# MERON

# PIAM+

## Banking on a Trusted Partner

## Financial Sector

### Executive Summary

In the fast-paced and highly regulated environment of global banking, effective and secure management of physical access to facilities is crucial. Meron's robust Physical Identity and Access Management (PIAM) solution can streamline and automate the hire-to-retire access process, ensure compliance with financial market regulations, enhance security through auditing, detecting insider threats, and implement access governance. Additionally, introducing the benefits of self-service, access approval, reporting, and dashboarding features. By adopting Meron's PIAM+ solution, banks can achieve safer, secure, productive, automated, and fully compliant workspaces.

### Introduction

The banking industry faces unique challenges in managing physical access to facilities, including branches, data centers, and corporate offices. These challenges are compounded by stringent regulatory requirements aimed at ensuring security and protecting sensitive information. Traditional methods of access management are often manual, inefficient, and prone to errors. A comprehensive Meron PIAM+ solution offers a modern approach to addressing these challenges, providing banks with the tools to automate and streamline their physical access management processes

### Key Capabilities:

**Workforce Hire to Retire – Identity & Access Lifecycle**

- **Onboarding** - From the moment an employee is hired, the Meron PIAM+ system can automatically assign the appropriate access levels based on their role, department, and location. This eliminates the need for manual intervention, reducing the risk of human error and ensuring that employees have the access they need from day one
- **Access Changes** - As employees move within the organization, whether through promotions, transfers, or role changes, their access needs will evolve. The Meron PIAM+ solution will seamlessly manage these changes, automatically updating access permissions to reflect new responsibilities and locations. This dynamic approach ensures that employees always have the correct access while minimizing the administrative burden on the security team
- **Secure Terminations** - When an employee leaves the organization, timely and secure access termination is critical to maintaining security. Meron PIAM+ solution will automate the deactivation of access credentials, ensuring that former employees can no longer access bank facilities. This proactive approach helps prevent unauthorized access and protects sensitive information.

**Self-Service Access Approvals**

- **Self Service Portal -** Empower workforce to manage their own access requests. Meron PIAM+'s user-friendly platform allows users to request access to specific areas, update their credentials, and track the status of their requests, thereby reducing the workload on the security team and improving efficiency.
- **Secure, Flexible Access** - Streamlined access approval workflow, ensuring that all access requests are properly vetted and approved by the appropriate authorities. This workflow can be customized to reflect the organization's specific policies and procedures, ensuring that access is granted based on predefined criteria and minimizing the risk of unauthorized access.

**Access Governance**

- **Role Based Access Control** - Employees only have access to the areas and resources necessary for their job functions. This principle of least privilege reduces the risk of insider threats by limiting access to sensitive areas and information..
- **Continuous Proactive Policy & Rule Enforcement** - Support robust access governance by enforcing policies, rules and standardizing access controls across the organization. This ensures that access rights are consistently applied and monitored, reducing the risk of policy violations and unauthorized access.
- **Access Attestations** – Set & Forget Access & Area Owner Attestations for scheduled (time based), and event based (Transfers, LOA, etc.)

**Measuring What Matters**

- **Advanced Reporting** - Detailed insights into access activities, security incidents, and compliance status. These reports can be customized & Scheduled to meet the specific needs of the organization, enabling security teams to make informed decisions and take proactive measures
- **Comprehensive Auditing** - Track and record all access events (Cradle to Grave), making it easier to identify and investigate suspicious activities. Regular audits help ensure that security protocols are being followed and provide a clear trail of evidence in the event of an incident.
- **Intelligent Dashboards -** Real-time, visual representation of key metrics, **risks**, and performance indicators. These dashboards provide an at-a-glance overview of access events, security incidents, and **compliance** status, enabling security teams to quickly identify trends, monitor performance, and address any issues.

**Predictably Consistent Enablement**

# MERON

# PIAM+

## Banking on a Trusted Partner

## Financial Sector *(contd.)*

### Key Capabilities *(contd.)*:

**Detecting Insider Threat –** Real Time Monitoring & Alerts capabilities that can detect unusual access patterns indicative of insider threats. By leveraging advanced analytics and machine learning, the system can flag potential security breaches and alert the security team to investigate further. This proactive approach helps mitigate risks and prevent unauthorized access.

**Visitor Management -** Streamline visitor management by automating the registration and credentialing process, banks can ensure that visitors are granted access only to authorized areas and for specified time periods. Not only enhancing security but also provide a clear record of all visitors, which is essential for compliance purposes

**Regulatory Compliance**

- **Enhanced Security and Auditability -** Financial market regulations require banks to maintain strict controls over physical access to their facilities. Meron solution provides enhanced security features, such as real-time monitoring, access logs, and audit trails. These capabilities ensure that banks can **demonstrate compliance** with regulatory requirements and quickly identify and address any security incidents.
- **Regular Compliance Reporting** - Generate detailed compliance reports, providing a comprehensive overview of access activities and security measures. These reports can be tailored to meet specific regulatory requirements, ensuring that **banks have the documentation** they need to demonstrate compliance during audits and inspections

**Sarbanes-Oxley Act (SOX)**

**Requirement -** SOX mandates that organizations maintain robust internal controls and accurate financial records

**MERON PIAM+** - Ensures that access to financial records and critical systems is strictly controlled and monitored. It provides detailed audit trails and logs of access events, which are essential for demonstrating compliance during audits.

**Basel II**

**Requirement -** Basel II sets international standards for banking regulations, including risk management and internal controls

**MERON PIAM+** - By automating access provisioning and ensuring that access controls are consistently applied across the organization, helps banks meet the risk management and internal control requirements of Basel II..

