the strategy to trust and verify identities and their corresponding authentication and authorization right are effectively controlled? How do we ensure that our investments in IAM solutions are the right ones?

## *Solutions*

DIT takes a disciplined approach forged from performing well over one hundred IAM client engagements, across a variety of industry sectors (e.g. financial, retail, education, healthcare, industrial, government), over the past decade. Our advisory, engineering, and integrations services address:

- Risk Management Framework
- Compliance and Audits
- Identity Lifecycle Management
- Access Controls Lifecycle Management
- IAM Technology Framework
- IAM Program Decision Support

Our IAM teams and resources are equipped to help organizations with virtually any aspect of the IAM lifecycle – from assessment of the state and maturity of your IAM-related policies, processes and technologies; to developing a prioritized road map and plan to address gaps in capability and vulnerability; to ensuring that the software tools and technologies are effectively deployed in support of the organizations' objectives.

Enterprise IAM Business  
Solutions

**Contact Information:**  
info@dttec.com  
(703) 524-3309

www.dttec.com

# DIT Identity & Access Management Solutions



## Challenges

Threats and risks inevitably arise from the failure of an organization to put into place policies, processes, and technologies that effectively execute this discipline. Many factors contribute to this:

- Policy definition and enforcement are not centralized
- Workflow and notification processes are not unified
- Creation, modification, and termination of accounts are manually fulfilled by various teams
- Difficulty in assessing who has access to what across vast ecosystems
- Multiple silos of IAM administration throughout the organization
- Errors, productivity loss, and significant confusion surrounding credential lifecycle management
- Privileged Access Management
- Compliance and audit requirements
- Legacy technologies, managed services, Cloud, and BYOD
- Federated Interoperability
- Operational Technologies (BAS, SCADA, PCAMS, Industrial Control Systems, etc.)
- Events such as acquisitions, divestures, partnerships, and reorganizations

## Compliance

Public Sector organizations must adhere to applicable laws and regulations addressing compliance. Specific compliance requirements include:

- Gramm-Leach-Bliley Act (GLB) Act
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Health Insurance Portability and Accountability Act (HIPAA)
- HSPD-7 (Critical Infrastructure Identification, Prioritization & Protection - 16 Sectors)
- HSPD-12 (Identity Management)
- ISO 27002
- NIST SP 800-53 Revision 4
- North American Electric Reliability Corp. (NERC) standards
- Payment Card Industry - Data Security Standard (PCI-DSS)
  - Establishes requirements for merchants who store, process and transmit cardholder data
  - All systems must be identified
  - Access to cardholder data limited to a business need-to-know
  - Each person with a computer must have a unique ID
  - Access to network resources and cardholder data must be tracked and monitored

DIT has the experience to ensure that your organization's IAM policies, workflows and validations effectively meet all relevant, regulatory compliance requirements; and, that the administrative and operational overhead costs to conduct and respond to compliance audits are substantially reduced as a result of centralized management and automation.



CYBERARK®



FORGEROCK™



# DIT Identity & Access Management Solutions

## Software Solutions

DIT is an authorized partner deploying the leading Identity and Access Management software platforms available. Each of these vendors' IAM software tools address a specific range of capabilities, and lifecycle configuration management requirements, that are world class leaders in delivering IAM capabilities that best support environments with unique challenges and characteristics. Our partners include:

- CyberArk Privileged Access Management
- RSA Via Lifecycle and Governance
- Omada Identity Suite for Identity & Access Governance
- Oracle Identity and Access Management Solutions
- Micro Focus Net IQ Identity and Access Management
- ForgeRock Identity Platform

These proven software platforms provide the opportunity to effectively rationalize, consolidate, and centralize the technology framework for enterprise IAM.

DIT is unique in that our staff applies skills in advisory services, in the context of your organizational requirements, your legacy technology landscape, and the capabilities of the leading IAM software platforms, to provide strategy and roadmap guidance; and, has the engineering expertise and experience to understand exactly what it will take to effectively configure the target landscape.

## Best Practices, Value Impact, and Return on Investment (ROI)

DIT helps organizations gain a clear understanding of the value of leveraging these platform capabilities and the priorities and options for deployment. In virtually every case, the reduction in administrative costs substantially outweighs the investment costs for change and support. Examples of focus areas include:

- Automation of Manual and Semi-Automated Processes
- Centralized Policy Definition and Enforcement
- Compliance and Audits Lifecycle Management
- Unified Workflow and Notification Processes/Services
- Enterprise IAM Visibility, Monitoring, and Reporting
- Enterprise IAM Organizational Alignment and Administrative Costs
- Annual License Fees, Capital Investments, Operational Expenses, and Other Expenditures

DIT offers Healthcare Sector entities the ability to rapidly review the current Identity & Access Management landscape, in order to support effective strategies, priorities and plans. We help our clients to better understand and determine the projected value impact and return on investment, that is essential in forming intelligent IAM investment decisions to be made going forward – and we understand specifically what it's going to take how to get the job done.

Please contact us at ([info@dttec.com](mailto:info@dttec.com)) or call (703) 524-3309 x2735 to gain further information or to speak with an IAM solutions consultant.

Enterprise IAM Business  
Solutions

### Contact Information

Kabir Kamboh  
Director, Business  
Development  
[kkamboh@dttec.com](mailto:kkamboh@dttec.com)  
(571) 483-2740

Ray Brisbane  
Cybersecurity and Asset  
Management Specialist  
[rbrisbane@dttec.com](mailto:rbrisbane@dttec.com)  
(571) 483-2735

[www.dttec.com](http://www.dttec.com)