**Gramm-Leach-Bliley Act (GLBA)**

**Requirement -** GLBA requires financial institutions to protect the security and confidentiality of customer information

**MERON PIAM+** - By managing physical access to areas where sensitive customer data is stored, Meron PIAM+ solution ensures that only authorized personnel can access this information. It also provides real-time monitoring and alerts for any unauthorized access attempts.

**Payment Card Industry Data Security Standard (PCI DSS)**

**Requirement -** PCI DSS requires organizations to implement strong access control measures to protect cardholder data

**MERON PIAM+** - Integrates with access control systems to ensure that only authorized individuals have access to areas where cardholder data is processed or stored. It also provides detailed reporting and compliance documentation to meet PCI DSS requirements

**Federal Information Security Management Act (FISMA)**

**Requirement -** FISMA requires federal agencies and contractors to develop, document, and implement an information security program.

**MERON PIAM+** - Comply with FISMA by providing comprehensive access management, regular audits, and real-time monitoring of access to sensitive information

**Customs-Trade Partnership Against Terrorism (C-TPAT)**

**Requirement -** C-TPAT requires organizations to implement security measures to prevent unauthorized access to facilities

**MERON PIAM+** - Ensure that all visitors/contractor are properly registered, escorted, and monitored while on-site, meeting the access control requirements of C-TPAT

**International Traffic in Arms Regulations (ITAR)**

**Requirement -** ITAR requires strict control over access to defense-related information and technologies..

**MERON PIAM+** - Solution can manage access to sensitive areas and information, ensuring that only authorized personnel with the necessary clearances can access these resources

**Prioritizing with Self Healing**

# MERON

# PIAM+

Banking on a Trusted Partner

## Financial Sector *(contd.)*

### Benefits – Smarter Way to Manage Physical Identity & Access credentials

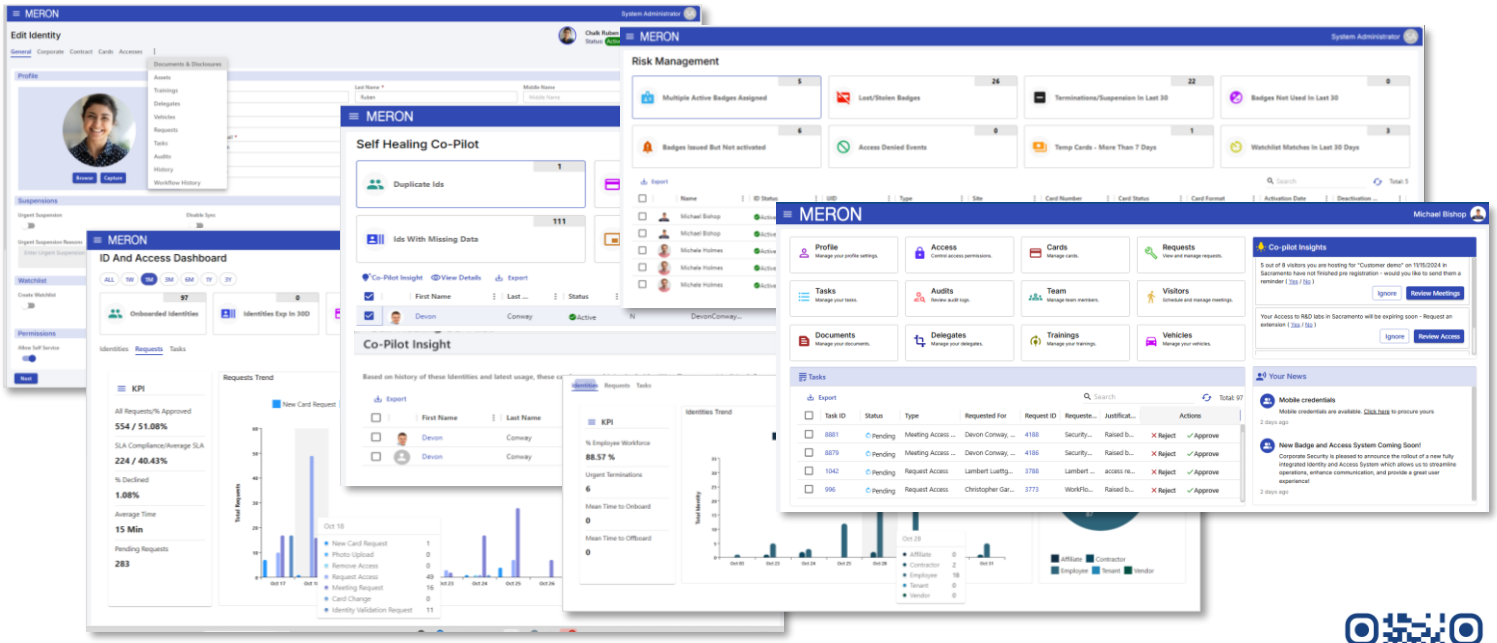
**Enhancing Security -** Through real-time monitoring, auditing, and role-based access control, the Meron PIAM+ solution ensures that only authorized individuals have access to bank facilities.

**Improving Productivity -** By automating access provisioning, changes, and termination, employees can quickly and efficiently access the areas they need, reducing downtime and increasing productivity.

**Facilitating Automation -** The Meron PIAM+ solution automates various access management tasks, reducing the administrative burden on security teams and allowing them to focus on more strategic activities.

**Ensuring Compliance -** With comprehensive reporting, auditing, and compliance features, banks can easily meet regulatory requirements and demonstrate their commitment to security and compliance.

**Promoting a Secure Environment -** By detecting insider threats and enforcing access governance, the Meron PIAM+ solution helps create a secure work environment, protecting both employees and sensitive information.




Scan QR Code to Learn More